ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA DOPRAVNÍ

Bc. Martin Fiala

IMPLEMENTACE MONITORINGU INFRASTRUKTURY LOKÁLNÍ DATOVÉ SÍTĚ PRO ZAJIŠTĚNÍ KVALITY SLUŽEB

Diplomová práce

2022

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
Fakulta dopravní
děkan
Konviktská 20, 110 00 Praha 1

K620.....Ústav dopravní telematiky

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení studenta (včetně titulů):

Bc. Martin Fiala

Studijní program (obor/specializace) studenta:

navazující magisterský – IS – Inteligentní dopravní systémy

Název tématu (česky): **Implementace monitoringu infrastruktury lokální datové sítě pro zajištění kvality služeb**

Název tématu (anglicky): Implementation of local data network infrastructure monitoring to ensure quality of service

Zásady pro vypracování

Při zpracování práce se řiďte následujícími pokyny:

- Popište základní problematiku počítačových sítí a nutných protokolů pro sledování infrastruktury lokální datové sítě
- Proveďte rešerši dostupných nástrojů pro sledování stavu lokálních datových sítí a následně i další připojené infrastruktury
- Proveďte implementaci vybraného nástroje na testovací lokální datovou síť a připojenou infrastrukturu
- Sběr dat z testovací lokální datové sítě a připojené infrastruktury
- Na základě zjištěných výsledků navrhněte kroky vedoucí ke zvýšení kvality služeb v testované lokální datové síti a připojené infrastruktuře.

ČVUT FD

Rozsah grafických prací: dle požadavků vedoucích práce

Rozsah průvodní zprávy: minimálně 55 stran textu (včetně obrázků, grafů a tabulek, které jsou součástí průvodní zprávy)

Seznam odborné literatury:

Mauro D. R., Schmidt K. J.: Essential SNMP. Second edition, O'Reilly, Sebastopol, 2005.ISBN 0-596-00840-6.

Lyon G.: NMAP Network Scanning. First Edition, Insecure.Com, Sunnyvale, 2008. ISBN 0-9799587-1-7

Braham B.: TCP/IP Addressing. Academic press, London, 1997

Vedoucí diplomové práce: **Ing. Jindřich Sadil, Ph.D.**
Ing. Lukáš Svoboda

Datum zadání diplomové práce: **14. července 2021**
(datum prvního zadání této práce, které musí být nejpozději 10 měsíců před datem prvního předpokládaného odevzdání této práce vyplývajícího ze standardní doby studia)

Datum odevzdání diplomové práce: **16. květen 2022**
a) datum prvního předpokládaného odevzdání práce vyplývající ze standardní doby studia a z doporučeného časového plánu studia
b) v případě odkladu odevzdání práce následující datum odevzdání práce vyplývající z doporučeného časového plánu studia

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE Fakulta dopravní L. S.

prof. Ing. Zdeněk Votruba, CSc.
vedoucí
Ústavu dopravní telematiky

doc. Ing. Pavel Hrubeš, Ph.D.
děkan fakulty

Potvrzuji převzetí zadání diplomové práce.

Fiala

Bc. Martin Fiala
jméno a podpis studenta

V Praze dne 14. července 2021

Poděkování

Na tomto místě děkuji vedoucím práce panu Ing. Jindřichu Sadilovi, Ph.D. a Ing. Lukášovi Svobodovi za odborné vedení a konzultace při zpracování mé diplomové práce. Také děkuji svým kolegům z Oddělení správy sítě Fakulty dopravní a z firmy Alef Nula, a.s., kteří mi při tvorbě diplomové práce ochotně pomáhali. Na závěr děkuji rodině a blízkým za jejich podporu během mého studia.

Čestné prohlášení

Předkládám tímto k posouzení a obhajobě práci, zpracovanou na závěr studia na ČVUT v Praze Fakultě dopravní.

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 Zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským o změně některých zákonů (autorský zákon).

V Praze dne 10. května 2022 ……

Podpis

Abstrakt

Diplomová práce se věnuje efektivnímu využití dat, která jsou poskytována infrastrukturou lokální datové sítě. Cílem této práce je na základě těchto dat docílit požadované kvality poskytované služby. K naplnění tohoto cíle je implementován monitorovací systém na testovací infrastrukturu a popsány všechny další procesy spojené s funkcí tohoto systému. V rámci vlastního nasazení systému jsou využita data z reálné testovací sítě. Na základě výsledků implementace jsou navržena doporučení, která mohou nabídnout a umožňují poskytovat vyšší kvalitu služby.

Klíčová slova

agent, datová síť, dostupnost, infrastruktura, koncové zařízení, kvalita služby, lokální datová síť, monitoring, problematická událost, proces, protokoly, SNMP, uživatel, Zabbix

Abstract

The diploma thesis deals with the effective use of data that are provided by the infrastructure of the local data network. The aim of this work is to achieve the required quality of service provided on the basis of this data. To meet this goal, a monitoring system is implemented on the test infrastructure and all other processes associated with the function of this system are described. Data from a real test network are used within the actual deployment of the system. Based on the results of the implementation, recommendations are proposed that can offer and allow to provide a higher quality of service.

Key words

agent, availability, end device, event, infrastructure, local data network, monitoring, problematic event, process, protocols, quality of service, SNMP, user, Zabbix

Obsah

Seznam použitých zkratek

ACK = Acknowledgement code

AP = Access Point

ARPNET = Advanced Research Projects Agency Network

CPU = central processing unit

DHCP = Dynamic Host Configuration Protocol

EIA = Electronic Industries Alliance

GPO = Group policy

gRPC = high performance Remote Procedure Call

GUI = Graphic User Interface

HTTP = Hypertext Transfer Protocol

IEEE = Institute of Electrical and Electronics Engineers

IETF = Internet Engineering Task Force

IOT = Internet of Things

ISO = International Organization for Standardization

IT = Informační technologie

JSON = JavaScript Object Notation

MAC = Media Access Control

MAN = Metropolitan Area Network

MIB = Management information base

MOS = Mean Opinion Score

MTBF = Mean Time Between Failures

MTTR = Mean time to repair

NETCONF = Network Configuration Protocol

NMS = Network Monitoring System

OID = Object Identifier

OSI = Open Systems Interconnection

PAN = Personal Area Network

POE = Power Over Ethernet

QFD = Quality function deployment

QoS = Quality of Service

RAM = Random-access memory

RFC = Request for Comments

SLA = Service-level agreement

SNMP = Simple Network Management Protocol

SSH = Secure Shell

SSL = Secure Sockets Layer

TCP = Transmission Control Procol

TIA = Telecommunications Industry Association

UDP = User Diagram Protocol

UPS = Uninterruptible Power Supply

UTP = Unshielded Twisted Pair

VLAN = Virtual Local Area Network

WAN = Wide Area Network

Wi-Fi = Wireless LAN

XML = Extensible Markup Language

YANG = Yet Another Next Generation

1. Úvod

Přenos dat ve smyslu toků informací mezi příjemcem a odesílatelem lze dnes obrazně připodobnit ke krvi v lidském těle. Tato tekutina zaručuje funkčnost celého organismu a při každodenních činnostech se jí nedostává dostatečné pozornosti. Většinou až do chvíle, než přestane obíhat. Poté se již dělá vše pro to, aby se opět dala do pohybu a plnila svou nesmírně důležitou funkci. Tento nadnesený příklad má poukázat na význam funkčního přenosu dat v dnešním světě, kde je skoro vše vystavěno na informačních technologiích, které potřebují pro svůj chod právě funkční datovou infrastrukturu.

V případně události na datové infrastruktuře, která vyústí ve výpadek, pak je pouze otázkou času, za jak dlouho se povede problém vyřešit. Důsledky jsou závislé na čase odstranění této závady. V lepším případě mohou tyto důsledky představovat pouze to, že zaměstnanci v organizacích místo kancelářských programů využijí kancelářské potřeby jako je tužka a papír. V hroším případě dojde například k pozastavení výroby v polo automatizované továrně. Většinou se jedná „pouze“ o ekonomické důsledky. Vedle toho je u většiny organizací je kladen důraz na efektivitu práce a ekonomický růst, čemuž má pomoci i postupná digitalizace. Dnešní trend v propojování všeho, vždy a všude, přikládá ještě vyšší význam základnímu stavebními kameni pro komunikaci v podobě datové infrastruktury.

Druhým aspektem, kterým se tato práce zaobírá je sledování kvality služby, kterou tato infrastruktura má naplňovat. Naplnění těchto požadavků lze velmi dobře sledovat na samotných uživatelích, či na své vlastní uživatelské rovině. V situacích, kdy není odezva systému zcela hladká, např. při hovorech dochází ke zpoždění mluveného slova, se pracovní efektivita rapidně snižuje. Přitom všem těmto případům by bylo možné předejít, či zkrátit jejich průběh, pokud by se správně využívaly informace, které o sobě infrastruktura sdílí. Stejně jako u lidského těla a jeho projevů. Pokud se tyto projevy sledují a nachází se jejich příčina včas, lze se s vyšší pravděpodobností vyhnout situaci, kdy tělo přestane fungovat.

Proto je tato práce zaměřena na implementaci nástroje, který umožní pozorovat chování datové infrastruktury. Na základě něj zjistit, kde nastala chyba v nejkratším možném čase a poskytovat tak co nejdéle koncovým uživatelům službu naplňujících jejich požadavky. Práce popisuje cestu k tomu, jak implementovat monitorovací systém a tím snížit počet hlášení od uživatelů, která upozorňují na problematické události.

V teoretické části jsou popsány základní charakteristiky lokální datové síti. Následně dojde k výběru vhodného dostupného nástroje. Praktická část je věnovaná samotné implementaci vybraného nástroje a zvolení správného nastavení pro testovací infrastrukturu, tak aby naplňovala základní požadavky kvality služby.

1.1 Vymezení oblasti

Samotná problematika lokálních datových sítí je velmi rozsáhla a podrobná. Pro účely diplomové práce bylo nutné se zaměřit na užší téma. K samotnému definování konkrétní problematiky byly využity postřehy z prostředí Fakulty dopravní. Ta jako jedna ze součástí Českého vysokého učení technického, spadá mezi nejvýznamnější vzdělávací instituce v České republice. Proto je zde dostupnost a kvalita služby využívaných systémů velmi důležitá.

Samostatná práce bude vztažena na generalizovanou datovou infrastrukturu a až následně u praktické části bude prostředí fakulty dopravní sloužit jako zdroj vstupních dat. Práce se nezaměřuje na vybudování nové sítě, ale na sledování stavu již vybudovaného systému. Cílem je nalézt možná zlepšení, která mají vliv na zvýšení kvality služeb v datové lokální síti. Pro sledování sítě bude vybrán nástroj, nejvíce vyhovující definovaným požadavkům.

1.2 Cíle práce

Cílem této diplomové práce je popsat proces implementace monitorovacího systému a přestavit základní souvislosti, které jsou podmínkou k pochopení tématu. Vedle toho by práce měla i poukázat na závislost mezi využitím dat a kvality nabízené služby dané datové infrastruktury.

2. Seznámení s problematikou

Tato kapitola má za cíl seznámit čtenáře s pojmy, principy a závislostmi. Mimo jiné se v této kapitole čtenář dozví, jak funguje přenos dat v síti, či jaká zařízení v ní může najít. Hloubka zkoumané problematiky odpovídá požadavkům implementace.

2.1 Použité názvosloví

Podkapitola *Použité názvosloví* obsahuje definice základních pojmů, tak jak se využívají v této práci. V oblasti informačních technologií je řada různých interpretací definic jednotlivých pojmů, proto je vhodné je upřesnit na začátku práce.

Monitoring

Pojem monitoring, v překladu sledování, znamená kontinuální sledování prvků, či jejich parametrů z důvodu kontroly jejich funkce.

Datové sítě

Základní definici sítě v technickém kontextu lze chápat jako propojení dvou a více prvků, které navzájem komunikují. Základem datové sítě je samotný přenos dat fungující na principu přenosu paketů (*kapitola 3*). Nicméně pro lepší představu se tato práce bude zabývat nikoliv

obecnou datovou sítí, ale počítačovou sítí. Ta splňuje podmínky datové sítě, kde například stolní počítač je zdrojem i příjemcem dat. Definici počítačové sítě lze popsat jako skupinu propojených zařízení (počítače, servery), která navzájem komunikuje. Jejich komunikace může probíhat pomocí různých přenosových technologií jako je např. Ethernet, či Wi-Fi. Avšak zařízení v celé síti pracují nezávisle s vlastním operačním systémem a na vlastním hardwaru. Vedle počítačové datové sítě, může existovat například i mobilní datová síť. [43] [31]

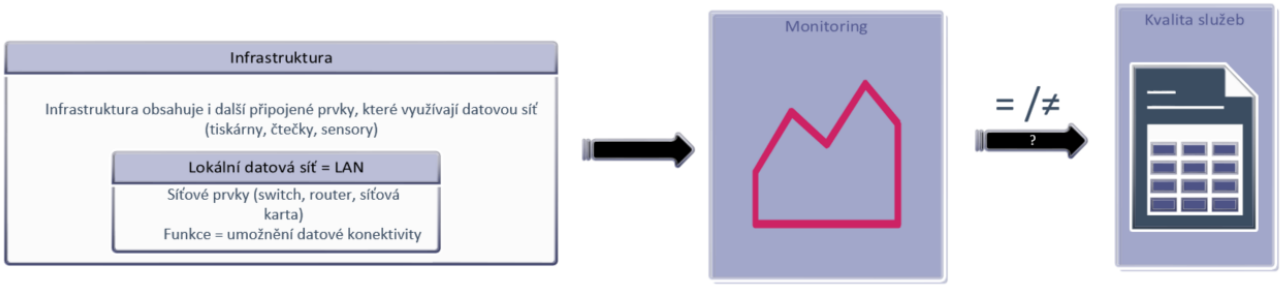
Infrastruktura

Infrastrukturu lze pojmout jako nadřazený pojem pro počítačovou síť. Infrastruktura obsahuje jak prvky počítačové sítě, tak i další prvky, které jsou na tuto síť připojené a jsou tedy na ní závislé. Pod prvky infrastruktury si lze představit tiskárny, kopírky, či různé druhy senzorů, které se nacházejí uvnitř budov. Infrastruktura dohromady se svými podmnožinami tvoří celek, který dokáže plnit požadavky uživatelů. [17]

Kvality služeb

Kvalita služeb popisuje, zda je služba schopná naplňovat požadovanou funkci. A lze ji dělit na vnitřní a vnímanou kvalitu služeb. Další vysvětlení se nachází v *kapitole 6*, která je zaměřena na problematiku kvality služeb. [12]

Obrázek 1 schematicky popisuje vztahy mezi pojmy a lze z něho jednoduše vyčíst, že hlavním úkolem je porovnat, zda stav sítě odpovídá požadavkům v podobě kvality služeb, či nikoliv



Obrázek 1 Schéma pojmy [autor]

Propustnost

Tato veličina popisuje skutečné množství přenesených dat mezi odesílatelem a příjemce za jednotku času [bps]. [6]

Šířka pásma

Šířka pásma v kontextu počítačových sítí vyjadřuje maximální možné množství přenesených dat pomocí datové cesty za jednotku času [bps]. Její význam lze označit i pojmem teoretická

maximální přenosová rychlost. Avšak vedle uživatelských dat je nutné přenést i data režijní, proto je skutečná přenosová rychlost vždy nižší. [6]

Zpoždění

Přehlcení síťového prvku pakety způsobuje zpoždění (latenci), které má na určité služby velmi zásadní význam. Dochází k němu při situacích, když je v síti více provozu, než síť dokáže zpracovat. Zpoždění, či latence udává kolik času trvá přenos paketů ze zdroje do cíle. Tato zpoždění lze rozdělit na dva typy - na fixní a proměnný. Fixní zpoždění, vzniká samotným procesem přenosu a je závislé na typu přenosového média. Proměnné zpoždění nelze předem definovat, protože záleží na řadě faktorů, ať na straně odesílatele, či příjemce. [10]

Jitter

Jitter je hodnota, která udává rozptyl zpoždění přijatých paketů. Popisuje, jak je dané internetové připojení stabilní. [10]

Zvuk

Zvuk má takové požadavky na datový přenos, aby na straně příjemce předal plnou a srozumitelnou informační hodnotu. Charakteristické pro něj je, že v rámci datové velikosti je stále stejný a jeho velikost je možné předpovídat i do budoucna. Avšak je velmi náchylný na zpoždění a na ztrátu paketů. Pokud by se ztracené pakety poslaly znovu, pozbyly by svého významu, protože samotný hovor se již nachází u jiné věty. Samotná velikost paketů se zvukem je tedy neměnná a dosahuje velikosti 200 bytů a maximální zpoždění, při kterém je zvuk stále srozumitelný, je 150 milisekund. [10]

Video

Může se zdát, že video bude mít velmi podobné požadavky na přenos, jako má zvuk, ale opak je pravdou. U videa velikost přenosu záleží na obsahu videa. Pokud jde o akční scény, kde je velké množství změn v obraze, tak se to odráží na větším množství přenesených bytů než v situacích, kdy se přenáší obraz např. noční oblohy. Svou roli zde také hraje aspekt predikce. Je totiž složité odhadnout, jak bude budoucí datový paket veliký. Maximální velikost paketu může být až 1500 bytů s maximálním zpožděním 400 milisekund. Větší zpoždění bude patrné ve výsledném obrazu. [10]

Data

Data lze vnímat i z jiného pohledu, kdy jde o konkrétní přenos v podobě dat. Příkladem může být zasílání záznamů do databáze. Zde je nutné mít jistotu, že data dorazila na cílovou adresu, kompletní a bez chyb. Pro jejich přenos se využívá orientovaný protokol transportní vrstvy TCP (Transmission Control Procol). Tento protokol v sobě obsahuje mechanismy, které zajistí, že data byla spolehlivě doručena. Podrobnější popis protokolu lze najít v *kapitole 3.* [10]

2.2 Úvod do počítačové sítě

Podkapitola *Úvod do počítačové sítě* seznámí čtenáře s typy počítačových sítí a také připomene význam a přínosy počítačové cítě jako celek. Počítačová síť byla vybrána jako konkrétnější podoba datové sítě viz *kapitola 2.1*.

2.2.1 Význam počítačové sítě

Role počítačové sítě je v dnešním světě zásadní, protože přenáší všechna data bez ohledu na geografické vzdálenosti. Také zásadně zvyšuje efektivitu v rámci využívání a přináší spoustu nových možností, jak pracovat s daty a výpočetním výkonem. Umožňuje získat jakákoliv data v řádech milisekund. [16]

2.2.2 Klíčové aspekty sítě

Tato podkapitola se zabývá základními aspekty sítě, které by měla splňovat každá současná lokální počítačová síť. Pokud dané aspekty nesplňuje může být zásadně ohrožena její funkčnost, či může dojít k ohrožení samotných dat uživatelů. Výčet uvedený níže popisuje obecně jednotlivé aspekty, které je dobré mít na paměti při práci se sítí. Každá síť má naplňovat tyto čtyři základní pilíře, které ohraničují požadavky na počítačovou síť. [10]

2.2.2.1 Tolerance chyb

Síť musí být schopná fungovat stále, i když se v ní objeví problémová událost, například výpadek jednoho ze síťových prvků. Řešením často bývá redundance, kdy se v řádu milisekund síť dokáže sama konvergovat a uživatel ani nezjistí, že se na síti objevila porucha. [10]

2.2.2.2 Rozšiřitelnost

Dalším požadavkem je možnost ji kdykoliv rozšířit. Je proto důležité při návrhu sítě myslet i na budoucí rozvoj, zda má síť predispozice k významnému rozvoji, či nikoliv. [10]

2.2.2.3 Bezpečnost

Základem každého systému je, aby byl bezpečný. Sítě nejsou výjimkou, i když na první pohled to nemusí být znát. Pro ilustraci lze uvést elektrické vedení, které dokáže přivodit smrt při jediném dotyku. Dnes i data mají podobný účinek jako elektrické vedení, protože pomocí nich lze ovládat nejrůznější systémy, například i letadlo. Proto je velmi důležité ošetřit veškeré možné způsoby, jak by se mohla modifikovat komunikace mezi odesílatelem a příjemcem. Síťová bezpečnost plní tři základní požadavky: důvěrnost, integritu a dostupnost. Tyto prvky jsou dle autora velmi důležité, a proto je vhodné je níže rozepsat. [10]

- **Důvěrnost**

Důvěrnost lze v počítačových sítích pochopit tak, že data jsou přístupná pouze oprávněné osobě. Mechanismus, pomocí kterého lze k tomuto dospět, se skládá ze tří kroků. Autentizace prověří, že přihlášení dané osoby je opravdu oprávněné (např. na základě dané role). Autorizace umožní dané osobě přiřadit konkrétní přístupová práva (např. právo pouze pro čtení). A posledním krokem je audit, který má za úkol evidenci všech významných změn v síti. Díky nim lze snadno a jednoduše zjistit, jaké kroky příjemce dat učinil v daném časovém horizontu. [30]

- **Integrita**

Významem tohoto požadavku je zjištění, zda s daty nebylo během komunikace manipulováno a data jsou beze změny. V praxi se tento požadavek naplňuje kontrolními součty, či digitálním podpisem. [30]

- **Dostupnost**

Dalším požadavkem je dostupnost, která označuje, zda je možné se připojit ke službě a tato služba zároveň může vykonávat svou funkci, jako je například dostupnost webových stránek. Samotná dostupnost často bývá součástí dohody o úrovni poskytovaných služeb (SLA) jako tzv. garantovaná časová dostupnost. Nejčastěji je vyjádřena jako procento času v daném období, obvykle za rok. Jako příklad lze demonstrovat 99% dostupnost. Tento údaj znamená, že poskytovatel služby ručí za to, že výpadek služby bude maximálně 3,65 dne. [30] [7]

- **Kvalita služeb (QoS)**

Tento pilíř se zabývá řízením datových toků. Pro představu je zde uveden příklad spěchající sanitky k akutnímu případu, kdy ostatní účastníci silničního provozu uvolňují prostor pro v dané situaci urgentně zasahující sanitku. Z tohoto příkladu vyplývá, že určitý účastník silničního provozu má jednoznačnou prioritu, ale i zde jsou limity, které nelze překročit (např. šířka silnice, kdy vozidla nemohou uhnout více než na okraj vozovky). V sítích nahrazuje šířku silnice, šířka pásma, kterou také nelze překročit.

2.2.3 Dělení sítí

Počítačové sítě lze rozdělit podle několika parametrů jako je například topologie nebo její velikost. Dělení umožňuje lepší pochopení dané struktury sítě a její funkcionality.

Dělení na základě parametru velikost:

- **PAN – Personal Area Network**

Pod touto sítí si lze představit síť, která je tvořena osobními zařízeními (mobilní telefon, notebook, bezdrátová sluchátka).

- **LAN – Local Area Network**

Lokální síť zahrnuje počítače a jiné připojené zařízení v určitém méně rozsáhlém celku (např. firma, škola). Může se jednat i o jednotlivé domácnosti, či budovy. Vznikla v 60. létech 20. století pro potřeby propojení kolejí, univerzit a výzkumných institucí. Avšak větší rozšíření přišlo až s příchodem technologie Ethernet a následné standardizace v roce 1983.[10] [41]

- **MAN – Metropolitan Area Network**

Metropolitní síť označuje síť, která zahrnuje větší geografické celky. Může se například jednat o propojení studentských kolejí, které se nacházejí v jednom městě, avšak na různých místech. MAN umožňuje přenos dat na vzdálenost až několika desítek kilometrů. [30]

- **WAN – Wide Area Network**

WAN sítě propojuje jednotlivé LAN sítě s přesahem geografických celků jako jsou státy. Jednou z nejznámějších a největších WAN sítí je Internet. První zmínka o této síti pochází z konce 50. let 20. století, kdy Americké letectvo propojilo velké množství telefonů, telefonních linek a modemů v rámci svého radarového obraného systému. Její hlavní rozvoj začal sítí Advanced Research Projects Agency Network (ARPNET) založené na IP adresách, kterou využívalo několik vzdělávacích institucí ve Spojených Státech Amerických. [19] [42]

Tato práce se zabývá sítí v rozsahu lokální sítě, a to z několika důvodů. Jedním z nich je, že nejčastěji se zaměstnanci při své práci setkávají se sítí lokální vytvořenou pro daný objekt, či organizaci, například školu. A druhým důvodem je její význam, protože základem většiny informačních systémů je lokální síť, kde se provádí většina operací.

Dělení na základě topologie

Dalším častým dělení počítačových sítí je na základě topologie sítě neboli na základě rozmístění uzlů a jejich propojení mezi sebou. Jejich ukázku lze vidět na *Obrázek 2*. Uzly představují jednotlivé síťové prvky (např. stolní počítač, tiskárna), které jsou spojeny kabelem, či jiným přenosovým médiem. Každá topologie představuje určité výhody a nevýhody. [33]

Sběrnice

Každý uzel je v této topologii připojen k jednomu společnému přenosovému prostředku tzv. sběrnici. Výhody této topologie jsou hlavně v jednoduché rozšiřitelnosti. Na druhou stranu, zde celá komunikace je závislá na jednom přenosovém mediu, které se může dostat do poruchy. Proto je tato topologie velmi nespolehlivá. [33]

Kruh

Kruhová topologie vzniká připojením zařízení do kruhu, kdy cesta prochází přes jednotlivé prvky systému v jednom směru. Výhodou kruhu je jednoduché předávání zpráv mezi prvky, bohužel pokud dojde k poruše jednoho prvku, tak celá síť přestane plnit svou funkci. [33]

Hvězda

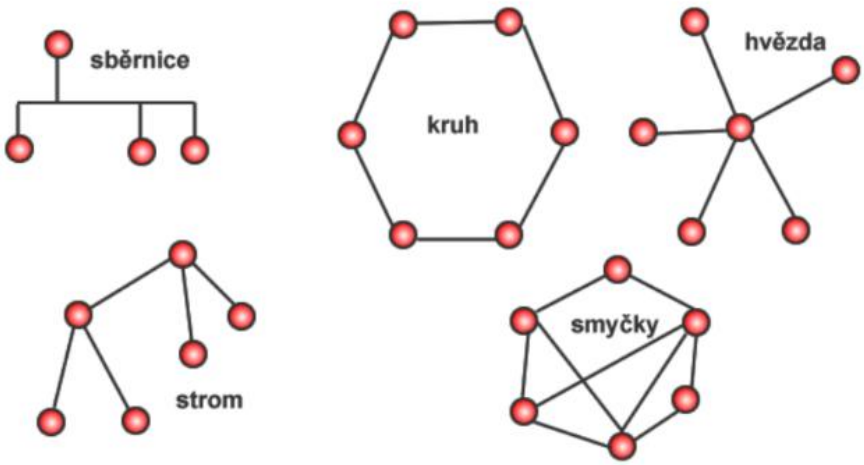
Hlavním znakem topologie hvězda je centrální prvek, přes který jde veškerá komunikace. S tím je spojená i její vyšší spolehlivost, přestože celý systém je závislý pouze na jednom prvku. Avšak tento prvek bývá dobře dimenzovaný a jeho spolehlivost je vyšší než spolehlivost koncových stanic. Nevýhodou této topologie jsou vyšší náklady na vybudování sítě z důvodu vyšší spotřeby kabeláže. [33]

Strom

Nejčastější topologii, kterou najdeme v lokálních počítačových sítích je strom. Strom vzniká propojením více hvězd. [33]

Smyčky

Nejnákladnější topologií jsou smyčky, kde mezi každými dvěma uzly je více propojení. Může tak tedy dojí i k situaci, kde je každý prvek spojen s každým. Hlavní výhodou této topologie je velmi vysoká spolehlivost, protože pokud jedna cesta mezi dvěma prvky přestane fungovat, tak je tu vždy alternativní cesta. [33]



Obrázek 2 Topologie sítí [33]

2.3 Přenosové medium

Pro úspěšný přenos dat je nutné, aby tyto zařízení byla propojena. Pro připojení existují tři možná řešení:

- metalickým kabelem
- optickým kabelem
- bezdrátově

Nejdříve je nutné přenášená data přeměnit na signál, který se následně přenese pomocí přenosového media. Popis přenosových medií se zde může zdát nadbytečný, nicméně pro spolehlivou přenosovou funkci sítě je stav a charakteristika přenosových medií velmi důležitá.

