VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

IMPLEMENTACE ZVOLENÉ TECHNOLOGIE PRO SPRÁVU SÍTĚ
IMPLEMENTATION OF SELECTED TECHNOLOGY FOR NETWORK MANAGEMENT

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE Bc. Bianka Fábryová
AUTHOR

VEDOUCÍ PRÁCE Ing. Viktor Ondrák, Ph.D.
SUPERVISOR

BRNO 2022

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Studentka:	**Bc. Bianka Fábryová**
Vedoucí práce:	**Ing. Viktor Ondrák, Ph.D.**
Akademický rok:	2021/22
Studijní program:	Informační management

Garant studijního programu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Implementace zvolené technologie pro správu sítě

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Navrhnout implementaci systému řízení sítě.

Základní literární prameny:

BIGELOW, S. J. Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů. 1. vydání. Praha: Computer Press, 2004. ISBN 80-251-0178-9.

CLEMM, A. Network management fundamentals. 1. vydání. Indianapolis: Cisco Press, 2007. ISBN 1-58720-137-2.

HORÁK, J. a M. KERŠLÁGER. Počítačové sítě pro začínající správce. 5. vydání. Brno: Computer Press, 2011. ISBN 978-80-251-3176-3.

MAURO, D. R. a K. SCHMIDT. Essential SNMP: Help for System and Network Administrators. 2. vydání. Sebastopol: O'Reilly Media, 2005. ISBN 0-596-00840-6.

TUNSTALL, C. a G. COLE. Developing WMI Solutions: A Guide to Windows Management Instrumentation. 1. vydání. Boston: Pearson Education, Inc, 2002. ISBN 0-201-61613-0.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2021/22

V Brně dne 28.2.2022

L. S.

doc. Ing. Miloš Koch, CSc. garant	doc. Ing. Vojtěch Bartoš, Ph.D. děkan

Abstrakt

Táto práca sa venuje tvorbe návrhu implementácie vybranej technológie pre management počítačovej siete v konkrétnej spoločnosti. Úvodná časť práce sa sústredí na zhrnutie teoretických východísk z danej oblasti. Ďalšia časť práce je zameraná na analýzu súčasného stavu riadenia siete v spoločnosti a na možnosti vhodného riešenia správy siete. V praktickej časti je na základe aplikácie teoretických poznatkov formulovaný návrh implementácie zvolenej technológie vrátane technických, manažérskych a ekonomických aspektov, ktoré je nutné pri implementácii posúdiť.

Kľúčové slová

SNMP, MIB, WMI, NetFlow, monitoring siete, bezpečnostná politika, management počítačovej siete, PRTG

Abstract

This thesis deals with proposal of implementation of chosen technology for computer network management within a particular company. The introductory part of this thesis focuses on a summary of theoretical background in the field. The next part of this thesis is focused on the analysis of the current state of network management in the company and the possibilities of a suitable network management solution. In the practical part, based on the application of theoretical knowledge, there is formulated a proposal for the implementation of the selected technology including technical, managerial and economic aspects that must be assessed during implementation.

Keywords

SNMP, MIB, WMI, NetFlow, network monitoring, security policy, computer network management, PRTG

Bibliografická citácia

FÁBRYOVÁ, Bianka. *Implementace zvolené technologie pro správu sítě* [online]. Brno, 2022 [cit. 2022-05-06]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/139279. Diplomová práca. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedúci práce Viktor Ondrák.

Čestné prehlásenie

Prehlasujem, že predložená diplomová práca je pôvodná a spracovala som ju samostatne. Prehlasujem, že citácia použitých prameňov je úplná, že som vo svojej práci neporušila autorské práva (v zmysle Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brne dňa 6. mája 2022 .....

podpis autora

Poďakovanie

Ďakujem vedúcemu diplomovej práce Ing. Viktorovi Ondrákovi, Ph.D. za odborné vedenie, cenné rady a ústretový prístup pri písaní tejto práce. Rovnako sa chcem poďakovať svojim rodičom za ich podporu pri štúdiu.

Obsah

ÚVOD

S neustálym rozvojom informačných technológií sa čoraz viac procesov presúva do virtuálneho priestoru, s čím narastajú aj nároky kladené na efektivitu a bezpečnosť počítačových sietí. Správa siete je pomerne náročnou činnosťou ako na čas, tak aj na samotný dohľad a údržbu všetkých technológií. Takáto práca zahŕňa monitoring technických prostriedkov, serverov, počítačov, sieťových prvkov, operačných systémov či ďalších zariadení, ako aj monitoring činnosti používateľov v sieti. Je preto prirodzené, že v stredných a veľkých podnikoch nemôže takúto úlohu zastávať malé IT oddelenie, ktoré zväčša podniky majú. Kontrola každého počítača vo väčšej sieti by zabrala nepomerne menej času, ak by mohla byť centralizovaná na jednom mieste a ak by technické oddelenie nemuselo kontrolné činnosti robiť osobne.

Úlohou správy siete je vytvoriť správcom sietí systém kontroly za dosiahnutia definovanej úrovne bezpečnosti. Technológie pre správu siete preto umožňujú udržiavanie kontroly, poskytujú prehľad o zariadeniach v sieti a taktiež umožňujú vykonávať niektoré úlohy na diaľku bez nutnej fyzickej kontroly.

Predovšetkým v stredných a veľkých podnikoch sa preto riadenie počítačovej siete v dnešnej dobe ukazuje ako nevyhnuteľné, zvlášť v spoločnostiach, ktoré by efektívnym riadením mohli získať množstvo benefitov. Jedná sa predovšetkým o znižovanie času detekcie chýb, zrýchlenie opráv, detekciu výpadkov či útokov a iných hrozieb. Vďaka technológiám, ktoré sú určené na správu siete, môžeme monitorovať siete tak, aby sme docielili efektivitu procesov a bezpečnosť.

Táto diplomová práca sa zaoberá implementáciou vybranej technológie pre management počítačovej siete v konkrétnej spoločnosti. Prvá časť práce popisuje teoretické východiská. Zameriava sa na popis významu správy siete, na model a oblasti správy, ale predovšetkým vysvetľuje technické aspekty monitoringu.

Praktická časť práce obsahuje analýzu súčasného stavu managementu siete vo vybranej spoločnosti, ako aj popis, porovnanie a výber jednej z možných technológií, ktoré by mohli byť použité pre správu siete.

Na základe analýzy a teoretických poznatkov je následne vytvorený návrh implementácie zvolenej technológie. Súčasťou návrhu je taktiež manažérske a ekonomické zhodnotenie, ako aj bezpečnostné politiky.

1 VYMEDZENIE PROBLÉMU A CIEĽ PRÁCE

Práca sa zameriava na problematiku správy počítačovej siete v konkrétnom podniku a implementáciu technológie pre správu siete.

Cieľom tejto práce je vytvorenie komplexného návrhu implementácie vybranej technológie pre spoločnosť. Medzi dielčie ciele patrí návrh konfigurácie technológie, návrh smerníc a zhodnotenie technických, manažérskych a ekonomických aspektov.

Teoretická báza, ako aj analýza súčasného stavu správy siete slúži ako východisko pre tvorbu návrhu. Návrh reflektuje úroveň bezpečnosti, ktorá vyvstáva z činnosti spoločnosti, s ohľadom na primerané ekonomické, technické a personálne náklady. Medzi zdroje, z ktorých táto práca čerpá, patrí predovšetkým odborná literatúra, doplnená o technické normy, produktové informácie jednotlivých technológií, konzultácie so zamestnancami podniku a o vlastné znalosti.

2 TEORETICKÉ VÝCHODISKÁ PRÁCE

Táto práca pojednáva o implementácii managementu počítačovej siete. Na úvod je preto potrebné vymedziť dôležité termíny z tejto oblasti. Nasledujúce podkapitoly sa preto venujú vysvetleniu pojmov, ako sú počítačová sieť a jej zložky, správa siete a jej význam, či jednotlivé protokoly, ktoré sú používané pre správu siete. Záver kapitoly je venovaný popisu a kategorizácii nástrojov pre správu siete.

2.1 Počítačová sieť

Počítačovú sieť môžeme definovať ako spojenie medzi dvoma alebo viacerými počítačmi, ktoré komunikujú prostredníctvom protokolov, a ktorých úlohou je vzájomná výmena dát.

Počítačová sieť sa z hľadiska prvkov, ktoré ju tvoria, delí na sieťovú infraštruktúru a koncové uzly. Sieťová infraštruktúra sa skladá z pasívnej vrstvy a aktívnych prvkov. Pasívna vrstva zodpovedá za prenos dát a je tvorená prenosovým prostredím, káblovými trasami, či rozvádzačmi. Prenos môže byť drôtový, cez metalickú alebo optickú kabeláž, alebo realizovaný bezdrôtovým prenosovým médiom. Aktívne prvky ako router, bridge, switch, hub alebo firewall umožňujú riadenie prenosu dát. Koncovými uzlami môžu byť počítače, tlačiarne, telefóny, smart zariadenia alebo iné zariadenia, ktoré je možné k sieti pripojiť [1].

Pri snahe o klasifikáciu sietí musíme rozlišovať rôzne aspekty, ako napríklad rozsah, prístup, využitie, či spôsob prepojenia prvkov v sieti a mnohé ďalšie. Konkrétna sieť môže byť zaradená vo viacerých kategóriách naraz [2].

Podľa rozsahu rozlišujeme osobnú sieť PAN (*Personal Area Network*), ktorá zväčša slúži jednému používateľovi na prepojenie počítača a periférnych zariadení. Je určená na veľmi krátke vzdialenosti. Väčšia sieť, ktorá môže byť jednoduchá (sieť medzi dvoma počítačmi), ale môže tiež pokrývať domácnosť, kanceláriu, poschodie, prípadne aj budovu, sa nazýva lokálna sieť LAN (*Local Area Network*). Naproti lokálnej sieti stojí rozľahlá sieť WAN (*Wide Area Network*), ktorá vznikne z viacerých navzájom prepojených sietí LAN. Je určená pre veľké vzdialenosti a slúži predovšetkým pre účely komunikácie. Jej typickým príkladom je internet. Okrem týchto typov rozoznávame aj

sieť MAN (*Metropolitan Area Network*), ktorá leží na pomedzí sietí LAN a WAN. Jedná sa o sieť pre univerzitné alebo mestské využitie [2].

Siete ďalej kategorizujeme podľa topológie. Topológia popisuje vzájomné usporiadanie jednotlivých komunikačných uzlov siete. Vzhľadom na rozmanitosť usporiadania rozpoznávame tri základné topológie, a to topológiu *bus* – zbernica, *ring* – kruh a *star* – topológiu hviezdy, prípadne ich kombinácie, pričom každá z týchto topológií má rozličné nároky a ponúka rôznu funkčnosť. Taktiež rozlišujeme fyzickú a logickú topológiu, teda reálne fyzické usporiadanie a logické prepojenie, ktoré sa môže líšiť od fyzického prepojenia komunikačných uzlov [2].

Siete môžeme kategorizovať aj z hľadiska spracovania informácií na architektúru *klient/server* a na architektúru *peer-to-peer*. Pri architektúre *klient/server* prevádza spracovanie dát serverový systém, ktorý ich následne poskytuje klientom. Táto architektúra je najrozšírenejšia a nájdeme ju v sieťových aplikáciách, akými sú databázy, web stránky či elektronická pošta. Na strane servera beží serverový softvér a u klienta zase klientsky softvér, pričom vzájomná komunikácia prebieha cez odpovedajúce protokoly. Architektúra *peer-to-peer*, alebo sieť typu rovný s rovným, neobsahuje ani servery, ani klientov, ale komunikačné uzly, ktoré plnia úlohy ako servera, tak aj klienta a sú rovnocenné. Každý uzol teda môže služby ako poskytovať, tak aj požadovať. Táto architektúra sa vyskytuje prevažne u veľmi malých jednoúčelových sietí [2].

2.2 Správa počítačovej siete

Správa počítačovej siete sa v minulosti zameriavala prevažne na chyby a vady hardvéru. Časom sa však hardvér čoraz viac technologicky zdokonalil a dnes sa takéto chyby vyskytujú omnoho menej ako v minulosti. O to viac sa však pri bežnej práci stretávame s problémami, ktoré sú spôsobené zvyšujúcim sa počtom softvérových nástrojov a zvyšujúcimi sa nárokmi na spoľahlivosť a výkon samotnej siete. Keďže je v dnešnej dobe sieť pracovným nástrojom, bez ktorého by väčšina spoločností nemohla fungovať, je potrebné, aby bola udržiavaná a adekvátne kontrolovaná. Pri väčších sieťach je teda nutné zabezpečiť správu zariadení v sieti, nakoľko v prípade prepojenia veľkého počtu zariadení sa ich správa stáva neprehľadnou a je problém ich všetky fyzicky kontrolovať, a preto sa nezaobídeme bez centralizovanej vzdialenej správy týchto zariadení [3].

Správu siete môžeme širšie definovať ako proces riadenia siete, ktorého cieľom je dosiahnutie maximálneho výkonu a produktivity siete. Takto definovaná správa siete je obmedzená zvolenou platformou a úrovňou jej implementácie v spoločnosti [4].

2.2.1 Význam správy siete

Správa siete môže byť náročná z hľadiska finančných, ale aj personálnych nákladov. Vzhľadom k tomuto faktu je nutné popísať, prečo je správa siete dôležitá. Správca siete musí vykonávať množstvo činností, medzi ktoré patrí napríklad:

- konfigurácia a inštalácia nových pracovných staníc,
- aktualizácia pracovných staníc a serverov,
- aktualizácia operačných systémov,
- aktualizácia ovládačov,
- inštalácia a aktualizácia antivírusových nástrojov,
- inštalácia a konfigurácia rozbočovačov, prepínačov a smerovačov,
- inštalácia novej a výmena poškodenej kabeláže,
- vytváranie a overovanie záloh,
- tvorba záznamov o zariadeniach, o ich konfigurácii, o opravách,
- pravidelné aktualizovanie záznamov o zariadeniach, ktoré odrážajú všetky zmeny a aktualizácie,
- evidencia výstrah a upozornení, ich ohlasovanie a riešenie,
- pravidelný monitoring a vyhodnocovanie výkonu siete [4].

Pri rozrastajúcich sa sieťach a zvyšujúcich sa nárokoch a potrebách používateľov siete by spoločnosti museli vynakladať veľké náklady na IT oddelenie, ktoré by rozhodne presahovali náklady na technológiu, ktorá by sieť monitorovala automatizovane. Z tohto dôvodu sa dnes využívajú technológie pre monitorovanie, údržbu a riešenie problémov v sieti [4].

2.2.2 Sieťový model správy OSI

Väčšina štandardov a termínov týkajúcich sa správy siete vznikla v súvislosti s vytváraním heterogénnych sietí pre vojenský a telefónny priemysel. Od 70. rokov 20. storočia, začali pracovné skupiny telekomunikačného priemyslu snahy o štandardizáciu technológií, čo dalo vzniku skupine ITU-T (*International Telecommunication Union Telecommunication Standardization Sector*). Táto skupina vytvorila model pre správu siete ISO *Telecommunications Management Network* (TMN). Rovnako ako referenčný model, aj model správy siete má byť otvoreným systémom, pričom každá oblasť tohto modelu má využívať vlastnú skupinu protokolov. Funkčný model správy sa označuje tiež skratkou FCAPS, kvôli začiatočným písmenám anglických slov, ktoré označujú základné funkčné oblasti sieťového managementu:

- ***Fault*** (Problém) – správa porúch,
- ***Configuration*** (Konfigurácia) – správa konfigurácie,
- ***Accounting and Administration*** (Účtovanie) – účtovná a evidenčná správa,
- ***Performance*** (Výkon) – správa výkonu,
- ***Security*** (Bezpečnosť) – správa bezpečnosti [2].

Obrázok 1: Model FCAPS

(Zdroj: 5)

2.2.2.1 Správa porúch

Oblasť správy porúch zahŕňa riešenie porúch siete, problémov a detekciu chýb, ku ktorým dochádza v pracovných staniciach, v serveroch, prostriedkoch siete, akými sú napríklad NAS servery, tlačiarne, rozbočovače a prepínače, či rozvod káblov. Riešenie problémov obsahuje niekoľko krokov, ako rozpoznanie problému, identifikáciu a izolovanie zdroja problému, riešenie a opätovná skúška chodu siete. Niektoré technológie správy dopomôžu zodpovedným osobám čeliť širšiemu okruhu problémov efektívnejšie a rýchlejšie. Nástroj správy siete môže preverovať jednotlivé prvky siete v závislosti na stanovenej schéme a sledovať tak správnosť ich fungovania [4].

V prípade, že nejaký systém prestane fungovať správne, platforma pre správu dokáže detegovať konkrétne udalosti, ktoré sa spájajú s chybovými stavmi, alebo s definovanou množinou udalostí. Moderné operačné systémy a rovnako aj hardvér, desktopové počítače, sú riadené udalosťami, takže softvér sa nachádza v stave pohotovosti do momentu, kedy obdrží príkaz, na ktorý reaguje. Udalosti môžu byť klasifikované podľa typu a závažnosti a zachytávané selektívne. Udalosti sú protokolované zvyčajne v databázovom súbore, prípadne môžu byť odosielané po sieti protokolom, ako napríklad SNMP (*Simple Network Management Protocol*), alebo iným proprietárnym protokolom. Detekcia, izolácia a pochopenie udalosti je prvým krokom pri správe chýb [2].

Napríklad nástroj správy siete môže získať informácie o konkrétnom systéme, ako sú problémy napätia či teploty a automaticky môže vygenerovať hlásenia pre technika. Iné chyby, ktoré sú bežné, ako nedostatok miesta na disku, sú riešiteľné aj bez nutnosti ľudského zásahu [4].

Alarmy

Pri správe porúch je nevyhnutné, aby nástroje pre správu siete vytvárali alarmy, teda upozornenia na stav detegovanej chyby, ktoré je možné klasifikovať podľa typu a závažnosti. Platformy pre správu siete sú teda v podstate inou formou prehliadača udalostí, obohatené o rôzne filtre a pravidlá pre sledované typy udalostí. V prípade, že nejaké zariadenie alebo systémová funkcia odošle alarm, nazýva sa tento systém pasívnym systémom správy. Ak sa však periodicky platforma pre správu dopytuje spravovaných zariadení, napríklad na odozvu príkazu Ping, tak sa jedná o aktívny systém

pre správu. Funkcie systému pre správu siete môžu byť buď aktívne, pasívne, alebo obojaké [2].

Alarmy môžeme kategorizovať aj na digitálne alebo analógové. Digitálny alarm je dvojstavový binárny systém, ktorého stav sa ukladá v registri alarmu a používateľ je informovaný o výstupe v stanovenom formáte. Analógový alarm má vlastnosť s určitou hodnotou, ktorou môže byť ľubovoľné číslo z rozsahu, prípadne, ak nie je rozsah definovaný, môže to byť ľubovoľná hodnota v rozmedzí číselných miest podporovaných registrom alarmu. Analógové hodnoty sa zvyčajne používajú s metrikami výkonu, nakoľko môžu uvádzať mieru alebo veličinu, napríklad počet zahodených rámcov za sekundu alebo počet najbližších smerovačov odpovedajúcich na príkaz vyhľadávania [2].

Rozsah hodnôt alarmu môže vyzerať nasledovne:

- **Veľmi nízky**: 0 – 20%,
- **Nízky**: 20 – 35%,
- **Stredný**: 35 – 65%,
- **Vysoký**: 65 – 80%,
- **Veľmi vysoký**: 80 – 100% [2].

Alarmy označujú chyby, ktoré je nutné opraviť, a preto je potrebné, aby ich systém vedel ohlasovať používateľovi. K informovaniu o chybovom stave sa používa viacero metód. Chyba sa môže napríklad zobraziť v aplikácii grafického užívateľského rozhrania, alarm môže generovať udalosť SNMP, ktorá je následne odoslaná inej aplikácii. Alarm môže byť vložený do e-mailu, alebo môže byť používateľ informovaný napríklad cez textovú správu [2].

2.2.2.2 Správa konfigurácie

Správa konfigurácie zahŕňa správu aktív, inventarizáciu, provisioning služieb a siete, zisťovanie konfigurácie prvkov siete, nastavenie operačných systémov, nasádzanie softvéru, aplikácií, či správu balíčkov [2].

Konfigurácia každého zariadenia má veľký vplyv na fungovanie ako samotného zariadenia, tak aj siete ako celku. Sledovanie informácií o konfigurácii všetkých zariadení

môže byť problematické či už z hľadiska času, alebo úsilia potrebných ku kontrole, či prípadnej aktualizácii. Nástroje pre správu siete umožňujú zhromažďovanie takýchto údajov automatizovane, pričom niektoré sú schopné posudzovať konfiguráciu na základe špecifických vlastností hardvéru a softvéru. Keď je potrebné vykonať nejaké zmeny v konfigurácii, môžu byť jednoducho vykonané vzdialene prostredníctvom nástroja pre správu. Napríklad, ak je potrebné nainštalovať konkrétny softvér, ktorý vyžaduje aktualizáciu operačného systému, s platformou pre správu siete je možné jednoducho overiť jednotlivé verzie operačného systému bez toho, aby museli technici skontrolovať každý počítač fyzicky. Rovnako v prípade, že je dostupná nová verzia firmvéru pre konkrétne zariadenie, nástroj pre správu konfigurácie umožní zistiť aktuálnu verziu firmvéru prepínača bez toho, aby musel byť zisťovaný manuálne na zariadení tak, že prevedie dopyt priamo na prepínač [4].