2.3.1 Metalický kabel

Nejdostupnější propojení je pomocí metalických kabelů UTP (unshielded twisted pair). Uvnitř se nachází 4 kroucené páry vodičů, které přenášejí data v podobě digitálního signálu. Jeho přenos funguje na principu změny napětí na vodiči. Barevné provedení kabelů je opět definované standardem od organizací TIA a EIA a nejčastěji se osazuje koncovkou RJ-45, která je součástí standardu pro Ethernet (802.3). Nejdelší možná délka kabelu bez přerušení je 100 m. Přenosová rychlost záleží na daném standardu, čím je požadovaná větší, tím je nutná instalace kvalitnějšího a dražšího kabelu. Metalický kabel má svá omezení, jako jsou menší vzdálenosti pro přenos dat a možné ovlivnění signálu elektrickou interferencí, avšak jeho výhodou je cena, která je oproti jiným přenosovým mediím významně nižší a také poskytuje možnost napájet připojená zařízení tzv. POE (Power Over Ethernet). Přehled standardů s maximální přenosovou rychlostí je uveden níže. [6] [19]

Standard	**Maximální přenos. rychlost**	**Název IEEE standardu**
100Base-Tx Ethernet	10 Mbps	802.3
100Base-T Ethernet	100 Mbps	802.3u
1000Base-T Ethernet	1000 Mbps	802.3ab
10GBase-T Ethernet	10 Gbps	802.3an

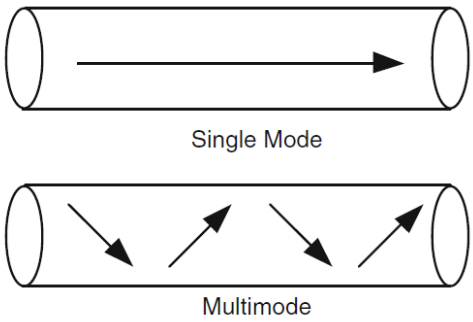
Tabulka 1 Porovnání standardů IEEE [10]

2.3.2 Optický kabel

Toto přenosové medium využívá pro přenos dat paprsek světla. Samotný kabel se skládá z optického vlákna (jádra) o šířce několika jednotek až desítek mikrometrů, které je ze skla, či

plastu. Vlákno je obklopeno pláštěm, které ho zároveň chrání před mechanickým poškozením. Princip přenosu spočívá v tom, že data jsou převedena na elektromagnetické vlny, které putují ve směru osy vlákna. Z fyzikálního pohledu je nutné dodržet podmínku, aby index lomu jádra byl vyšší než index lomu obalu. Hlavní předností optického kabelu je rychlost přenosu dat na dlouhou vzdálenost, lze dosahovat rychlosti desítek Gbps na vzdálenost i desítek kilometrů. Na druhou stranu jsou pořizovací a instalační náklady mnohem vyšší než na metalický kabel. [6]

Optický kabel se vyrábí ve dvou typech, single mode a multimode. Typ single mode přenáší v jeden čas pouze jeden signál, avšak toto médium nabízí přenos na delší vzdálenost. Na rozdíl od multimode, kde se zároveň přenáší více signálů z důvodu širšího vlákna (viz *Obrázek 3*). [6]



Obrázek 3 Typy optického kabelu [6]

Standard	Maximální vzdálenost	Vlnová délka
1000BASE-LX	5 km	1310 nm
10GBASE-LX4	10 km	1310 nm
10GBASE-E	40 km	1550 nm
100GBASE-LR4	10 km	1310 nm

Tabulka 2 Porovnání typů optických kabelů [10]

2.3.3 Bezdrátové připojení

Jak metalický, tak i optický kabel poskytují spolehlivé připojení, nicméně je nutné mít zařízení stále na jednom místě a vždy k němu mít dotažený kabel. Tyto podmínky jsou však značným omezením pro dnes velmi oblíbená přenosná zařízení (notebook, mobilní telefon apod.), i tato zařízení potřebují datovou konektivitu. Proto dalším možným způsobem přenosu dat je pomocí

mikrovlnných vln, pro které není nutné žádné fyzické propojení. Na druhou stranu přínos v podobě mobility je vykoupen nižší propustností média, větším množstvím chyb v přenosu a menším dosahem signálu. Nejčastěji je bezdrátový přenos využíván mobilní buňkovou sítí a sítěmi na základě standardů 802.11. Další limitací pro sítě standartu 802.11 je možné šíření mikrovlnných vln pouze na vyhraněných bez licenčních pásmech. Tato pásma mohou využívat všichni, a proto je nutné myslet i na bezpečnostní rizika a možné omezení kapacity. Z tohoto důvodů jsou regulačními úřady v dané zemi regulovány vysílací výkony těchto zařízení. Pro přenos dat v lokálních sítích jsou výhradně využívaná zařízení na bázi standardů 802.11, které přenáší data na pásmech 2.,4 GHz, 5 GHz. A nově i v pásmu 6 GHz.

IEEE WLAN Standard	Frekvenční pásmo	Maximální přenosová rychlost
802.11b	2,4 GHz	11 Mbps
802.11g	2,4 GHz	54 Mbps
802.11n	2,4 a 5 GHz	600 Mbps
802.11ac	5 GHz	6400 Mbps
802.11ax	2,4 GHz a 5 GHz	9600 Mbps

Tabulka 3 Porovnání standardů 802.11 [autor]

2.4 Síťová zařízení

Síťová zařízení jsou základem každé funkční počítačové sítě. Pokud by zařízení nemělo síťovou kartu, tak by nemohlo komunikovat s jiným zařízením na síti. A dalším aspektem je organizace počítačové sítě. Síťové prvky umožňují logické uspořádání sítě a tím předcházení chaosu bez možnosti správy. V této kapitole bude popsáno 7 hlavních zařízení, která najdeme ve většině lokálních sítí.

2.4.1 Síťová karta

Síť je složená z jednotlivých uzlů, v lokální počítačové síti se jedná o síťové prvky. Pokud počítač má být součástí sítě, tak musí mít síťovou kartu jako jednu ze součástí základní desky, nebo jako dedikovanou. Tato karta může být připojena k síti, jak pomocí Ethernetu, tak i pomocí Wi-Fi, záleží na tom, k jakému účelu je navržena. U stolních počítačů se nejčastěji nachází síťová karta s podporou Ethernetu, tedy na stolním PC se nachází konektor pro RJ-45. A u přenosných počítačů lze najít více síťových karet, jak pro kabelové připojení Ethernet, tak i bezdrátové připojení Wi-Fi. Síťovou kartu nemusí obsahovat pouze počítače, ale i další zařízení jako tiskárny, či jiná zařízení v domácnosti. [6]

Obrázek 4 Síťová karta [38]

2.4.2 Patch panel

Zařízení, které nemá žádnou vnitřní logickou funkci, ale slouží pouze k agregování a organizaci většího počtu síťových kabelů. Často je lze najít v serverovnách, či na jednotlivých patrech budov. Dělí se dle počtu portů na 48 portů, 24 portů a 12 portů. [40]

2.4.3 Switch

Switch (přepínač) je označováno za L2 zařízení (L2 vysvětleno v *kapitole 3*), které propojuje zařízení na linkové vrstvě OSI modelu. Ke své funkci využívá tabulku MAC adres. Pomocí protokolu ARP zjistí, která zařízení jsou připojena do jeho portů. Pokud switch obdrží rámec, tak ho rozbalí a zkontroluje hlavičku, která obsahuje MAC adresu. Pokud ji zná, odešle rámec na daný port. V případě, že adresu nezná, tak rámec odešle na všechny porty. Přínos, který přináší switch v síti je segmentace a optimalizace provozu. Switch často do sebe sdružuje zařízení z určitých celků, jako je například kancelář, či počítačová učebna. Předchůdcem přepínače byl rozbočovač (hub), který také propojoval zařízení mezi sebou, avšak nedokázal adresovat rámce na konkrétní port a vždy všechny rámce zasílal na všechny porty mimo portu příchozího. Tento postup mohl způsobovat zahlcení sítě.

2.4.4 Router

Tento síťový prvek (směrovač), často bývá prvkem pro lokální síť hraničním a často na něm dochází ke spojení více LAN sítí. Na rozdíl od přepínače pracuje již na L3 vrstvě (L3 vysvětleno v *kapitole 3*), tedy paket rozbalí až na síťovou vrstvu a podle cílové IP adresy vybere na jaký další prvek paket odešle. Často, zde bývá tzv. default route, která definuje, kam odchází provoz, pokud daný adresní rozsah není v tabulce route. Směrovač často nabízí porty pro různé technologie, jako jsou například metalické, či optické kabely.

2.4.5 Přístupový bod

Přístupový bod neboli access point (AP) je zařízení, které je schopno poskytovat datovou konektivitu bezdrátovým zařízením. Jedná se o zařízení s rádii, které předává následně provoz na další síťové prvky již pomocí kabelového propojení.

2.4.6 Kontrolér

Zařízení, které spravuje a řídí připojené přístupové body v síti. Umožňuje také oddělení provozu bezdrátové sítě od sítě jiné.

2.4.7 Firewall

Prvek, který nenajdeme v každé síti. Nicméně jeho využití je velmi vhodné v rámci bezpečnosti, protože umožňuje jasné definování, jaký provoz může jít ven z lokální datové sítě, a naopak který může jít zvenku dovnitř. Dnes lze v těchto zařízeních nalézt i umělou inteligenci, která je schopná se pravidla učit sama a tím snížit práci administrátora sítě.

2.5 Významné komponenty

Každé síťové zařízení má své komponenty na základě, kterých může vykonávat svou funkci. Samotná zařízení se často vybírají právě na základě parametrů u jednotlivých komponent. Nevhodně nadefinované parametry těchto komponent mohou později způsobit problémy. Nicméně komponenty s vyššími parametry mají významně vyšší cenu a následně i vyšší režii. Proto je nutné velmi zvážit potřeby na dané zařízení. Pro seznámení byly vybrány následující 4 komponenty:

Procesor

Procesor (CPU) lze označit za mozek počítače, který zpracovává strojové instrukce. Skládá se z milionů až miliard drobných elektrických součástek. Jeho základním parametrem, které popisuje jeho vlastnosti je pracovní frekvence. Jeho zatížení má přímý vliv na výkon zařízení. [39]

RAM

Operační paměť, která umožňuje přímý zápis a čtení dat bez omezení. U síťových prvků tu lze najít tabulky s MAC adresami okolních zařízení. Při vypnutí napájení dochází ke smazání zapsaných dat.

Fyzická paměť

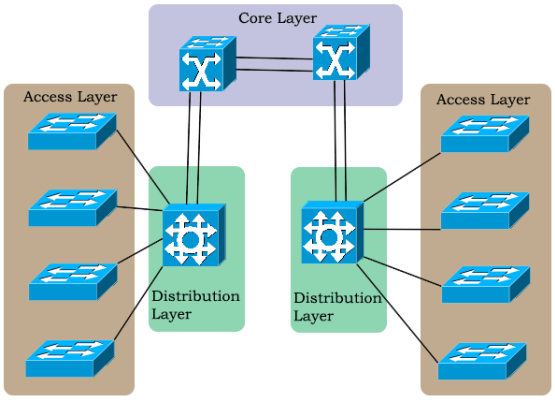
Využívá se pro ukládání dat programů, či samotných uživatelských dat.

Standardy na rozhraních

V posledním případě nejde zcela o komponentu, ale o spíše vlastnost komponent. Z nichž nevýznamnější je oboustranná kompatibilita. Při rozdílnosti standardů může dojít k omezení výkonu zařízení, či zcela omezení jeho funkce. Například rozdílné standardy na síťové kartě počítače a rozhraní přepínače mohou vést k menší přenosové rychlostí.

2.6 Hierarchie síťové vrstvy

Síťové prvky lze rozdělit na tři vrstvy na základě jejich funkce a to na: páteřní (core), distribuční (distribution) a přístupovou (acess). Toto dělení je vhodné z důvodu určení přesnějších požadavků na dané zařízení a jeho role v lokální datové síti. Často se také používá při návrhu lokální datové sítě a dokáže zrychlit práci při hledání problému na síti. [19]



Obrázek 5 Hierarchie síťových prvků [1]

Přístupová vrstva - zajišťuje propojení mezi koncovými zařízeními a prvky distribuční vrstvy. Vlastností této vrstvy je, že propojuje velké množství rozdílných zařízení. Přístupové vrstva má za úkol provádět přeposílání paketů a vedle toho může vykonávat základní bezpečnostní principy, jako je například filtrace MAC adres, či prevence proti falešnému DHCP serveru.

Distribuční vrstva - funkce této vrstvy je přijímat data od prvků z přístupové vrstvy a přeposílat je o vrstvu výše do páteřní vrstvy. V této vrstvě se lze setkat s redundancí zařízení, které na jednu stranu přináší větší spolehlivost, ale na druhou stranu vyšší požadavky na správnou konfiguraci.

Páteřní vrstva - většinou bývá hraniční vrstvou větších lokálních datových sítí. U menších sítí se tato vrstva nevyužívá. Funkcí zařízení této vrstvy je hlavně směrování paketů mezi více sítěmi. Základní podmínkou této vrstvy je její vysoká propustnost. [19] [1]

2.7 Přínosy počítačové sítě

Počítačová síť a s ní spojený přenos informací rapidně změnil svět. Nyní je možné sdílet s celým světem veškeré informace v řádech milisekund a nemusí jít pouze o holá data, ale i náhradu běžné komunikace mezi lidmi pomocí video hovoru, či sociálních sítí. Za další přínos lze považovat možné využívání jednoho zdroje, či zařízení více subjekty např. sdílené uložiště, či využívání centrálního výpočetního centra. Jedinou podmínkou je být připojen do společné sítě. A díky rozvoji bezdrátových technologií je dnes možné se připojit téměř

odkudkoliv. Proto lze shrnout hlavní přínosy počítačové sítě do dvou termínů: propojení a sdílení. [41]

3. Protokoly pro sledování sítě

Tato diplomová práce je zaměřena na implementaci nástroje pro sledování sítě, proto v této části budou uvedeny protokoly, které je možné využít pro mapování stavu sítě. Nicméně pro pochopení funkcí protokolů, je nutné zohlednit i význam standardů.

Základ těchto protokolů je získávání dat z databází zařízení a předávání je NMS (Networking Monitoring Systém). Tento systém do sebe centralizuje sběr dat ze sítě a informuje administrátora o stavu sítě.

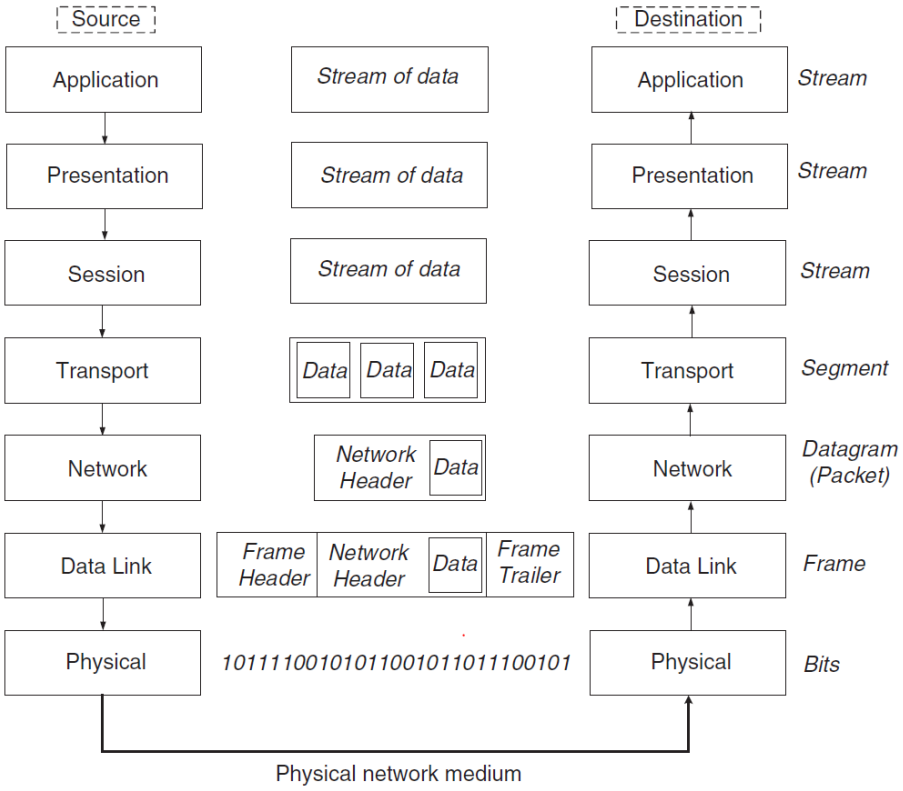
3.1 Pravidla a standardy

Počítačová síť se skládá z mnoha různých prvků a různých technologií, avšak funkcí sítě je vzájemná komunikace. Proto je nutné, aby se zařízení na sítí navzájem dorozuměla. V neprospěch věci si každý z výrobců zpočátku navrhoval své vlastní řešení komunikace. Řešením tohoto problému se staly standardy, kdy nezávislý subjekt jako je např. organizace ISO (International Organization for Standardization) vydala 7 vrstvý standart OSI (Open Systems Interconnection). Následně byla v roce 1984 přijata jako mezinárodní norma ISO 7498. Tento standard sloužil jako základ pro další vytváření norem. Hlavním znakem standardů v počítačových sítí je vrstvení, které umožňuje složité principy zjednodušit na jednotlivé komponenty a tím také umožní jejich pochopení. A pokud dojde například k nefunkční komunikaci, pak lze systémově hledat chybu na základě kontroly funkcionalit jednotlivých vrstev.

Mezi další organizace, které stojí za nejrozšířenějšími standardy, je Institute of Electrical and Electronics Engineers (IEEE). IEEE je zodpovědná za standart 802.3, kterým je popsaná technologie Ethernet, či 802.11 (Wi-FI) více *v kapitole 2.3*. Vedle ní existuje i organizace Internet Engineering Task Force (IETF), která stojí za architekturou Internetu a udržují Requests for Comments (RFC), kde lze najít veřejně dostupný podrobný popis standardů.

3.1.1 ISO model

ISO model se skládá ze 7 vrstev, kde každá z nich má svůj vlastní úkol. Důležitým aspektem tohoto modelu je spojitost mezi jednotlivými vrstvami, kde nižší vrstva je vstupem do vrstvy vyšší. Mezi vrstvami dochází k procesu zapouzdření, kdy informace z předchozí vrstvy je obalena informací z vrstvy aktuální.



Obrázek 6 OSI 7 vrstvý model [6]

Pro pochopení fungování počítačové sítě je nutné znát funkci jednotlivých vrstev, proto zde bude v jednoduchosti popsána každá vrstva z OSI modelu.

Physical layer L1 (fyzická vrstva)

Hlavním úkolem fyzické vrstvy je zajistit přenos jednotlivých bitů (0 nebo 1). Její funkci si lze představit jak převod binárních dat na určité napětí, které se následně přenese po datové cestě. [6]

Data link layer L2 (linková vrstva)

Linková vrstva pracuje s přenesenými bity a dává je do prvních logických celků. V tomto případě jde o rámce (frames). A také operuje při chybnému přenosu, který je často detekován tím, že zařízení příjemce nepotvrdí správné doručení dat. Úprava přenosu je možná pomocí zmenšení rámce, či zpomalení množství přenášených dat. [6]

Network layer L3 (síťová vrstva)

Síťová vrstva má na starost, že data dorazí ke správnému adresátovi. Zde je nejlepším příkladem Internet Protocol (IP), který pro adresaci využívá IP adresy. Síťová vrstva zapouzdří rámec z linkové vrstvy a přidá zdrojovou a cílovou adresu. V kontextu L3 vrstvy se data nazývají pakety. [6]

Transport layer L4 (transportní vrstva)

Transportní vrstva je zodpovědná za navázání úspěšného spojení. Jejím úkolem je i toto spojení založit a následně po přenosu dat v segmentech zase ukončit. Pro tuto vrstvu je zásadní označení portu, díky kterému druhá strana ví, o jakou aplikaci se jedná. Zároveň kontroluje, zda přenášená data dorazila do svého cíle. Pokud ne, tak umožňuje data znovu odeslat. Nejdůležitějším protokolem této vrstvy je Transmission Control Protocol (TCP). [6]

Session layer L5 (relační vrstva)

Tato vrstva má za úkol spravovat spojení mezi aplikacemi. Využívá k tomu následující kroky jako je přihlášení, zabezpečení a ukončení přenosu dat. [30]

Presentation layer L6 (prezentační vrstva)

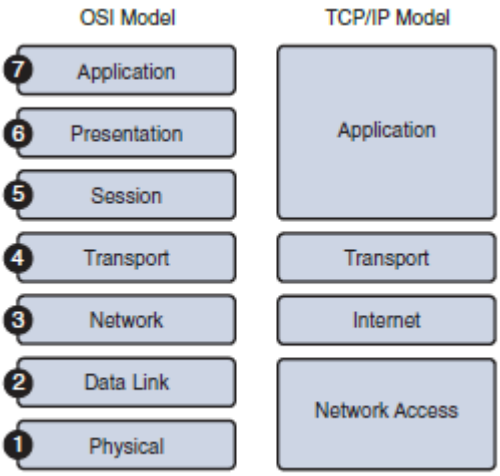
Prezentační vrstva umožňuje reprezentaci dat na koncovém zařízení. Její hlavní funkce je překlad dat a jejich organizace mezi dva systémy pomocí komprese, či dekomprese a šifrování. [30]

Application layer L7 (aplikační vrstva)

Nejvyšší aplikační vrstva má za cíl zprostředkovat koncovou komunikaci mezi aplikačním softwarem a sítí. Prakticky to lze označit za uživatelské prostředí, kde uživatel získá, či vkládá svá data. Např. HTTP (Hypertext Transfer Protocol). [30]

3.1.2 TCP/IP model

Model TCP/IP je základním přenosovým modelem na základě, kterého funguje většina počítačových sítí. Tento model vznikl na základě předchozího OSI modelu a skládá se ze čtyř vrstev. Každá vrstva plní přesně danou funkci, vrstvy jsou navzájem závislé. Pokud dojde k porovnání OSI modelu a modelu TCP/IP (viz *Obrázek 7*), tak lze zjistit, že se liší v počtu vrstev. OSI model je podrobnější, a tudíž umožňuje lepší pochopení principů počítačové sítě a jeho struktura se často využívá jako diagnostická pomůcka při odhalování chyb na síti. Na druhou stranu protokol TCP/IP lépe představuje operace ve dnešních sítích, kde je velmi rozšířený. Aplikační vrstva sdružuje jak aplikační, tak i prezentační a relační vrstvu. Podobné je to u data linkové vrstvy a fyzické, které jsou obě součástí vrstvy síťového rozhraní. Vysvětlení funkcí jednotlivých vrstev lze nalézt níže. [6] [3]

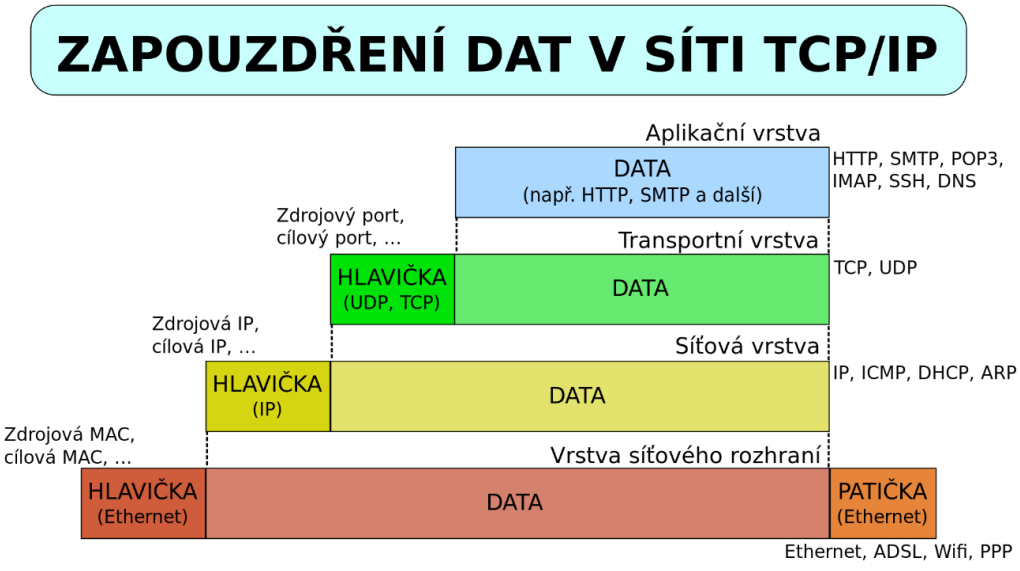


Obrázek 7 Porovnání OSI a TCP/IP modelu [19]

Význam vrstev modelu TCP/IP [10]

- Aplikační vrstva – její funkcí je reprezentovat přenášená data uživateli
- Transportní vrstva – zajišťuje propojení služeb na rozdílných zařízeních
- Síťová vrstva – je zodpovědná za zvolení nejlepší cesty při průchodu sítí
- Vrstva síťového rozhraní – stará se o funkci přenesení dat mezi více zařízeními.

Pro správné pochopení byl vybrán *Obrázek 8*, kde je názorně prezentován postup, jaká další data se přidají k přechozím datům. Celý proces se nazývá zapouzdření. Důležité je mít na paměti skutečnost, že se jedná o proces dvoucestný, takže při odesílání se prvotní data zapouzdří se všemi hlavičkami až do rámce, který je na úrovni fyzické vrstvy nemapován na jednotlivé bity. A následně při přijetí rámce adresátem, se rámec po jednotlivých vrstvách rozbaluje až do finálních dat v aplikační vrstvě. [6]



Obrázek 8 Zapouzdření data v sítí TCP/IP [27]

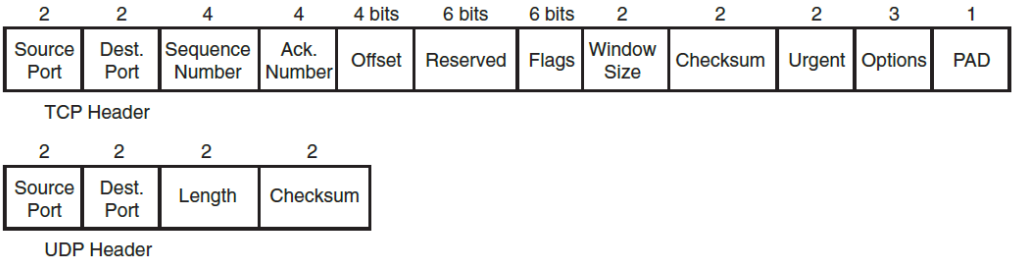
Jak bylo zmíněno výše, tak každá vrstva má svou funkci. Pro naplnění těchto funkcí se využívají síťové protokoly.

3.1.3 Definice síťového protokolu

Ve světě výpočetní techniky je protokol jakýmsi výběrem různých pravidel a procedur pro přenos dat mezi zařízeními. Pokud by žádné protokoly v sítích neexistovaly bylo by nemožné, aby se zařízení domluvila. Pro ilustraci lze uvést příklad, počítač odesílá jedna data rozdělená do 8bitových paketů, avšak příjemce očekává data o v 16bitových paketech. Proto se výrobci dohodli pomocí standardizačních organizacích na standardech, které dále umožní vzájemnou interoperabilitu. Mezi známé a rozšířené protokoly patří např. HTTP a HTTPS, který se využívá pro zobrazení webových stránek. Nebo protokol SSH, který umožňuje vzdálený bezpečný přístup k síťovému zařízení. [34]

Protokol TCP a UDP

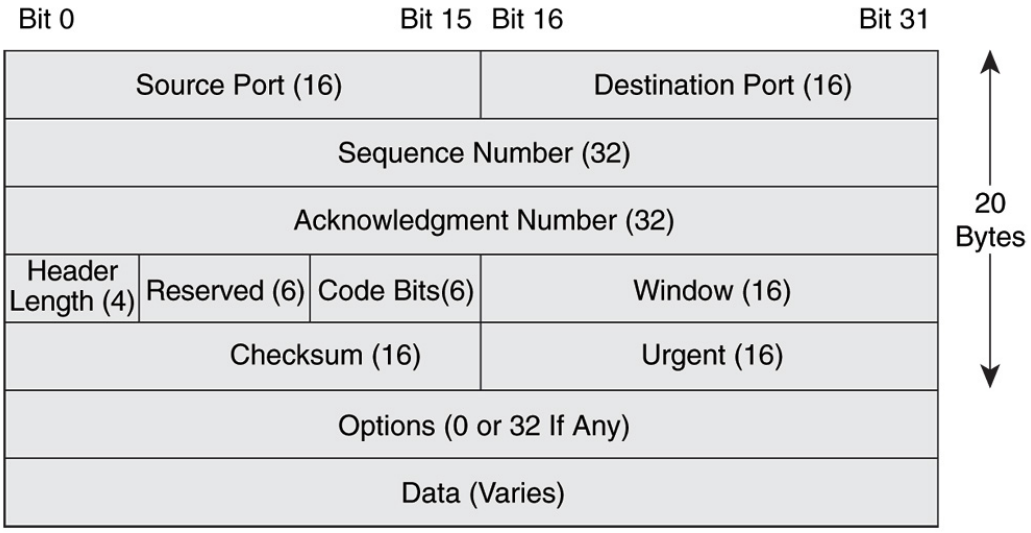
Mezi protokoly transportní vrstvy se řadí protokoly TCP a UDP. Znalost jejich odlišnosti vede k pochopení schopnosti počítačové sítě plnit různé požadavky. Hlavním smyslem sítě je přenášet informace, které mohou mít tyto tři formáty (data, zvuk, video). Každý formát má své požadavky na přenos. Proto existuje transportní protokol TCP, který umožňuje spolehlivý přenos dat na základě toho, že komunikuje během přenosu s adresátem. Hned na začátku spojení se využívá tzv. třícestné potřesení rukou a jeho funkcí je zajistit spolehlivý přenos pomocí speciálních paketů s příznaky. Nejdříve odesílající zašle zprávu s příznakem SYN. A adresát odpoví paketem s příznakem SYN ACK, která označuje potvrzení prvotní zprávy. Poté odesílatel zašle další paket s příznakem ACK RECEIVED a začne samotný datový přenos (např. datový soubor). TCP má v sobě také mechanismus dohlížející na to, aby doručená data byla kompletní. Takže pokud odesílatel zjistí, že nějaký z paketů nedorazil adresátovi, či nedorazil vcelku, tak ho zašle znovu. Princip toho je takový, že pokaždé příjemce odesílá potvrzení ACK původnímu odesílateli. Pokud toto potvrzení nepřijde, tak odesílatel pošle paket znovu, a to tak, že ho rozdělí na více částí, aby příjemce již měl dostatečnou paměť na zpracování dat. Protokol UDP (Unit Datagram Protocol) tento kontrolní mechanismus nemá. Na druhou stranu díky tomu umožňuje rychlejší přenos dat, kdy se nemusí čekat na kontrolní pakety. Avšak nic nezajistí, že data byla příjemcem přijata.