2.2.2.3 Účtovná a evidenčná správa

Účtovná a evidenčná správa zahŕňa sledovanie využitia zdrojov jednotlivými používateľmi alebo procesmi, vytváranie reportov tohto sledovania, reguláciu prístupu ku zdrojom a optimalizáciu sieťových zdrojov [2].

Sieť poskytuje konečné množstvo zdrojov svojim používateľom. Samotná prevádzka siete, ako aj každé navýšenie zdrojov sú finančne náročné, a preto je potrebné kontrolovať, akým spôsobom je sieť využívaná. Platformy pre správu siete umožňujú vykonávať takúto kontrolu prostredníctvom nástrojov pre analýzu nákladov podľa kvantifikácie aktivít sieťových používateľov. Pre funkčný systém je najprv potrebné analyzovať skupiny a jednotlivcov, ktorí pristupujú k zdrojom, napríklad k serverom, aplikáciám, tlačiarňam a iným sieťovým prvkom, čím sa vytvorí vzor použitia týchto zdrojov. Na základe definície vzorov môže následne správca efektívnejšie plánovať ďalšie činnosti, ako napríklad aktualizácie. V prípade, že sa potom nejaký zdroj, napríklad konkrétny server, využíva veľkým počtom používateľov, čo znižuje jeho výkon pre ďalších užívateľov, môže sa učiniť rozhodnutie pre vyčlenenie ďalšieho servera na danú činnosť [4].

2.2.2.4 Správa výkonu

Správa výkonu je oblasť správy siete zaoberajúca sa zhromažďovaním meraných ukazovateľov o systéme a súčastiach siete, meraním výkonnosti a meraním zaťaženia prvkov v sieti, ako aj poskytovaním funkcií merania softvéru. Môže byť reaktívna a proaktívna. Reaktívna správa výkonu sa zameriava na reakcie na problémy. Proaktívna správa výkonu využíva simulačných metód, na základe ktorých sa plánujú zmeny v sieti (používa sa napríklad metóda *what if*) [2].

Platformy pre správu siete obsahujú nástroje pre zisťovanie činnosti a výkonu siete, ktoré umožňujú sledovať širokú škálu vlastností. Na základe odchýlok od základných hodnôt je potom možné identifikovať potenciálne problémy v sieti. Sledovaním týchto ukazovateľov bude môcť správca predvídať správanie siete a implementovať prostriedky pre elimináciu neležaného stavu, ako napríklad zaplnenie úložiska, alebo iné závažnejšie problémy výkonu siete [4].

2.2.2.5 Správa bezpečnosti

Správa bezpečnosti zahŕňa riadenie prístupu používateľov k zdrojom, prostredníctvom inštalácie modelu, ktorý umožňuje stanovovanie pravidiel ACL (*Access Control List*), sledovanie zásad, správu identity používateľov a systémov prostredníctvom vlastných funkcií, prípadne s využitím adresárových služieb a detekciu pokusov o neoprávnené akcie a reakcie na tieto pokusy [2]. Správa bezpečnosti teda napríklad umožní zistiť, ktorí používatelia pristupovali k citlivým súborom, alebo k súborom a zdrojom, na ktoré nemajú oprávnenie. Informácie o neúspešných pokusoch prihlásenia a iných činnostiach sú hlásené centrálne, a tak ich môže správca ihneď preskúmať [4].

2.3 Management IT služieb

Riadenie služieb informačných technológií ITSM (*Information Technology Service Management*) je výraz, ktorý označuje skutočnú prax riadenia a managementu služieb ICT, vrátane navrhovania, vytvárania a dodávania IT riešení. Organizácia, ktorá zavedie zásady ITSM, môže zosúladiť IT služby s obchodnými cieľmi, stratégiou, či finančnými a personálnymi požiadavkami, čím zefektívni ich poskytovanie.

Pre zavedenie ITSM v organizácii je možné použiť viacero zdrojov, ako normy, napríklad ISO 20000, či knižnicu ITIL, teda rámec, ktorý pozostáva z osvedčených postupov na zavádzanie ITSM v organizácii.

2.3.1 ISO/IEC 20000

Norma ISO/IEC 20000 je medzinárodným štandardom, ktorý definuje požiadavky na zriadenie, implementáciu, udržiavanie a kontinuálne zlepšovanie managementu IT služieb. Systém managementu služieb SMS (*Service Management System*), podporuje tiež správu životného cyklu služby skladajúceho sa z piatich etáp, ktorými sú plánovanie služby, jej návrh, prechod, dodávka a zlepšovanie. Rozhodnutie o zavedení managementu služieb musí byť strategickým rozhodnutím a musí vychádzať z cieľov spoločnosti. Dôraz je kladený na monitorovanie, meranie a preskúmavanie. Tieto procesy musia byť vykonávané pravidelne, musia byť zaznamenávané a vyhodnocované [6].

ITSM implementujeme podľa druhej časti normy ISO/IEC 20000-2:2018. Požiadavky pre implementáciu normy sú nasledovné:

1. **Kontext organizácie** – porozumenie organizácii a kontextu, porozumenie potrebám a očakávaniam zainteresovaných strán, určenie rozsahu SMS a vytvorenie SMS,
2. **Vedenie** – vedenie a záväzok, vytvorenie a komunikovanie politiky a roly, zodpovednosti a právomoci,
3. **Plánovanie** – opatrenia pre riešenie rizík a príležitostí, ciele managementu služieb a plán ich dosiahnutia,
4. **Podpora SMS** – zdroje, kompetencie, povedomie, komunikácia, dokumentované informácie a znalosti,
5. **Prevádzka SMS** – plánovanie a riadenie prevádzky, portfólio služieb, vzťahy a dohody, dopyt a ponuka, návrh, zostavenie a prechod služieb, riešenie, plnenie a zaistenie služieb,
6. **Hodnotenie výkonnosti** – monitorovanie, meranie, analýza a hodnotenie, interný audit, preskúmavanie vedením a predkladanie výkazov o službách,
7. **Zlepšovanie** – nezhoda a nápravné opatrenia a neustále zlepšovanie [7].

2.3.1.1 Management udalostí (Event management)

Udalosť (*Event*) môže byť definovaná ako akákoľvek zistiteľná zmena stavu, ktorá je významná pre poskytovanie IT služieb, či pre management IT infraštruktúry, a ktorá môže viesť k odchýlkam od chodu služby. Udalosti sú hlásené ako stavové správy, ktoré zvyčajne vytvára IT služba, konfiguračná položka, či monitorovací nástroj [6].

Správa udalostí je proces detekcie a kategorizácie udalostí. Tie môžeme deliť do troch skupín:

- **Informačná** (*Informational*) – udalosť, ktorá sa zaznamenáva pre ďalšie potreby,
- **Výstražná** (*Warning*) – udalosť, ktorá značí presiahnutie predom definovanej hodnoty,
- **Výnimočná** (*Exception*) – udalosť, ktorá značí neštandardný stav. Tento typ udalosti vyžaduje pohotovú reakciu [6].

Medzi hlavné ciele managementu udalostí patrí zodpovednosť za udalosti v priebehu ich životného cyklu, vrátane detekcie udalostí, posudzovania, vyhodnocovania a reagovania na udalosti. Zavedenie managementu udalostí by malo organizácii priniesť skrátenie doby trvania výpadkov IT služieb a predchádzanie výpadkov služieb, čo by malo viesť k zabezpečeniu dostupnosti služby a k zvyšovaniu spokojnosti používateľa. Automatizáciou operácií správy udalostí sa eliminuje použitie používateľov IT služieb, ako nástroja k ohlasovaniu udalostí. Dôjde k zvýšeniu efektivity a k uvoľneniu ľudských zdrojov pre inú prácu [6].

2.3.1.2 Management incidentov (Incident management)

Incident je neočakávané prerušenie služby, obmedzenie kvality služby alebo porucha konfiguračnej zložky, ktorá zatiaľ neovplyvnila IT službu [6].

Správa incidentov sa sústredí na skorú detekciu incidentov, zodpovedá za zaznamenávanie incidentov a za ich urýchlené riešenie. Proces riadenia incidentov sa zameriava na čo najrýchlejšie obnovenie služby tak, aby mal incident minimálny vplyv na fungovanie služby, ako aj minimálne finančné škody pre organizáciu. Incident

management tiež zaisťuje, aby dodávané služby napĺňali kvalitu podľa SLA (*Service Level Agreement*) [6].

2.3.2 ITIL

ITIL (*Information Technology Infrastructure Library*) je rámec obsahujúci odporučenia a osvedčené postupy vychádzajúce z praxe, ktorý slúži k zaisteniu efektívnej dodávky IT služieb. V súčasnosti je štandardom pre oblasť riadenia IT služieb. Knižnica ITIL sa delí na niekoľko častí. Jadro ITIL verzie 3 obsahuje 5 kľúčových fáz životného cyklu služby, zahŕňajúcich 26 procesov. Každá z fáz je zároveň témou jednej z piatich publikácií:

- **Stratégia služby** (*Service Strategy*) – poskytuje rámec pre definovanie stratégie IT služby, ktorá bude vytvárať hodnotu pre podnik, bude vychádzať z konkrétnych potrieb, a pomocou ktorej bude dosiahnuté strategickej výhody. Obsahuje procesy: management stratégie, management požiadaviek, management portfólia služieb, management financií a management obchodných vzťahov,
- **Návrh služby** (*Service Design*) – poskytuje rámec pre návrh IT služby vrátane architektúry, procesov, politík a dokumentov, s cieľom naplnenia obchodných požiadaviek. Taktiež obsahuje odporúčania pre zmeny služieb a ich kontinuálne zlepšovanie. Obsahuje procesy, ako management katalógu služieb, management dostupnosti, management informačnej bezpečnosti, management úrovní služieb, management kapacít, koordináciu dizajnu, management dodávateľov a management kontinuity služieb IT,
- **Prechod služby** (*Service Transition*) – poskytuje rámec pre plánovanie a riadenie realizácie nových a upravovaných služieb. Medzi procesy patria plánovanie
  a podpora prechodu, management zmien**,** hodnotenie zmien**,** management aktív a konfigurácií**,** management vydaní a nasadení**,** overenie a testovanie služby a management znalostí,
- **Prevádzka služby** (*Service Operation*) – poskytuje rámec pre riadenie a plnenie aktivít spojených s poskytovaním a podporou IT služby. Zahŕňa management

prístupu, management udalostí, naplnenie požiadaviek služby, management incidentov a zvládanie problémov,

- **Neustále zlepšovanie služby** (*Continual Service Improvement*) – poskytuje rámec pre neustále zlepšovanie účinnosti a efektívnosti, zvyšovanie kvality a vytváranie hodnoty IT služieb. Zahŕňa tzv. 7-stupňový proces zlepšovania [8].

2.4 SNMP (Simple Network Management Protocol)

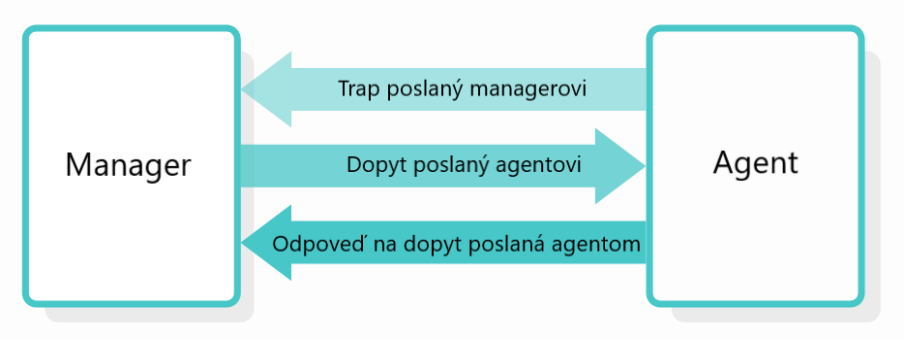
Pre správu a monitoring zariadení pripojených do sietí bolo potrebné vytvoriť protokol, ktorý by bol schopný podporovať celý rad rôznych zariadení. Protokol SNMP (*Simple Network Management Protocol*), alebo jednoduchý manažérsky protokol siete je protokol aplikačnej vrstvy, ktorý bol vytvorený v roku 1988 a je súčasťou sady RFC (*Requests for Comments*). Protokol SNMP bol vytvorený pre sledovanie a správu siete. Okrem sledovania siete, teda zbierania údajov o zariadeniach v sieti, systémoch a službách, umožňuje aj prenos požiadaviek na zmeny konfigurácie v spravovanom zariadení. Vďaka svojej jednoduchosti a univerzálnosti sa stal široko prijímaným štandardom pre správu siete, a práve preto je implementovaný v architektúre väčšiny operačných systémov a rovnako ho podporujú aj výrobcovia sieťových produktov [4].

2.4.1 Architektúra SNMP

Protokol SNMP používa dvojčlennú architektúru *manager/agent*, nakoľko rozdeľuje zariadenia na monitorované (agent) a monitorujúce (manager). Typicky sa manager, správca, nasadzuje len na správcovských staniciach, pretože funguje ako monitorujúce zariadenie slúžiace k prehliadaniu, zberu a analýze dát a vzdialenému riadeniu sieťových zariadení. Na monitorovaných zariadeniach sa naopak nasádza agent, ktorý poskytuje informácie o správe, sledovaním rôznych prevádzkových aspektov zariadenia [9].

Pre komunikáciu medzi managerom a agentom sa štandardne používa protokol UDP (*User Datagram Protocol*), používateľský datagramový protokol, na portoch 161 pre *polling* a 162, na ktorom manager očakáva SNMP *trap*. Termín *polling* označuje dopyt managera na informácie od agentov, periodicky v pevne stanovených intervaloch, alebo podľa potreby. *Trap* je termín označujúci vyslanie správy agentom. *Trap* je odosielaný asynchrónne, teda nie ako odpoveď na vyžiadanie od managera, ale obvykle

na základe dopredu nadefinovanej metriky, ako napríklad presiahnutie stanovenej hodnoty teploty. *Polling* a *trap* sa všeobecne používajú na zisťovanie stavu zariadenia. Pri *pollingu* je preto nepraktické, ak sa manager dopytuje v príliš krátkych intervaloch, nakoľko sa tak zvyšuje záťaž siete. Intervaly však nemôžu byť ani zriedkavé, pretože manager nebude mať dostatočný prehľad o zariadeniach. Dôležitý je tiež fakt, že *polling* a *trap* sa môžu diať súčasne, manager sa môže dopytovať agenta a zároveň môže agent odosielať *trap* [9].



Obrázok č. 2: Vzťah medzi managerom a agentom

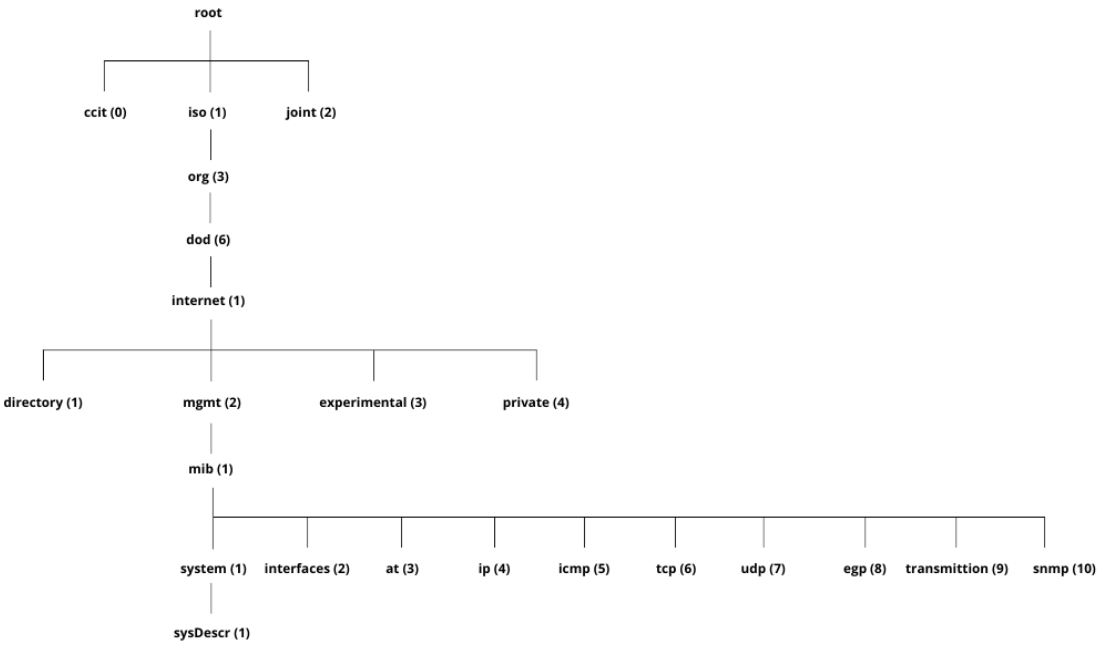
(Zdroj: Vlastné spracovanie podľa: 9, s. 4)

2.4.2 MIB (Management information base)

Spravované zariadenie obsahuje agenta a MIB (*Management Information Base*) databázu. MIB je báza spravovacích informácií, ktoré môže manager použiť na určenie celkového stavu zariadenia, na ktorom sa nachádza agent. Za správu MIB zodpovedá samotný agent. Pretože nie je možné zachytávať všetky informácie v reálnom čase, musia sa ukladať v mieste vzniku. Na dopyt managera odosiela agent požadované informácie o objektoch a vykonáva zmeny hodnôt objektov [9].

MIB je objektovo orientovaná databáza, v ktorej sú objekty organizované v hierarchickej, stromovej štruktúre. Štruktúra manažérskych informácií SMI (*Structure of Management Information*) poskytuje spôsob, ako definovať spravované objekty a ich vlastnosti. Zatiaľ čo MIB definuje objekty samotné, SMI definuje pravidlá pre ich popis [9].

Objekty MIB databázy sú určené jedinečnou adresou, identifikátorom OID (*Object identifier*). Adresa je tvorená cestou od koreňa stromu MIB k objektu. Napríklad premenná *sysDescr*, označujúca textový popis entity, má adresu .1.3.6.1.2.1.1.1 [4].



Obrázok č. 3: Ukážka stromovej štruktúry MIB pre sysDescr

(Zdroj: Vlastné spracovanie)

Každý objekt nadobúda určitú hodnotu. U niektorých objektov by však bolo nemožné snažiť sa ich určiť len jednou hodnotou (singulárne objekty), preto existujú aj stĺpcové objekty, ktorých údaje sú prezentované tabuľkou [4].

2.4.3 SNMP správy

Protokol SNMP používa ku komunikácii medzi riadiacou stanicou (manager) a agentami, SNMP správy. Správa dopytu, ktorú odosiela manager agentovi, sa skladá z hlavičky, ktorá obsahuje číslo SNMP verzie, informácie o veľkosti dopytu a *community string*, ktorý plní funkciu autentifikačného mechanizmu a tela správy, ktoré tvorí PDU (*Protocol Data Unit*) [4].

Protokol SNMP využíva ku komunikácii päť operácií:

- ***GetRequest*** – túto operáciu používa manager a slúži k získavaniu hodnôt (obvykle v jednoduchej forme) jedného, či viacerých objektov od agenta. Keď agent obdrží správu, skontroluje ju, nájde požadované hodnoty objektov a odošle paket *GetResponse* naspäť managerovi,

- ***GetResponse*** – je operácia vygenerovaná agentom ako odpoveď na *GetRequest* a nesie vyžiadanú informáciu. V prípade, že je v pakete dopytu chyba, paket *GetResponse* vráti chybovú správu,
- ***GetNextRequest*** **–** manager používa paket *GetNextRequest*, aby získal od agenta hodnoty, ktoré sú obvykle umiestnené v tabuľke. Manager odosiela pakety *GetNextRequest*, pokiaľ neprečíta všetky hodnoty tabuľky. Ak nedôjde k chybe, bude agent vracať pakety *GetResponse* po každom *GetNextRequest* pakete,
- ***SetRequest*** – tento paket používa manager k modifikácii hodnôt objektu. Ak nenastane chyba, agent vykoná potrebné zmeny a vráti paket *GetResponse* pre potvrdenie operácie,
- ***Trap*** – *trap* je vyslaný agentom managerovi ako upozornenie na definovanú udalosť. *Trap* je odosielaný na port 160 a má rozdielny formát, ako predošlé typy. Hlavička paketu *trapu*, obsahuje OID a adresu agenta, nasledovanú typom *trapu*, časovou pečaťou a rôznymi ďalšími poľami [4].

2.4.4 Verzie SNMP

Pracovná skupina pre internetové inžinierstvo IETF (*Internet Engineering Task Force*) sa zaoberá vytváraním štandardov TCP/IP a internetovými protokolmi, vrátane protokolu SNMP. IETF publikuje tzv. RFC (*Request for Comments*), alebo Žiadosti o komentáre, čo je označenie radu špecifikácií, opisujúcich internetové protokoly. Protokol SNMP má v súčasnosti tieto verzie:

- **SNMP verzia 1** (SNMPv1) – je štandardná verzia protokolu SNMP. Základom zabezpečenia SNMPv1 je *community string*, teda textový reťazec, vystupujúci ako heslo. Ak aplikácia, ktorá používa protokol SNMP pozná daný reťazec, získa prístup k informáciám o zariadení. SNMPv1 má zväčša tri typy *community string*, a to iba na čítanie, na čítanie a zápis a *trap*,
- **SNMP verzia 2** (SNMPv2) – táto verzia mala vylepšovať prvú verziu predovšetkým z hľadiska zabezpečenia. Boli v nej zavedené nové typy PDU, *GetBulkRequest*, čo je príkaz, ktorý prečíta údaje z veľkej sekcie tabuľky naraz a *InformRequest*, ktorý slúži na komunikáciu medzi managermi, je podobný ako *trap*, ale vyžaduje potvrdenie,

- **SNMP verzia 2 na báze community string** (SNMPv2c) – je SNMP verzia 2, ktorej zabezpečenie je rovnaké ako u prvej verzie,
- **SNMP verzia 3** (SNMPv3) – je ďalšou verziou protokolu, ktorá má úplný status štandardu IETF. Táto verzia je vylepšená z pohľadu komunikácie a bezpečnosti, predovšetkým v spôsobe autentizácie a šifrovania. Zaviedol sa aj nový typ PDU *ReportRequest*, primárne určený na hlásenie problémov so spracovaním SNMP správ. Napriek vylepšeniam nie je táto verzia príliš rozšírená [9].