Obrázek 9 Porovnání hlaviček TCP a UDP [41]

Číslo portu

Hlavička většiny síťových protokolů obsahuje zdrojový a cílový port (např. *Obrázek 10*). Označení portů je nutné pro umožnění fungování více služeb na jedné koncové stanici v jednom okamžiku. Pro pochopení si lze představit internetový prohlížeč, s větším množství záložek. V hlavičce bude jako cílový port označen port 80 (služba HTTP), či její zabezpečenější varianta HTTPS, která naslouchá na portu 443. Zdrojový port je často dynamicky zvolen z intervalu volných portů (1024 až 65535) a pomocí něho se identifikuje odchozí služba. [6]



Obrázek 10 Hlavička protokolu TCP [19]

Dělení protokolů

Samotné protokoly lze rozdělit na dvě skupiny. Na proprietární protokol a na protokol otevřený tzv. open-source. Proprietární protokol vzniká pod taktovkou konkrétního výrobce a často bývá vyvíjen pro konkrétní zařízení. Často se stává, že výrobce daný protokol uvolní a stává se z něho volně použitelný protokol. Open-source má výhodu, že ho může využít kdokoliv, avšak na druhou stranu může postrádat speciální funkcionality, které jsou vázané ke konkrétnímu hardwaru.

3.1.4 SNMP

SNMP (Simple Network Management Protocol) je velmi používaný síťový protokol, který slouží ke správě prvků v počítačových sítích. Umožňuje jak samotné vyčítání dat z jednotlivých zařízení, tak i jejich jednoduchou konfiguraci. SNMP protokol využívá UDP a pracuje na portu 161 a 162. Hlavní jeho výhodu je, že je implementován ve většině zařízení. První verze tohoto protokolu je součásti standartu RFC 1157. Proto ho nalezneme v síťových zařízeních všech výrobců. Nejedná se pouze o síťové prvky v úzkém slova smyslu jako jsou routery a switche, ale i veškerá další zařízení, která jsou součástí datové infrastruktury. Jako jsou např. tiskárny, UPS (Uninterruptible Power Supply), či koncová zařízení s libovolným operačním systémem. [25]

Samotný protokol vznikl v roce 1988 s cílem získat nástroj, který umožní správu a vzdálené ovládání v rozrůstajících se sítích. [25]

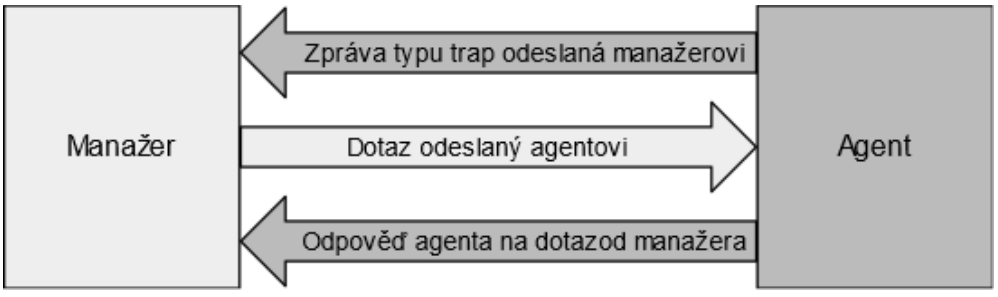
SNMP obsahuje tři komponenty, pomocí kterých lze vytvořit řídící systém pro lokální síť. Tyto komponenty jsou následující:

SNMP manager

Je hlavním prvkem, který sbírá data a umožňuje jejich prvotní zobrazení. Lze si ho představit jako software, který běží na koncové stanici správce lokální sítě. SNMP manager má možnost nahlížet do databází SNMP agentů, či zadávat základní konfigurační příkazy do síťových prvků. Často bývá součástí systému na řízení sítě neboli NMS. [19]

SNMP agent

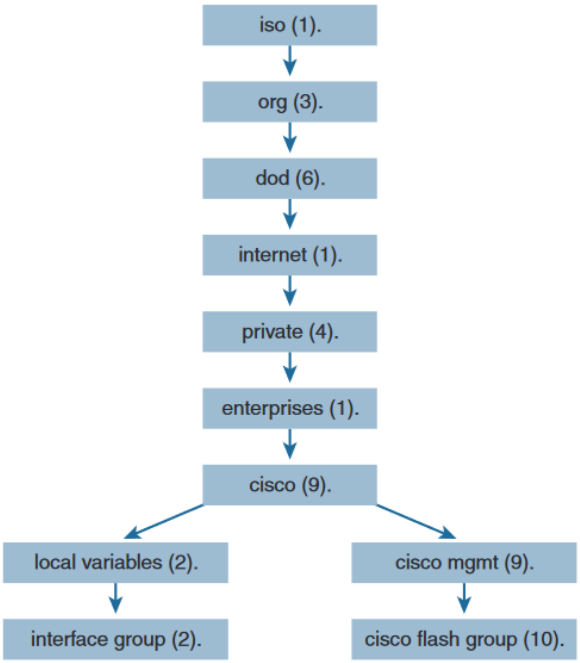
SNMP agent je software, který běží na zařízení v síti, které chceme sledovat, či řídit. Jeho chování lze označit dvěma prvotními cíli. První z nich je odpovídat na dotazy od řídícího prvku (SNMP manager) nebo přímo zasílat definované zprávy prvku tzv. trap v případě anomálního chování na prvku.



Obrázek 11 Vztah mezi manažerem a agentem [25]

Management Information Base (MIB)

Poslední části je databáze. kde agent uchovává svá veškerá provozní data, která jsou následně sbírána pro řízení, či dohled nad sítí. Pokud chce SNMP manager získat určitý údaj musí ho identifikovat pomocí OID (Object ID).



Obrázek 12 Management Information Base [19]

Pro ilustraci využití OID lze uvést jeden příklad, který bude mít za cíl získat ze zařízení Cisco informaci o využití řídící jednotky. Pro zjištění OID se postupuje z vrchu. Tedy se vychází z řetězce 1.3.6.1.4.1.9.2. Avšak pokud by byl zadán pouze tento řetězec, tak by došlo k vypsání většího množství parametrů. Pokud je nutné zjistit pouze jeden konkrétní parametr, je nutné navštívit stránky výrobce zařízení a dohledat zbývající část OID. V tomto případě je úplné znění OID 1.3.6.1.4.1.9.2.1.58.0. [19]

SNMP zprávy

Mezi komponenty SNMP se využívají tři druhy zpráv a každý z nich má svůj význam.

Typ zprávy	**Význam zprávy**
get	SNMP manager je využívá pro sběr dat z agentů.
set	Pomocí těchto zpráv může SNMP manager změnit parametry na agentovi.
trap	Touto zprávou agent ohlašuje dohledovému systému, že nastala mimořádná událost.

Tabulka 4 SNMP zprávy [25]

Verze SNMP

První verze SNMP je z roku 1988, pro možnost získání dat z MIB stačilo pouze znát hodnotu parametru community string. Tento parametr je vlastně jediné zabezpečení proti neoprávněnému čtení dat. Samotné zasílání dat probíhá v nešifrované podobě. Comunity string má dvě podoby. Jedna z nich má pouze právo ke čtení a druhá umožňuje i zápis do konfigurací zařízení. Proto s postupným vývojem bylo nutné tyto bezpečnostní rizika omezit. Řešení přináší až verze SNMPv3, která umožňuje šifrování dat a autentizaci uživatelů. Před příchodem verze SNMPv3 vznikla ještě SNMPv2, která nesla pouze malá vylepšení. [19]

Výhody a nevýhody SNMP

Protokol SNMP je v oblasti informačních technologií již velmi dlouhou dobu, proto je vhodné vyjmenovat jeho výhody a nevýhody, které časem vznikly.

Výhody SNMP

Mezi jeho hlavní výhody patří jeho rozšířenost. SNMP agenta nalezneme v nejrůznějších zařízeních mimo počítače i v tiskárnách atd. Databázím MIB je možnost velmi dobře porozumět díky kvalitní dokumentaci výrobců. Nespornou výhodou SNMP je jeho využitelnost pro řízení chyb v síti a jeho univerzálnost mezi zařízeními různých výrobců.

Nevýhody SNMP

SNMP se může dnes zdát velmi zkostnatělé a uživatelsky nekonformní. Nicméně jeho princip je jednoduchý a nabízí možnost jej začít využívat téměř ihned. Bohužel jeho prvotní návrh nebyl dimenzovaný na možnosti, které nabízejí nové produkty. Proto SNMP dochází ke svým limitům. Také výrobci novějších zařízení začínají pomalu omezovat jeho funkce. Protože často výrobci mají svá řešení, která chtějí svým zákazníkům prodat.

3.1.5 NETCONF

Tento protokol přichází se vznikem nového datového modelu YANG (Yet Another Next Generation) v roce 2006, který se nachází uvnitř síťových prvků a agreguje do sebe řídící a stavová data v čitelné formě díky kořenové struktuře. NETCONF (Network Configuration Protocol) vznikl jako vylepšený následovník SNMP, který již netrpí limitacemi a jehož autorem je organizace IETF. Připojení na zařízení je zajištěno pomocí služby SSH a samotný přenos dat je formátu XML. [2] [23]

3.1.6 RESTCONF

RESTCONF je další protokol, který se dá využít pro sběr dat ze sítě, vznikl jako podmnožina protokolu NETCONF, který funguje na bázi RestAPI a data zasílá v podobě HTTP ve formátu JSON. [24]

3.1.7 gRPC

Protokol vyvinutý společností Google, který zprostředkovává data na základě požadavků. Tyto požadavky se zasílají na zařízení a to odpovídá. Výhodou tohoto protokolu je, že je nezávislý na programovacím jazyku a jeho nastavení je jednoduché.

Získávání dat ze zařízení nemusí probíhat pouze na základě protokolů uvedených v této práci. Existuje celá řada dalších jiných protokolů pomocí, kterých mezi sebou zařízení komunikují Avšak zásadní predispozice k tomu, aby sběr dat ze zařízení mohl probíhat je jeho podpora na obou zařízeních, jak na kolektoru dat (manažér), tak i na sledovaném zařízení. Protokoly, které zařízení podporuje lze nalézt v technické dokumentaci.

4. Kvalita služeb

Součástí tématu této práce je pomocí nástroje zajistit kvalitu služby, proto je zde na místě blíže rozebrat téma kvality služeb a představit základní metriky této oblasti, či její možná dělení. Vedle toho se zaměřit se na její samotný význam, který spočívá v rámci této práce v definování vnitřní kvality služby na základě různých parametrů pro jednotlivá zařízení. S cílem zaručit plnou funkcionalitu těchto zařízení.

4.1 Úvod do problematiky kvality služeb

S termínem kvalita služby se lze setkat dnes čím dal tím častěji, a jeho pochopení může být často zavádějící. Při definování významu pojmu kvalita služeb (Quality of Service) v oblasti lokálních datových sítí je značně komplikované najít jednoznačnou definici. Proto je zde důležité zohlednit interpretaci Mezinárodní telekomunikační unie (International Telecommunication Union), která definuje kvalitu služby takto: *„Celkový efekt provozních charakteristik, který určuje stupeň satisfakce služby“* [12] . Při zhodnocení významu lze vyvodit její značnou obecnost. V její formulaci nejsou zmíněné žádné konkrétní charakteristiky a ani metriky podle kterých lze hodnotit satisfakci služby. Na druhou stranu lze tento pojem využít v různých oblastech. Avšak formálně nejvíce spadá do oblasti datových sítí, kde se s ním lze také nejčastěji setkat. [12]

4.2 Dělení kvalit služeb

Literatura zohledňuje dva pohledy, z kterých lze tuto problematiku chápat. Jedná se o vnitřní a vnímanou kvalitu služby.

4.2.1 Vnitřní kvalita služeb (Instrinsic QoS)

Vnitřní kvalita služeb definuje úroveň, na které síť poskytuje hlavně přenosové služby pro aplikace. Pokud je nutné zhodnotit funkci sítě, pak se k tomu využívají jednotlivé výkonnosti charakteristiky sítě. Pro měření se využívají koncové body, kde se daná služba poskytuje.

Například se může jednat o koncovou stanici, kde uživatel přistupuje a pracuje s danou aplikací. Požadované výkonnostní charakteristiky sítě byly definovány při technickém návrhu sítě tak, aby splnily prvotní požadavky. Při návrhu sítě se zohledňují limity zařízení, ze kterých se síť skládá a dále lze tyto charakteristiky upravit i konfigurací a architekturou sítě. Při popisování vnitřní síťové kvality služby lze využít i pojem kvalita síťových služeb (network-level QoS). [12]

4.2.2 Vnímaná kvalita služeb (Percieved QoS)

Vnímaná kvalita služeb se zaměřuje pouze na kvalitu služby konkrétní aplikace z pohledu koncového uživatele, který jí využívá. Tato kvalita služby závisí na více aspektech než pouze na komunikačních procesech aplikace. Pod tyto další aspekty lze přiřadit i samotné zařízení, kde aplikace běží, či organizační postupy pro práci s danou aplikací. Nicméně velký vliv hraje i subjektivní očekávání uživatele, které často může odsunout do pozadí objektivní funkci aplikace. Pro vnímanou kvalitu služeb se používá termín aplikační kvalita služeb (application-level QoS). [12]

Tato práce se zabývá vnitřní kvalitou služeb, kterou lze lépe kvantitativně uchopit a při dlouhodobějším sledování sítě jsou tyto identifikátory průkaznější. Dnes je hlavním požadavkem na každou lokální datovou síť nepřerušovaný a bezchybný přenos dat. Vedle toho každá aplikace, či uživatel může mít různé požadavky na datovou síť (např. přenosová rychlost, latence). A zde je důležité si uvědomit skutečnost, že sít je jednotné sdílené přenosové medium pro různé potřeby. Tedy často může docházet k tomu, že jeden provoz ovlivňuje druhý. Následkem mohou být výpadky v hovoru, či v hraničních případech celková nedostupnost služby. Hlavním cílem kvality služeb je uzpůsobit síť tak, aby naplňovala požadavky, které jsou na ní kladeny. [12]

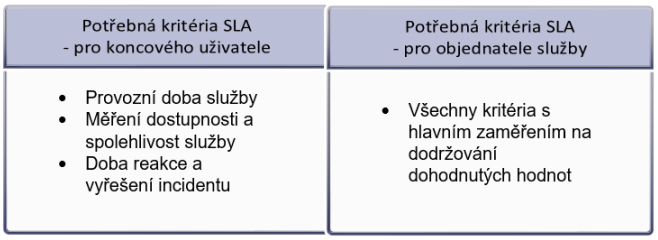
4.3 QoS metriky

Kvalitu služby lokální datové sítě nelze vyjádřit pouze jedním měřítkem, protože parametry kvality služby jsou na sobě nezávislé. Tudíž pokud lze dosáhnout vysoké přenosové rychlosti (např. 1Gbps) nemusí to nutně znamenat, že všechny služby budou zcela plnit svou funkci. Pokud na síti bude docházet k přenosovým zpožděním, tak funkcionalita sítě může být značně omezena. Proto je potřeba kvalitu služeb kvantitativně hodnotit na základě více parametrů jako může být zpoždění, propustnost, či dostupnost. [15]

Kvalita služeb datové sítě je často smluvně ohraničena kritérii SLA. Konkrétněji se jedná o dohodu mezi dodavatelem a objednavatelem služby, která má za úkol dohlížet na korektní zajišťování služeb. Její podoba je formalizovaný popis služby, který obsahuje rozsah, úroveň a kvalitu služby. SLA obsahuje následující kritéria:

- Obsah a popis služby
- Provozní doba služby
- Měření dostupnosti a spolehlivosti služby
- Měření výkonosti služby
- Doba reakce a vyřešení incidentu
- Schválení změny služby a její implementace
- Zodpovědnosti obou stran
- Postupy pro komunikaci
- Reporting
- Proces revize
- Bezpečnostní parametry

Pokud jde o i potřeby koncového uživatelé, tak hlavními faktory, kterého ovlivní, jsou provozní doba služby, měření dostupnosti služby a její spolehlivost. Případně doba reakce, pokud nastane incident. Ostatní faktory jsou důležitější pro projektové řízení ve firmě, kde na základě těchto údajů lze vyvolávat strategické změny. Proto je vhodné tyto dva pohledy ohledně SLA oddělit na:



Obrázek 13 Korelace SLA s konkrétními subjekty [autor]

Z hlediska rozsahu této práce není možné pracovat se všemi kritérii, které v rámci kvality služeb lze měřit. Proto se práce zaměřuje pouze na konkrétní metriky kritérií, které mají největší výsledný vliv na koncového uživatele (metrikami se zabývá *kapitola 9.1*).

4.4 Požadavky uživatelů na lokální datové síti

Pro koncového uživatele je nejdůležitějším požadavkem dostupnost služby, která jasně ovlivňuje, zda uživatel lokální datové sítě může pracovat, či nikoliv. Pokud uživatelé nemohou pracovat se svými aplikacemi delší dobu, může dojít k velkým negativním důsledkům. Může dojít jak k ekonomickým ztrátám, tak i ke reputačním.

Druhým požadavkem, který může negativně ovlivnit efektivitu práce s aplikacemi je velká latence. Pokud je její hodnota do 100 milisekund je pro většinu uživatelů latence nedetekovatelná. Pokud však dochází k větším zpožděním, pak je práce s aplikacemi nekomfortní až nemožná a výsledkem často bývá větší počet stížností na poskytovatele služby.

Pro definování spokojenosti uživatelů existuje celá škála metod. Jako jsou například metody kvality, rizikové analýzy či analýzy stavu IS-IS a následně AS-IS. Pokud je cílem se zaměřit například na objektivní hodnocení kvality hlasu, tak lze využít metodiku MOS (Mean Opinio Score). [15]

4.5 Výpočet parametru dostupnosti

V SLA se často definuje dostupnost konkrétních služeb, či zařízení. Pokud dojde k překročení těchto hodnot, může objednavatel služby vymáhat po poskytovateli smluvní náhrady. Pro výpočet počátečních hodnot je nutné brát v úvahu hodnoty parametrů, které se přímo podílejí na výsledné hodnotě dostupnosti. Lze je také použít pro budoucí predikci.

Název	Zkratka	Význam parametru
Mean time between failures	MTBF	Průměrná doba, kterou zařízení bude pracovat, než nastane jeho výpadek.
Mean time to repair	MTTR	Průměrná doba, která je nutná na opravu systému.
Availability	-	Definovaná hodnota dostupnosti

Tabulka 5 Parametry dostupnosti [6]

Hodnotu dostupnosti pro konkrétní prvek se vypočítá takto:

$$\text{Dostupnost} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}$$

Pro ukázkový příklad byl vybrán 12portový switch 2950 od výrobce Cisco, který má ve své technické dokumentaci definovánu hodnotu MTBF na 482,776 hodin. Čas na výměnu není v dokumentaci uveden, tak určená hodnota je 24 hodin, která odpovídá době doručení nového zařízení při reklamaci zařízení u partnerské firmy. [6]

$$\text{Dostupnost} = \frac{483}{483+24} = 95{,}3\%$$

Na příkladu lze demonstrovat, že pokud je prioritou maximální dostupnost, je nutné, co nejvíce eliminovat čas opravy. Proto je vhodné mít v zásobě náhradní zařízení, či jasně popsané postupy na opravu zařízení. S tímto souvisí i nutnost zálohování konfigurací síťových prvků.

Pokud správce systému zajímá dostupnost celé lokální sítě, je nutné vypočítat hodnotu dostupnosti pro každý prvek a následně tyto hodnoty mezi sebou vynásobit. [6]

5. Monitoring sítě

Následující kapitola této práce je zaměřena na představení problematiky monitoringu sítě z pohledu řízení sítě a představení jeho významu pro infrastrukturu.

5.1 Význam monitoringu sítě

Noční můrou každého správce sítě je noční telefonát. Uživatel, který v noci dodělává podklady pro odevzdání v hraničním termínu si stěžuje, že mu nefunguje připojení do vzdálené aplikace. Samotný uživatel je značně nervózní, protože v tuto chvíli s aplikací opravdu potřebuje nutně pracovat. Pokud síť disponuje vzdálenými přístupy, je správce sítě schopen problém vyřešit. Avšak pokud se jedná o fyzický problém na zařízení, kdy je nutné ho vyměnit celé, či nějakou jeho část, je situace složitější. Čas na vyřešení problému se může značně prodloužit třeba i na den. Výsledkem tohoto výpadku může být například pozdější výplata mezd. Nicméně pokud se podobný scénář odehraje ve firmě, která má nepřetržitou výrobu, může dojít ještě k zásadnějším následkům. Proto je nezbytně nutné těmto situacím předcházet. Možným řešením, které bývá dnes základem každé lokální datové sítě, je monitoring sítě.

Anglické slovo monitoring lze přeložit do češtiny jako sledování, či dohlížení. A ve spojitosti s lokální datovou sítí je jeho významem hlavně hlídání funkčnosti samotné sítě. Zda všechny její prvky pracují správně a zda naplňuje definované požadavky. V situacích, kdy dojde k výpadku, či jinému problému, tak informuje správce systému. Ten má již připravené postupy, které definují kroky pro co nejrychlejší odstranění problémů. *Tabulka 6* shrnuje přínosy a zápory, které obnáší to, zda se správce lokální datové sítě rozhodne pro implementaci monitoringu sítě, či nikoliv. [32]

Monitoring sítě je implementovaný	Monitoring sítě není implementovaný
• rychlá detekce problému • možnost implementace workflow při detekci • centralizovaný dohled všech zařízení • možnost využít systému rolí • jasné výstupy o aktuálním stavu sítě	• ušetřený čas při spravování dalšího systému • úspora dalšího hardwaru • úspora času při přidávání nových zařízení do sítě • absence bezpečnostního rizika při centralizaci dat o síti • vyšší nároky na dokumentaci

Tabulka 6 Porovnání implementace monitoringu sítě [autor]

5.2 Přístupy k monitorování sítě

Pro monitorování sítě lze zvolit dva přístupy: aktivní, či pasivní. Záleží na využitém nástroji, zda podporuje využití obou přístupů. Aktivní monitoring lze také označit za proaktivní, kdy dochází k simulaci chování uživatelů a s tím spojené odezvě sítě. Nicméně tento přístup je velmi náročný na propustnost sítě, protože je zde nutné nepřetržitě zasílat velké množství dat do agregačního prvku. [9]

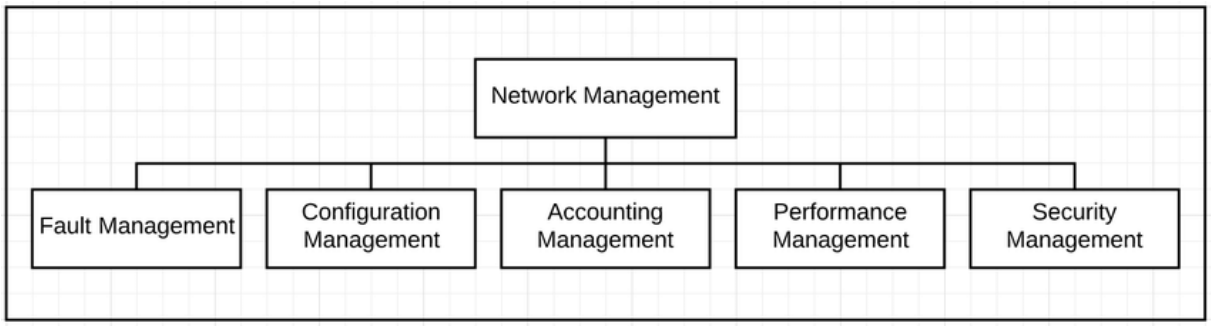
Druhý přístup je pasivní, kdy dochází ke sběru a vyhodnocení pouze aktuálních dat. Tato data na rozdíl od aktivního sledování sítě nejsou sbírána kontinuálně, ale pouze v daných

intervalech. Zde záleží, jaká data se sbírají. Pokud jde čistě o statické hodnoty, jako může být například název zařízení, či verze jeho operačního systému, stačí tento údaj získávat každou hodinu na rozdíl od vytížení řídící jednotky, u které se data dynamicky mění. [9]

Hlavním hlediskem, které je nutné na začátku určit je, zda je síť vůbec řízena. Neboli že její provoz a další vývoj je na základě určitého plánu s cílem plnit předem definované požadavky. Pokud nejsou definované žádné požadavky, nelze potom označit, zda systém je funkční, či nikoliv. Proto je zde důležité si definovat, co vlastně znamená řízení sítě (Network Management).

5.3 Network management

Jak bylo řečeno výše, tak počítačová síť se skládá z mnoha prvků. Každý z těchto prvků má svojí funkci a možná nastavení. Často bývá centrálním prvkem pouze administrátor sítě. Lidské kapacity jsou schopné sledovat pouze omezené množství informací. Cílem řízení počítačové sítě je co nejvíce předejít výpadkům, či jiným událostem, které mohou ovlivnit její funkci. Pro řízení počítačové sítě existuje model, který se skládá z pěti pilířů a jeho tvůrcem je organizace ISO. Představuje koncepční přístup pro řízení sítě. Význam tohoto modelu je prezentovat všechny komponenty sítě, které je nutné spravovat. [6]

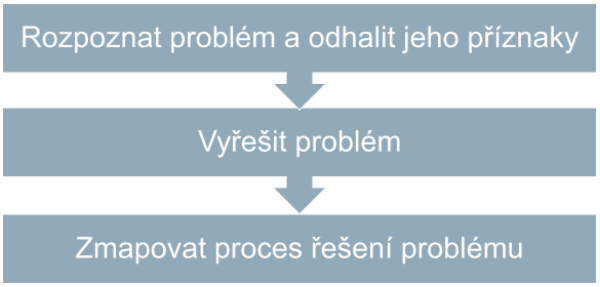


Obrázek 14 ISO – Network management [25]

5.3.1 Fault Management

Fault management (řízení chyb) se zabývá detekcí a následnou nápravou chyb, které v síti nastaly. Může jít například o výpadek konektivity na jednom patru z důvodu přerušení datové cesty při rekonstrukci. Při zjištění určité abnormality v síti je nutné najít její příčinu a tu následně odstranit. Detekce chyby bývá nejčastěji provedena samotným uživatelem, který zjistí, že mu určitá funkcionalita na jeho zařízení nepracuje, tak jak je on zvyklý. Avšak tento přístup není správný, protože na daný problém měl přijít sám administrátor pomocí testů dostupnosti, při pohledu na telemetrická data, či při porovnávání dat z logů. [6] [22]

Řízení chyb obsahuje kroky (*Obrázek 15*), jak by měl správce systému postupovat, pokud dojde k problematické události. [25]



Obrázek 15 Proces při řízení chyb [25]

Často se zapomíná na zmiňovaný třetí krok. Avšak tento krok je velmi důležitý pro budoucí fungování systému, protože může dojít k obdobné situaci později, či ji bude řešit někdo jiný bez předešlé zkušenosti. Pokud jsou problémy a jejich řešení kvalitně dokumentovány, může systém vykazovat lepší hodnoty celkové dostupnosti. [25]

5.3.2 Configuration Manegement

Při změně prvků v síti, či jejich rozšiřování je velké riziko, že dojde k chybě, která ovlivní celou síť. I přesto, že může jít jen o překlep během konfigurace. Proto je zde nutné mít všechna nastavení konkrétního zařízení dobře zdokumentovaná a zálohovaná. Pokud jsou známá propojení zařízení a význam jejich konfigurací, je při výpadku následně rychlejší náprava. Nicméně často se vedle zálohování konfigurací zapomíná na mapování typu zařízení, verze jejich systému, či data jejich uvedení do provozu, dle doporučení z knihy *Essential SNMP* [25], Autoři uvádí, že je vhodné mít následující informace v databázi ke všem prvkům infrastruktury. [6] [22] [25]

- verze operačního systému, či firmwaru
- počet síťových rozhraní a jejich rychlost
- počet a velikost paměťových disků
- počet procesorů
- velikost operační paměti

Pokud se tyto informace pravidelně aktualizují při změnách, mohou velmi dobře pomoci urychlit proces řešení problému na síti.

5.3.3 Accounting Management

Význam následujícího pilíře je mapování, co jaký uživatel, kdy a kde vykonal. Hlavní výhodou tohoto řízení je pomoc při hledání osoby, která způsobila chybu, či se podílela na vzniku výpadku. [6] [25]

5.3.4 Performance management

V síti je důležité sledovat její výkon, zda nedochází na žádných prvcích ke zpoždění, či zhoršení kvality služeb, které jsou definované v rámci SLA. Lze sledovat i další parametry jako je počet opakovaných odesílání, využití přenosového media apod. Cílem je mít výkon sítě

optimální, tak aby naplnila požadavky a na druhou stranu nebyla předimenzovaná. Příliš předimenzovaná síť je nákladná na provoz. [6]

Hlavní rolí řízení výkonu je jasně definovat hranice, u kterých je při jejich překročení nutné spustit konkrétní akce a rozhodnout, zda se již jedná o závažný problém, který je potřeba řešit. [25]

5.3.5 Security management

Řízení bezpečnosti je důležité hlavně z preventivního významu. Často se jedná o aplikaci antivirových programů na jednotlivých koncových stanicích, přísné bezpečnostní politiky a snaha o to mít všechna data zálohovaná. Avšak má i druhý význam, a to v případech, kdy dojde k bezpečnostními incidentu, tak aby měl, co nejmenší důsledky na celý systém. Samotnou bezpečnost lze vnímat ze dvou pohledů. Prvním z nich je síťová bezpečnost, kdy se útočník snaží dostat do lokální sítě z vnějšího prostředí. Druhým pohledem, na který se často zapomíná, je vnitřní bezpečnost, kdy se fyzicky zamezí přístupu k zranitelným prvkům infrastruktury. [6] [25]

Tato práce je hlavně zaměřena na dvě části z konceptu řízení sítě, a to řízení chyb a řízení výkonu lokální datové sítě. Pro tyto účely je vhodné síť centrálně monitorovat pomocí jediného nástroje.

6. Nástroje pro sledování sítě

Tato kapitola je zaměřena na představení nástrojů pro sledování sítě (monitoring sítě). I přesto, že je tato práce zaměřena na dostupné nástroje, tak je důležité zmínit i nástroje placené. Ať už z důvodu implementace, či práce se samotným nástrojem.

Určitě je možné sledovat síť bez využití nástroje, pouze pomocí manuálních příkazů. Tento přístup je velmi neefektivní a časově velmi náročný, ale je nutné ho občas využít v případě hledání příčiny problému na síti. Proto existuje celá řada nástrojů, které sbírají data automaticky a umožňují nastavení logických podmínek, které mohou informovat správce lokální datové sítě o problému. Tyto nástroje lze označit jako monitorovací, či dohledové systémy. V první části této kapitoly budou tyto nástroje krátce představeny s důrazem na jejich funkcionality. Ve druhé části budou představeny přístupy a možné využití nástrojů pro diagnostiku sítě. Všechny nástroje v této kapitole používají určité protokoly viz *kapitola 3.*

Nástrojů pro sledování lokální datové sítě a celé infrastruktury je celá řada a jejich význam stále roste. Důvodem je stále významnější role síťové konektivity ve všech odvětvích. Nástroje se nejčastěji dělí na základě toho, zda se jedná o volně šiřitelný produkt tzv. opensource, či produkt placený. Níže *Tabulka 7* shrnuje jejich základní rozdíly.

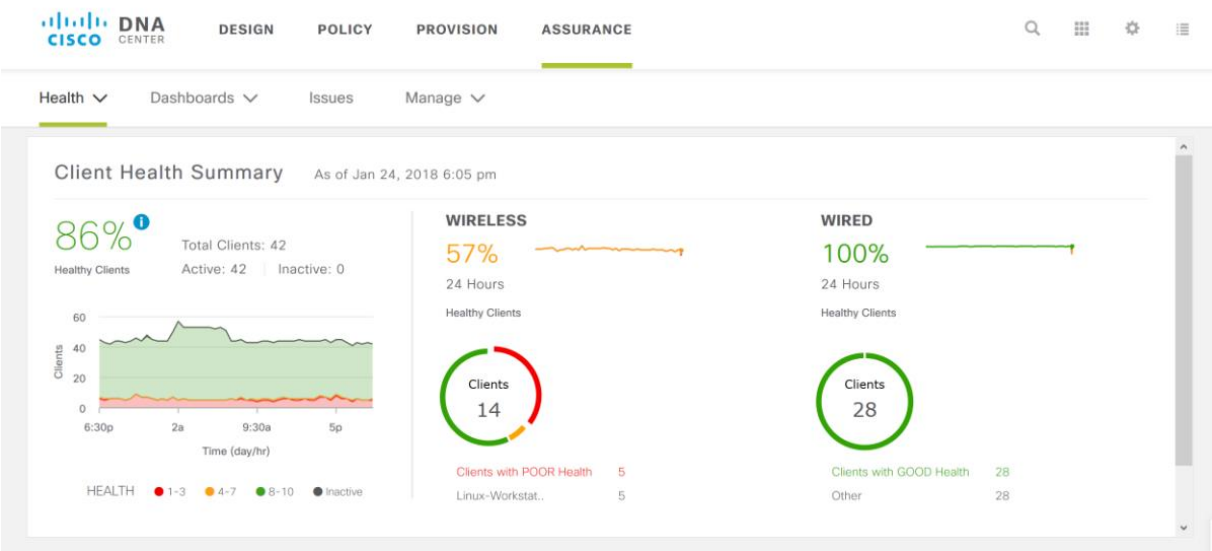
opensource nástroj	placený nástroj
• nástroj je vyvíjen a testován otevřenou komunitou • každý má přístup k úpravě a sdílení zdrojového kódu • k implementaci a úpravě nástroje je nutné mít alespoň základní znalosti IT • možnost individuálních úprav nástroje pro vlastní potřeby • podpora pouze v rámci komunit • bezplatný nástroj	• nástroj je vyvíjen a testován organizací prodávající tento produkt • pouze organizace může upravovat zdrojový kód • implementace je jednoduchá • k nástroji je dostupná podpora, která umí rychle pomoci • standartně nabízí od laděnější funkcionality • jednorázová platba, či možnost předplatného

Tabulka 7 Porovnání vlastností placeného a opensource nástroje [20]

Samotných nástrojů je v obou kategoriích velké množství, v řádech desítek. Cílem této práce není představit jednotlivé nástroje, ale provést jejich celkové zhodnocení za účelem výběru jednoho nástroje. Nicméně k tomuto tématu vzniklo mnoho publikací. Tato práce se bude odkazovat na článek *Tools for distributed systems monitoring* [11], kde autor představuje jednotlivé nástroje. Další jejich srovnání lze nalézt v článku *IT Infrastrucure-Monitoring Tools* [13].

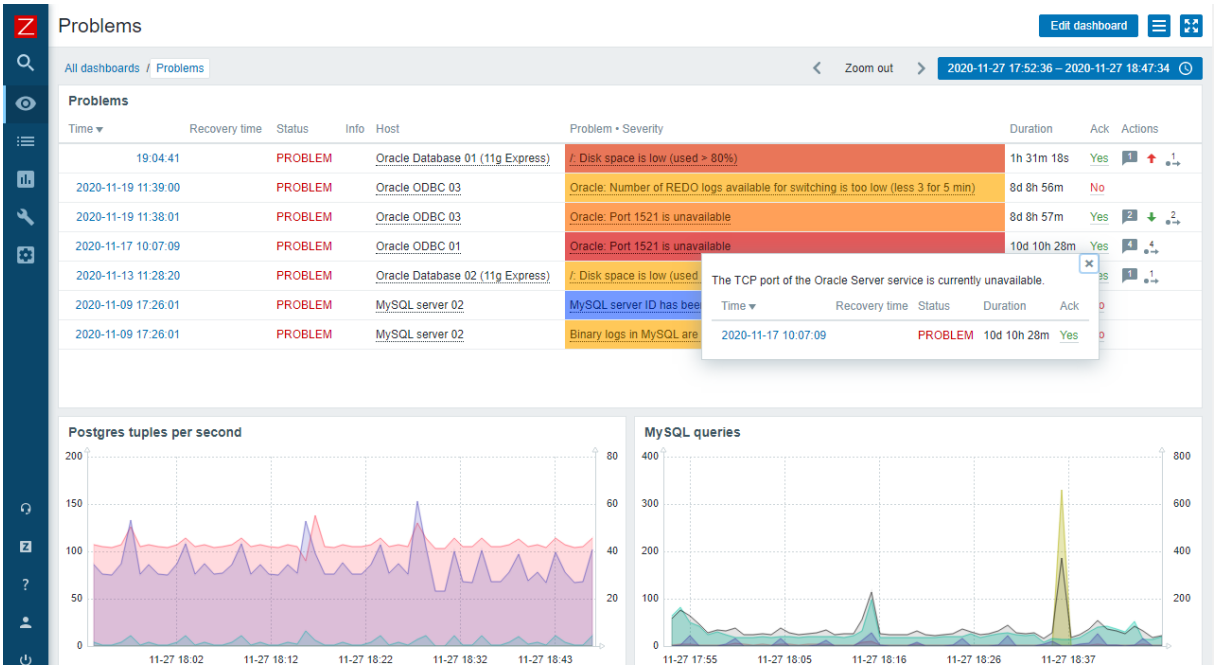
6.1 Porovnání opensource a placeného nástroje pro sledování sítě

Při výběru nástroje je velmi důležité zohlednit aspekt opensoruce (volně dostupný a upravitelný zdrojový kód) nástroje, či placeného nástroje. Proto v rámci této práce budou ukázkově porovnány dva, kde každý z nich zastupuje jednu skupinu. Jako příklady jsou vybrány nástroje, s kterými se autor setkává v rámci své praxe (Cisco DNA a Zabbix). Hlavním rozdílem, který lze v praxi rozpoznat je náročnost implementace samotného nástroje. U nástroje placeného jde vše nastavit pomocí několika kliků a sám ještě nabízí průvodce, který provede uživatele prvotním nastavením. Dalším rozdílem je samotná práce s nástrojem, kde u placených nástrojů je možné zjistit hlavní informace z přehledných dynamických grafů na úvodní stránce. Nicméně pokud je nutné zjistit další informace, které nenabízí webové rozhraní je nutné požadované informace zjistit pomocí příkazové řádky. Pokud dojde k problému na síti nabízí nástroj i základní nápovědy pro odstranění příčiny.



Obrázek 16 Ukázka placeného nástroje Cisco DNA Center [4]

Při implementaci opensource nástroje je nutné počítat s delší časovou náročností. Většina opensource nástrojů je dobře dokumentovaná tak, že samotnou instalaci zvládne i laik. Samotné uvedení nástroje do provozu je jedna věc. Nicméně pokud se využije pouze základní nastavení, stane se nástroj nepoužitelný z důvodů velkého množství problematických zpráv od jednotlivých zařízení. Proto je zde důležitá i další fáze, v rámci které se nastaví nástroj pro potřeby konkrétní sítě. Velkou výhodu však opensource nástroj skrývá v možnosti sledovat jakákoliv zařízení. Stačí pouze, aby komunikovala na základě stejných protokolů. Některé placené nástroje omezují centrální sledování jen na zařízení konkrétního výrobce.



Obrázek 17 Ukázka bezplatného nástroje Zabbix [35]

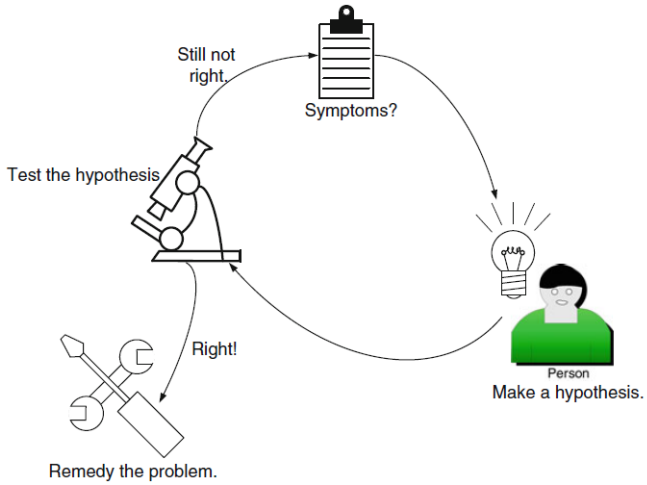
Avšak, zde je nutné od sebe ještě odlišit monitorovací nástroj a službu zaměřenou na monitoring infrastruktury. Monitoring infrastruktury je možné provozovat jako vlastní službu s využitím vlastních zdrojů, či využít monitoring jako placenou komplexní službu od jiného subjektu.

6.2 Diagnostické nástroje

Cílem monitorovacích systémů je upozornit včas na problematickou událost, pokud nastane, a oznámit anomálie v síti, které později mohou vyústit ve výpadek. Pokud však dojde k výpadku, je nutné problém vyřešit. Zde může pomoci několik dalších nástrojů a postupů, které se využívají v praxi.

6.2.1 Postup při hledání problému na síti

Při hledání problému jde hlavně o čas. Administrátor sítě často bývá pod velkým tlakem. To je často kontraproduktivní, protože při hledání příčiny často zapomene vykonat důležité dílčí úkony. Proto i na hledání problému v síti existuje vyzkoušená metodika, která doporučuje systematický postup ze spodu dle vrstev modelu OSI. Samotné hledání příčiny není pouze o odborných znalostech v IT, ale i znalosti vnitřního prostředí, kde daná lokální sít funguje. Ale také i o intuici a předchozích zkušenostech. [6]



Obrázek 18 Systém hledání chyby [6]

Obrázek 18 zobrazuje postup při hledání chyb, kde je nutné si nejdříve uvědomit určité vysvětlení, proč se problém na síti stal. Často tomu napomáhá komplexní zjištění okolností. Zde může posloužit výstup z monitorovacích systémů. Následně otestovat, zda předpokládané vysvětlení příčiny bylo správné, či ne. Pokud se problém neodstraní je nutné hledat další jiná řešení.

Níže budou popsány jednotlivé kroky, které se při hledání chyb v síti využívají.

Fyzický vrstva

Prvním přístupem je kontrola datové konektivity, kde hlavním výsledkem je to, zda zařízení jsou mezi sebou správně spojena na fyzické úrovni. K zjišťování, zda dvě zařízení jsou mezi sebou propojená může na první pohled stačit indikační led dioda, kterou najdeme u všech internetových zásuvek, jak např. u počítačů, tak i u portů síťových prvků. Pro pokročilejší zjišťování stavu lze využít sofistikovanější zařízení, které využívají reflektometry na časové bázi. Výsledek těchto měření je informace o tom, zda jsou kabely propojené, či poškozené. V případě jeho poškození je zařízení schopno dopočítat vzdálenost poruchy od začátku kabelu. Princip, na kterém fungují je podobný jako u radaru. Ze zařízení je vyslán impulz, který když se na konci vodiče odrayí zpět do výchozího zařízení. Zařízení na základě času a rychlosti vypočte vzdálenost místa poruchy dle vzorce. [6]

$$\text{délka vodiče} = \frac{1}{2} \text{ x propagační rychlost x čas cesty pulzu}$$

U počítačů se také může kontrolovat, zda síťová karta uvnitř zařízení se chová správně. K tomuto účelu se může využívat adresa loopback.

Linková vrstva

Pokud je fyzické propojení v pořádku je doporučeno se posunout o vrstvu výše. Zde je nutné zkontrolovat rozhraní na síťových prvcích, zda je například daný port na přepínači ve stavu provozu, či ne.

Síťová vrstva

Na této třetí vrstvě se často nalezne problém, protože zde se zkoumá správná adresace klientů a jejich maska (určuje dělení počítačové sítě na podsítě). Právě v adrese se často chybuje z důvodu překlepu. Další možností jsou špatná nastavení VLAN (Virtual local are network), která umožňují vytvoření virtuálních podsítí uvnitř sítě, které umožní logické oddělení zařízení. Pro ověření spojení se zde hojně využívá nástroj Ping, který nalezneme jak v operačních systémech Windows, tak i jiných. Jeho funkce je založena na protokolu ICMP (Internet Control Message Protocol). Funkce tohoto protokolu ve vyslání paketu ze zařízení, kde je zadán tento příkaz. A pokud je adresované zařízení dosažitelné, tak odpoví. V odpovědi je možné zjistit zpoždění i velkost paketů. Příkaz `ping` nabízí možné nastavení pomocí parametrů. Lze nastavit počet dotazů (-n), či velikost odeslaného paketu (- l).

```
C:\WINDOWS\system32>ping 8.8.8.8 -n 10 -l 68

Pinging 8.8.8.8 with 68 bytes of data:
Reply from 8.8.8.8: bytes=68 time=21ms TTL=117
Reply from 8.8.8.8: bytes=68 time=23ms TTL=117
Reply from 8.8.8.8: bytes=68 time=18ms TTL=117
Reply from 8.8.8.8: bytes=68 time=18ms TTL=117
Reply from 8.8.8.8: bytes=68 time=19ms TTL=117
Reply from 8.8.8.8: bytes=68 time=18ms TTL=117
Reply from 8.8.8.8: bytes=68 time=18ms TTL=117
Reply from 8.8.8.8: bytes=68 time=18ms TTL=117
Reply from 8.8.8.8: bytes=68 time=18ms TTL=117
Reply from 8.8.8.8: bytes=68 time=18ms TTL=117

Ping statistics for 8.8.8.8:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 18ms, Maximum = 23ms, Average = 18ms
```

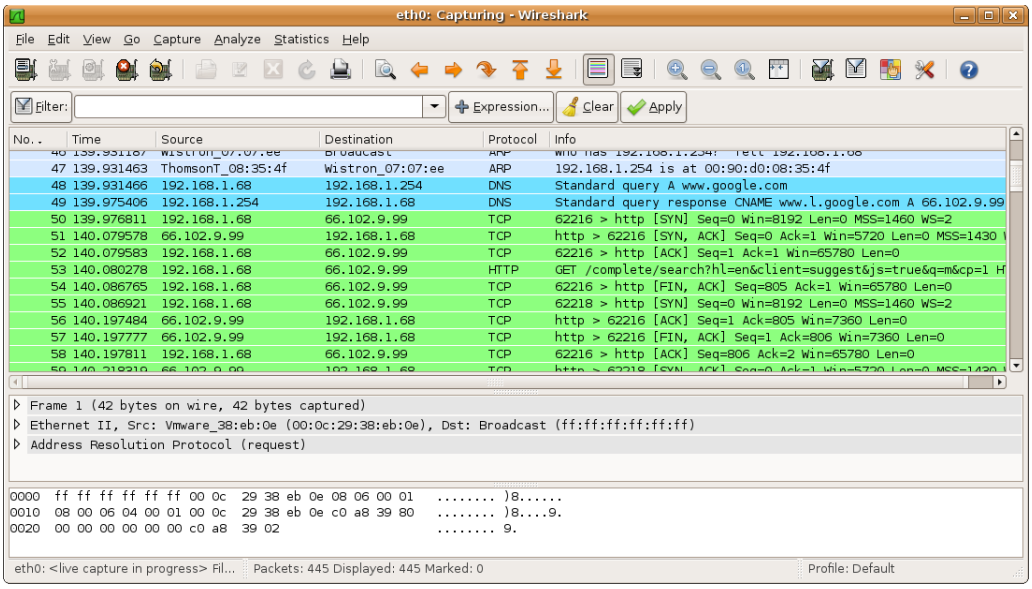
Obrázek 19 Využití příkazu ping [autor]

Transportní vrstva

Pokud jde o firemní síť tak jsou zde často implementovány firewally, které blokují komunikaci na základě pravidel. Pravidla mohou být zavedena na základě služeb, či na definování dovolených a zakázaných adresních rozsahů.

Sledování paketů na síti

Další přístup spočívá v samotném sledování síťového provozu na základě paketů. Z odchyceného provozu lze zjistit několik důležitých parametrů. Mezi tyto parametry patří například zdrojová a cílová adresa, označení protokolů a druh služby.



Obrázek 20 Využití nástroje Wireshark [44]

Samotné přístupy pro sledování sítě si lze rozdělit dál i na základě zkoumaného objektu a hloubky. Lze sledovat síť pouze na bázi paketů, které odhalí, jaké služby uživatelé sítě

využívají, či jaký provoz v lokální síti prochází. Zde lze odhalit podezřelou komunikaci, kde není známa druhá strana, s kterou zařízení komunikuje. Při samotném zkoumání se často postupuje od spodních vrstev OSI modelu. Samotné jednodušší nástroje se často integrují do větších komplexnějších systémů, které se snaží poskytnou celistvý vhled do aktuálního stavu celé infrastruktury. Nicméně základním rozhodovacím parametrem, který určí, jaká všechna data lze získat ze síťového zařízení, je jejich podpora samotným zařízením na bázi protokolů.

7. Výběr vhodného nástroje pro sledování sítě

V dnešní době jsou lokální počítačové sítě rozsáhlé. Hlavním důvodem je možnost připojit různá zařízení, která jsou od různých výrobců. Proto se stává ze sledování sítě velmi komplexní záležitost, kde je třeba brát v úvahu velké množství parametrů. To se odráží i na výběru nástroje pro sledováni sítě. Je možné využívat více nástrojů, ale z pohledu operačního času a centralizovanosti to není vhodné. Pro srovnání možných nástrojů bude využita metoda kvality QFD. O této metodě je možné se více dozvědět v následující literatuře: *Metody kvality užívané ve fázi vývoje výrobku – aplikace v automobilovém průmyslu.* [18] Pro možnost realizace QFD jsou nutným vstupem požadavky na daný nástroj. Požadavky lze získat z odpovědí na kritéria, která je nutné brát na zřetel při výběru nástroje.

U každého požadavku byla určena jeho priorita na škále 1 až 9. Tato priorita vyjadřuje, jak je daný požadavek na nástroj důležitý. Hodnoty ve sloupci pod daným nástrojem určují korelaci mezi požadavkem na nástroj a funkcionalitami nástroje. Pro ohodnocení korelace byla zvolena tato výběrová škála:

0 = žádná korelace, 1 = nízká korelace 3 = střední korelace, 9 = úplná korelace

Výsledek matice QFD se nachází v posledním řádku tabulky. Hodnoty v tomto řádku vznikly jako součin priority a korelací pro porovnávaný nástroj. Nástroje s nejvyššími hodnotami představují nástroje, které nejvíce naplňují definované požadavky.

7.1.1 Kritéria pro výběr nástroje pro sledování sítě

Nalézt odpovědi na daná kritéria je nutným krokem k výběru vhodného nástroje. Pokud by tento krok nebyl zrealizován, mohlo by dojít k tomu, že při použití nástroje budou nalezeny jeho limitace a může následovat výměna již implementovaného nástroje.

Má být vybraný nástroj placený, či open-source?

Důležitým hlediskem je rozhodnutí, zda se na sledování sítě vyčlení finanční prostředky, či nikoliv. Placený produkt často bývá již hotový a není mnoho cest, jak ho upravit dle vlastních potřeb. Na druhou stranu jeho výhodou je, že uživatel dostává funkční řešení na pár kliků. A pokud je platícím zákazníkem, má zpravidla větší možnost rychlé komunikace s dodavatelem,

a tím lze operativně řešit vzniklé problémy na monitorovacím systému. Nástroj open-source nabízí nepřeberné možnosti, jak ho rozšířit o možné doplňky. Také poskytuje širokou základnu uživatelů na diskusních portálech.

Jaká zařízení se budou sledovat?

Dalším velmi důležitým kritériem jsou zařízení, která budou sledována. Zda půjde pouze o koncové stanice v podobě stolních počítačů a notebooků, nebo se v síti budou nacházet i tiskárny, různé sensory pro detekci podmínek v kanceláři, či do sítě bude připojen i například kávovar nebo klimatizace.

Jaký je operační systém sledovaných zařízení?

Následující kritérium je důležité z pohledu kompatibilit. Pro přehledné a automatické výstupy ze zařízení je možné využít agenta. Ne však od všech nástrojů jsou agenti poskytování na všechny operační systémy. A pokud nebude dostupný agent, je nutné zjistit, zda mezi zařízeními je kompatibilita v používaných standardech.

Je nástroj stále aktivně vyvíjen?

Toto kritérium má velmi velký význam ve dvou rovinách. První rovina je bezpečnost, která je zásadní, protože pokud má nástroj pro sledování sítě v sobě bezpečnostní nedostatky, je velmi jednoduché pro útočníka přebrat kontrolu nad celou sítí. Pro nástroje, které jsou stále vyvíjeny, jsou bezpečnostní hrozby odhalovány i zpětně a následně vydáním opravných funkcí odstraněny. A druhou rovinou je vývoj nových funkcionalit nástroje.

Kolik zařízení se bude sledovat?

Nástroje pro sledování mohou mít své limitace ohledně počtu sledovaných zařízení. Proto je zásadní vědět, kolik zařízení se v infrastruktuře nachází, a zda je v plánu počty zařízení navyšovat.

Jaké veličiny a parametry je nutné sledovat?

Pro samotné sledování sítě je důležité vědět, co má být jeho cílem. Na základě toho lze vytipovat parametry. Může jít například o množství odeslaných a přijatých paketů na koncovém zařízení.

Jak nástroj informuje administrátora o problémech na síti?

Posledním kritériem je, jak může daný nástroj komunikovat s administrátorem sítě v případě problému. Zda nástroj umí pouze ve svém GUI zobrazit varovnou hlášku, nebo umí i aktivně informovat administrátora například pomocí SMS.

7.1.2 Matice QFD pro výběr nástroje

Nabídka nástrojů pro aktivní sledování infrastruktury je velmi široká. Lze najít více než 20 různých řešení. Proto bylo vybráno pět nejznámějších a nejlépe hodnocených nástrojů na základě tohoto článku: *IT Infrastructure-Monitoring Tools* [13]. V levé části tabulky jsou definované požadavky na monitorovací systém. Tyto požadavky byly určeny na základě průzkumu testovací sítě.

	Priorita	Ideál	Nagios	Zabbix	SolarWinds	PRTG	WhatsUp gold
Nástroj je bezplatný?	9	9	0	9	0	0	3
Nástroj umožňuje sledovat mimo PC i další připojená zařízení.	6	9	9	9	9	9	6
Nástroj umí sledovat zařízení s různými operačními systémy	9	9	9	9	9	9	1
Nástroj je stále aktivně vyvíjen.	9	9	6	6	9	9	9
Nástroj umí sledovat základní parametry z pohledu kvality služeb	9	9	9	9	9	9	9
Nástroj umožňuje sledovat 1000 a více zařízení.	3	9	3	9	3	9	6
Nástroj informuje správce pomocí SMS a emailu.	6	9	6	9	3	9	6
Vhodnost nástroje na základě požadavků.		459	315	432	324	378	288
	%	100,00	68,63	94,12	70,59	82,35	62,75

Tabulka 8 Část matice QFD pro výběr nástroje [autor]

Na základě skalárního součinu korelací a priorit (*Tabulka 8*) pro dané nástroje lze určit, že nejvhodnějším nástrojem pro aktivní monitoring je systém Zabbix. Hlavní důvodem, proč byl na základě analýzy vybrán tento nástroj, je jeho bezplatnost. Tato vlastnost je velmi důležitá, protože není nutné na jeho implementaci získat žádné finanční prostředky.

8. Vlastní implementace vybraného nástroje pro monitoring infrastruktury

Tato kapitola se bude zabývat jednotlivými kroky při implementaci nástroje pro monitorování sítě. Při bližším průzkumu dostupných nástrojů lze zjistit, že tyto nástroje umožňují sledování stavů nejen síťových prvků, ale i dalších připojených zařízení, které umožňují síťovou konektivitu jako jsou například tiskárny, UPS či sensory. Proto zde lze mluvit již o monitorování celé infrastruktury. V *kapitole 7* byl vybrán jako nejvhodnější nástroj pro testované prostředí monitorovací systém Zabbix. V následujících podkapitolách bude představen postup při vlastní implementaci systému na testované síti. Dílčím cílem je, aby i samotný čtenář po přečtení a využití oficiální dokumentace mohl svou infrastrukturu začít kvalitně monitorovat.

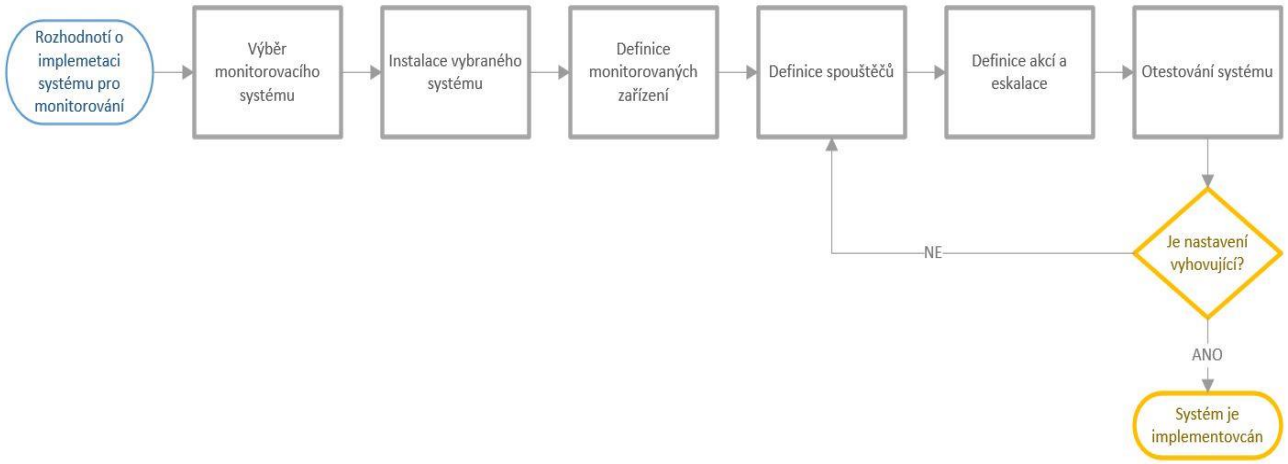
V textu se lze setkat s obrazovou dokumentací a významnými příkazy. Příkazy, či části skriptu jsou graficky odděleny např. `ipconfig`. Funkce i příkazy se mohou lišit s příchodem

novějších verzí nástroje. V textu je zahrnuta metrika popisující datové přenosy. Pro jejich vyjádření jsou použity jednotky bit/s. Pro převod dat lze použít následující vzorec:

1 bajt [B] = 8 bitů [b]

8.1 Přehled kroků při implementaci monitoringu infrastruktury

Vlastní implementace se skládala z následujících kroků, které jsou uvedeny v diagramu níže. Jednotlivé kroky budou v rámci praktické časti této práce realizovány.