Rozdiely vo verziách SNMP musíme poznať práve preto, že zariadenia v sieti nemusia byť kompatibilné so všetkými verziami kvôli ich nízkej rozšírenosti, a preto nebudú podporovať všetky typy operácií. Pri kompatibilite so SNMPv1 bude zariadenie podporovať operácie *GetRequest, GetNextRequest, SetRequest, GetResponse,* a *Trap*. Ak je produkt kompatibilný so SNMPv2 a SNMPv3, tak bude podporovať aj operácie *GetBulk, Inform, Notification* a *Report* [9].

2.5 RMON (Remote Network Monitoring)

Protokol SNMP používa architektúru *klient/server*, ktorá je však pri častom dopytovaní agentov stanicami pre správu (napríklad zisťovanie dátových tokov) príliš zaťažujúca. Ako riešenie tohto problému vznikol RMON (*Remote Network Monitoring*). Vzťah *klient/server* je obrátený, nakoľko agenti spracúvajú všetky úlohy a stanice pre správu majú prakticky rolu klienta, takže už nemusia zhromažďovať aktualizované dáta. Agenti RMON, ktorých nazývame sondy, predajú managerom súvisiace informácie odoslaním *trapu*. Vzniká teda samostatné monitorovanie na strane sondy, čím sa znižuje zaťaženie siete. Sondy môžu byť súčasťou aktívneho prvku, alebo sú samostatne pripojené na port. Pretože sondy RMON sú sofistikovanejšie, ich objekty sa tiež odlišujú od objektov SNMP. RMON MIB objekty sú zamerané na monitoring sietí Ethernet a Token Ring [4].

2.5.1 Základné skupiny RMON MIB

Hlavné objekty RMON1 MIB spadajú do deviatich kategórií:

- ***Statistics*** – poskytuje štatistiky o sieťových rozhraniach,

- ***History*** – určuje spôsob, akým sú zhromažďované dáta skupiny *statistics* (napríklad vzorkovacia frekvencia),
- ***Alarm*** – skupina ovláda výstrahy, ktoré signalizujú prekročenie prahových hodnôt udalostí,
- ***Hosts*** – sleduje MAC adresy hostiteľov zistených v sieti, čím vytvára štatistiky návštevnosti,
- ***HostTopN*** – na základe štatistických informácií o hostiteľoch v sieti vytvára zoznamy hostiteľov podľa stanovených parametrov,
- ***Matrix*** – sleduje vzájomnú komunikáciu medzi hostiteľmi na základe prenosu dát,
- ***Filter*** – používa sa k výberu špecifických paketov, ktoré sú zachytávané za účelom generovania štatistík,
- ***Capture*** – používa nastavenie v skupine *filter* k zachytávaniu vybraných paketov,
- ***Event*** – definuje nastavenia pre generovanie udalostí podľa prekročenia prahových hodnôt,
- ***TokenRing*** – uchováva štatistiky a informácie o konfigurácii pre *token ring* [4].

Rovnako ako pri SNMP, má aj RMON viacero verzií. Modernejšia RMON2 pridáva ďalšie skupiny:

- ***protocolDir*** – určuje hlavný adresár, ktorý obsahuje všetky implementované protokoly,
- ***protocolDist*** – obsahuje štatistiky o premávke, ktoré generuje každý protokol,
- ***addressMap*** – obsahuje mapovanie adries IP na MAC adresy,
- ***NlHost*** – obsahuje štatistiky na úrovni sieťovej vrstvy o premávke z a do zariadení,
- ***nlMatrix*** – obsahuje štatistiky na úrovni sieťovej vrstvy o komunikácii medzi zariadeniami,

- ***alHost*** – obsahuje štatistiky na úrovni aplikačnej vrstvy o premávke z a do zariadení,
- ***alMatrix*** **-** obsahuje štatistiky na úrovni aplikačnej vrstvy o komunikácii medzi zariadeniami,
- ***usrHistory*** – obsahuje periodické vzorky premenných špecifikovaných používateľom,
- ***probeConfig*** – definuje konfiguračné parametre,
- ***rmonConformance*** – udáva požiadavky na zhodu [4].

Druhá verzia umožňuje monitoring na všetkých úrovniach referenčného modelu OSI, zatiaľ čo RMON v prvej verzii pracuje len s rámcami [4].

2.6 LLDP (Link Layer Discovery Protocol)

LLDP (*Link Layer Discovery Protokol*) je protokol linkovej vrstvy vyvinutý pre mapovanie zariadení v sieti. LLDP je otvorený protokol, ktorý bol špecifikovaný v IEEE štandarde 802.1AB. Tento protokol umožňuje sieťovým zariadeniam v periodických intervaloch vysielať oznámenia s informáciami o sebe samých susedným zariadeniam v sieti. LLDP je navrhnutý tak, aby informácie, ktoré zariadenie vysiela, boli uložené v MIB databáze, takže môžu byť spravované cez protokol SNMP. Rámec LLDP tvorí preambula, cieľová MAC adresa (*multicast* adresa), zdrojová MAC adresa a *Ethertype*. PDU protokolu LLDP obsahuje informačné polia TLV (*type-length-value*), ktorými sú *Chassis* ID, *Port* ID, TTL (*Time To Live*), voliteľné polia TLV a *End of* LLDPPDU. Rámec ukončuje kontrolný súčet. Nenulová hodnota TTL určuje dobu platnosti záznamu. Pokiaľ nie je záznam aktualizovaný, je po vypršaní TTL zahodený [10].

2.7 DMI (Desktop Management Interface)

S vývojom v oblasti technológií, narastala aj rôznorodosť komponentov počítačov, čo viedlo k problémom s ich manažovaním. Správa systému s veľkým počtom rôznych komponentov od rozdielnych výrobcov, z ktorých každý z nich vyžadoval rôzny súbor riadiacich údajov a funkcií, tento problém ešte viac prehlbovala. DMI (*Desktop Management Interface*) je rozhranie, ktoré bolo vyvinuté za účelom zjednodušenia správy

a sledovania komponentov počítačov. DMI je nezávislé na konkrétnom počítači alebo operačnom systéme, ako aj na konkrétnom protokole pre správu. V prípade zmeny stavu vlastnosti niektorého komponentu, vyprodukuje DMI oznámenie. Je možné definovať, na ktoré oznámenia bude aplikácia pre správu upozornená [11].

DMI sa skladá zo štyroch súčastí:

- **MIF** (*Management Information Format*) – definuje formát pre popis manažovaných informácií. Každý komponent počítača má súbor MIF, ktorý obsahuje skupiny popisujúce jeho manažovateľné charakteristiky,
- **DMI** (*Service Provider*) – servisná vrstva, umožňuje vzdialenú správu a prístup k MIF platformám pre správu,
- **CI** (*Component Interface*) – rozhranie pre interakciu medzi servisnou vrstvou a komponentami. Rozhranie obsahuje popis prístupu k informáciám a umožňuje správu komponentov,
- **MI** (*Management Interface*) – rozhranie pre interakciu medzi servisnou vrstvou a platformami pre správu [12].

Ako SNMP, tak aj DMI sú otvorené štandardy. Každý podporuje manažovanie objektov vo svojej cieľovej oblasti, ktorými sú počítač a sieť. Nedokážu však definovať vzťahy s manažovanými objektami mimo svojej domény. Preto môže byť pre platformy pre správu problematické určiť dôvod chybového stavu, ktorý môže súvisieť práve so vzťahom objektov týchto oblastí. Tento problém rieši WBEM (*Web-Based Enterprise Management*), čo je súbor štandardov použiteľných pre správu distribuovaných počítačových prostredí. Súčasťou WBEM je CIM (*Common Information Model*), štandard, ktorý definuje manažované komponenty ako spoločnú množinu objektov a vzťahov medzi nimi [11].

2.7.1 WMI (Windows Management Instrumentation)

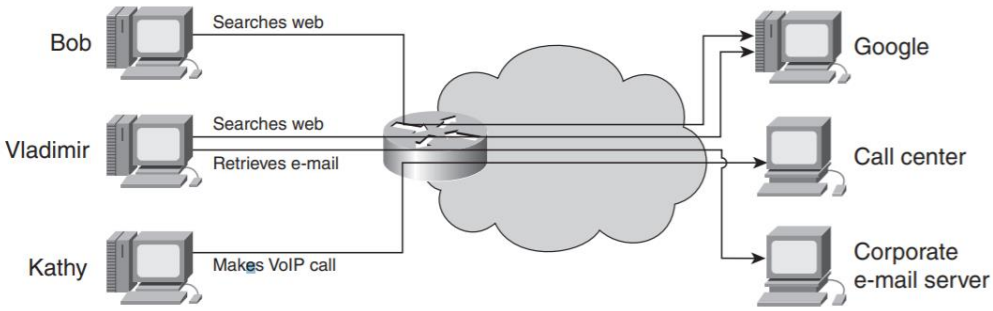
WMI (*Windows Management Instrumentation*) môžeme chápať ako infraštruktúru pre správu dát a operácií v operačných systémoch Windows. WMI tiež umožňuje poskytovanie údajov o správe ďalším súčastiam operačného systému, ako aj iným platformám. Je implementáciou WBEM, ktorá používa štandard CIM. Prostredníctvom

WMI môžeme spravovať počítače ako lokálne, tak aj vzdialene. Vzdialené pripojenie sa uskutočňuje cez DCOM (*Distributed Component Object Model*), prípadne cez WinRM (*Windows Remote Management*). Vzhľadom k rozšírenosti systému Windows, podporuje WMI aj množstvo predajcov nástrojov pre správu siete. WMI je v systémoch Windows predinštalované, ale nemusí byť automaticky povolené [13].

2.8 Monitorovanie toku siete

Pri monitorovaní siete hrá významnú úlohu *flow monitoring* alebo monitorovanie sieťových tokov, ktoré si kladie za cieľ získavať informácie o sieťovej premávke prostredníctvom zhromažďovania a analyzovania premávky prechádzajúcej sieťou. Pomocou analýz týchto dát môžeme napríklad zistiť, ktoré zariadenia v sieti najviac komunikujú, aká sieťová premávka je medzi dvoma bodmi v sieti, kde v sieti sa nachádzajú úzke miesta, ako plánovať prideľovanie šírky pásma, alebo ako sú využívané sieťové prepojenia. Monitorovanie v neposlednej rade umožní detegovať možné bezpečnostné udalosti. Pre monitorovanie toku siete bolo vytvorených niekoľko štandardov, spomedzi ktorých sú najvýznamnejšie NetFlow, sFlow, a IPFIX (*Internet Protocol Flow Information Export*) [14].

Jednotka, s ktorou pracuje monitoring toku siete sa nazýva IP tok (*IP flow*). Každý IP tok prechádzajúci cez smerovač umožňuje tvorbu novej štatistickej informácie. Tok pozostáva zo všetkých IP paketov, ktoré sú prenesené v rámci jedného komunikačného spojenia, prechádzajúcich cez pozorovací bod (*Observation Point*) v určitom časovom okamihu. Napríklad súbor, ktorý sa prenáša, je rozdelený do jednotlivých paketov. Všetky tieto pakety tvoriace tok sú súčasťou jedného spoločného prenosu a môžu prechádzať cez rovnaký prepínač [14].



Obrázok č. 4: IP prevádzka prechádzajúca smerovačom

(Zdroj: 14)

Každý IP tok je jednoznačne identifikovaný týmito parametrami:

- **zdrojová adresa**,
- **zdrojový port**,
- **cieľová adresa**,
- **cieľový port**,
- **typ protokolu** – definuje, či je paket prenášaný protokolom TCP alebo UDP,
- **typ služby** – identifikuje typ služby, ktorý sa používa pre rozlišovanie rôznych kategórií sieťovej premávky,
- **vstupné logické rozhranie** – softvérová entita pozostávajúca z adresy IP a obsahujúca atribúty, ako zdrojový port, domovský uzol a ďalšie [14].

Pri každom toku sú zhromažďované dáta, ktoré spolu vytvárajú záznam toku. Záznam toku obsahuje kľúče, ktoré tok identifikujú, ako napríklad čas, kedy bol tok započatý, čas, kedy bol ukončený, či koľko paketov bolo prenesených [14].

2.8.1 Využitie monitorovania IP tokov

Monitorovanie IP tokov poskytuje široké využitie a prináša mnoho výhod, ako napríklad monitoring rozsiahlych vysokorýchlostných sietí. Vďaka štatistickým údajom, ktoré monitoring sieťových tokov prináša, sme schopní získavať informácie o sieti, ktoré sú uplatniteľné predovšetkým pre správu účtovania a správu výkonu. Medzi možnosti uplatnenia monitorovania IP tokov patrí:

- **Bezpečnosť siete, detekcia a obrana proti útokom na sieť** – monitoring IP tokov odhaľuje anomálie a podozrivé správanie v sieti, čím umožňuje detegovať ako vnútorné, tak aj vonkajšie napadnutie siete, či iné neštandardné situácie, ktoré môžu viesť k vzniku bezpečnostných udalostí. Táto schopnosť je základným dôvodom pre implementáciu monitorovania toku v organizácii,
- **Plánovanie kapacít** – monitorovanie toku umožňuje získať potrebné informácie pre plánovanie kapacít, ako napríklad historické údaje sieťovej premávky, či vysokú, alebo rýchlo rastúcu premávku v segmentoch siete, alebo úzke hrdlá v sieti,

- **Využívanie zdrojov** – monitorovanie tokov umožňuje získať podrobné údaje o využívaní siete a sieťových zdrojov jednotlivými používateľmi či aplikáciami. Týmto spôsobom je možné napríklad zistiť, či niektorý z používateľov koná neoprávnene. Tieto informácie sú dôležité predovšetkým pre poskytovateľov sietí, ktorí ich môžu využiť, ak budú chcieť účtovať poplatky na základe skutočnej spotreby, namiesto paušálnych poplatkov. Vďaka informáciám o využívaní siete je možné optimalizovať aj zaťaženie aktívnych prvkov, alebo merať výkon aplikácií, či novej konfigurácie siete. Organizácia tak bude efektívnejšie rozhodovať o investíciách a nové technológie zadováži, len ak budú skutočne potrebné [14].

2.8.2 NetFlow a IPFIX

NetFlow je proprietárny protokol vytvorený spoločnosťou Cisco, ktorý sa špecializuje na zhromažďovanie dát o sieťovej premávke. Tento protokol bol vyvinutý špeciálne pre zber a prenos veľkých objemov dát, a preto dokáže pracovať efektívnejšie a vyžaduje menšiu réžiu, než protokoly pre správu [14].

Architektúra NetFlow sa skladá z exportéra, z kolektora a z aplikácie, ktorá vykonáva analýzy. Exportér agreguje pakety do tokov a exportuje záznamy do kolektora. Kolektorom označujeme príjemcu, ktorého úlohou je zbierať, ukladať a predbežne spracovávať záznamy tokov prijatých od exportérov a sprístupňovať ich analyzujúcim aplikáciám. Tie následne analyzujú dáta na základe požadovaného dopytu používateľa a zobrazujú ich v užívateľsky prijateľných výstupoch vo forme grafov, tabuliek, historických pohľadov, či správ [14].

NetFlow existuje vo viacerých verziách, avšak najrozšírenejšou je NetFlow v5, ktorý má všetky vyššie spomenuté vlastnosti. Napriek tomu, že základné operácie vo všetkých verziách zostávajú rovnaké, majú jednotlivé verzie rozličné vlastnosti a ponúkajú iné možnosti. Napríklad NetFlow v7 zachytáva IP toky prepínačov, namiesto smerovačov. NetFlow vo verzii 8 umožňuje agregáciu tokov do jedného, čo znižuje objem exportu a zjednodušuje zber. Verzia 9 zase umožňuje formátovať exportované záznamy pomocou špeciálnej šablóny. Okrem spoločnosti Cisco, ponúka množstvo výrobcov vlastné implementácie NetFlow, ako napríklad jFlow od spoločnosti Juniper.

Preto je potrebné, aby sme pri nasadzovaní tejto technológie pamätali aj na kompatibilitu [13].

Štandard IPFIX (*Internet Protocol Flow Information Export*), je z technického hľadiska podobný štandardu NetFlow v9. Rozdiel je predovšetkým v tom, že IPFIX je otvorený štandard, ktorý vznikol ako potreba vytvorenia spoločného štandardu, nakoľko NetFlow je proprietárnym protokolom spoločnosti Cisco [14].

2.8.3 sFlow

Štandard sFlow, inak nazývaný aj *sampled flow*, používa namiesto sledovania tokov stavovo ako NetFlow, vzorkovanie toku paketov. Tento štandard je pomerne rozšírený v poslednej, piatej verzii. Architektúru sFlow tvorí agent sFlow a centrálny kolektor. Agent sFlow pomocou vzorkovania vytvára štatistiky premávky zo zariadenia, ktoré monitoruje, teda záznamy toku paketov. Tie sú následne exportované spolu so záznamami počítadiel vo forme sFlow datagramov do kolektora na analýzu. Vzorkovanie paketov a použitie protokolu UDP na ich odosielanie na jednej strane podstatne urýchľuje export, nevyžaduje veľa pamäte a znižuje zaťaženie, no na druhej strane môže byť znížená presnosť získaných výsledkov. Strata by však mala byť len zanedbateľná. Práve preto je sFlow vhodným štandardom, ktorý je často využívaný vo vysokorýchlostných sieťach [15].

Pri technológiách, ktoré využívajú vzorkovanie, je nutné dbať na nastavenie vhodnej vzorkovacej frekvencie. Ak je vzorkovacia frekvencia rovná 1, zachytávajú sa všetky pakety a výsledky sú presnejšie, ak sa rovná 0, vzorkovanie je deaktivované. Častým vzorkovaním však prichádzame o výhodu a podstatu štatistického vzorkovania [15].

2.9 Nástroje pre správu sietí

Nástroj pre správu siete označuje softvérový balík, ktorý používa správca siete na neustály monitoring siete a zabezpečenie fungovania všetkých systémov a zariadení v sieti a na upozorňovanie na problémy a chyby, či prekročenie hraničných hodnôt. Monitoring siete prostredníctvom softvérového nástroja umožňuje správcovi siete

rozpoznávať a zachytávať udalosti, v prípade potreby urýchlene zasiahnuť, a to aj vzdialene.

Framework pre správu integruje viacero rôznych sieťových nástrojov do používateľského prostredia a do aplikačného rozhrania API (*Application Programming Interface*). Nástroje môžu byť buď s otvoreným kódom, ktoré sú voľne šíriteľné, alebo uzavreté a proprietárne. Väčšina nástrojov je predávaná so základným nastavením a funkcionalitou, pričom rozšírená funkcionalita je zväčša súčasťou samostatne predávaných doplnkov. Cena nástrojov sa líši podľa druhu nástroja. Skladá sa z nákladov na základný systém, zložený z počtu konzol, alebo z počtu nasadených serverov pre správu, či počtu klientskych licencií, alebo ďalších kombinácií. Framework pre správu siete je navrhnutý tak, aby bolo možné prispôsobovať jednotlivé funkcie. Najčastejšie funkcie, ktoré obsahujú nástroje pre monitoring siete sú:

- sledovanie aktivity systémov,
- sledovanie aktivity používateľov,
- sledovanie využívania sieťových prostriedkov,
- správa aktív,
- nasadenie operačných systémov a softvéru,
- kontrola zhody s licenciou,
- správa zálohovania,
- antivírusová a antispyvérová ochrana,
- správa úložísk,
- správa zabezpečenia,
- správa adresárových služieb [2].

Na trhu je dnes veľmi veľké množstvo rôznych monitorovacích nástrojov správy siete. Nástroje môžeme rozdeliť napríklad podľa toho, či chceme open-source softvér, alebo investujeme do plateného riešenia, alebo ich môžeme rozdeliť podľa monitorovacích úloh, na ktoré sa špecifikujú. Je preto potrebné, aby sme vopred definovali požiadavky správy siete pre konkrétnu organizáciu, pretože iba tak zistíme, čo

vlastne od monitorovacieho nástroja očakávame. Po definovaní požiadaviek na nástroj pre monitoring siete môžeme vybrať práve ten, ktorý bude tieto požiadavky napĺňať.