Obrázek 21 Přehled kroků instalace monitorovacího systému [autor]

Před samotnou implementaci je doporučeno promyslet samotný proces využívání monitorovacího nástroje. Jedním ze způsobů je, si položit následující otázky. Formulace těchto otázek proběhla na základě odborné konzultace.

Co a proč se má sledovat?

Zásadní otázka, bez které není možné kvalitně implementovat monitoring infrastruktury. Odpovědi mohou být různé, lze sledovat všechna zařízení, či jen ta nejdůležitější. A na nich jen konkrétní parametry, či veškerá data. Nejčastějším důvodem je znalost aktuálního i historického stavu spravované infrastruktury.

Jak to lze sledovat?

Pro sledování zařízení v infrastruktuře může být více způsobů. Lze sledovat zařízení pomocí doptávání se NMS, či pomocí sbírání dat pomocí agentů, kteří jsou instalovaní na zařízeních.

Kdo má jaké kompetence pro sledování?

Otázka kompetencí i v tomto tématu hraje velkou roli. Při využívání monitoringu lze využít systém rolí, kde daný uživatel má práva pouze na konkrétní data. Například pro sledování

grafů postačí pouze jen pro čtení, která nemá možnost jakýmkoliv způsobem upravovat monitorovací systém.

Co se stane, když hodnoty překročí určitou podmínku?

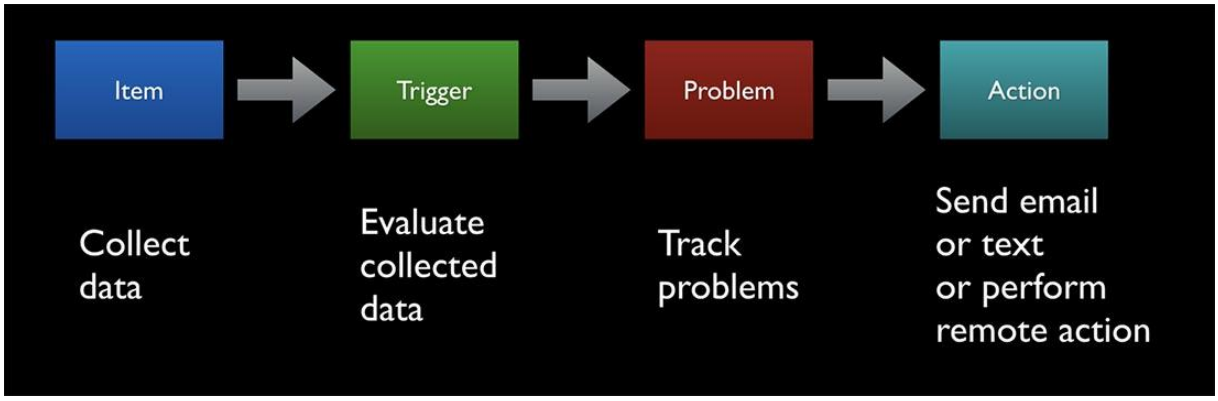
Z pohledu autora nejdůležitější bod je definování postupu při detekci problémové události. Zde je nutné definovat, kdo se o problému dozví, kdy se o něm dozví, a také jak se o problému dozví. Nabízí se možnost řešení problémů eskalovat. Pokud nedojde k vyřešení problému do určité doby, systém oznámí stav další osobě.

Kdo bude dohlížet na to, že data jsou relevantní?

Poslední bodem je relevantnost dat celého systému. Pokud data v něm nebudou správná a monitoring bude informovat o falešných událostech, stává se z nápomocného systému, systém zcela postrádající smysl.

8.2 Význam nástroje Zabbix

Smyslem monitorovacího nástroje Zabbix je sbírat data ze sítě a na základě definovaných spouštěčů vyhodnotit, zda se jedná o problém, či nikoliv. Pokud dojde ke kladnému vyhodnocení limitní podmínky, tak má na starost vyvolat konkrétní akci, která vede k informování zodpovědné osoby (alert) za dané zařízení a následně odstranění problému. Na rozdíl od sledování sítě lidským činitelem může systém fungovat nepřetržitě. Stěžejním aspektem, který rozhoduje o funkčním monitorování sítě je jeho nastavení. Pokud systém bude fungovat správně, odrazí se to i na vyšší kvalitě poskytované služby. *Obrázek 22* popisuje proces sledování sítě, který se skládá ze 4 základních kroků, které budou v následujících jednotlivých kapitolách podrobně rozebrány. [29]



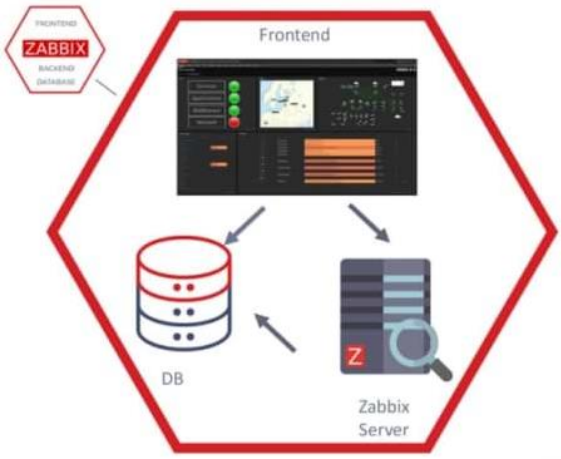
Obrázek 22 Proces monitorování infrastruktury [26]

8.3 Instalace nástroje

Pro instalaci nástroje je nutné mít hardware, který plní minimální systémové požadavky. Tyto požadavky jsou úměrné tomu, jak velkou síť je cílem monitorovat. V tomto případě se jedná o infrastrukturu, do níž může být připojeno až 300 zařízení. S tím faktem, že je nutné nechat i možnou rezervu pro budoucí rozvoj. Samotné požadavky lze dělit na požadavky na hardware a software. [29]

Minimální požadavky na hardware jsou 128 MB operační paměti a minimálně prostor pro 256 MB na paměťovém disku. Také záleží na tom, jak daleko do historie, je důležité data ukládat. Dalším faktorem je rozhodnutí, zda bude Zabbix provozován na fyzickém stroji, či na virtuálním stroji, který je nepřetržitě provozován na serveru.

V případě této práce byl využit hardware s následujícími vlastnostmi RAM 8 GB, 4 CPU a 40 GB paměti na disku. Samotný systém bude provozován na virtuálním stroji, z důvodu dostupnosti a lepšího řízení. Pro fungování monitorovacího systému je nutné mít instalováno několik komponentů (databáze, webové rozhraní a Zabbix server). Komponenty můžou být v provozu na jednom, či různých zařízeních. [29]



Obrázek 23 Komponenty monitorovacího systému Zabbix [14]

8.3.1 Průběh instalace

Samotný proces instalace zde bude shrnut do tři bodů na základě zkušenosti z implementace. Podrobnější rozpis postupu lze najít na stránkách *www.zabbix.com*. Při instalaci je rozhodující, na jakou platformu se systém instaluje, na základě toho jsou modifikovany příkazy. V tomto případě se jednalo o operační systém CentOS 7. V neposlední řadě, také záleží na způsobu instalace. Systém lze stáhnout již v podobě hotového operačního systému tzv. appliance, kde není nutné instalovat zvlášť všechny tři komponenty. Také lze využít kontejnery, které si lze představit jako předinstalované baličky, které je nutné pouze spustit. Pro možnost definovat

vlastní parametry monitorovacího nástroje byla každá komponenta nainstalovaná zvlášť na jednom zařízení.

Komponenta	Druh softwaru
Zabbix	Verze 5.0 LTS
Webový server	Apache
Databáze	MySQL

Tabulka 9 Popis instalovaných komponent [autor]

Pro možné spuštění monitorovacího nástroje je nutné, aby všechny tři komponenty byly správně nainstalovány. Samotné spuštění Zabbixu lze provést příkazem na platformě CentOS7:

```
# sudo systemctl enable zabbix-server
```

A ke kontrole stavu monitorovacího systému lze využít tento příkaz:

```
# sudo service zabbix-server status
```

Pokud výpis z příkazu neindikuje žádnou chybu, lze monitorovací systém začít využívat. Pokud došlo k chybě, je nutné se podívat do logů dané komponenty a nalézt konkrétní chybu. V případě této práce došlo k překročení výpočetní paměti. K vyřešení bylo nutné navýšit základní parametr *CacheSize*.

```
/etc/zabbix/zabbix_server.conf
### Option: CacheSize
#       Size of configuration cache, in bytes.
#       Shared memory size for storing host, item and trigger data.
#
# Mandatory: no
# Range: 128K-64G
# Default:
CacheSize=64M
```

Obrázek 24 Úprava konfigurace z důvodu navýšení paměti [autor]

8.4 Prvotní nastavení nástroje

Prvotní nastavení bylo provedeno na základě doporučení z knihy: *Zabbix: Enterprise Network Monitoring Made Easy* [29]. Základním a nejdůležitějším krokem je změna předefinovaných přístupových údajů. Pokud by nedošlo k jejich změnění, mohlo by dojít k přístupu neoprávněné osoby k datům.

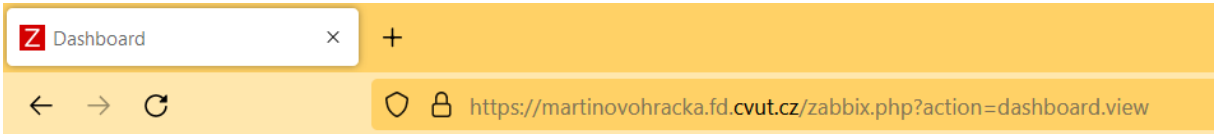
Běžně se přistupuje na webové rozhraní monitorovacího systému pomocí IP adresy. V situacích, kdy systém používá více lidí může být vhodnější využít doménové jméno. K jeho

využívání je nejdříve nutné vlastnit doménu. Následně dojde k naparování IP adresy na dané doménové jméno.

Posledním prvotním nastavením, které je doporučeno provést je zabezpečení dat přenášených mezi webovým rozhraním a Zabbix serverem. V základním nastavení tato komunikace probíhá v nešifrované podobě (tzv. plaintext). Pro nastavení je nutné implementovat protokol SSL (secure sockets layer), který představuje vloženou vrstvu mezi transportní a aplikační vrstvy, která zajišťuje šifrování komunikace. Pro generování certifikátů lze využít volně dostupné nástroje. V tomto případě byl využit nástroj Certbot (*https://certbot.eff.org/*). Postup instalace opět záleží na operačním systému, kde je provozován Zabbix-server. V tomto případě se jedná o systém CentOS 7 a pro instalaci, byl využít následující příkaz. [37]

```
# sudo certbot --nginx
```

Po instalaci je možný již pouze zabezpečený přístup přes protokol HTTPS.



Obrázek 25 Ukázka indikace komunikace přes protokol HTTPS [autor]

8.5 Definice jmenné konvence

Před dalšími kroky je vhodné se zaměřit na revizi, či vytvoření systému názvů pro zařízení. Pro definování jmenné konvence neexistuje jednoznačný postup, protože každá organizace může mít jiné uspořádání a požadavky na identifikaci. Na druhou stranu existuje několik doporučení, která se v praxi uplatňují. Zásadním doporučením je, že každý název vede k unikátnímu zařízení a při jeho interpretaci lze zařízení lokalizovat. V rámci této práce byla definovaná následující jmenná konvence ve dvou typech dle zařízení. [29]

TYP SÍŤOVÉHO PRVKU.VRSTVA ZAŘÍZENÍ.BUDOVA.PODLAŽÍ.POŘADOVÉ ČÍSLO.ČÍSLO MÍSTOSTI
SW.A.B1.1NP.01.100

Tabulka 10 Příklad jmenné konvence pro síťové prvky [autor]

BUDOVA.ČÍSLO MÍSTNOSTI.TYP ZAŘÍZENÍ POŘADOVÉ ČÍSLO
B1.10.1.PC1

Tabulka 11 Příklad jmenné konvence pro ostatní zařízení [autor]

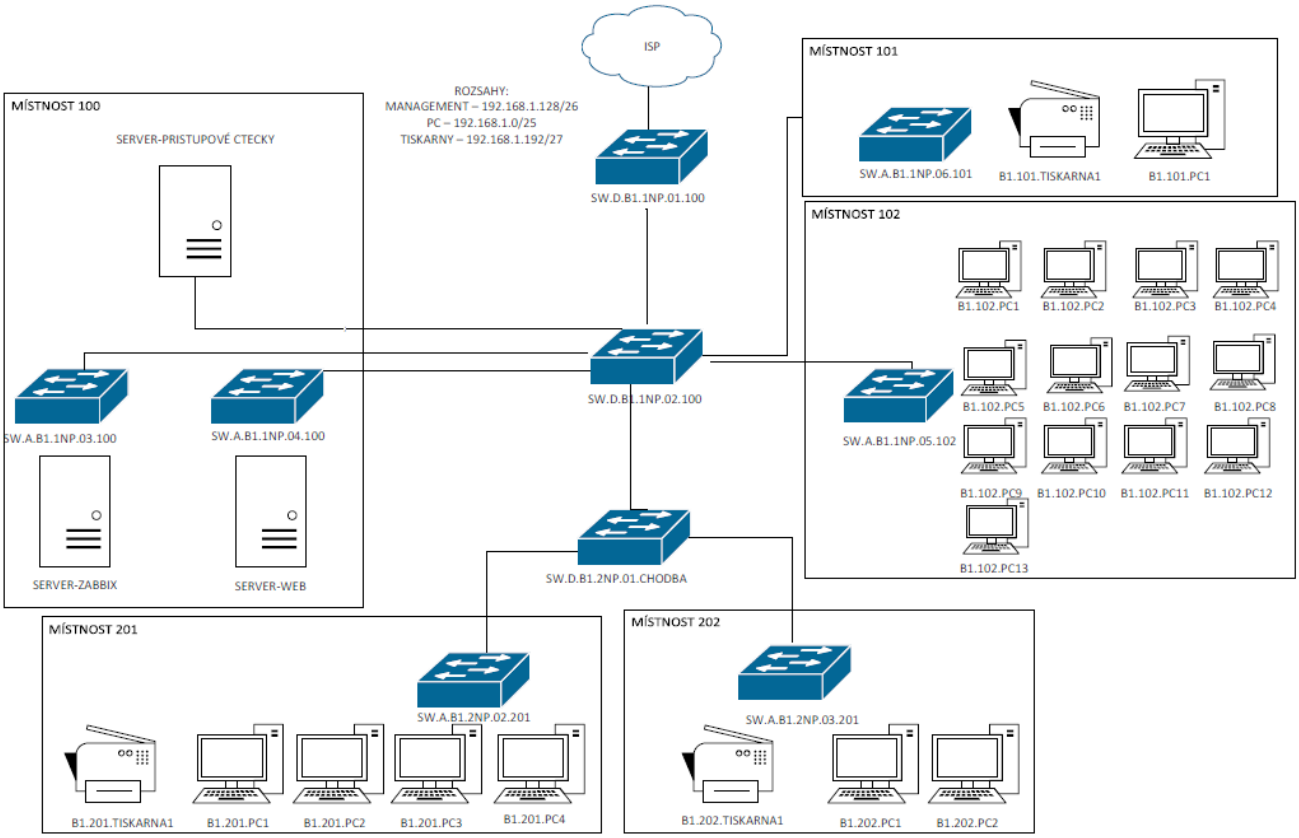
8.6 Definování sledovaných zařízení

Pro funkční implementaci monitorovacího systému je nezbytné pochopit provázanost mezi zařízeními sledované infrastruktury, buď na základě logické, či fyzické topologie. Vedle toho mít představu, zda bude nutné sledovat všechna zařízení na testované infrastruktuře, či jen některá. Každé sledované zařízení přináší určité náklady, ať z pohledu propustnosti sítě, tak i určitého výpočetního výkonu na straně monitorovacího serveru a databáze. V rámci této práce došlo k definici testovací topologie, která obsahuje různá zařízení tak, aby byla možnost prokázat funkčnost monitorovacího systému na heterogenním prostředí, které se skládá ze zařízení různých výrobců a typů. Pokud dochází k monitorování sítě, ve které neexistuje topologie, tak je vhodné ji vytvořit. U menších sítí může postačit příkaz *show cdp neighbors*, který vypíše sousední síťové prvky.

```
K4           #show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

                 Gig 1/0/          122              S I   WS-C2950T Gig 0/2
SEPFCFBFB109831  Gig 1/0/          137            H P M   IP Phone  Port 1

                 Gig 1/0/          150              S I   WS-C2960C Gig 0/10

                 Gig 1/0/          178            R S I   WS-C2960X Gig 1/0/35

                 Gig 1/0/          138              S I   WS-C2960C Gig 0/10

Total cdp entries displayed : 5
```

Obrázek 26 Výpis příkazu na show cdp neighbors [autor]

U rozsáhlejších síti může být tento proces značně zdlouhavý. Z tohoto důvodu existují nástroje, které při zadání přístupových údajů k síťovým prvkům umožňují automatické vygenerování topologie. Avšak většina těchto nástrojů je placená a poskytují své služby až pro velké korporátní sítě tzv. enterprise. Příkladem těchto nástrojů je IP Fabric, či Cisco DNA. Jediné bezplatné nástroje, které umožňují vygenerování topologie infrastruktury a byly v rámci této práce nalezeny je NeDI a Cisco Network Assistant. Práce s těmito nástroji je náročnější a výsledky kvalitou nelze srovnávat s placenými nástroji.



Obrázek 27 Topologie testované sítě [autor]

8.7 Přidání zařízení do monitorovacího systému

Následující podkapitola popisuje postup pro přidání zařízení do systému Zabbix. Poukazuje na význam rozdělení zařízení do skupin a lze v ní najít ukázku centrálního řízení na základě využití globálních politik. Obsah této podkapitoly vychází z konzultací a předchozích zkušeností autora.

8.7.1 Vytvoření vlastních skupin zařízení

Před samotným přidáním zařízení je vhodné si vytvořit vlastní skupiny zařízení. Výhodou tohoto přístupu je budoucí lepší škálovatelnost a delegace relevantních informací ke konkrétním subjektům. V tomto případě bylo vytvořeno 5 skupin na základě testovací infrastruktury (*Obrázek 27*). Zařízení byla zařazena do skupin na základě rozdílných požadavků na sledování kvality služby.

Název skupiny
Skupina_síťové prvky = obsahuje síťové prvky
Skupina_tiskárny = obsahuje pouze tiskárny a skenery

Skupina_koncové stanice = obsahuje koncové stanice v kancelářích
Skupina_PC_mistnost = obsahuje koncové stanice z PC místností
Skupina_servery = obsahuje servery, na kterých běží důležité aplikace

Tabulka 12 Vlastní skupiny pro monitorovací systém [autor]

8.7.2 Postup při přidání zařízení sledované pomocí protokolu

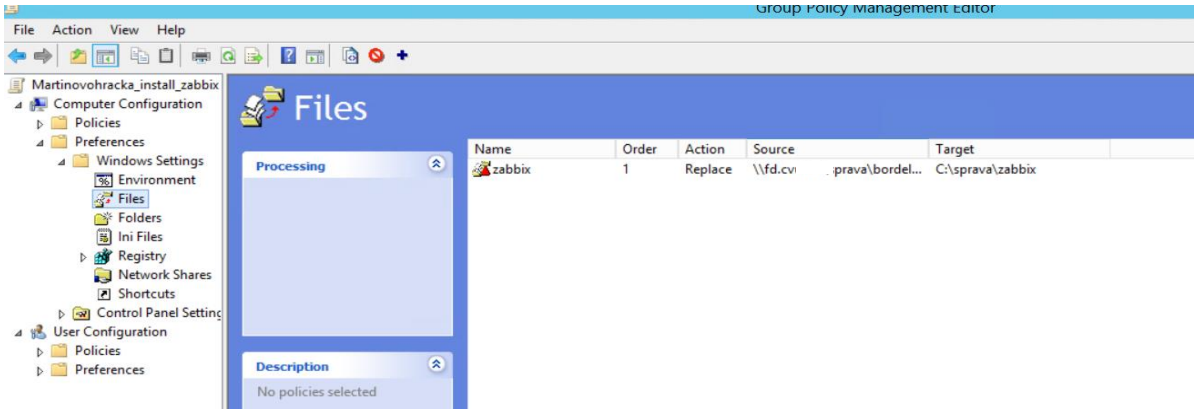
Samotné přidání zařízení do monitorovacího systému může probíhat dvěma cestami, manuálně, či automaticky. Pokud se přidá zařízení manuálně, je nutné vyplnit parametry, jako je název, skupina a adresa rozhraní, z kterého bude probíhat vyčítání dat. Pro vyčítání dat je možné využít několik způsobů. Buď přes protokoly, které umožňují vyčítání dat (*viz Kapitola 3*) nebo pomocí agenta konkrétního monitorovacího systému. Výhodou vyčítání pomocí protokolů (pasivní monitoring) je jednoduší připojení k monitorovacímu systému. Není zde nutné nic instalovat, postačí pouze nakonfigurovat síťový prvek (např. SNMP komunitu u protokolu SNMP). Nevýhodou je však možnost vyčítat méně dat a více omezení, než u aktivního monitoringu. Ne všichni výrobci podporují všechny protokoly. Zde je potřeba brát v úvahu konkrétní verzi operačního systému, i zde se může lišit podpora daných funkcionalit.

Příkaz pro konfiguraci SNMP komunity na zařízení Cisco, která umožňuje pouze čtení dat:

```
# snmp-server community public RO
```

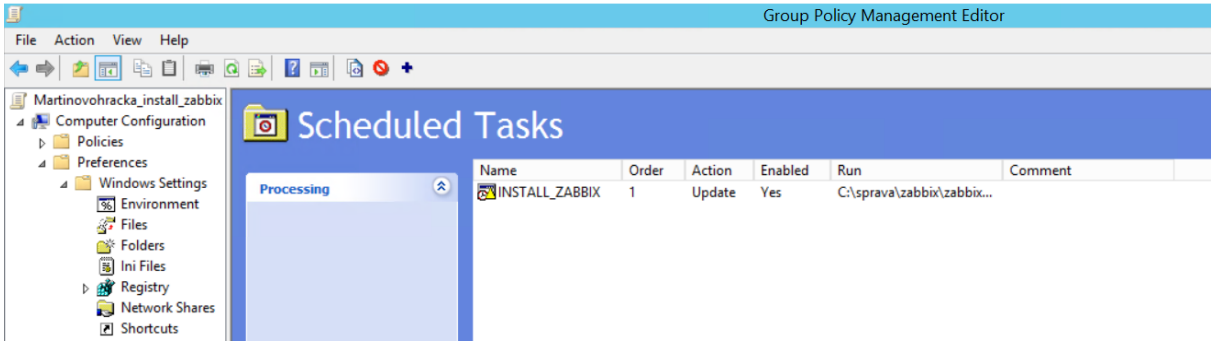
8.7.3 Postup při přidání zařízení sledované pomocí agenta

V případě vyčítání dat pomocí agenta je přínosem větší množství vyčítaných dat a podpora aktivního monitoringu, kdy aktivní síťový prvek zahlásí událost v případě problému. Na druhou stranu je potřeba na zařízení v infrastruktuře instalovat další software, který zabírá paměť a vytěžuje procesor. Nicméně se jedná o soubor o velikosti 10 MB. A při optimalizaci intervalů zasílání dat lze tyto datové náklady ještě snížit. Druhým negativním jevem může být nutnost distribuce agenta na zařízení. Avšak i na tento problém existují řešení v podobě implementace agenta do základní instalace operačního systému, či následné distribuce a instalace softwaru pomocí globálních politik. Zde je nutná predispozice, mít zařízení v jedné doméně s možností úprav. Pro potřeby této práce byla zvolená instalace s pomocí globální politiky doménové služby Active directory. Samotná distribuce spočívala v nakopírování instalačního balíčku Zabbix agenta na všechny cílové koncové stanice do složky Zabbix. Tento agent je volně dostupný na stránkách *www.zabbix.com.*



Obrázek 28 Nakopírování instalátoru Zabbix agent pomocí GPO [autor]

Po nakopírování instalátoru je nutné naplánovat událost, která pomocí skriptu spustí instalaci Zabbix agenta a přiřadí mu základní parametry, jako je adresa Zabbix serveru.



Obrázek 29 Vytvořená událost pro spuštění instalačního souboru [autor]

Script zabbix_install.bat

```
cd c:\sprava\zabbix

msiexec /l*v log.txt /i zabbix.msi /qn^

 LOGTYPE=file^

 LOGFILE="%INSTALLFOLDER%\za.log"^

 SERVER=*IP adresa Zabbix serveru*^

 SERVERACTIVE=*IP adresa Zabbix serveru*
```

Pro dokončení přidání zařízení do monitorovacího systému je vhodné si vytvořit akci pro zařízení monitorované pomocí protokolů (*Configuration* > *Actions* > *možnost Discovery actions*). Zde je možné nadefinovat podmínky na základě, kterých se automaticky přiřadí do dané skupiny (např. adresní rozsah, či přítomností konkrétní služby) a zároveň na sebe naváže konkrétní šablonu (template), která obsahuje seznam MIB. Tyto MIB lze vyčítat z konkrétních zařízení.

Name ▲	Conditions	Operations
akce_skupina_tiskárny	Host IP equals [redacted]	**Add to host groups:** Skupina_Tiskárny **Link to templates:** Printer Xerox WorkCentre 7855

Obrázek 30 Discovery action pro tiskárny [autor]

V případě, kdy na zařízeních na infrastruktuře je instalovaný agent s předefinovanou adresou Zabbix serveru, jeho přidání k Zabbix serveru probíhá následujícím způsobem:

Configuration > Actions > možnost Autoregistration actions

Zde je podmínka definovaná na základě jména koncové stanice, která odpovídá konkrétní PC místnosti.

Name ▲	Conditions	Operations
Auto_registrace_učebna	Host name cont	**Add to host groups:** Skupina_PC_ucebna **Link to templates:** Template OS Windows by Zabbix agent, Template OS Windows by Zabbix agent active

Obrázek 31 Ukázka auto registrace Zabbix agenta [autor]

Úspěšně přidané zařízení tzv. hosty lze nalézt v sekci *Monitoring* > *Hosts*. Pokud dochází k neúspěšné komunikaci s agentem, je zde na místě zkontrolovat odchozí a příchozí pravidla ve firewallu. Ověření skutečnosti, že jsou porty otevřené a provoz může procházet mezi odesílatelem a příjemcem lze ověřit pomocí nástroje NMAP. Tento nástroj umožňuje skenování portů na konkrétním zařízení, či na zařízeních vyskytujících se na celém rozsahu.

```
[root@darkstar ~]#
[root@darkstar ~]# nmap -PN sS -O Scanme.Nmap.Org

Starting Nmap 5.21 ( http://nmap.org ) at 2010-04-01 11:19 IDT
Nmap scan report for Scanme.Nmap.Org (64.13.134.52)
Host is up (0.18s latency).
rDNS record for 64.13.134.52: scanme.nmap.org
Not shown: 993 filtered ports
PORT      STATE  SERVICE
25/tcp    closed smtp
53/tcp    open   domain
70/tcp    closed gopher
80/tcp    open   http
113/tcp   closed auth
8009/tcp  open   ajp13
31337/tcp closed Elite
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.15 - 2.6.26

OS detection performed. Please report any incorrect results at http://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 16.99 seconds
[root@darkstar ~]#
```

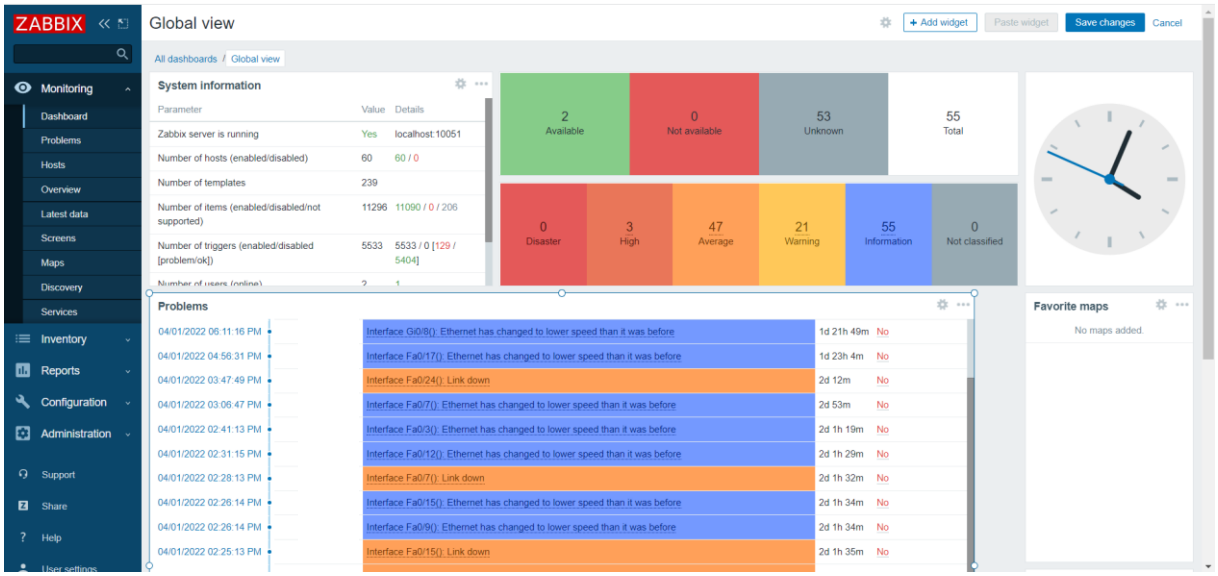
Obrázek 32 Ukázka nástroje NMAP [28]

9. Využití naměřených dat v rámci vlastní implementace monitoringu infrastruktury

Tato kapitola pokračuje ve vlastní implementaci monitorovacího nástroje Zabbix. Avšak na základě sebraných dat z testovací infrastruktury uzpůsobuje chování nástroje potřebám testovací organizace. Převládající funkce této organizace je administrativní s tím že poskytuje i několik aplikací vnějším subjektům. Pokud by se monitoring implementoval například v organizaci, kde je hlavní funkcí prodej nebo výroba, tak by nastavení plnilo jiné požadavky. Tudíž kroky pro implementaci systému jsou univerzální, nicméně nastavení jednotlivých částí systému je již plně závislé na aktuálním prostředí, které je nutné znát. Podkladem k této kapitole byla konzultace s osobou zabývající se implementací monitorovacích systému a osobou, která je součástí testovací organizace.