2.9.1 Open-source nástroje

Open-source nástroje, alebo nástroje s otvoreným zdrojovým kódom označujú názov pre počítačový softvér s takou licenciou, ktorá umožňuje, aby bol kód daného softvéru šíriteľný voľne a bez obmedzení. Znamená to, že si takýto typ softvéru môže zaobstarať prakticky ktokoľvek a softvér môže voľne využívať a prípadne ďalej modifikovať s podmienkou, že ponechá kód aj naďalej otvorený. Významná výhoda tohto typu softvéru tkvie predovšetkým v jeho cene, nakoľko je zväčša k dispozícii zadarmo, prípadne môže byť spoplatnená podpora k softvéru. Ak má organizácia nižší rozpočet, ktorý môže vyčleniť pre nástroj na monitoring siete, je voľba softvéru s otvoreným zdrojovým kódom dobrým a lacným riešením. Rovnako vhodným riešením je v prípade, keď chce správca siete takýto program len na skúšku, prípadne začína s implementáciou monitoringu siete ako takou. Výhodu v podobe ceny však znižuje nevýhoda v podobe obmedzenejšej funkcionality. Open-source nástroje poskytujú zväčša iba základné funkcie a môžu byť náročnejšie z hľadiska konfigurácie, ako aj ovládania. Naviac, ak je podpora k softvéru bezplatná, je zväčša poskytovaná komunitou, a preto nemusí zaručovať spoľahlivosť a v prípade bezpečnostných dier softvéru vydavateľ taktiež nezaručí nápravu. Ak však takýto druh softvéru naplní funkčné požiadavky kladené spoločnosťou, jeho zaobstaranie bude dobrá východzia voľba [16].

2.9.2 Špecializované nástroje

Ďalším typom softvéru pre monitorovanie siete, s ktorým sa môžeme stretnúť, je nástroj ktorý je špecializovaný na konkrétny typ úlohy alebo konkrétnu oblasť siete. Jedná sa napríklad o technológie, ktoré sú primárne určené na *packet sniffing*, teda zachytávanie a analyzovanie paketov v sieti. Takýto monitorovací systém umožní monitorovať problémy v sieti, odhaľovať pokusy o útoky na sieť, získavať informácie o sieti a o jej využívaní, monitorovať dáta a vytvárať analýzy dát, sledovať výkonnosť, vytvárať štatistiky, či zhromažďovať informácie o zabezpečení siete a mnohé ďalšie. Vďaka špecializácii poskytuje takýto monitorovací nástroj podrobné informácie zo špecifickej oblasti, ako monitoring šírky pásma, práve kvôli analyzovaniu paketov, ale nedokáže

vykonávať funkcie rozsiahlejšieho monitoringu v inej oblasti. Špecializované nástroje teda využijú spoločnosti, ktorých primárnou požiadavkou je monitorovanie sieťovej prevádzky a riešenie problémov v sieti [16].

2.9.3 Nástroje zamerané na správu podnikovej siete

Monitorovacie systémy vo veľkých podnikových sieťach sú zvyčajne súčasťou oveľa väčšieho systému. Zložitosť je priamoúmerná rastu podnikových procesov a funkcií. Monitorovací nástroj, ktorý je zameraný na správu podnikovej siete, musí preto napĺňať potreby nadštandardného monitorovania viacerých vzájomne prepojených systémov. Tento fakt sa odzrkadľuje aj v zložitosti a vo vysokých nákladoch takéhoto riešenia, ktoré si malé a stredné podniky zväčša nemôžu dovoliť. Funkcionalita tohto nástroja tiež prekonáva potreby malých a stredných podnikov [16].

2.9.4 Multifunkčné nástroje

Nástroje typu *all in one*, teda všetko v jednom, obsahujú štandardné monitorovacie funkcie, no zároveň zahŕňajú aj špeciálnu funkcionalitu, ktorá sa viaže ku konkrétnym monitorovacím oblastiam. Takýto nástroj monitoruje sieť so všetkými zariadeniami, systémami a aplikáciami, ako aj sieťovú prevádzku. Podporuje tradičné monitorovacie protokoly, ako SNMP, či protokoly pre monitorovanie tokov, ale pri monitoringu umožňuje aj využitie ďalších protokolov. Riešenie sa vyznačuje pomerne rýchlou implementáciou a jednoduchou konfiguráciou. Tvorcovia týchto technológií zvyčajne poskytujú zákazníkom podporu. Licencovanie nástroja je zväčša škálovateľné, takže si zákazník môže vybrať vhodný typ licencie vzhľadom k veľkosti podniku, či k požiadavkám kladeným na správu siete [16].

2.10 SWOT analýza

Rozhodnutie o implementovaní technológie pre správu siete musí vychádzať z dlhodobej stratégie vedenia spoločnosti, nakoľko môže byť finančne nákladným a dlhodobým projektom. Plánovanie strategických rozhodnutí zahŕňa stanovenie dlhodobých cieľov podniku, ktoré môžeme definovať pomocou SWOT analýzy. SWOT analýza je nástroj, ktorý sa používa pre zhodnotenie súčasného stavu organizácie z rôznych hľadísk. SWOT

analýza pozostáva zo štyroch menších celkov, a to z analýzy silných a slabých stránok organizácie, analýzy príležitostí a z analýzy hrozieb v podnikateľskom prostredí. Dielčie celky vychádzajú z analýzy súčasného stavu, ako aj z predpovedania budúcich trendov, ktorými sa môže potencionálne spoločnosť uberať. Prostredníctvom tejto analýzy môžeme posúdiť, či sú vytvorené vhodné podmienky a či je organizácia pripravená realizovať zamýšľaný projekt [17].

2.11 Zhrnutie teoretických východísk

V tejto časti práce boli popísané základné princípy potrebné pre vysvetlenie problematiky správy siete. Úvod do teoretických východísk práce otvorila definícia počítačovej siete, vrátane delenia do rôznych kategórií a popis jednotlivých prvkov počítačovej siete. Následne sa práca zameriavala na vysvetlenie správy počítačovej siete a jej významu. Pre vytvorenie hlbšieho pohľadu do problematiky bol popísaný aj sieťový model správy OSI a funkčné oblasti sieťového managementu, teda správa porúch, správa konfigurácie, účtovná a evidenčná správa a správa výkonu. Teoretickú bázu ďalej dotvára stručný popis a možné zdroje pre zavádzanie riadenia služieb informačných technológií ITSM, akými sú normy ISO/IEC 20000, ale aj knižnica ITIL. Po zasadení monitoringu siete do určitého teoretického rámca boli v práci následne popisované technické aspekty monitoringu. Protokoly správy siete boli popísané od tradičnejších, akými je protokol SNMP či RMON, až po štandardy pre monitoring sieťových tokov. V závere kapitoly boli stručne uvedené a kategorizované nástroje pre správu sietí. Tieto teoretické východiská sú ďalej využité v analytickej časti, ako aj vo vlastnom návrhu riešenia práce.

3 ANALÝZA SÚČASNÉHO STAVU

Táto časť diplomovej práce sa venuje predstaveniu a analýze spoločnosti, pre ktorú je vytváraný návrh implementácie vybranej technológie pre management počítačovej siete. Analyzovaná spoločnosť je pre potreby diplomovej práce anonymizovaná. Analýza vychádza z konzultácií so zamestnancami technickej sekcie spoločnosti. Táto kapitola obsahuje okrem samotnej analýzy súčasného stavu spoločnosti aj požiadavky kladené samotnou spoločnosťou, teda vedením a zamestnancami, ktoré je potrebné pri návrhu zohľadniť. V ďalšej časti sú analyzované vybrané platformy pre správu siete.

3.1 Predstavenie spoločnosti

Ako už bolo spomenuté v úvode kapitoly, vybraná spoločnosť je pre potreby tejto práce anonymizovaná, a preto sú nasledujúce firemné údaje zavádzajúce.

Obchodný názov	XYZ, s.r.o.
IČO	12345678
Sídlo	Mesto A, Ulica, č. p. 1
Právna forma	spoločnosť s ručením obmedzeným
Veľkosť firmy	celkom 3 pobočky a cca. 103 zamestnancov
NACE	71200 Technické testovanie a analýzy

Analyzovaná spoločnosť vykonáva činnosti skúšobného laboratória. Zaoberá sa skúšaním, certifikáciou a posudzovaním zhody a technických požiadaviek strojových zariadení, riadenia výroby, systémov manažérstva a mnohých ďalších. Spoločnosť pôsobí na trhu skúšobníctva úspešne viac ako 30 rokov a má vybudovanú medzinárodnú klientelu. Aktuálne má tri geograficky oddelené pobočky, z ktorých je jedna centrálna a ďalšie dve sú vyhradené pre účely skúšobníctva a testovania. V súčasnosti spoločnosť zamestnáva približne 103 zamestnancov.

3.1.1 Predmet podnikania a činnosti

Medzi hlavné činnosti spoločnosti patrí overovanie technických zariadení, skúšanie technických zariadení, strojov a materiálov a posudzovanie zhody výrobkov, certifikácia strojových, tepelných, tlakových zariadení, certifikácia zariadení v energetike, certifikácia systémov manažérstva, osôb a výrobkov, kalibrácia meradiel a elektrických veličín prístrojov.

3.1.2 Vízia, stratégia a ciele

Firma sa podľa svojej vízie usiluje byť stabilne rastúcou spoločnosťou, ktorá bude svojim zákazníkom prinášať hodnotu zvyšovaním bezpečnosti, a ktorá bude konkurencieschopnou spoločnosťou s medzinárodným postavením.

Stratégia podniku sa sústredí na získanie dominantného postavenia medzi spoločnosťami s rovnakým zameraním, a to predovšetkým rozširovaním svojej ponuky pre zákazníkov, dodávaním kvalitne vypracovaných riešení, zvyšovaním kvalifikácie a vzdelávaním zamestnancov a budovaním dobrých obchodných vzťahov.

Podnik taktiež vymedzil dielčie strategické ciele, ktorými sú:

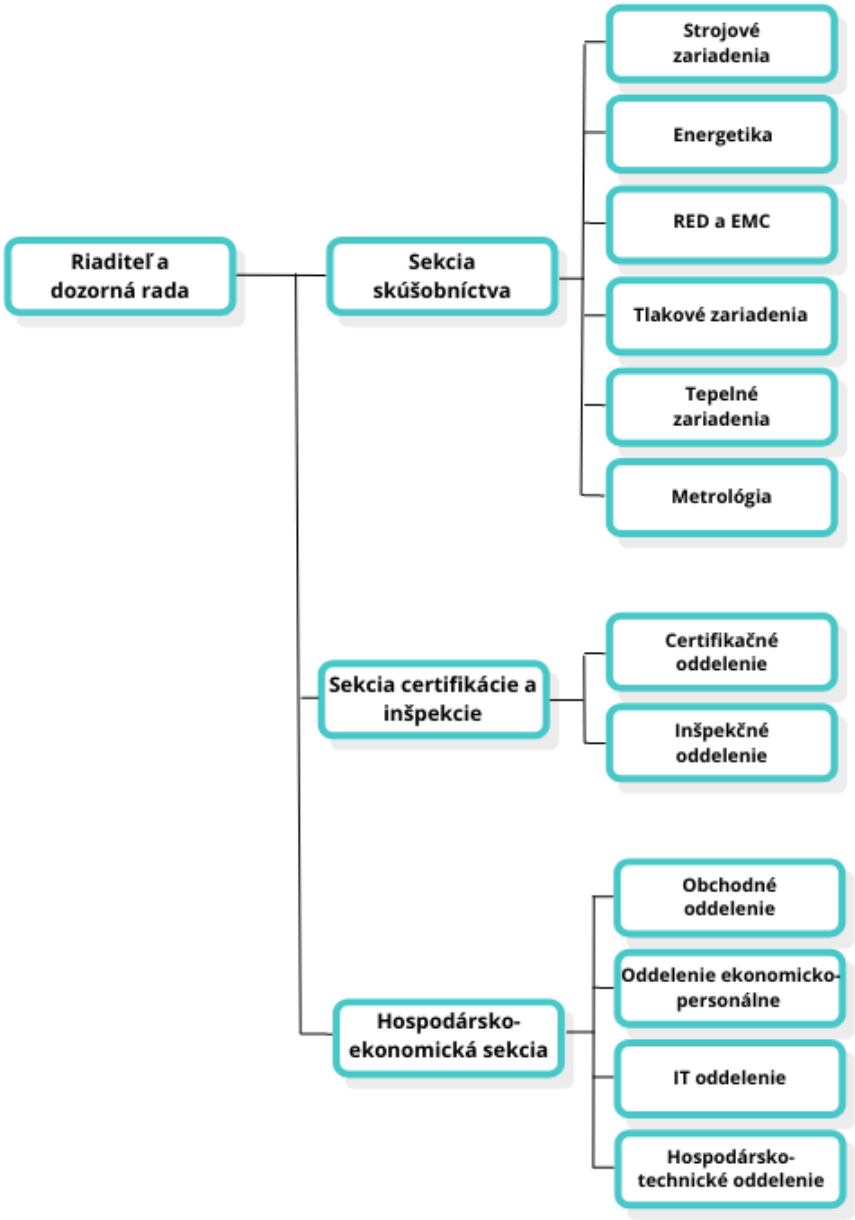
- kontinuálne uplatňovanie PDCA cyklu,
- zlepšovanie stávajúcich služieb a hľadanie príležitostí pre vytváranie nových služieb,
- udržiavanie spokojných zákazníkov a zvyšovanie zákazníckej skúsenosti,
- zvyšovanie efektívnosti budovaním spolupracujúcich tímov a jasným definovaním procesov,
- zvyšovanie produktivity zlepšovaním pracovných podmienok, školením zamestnancov, zlepšovaním a udržiavaním pracovného prostredia, údržbou zariadení a vytváranie a udržiavanie pozitívnej firemnej kultúry.

3.1.3 Organizačná štruktúra spoločnosti

Vo vedení spoločnosti stojí výkonný riaditeľ, na ktorého činnosť dohliada dozorná rada. Ďalej je organizačná štruktúra rozčlenená na tri sekcie a to Sekciu skúšobníctva, Sekciu

certifikácie a inšpekcie a Hospodársko-ekonomickú sekciu, ktoré sú ďalej členené na jednotlivé oddelenia a skúšobné laboratóriá.

Pre potreby tejto práce bude kľúčovým hlavne oddelenie IT. Toto oddelenie má troch pracovníkov, ktorí sú zodpovední za informačno-komunikačné technológie v spoločnosti.



Obrázok č. 5: Organizačná štruktúra spoločnosti

(Zdroj: Vlastné spracovanie)

3.2 Analýza informačných systémov

Informačný systém bude popísaný podľa dvoch zložiek, ktorými sú softvér a hardvér.

3.2.1 Softvér

V spoločnosti je používaný celý rad rôznych typov softvéru. Na serveroch aj pracovných staniciach sú používané operačné systémy spoločnosti Windows. U serverov je použitá verzia Windows Server 2016. Všetky pracovné stanice majú momentálne inštalovanú verziu Windows 10. Každá pracovná stanica je chránená antivírusovým systémom od spoločnosti ESET, konkrétne ide o ESET NOD32 Antivirus. Všetky počítače majú taktiež inštalovaný balík spoločnosti Microsoft Office 2019 pre podnikateľov, pričom najvyužívanejším nástrojom je Outlook. Bezpečné vzdialené pripojenie zamestnancov z domu a z externých laboratórií do firemnej siete je realizované cez VPN (*Virtual Private Network*) a to konkrétne OpenVPN.

Všetky počítače majú nainštalovanú aplikáciu NOPRALA vytvorenú oddelením IT, ktorá slúži ako firemný informačný systém, predovšetkým pre zadávanie dopytov, otváranie úloh a spracovávanie ekonomickej agendy pre každý úsek a každé laboratórium. Táto aplikácia slúži zároveň ako databáza všetkých úloh a obsahuje informácie o typoch vykonaných skúšok, kalibrácií, certifikácií, inšpekcií, prípadne o iných vykonaných službách spolu s podrobnosťami o začiatku a ukončení úlohy, použitých metódach prác a taktiež aj ako databáza zákazníkov. Jedná sa o kľúčový informačný systém v spoločnosti, na ktorý sú následne napojené externé informačné systémy na spracovanie dochádzky, fakturáciu a ďalšie.

Ďalším dôležitým systémom je MyPortal, do ktorého sa pristupuje cez webové rozhranie, a ktorý slúži predovšetkým ako dochádzkový systém zaznamenávajúci príchody, odchody a prípadný pohyb v rámci sekcií budovy prostredníctvom čipových kariet. Do systému majú prístup všetci zamestnanci, aby mohli sledovať počet odpracovaných hodín, nakoľko firma nemá stanovenú presnú dennú pracovnú dobu. Každý zamestnanec má hierarchicky priradené práva prístupu k dochádzkovým informáciám. Vedúci pracovníci teda majú prístup ako k svojim dátam, tak aj k dátam podriadených pracovníkov, ktorých vedú.

Tretí významný informačný systém je cloudová platforma Nextcloud Hub. Tento produkt je využívaný predovšetkým kvôli pokročilejšej funkcii kalendáru a plánovania dopytov. Vedúci pracovníci jednotlivých úsekov tak môžu jednoduchšie alokovať zamestnancov ku konkrétnym zákazkám, časom a miestam. Ďalej je v spoločnosti používaný softvér Softip Packet, ktorý je ekonomicko-finančným nástrojom.

Vzhľadom na zameranie tejto spoločnosti, využíva každé skúšobné laboratórium ďalšie špecifické softvérové nástroje, ktoré sú kľúčové pri meraniach a skúškach. Takýmto nástrojom je napríklad AMR Win Control, slúžiaci na spracovanie dát získaných z meracích senzorov a snímačov.

3.2.2 Hardvér

Budova, v ktorej sídli spoločnosť má 6 poschodí. Serverovňa sa nachádza na prvom poschodí. Z tohto miesta vychádza chrbticové vedenie, ktoré prepája dátové rozvádzače v ostatných piatich poschodiach. Každé poschodie má potom vlastnú horizontálnu sekciu s metalickým vedením.

V budove je použitých sedem 24-portových switchov spoločnosti Cisco. Každá kancelária má len jednu dátovú zásuvku, odkiaľ sú kvôli značnému poddimenzovaniu pripojené ďalšie aktívne prvky, 5-portové Wi-Fi routere Mikrotik, na ktoré sa pripájajú koncové zariadenia.

V súčasnosti sa firemná sieť skladá z deviatich serverov a zo 124 počítačov z čoho je 98 notebookov. Všetky pracovné stanice sú značky HP alebo Dell. Všetci používatelia sú zaradení do domény. V spoločnosti sa ako centrálne úložisko používa Windows File server. Hardvérové vybavenie ďalej obsahuje 48 tlačiarní, 35 IP kamier, periférne zariadenia a telefóny.

Do firmy je zavedená optická sieť od poskytovateľa internetu Orange. V celom objekte sú oddelené dve Wi-Fi siete, jedna pre zamestnancov a jedna pre návštevníkov firmy. Prostredníctvom Wi-Fi je tiež pripojená väčšina zariadení, predovšetkým komora pre meranie elektromagnetickej kompatibility, komora pre meranie rádiového spektra aj dozvuková a bezdozvuková komora a ďalšie.

3.3 SWOT analýza

Silné stránky

- široké portfólio špecifických služieb a činností,
- rýchlosť a flexibilita v poskytovaní služieb oproti konkurencii,
- zamestnanci sú vyškolení experti s dlhoročnou praxou,
- pravidelné vzdelávanie pracovníkov zamerané na udržanie svojej špecializácie a zároveň aj školenia zamerané na rozšírenie vedomostí v daných problematikách a na nové typy služieb,
- nadpriemerné jazykové schopnosti a ďalšie vzdelávanie na pravidelnej báze,
- profesionalita a prozákaznícky prístup.

Slabé stránky

- slabá alebo žiadna personálna zastupiteľnosť,
- neefektívnosť niektorých procesov,
- čiastočne zlá organizácia času,
- príliš vysoký vekový priemer zamestnancov,
- nedostatok zamestnancov, vďaka čomu je potrebné odkladať niektoré vedľajšie činnosti,

Príležitosti

- orientácia na nové trhy mimo EÚ,
- zlepšovanie stávajúcich služieb a vytváranie nových,
- trendy v oblasti informačnej a kybernetickej bezpečnosti alebo IoT zariadenia,
- použitie nových technológií pre zabezpečenie plynulého neprerušovaného chodu procesov,
- použitie nových technológií pre zefektívnenie skúšobných postupov, ako automatizácia opakovaných činností a s tým spojená možnosť simultánneho

vykonávania viacerých činností a možnosť riadenia skúšobných činností diaľkovo.

Hrozby

- dlhý čas vyškolenia kvalifikovaného experta, čo je problematické pri zavádzaní nových činností,
- dlhý čas prispôsobovania sa novým trendom, ktoré nesúvisia s aktuálne vykonávaným portfóliom služieb,
- rozrastajúca sa konkurencia.

3.4 Identifikované problémy a dôvody pre zavedenie monitoringu siete

Sieť, ako aj všetky zariadenia sú závislé od údržby, ktorú poskytujú traja zamestnanci IT oddelenia, čo je samé o sebe problematické pri takom množstve zariadení. Sieť, ktorá je v budove vytvorená, bola naviac budovaná niekoľko rokov postupne, s dôrazom na nízke investície, a je prakticky nezdokumentovaná. Pracovníci sa nemôžu venovať iným činnostiam, ktoré vyžadujú ich pozornosť, ako napríklad zlepšovaniu stávajúceho firemného softvéru pre zvyšovanie efektivity procesov, nakoľko sa neustále zaoberajú problémami vzniknutými v sieti, alebo updatami a konfiguráciou nových systémov a počítačov, či ich opravami. Tieto činnosti zaberajú väčšinu ich pracovného času. Problematický je aj fakt, že pre týchto zamestnancov neexistuje zastupiteľnosť.