9.1 Definice sledovaných parametrů

Pro zjištění všech možností, co monitorovací systém Zabbix nabízí je vhodné pro začátek vybrat základní šablony, které jsou součástí systému. Tyto šablony obsahují sledované položky (*Items*) a spouštěče (*Triggers*). Liší se v závislosti na výrobci i typu zařízení. Pokud se ponechá výchozí nastavení, může po 24 hodinách vypadat základní obrazovka Zabbixu, která informuje o problémech vypadat jako *Obrázek 33*.



Obrázek 33 Základní obrazovka systému Zabbix [autor]

V tomto stavu je monitorovací systém nepoužitelný. Osoba spravující síť nemá možnost rozeznat důležité problémy a po chvíli přestane věnovat monitorovacímu systému pozornost, protože data jsou pro její potřeby naprosto nerelevantní a systém pro monitoring sítě ztrácí zcela smysl. Při definování parametrů je důležité mít na paměti, proč dané parametry je třeba sledovat. Hlavním smyslem lokální datové infrastruktury je přenášet spolehlivě data, a proto je

nutné sledovat parametry, které mohou napovídat tomu, že dané zařízení se brzy dostane do poruchového stavu, či na něm bude docházet ke zpoždění. V *kapitole 5* byly vybrány dva nejdůležitější přístupy pro řízení lokální datové sítě performance management (řízení výkonu) a fault management (řízení chyb).

performance management	fault management
zatížení procesoru (CPU)	teplota zařízení
využití operační paměti (RAM)	napájení zařízení
zatížení síťových rozhraní	dostupnost zařízení

Tabulka 13 Ukázka možných hlídaných parametrů [autor]

Tabulka 13 představuje ukázku parametrů, které lze sledovat na zařízeních. Pokud dojde například k vysokému zatížení procesoru u zařízení, může dojít k zahazování paketů u síťového prvku, či ke zpomalení procesů v případě stolního počítače. Podobné vlastnosti platí i u operační paměti (RAM), kde nedostatek místa může způsobit nemožnost aktivovat další proces, a to může vést až k restartování zařízení. Pokud se detekuje vysoké přenosové zpoždění, tak při přenosech dat to nemusí být pro uživatele omezující, avšak pokud jde o přenos zvuku, či videa může dojít k výpadkům komunikace (více *kapitola 2*). Parametry ovlivňující výkon zařízení lze zařadit do problematiky řízení výkonu.

Hodnoty parametrů ze skupiny řízení chyb popisují stav hlavních komponent zařízení, které mají podíl na provozu zařízení, pokud dojde k detekci nestandartních hodnot těchto veličin. Pro ilustraci lze uvést příklad větrání zařízení. V situaci, kdy vyčtené hodnoty informují o nestandartním chování, lze predikovat budoucí výpadek celého zařízení z důvodu jeho přehřátí. Tyto parametry se mohou lišit na základě jednotlivých zařízení. Pro optimální nastavení bude definovaná tabulka parametrů pro každou skupinu zařízení zvlášť.

Skupina síťové prvky

Nejstěžejnější zařízení, na kterých závisí funkčnost komunikace uvnitř lokální datové sítě, jsou právě síťové prvky. Na základě topologie testovací sítě se zde nalézá pouze přístupová a distribuční vrstva (*kapitola 8.7*). Vyšší vrstva tzv. páteřní je poskytovaná jiným subjektem.

Distribuční prvky poskytují datovou konektivitu prvkům přístupovým. Na základě topologie je vidět, že distribuční prvek SW.A.B1.1NP.01.100 je hraničním uzlem testovací infrastruktury. Tudíž přehled provozu na vstupním a výstupním rozhraní tohoto prvku jasně popisuje aktuální stav mezi LAN a WAN. Zde je důležitý aspekt právě hierarchie, kde nefunkční hraniční prvek omezuje funkčnost celé vnitřní infrastruktury. Proto je zásadní správně odhadnout standartní chování vnitřní sítě na základě zkoumání předchozího chování. Tuto problematiku lze konkrétněji popsat pomocí datových toků na hraničním prvku. Pokud by docházelo k nestandartním datovému provozu (větší, či menší datové přenosy) mohlo by to nasvědčovat možnému bezpečnostnímu incidentu, či problému na straně poskytovatele sítě. Na druhou

stranu to může také značit, že v testované síti dochází k podivnému chování např. uživatel distribuuje zakázaný obsah, nebo je problém na samotné infrastruktuře.

performance management	parametr	jednotky
CPU	zatížení procesoru	[%]
RAM	využití operační paměti	[%]
fyzická paměť	využití paměti	[%]
propustnost rozhraní	odeslaná data	[Mb/s]
propustnost rozhraní	přijatá data	[Mb/s]
propustnost rozhraní	využití šířky pásma	[%]
fault management		
teplota	stav větráku	[1-6]
napájení	stav napájení	[1-6]
dostupnost zařízení	ICMP ping	up (1) down (0)
kvalita datového přenosu	čas odpovědi ICMP	[ms]

Tabulka 14 Parametry pro skupinu síťové prvky [autor]

Skupina koncová zařízení

Do této skupiny spadají všechna koncová zařízení, která jsou využívána v kancelářích. Může se jednat o stolní počítač, či přenosný laptop. Tato zařízení využívají jako svůj pracovní nástroj zaměstnanci konkrétní organizace, proto je tedy nutné zaručit jejich funkci a zároveň dohlížet na to, že jejich funkce dosahuje své kvality. Konkrétněji, že koncová stanice splňuje požadavky uživatele jako je například hladká odezva systému.

performance management	parametr	jednotky
CPU	zatížení procesoru	[%]
RAM	využití operační pamětí	[%]
fyzická paměť	využití paměti	[%]
zabezpečení	stav služby antiviru	stopped (6) running (0)
tisk	stav služby tiskových front	stopped (6) running (0)
sdílené disky	stav služby sdílených disků	stopped (6) running (0)
aktualizace	stav služby aktualizací	stopped (6) running (0)
fault management		
dostupnost zařízení	ICMP ping	up (1) down (0)

Tabulka 15 Parametry pro skupinu koncová zařízení [autor]

Skupina PC místnost

Na první pohled by se mohlo zdát logičtější dát zařízení v počítačové místnosti do stejné skupiny, jako jsou zařízení v kancelářích. Nicméně je zde několik aspektů, které tyto zařízení odlišují. Za prvé: osoba, která spravuje počítačové učebny může být jiná než osoba spravující zařízení v kancelářích. A druhým rozdílem je také to, že zařízení v počítačových místnostech mohou být volně dostupná, a tedy uživatelé nemusí být pouze zaměstnanci, či studenti ve škole, ale i další návštěvníci, pokud se například jedná o knihovnu nebo školící místnost.

performance management	parametr	jednotky
CPU	zatížení procesoru	[%]
RAM	využití operační pamětí	[%]
fyzická paměť	využití paměti	[%]
zabezpečení	stav služby antiviru	stopped (6) running (0)
aktualizace	stav služby aktualizací	stopped (6) running (0)

správa zařízení	stav služby úlohy	stopped (6) running (0)
fault management		
dostupnost zařízení	ICMP ping	up (1) down (0)

Tabulka 16 Parametry pro skupinu PC místnost [autor]

Skupina servery

Zařízení v této skupině se liší tím, že jsou v provozu nepřetržitě a zároveň jsou na nich provozovány důležité interní aplikace. Může jít o hostování webových stránek, či provoz interních databází. Často se může jednat o virtualizační platformy, u kterých je možné sledovat i jiné parametry, jako je například kompatibilita verzí, a též mohou mít jiného správce.

performance management	parametr	jednotky
CPU	zatížení procesoru	[%]
RAM	využití operační paměti	[%]
fyzická paměť	využití paměti	[%]
propustnost rozhraní	odeslaná data	[Mb/s]
propustnost rozhraní	přijatá data	[Mb/s]
propustnost rozhraní	využití šířky pásma	[%]
fault management		
dostupnost zařízení	ICMP ping	up (1) down (0)
kvalita datového přenosu	čas odpovědi ICMP	[ms]

Tabulka 17 Parametry pro skupinu servery [autor]

Skupina tiskárny

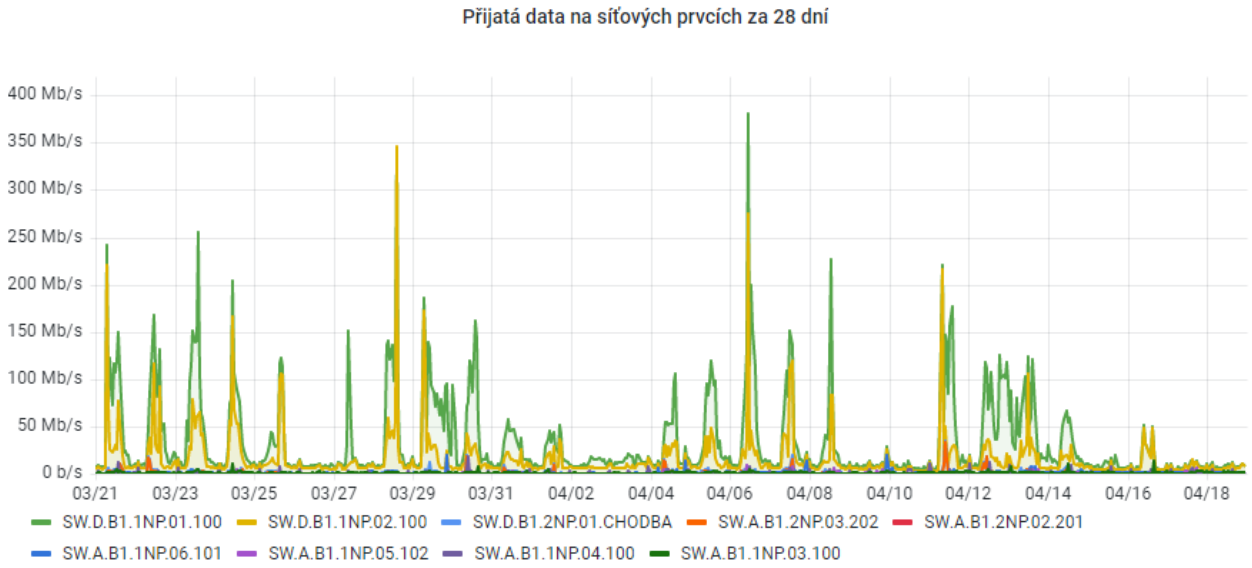
Tiskárny se nemusejí zdát jako prvek, který je nutný sledovat. Opak je pravdou, tiskárny i kopírky jsou vedle koncových stanic dalším důležitým nástrojem. Pomocí těchto zařízení mohou uživatelé plnit svou agendu. A na rozdíl od ostatních zařízení jsou závislé na spotřebním materiálu, který je nutné doplňovat.

fault management	parametr	jednotky
dostupnost zařízení	ICMP ping	up (1) down (0)
spotřební materiál	Stav materiálu	[%]

Tabulka 18 Parametry pro skupinu tiskárny [autor]

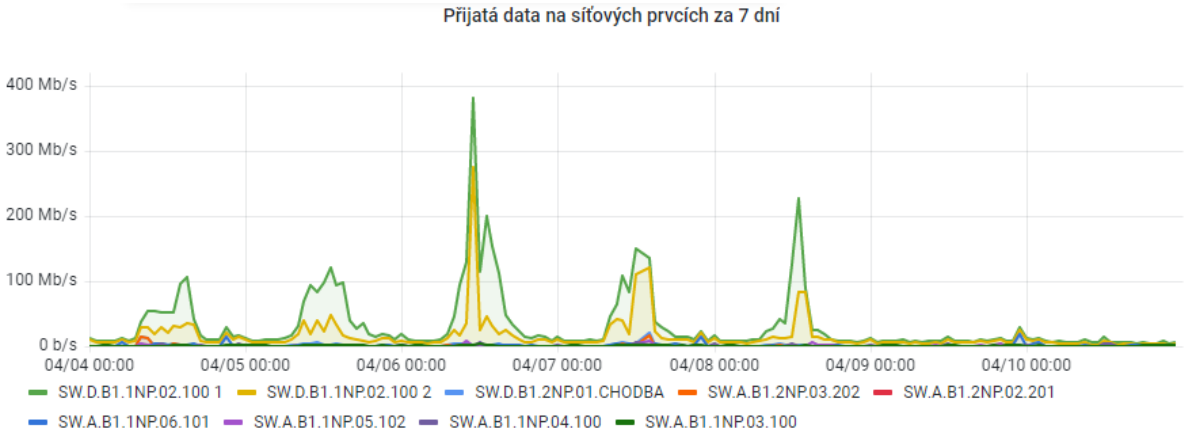
9.2 Sběr dat v testovací infrastruktuře

Pro správné nastavení monitorovacího nástroje je nutné sebrat data z testovací infrastruktury. Každá infrastruktura má rozdílné chování. Některá je zatížená nepřetržitě a jiná zase pouze přes den během všedních dnů. A i samotné pozorování distribuce provozu po síti slouží jako podklad k definování správných hraničních hodnot u vybraných parametrů, tak i pro určení odpovídající úrovně nalezeného problému.



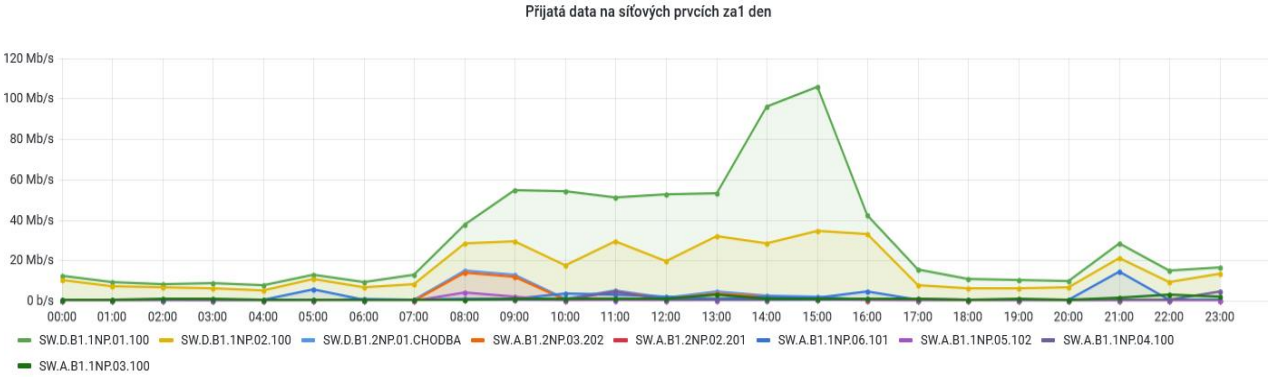
Graf 1 Průběh přijatých datových toků na síťových prvcích za dobu 28 dní [autor]

Na *Graf 1* lze vidět průběh přijatých datových toků během vybraných 4 pracovních týdnů. Přijatý provoz je generován na základě činnosti uživatelů v organizaci. Nejvíce přijatého provozu přechází přes síťové prvky SW.D.B1.1NP.01.100 a SW.D.B1.1NP.02.100. Tento výsledek potvrzuje fakt, že tyto dva prvky jsou součástí distribuční vrstvy. Při bližším pohledu na data lze vyčíst časové rozložení mezi pracovním týdnem a víkendem, kdy provozní zatížení síťových prvků je zcela rozdílné. Nicméně pouze stanovení limitních prvků na základě pracovních dnů a dnů volna je stále nevypovídající. Proto je možné se zaměřit na provoz i z hlediska denní doby. Pro lepší prezentaci byl vybrán právě jeden referenční týden od pondělí 4. dubna do neděle 10. dubna.



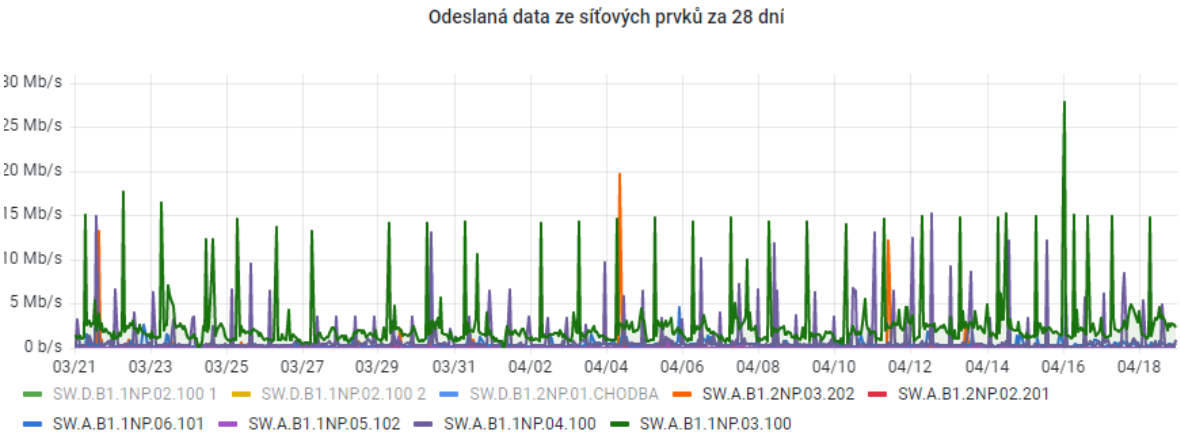
Graf 2 Průběh přijatých datových toků na síťových prvcích za dobu 7 dní [autor]

Graf 2 dokazuje, že generovaný přijatý provoz vzniká hlavně během pracovní doby. Ale na druhou stranu je dobré si uvědomit, že ani provoz během dnů klidu není nulový.



Graf 3 Průběh přijatých datový toků na síťových prvcích za dobu 7 dní [autor] [autor]

Graf 3 ukazuje pozvolný nárůst provozu od sedmé ráno a jeho útlum kolem páté hodiny odpolední. Největší zatížení lokální datové infrastruktury je od 8 do 16 hodin. Tyto informace mohou být také vhodné pro plánování odstávek, či mohou sloužit jako podklad dat pro management.



Graf 4 Odchozí datový tok ze síťových prvků přístupové vrstvy za 28 dní [autor]

Největší provoz na přístupové vrstvě vzniká na prvcích SW.A.B1.1NP.03.100 a SW.A.B1.1NP.04.100 (*Graf 4*). Tento výsledek je dán tím, že na ty to prvky jsou napojené servery, na kterých běží například webové stránky organizace a interní aplikace. U vzniklého provozu je zajímavý jeho časový průběh, který je rozptýlen během celého dne, na rozdíl od provozu, který je generován koncovými stanicemi. Důležitou informací je 4násobný nárůst provozu okolo sedmé hodiny ranní. Příčina tohoto provozu může být pravděpodobně způsobena pravidelnou synchronizací databází.

Analýza naměřených dat posloužila jako vstup pro definování standartního chování uvnitř testovací organizace v určitých časových obdobích. Tato časová období byla rozdělena na tři kategorie:

- Nízké využití – období od pátku 16:00 do neděle 23:59 - Vn
- Střední využití – období od pondělí do čtvrtka mezi 16:00 – 8:00 - Vs
- Vysoké využití – období od pondělí do pátka mezi 8:00 – 16:00 hodinou – Vv
  *státní svátky se řadí do kategorie nízké využití

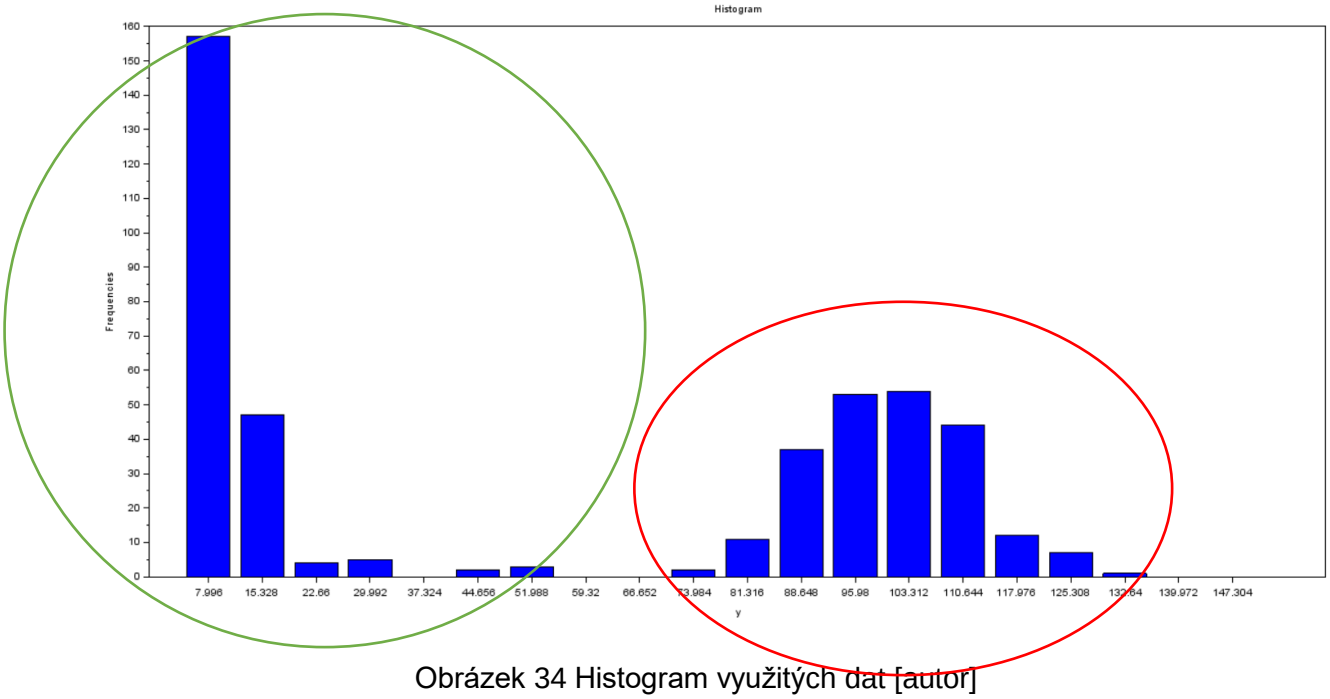
9.3 Určení hranic standardního a nestandardního chování na základě shlukování

Následující část se zabývá definování limitních hodnot pro datové toky. Na základě hodnot přijatých a odchozích datových toků lze rozpoznat nestandardní chování způsobené bezpečnostním incidentem, či vadou zařízení na infrastruktuře. Z naměřených dat byl vybrán datový soubor obsahující hodnoty datových toků z testovací infrastruktury za 28 dní. Během těchto dní nedošlo k žádnému nestandartnímu chování, a tedy po vyčištění dat bylo rozpoznáno standartní chování. Nasbíraná data představují data spojitá a jejich rozdělení odpovídá Poissonovu rozdělení pravděpodobností. Toto rozdělení obsahuje proměnné s následujícími vlastnostmi:

- nezávislost parametrů na předchozích a budoucích stavech
- v rámci krátkého časového období je hodnota konstantní (v tomto případě rovna frekvenci vyčítání)
- absence možné situace, při které nastanou dva stavy současně [45]

Pro možnou klasifikaci stavů bylo na základě konzultací, porovnávání způsobu modelování a rozložení dat vybrán přístup, který využívá model směsí Poissonových komponent v kontextu shlukové analýzy. Pomocí tohoto přístupu lze nalézt střední hodnoty a rozptyly jednotlivých shluků. Výsledné hodnoty jsou zásadní pro zvolení vhodných optimálních hodnot pro konkrétní zařízení při daném zatížení. [8]

Pro ukázku postupu byl vybrán distribuční síťový prvek SW.D.B1.1NP.NA.100 a jeho příchozí provoz při nízké zátěži (pátek od 16:00 do neděle do 23:59). Po vykreslení histogramu (*Obrázek 34*), lze vidět četnosti dat pro dané intervaly hodnot. První shluk (zelený) označuje standardní chování a druhý shluk (červený) označuje chování nestandardní. Nestandardní chování nebylo možné vytvořit v testovací síti, protože síť musela stále plnit svou funkci. Proto byly pro shlukovou analýzu vygenerovány data taktéž z Poissonova rozdělení na základě maximálních hodnot standartního chování. Tato data prezentují nestandardní příchozí datové toky na vstupním rozhraní definovaného síťového prvku.



Obrázek 34 Histogram využitých dat [autor]

Po využití programu (viz *Přílohy*) pro modelování a klastrování Poissonových komponent je nejdůležitější hodnota LaE (λ), která představuje odhad parametru modelu pro vybranou komponentu. Na základě charakteristik Poissonova rozdělení platí:

Střední hodnota Poissonova rozdělení je: [45]

$$E(X) = \lambda$$

Rozptyl Poissonova rozdělení je: [45]

$$D(X) = \lambda$$

Výsledkem je tedy, že střední hodnota příchozích dat je 9,99 Mbit/s. Tyto data reprezentují standardní chování zařízení SW.D.B1.1NP.NA.100 během nízké zátěže. A pro nestandardní chování je střední hodnota 98,66 Mbit/s. Horní hranice shluku pro standardní chování je 19,98 Mbit/s. O nestandardní chování se tedy jedná, pokud naměřená data překročí vypočtenou horní hranici shluku. Výsledky byly zaokrouhleny na celá čísla, tato forma je vhodnější pro nastavení monitorovacího nástroje.

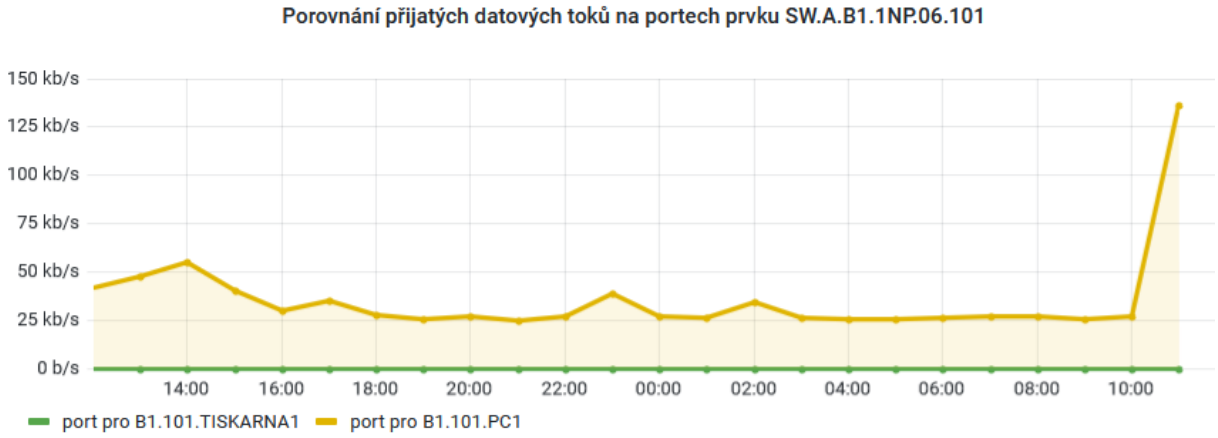
PŘIJATÝ PROVOZ	SW.D.B1.1NP.01.100	SW.D.B1.1NP.02.100	SW.D.B1.2NP.01.CHODBA
vysoká využití	150 Mbit/s	40 Mbit/s	7 Mbit/s
střední využití	5o Mbit/s	25 Mbit/s	5 Mbit/s
nízké využití	20 Mbit/s	10 Mbit/s	1 Mbit/s
ODCHOZÍ PROVOZ	SW.D.B1.1NP.01.100	SW.D.B1.1NP.02.100	SW.D.B1.2NP.01.CHODBA
vysoká využití	30 Mbit/s	15 Mbit/s	2 Mbit/s
střední využití	25 Mbit/s	10 Mbit/s	2 Mbit/s
nízké využití	20 Mbit/s	10 Mbit/s	1 Mbit/s

Tabulka 19 Limitní hodnoty pro prvky distribuční vrstvy [autor]

PŘIJATÝ PROVOZ	SW.A.B1.2NP. 03.202	SW.A.B1.2NP. 02.201	SW.A.B1.1NP. 06.101	SW.A.B1.1NP. 05.102	SW.A.B1.1NP. 04.100	SW.A.B1.1NP. 03.100
vysoká využití	7 Mbit/s	2 Mbit/s	4 Mbit/s	2 Mbit/s	3 Mbit/s	4 Mbit/s
střední využití	5 Mbit/s	1 Mbit/s	3 Mbit/s	1 Mbit/s	2 Mbit/s	2 Mbit/s
nízké využití	1 Mbit/s	1 Mbit/s	2 Mbit/s	1 Mbit/s	2 Mbit/s	2 Mbit/s
ODCHOZÍ PROVOZ	SW.A.B1.2NP. 03.202	SW.A.B1.2NP. 02.201	SW.A.B1.1NP. 06.101	SW.A.B1.1NP. 05.102	SW.A.B1.1NP. 04.100	SW.A.B1.1NP. 03.100
vysoká využití	2 Mbit/s	1 Mbit/s	2 Mbit/s	2 Mbit/s	3 Mbit/s	6 Mbit/s
střední využití	2 Mbit/s	1 Mbit/s	2 Mbit/s	1 Mbit/s	2 Mbit/s	5 Mbit/s
nízké využití	1 Mbit/s	1 Mbit/s	1 Mbit/s	1 Mbit/s	2 Mbit/s	3 Mbit/s

Tabulka 20 Limitní hodnoty pro prvky přístupové vrstvy [autor]

Definování limitních hodnot může probíhat ještě na nižší vrstvě samotných fyzických portů na síťových zařízení. Z toho důvodu, že každá skupina zařízení generuje datové toky o jiných velikostech. Pro srovnání lze porovnat datový provoz na dvou vybraných portech zařízení SW.A.B1.1NP.06.101.



Graf 5 Porovnání přijatých datových toků na portech zařízení SW.A.B1.1NP.06.101 [autor]

Graf 5 jednoznačně poukazuje na skutečnost, že koncová stanice v podobě stolního počítače má řádově jiné datové přenosy než připojená tiskárna. Nicméně tiskárny by dle doporučení pro návrh sítě měli být skryté v síti privátní, tudíž nejsou umožněna připojení z vně sítě. Na druhou stranu může dojít k technické závadě na zařízení, které následně může začít generovat velké množství provozu. Tento provoz může následně negativně ovlivnit provoz v dohledávané infrastruktuře. Proto je vhodné i tyto možné situace včas rozeznat. Pro ošetření i těchto případů bylo na základě sebraných dat určeny limitní hodnoty provozu na jednotlivých rozhraních síťových zařízeních přístupové vrstvy. Zde hodnoty jsou zaokrouhleny na jedno desetinné místo, protože hodnoty u některých skupin portů jsou velmi malé. Lze definovat i další skupiny

portů jako například skupina pro IOT zařízení a další zařízení. Nicméně, pro stanovení limitních hodnot datových toků je nutné sledovat hodnoty na základě reálného chování. V rámci této testovací infrastruktury nebyly tyto další druhy zařízení připojeny.

PŘIJATÝ PROVOZ	porty pro tiskárny	porty pro koncové stanice	porty pro servery	porty pro IP telefony
vysoká využití	150 kbit/s	2 Mbit/s	1 Mbit/s	0,1 Mbit/s
střední využití	100 kbit/s	1,5 Mbit/s	0.5 Mbit/s	0,1 Mbit/s
nízké využití	50 kbit/s	0.5 Mbit/s	0.3 Mbit/s	0,1 Mbit/s
ODCHOZÍ PROVOZ				
vysoká využití	1 Mbit/s	2.5 Mbit/s	0.5 Mbit/s	0,1 Mbit/s
střední využití	0.5 Mbit/s	1 Mbit/s	0.2 Mbit/s	0,1 Mbit/s
nízké využití	0.5 Mbit/s	0.5 Mbit/s	0.2 Mbit/s	0,1 Mbit/s

Tabulka 21 Definice limitních hodnot pro jednotlivé skupiny portů [autor]

9.4 Definování severity událostí

Z výsledků analýzy dat a pročtení produktové dokumentace, byly stanoveny hraniční hodnoty a na jejich základě bude rozhodnuto, zda se jedná o nestandartní chování (událost), které je nutné řešit. I zde nutné opět uplatnit určitou granularitu, bez ní by mohlo dojít k situaci, kdy podstatné informace se ztratí v množství informací menšího, či pouze informativní charakteru. Proto vedle hraničních hodnot byly určeny i hladiny priorit, které jsou spojeny s danou událostí. Lze zde využít označení severita události. Tyto priority mohou mít následně přímou závislost na dalších akcích v případě, že nastane anomálie ve sledované infrastruktuře. V rámci této práce bylo definováno 6 úrovní událostí.

úroveň	popis	barva
neklasifikováno	Událost, u které není definována žádná úroveň závažnosti.	
informace	Událost, která je pouze informačního charakteru, kterou je nutné brát na zřetel.	
varování	Událost, která je již varovného charakteru a mohla by mít v blízké době vážnější důsledky.	
začínající problém	Událost, která poukazuje na vzniklý problém.	
problém	Událost, která interpretuje, že nastala významná událost, která se neobejde bez zásahu.	
vážný problém	Událost katastrofického charakteru, která bez zásahu bude znamenat nefunkčnost monitorovaného systému.	

Tabulka 22 Tabulka severit událostí [autor]

Zohlednění vážnosti vzniklé události je zásadní. Bez této škálovatelnosti by smysluplnost monitorovacího nástroje byla velmi omezena. Nicméně, správné nastavení těchto úrovní je komplexní proces kdy musí být zohledněny potřeby konkrétního prostředí. Nejčastěji se tyto hodnoty určují na základě možných důsledků. Proto je zde vhodné si ke každé události definovat možná rizika a jejich význam. Na základě expertního posouzení a zkušeností z testovacího prostředí byly určeny limitní hodnoty a úrovně události následovně:

Skupina síťové prvky - sk	parametr - p	jednotky	limitní podmínka -l	frekvence - f	časové okno - o	severita problému -s	zvýšení severity -z	časové období -č
CPU	zatížení procesoru	[%]	zatížení větší než 80 %	1 min	15 x	začínající problém	2 x časové okno	Vv, Vs,Vn
RAM	využití operační paměti	[%]	zatížení větší než 80 %	1 min	15 x	začínající problém	2 x časové okno	Vv, Vs,Vn
flash paměť	využití paměti	[%]	zatížení větší než 90 %	5 min	3 x	varování	x	x
propustnost rozhraní	odeslaná data	[Mb/s]	*	3 min	5 x	problém	2 x časové okno	Vv, Vs,Vn
propustnost rozhraní	přijatá data	[Mb/s]	*	3 min	5 x	problém	2 x časové okno	Vv, Vs,Vn
propustnost rozhraní	využití šířky pásma	[%]	využití větší než 90 %	3 min	4 x	problém	2 x časové okno	Vv, Vs,Vn
teplota	stav větráku	[1-6]	stav napájení ≠ 1	5 min	2 x	varování	2 x časové okno	Vv, Vs,Vn
napájení	stav napájení	[1-6]	stav napájení ≠ 1	5 min	2 x	varování	2 x časové okno	Vv, Vs,Vn
dostupnost zařízení	ICMP ping	up (1) down (0)	icmp ping = 0	1 min	3 x	vážný problém	2 x časové okno	Vv, Vs,Vn
kvalita datového přenosu	čas odpovědi ICMP	[ms]	průměr > 40 ms	1 min	5 x	varování	3 x časové okno	Vv, Vs,Vn
Skupina koncová zařízení								
CPU	zatížení CPU	[%]	zatížení větší než 90 %	3 min	10 x	varování	x	x
fyzická paměť	využití paměti	[%]	využití větší než 90 %	5 min	30 x	varování	x	x
RAM	využití operační paměti	[%]	využití větší než 90 %	3 min	10 x	varování	x	x
zabezpečení	stav služby antiviru	stopped (6) running (0)	stav služby = 6	5 min	10 x	začínající problém	x	x
tisk	stav služby Spooler	stopped (6) running (0)	stav služby = 6	10 min	20 x	varování	x	x
sdílené disky	stav služby sdílených disků	stopped (6) running (0)	stav služby = 6	5 min	10 x	varování	x	x
aktualizace	stav služby Update	stopped (6) running (0)	stav služby = 6	60 min	120 x	informace	x	x
dostupnost zařízení	ICMP ping	up (1) down (0)	icmp ping = 0	5 minut	15 x	informace	x	x
Skupina počítačová místnost								
CPU	zatížení CPU	[%]	zatížení větší než 80 %	3 min	5 x	informace	x	x
fyzická paměť	využití paměti	[%]	využití větší než 80 %	20 min	2 x	informace	x	x
RAM	využití operační paměti	[%]	využití větší než 80 %	3 min	3 x	informace	x	x
zabezpečení	stav služby antiviru	stopped (6) running (0)	stav služby = 6	5 min	2 x	varování	x	x
aktualizace	stav služby Update	stopped (6) running (0)	stav služby = 6	60 min	2 x	informace	x	x
správa úloh	stav služby Task manager	stopped (6) running (0)	stav služby = 6	30 min	2 x	informace	x	x
dostupnost zařízení	ICMP ping	up (1) down (0)	icmp ping = 0	10 min	3 x	informace	x	x
Skupina servery								
RAM	využití operační paměti	[%]	využití větší než 75 %	3 min	3 x	problém	4 x časové okno	Vs,Vn
CPU	zatížení CPU	[%]	zatížení větší než 75 %	3 min	3 x	problém	4 x časové okno	Vs,Vn
fyzická paměť	využití paměti	[%]	využití větší než 75 %	5 min	3 x	varování	5 x časové okno	Vs,Vn
propustnost rozhraní	odeslaná data	[Mb/s]	*	3 min	3 x	problém	3 x časové okno	Vs,Vn
propustnost rozhraní	přijatá data	[Mb/s]	*	3 min	3 x	problém	3 x časové okno	Vs,Vn
propustnost rozhraní	využití šířky pásma	[%]	využití větší než 90 %	3 min	3 x	problém	3 x časové okno	Vs,Vn
dostupnost zařízení	ICMP ping	up (1) down (0)	icmp ping = 0	1 min	3 x	vážný problém	x	x
kvalita datového přenosu	čas odpovědi ICMP	[ms]	průměr > 40 ms	3 min	3 x	problém	3 x časové okno	Vs,Vn
Skupina tiskárny								
dostupnost zařízení	ICMP ping	up (1) down (0)	icmp ping = 0	5 min	3 x	informace	2 x časové okno	Vs
spotřební materiál	stav materiálu	[%]	zásoba materiálu < 10 %	30 min	4 x	informace	x	x

*tyto parametry jsou definované zvlášť v *Tabulka 19* v *Tabulka* 20

Tabulka 23 Tabulka parametrů a jejich severity [autor]

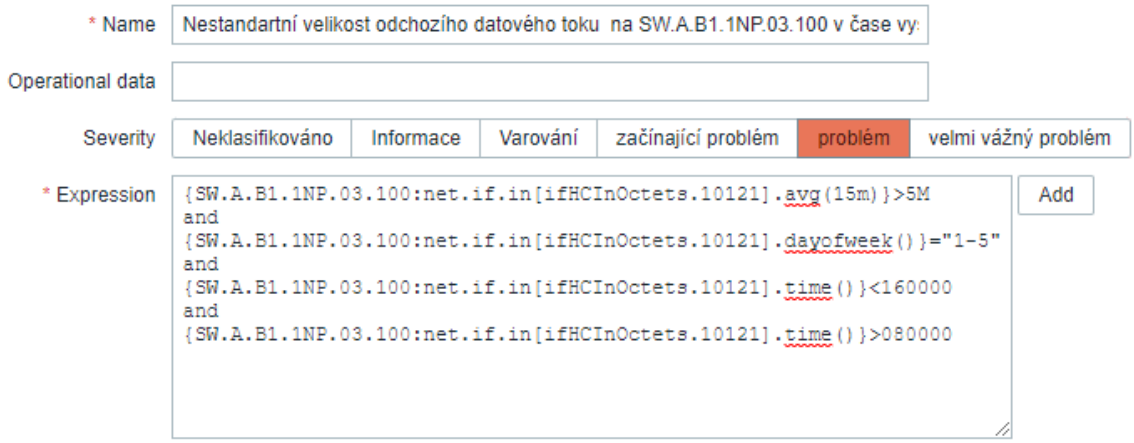
Tabulka 23 obsahuje soupis měřených parametrů a souvisejících veličin. Zde je zásadní závislost na čase, protože právě ten dokáže určit, zda se jedná pouze o krátkodobou událost, která vzniká v rámci standartního provozu, či se jedná o skutečně nestandartní chování. Pro tyto účely byla zavedena veličina časové okno. Tato veličina (o) definuje čas, po který musí být platná limitní podmínka (l). Veličina zvýšení severity (z) je zavedena z důvodu ošetření možné neudělení priority událostem, které mají kritickou vazbu na poskytovanou kvalitu služby. Práce s parametry je uvedena v logickém diagramu na *Obrázek 36*.

9.5 Definování spouštěčů a akcí

Monitorovací systém umožňuje nepřetržité sledování sítě a základní vyhodnocení těchto dat. K tomu, aby došlo k akci, je nutné systému nadefinovat spouštěče. Tyto spouštěče obsahují v sobě logickou podmínku. Pokud je tato podmínka označena za splněnou, spouštěč se stane aktivním. Zde záleží na tom, jaké požadavky jsou kladené na práci se spouštěčem. Řešení, které se proto využívá, je právě severita vzniklé události. Samotný spouštěč tedy vedle vnitřní limitní podmínky obsahuje i severitu události. Tyto spouštěče se dají nastavovat centrálně v rámci konkrétních šablon nebo v nastavení jednotlivého hosta.

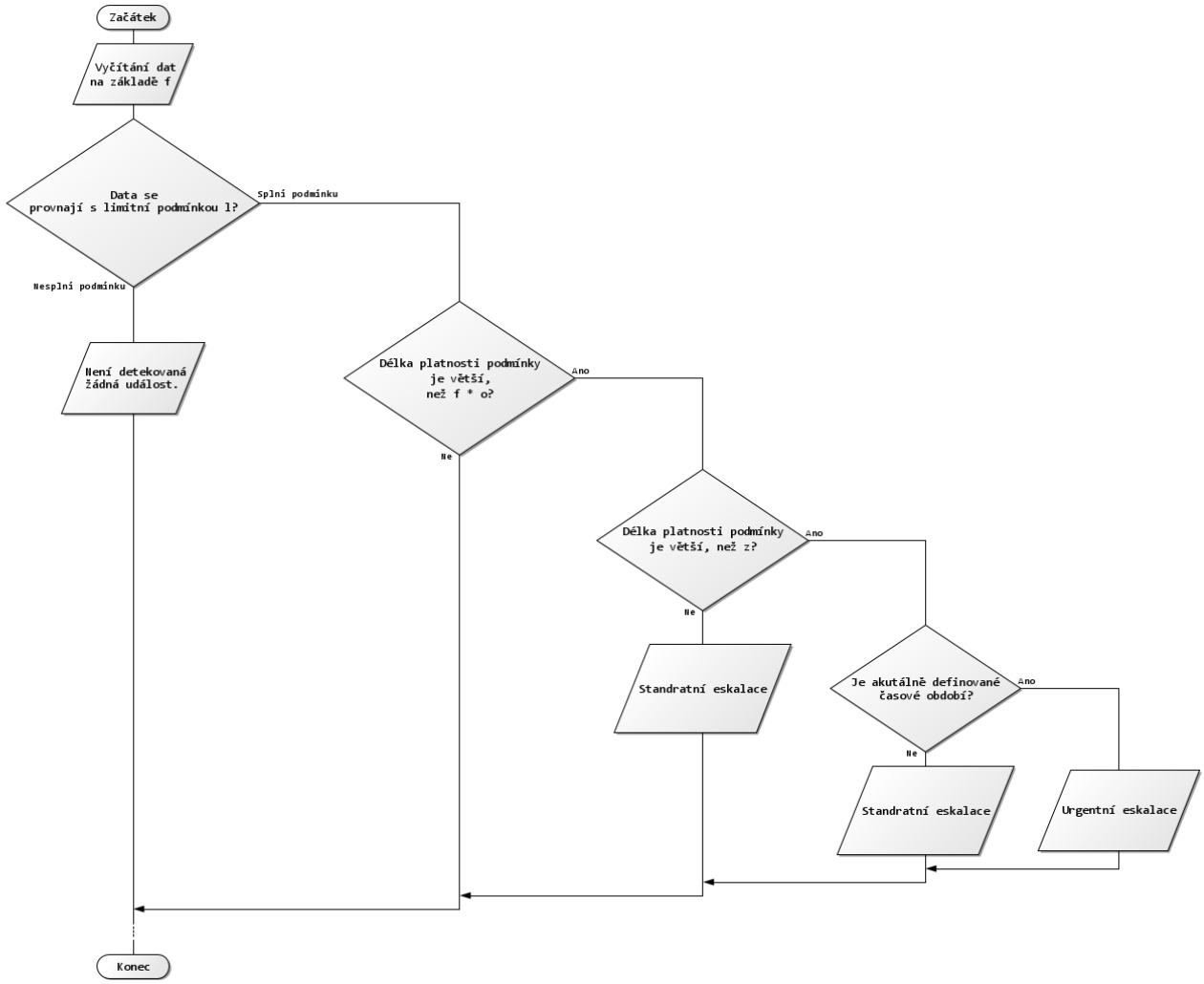
Zabbix nabízí velké množství logických funkcí pomocí, dle kterých si lze nastavit různé scénáře. *Obrázek 35* reprezentuje podmínku pro aktivaci spouštěče, který oznamuje událost o nestandartním odchozím datovém toku v čase vysoké zátěže na prvku

SW.A.B1.1NP.03.100. Definovaná severita události je v tomto případě problém (2. nejzávažnější).



Obrázek 35 Příklad definice spouštěče [autor]

Pokud je tedy spouštěč aktivní následuje provedení akce, která je navázaná na severitu události. Akce definuje určitý úkon, který nastane ihned po spouštění spouštěče. Samotná akce může mít dvě podoby, buď dojde k odeslání zprávy pomocí nastavených informačních kanálů (alert), či lze využít možnost vzdáleného spuštění příkazu na konkrétním hostovi. Může jít o zadání příkazu pomocí SSH konzole, či samotného agenta. U zadávání skriptů je nutné dbát obezřetnosti, bez otestovaného postupu může dojít k neúmyslným chybám v konfiguraci zařízení a následným výpadkům. V této práci jsou využity pouze akce, které distribuují zprávu. Tyto akce jsou generovány na základě navrženého logické diagramu.



Obrázek 36 Logický diagram vyhodnocení měřených dat [autor]

Zde je vhodné si položit otázku, komu se jaké zprávy budou doručovat a jak. Zde je příhodné využít jako zdroj informací matici odpovědností. Ke každé skupině zařízení je nutné najít odpovědnou osobu, která svými zkušenostmi a vědomosti schopná pokrýt danou problematiku. Přitom je třeba brát i do úvahy i možnou zastupitelnost a limity výkonosti jednotlivců. Možným scénářem může být také situace, kdy dochází k pronájmu služby od jiného subjektu, tudíž je vhodné přidat i tyto subjekty do matice odpovědnosti.

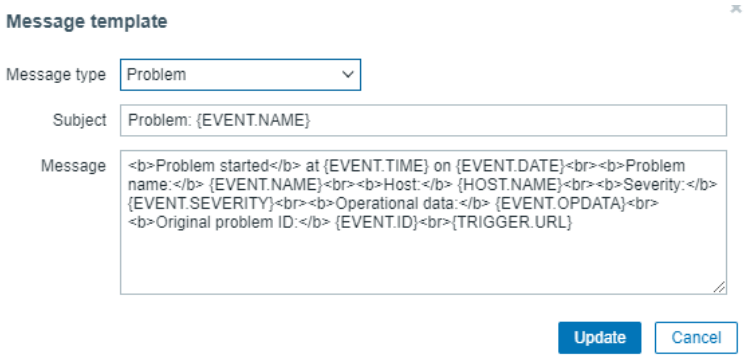
Samotný proces události byl na základě severit navržen takto:

Obrázek 37 Návrh procesů akcí v případě události [autor]

Obrázek 37 prezentuje jeden z možných scénářů, i zde velmi záleží na procesech uvnitř organizace. Pro předání zpráv byly vybrány dvě informační technologie, elektronická pošta a SMS zpráva. Existuje cela řada dalších možností, jako jsou např. MS Teams a Jira. Avšak elektronická pošta patří k nerozšířenějšímu způsobu komunikace uvnitř organizací a přes mobilní telefon lze kontaktovat osobu i mimo pracoviště. V tomto případě je mobilní telefon až krajním řešením u události s největší severitou.

Při řešení událostí je zásadní doba, kdy se začnou řešit. Proto je vhodné zde otevřít téma eskalace problému, která má za cíl zvyšovat prioritu událostí vzhledem k časové prodlevě. *Obrázek 37* definuje standartní eskalaci, tak že při naplnění časové podmínky, během které se na událost nijak nereaguje, přechází stav automaticky do události vyšší severity, se kterou je i spojená definovaná akce. V případě kritických událostí a naplnění podmínky zvýšení severity, dochází ihned k navýšení severity bez aplikace reakčních časů.

Pro nastavení zasílání elektronických zpráv je nutné znát nastavení serveru pro odchozí poštu. Na rozdíl od nastavení SMS zpráv není nutné zadávat žádný skript a ani vykonávat jiné nastavení na straně Zabbix serveru. K odesílání SMS zpráv je nutné vlastnit SMS bránu. V případě této práce byla nastavena brána od výrobce SMSEagle. Samotný obsah zpráv je generován na základě šablon prostřednictvím proměnných atributů (*Obrázek 38*).



Obrázek 38 Definování obsahu zprávy [autor]

U hodnot jednotlivých parametrů je vhodné odddělit od sebe dva druhy chování i na základě toho, zda konkrétní událost probíhá krátkodobě, či dlouhodobě. Pro ilustraci lze uvést příklad, kdy dochází ke změně topologie sítě. V rámci tohoto úkonů dojde k přepočítání ARP tabulek na síťových prvcích. Následně tedy může vystoupat hodnota RAM nad hraniční hodnotu, která by generovala oznámení. Nicméně po dokončení přepočtu se hodnoty vrátí pod hraniční limity. A lze očekávat v dalším časovém měřítku standartní chování. Avšak na druhou stranu může nastat situace, kdy dojde na zařízení k chybě, která přetrvává a lze predikovat budoucí výpadek zařízení. Nicméně v této situaci je nutné, co nejdříve informovat správce. Protože hrozí výpadek požadované služby např. chyba na zdroji zařízení.

Hlavním rizikem spouštěčů je jejich hromadná aktivace, například v situaci výpadku hlavního hraničním prvku. Proto je nutné při nastavování systému neopomenout vzájemně prvky provázat. Prakticky nastavení probíhá tak, že u nadřazeného prvku provážeme spouštěče s prvkem hierarchicky nižším. Pokud nadřazený spouštěč bude vyhodnocen jako pozitivní, tak spouštěč na zařízení pod ním nebude moc být aktivován. [29]

10. Otestování funkčnosti implementovaného systému

Před finální vyhodnocením implementace je nutné nástroj otestovat. Samotné testování bude probíhat podle 3 přesně definovaných scénářů. Tyto scénáře byly definovány na základně konzultace a možném rozsahu zásahů do testovací sítě. Každý ze scénářů se zaměřil na jinou skupinu zařízení a dohledávání rozdílné funkcionality (*Tabulka 24*). Testování prověří správné nastavení celého systému a lze ho také využít pro seznámení budoucích uživatelů se systémem.

název zařízení	skupina zařízení	předmět testu	výsledek testu
SW.A.B1.1NP.05.102	skupina síťová zařízení	nedostupnost síťového zařízení	obdržený alert velmi vážný problém po 3 min
B1.102.PC1	skupina PC místnost	deaktivace antiviru	obdržený alert po 51 minutách
B1.101.TISKARNA1	skupina tiskárny	nedostupnost tiskárny	obdržený alert informace po 15 min a alert varování po 30 min

Tabulka 24 Testovací scénáře [autor]

V rámci testovacího scénáře proběhlo otestování situace, kdy došlo k vypnutí rozhraní na zařízení SW.D.B1.1NP.NA.100. Monitorovací systém konstantně vyčítá data z prvku SW.A.B1.1NP.05.102. V případě parametru dostupnosti prvku je frekvence vyčítání dat každou minutu. V 15:01 byl na switchy SW.D.B1.1NP.NA.100 vypnuto rozhraní, které poskytuje datové propojení k zařízení SW.A.B1.1NP.05.102. V tu chvíli dojde k naplnění limitní podmínky, která je u tohoto parametru ICMP ping = 0. Následně dojde k porovnání délky pozitivní platnosti limitní podmínky, která je v tomto případě 3 minuty. I zde je tato podmínka platná, nakonec dojde k vyhodnocení časového období. U tohoto parametru není časové období definované, protože již svojí závažností je definovaný severitou události velmi vážné. *Obrázek 39* ukazuje, že v 15:04 byla odeslaná SMS zpráva a email osobě, která je zodpovědná za zařízení. Akce jsou definované na základě návrhu na *Obrázek 37.* Tento stav nebylo z důvodů dopadu na testovací infrastrukturu možné nechat trvat dlouhodobě, proto bylo rozhraní na prvku topologicky výše opět spuštěno. A systém informuje 15:07 správce o vyřešení události.

Ukázka testovacího scénáře – nedostupné zařízení SW.A.B1.1NP.05.102

Actions

Step	Time	User/Recipient	Action	Message/Command	Status	Info
	04/27/2022 03:07:39 PM	mfiala (Zabbix Administrator) *martin.fiala@fd.cvut.cz*		**Resolved in 3m 0s: Unavailable by ICMP ping** Problem has been resolved at 09:07:34 on 2022.04.27 Problem name: Unavailable by ICMP ping Problem duration: 3m 0s Host: SW.A.B1.1NP.05.102 Severity: velmi vážný problém Original problem ID: 983739	Sent	
	04/27/2022 03:07:39 PM	mfiala (Zabbix Administrator) *00420608975245*		**Resolved in 3m 0s: Unavailable by ICMP ping** Problem has been resolved at 09:07:34 on 2022.04.27 Problem name: Unavailable by ICMP ping Problem duration: 3m 0s Host: SW.A.B1.1NP.05.102 Severity: velmi vážný problém Original problem ID: 983739	Sent	
	04/27/2022 03:07:34 PM					
1	04/27/2022 03:04:39 PM	mfiala (Zabbix Administrator) *00420608975245*		**Problem: Unavailable by ICMP ping** Problem started at 09:04:34 on 2022.04.27 Problem name: Unavailable by ICMP ping Host: SW.A.B1.1NP.05.102 Severity: velmi vážný problém Operational data: Down (0) Original problem ID: 983739	Sent	
1	04/27/2022 03:04:39 PM	mfiala (Zabbix Administrator) *martin.fiala@fd.cvut.cz*		**Problem: Unavailable by ICMP ping** Problem started at 09:04:34 on 2022.04.27 Problem name: Unavailable by ICMP ping Host: SW.A.B1.1NP.05.102 Severity: velmi vážný problém Operational data: Down (0) Original problem ID: 983739	Sent	
	04/27/2022 03:04:34 PM					

Obrázek 39 Zobrazuje přehled akcí při testovacím scénáři [autor]

11. Návrhy ke zvýšení kvality služby

V rámci implementace monitorovacího systému na testovací síť, byly nalezeny čtyři základní oblasti, které při realizaci v rámci organizace umožní zvýšení poskytované kvality služby.

11.1 Využívání monitorovacího systému z pohledu okamžitých akcí

Během praktické části byl implementován a otestován nástroj pro sledování infrastruktury v reálném čase. Pokud se jeho využívání stane součástí běžné pracovní agendy, dojde k rapidnímu poklesu času potřebného k odstranění událostí na infrastruktuře a celkově lepšímu poskytování služby, díky včasné a automaticky předané informaci konkrétní osobě, na základě přidělené odpovědností. V případě přehlédnutí, nebo vynechání řešení aktuální události, umožňuje její povýšení na problémy vyšší severity na základě odpovídajících podmínek vycházejících ze sledování chování sítě. S tím je také spjata možnost lépe informovat samotné uživatele. Tím nebude docházet k situacím, kdy uživatel nalezne jako první skutečnost, že služba nenaplňuje svou kvalitu. Tím se zvýší i důvěra uživatelů v samotný systém. A v případech, kdy poskytovaná služba je ovlivněna, je možné lépe organizovat provozní důsledky a tím předejít úplnému zastavení provozu organizace.