V organizácii sa taktiež používa veľké množstvo rôznych druhov softvérov, namiesto jedného riešenia na mieru. Množstvo z nich závisí od internetového pripojenia a od správnej funkčnosti siete. Veľkým problémom sú tiež výpadky napájania, alebo poruchy počas skúšok, ktoré môžu trvať niekoľko hodín aj dní, a ktoré prebiehajú častokrát v noci alebo cez víkendy. Pri výpadku elektrickej siete a následnej strate dát je teda potrebné začať skúšanie znovu. Rovnako potrebné sú kamery, ktoré nahrávajú priebeh niektorých skúšok a monitorujú bezpečnosť priestorov. Efektívnosť procesov je závislá aj od zdieľaných údajov na sieti, ktoré musia byť neustále dostupné.

Okrem bežných problémov vyplývajúcich z činnosti sa spoločnosť potýka aj s využívaním počítačových prostriedkov a zdrojov na súkromné účely. Jedná sa napríklad o hranie hier a sledovanie sociálnych médií počas pracovnej doby. Tento problém je

riešený blacklistom. Vzhľadom na vyšší počet zamestnancov sa však takáto činnosť v sieti nedá kontrolovať bez monitorovacieho nástroja.

Pri menovaní dôvodov pre zavedenie nástroja na monitorovanie siete vyvstáva predovšetkým potreba požiadavky na správu porúch, konfigurácie a výkonu. Monitorovanie systémov a sietí umožní správcovi kontrolovať zdroje, ich využitie a spotrebu. Nepretržité monitorovanie pomáha zvyšovať výkon siete tým, že identifikuje problémy v sieti a napomáha zachovávať stav hardvéru, čím sa minimalizuje čas do opravy a skracuje prerušenie procesov.

3.5 Definícia požiadaviek spoločnosti na monitorovací nástroj

Na základe výsledkov vykonaných analýz a konzultácií s technickými pracovníkmi boli definované požiadavky, ktoré spoločnosť kladie na nový monitorovací nástroj. Najväčšie nedostatky, s ktorými sa spoločnosť potýka v oblasti managementu počítačovej siete, sú riešiteľné predovšetkým správou porúch a správou konfigurácie.

Pre spoločnosť je potrebné nájsť nástroj, ktorý umožní monitoring siete a dokáže informovať správcu o celkovom stave siete, výkone a možných problémoch v sieti.

Definované boli nasledujúce požiadavky na nástroj – monitoring:

- podpora štandardných monitorovacích protokolov,
- monitoring šírky pásma a využitie,
- zisťovanie dostupnosti sieťových zariadení (smerovače, prepínače, firewall, servery a ďalšie) a monitoring zdravia zariadení, pamäte, diskov, CPU,
- zisťovanie dostupnosti kritických služieb (aplikácie, e-mail, web server, FTP server a ďalšie),
- možnosť škálovateľnosti,
- uchovávanie histórie,
- možnosť automatizovanej nápravy a preddefinovanej reakcie na udalosť,
- možnosť konfigurácie zariadení na diaľku,
- možnosť monitorovania pracovných staníc s operačným systémom Windows,

- aktívny vývoj softvéru, ktorý zohľadní nové trendy a zabezpečí rýchle reakcie na problémy a chyby,
- upozorňovanie na udalosti v sieti, ako sú výpadky, zlyhanie prvkov v sieti, zmeny stavu zariadení, prekročenie hraničných hodnôt a ďalšie. Oznamovanie v preferovanej forme e-mailu a SMS správ,
- možnosť prístupu viacerých používateľov s definovateľnými právomocami a obsahom,
- ľahko ovládateľný,
- ľahko nastaviteľný,
- prehľadné a jednoducho navigovateľné používateľské rozhranie s grafickou vizualizáciou,
- dostupnosť podpory a dokumentácie,
- možnosť použitia skúšobnej verzie,
- prijateľná cena.

3.6 Analýza nástrojov pre správu siete

Nástroje, ktoré budú analyzované v nasledujúcich podkapitolách, boli vybrané na základe požiadaviek spoločnosti. Po zhodnotení týchto požiadaviek sme prišli k záveru, že vhodné monitorovacie riešenie pre vybranú spoločnosť bude nástroj, ktorý obsahuje ako štandardné monitorovacie funkcie, tak aj špeciálne funkcie, pre vybrané monitorovacie oblasti. Takýto nástroj monitoruje sieť so všetkými zariadeniami, systémami a aplikáciami, ako aj sieťovú prevádzku. Pri výbere boli tiež zohľadnené nároky na počet monitorovaných zariadení, a preto sa budeme sústrediť na nástroje, ktoré sú vhodné pre malé a stredné podniky. Naviac sme sa zamerali na nástroje, ktoré sú celosvetovo najviac používané a majú najlepšie používateľské hodnotenie, nakoľko tieto sú overené v praxi a majú vybudovanú veľkú podpornú používateľskú komunitu.

Pri každom nástroji budeme popisovať jeho funkcie, výhody a nevýhody a cenovú politiku nástroja, ako aj služieb s ním spojenými, pokiaľ ich poskytovatelia týchto technológií zverejňujú.

Z veľkého množstva nástrojov pre správu siete boli pre podrobnejšiu analýzu vybrané nástroje Nagios, PRTG Network Monitor, Zabbix a WhatsUp Gold.

3.6.1 Nagios

Systémy pre monitorovanie sietí Nagios sú vyvíjané spoločnosťou Nagios Enterprises založenej v roku 2007. Autorstvo patrí Ethanovi Galstadovi a ďalším vývojárom, ktorí sa podieľali na tvorbe prvej verzie produktu od roku 1999 [18].

Nagios je komplexný systém monitorovania IT infraštruktúry, ktorý deteguje a napomáha riešiť problémy spojené s kritickými procesmi. Je schopný monitorovať kritické servery, rôzne typy sieťových zariadení, služieb, protokolov a aplikácií, pomocou vstavaných interných funkcií, ale aj externých pluginov tretích strán. Umožňuje viesť záznamy o udalostiach, výpadkoch a zlyhaniach a ponúka systém upozornení pri identifikácii neželaných stavov. Nagios pracuje ako multiplatformový softvér [18].

Základom monitorovacieho systému je Nagios démon, ktorý umožňuje spúšťanie pluginov cez *process scheduler*, plánovač procesov, nainštalovaných na vzdialených hostiteľoch, teda na monitorovaných zariadeniach. Pluginy zhromažďujú údaje a posielajú ich naspäť. Po spracovaní dát, následne démon odosiela notifikácie používateľom a aktualizuje GUI, prípadne vykonáva iné naplánované úlohy. Nagios je možné používať bez agentov, len s použitím pluginov, alebo s agentami, ako napríklad agent NRPE (*Nagios Remote Plugin Executor*), ktorý spúšťa kontroly a pluginy na vzdialených zariadeniach, alebo agent NSClient++, ktorý umožňuje monitoring systémov Windows [18].

Z portfólia spoločnosti nás budú zaujímať produkty Nagios XI a Nagios Core. Nagios Core sa zaraďuje medzi riešenia s otvoreným kódom a je poskytovaný bezplatne k stiahnutiu, užívaniu a upravovaniu. Naproti Nagios Core stojí komerčne používaná verzia Nagios XI, ktorý vznikol z požiadavky na väčšiu škálovateľnosť a doplnenie o podnikové funkcie, ktoré pôvodnému Nagios Core chýbajú. Nagios Core naviac vyžaduje pokročilé technické znalosti. Tento problém rieši XI prívetivým webovým používateľským rozhraním, ktoré je vhodné aj pre netechnických používateľov. Nagios Core je síce zdarma, ale vyžaduje investíciu do netechnických zdrojov, akými sú zaškolení technickí zamestnanci a taktiež je časovo náročnejší [18].

Prehľad funkcií Nagios Core:

- monitoring sieťových zariadení pomocou agentov,
- monitoring sieťových služieb cez protokoly ako SMTP, POP3, HTTP, NNTP, Ping a ďalšie,
- monitoring ostatného hardvéru prostredníctvom pluginov,
- podpora vzdialeného monitorovania, vrátane vzdialene spustiteľných skriptov a doplnkov,
- schopnosť hierarchickej definície sieťových zariadení,
- podpora *auto-discovery* cez plugin,
- možnosť vývoja vlastných pluginov,
- možnosť vytvárania a odosielania upozornení formou e-mailu, textovej správy alebo ďalších,
- možnosť definície reakcií na udalosti pre proaktívne riešenie problémov,
- podpora distribuovaného monitoringu,
- možnosť zobrazenia vo webovom rozhraní [18].

Prehľad funkcií Nagios XI:

- jednoduché používateľské webové rozhranie, obsahujúce všetky potrebné informácie o aktuálnom stave zariadení, ako aj historické údaje, či grafické a tabuľkové výstupy,
- prispôsobiteľné panely s informáciami o statuse zariadení v sieti,
- prediktívne plánovanie kapacít,
- hromadné úpravy a zmeny, ako napríklad aktualizácia stoviek zariadení naraz,
- plánovanie správ a upozornení pre kľúčové osoby prostredníctvom textových správ a e-mailov, či v iných formách,
- možnosť použitia sprievodcu konfiguráciou, ktorý navádza používateľa pri procese monitorovania nových zariadení, služieb a aplikácií,

- možnosť prístupu viacerých používateľov naraz, s možnosťou prispôsobenia používateľského rozhrania tak, aby mohli používatelia pristupovať iba k informáciám, na ktoré majú oprávnenie [18].

Cenová politika:

- Nagios Core – zdarma,
- Nagios XI – štandardná licencia pre 300 monitorovaných uzlov stojí približne 4 308,71 € [18].

Minimálne systémové požiadavky:

- pevný disk 20 GB,
- pamäť 2 GB,
- dvojjadrové CPU, 2.4 GHz,
- operačný systém CentOS, Redhat Enterprise Linux, Ubuntu, Debian,
- databáza MySQL, Maria DB, PostgreSQL [18].

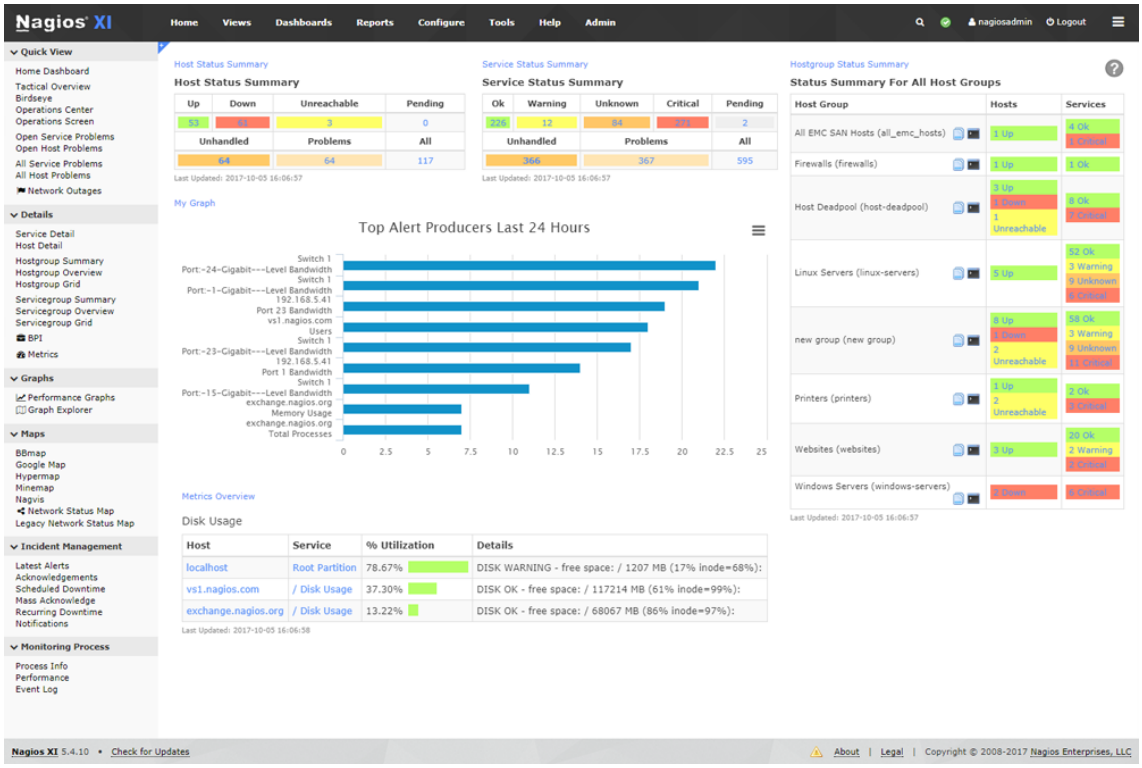
Systémové požiadavky sa odvíjajú od počtu monitorovaných uzlov. Menej ako 500 uzlov bude vyžadovať približne 2 500 monitorovacích služieb. Miesto na pevnom disku by malo mať približne 120 GB, štvorjadrové CPU a RAM 8 GB [18].

Výhody:

- možnosť jednoduchého nastavenia monitorovania najčastejšie monitorovaných zariadení cez sprievodcu,
- podpora monitoringu bez agenta, s agentom, alebo kombinácia oboch,
- 30-denná skúšobná verzia pri Nagios XI,
- Nagios Core bez licenčných poplatkov,
- prívetivé webové používateľské rozhranie,
- grafické a tabuľkové vizualizácie technických dát pre obchodné potreby,
- nástroj podporuje rozšíriteľnú architektúru.

Nevýhody:

- konfigurácia Nagios Core je komplikovaná,
- spoplatnená technická podpora.



Obrázok č. 6: Používateľské rozhranie Nagios XI

(Zdroj: 19)

3.6.2 PRTG Network Monitor

Ďalším analyzovaným nástrojom je PRTG (*Paessler Router Traffic Grapher*) Network Monitor, ktorý v roku 1997 vytvorila nemecká spoločnosť Paessler AG, na čele s Dirkom Paesslerom [20].

PRTG Network Monitor je komplexným riešením monitorovania sietí, systémov a aplikácií v IT infraštruktúre. Poskytuje veľké množstvo monitorovacích funkcií, vďaka ktorým umožňuje monitorovať sieť a predchádzať problémom, ktoré by potencionálne mohli v sieti vzniknúť. Okrem toho umožňuje monitoring šírky pásma a premávky, využitie siete a dostupnosti zariadení, hardvéru, softvéru, webových a cloudových

služieb, e-mailov, virtuálneho prostredia, databáz či periférnych zariadení a umožňuje aj monitoring viacerých vzdialených miest naraz. Umožňuje vytvárať podrobné štatistiky o všetkých zariadeniach. Je vhodný pre všetky typy sietí, či už vo veľkých špecializovaných zariadeniach v priemyselnom prostredí, alebo v malých a stredných firmách [20].

PRTG pozostáva z hlavného servera a zo sond. Základný server PRTG tvorí centrálnu časť, nakoľko obsahuje samotný nástroj správy, hlavné úložisko, API server, web server, mechanizmus pre vytváranie a odosielanie notifikácií, a ďalšie. PRTG sondy vykonávajú monitorovanie a všetky údaje z monitoringu odosielajú hlavnému serveru. Môžu byť lokálne, vzdialené, ale aj klastrové. Monitoring funguje bez agentov a PRTG nevyžaduje žiadne ďalšie doplňujúce pluginy [20].

Samotné monitorovanie prebieha prostredníctvom senzorov, ktoré je možné priradiť ku každému zariadeniu, aplikácii či službe, vzhľadom na to, čo konkrétne chceme monitorovať. Platforma poskytuje množstvo senzorov, či už je to SNMP senzor, alebo iné senzory ako Ping, WMI, ICMP, HTTP, DNS, FTP, SMTP, POP3, IMAP, WMI, MQTT, SOAP, SSH, DICOM a mnohé ďalšie. Systém obsahuje preddefinované šablóny senzorov, ktoré zabezpečia kontrolu bežných zariadení aj aplikácií. Tieto šablóny podstatne uľahčujú konfiguráciu systému. Samotná konfigurácia je pomerne jednoduchá aj vďaka tzv. *smart setup*. Systém má tiež *auto-discovery*, ktoré umožňuje automatické rozpoznanie zariadení v sieti. Podporuje väčšinu renomovaných dodávateľov IT (Cisco, VMware, Hyper-V, Microsoft, HPE, Oracle, Juniper, HP, Dell, APC a ďalšie). Používateľské prostredie PRTG Network Monitor je prívetivé a ľahko ovládateľné. Používateľ má možnosť pristupovať k monitorovaciemu nástroju cez webové rozhranie a cez počítačovú alebo mobilnú aplikáciu [20].

Prehľad funkcií PRTG Network Monitor:

- monitorovanie sieťových zariadení, šírky pásma, aplikácií, virtuálnych serverov, cloudových služieb, monitorovanie využitia systému (napríklad zaťaženie procesora, voľná pamäť alebo voľné miesto na disku), monitoring výkonu databázy a tabuľkových hodnôt, e-mailových a webových serverov, či monitoring dostupnosti softvéru ako služby,

- monitoring bez agentov, prostredníctvom senzorov ako Ping, WMI, ICMP, HTTP, DNS, FTP, SMTP, POP3, IMAP, či WMI a ďalšie,
- podpora distribuovaného monitorovania, prostredníctvom vzdialených sond,
- detailné logové záznamy,
- podpora *auto-discovery* a *smart setup*,
- jednoduché a prehľadné užívateľské prostredie s možnosťou použitia desktopovej či mobilnej, alebo webovej aplikácie. Užívateľské prostredie je prispôsobiteľné, zobrazuje mapy, informačné panely a vizualizuje sieť v reálnom čase,
- komplexný prispôsobiteľný systém správ a upozornení s rôznymi formami, ako e-mail, SMS, Slack, Microsoft Teams, push notifikácie, HTTP požiadavka, exe, skript, syslog atď.,
- možnosť definovania používateľov a pridelenia oprávnení,
- možnosť vytvorenia klastra z dvoch alebo viacerých základných serverov, pre zabezpečenie vysokej dostupnosti monitorovania,
- automatická kontrola zálohovania,
- monitorovanie SLA [20].

Cenová politika

Z portfólia spoločnosti nás bude zaujímať PRTG Network Monitor. Licencovanie reflektuje počet senzorov. Prvá licencia začína na 500 senzoroch a nasledujú verzie s 1 000, 2 500 a 5 000 senzormi, XL1 verzia, ktorá má približne 10 000 senzorov a neobmedzená Enterprise verzia. V našom prípade by bola vhodná verzia s 2 500 senzormi, ktorá je určená približne pre 250 zariadení. Cena tejto verzie je 4 950 € [20].

Minimálne systémové požiadavky

Je potrebné, aby hlavný server s PRTG, ako aj diaľkové sondy bežali na operačných systémoch Windows Server 2012 R2/2016/2019 alebo Windows 10 a zároveň servery aj sondy musia byť 64-bitové systémy. Nutnou podmienkou je nainštalovaný Microsoft

.NET Framework 4.7.2. Odporúčania pre server sú ďalej rozčlenené vzhľadom k počtu monitorovaných zariadení a z toho vyplývajúceho počtu senzorov:

- počet senzorov na server: 1 000 - 2 500 senzorov (cca. 250 zariadení) - licencia PRTG 2 500,
- odporúčaný hardvér servera: minimum 8 CPU jadier, 8 GB RAM,
- miesto na disku (na cca. 1 rok údajov): 750 GB,
- počet súbežne aktívnych administrátorských relácií: < 20,
- počet diaľkových sond: < 60 [19].

Požiadavky pre diaľkové sondy:

- odporúčaný hardvér sondy (200 až 2 000 senzorov): minimum 4 CPU jadrá, 4 GB RAM,
- miesto na disku: 40 GB [20].

Výhody:

- široké možnosti monitoringu,
- jednoduché nastavenie,
- podpora rôznych operačných systémov,
- spoločnosť ponúka možnosť hosťovaného monitorovania, pri ktorom spravuje hlavný server,
- dostupná skúšobná verzia,
- každá licencia obsahuje všetky funkcie, takže nie je potrebné dokupovať ďalšie moduly. Pri prechode na vyššiu verziu stačí doplatiť cenový rozdiel.
- technická podpora na dobrej úrovni.

Nevýhody:

- cena,
- zložité licencovanie na základe senzorov, ktoré môže byť mätúce,

- obmedzené použitie niektorých funkcií, ktoré zaťažujú CPU, ako sú často obnovované mapy, časté a veľké správy, neustále monitorovacie dopyty, časté automatické zisťovanie siete atď.,
- stabilita aplikácie,
- založené na Windows operačných systémoch,
- vytváranie máp je komplikované.

Obrázok č. 7: Používateľské rozhranie PRTG Network Monitor

(Zdroj: 20)

3.6.3 Zabbix

Zabbix je monitorovací nástroj, ktorého prvá verzia vyšla v roku 2001, a ktorý bol vytvorený a je udržiavaný litovskou spoločnosťou Zabbix LLC, na čele s tvorcom a majiteľom Alexeiom Vladishevom [21].

Zabbix je open-source nástroj, ktorý vychádza pod licenciou GNU General Public License verzie 2. Tento nástroj umožňuje monitorovanie sieťových prvkov, serverov, aplikácií, cloudových služieb, monitorovanie virtuálnych strojov, služieb, web serveru, či databáz. Okrem toho dokáže monitorovať IoT zariadenia, či niektoré priemyselné protokoly. Umožňuje automatickú detekciu problémov v sieti v reálnom čase, ktoré kategorizuje podľa rôznych stupňov závažnosti. Deteguje anomálie pomocou základného

monitorovania, ale umožňuje aj proaktívnu predikciu trendov. Zabbix je použiteľný ako v malých, tak aj vo veľkých podnikoch s veľkým počtom zariadení [21].

Centrálnym komponentom Zabbixu je server, ktorý funguje ako centrálne úložisko. Agenti aktívne monitorujú zariadenia a aplikácie a odosielajú všetky zhromaždené monitorovacie dáta Zabbix serveru na ďalšie spracovanie. Agenti vykonávajú pasívne aj aktívne kontroly. Zabbix podporuje aj monitorovanie bez agentov, s využitím protokolov ako SNMP, či rozhranie IPMI (*Intelligent Platform Management Interface*) či JMX (*Java Management Extensions*). Voliteľnou súčasťou Zabbixu je Zabbix proxy, ktorý zhromažďuje monitorovacie údaje namiesto servera, čo umožňuje vytvorenie distribuovaného monitoringu a rozloženie záťaže servera [21].

Prístup k používateľskému rozhraniu je zabezpečený webovým rozhraním. Je pomerne jednoducho ovládateľné a prehľadné. Výhodou platformy je možnosť konfigurovateľnej vizualizácie. Používatelia tak môžu vytvoriť prehľadný vizuálny systém celej IT infraštruktúry s rôznymi grafmi, tabuľkami, mapami, či inými výstupmi [21].

Prehľad funkcií:

- monitoring sieťových zariadení, cloudových služieb, virtuálnych strojov, operačných systémov, databáz, aplikácií, služieb, IoT, web servera, a mnohých ďalších,
- metriky rôznych typov,
- monitoring s agentom aj bez agenta,
- možnosť vytvárania vlastných skriptov,
- distribuovaný monitoring,
- podpora syntetického monitoringu s možnosťou vytvárania scenárov,
- automatická detekcia anomálií a problémov a predikcia trendov,
- podpora analýzy koreňovej príčiny,
- možnosť konfigurácie správ a notifikácií a ich odosielanie na základe typu a role príjemcu. Nástroj umožňuje aj eskaláciu hlásení a auto-sanačné opravné skripty,

- odosielanie výstražných a informačných správ prostredníctvom viacerých kanálov, či už cez výstražné systémy, alebo e-mail, SMS, komunikačné platformy ako MS Teams a pod.,
- široké možnosti definovania rolí a podpora rôznych metód autentifikácie,
- SLA monitoring a ITIL metriky,
- široké možnosti integrácie,
- rýchle nasadenie,
- možnosť využitia predpripravených šablón na monitoring,
- podpora *auto-discovery*,
- možnosť zabezpečenia vysokej dostupnosti nasadením sekundárneho Zabbix servera [21].

Minimálne systémové požiadavky

Systémové požiadavky sa odvíjajú od počtu monitorovaných uzlov. Na cca. 500 monitorovaných uzlov je potrebné, aby hlavný server spĺňal tieto minimálne podmienky:

- 4 GB RAM,
- štvorjadrové CPU,
- miesto na pevnom disku najmenej 120 GB,
- operačné systémy typu unix alebo linux,
- databáza MySQL, Maria DB, PostgreSQL, Oracle,
- pre frontend je potrebný Apache a PHP [21].

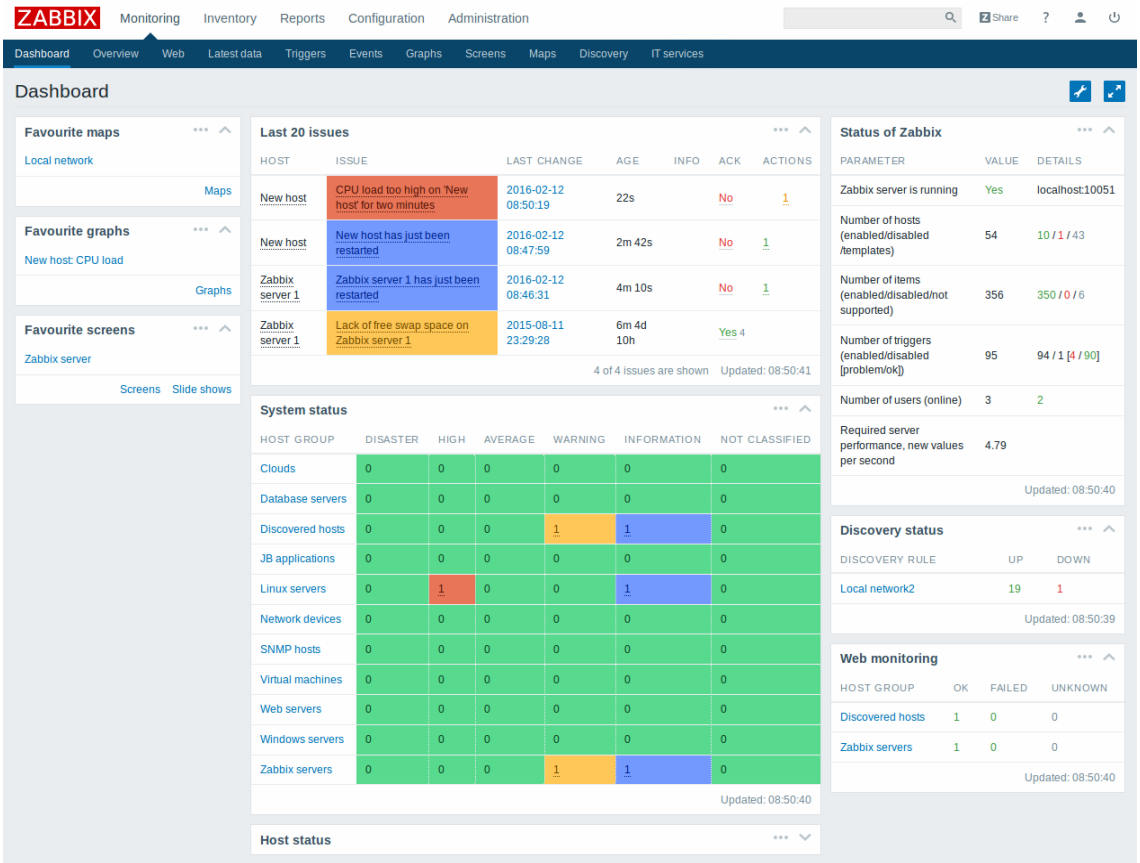
Výhody:

- bezplatná platforma,
- vysoko prispôsobiteľné panely,
- prepracovaný systém upozornení,
- systém šablón,

- možnosť monitoringu a agentom aj bez agenta.

Nevýhody:

- server Zabbix nie je možné inštalovať na OS Windows,
- vyžaduje pokročilé technické znalosti,
- je náročný na zdroje,
- nemá podrobnú dokumentáciu a oficiálnu technickú podporu.



Obrázok č. 8: Používateľské rozhranie Zabbix

(Zdroj: 22)

3.6.4 WhatsUp Gold

Monitorovací nástroj s názvom WhatsUp Gold bol pôvodne vytvorený spoločnosťou Ipswitch, Inc. v roku 1996. Túto spoločnosť v roku 2019 akvizovala americká spoločnosť Progress Software Corporation, zaoberajúca sa vývojom podnikových aplikácií, ktorá vyvíja a udržuje tento produkt aj naďalej [23].

WhatsUp Gold sa v základnej edícii zameriava na monitoring výkonu siete. Podporuje funkciu *auto-discovery*, vďaka ktorej dokáže prehľadať systém a nájsť všetky sieťové zariadenia, vrátane novo pridaných. Taktiež má funkciu mapovania topológie siete s automatickou aktualizáciou. Systém umožňuje včasnú detekciu udalostí a problémov, na ktoré sú kľúčoví používatelia upozornení cez notifikácie formou e-mailu, alebo SMS. Upozornenia majú široké konfiguračné možnosti. Rozšírenie funkcionality je zabezpečené prídavnými modulmi. Tieto umožňujú napríklad analýzu sieťovej prevádzky s podporou protokolov ako NetFlow, sFlow, J-Flow, SEL, QUIC a IPFIX. Tiež umožňujú monitoring aplikácií, cloudových služieb, webového servera, databáz, mail servera, či súborového servera a ďalších prostredníctvom protokolov ako WMI, SNMP, TCP, UDP, SSL a iných. Podporuje správu konfigurácie, vďaka ktorej je možné robiť zmeny v konfigurácii u veľkého počtu zariadení naraz, alebo nakonfigurovať nové zariadenie jednoducho podľa predošlých [23].

Základné zložky, ktoré tvoria WhatsUp Gold sú hlavný server, databáza a kolektor, ktorý je centralizovaný, alebo založený na agentoch a používateľské rozhranie [23].

Prehľad funkcií:

- monitoring bez agenta aj s agentom,
- monitorovanie výkonu siete, monitorovanie šírky pásma a analýza paketov, monitorovanie aplikácií, monitorovanie virtualizácie, správa konfigurácie, log management a failover management,
- podpora *device discovery*,
- mapovanie a dokumentácia sieťových zariadení,
- podpora distribuovaného monitoringu,
- používateľské prostredie vo forme desktop, webovej aj mobilnej aplikácie,
- prispôsobiteľné oznámenia formou e-mailu a SMS,
- možnosť definície rolí používateľov,
- podpora monitoringu SLA [23].

Cenová politika

Spoločnosť ponúka základný balík a kompletnú edíciu, ktoré je možné kúpiť s ročným predplatným, alebo ako trvalú licenciu. Okrem toho spoločnosť ponúka k zakúpeniu aj prídavné moduly, ktoré sú súčasťou kompletnej edície. Licencovanie je následne závislé na počte serverov a monitorovaných zariadení. Najnižšia licencia začína na 25 zariadeniach, nasleduje menej ako 100, 300, 500, 1 000, 2 500 a licencia nad 2 500 zariadení. Licenciu 500 môžeme rozdeliť napríklad na monitoring 250 zariadení, 20 aplikácií a 5 zdrojov toku. Spoločnosť konkrétnu cenu na svojich stránkach nezverejňuje, preto je potrebné vyžiadať si oficiálnu cenovú ponuku po zadaní jednotlivých parametrov. Niektoré zdroje však uvádzajú cenu približne 2 440 € za 25 zariadení [23].

Minimálne systémové požiadavky

Server WhatsUp Gold podporuje iba operačný systém Windows Server 2012 R2/2016/2019 a zároveň server musí byť 64-bitový systém. Odporúčania pre server:

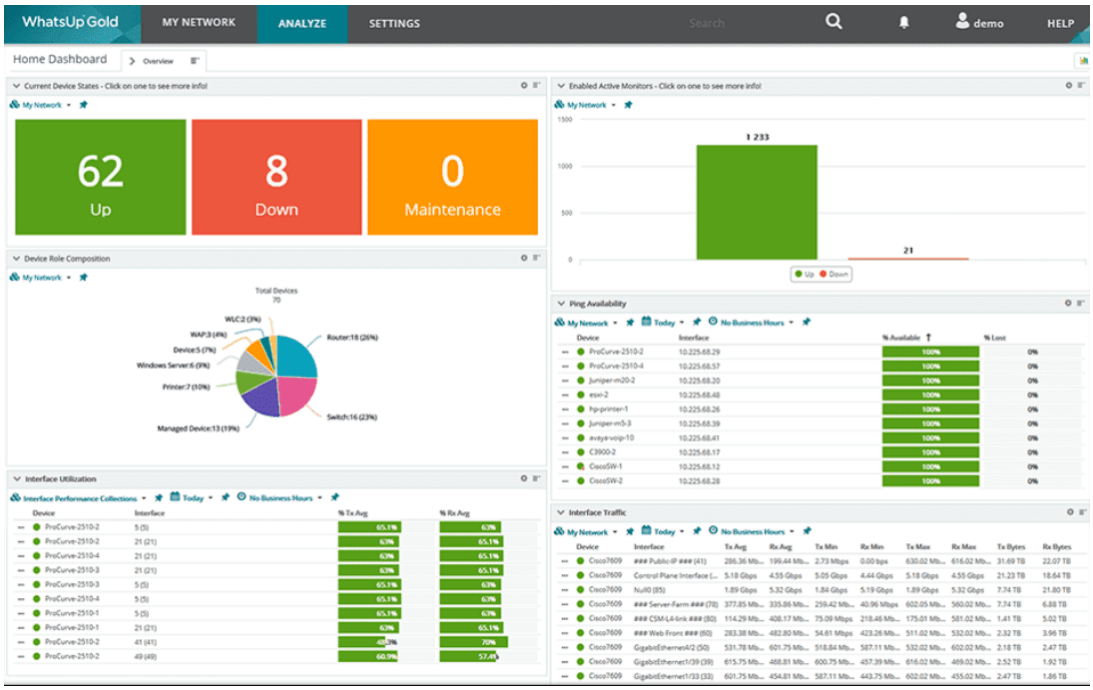
- odporúčaný hardvér servera: minimum 4 CPU jadrá, 8 GB RAM,
- miesto na disku (na menej ako 500 zariadení): 25 GB [23].

Výhody:

- intuitívne používateľské prostredie a jednoduchá navigácia,
- široký výber preddefinovaných monitorovacích šablón,
- monitoring bez agentov s veľkým výberom protokolov,
- podpora zahrnutá v cene,
- ponúka bezplatnú skúšobnú verziu.

Nevýhody:

- musí byť inštalovaný lokálne,
- pri veľkom počte monitorovaných zariadení je používateľské prostredie neprehľadné a ťažkopádne,
- nejasné licencovanie a cena.



Obrázok č. 9: Používateľské rozhranie WhatsUp Gold

(Zdroj: 23)

3.7 Zhrnutie analýzy

V tejto časti práce bola analyzovaná spoločnosť XYZ, s.r.o., zaoberajúca sa skúšaním, posudzovaním zhody výrobkov a certifikáciou. Na základe analýzy boli definované dôvody pre zavedenie nástroja na monitorovanie siete s dôrazom na potrebu správy porúch, konfigurácie a výkonu. Po zhodnotení požiadaviek, ktoré na monitorovací nástroj kladie spoločnosť, ako aj zhodnotení dôvodov pre zavedenie riešenia pre monitorovanie siete, boli vybrané nástroje pre správu siete, ktoré obsahujú ako štandardné monitorovacie funkcie, tak aj špeciálne funkcie, pre vybrané monitorovacie oblasti. Konkrétne sme analyzovali nástroje Nagios, PRTG Network Monitor, Zabbix a WhatsUp Gold. Pri každom nástroji bola popísaná jeho funkcionalita, systémové požiadavky, výhody a nevýhody a cenová politika.

4 VLASTNÝ NÁVRH RIEŠENIA

Posledná kapitola je venovaná výberu konkrétnej technológie, ktorá naplní požiadavky kladené spoločnosťou a reflektuje výsledky analýzy súčasného stavu spoločnosti. Následne je zhotovený návrh implementácie tejto technológie v spoločnosti XYZ, s.r.o., vrátane technických aspektov a aspektov managementu nasadenia novej technológie do spoločnosti.

4.1 Výber monitorovacieho nástroja

Pre výber konkrétneho softvérového riešenia použijeme systém hodnotenia podľa vybraných kritérií, znázornených v tabuľke č. 1. Tieto kritériá, majú priradenú dôležitosť (D) na stupnici 1 až 5 od najmenej dôležitého po najdôležitejšie. Jednotlivé kritéria sú ďalej ohodnotené na základe rovnakej stupnice. Celkové hodnotenie je súčtom jednotlivých súčinov dôležitosti kritéria a hodnoty kritéria.

Pri hodnotení naplnenia kritérií jednotlivých nástrojov sme vychádzali z dostupných verejných zdrojov, ktoré sú určené na porovnávanie funkcionality týchto nástrojov, z používateľských skúseností a z vlastných skúseností s týmito nástrojmi.

Tabuľka č. 1: Hodnotenie vybraných monitorovacích nástrojov

(Zdroj: Vlastné spracovanie)

Hodnotiace kritérium	D	Nagios	PRTG	Zabbix	WhatsUp Gold
Monitoring sieťových zariadení a kritických služieb	5	4	5	5	4
Preddefinované reakcie na udalosti	3	3	4	4	3
Integrácia a jednoduchosť nasadenia	3	3	5	3	3
Podporované OS Windows	2	1	5	1	5
Monitoring bez agentov	3	2	5	3	3
Škálovateľnosť	2	3	4	3	3
Distribuovaný monitoring	4	5	5	4	4

Notifikácie	5	4	5	5	5
História	3	5	5	5	5
Syslog	3	5	5	5	5
Nevyžaduje ďalšie pluginy	4	1	4	2	2
Používateľské rozhranie	2	4	5	3	5
Prístup viacerých používateľov	3	5	5	5	5
Jednoduché a intuitívne ovládanie	4	3	5	4	3
Podpora a dokumentácia	3	3	4	3	2
Skúšobná verzia	1	5	5	5	5
Cena	3	3	3	5	2
Hodnotenie	**-**	**295**	**395**	**325**	**320**

4.1.1 Hodnotenie monitorovacích nástrojov

Nagios

Nagios je kvalitný monitorovací nástroj s komplexnou monitorovacou spôsobilosťou. Nižšie hodnotenie získal kvôli nesplneniu požiadavky na podporu platformy OS Windows, ďalej kvôli potrebe ďalších pluginov a tiež kvôli obmedzenej funkcionalite pri monitoringu bez agentov. Nagios má okrem toho pomerne komplikovanú konfiguráciu.

PRTG Network Monitor

PRTG Network Monitor spĺňa požiadavky kladené spoločnosťou najlepšie z vybraných nástrojov. V jednom nástroji, bez potreby ďalších doplnkov, poskytuje správu všetkých sieťových zariadení rôznych výrobcov, ako aj správu aplikácií. Výhodou tohto produktu je jeho vývoj pre platformu OS Windows, monitoring bez agentov, či distribuovaný monitoring a škálovateľnosť. Nástroj je napriek robustnej funkcionalite pomerne jednoducho konfigurovateľný, ako aj ovládateľný. Jedinou pozorovanou nevýhodou je, že v porovnaní s ostatnými monitorovacími nástrojmi je financovanie pri tomto riešení o niečo drahšie.

Zabbix

Výhodou Zabbixu je nepochybne cena, nakoľko sa jedná o open-source. Tento nástroj spĺňa väčšinu požiadaviek výborne, ale nepodporuje platformu OS Windows a taktiež vyžaduje ďalšie pluginy a doplnky. Tento fakt by mohol viesť ku komplikáciám pri implementácii. Problémové sú tiež ťažko zrozumiteľná dokumentácia a nasadenie nástroja.

WhatsUp Gold

WhatsUp Gold ponúka výkonný nástroj pre správu siete. Pozitívne hodnotenie získal predovšetkým za kvalitný systém notifikácií, podporu platformy OS Windows a za používateľské prostredie. Nasadenie a počiatočná konfigurácia sú však časovo aj technicky náročné. Problematická je podpora a návody, ktoré sú ťažko zrozumiteľné pre menej zdatných technikov. Tento produkt je ponúkaný v základnej verzii, ktorá má obmedzenú funkcionalitu. Rozšírenie funkcionality je možné prostredníctvom ďalších doplnkov, alebo prechodom na vyššiu verziu, čo je nepomerne finančne náročnejšie, ako u iných produktov, ktoré majú túto funkcionalitu už v základnej verzii.

4.1.2 Výber konkrétneho riešenia

Na základe výsledkov z hodnotiaceho systému usudzujeme, že monitorovacím nástrojom, ktorý dosiahol najlepšie celkové hodnotenie, je PRTG Network Monitor. Po konzultáciách o výbere konkrétneho riešenia s managementom spoločnosti a s technickými pracovníkmi sme prišli k záveru, že práve tento systém bude v organizácii implementovaný, nakoľko spomedzi analyzovaných možností najlepšie spĺňa požiadavky kladené spoločnosťou.

4.2 Technické aspekty

V tejto podkapitole sú spracované podmienky pre nasadenie novej technológie pre monitorovanie sietí, postup inštalácie tejto technológie a návrh nastavenia parametrov.

4.2.1 Podmienky pre nasadenie technológie

Pre danú spoločnosť sme sa rozhodli zvoliť licenciu, ktorá obsahuje 2 500 senzorov, čo by malo plne pokrývať monitorovacie potreby spoločnosti.

4.2.1.1 Systémové požiadavky na PRTG Network Monitor

Je potrebné, aby hlavný server s PRTG Network Monitor, ako aj diaľkové sondy bežali na operačných systémoch Windows Server 2019, Windows Server 2016, Windows Server 2012/2012 R2 a zároveň servery aj PC musia byť 64-bitové systémy. Nutnou podmienkou je .NET Framework 4.7.2 alebo novší.

Odporúčania pre server sú ďalej rozčlenené vzhľadom k počtu monitorovaných zariadení a z toho vyplývajúceho počtu senzorov:

- počet senzorov na server: 1 000 - 2 500 senzorov (cca. 250 zariadení),
- licencia: PRTG 2 500,
- odporúčaný hardvér servera: minimum 8 CPU jadrá, 8 GB RAM,
- miesto na disku (na cca 1 rok údajov): 750 GB,
- používateľské účty na PRTG servery: < 20,
- diaľkové sondy: < 60.

Požiadavky pre monitorované zariadenia:

- monitorovanie SNMP - zariadenia musia podporovať a mať povolený protokol SNMP a mať nainštalovaný softvér kompatibilný s týmto protokolom,
- monitorovanie WMI - zariadenia musia podporovať OS Windows,
- monitorovanie IP toku - zariadenia musia byť schopné odosielať dátové pakety NetFlow.

Ako prvé je potrebné skontrolovať technický stav všetkých zariadení a ich systémov tak, aby zodpovedali odporúčaným podmienkam pre inštaláciu. Túto kontrolu vykonajú zamestnanci IT oddelenia.

4.2.1.2. Server

Pre nasadenie monitorovacej technológie je potrebné, aby bol najprv zadovážený server, na ktorom bude inštalovaný PRTG Network Monitor. Pre tieto potreby bude zakúpený nový server DELL PowerEdge R430.

Parametre serveru:

- prevedenie: Rack 1U,
- počet inštalovaných procesorov: 1x Intel Xeon E5-2609 v4,
- počet podporovaných procesov: 2x,
- počet jadier: 8,
- operačná pamäť: 8 GB (1x8) pamäte, DDR4 s frekvenciou 2 666 MHz, s 12 slotmi (6 na jedno CPU) pre 32 GB pamäte. Maximálne rozšírenie pamäte je 384 GB,
- počet inštalovaných diskov: 1x 300 GB HDD SAS,
- počet podporovaných diskov: 4x Hot-Plug,
- inštalovaný zdroj: 1x 550 W,
- porty: 4x 1Gb LAN, 3x USB 2.0, 1x USB 3.0, 1x VGA, 1x RS232.

K serveru bude potrebné zakúpiť naviac ďalší disk. Preto bol vybraný disk DELL Server disk s kapacitou 2 TB. Inštaláciu serveru zabezpečí IT oddelenie spoločnosti.

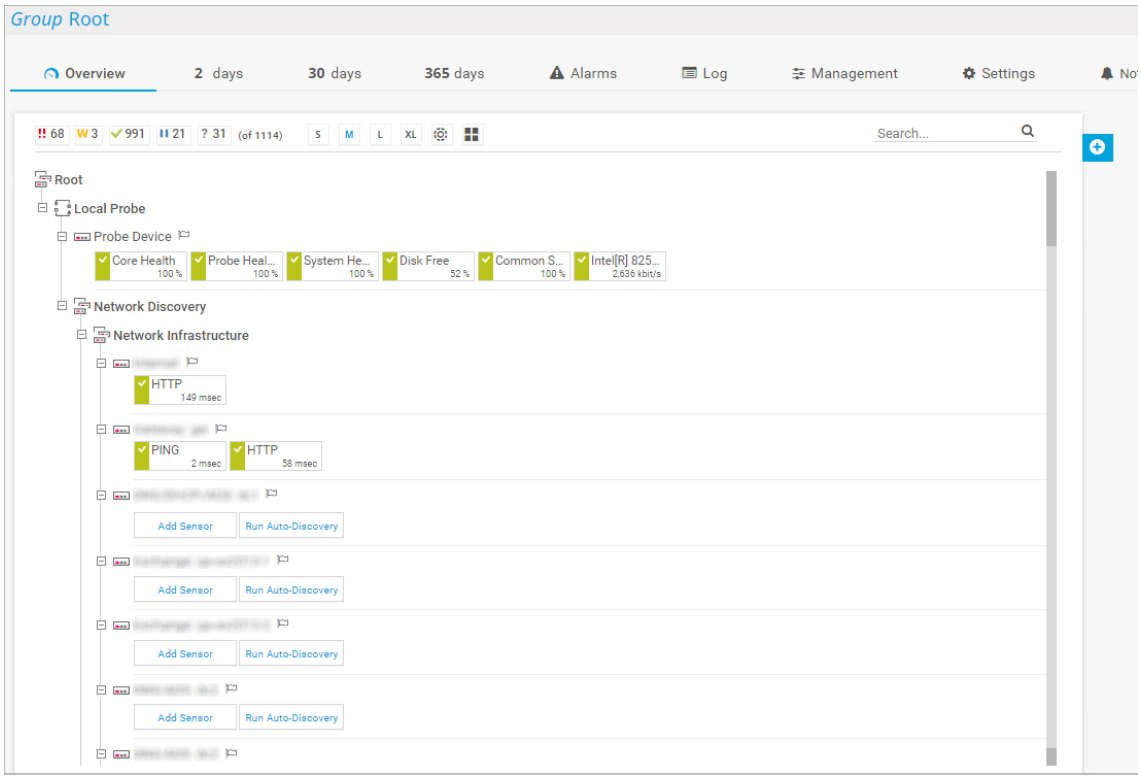
4.2.1.3. Operačný systém

Vzhľadom na to, že server je predávaný bez operačného systému a že PRTG Network Monitor podporuje výhradne operačné systémy Windows, bol vybraný produkt Windows Server 2016 Standard. Inštaláciu operačného systému zabezpečí IT oddelenie spoločnosti.

4.2.2 Postup inštalácie PRTG Network Monitor

Ako už bolo spomenuté, nástroj PRTG Network Monitor má jednoduchú inštaláciu. Po stiahnutí inštalačného súboru spustíme ***s**mart **s**etup*. Sprievodca nás prevedie inštaláciou

na serveri, ktorá obsahuje bežné počiatočné nastavenia, ako jazyk, potvrdenie licenčných podmienok, kontaktná e-mailová adresa. V ďalšom kroku nasleduje možnosť výberu expresného alebo vlastného módu inštalácie. Zvolenie expresného módu nám ihneď umožní automatické vyhľadanie zariadení tzv. *auto-discovery* siete pomocou štandardných protokolov ako SNMP. Počas inštalačného procesu je automaticky aktivovaná licencia cez internet. Po ukončení inštalácie otvoríme webové rozhranie PRTG a prihlásime sa defaultnými údajmi *prtgadmin.*



Obrázok č. 10: Strom zariadení po spustení auto-discovery

(Zdroj: 20)

Po otvorení aplikácie sa zobrazia nájdené dostupné zariadenia tzv. *device tree*, zoradené hierarchicky, s preddefinovanými senzormi. Zariadenia sú rozpoznané skrz Ping IP adries zariadení v rozsahu privátnej siete, takže pre zariadenia v iných podsieťach je potrebné opakovane spustiť *auto-discovery* v ďalšom podrobnejšom setupe. V rámci tohto vyhľadávania zadáme programu aj poverenia správcu Active Directory, čím zaistíme monitoring počítačov aj serverov s OS Windows cez WMI. Zariadenia bez IP adresy, ktoré neboli rozpoznané, doplníme manuálne.

Po tejto inicializácii nastavíme prihlasovacie údaje pre administrátora a vytvoríme ďalšie dva účty pre ostatných pracovníkov IT oddelenia a ďalšie účty pre vedúceho pracovníka všetkých skúšobných oddelení, zástupcu riaditeľa a riaditeľa, nakoľko tieto osoby budú kontaktnými osobami, na ktoré budú eskalované upozornenia.

Ak budeme pristupovať na webové rozhranie PRTG aj z iného počítača, musíme nastaviť SSL/TLS pripojenie. Po inštalácii a úvodných nastaveniach ďalej pokračujeme prihlásení ako administrátor a môžeme začať nastavovaním senzorov a dodatočných senzorov, ktoré neboli automaticky pridelené.

4.2.3 Návrh nastavenia konkrétnych parametrov

4.2.3.1 Nastavenie senzorov

Senzory budú pridané vždy s nadväznosťou na hierarchické usporiadanie monitorovaných zariadení (možnosť vybrať všetky zariadenia v sieti, jedno zariadenie, alebo ľubovoľnú skupinu zariadení). V tomto prípade budú vybraté okrem senzorov priradených zariadeniam po procese *auto-discovery* nasledovné senzory:

Tabuľka č. 2: Zoznam senzorov priradených k zariadeniam

(Zdroj: Vlastné spracovanie)

Senzor	**Popis**
Všetky zariadenia	
Ping Sensor	Umožňuje zisťovanie dostupnosti zariadenia cez sieť; ping time a packet loss.
Core server	
Core Health sensor	Monitoruje stav hlavného servera PRTG.
SNMP Dell PowerEdge Physical Disk sensor	Monitoruje fyzický disk na serveri Dell PowerEdge cez SNMP.
SNMP Dell PowerEdge System Health sensor	Monitoruje stav systému servera Dell PowerEdge cez SNMP.

Všetky servery	
Syslog Receiver sensor	Prijíma syslog správy.
SNMP Hardware Status Sensor	Monitoruje stav hardvérového komponentu servera cez SNMP.
Web server	
Cloud Ping sensor	Monitoruje čas odozvy Ping cieľového servera cez TCP z rôznych miest cez cloud.
Cloud HTTP sensor	Monitoruje čas načítania web servera cez HTTP z rôznych miest cez cloud.
HTTP Data Advanced sensor	Monitoruje prístup k web serveru a získava kódované dáta.
HTTP Advanced sensor	Monitoruje zdrojový kód web stránky cez HTTP.
HTTP Full Web Page sensor	Monitoruje čas sťahovania web stránky.
Všetky servery a PC	
IPMI System Health sensor	Monitoruje stav systému cez IPMI, teplotu a obvodovú teplotu, otáčky ventilátora za minútu (RPM), napätie, stav napájacieho zdroja.
SNMP Disk Free sensor	Monitoruje voľné miesto na disku cez protokol SNMP.
SNMP Memory Sensor	Monitoruje využitie pamäte cez SNMP.
SNMP CPU Load sensor	Monitoruje zaťaženie procesora cez SNMP.
WMI Disk Health sensor	Monitoruje stav disku v systéme Windows cez WMI.
Windows Network Card sensor	Monitoruje využitie šírky pásma a prevádzku sieťového rozhrania cez WMI.
Windows System Uptime sensor	Monitoruje dobu prevádzky systému Windows cez WMI.

Windows Updates Status (PowerShell) sensor	Monitoruje stav aktualizácií systému Windows cez WMI.
WMI Security Center sensor	Monitoruje stav zabezpečenia PC so systémom Windows cez WMI.
WMI Battery sensor	Monitoruje dostupnú kapacitu a stav batérií zariadenia cez WMI.
SSL Certificate sensor	Monitoruje certifikát SSL/TLS.
SSL Security Check sensor	Monitoruje podporu konkrétnej verzie SSL/TLS.
DC server	
The Active Directory Replication Errors Sensor	Monitoruje chyby replikácie v DC.
LDAP sensor	Monitoruje adresárové služby cez LDAP.
Mail server	
POP3 Sensor	Monitoruje čas odozvy mail serveru cez POP3.
SMTP Sensor	Monitoruje čas odozvy mail serveru cez SMTP.
IMAP Sensor	Monitoruje mail server cez IMAP, vrátane času odozvy, počtu e-mailov a umožňuje kontrolu definovaných kľúčových slov.
SMTP&IMAP Round Trip sensor	Monitoruje čas doručenia e-mailu do schránky IMAP cez SMTP.
SMTP&POP3 Round Trip sensor	Monitoruje čas doručenia e-mailu do schránky POP3 cez SMTP.
SNMP System Uptime sensor	Monitoruje dobu prevádzky zariadenia cez SNMP.
SNMP Traffic sensor	Monitoruje prevádzku na zariadení cez SNMP.
Switch	
SNMP Cisco ADSL sensor	Monitoruje štatistiky ADSL Cisco switchu.

SNMP Cisco System Health Sensor	Monitoruje stav systému zariadenia Cisco cez SNMP.
SNMP Traffic Sensor	Monitoruje prevádzku na zariadení cez SNMP.
UPS	
SNMP APC Hardware sensor	Monitoruje výkon na zariadení UPS APC cez SNMP.
Tlačiareň	
SNMP Printer Sensor	Monitoruje tlačiareň cez SNMP, napríklad stavy tonera, papiera, zaseknutia.
The Windows Print Queue Sensor	Monitoruje tlačový front zariadenia.

4.2.3.2. Nastavenie notifikácií

PRTG má nasledujúce stavy senzorov, ktoré sú farebne odlíšené, a ktoré zároveň odrážajú prioritu:

- ***Up*** – zelená – senzor prijíma údaje zo zariadenia,
- ***Warning*** – žltá – systém sa nemôže dostať k zariadeniu, ale opätovne sa o to pokúša, preto hlási upozornenie. Tento stav sa zmení na *Down*, alebo *Up*, po vypršaní určeného limitu,
- ***Down*** – červená – systém sa nemôže dostať k zariadeniu, alebo bola detegovaná chyba,
- ***Down (Acknowledged)*** – bledoružová – po vyslaní alarmu o stave zariadenia bol jeho stav potvrdený a ďalšie upozornenia nie sú odosielané,
- ***Paused*** – modrá – senzor je pozastavený na vyhradenú dobu,
- ***Unusual*** – oranžová – senzor zaznamenal nevšedné hodnoty oproti obvyklým hodnotám,
- ***Unknown*** – sivá – senzor zatiaľ neprijal žiadne údaje. Pravdepodobne došlo k chybe v sieťovej komunikácii.

Všetky senzory budú zároveň nastavené tak, aby po vykonaní dvoch neúspešných skenovaní zariadenia, zmenili svoj status na *Warning* a následne zmenili status na *Down* po zlyhaní tretej požiadavky, aby sa predišlo falošným notifikáciám spôsobených nepripojením v dôsledku preťaženia siete.

Zmeny stavu senzorov budú hlásené prostredníctvom okna správ v aplikácii a e-mailu. Aktualizácia senzorov bude implicitne nastavená na 5 minútový interval vzhľadom k tomu, že budú použité aj senzory fungujúce pomocou rozhrania WMI, ktoré je viac zaťažujúce. Aktualizácia senzorov u počítačov a tlačiarní, ktoré sa bežne používajú počas pracovnej doby, bude prebiehať vo vymedzenom časovom intervale každý pracovný deň od 06:00 do 20:00.

Eskalácia alarmov bude nastavená podľa nasledujúcich podmienok:

- pri stave *Down* bude odoslané upozornenie kontaktu 1. úrovne po uplynutí 30 sekúnd. Po potvrdení stavu kontaktom 1. úrovne bude alarm zastavený. Medzi kontakty 1. úrovne patria traja zamestnanci IT oddelenia spoločnosti,
- v prípade, že nedôjde k potvrdeniu kontaktom 1. úrovne, bude upozornenie zaslané kontaktu 2. úrovne po uplynutí 600 sekúnd od zmeny stavu senzora na *Down*. Po potvrdení stavu kontaktom 2. úrovne bude alarm zastavený. Medzi kontakty 2. úrovne patrí vedúci pracovník všetkých skúšobných oddelení,
- v prípade, že nedôjde k potvrdeniu kontaktom 2. úrovne, bude upozornenie zaslané opäť kontaktu 1. úrovne po uplynutí 900 sekúnd od zmeny stavu senzora na *Down*. Po potvrdení stavu kontaktom 1. úrovne bude alarm zastavený,
- v prípade, že nedôjde k potvrdeniu kontaktom 1. úrovne, bude upozornenie zaslané kontaktu 3. úrovne po uplynutí 1 500 sekúnd od zmeny stavu senzora na *Down*. Po potvrdení stavu kontaktom 3. úrovne bude alarm zastavený. Medzi kontakty 3. úrovne patrí zástupca riaditeľa,
- v prípade, že nedôjde k potvrdeniu kontaktom 3. úrovne, bude upozornenie zaslané opäť kontaktu 1. úrovne po uplynutí 1 800 sekúnd od zmeny stavu senzora na *Down*. Po potvrdení stavu kontaktom 1. úrovne bude alarm zastavený,

- v prípade, že nedôjde k potvrdeniu kontaktom 1. úrovne, bude upozornenie zaslané kontaktu 4. úrovne po uplynutí 2 400 sekúnd od zmeny stavu senzora na *Down*. Po potvrdení stavu kontaktom 4. úrovne bude alarm zastavený. Medzi kontakty 4. úrovne patrí riaditeľ spoločnosti.

4.3 Aspekty managementu

V tejto podkapitole budú vymedzené aspekty managementu súvisiace so zavádzaním technológie PRTG Network Monitor.

4.3.1 Organizačné začlenenie technológie, zodpovednosti a právomoci

Zavedenie nástroja pre monitorovanie siete bude vykonávať IT oddelenie s podporou vrcholového vedenia organizácie. IT oddelenie sa skladá z troch technikov. Vedúci tohto oddelenia bude zodpovedať za nákup licencie monitorovacieho systému spolu s vedúcou pracovníčkou ekonomicko-personálneho oddelenia. Ďalej bude vedúci pracovník IT oddelenia zodpovedný za vykonanie inštalácie a správu systému a ako jediný bude mať administrátorské práva a absolútnu právomoc pri nastavovaní senzorov, filtrov a systému notifikácií, vrátanie definície kontaktných osôb. Primárnymi kontaktnými osobami budú všetci pracovníci IT oddelenia a v prípade eskalácie problémov budú okrem primárnych kontaktov definované aj kontakty vyšších úrovní, ktorými budú vedúci pracovník všetkých skúšobných oddelení, zástupca riaditeľa a riaditeľ. Vedúci pracovník IT bude zodpovedný za vyhodnocovanie a reakcie na problémové situácie. Taktiež bude zodpovedať za vytvorenie a nastavenie ďalších účtov pre podriadených pracovníkov IT oddelenia.

Podriadení pracovníci IT oddelenia budú kontrolovať a vyhodnocovať prevádzku zariadení, nebudú mať právomoc pridávať senzory, nastavovať filtre a upozornenia. V prípade vyhodnotenia neštandardného problémového stavu, budú zodpovední za overenie tohto stavu a posúdenie nutnosti zásahu. Nutnosť zásahu budú pracovníci urýchlene delegovať na vedúceho pracovníka oddelenia IT.

Ostatní pracovníci spoločnosti nebudú mať prístup k systému. Vedúci IT oddelenia bude každý týždeň na pravidelných poradách reportovať priebežný stav vedeniu

spoločnosti. V prípade problematického stavu, bude okamžite informovať vedenie a príslušné oddelenia a úseky, ktoré daný stav ovplyvní.

4.3.2 Zostavenie implementačného tímu, zodpovednosti a právomoci

Povereným pracovníkom pre implementáciu systému je vedúci pracovník IT oddelenia. Taktiež bude zodpovedný za zostavenie implementačného tímu, ktorý bude mať nasledovné zloženie:

- **Generálny riaditeľ a dozorná rada** – riaditeľ spoločnosti a dozorná rada budú zodpovední za zadanie, dohľad a za dodržiavanie projektu implementácie vybranej technológie,
- **Vedúci pracovník IT oddelenia a vedúca pracovníčka Ekonomicko-personálneho oddelenia** – vedúci pracovník IT oddelenia je spolu s vedúcou pracovníčkou Ekonomicko-personálneho oddelenia zodpovedný za vytvorenie projektu na výber a objednávku zvolenej technológie. Projekt odovzdajú vedeniu na schválenie. Rovnako sú zodpovední za informovanie o priebehu tohoto projektu. Vedúci pracovník Oddelenia IT je tiež zodpovedný za implementáciu systému a za reportovanie priebehu vedeniu spoločnosti. Rovnako zodpovedá za správne nastavenie systému, senzorov a alertov a za monitorovanie počas skúšobnej fázy, ako aj po prechode do režimu rutinnej prevádzky.
- **Pracovníci IT oddelenia** – pracovníci oddelenia IT budú zodpovední za monitoring, zhodnotenie stavu a za reportovanie vedúcemu oddelenia.

4.3.3 Časový harmonogram implementácie

Časový harmonogram projektu je vytýčený v tabuľke číslo 3. Harmonogram obsahuje orientačné doby trvania jednotlivých činností projektu, ktoré sú odhadované za pomoci technických pracovníkov spoločnosti. Predpokladaný začiatok projektu je stanovený na 01.04.2022. Projekt je rozdelený na dve fázy a to iniciačnú a implementačnú. Každá fáza bude trvať približne dva mesiace. Predpokladané ukončenie projektu je totožné s počiatkom prechodu na režim rutinnej prevádzky. Termín ukončenia je stanovený na 03.08.2022.

Časový plán počíta iba s pracovnými dňami a reflektuje víkendy a sviatky. Školenie pracovníkov ohľadom technológie začne po dohode so školiacou inštitúciou najskôr 7 dní od objednávky školenia. Okrem činností a termínov obsahuje časový harmonogram aj zodpovednosti v jednotlivých činnostiach.

Tabuľka č. 3: Časový harmonogram implementácie

(Zdroj: Vlastné spracovanie)

Činnosť	**Zodpovednosť**	**Predchodca**	**Doba trvania**	**Začiatok**	**Koniec**
Iniciačná fáza				01.04. 2022	24.05. 2022
A. Definovanie potreby implementácie nástroja monitoringu siete a zhodnotenie požiadaviek spoločnosti a analýza	IT odd. + externý konzultant	-	10	01.04.	14.04.
B. Zostavenie implementačného tímu	Vedúci IT odd.	-	0,25	01.04.	01.04.
C. Vytýčenie rolí, pridelenie zodpovedností a právomocí	Riaditeľ + vedúci IT odd.	-	1	01.04.	01.04.
D. Analýza trhu technológií	Externý konzultant	A	20	19.04.	16.05.
E. Výberové riadenie pre výber technológie	Riaditeľ + IT odd.	D	5	17.05.	23.05.
F. Nákup licencie	Vedúci IT odd. + vedúca Ekonomicko-personálneho odd.	E	0,25	24.05.	24.05.

G. Výberové riadenie pre nákup služieb školiacej inštitúcie	Riaditeľ + vedúci IT odd.	E	0,25	24.05.	24.05.
H. Výber školiacej inštitúcie a nákup	Vedúci IT odd. + vedúca Ekonomicko-personálneho odd.	E	0,25	24.05.	24.05.
Implementačná fáza			37	25.05.	03.08.
I. Implementácia technológie	Vedúci IT odd.	F,G,H	4	25.05.	30.05.
J. Školenie	Externý školiteľ	F,G,H,I	3	01.06.	03.06.
K. Výber a nastavenie senzorov	Vedúci IT odd.	J	7	06.06.	14.06.
L. Vytvorenie a nastavenie používateľských účtov	Vedúci IT odd.	K	1	15.06.	15.06.
M. Nastavenie notifikácií	Vedúci IT odd.	L	5	16.06.	22.06.
N. Zostavenie politík	Vedúci IT odd.	M	3	23.06.	27.06.
O. Zostavenie smerníc	Vedúci IT odd.	M	3	23.06.	27.06.
P. Školenie pracovníkov obsahom politík a smerníc	Vedúci IT odd.	N,O	1	28.06.	28.06.
Q. Skúšobná prevádzka	Riaditeľ + vedúci IT odd.	P	20	29.06.	27.07.
R. Úpravy konfigurácie po skúšobnej prevádzke	Vedúci IT odd.	R	4	28.07.	02.08.
S. Prechod na režim rutinnej prevádzky	Riaditeľ + vedúci IT odd.	S	0,1	03.08.	03.08.
Ukončenie projektu	Riaditeľ + vedúci IT odd.		88,1	03.08. 2022	03.08. 2022

4.3.4 Režim skúšobnej prevádzky

Skúšobná prevádzka je odhadovaná na 4 týždne, respektíve 20 pracovných dní. Skúšobná prevádzka by mala byť ukončená najneskôr do doby 6 týždňov. Cieľom skúšobnej prevádzky je testovanie systému a ladenie konfigurácie jednotlivých zariadení, ako aj služieb a predovšetkým prahových hodnôt výstrah a upozornení. Za naplnenie činností skúšobnej prevádzky bude zodpovedať vedúci pracovník IT oddelenia. Podnet na predĺženie skúšobnej prevádzky podá taktiež vedúci pracovník IT oddelenia. O jej prípadnom predĺžení rozhodne riaditeľ spoločnosti, ktorý po ukončení skúšobnej prevádzky a konfiguračných úpravách, rozhodne o prechode na režim rutinnej prevádzky.

Počas skúšobnej prevádzky sa bude sledovať, či nedochádza k chybovosti systému a či dochádza k skutočnému predchádzaniu problematických situácií. Skúšobná prevádzka sa bude zameriavať predovšetkým na:

- **Optimalizáciu senzorov** – posúdenie vhodnosti vybranej licencie a vhodnosti vybraných senzorov. Je potrebné optimalizovať vybrané senzory tak, aby boli zaistené požiadavky monitoringu, ktoré spoločnosť kladie na systém, a z toho plynúca potreba zavedenia iných senzorov, či odstránenie senzorov kvôli ich nepotrebnosti,
- **Optimalizáciu alertov** – optimalizácia upozornení na základe zistených nedostatkov pre zachovanie požadovanej efektívnosti. Je potrebné otestovať skutočné odosielanie notifikácií pri vzniknutých problémoch, testovať, či sú notifikácie odosielané definovaným spôsobom a či sú odosielané všetkým definovaným kontaktom s potrebnou eskaláciou. Rovnako je potrebné určiť odchýlky v intenzite odosielania upozornení a optimalizovať ju,
- **Optimalizáciu používateľského rozhrania** – internetový prehliadač a aplikácie. Je potrebné sledovať a optimalizovať nastavenie používateľského rozhrania tak, aby bolo užívateľsky čo najvhodnejšie, aby zobrazovalo len podstatné a využiteľné informácie,
- **Sledovanie výkonnosti, rýchlosti a presnosti systému a vyťaženia úložiska.**

4.3.5 Režim rutinnej prevádzky

Režim rutinnej prevádzky nezačne skôr, ako bude ukončený režim skúšobnej prevádzky, ako aj všetky potrebné konfiguračné úpravy. O začatí režimu rutinnej prevádzky rozhodne riaditeľ spoločnosti. Rutinná prevádzka bude prebiehať podľa pravidiel stanovených v smerniciach. Zodpovednosť za stanovenie smerníc má vedúci pracovník IT oddelenia, ktorý má spolu so svojimi podriadenými spolupracovníkmi zodpovednosť za monitoring systému tak, ako je to stanovené v podkapitole 4.3.1 Organizačné začlenenie technológie, zodpovednosti a právomoci. Rutinná prevádzka sa bude zameriavať predovšetkým na sledovanie funkčnosti monitorovacieho systému, na fyzické kontroly hardwaru, na kontrolu softvéru a na reakcie na notifikácie tak, ako je to stanovené v zodpovednostiach a právomociach pracovníkov IT oddelenia.

4.3.6 Návrh smerníc potrebných pre prevádzku zvolenej technológie

Pri návrhu smerníc je potrebné dbať na zaistenie dodržiavania zodpovedností a právomocí zamestnancov, na zaistenie korektného a bezpečného používania monitorovacieho nástroja, na tvorbu dokumentácie a systému školenia.

S obsahom smerníc budú oboznámení všetci zainteresovaní zamestnanci pred nadobudnutím ich platnosti a rovnako budú pravidelne raz ročne preškolení.

4.3.6.1 Smernica o použití monitorovacieho nástroja

Táto smernica bude upravovať:

- **Povolený spôsob narábania s monitorovacím nástrojom** – návod na použitie,
- **Povinnosti a zodpovednosti používateľa monitorovacieho nástroja** – používateľom sa rozumie zamestnanec IT oddelenia,
- **Povinnosti a zodpovednosti používateľa v prípade výskytu výnimočných situácií** – presné vytýčenie reakcií v zmysle identifikácie stavu, formy, typu a času hlásenia, ako aj osobu, ktorej bude udalosť hlásená,
- **Správu účtov a prístupových údajov** – stanovenie zodpovednej osoby s administrátorskými právami, vytýčenie jej práv a povinností. Definovanie

účtov a práv, ktoré budú mať jednotliví používatelia. Definovanie práce s prístupovými údajmi a zmenou údajov.

4.3.6.2. Smernica o hardvérovom vybavení

Táto smernica bude upravovať:

- **Pravidlá pre manipuláciu s hardvérovým vybavením** – pravidlá pre použitie zariadení. Povolenie manipulovať s vybavením majú len zodpovedné osoby, zodpovednosť môže byť delegovaná na iné osoby,
- **Povinnosti a zodpovednosti zamestnancov** – zamestnanci budú môcť manipulovať len so zariadeniami, ktoré budú slúžiť ako ich pracovný nástroj a len za pracovným účelom. Za funkčnosť týchto zariadení sú zodpovední zamestnanci IT oddelenia. Zamestnanci majú povinnosť neodkladne nahlasovať akékoľvek problémy so zariadeniami pracovníkovi IT oddelenia.

4.3.6.3. Smernica o softvérovom vybavení

Táto smernica bude upravovať:

- **Pravidlá pre manipuláciu so softvérovým vybavením** – zamestnanci majú zákaz manipulovať so softvérovým vybavením, inštalovať, prenášať alebo mazať akýkoľvek softvér alebo dáta,
- **Povinnosti a zodpovednosti zamestnancov** – v prípade potreby inštalácie alebo odinštalovania softvéru zamestnanec deleguje túto požiadavku na pracovníka IT oddelenia. Za údržbu a aktuálnosť softvéru sú zodpovední zamestnanci IT oddelenia. Zamestnanci majú povinnosť neodkladne nahlasovať akékoľvek problémy so softvérom pracovníkovi IT oddelenia.

4.3.6.4. Smernica o bezpečnosti

Táto smernica bude upravovať:

- **Heslá a prístupové údaje**,
- **Pravidlá bezpečnej práce a reakcie na udalosti a incidenty**,

- **Zakázané použitie internetových stránok a sociálnych médií**,
- **Zakázané použitie zariadení v súkromnom vlastníctve**.

4.4 Ekonomické zhodnotenie

Táto podkapitola obsahuje ekonomické zhodnotenie a prínosy implementácie vybranej technológie.

4.4.1 Náklady

Nasledujúca tabuľka zobrazuje ekonomické náklady zavedenia novej technológie. Náklady nasadenia PRTG Network Monitor sa skladajú z licencie s 2 500 senzormi, ktorá je určená približne pre 250 zariadení a z nákladov na údržbu. Okrem tejto licencie bude potrebné, aby spoločnosť zakúpila nový server, ako aj licenciu operačného systému.

Inštaláciu operačného systému, ako aj inštaláciu a konfiguráciu technológie PRTG Network Monitor zabezpečí vedúci IT oddelenia.

Tabuľka č. 4: Náklady na zavedenie a použitie monitorovacieho nástroja

(Zdroj: Vlastné spracovanie)

Položka	Cena (€)
Licencia PRTG Network Monitor 2500	4 950,00
Server DELL PowerEdge R430	1 699,00
DELL Server disk 3,5" 2TB NLSAS 7200 HotPlug	198,62
Licencia Windows Server 2016 Standard	718,80
Zaškolenie IT personálu – 3 osoby	594,00
Náklady celkom za 1. rok	**8 160,42 € s DPH**
Náklady na údržbu (25% z ceny licencie)	1 237,50
Náklady celkom za 2. a ďalšie roky	**1 237,50 € s DPH**

Cena použitej technológie PRTG Network Monitor je vyčíslená na 4 950 € (Eur). Jedná sa o jednorazovú platbu za licenciu. Okrem tejto platby je potrebné počítať s cenou za údržbu, ktorá obsahuje bezpečnostné aktualizácie, podporu, nové funkcie, či opravy,

od druhého roku používania, ktorá je vyčíslená na 25% z ceny licencie za rok, teda na 1 237,50 € (Eur) s DPH. Spoločnosť, ktorá ponúka zaškolenie pre prácu s technológiou PRTG Network Monitor, stanovila cenu za zaškolenie troch ľudí na 594 € (Eur). Server, spolu s operačným systémom, je vyčíslený na 2 616,42 € (Eur) s DPH. Celkové náklady spoločnosti na implementáciu technológie za prvý rok sú preto vyčíslené na sumu 8 160,42 € (Eur) s DPH. Za každý ďalší rok používania budú celkové náklady 1 237,50 € (Eur) s DPH.

4.4.2 Prínosy pre firmu a záverečné odporúčania

Hlavným prínosom plynúcim zo zavedenia PRTG Network Monitor je samotný monitoring siete a zariadení, ktorý v spoločnosti doteraz neexistoval. Zavedenie tohto nástroja prinesie efektívnejšie fungovanie všetkých zariadení a služieb v zmysle zachovania ich dostupnosti a zdravia týchto zariadení. Očakávanými prínosmi je zvýšenie efektivity práce, zníženie straty informácií v dôsledku monitorovania a udržiavania hardvérového vybavenia a monitoring zariadení, ktoré vykonávajú dôležité činnosti počas testov technických zariadení. Zavedenie monitoringu siete povedie k prehľadnej správe, a tým aj k rýchlejšiemu vyhodnoteniu a k reakciám na problémy, čím dôjde k optimalizácii nákladov.

Napriek tomu, že v spoločnosti dochádza k incidentom, nie je vedená ich evidencia. Organizácia tiež finančne nevyčísluje dopady týchto incidentov, a preto nie je možné v súčasnosti kvantifikovať prínosy zavedenia monitorovacieho systému. Záverečným odporučením je preto zavedenie evidenčného systému udalostí a incidentov a kvantifikácia ich dopadov.

ZÁVER

Cieľom tejto diplomovej práce bolo vytvoriť návrh implementácie vybranej technológie pre management počítačovej siete v spoločnosti XYZ, s.r.o., zaoberajúcou sa skúšaním, certifikáciou a posudzovaním zhody a technických požiadaviek strojových zariadení.

Na základe analýz súčasného stavu bolo zistené, že nedostatky managementu siete spoločnosti spočívajú predovšetkým v správe porúch, konfigurácie a výkonu. Okrem toho boli definované požiadavky na monitorovací nástroj samotnou spoločnosťou. Z niekoľkých dostupných technických riešení bol po analýzach týchto nástrojov zvolený, ako prostriedok pre monitoring siete, nástroj spoločnosti Paessler, PRTG Network Monitor. Medzi hlavné dôvody pre výber PRTG Network Monitor patrí fakt, že tento nástroj najlepšie spĺňa požiadavky spoločnosti, je to nástroj s komplexnou monitorovacou spôsobilosťou, poskytuje správu všetkých sieťových zariadení rôznych výrobcov, ako aj správu aplikácií. Okrem toho nevyžaduje ďalšie doplnky, je vyvíjaný pre platformu Windows, umožňuje monitoring bez agentov a naviac je pomerne jednoducho konfigurovateľný, čo podstatne uľahčuje prácu pracovníkov IT oddelenia spoločnosti.

Okrem samotného výberu monitorovacej technológie sa práca venovala aj návrhu jej nasadenia, ktorý zahŕňa technické aspekty implementácie, postup inštalácie, či návrh nastavenia konkrétnych parametrov. V rámci návrhu bol vytvorený aj časový harmonogram, obsahujúci konkrétne termíny implementácie, ako aj zodpovednosti za konkrétne činnosti. Súčasťou sú tiež návrhy smerníc, ktoré spoločnosť využije pre prevádzku implementovanej technológie. Návrh uzatvára ekonomické zhodnotenie obsahujúce náklady, ktoré je potrebné vynaložiť na realizáciu implementácie technológie pre monitoring siete, ako aj prínosy pre spoločnosť.

Tým, že spoločnosť nasadí takúto technológiu, bude môcť efektívnejšie riešiť problémy, ktoré nastávajú výpadkami siete, či zariadení v sieti, čím dochádza ku strate údajov a služieb, ktoré sú potrebné pre fungovanie činností v spoločnosti. Riešenie, ktoré ponúka firma Paessler, sa v tomto prípade ukazuje ako najlepšie, či už vzhľadom k cene alebo jednoduchosti použitia.

ZOZNAM POUŽITÝCH ZDROJOV

(1) ONDRÁK, V. *Počítačové sítě* [prednáška]. Brno: VUT FP, 2018.

(2) SOSINSKY, B. *Mistrovství - počítačové sítě*. Brno: Computer Press, 2010. ISBN 978-80-251-3363-7.

(3) KRETCHMAR, J. M. a L. DOSTÁLEK. *Administrace a diagnostika sítí pomocí Opensource utilit a nástrojů*. 1. vyd. Brno: Computer Press, a.s., 2005. ISBN 80-251-0345-5.

(4) BIGELOW, S. J. *Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů*. 1. vyd. Praha: Computer Press, 2004. ISBN 80-251-0178-9.

(5) FCAPS. *Eramon* [online]. Gersthofen: Eramon, ©2022 [cit. 2022-05-06]. Dostupné z: https://eramon.de/en/product/fcaps/.

(6) ONDRÁK, V., SEDLÁK, P. a V. MAZÁLEK. *Problematika ISMS v manažerské informatice*. Brno: Akademické nakladatelství CERM, s.r.o., 2013. ISBN 978-80-7204-872-4.

(7) ČSN ISO/IEC 20000-2. *Informační technologie – Management služeb – Část 2: Návod pro použití systému managementu služeb.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2020. Triediaci znak 36 9074.

(8) VAN BON, J., ed. *Foundations of ITIL V3*. Zaltbommel: Van Haren Publishing, 2007. ISBN 978-9087530570.

(9) MAURO, D. R, a K. SCHMIDT. *Essential SNMP: Help for System and Network Administrators*. 2. ed. Sebastopol: O'Reilly Media, 2005. ISBN 0-596-00840-6.

(10) IEEE 802.1AB. *IEEE Standard for Local and metropolitan area networks - Station and Media Access Control Connectivity Discovery*. New York: The Institute of Electrical and Electronics Engineers, Inc., 2005. ISBN 0-7381-4688-9 SS95332.

(11) TUNSTALL, C. a G. COLE. *Developing WMI Solutions: A Guide to Windows Management Instrumentation*. 1. ed. Boston: Pearson Education, Inc, 2002. ISBN 0-201-61613-0.

(12) DSP0005. *Desktop Management Interface Specification.* Portland: Distributed Management Task Force, Inc., 2003.

(13) Windows Management Instrumentation. *Microsoft* [online]. Redmont: Microsoft, ©2022 [cit. 2022-05-06]. Dostupné z: https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page.

(14) CLEMM, A. *Network management fundamentals*. 1. vyd. Indianapolis: Cisco Press, 2007. ISBN 1-58720-137-2.

(15) PHAAL, P. a M. LAVINE. *sFlow Version 5.* [online]. ©2022. [cit. 2022-05-06]. Dostupné z: https://sflow.org/sflow_version_5.txt.

(16) Selection Criteria. *Paessler* [online]. Nuremberg: Paessler, ©2022 [cit. 2022-05-06]. Dostupné z: https://www.paessler.com/learn/whitepapers/selection-criteria.

(17) SCHWALBE, K. *Information Technology Project Management*. 7. ed. Boston: Cengage Learning, 2018. ISBN: 978-1-337-10135-6.

(18) *Nagios.com* [online]. Minneapolis: Nagios Enterprises, ©2022 [cit. 2022-05-06]. Dostupné z: https://www.nagios.com/.

(19) Products. *Nagios* [online]. Minneapolis: Nagios Enterprises, ©2022 [cit. 2022-05-06]. Dostupné z: https://www.nagios.com/products/nagios-xi/.

(20) *Paessler.com* [online]. Nuremberg: Paessler, ©2022 [cit. 2022-05-06]. Dostupné z: https://www.paessler.com/.

(21) *Zabbix.com* [online]. New York: Zabbix, ©2022 [cit. 2022-05-06]. Dostupné z: https://www.zabbix.com/.

(22) Global Dashboard. *Zabbix* [online]. New York: Zabbix, ©2022 [cit. 2022-05-06]. Dostupné z: https://www.zabbix.com/global_dashboard.

(23) *Progress.com* [online]. Bedford: Progress Software Corporation, ©2022 [cit. 2022-05-06]. Dostupné z: https://www.whatsupgold.com/.

(24) HORÁK, J. a M. KERŠLÁGER. *Počítačové sítě pro začínající správce*. 5. vyd. Brno: Computer Press, 2011. ISBN 978-80-251-3176-3.

(25) ČSN ISO 7498-4. *Systémy na spracovanie informácií - Prepojenie otvorených systémov (OSI) - Základný referenčný model - Časť 4: Základná štruktúra*

spracovania. Praha: Federální úřad pro normalizaci a měření, 1993. Triediaci znak 36 9617.

(26) DOSTÁLEK, L. a A. KABELOVÁ. *Velký průvodce protokoly TCP/IP a systémem DNS*. Brno: Computer Press, 2008. ISBN 978-80-251-2236-5.

(27) RUDOLF, V. a P. ŠMRHA. *Internetworking pomocí TCP IP*. České Budějovice: Kopp, 1994. ISBN 80-85828-09-X.

ZOZNAM POUŽITÝCH OBRÁZKOV

ZOZNAM POUŽITÝCH TABULIEK

ZOZNAM POUŽITÝCH SKRATIEK

ACL	Access Control List
API	Application Programming Interface
CI	Component Interface
CIM	Common Information Model
CPU	Central Processing Unit
DCOM	Distributed Component Object Model
DICOM	Digital Imaging and Communications in Medicine
DNS	Domain Name System
DMI	Desktop Management Interface
EÚ	Európska Únia
FCAPS	Fault, Configuration, Accounting, Performance, Security
FTP	File Transport Protocol
GNU	GNU's Not Unix
GUI	Graphical User Interface
HDD	Hard Disk Drive
HTTP	Hypertext Transfer Protocol
IT	Information Technology
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
ICMP	Internet Control Message Protocol
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers

IETF	Internet Engineering Task Force
IMAP	Internet Messaging Access Protocol
IoT	Internet of Things
IP	Internet Protocol
IPFIX	Internet Protocol Flow Information Export
IPMI	Intelligent Platform Management Interface
ISO/IEC	International Electrotechnical Commission
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
JMX	Java Management Extensions
LAN	Local Area Network
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MAN	Metropolitan Area Network
MI	Management Interface
MIB	Management Information Base
MIF	Management Information Format
MQTT	MQ Telemetry Transport
NAS	Network Attached Storage
NNTP	Network News Transfer Protocol
NRPE	Nagios Remote Plugin Executor
OID	Object identifier
OS	Operačný systém

OSI	Open Systems Interconnection
PAN	Personal Area Network
PDCA	Plan, Do, Check, Act
PDU	Protocol Data Unit
POP3	Post Office Protocol
PRTG	Paessler Router Traffic Grapher
QUIC	Quick UDP Internet Connections
RAM	Random Access Memory
RFC	Requests for Comments
RMON	Remote Network Monitoring
RPM	Revolutions per minute
RS232	Sériový port
SEL	Schweitzer Engineering Laboratories Protocol
SLA	Service Level Agreement
SMB	Server Message Block Protocol
SMI	Structure of Management Information
SMS	Service Management System
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SSH	The Secure Shell Protocol
SSL	Secure Sockets Layer
SWOT	Strengths, Weaknesses, Opportunities, Threats

TCP	Transmission Control Protocol
TLS	Transport Layer Security
TLV	Type – Length – Value
TMN	Telecommunications Management Network
TTL	Time To Live
UDP	User Datagram Protocol
USB	Universal Serial Bus
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
VGA	Video Graphics Array Connector
VPN	Virtual Private Network
WBEM	Web-Based Enterprise Management
WinRM	Windows Remote Management
WMI	Windows Management Instrumentation
.NET	Microsoft Dot Net