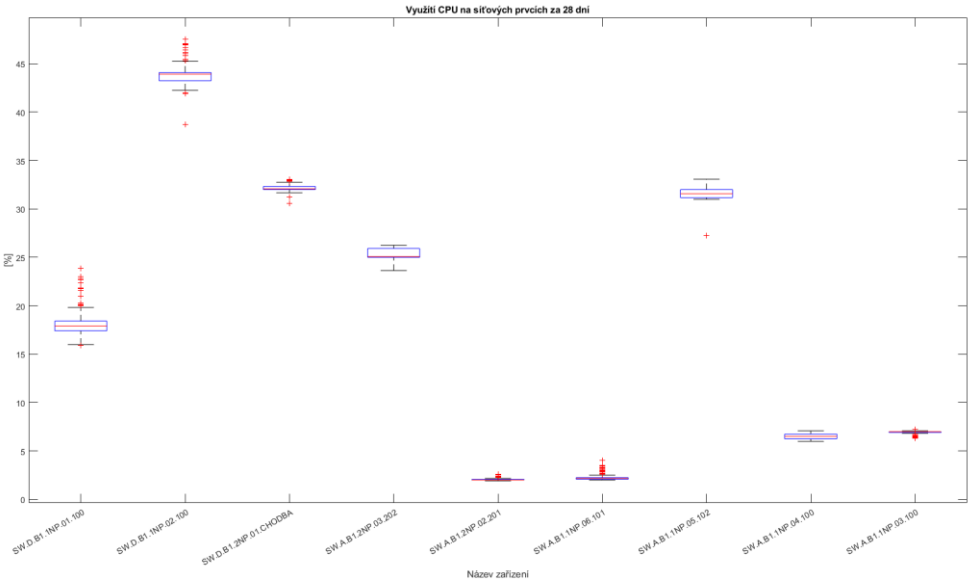
11.2 Využívání monitorovacího systému z pohledu plánování

Dlouhodobé využívání monitorovacího systému přináší možnost náhledu do historických dat. Tato možnost je velmi přínosná pro plánování. Správce může sledovat trendy u zařízení, či kapacit přenosových medií. Na základě těchto dat realizovat včasný zásah do infrastruktury. Díky tomu lze infrastrukturu adekvátně nastavit bez překročení jejích stávajících limitů. Výstupy mohou sloužit i jako podklad pro rozhodování managementu v oblasti dalšího vývoje IT v organizaci, či organizačních procesů. Také lze na základě sebraných dat pozorovat změny uživatelského chování, či rozeznat změnu v samotných potřebách uživatelů.

11.3 Využívání monitorovacího systému z pohledu analýzy infrastruktury

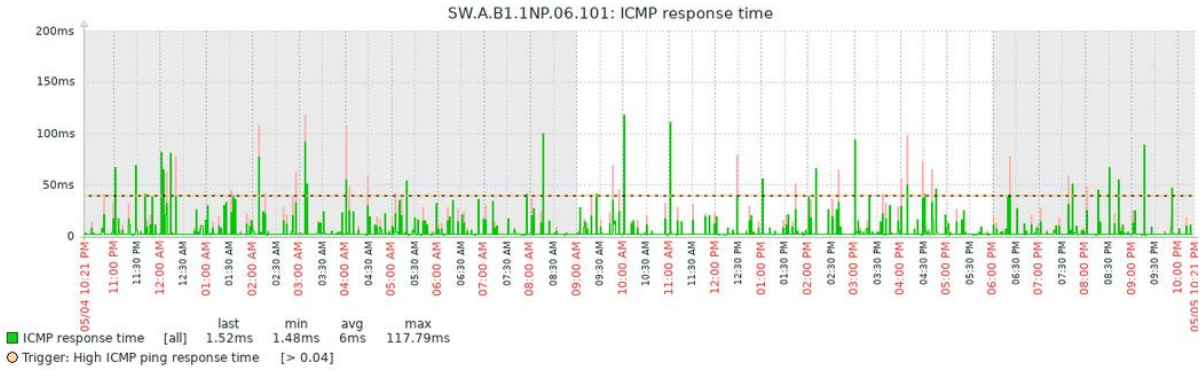
Při samotné implementaci dojde ke sběru dat ze sítě, tudíž lze odhalit problémy v aktuální síti, ať z pohledu topologie, či konkrétních parametrů u samotných prvků infrastruktury jako je například kapacita datových cest. Lze také zjistit aktuální verze zařízení a na základě nich provést kontrolu možných rizik pro dané zařízení a tím předejít možným bezpečnostním incidentům.

Na základě sběru dat lze konstatovat, že testovací síť splňuje kapacitní požadavky a nabízí i dostatečnou rezervu. Charakteristiky komponent zařízení dosahují optimálních hodnot. Například při zatížení dosahují procesory maximálního využití do 50 % (*Graf 6*).



Graf 6 Zobrazení vytížení CPU na síťových prvcích

Zařízení, které je doporučeno zkontrolovat je switch z označením SW.A.B1.1NP.06.101, který překračuje definovanou limitní hodnotu zpoždění 40 milisekund. A tudíž připojená zařízení mohou mít omezenou kvalitu využívaných služeb např. horší kvalita video hovoru.



Graf 7 Zobrazení průběhu zpoždění na zařízení SW.A.B1.1NP.06.101 [autor]

12. Další možné přínosy

Vedle samotného přínosu využívání dat v rámci monitorování infrastruktury, lze tato data využít i k dalším aspektům, které přímo ovlivňují pracovní prostředí zaměstnanců v organizaci, či nabízejí další příležitosti pro ekonomický růst.

12.1 Využívání dat z infrastruktury

Na základě toho, že v dnešním světě má již jakékoliv elektronické zařízení možné propojení do datové sítě, je vhodné tato data centralizovat a využívat. Může jít například o prvky IOT jako jsou například senzory. V rámci konceptu smart building lze najít senzory měřící teplotu

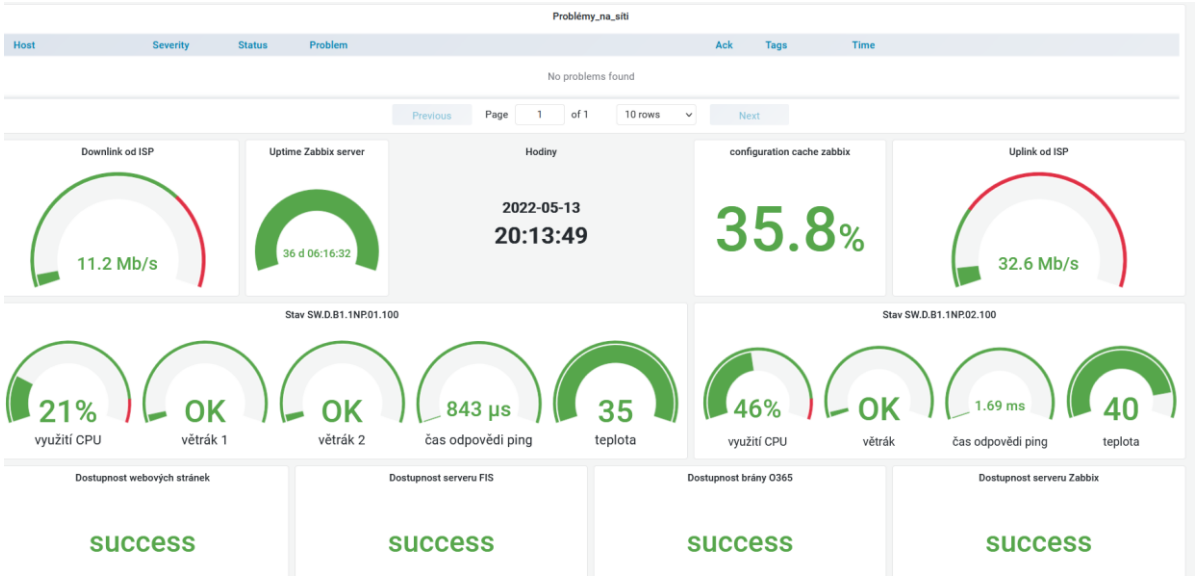
vzduchu, či jeho vlhkost. Všechny tyto vlastnosti prostředí v budově mají velký dopad na samotného uživatele a ovlivňují jeho pracovní efektivitu. Vedle toho dnes existují i světelné zdroje, které lze připojit k datové síti a díky znalostem dat, lze optimalizovat energetické náklady. Největší možné přínosy těchto dat lze získat pouze, pokud se stanou součástí samotných procesů uvnitř organizace. Potom lze například kontrolovat situace, kdy dochází k využívání světelných zařízení i mimo provozní dobu budovy.

Vedle toho samotná síťová zařízení umožňuji spouštět vlastní aplikace, které využívají aktuální sebraná data. U přístupových bodů může jít o možnost vyhodnotit polohu uživatelů a dobu, kterou na konkrétním místě stráví. Nicméně zde velmi záleží na primárním cíli daného řešení. V rámci testovací organizace je primární funkce infrastruktury rozdílná než například funkce v rámci obchodního domu. U specifických řešení, poptávají subjekty řešení v rámci infrastruktury od jednoho dodavatele. Tudíž lze využít potom již integrované nástroje, avšak toto řešení neumožňuje centralizovat sběr dat na jednom místě v případě různých výrobců.

Možností využití dat z infrastruktury existuje celá řada a rozvoj stále posiluje. Nicméně hlavním hlediskem, které je, pro možné přínosy sledování dat zásadní, je definice samotného využití. Data, která jsou pouze zobrazovaná mohou být zajímavá a v případě časového uspořádání i vhodná pro plánování. Avšak jejich celkový přínos a maximální využití lze docílit pouze při napojení dat na konkrétní akce.

12.2 Vizualizace dat z infrastruktury

Sbíraná data je vhodné vizualizovat z důvodu jejich lepšího pochopení a přehlednosti. Vizualizace dat je možná rovnou v prostředí systému Zabbix. Na druhou stranu tento systém nepodporuje tvorbu agregačních nástěnek, protože se jedná o nástroj primárně určený pro sběr dat. Nicméně na trhu existují bezplatné nástroje pouze pro vizualizaci dat. Tudíž může být vhodné tyto nástroje propojit. Nejoblíbenějším nástrojem je Grafana, který umožňuje kvalitní grafické zpracování. Nástroj lze napojit na různé zdroje dat pomocí doplňků. Jeden z těchto doplňků existuje i pro monitorovací systém Zabbix. Pokud jsou tato data stále na očích správcům, mají tak k dispozici přehled o aktuálním dění na spravované infrastruktuře. Při využití možnosti barevných škál, které jsou navázané na logické podmínky, lze jasně upozornit na vznikající problematickou událost. *Obrázek 40* ukazuje vytvořenou nástěnku na základě dat z testovací sítě. [5]



Obrázek 40 Ukázka nástěnky v prostředí Grafana [autor]

13. Závěr

Tato práce měla za cíl implementovat monitorovací systém na testovací infrastrukturu. Její samotný postup byl definovaný na základě schématu, který je uveden na *straně 50* této práce. Schéma poukazuje na pořadí jednotlivých kroků. Práce je postavena na informacích ze zdrojové literatury a vědeckých článků. Pro praktickou část byly kromě literatury využity i konzultace se subjekty z testovací organizace

Na začátku této práce byl kladen velký důraz na správné definování terminologie tak, aby při čtení práce nedocházelo ke zmatení pojmů. Vedle toho je teoretická část koncipovaná jako přehledný úvod do problematiky počítačových sítí, kde je zdůrazněn význam společných standardů, které umožňují vzájemnou komunikaci. Další část práce je věnovaná rešerši možných přístupů a způsobů, jak monitorovat celou síťovou infrastrukturu. Pomocí metody QFD byl vybrán nejvhodnější nástroj na základě požadavků testovací infrastruktury. Vybraný nástroj byl implementován a následně byly představeny jednotlivé kroky, které je nutné realizovat, aby systém byl plně funkční a pomohl plnit definované kvality služby. V této části je zásadní si v rámci organizace uvědomit, co a proč je potřeba monitorovat. Každá organizace může mít jiné požadavky na monitorování infrastruktury.

V rámci praktické části proběhl sběr dat z testovací infrastruktury, který umožnil pochopit standartní chování uvnitř organizace. Data posloužila jako vstup při definování limitních hodnot mezi standartním a nestandartním chováním. Pro definování těchto dat byla využita shlukovací analýza. Přínosem těchto dat je informace o aktuálním stavu infrastruktury a o tom, zda má daná infrastruktura nedostatky, které mohou omezit kvalitu poskytované služby. V případě vzniku problematických událostí jsou definovány také severity, které umožní určovat rozdílné způsoby akcí na základě rozsahu možných následků. Pro ověření funkčnosti systému došlo k otestování 3 zkušebních scénářů v podobě nedostupnosti jednoho síťového zařízení a tiskárny. A následně ke simulaci vypnutí antiviru na koncovém zařízení.

Na závěr byly shrnuty možnosti, které pomohou k plnění kvalit poskytované služby, včetně potencionálních kroků, které vedou i ke zvýšení spokojenosti samotných uživatelů. Hlavními kroky je včasná detekce problémových situací, díky které dojde k prodloužení doby funkčnosti systému. V diplomové práci byly představeny také další možnosti, jak využívat data ze zařízení. Avšak nejdůležitější je znalost účelu užití těchto naměřených dat.

14. Zdroje

[1] Access, Distribution, and Core Layers Explained. *ComputerNetworkingNotes* [online]. 4.5.2021 [cit. 2022-04-22]. Dostupné z: https://www.computernetworkingnotes.com/ccna-study-guide/access-distribution-and-core-layers-explained.html

[2] Bertolina, M. (2012). Netconf element management system. Journal of Computer Science and Technology,12(2),87-90.Retrieved dostupné z: http://ezproxy.techlib.cz/login?url=https://www.proquest.com/scholarly-journals/netconf-element-management-system/docview/2544434111/se-2

[3] Braham B.: TCP/IP Addressing. Academia press, London, 1997

[4] *Cisco DNA Center Reviews & Product Details* [online]. 2021 [cit. 2022-05-04]. Dostupné z: https://www.g2.com/products/cisco-cisco-dna-center/reviews

[5] *Computerworld*. Praha: Internet Info DG, 2022. ISSN 12109924.

[6] COWLEY, John. *Communications and Networking: An Introduction*. 2nd. Londýn: Springer, 2013. ISBN 1447143574.

[7] Dostupnost (Availability). Managementmania [online]. 6.9.2016 [cit. 2022-02-17]. Dostupné z: https://managementmania.com/cs/dostupnost-availability

[8] E.Uglickich, I.Nagy. Recursive mixture estimation with univariate multimodal Poisson variable. Research report 2394. May 2022. ÚTIA AV ČR.

[9] EDWARDS, Jeff. Active Vs. Passive Monitoring: Which is Best for Your Network?. *Progress WhatsUp Gold* [online]. 12.3.2020 [cit. 2022-04-02]. Dostupné z: https://www.whatsupgold.com/blog/active-vs.-passive-monitoring-which-is-best-for-your-network

[10] Enterprise Networking, Security, and Automation [online]. V7.02. San Jose, Kalifornie: Cisco, 2020 [cit. 2021-4-26]. Dostupné z: https://www.netacad.com

[11] Foundations of Computing and Decision Sciences: Tools for distributed systems monitoring. 41. 2016. ISSN 0867-6356. Łukasz KUFEL.

[12] Hardy W.C.: QoS Measurement and Evaluation of Telecommunications Quality of Service. ISBN: 0-471-49957-9, John Wiley & Sons, June 2001.

[13] HERMANTES, Josune, Gorka GALLARDO a Nicolas SERRANO. IT Infrastructure-Monitoring Tools. *IEEE software*. 2015, **32**(4), 88-93. ISSN 0740-7459.

[14] *How To Run Zabbix Server 6 in Docker Containers* [online]. 2022 [cit. 2022-05-04]. Dostupné z: https://techviewleo.com/how-to-run-zabbix-server-in-docker-containers/

[15] HRDLIČKA, Miroslav. *Zajištění kvality služby v bezdrátových sítích*. Praha, 2005. Diplomová. Univerzita Karlova v Praze. Vedoucí práce Jan Janeček.

[16] Importance of Computer Networking. *Geeksforgeeks* [online]. 18.8.2020 [cit. 2022-02-17]. Dostupné z: https://www.geeksforgeeks.org/importance-of-computer-networking/

[17] ITIL® V3 Foundation Course Glossary. *Axelos* [online]. 2011 [cit. 2022-03-26]. Dostupné z: https://www.axelos.com/resource-hub/glossary/itil-v3-glossaries-of-terms

[18] J. Machan, J. Tobiška, D. Bakušová, P. Baumruk. Metody kvality užívané ve fázi vývoje výrobku - aplikace v automobilovém průmyslu, II. přepracované vydání. Praha 2012. ISBN 978-80-87042-50-2.

[19] JOHNSON, Allan. 31 Days Before your CCNA Exam : A Day-By-Day Review Guide for the CCNA 200-301 Certification Exam. Indianapolis: Cisco Press, 2020. ISBN 0135964083.

[20] KHILLAR, Sagar. Difference Between Open Source and Proprietary Software. *DifferenceBetween.net* [online]. 5.4.2018 [cit. 2022-04-02]. Dostupné z: http://www.differencebetween.net/technology/difference-between-open-source-and-proprietary-software/

[21] KRAJÍČEK, Ing. Tomáš. Diagnostika počítačů (Computer Diagnostics), podzim 2005 [online]. 2005 [cit. 2022-01-18]. Dostupné z: https://is.muni.cz/el/fi/podzim2005/PV171/

[22] LAMMLE, Todd a Andy BARKL. *CCDA: Cisco Certified Design Associate Study Guide, 2nd Edition (640-861)* [online]. 2nd. Sybex Inc; Bk&CD Rom edition, 2003. ISBN 978-0782142006. Dostupné také z: https://cleerlinefiber.com/2019/03/19/singlemode-vs-multimode-fiber-optic-cables/

[23] M. Dallaglio, N. Sambo, F. Cugini and P. Castoldi, "Control and management of transponders with NETCONF and YANG," in Journal of Optical Communications and Networking, vol. 9, no. 3, pp. B43-B52, March 2017, doi: 10.1364/JOCN.9.000B43.

[24] M. Jethanandani, "YANG, NETCONF, RESTCONF: What is this all about and how is it used for multi-layer networks," *2017 Optical Fiber Communications Conference and Exhibition (OFC)*, 2017, pp. 1-65.

[25] MAURO, Douglas R. a Kevin J. SCHMIDT. Essential SNMP. Second edition. Sebastopol: O'Reilly, 2005. ISBN 0-596-00840-6.

[26] *Monitoring & Auto-Healing FileMaker Server with Zabbix* [online]. 2019 [cit. 2022-05-04]. Dostupné z: https://www.soliantconsulting.com/blog/filemaker-server-zabbix/

[27] MUDRÁK, David. *Schéma zapouzdření aplikačních dat na vrstvách TCP/IP* [online]. 11.10.2008 [cit. 2022-03-26]. Dostupné z: https://cs.wikipedia.org/wiki/TCP/IP#/media/Soubor:Tcpip_zapouzdreni.svg

[28] *Nmap* [online]. 2022 [cit. 2022-05-04]. Dostupné z: https://cs.wikipedia.org/wiki/Nmap

[29] OLUPS, Rihards, Andrea DALLE VACCHE a Patrik UYTTERHOEVEN. *Zabbix: Enterprise Network Monitoring Made Easy*. Birmingham: Packt Publishing, 2017. ISBN 9781787129047.

[30] PÁV, Ing. Miroslav, SYŘÍNEK, Mgr. Jan, ed. *CCNA Exploration - Základy síti* [online]. Plzeň, 2011, doplnit! [cit. 2022-01-18]. Dostupné z: http://www.nidv.mysh.cz/data/resources/ccna_exploration_1_tisk_[9141179].pdf

[31] PETERKA, Jiří. Terminologie datových sítí. *EArchiv.cz* [online]. 2015 [cit. 2022-03-26]. Dostupné z: https://www.earchiv.cz/b00/b0003002.php3

[32] PILÍK, Tomáš. *Implementace dohledové nadstavby stávajícího zálohovacího systému*. Praha, 2016. Diplomová. České vysoké učení technické v Praze. Vedoucí práce Pavel Troller.

[33] Počítačové sítě. BISKUPSKÉ GYMNÁZIUM ŽĎÁR NAD SÁZAVOU [online]. [cit. 2022-02-17]. Dostupné z: http://www.bigyzr.cz/shared/clanky/2893/ICT-Pripravy/pripravy_site_11-12.pdf

[34] Protocol. Britannica Academic [online]. [cit. 2022-02-17]. Dostupné z: https://academic-eb-com.ezproxy.techlib.cz/levels/collegiate/article/protocol/473123

[35] Screenshoty Zabbix. In: *Zabbix* [online]. [cit. 2022-05-13]. Dostupné z: https://www.zabbix.com/cz/screenshots

[36] *Single Mode vs. Multimode Fiber Optic Cables* [online]. Missoula, 2019 [cit. 2022-03-09]. Dostupné z: https://cleerlinefiber.com/2019/03/19/singlemode-vs-multimode-fiber-optic-cables/

[37] *SSL* [online]. 2022 [cit. 2022-05-04]. Dostupné z: https://www.ssls.cz/slovnik/ssl.html

[38] SWEEX síťová karta 10/100/1000 Mbps, Gigabit, PCI. *Tsbohemia.cz* [online]. [cit. 2022-03-26]. Dostupné z: https://www.tsbohemia.cz/

[39] *Techopedia: Processor* [online]. Edmonton, Kanada, 2020 [cit. 2022-05-11]. Dostupné z: https://www.techopedia.com/definition/28254/processor

[40] *TechTarget patch panel* [online]. 2021 [cit. 2022-03-09]. Dostupné z: https://cleerlinefiber.com/2019/03/19/singlemode-vs-multimode-fiber-optic-cables/

[41] *What Is a LAN?* [online]. 2022 [cit. 2022-01-18]. Dostupné z: https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html

[42] *What Is a WAN? Wide-Area Network* [online]. 2022 [cit. 2022-01-18]. Dostupné z: https://www.cisco.com/c/en/us/products/switches/what-is-a-wan-wide-area-network.html

[43] WINKELMAN, Dr. Roy. *What Is a WAN? Wide-Area Network* [online]. Florida Center for Instructional Technology College of Education, University of South Florida, 2013 [cit. 2022-01-18]. Dostupné z: https://www.cisco.com/c/en/us/products/switches/what-is-a-wan-wide-area-network.html

[44] *Wireshark* [online]. [cit. 2022-05-04]. Dostupné z: https://cs.wikipedia.org/wiki/Wireshark

[45] *Základní typy rozdělení pravděpodobnosti diskrétní náhodné veličiny* [online]. 27.2.2012 [cit. 2022-05-09]. Dostupné z: https://homel.vsb.cz/~oti73/cdpast1/KAP04/PRAV4.HTM

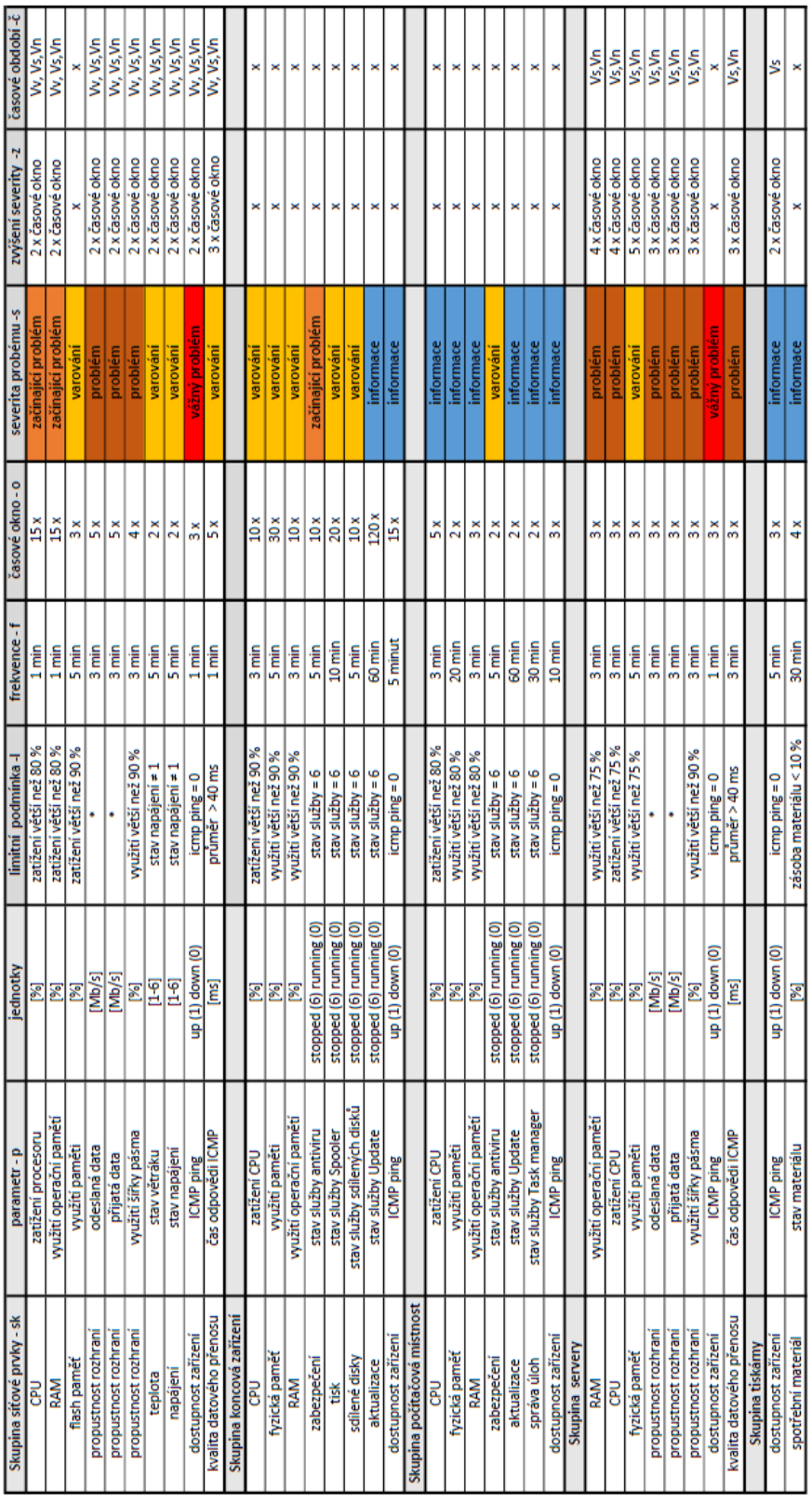
15. Seznam obrázků

16. Seznam tabulek

17. Seznam příloh

18. Přílohy

Příloha 1 Tabulka parametrů a limitních hodnot [autor]



Skupina síťové prvky - sk	parametr - p	jednotky	limitní podmínka - l	frekvence - f	časové okno - o	severita problému - s	zvýšení severity - z	časové období - č
CPU	zatížení procesoru	[%]	zatížení větší než 80 %	1 min	15 x	začínající problém	2 x časové okno	Vv, Vs,Vn
RAM	využití operační paměti	[%]	zatížení větší než 80 %	1 min	15 x	začínající problém	2 x časové okno	Vv, Vs,Vn
flash paměť	využití paměti	[%]	zatížení větší než 90 %	5 min	3 x	varování	x	x
propustnost rozhraní	odeslaná data	[Mb/s]	*	3 min	5 x	problém	2 x časové okno	Vv, Vs,Vn
propustnost rozhraní	přijatá data	[Mb/s]	*	3 min	5 x	problém	2 x časové okno	Vv, Vs,Vn
propustnost rozhraní	využití šířky pásma	[%]	využití větší než 90 %	3 min	4 x	problém	2 x časové okno	Vv, Vs,Vn
teplota	stav větráku	[1-6]	stav napájení ≠ 1	5 min	2 x	varování	2 x časové okno	Vv, Vs,Vn
napájení	stav napájení	[1-6]	stav napájení ≠ 1	5 min	2 x	varování	2 x časové okno	Vv, Vs,Vn
dostupnost zařízení	ICMP ping	up (1) down (0)	icmp ping = 0	1 min	3 x	vážný problém	2 x časové okno	Vv, Vs,Vn
kvalita datového přenosu	čas odpovědi ICMP	[ms]	průměr > 40 ms	1 min	5 x	varování	3 x časové okno	Vv, Vs,Vn
Skupina koncová zařízení								
CPU	zatížení CPU	[%]	zatížení větší než 90 %	3 min	10 x	varování	x	x
fyzická paměť	využití paměti	[%]	využití větší než 90 %	5 min	30 x	varování	x	x
RAM	využití operační paměti	[%]	využití větší než 90 %	3 min	10 x	varování	x	x
zabezpečení	stav služby antiviru	stopped (6) running (0)	stav služby = 6	5 min	10 x	začínající problém	x	x
tisk	stav služby Spooler	stopped (6) running (0)	stav služby = 6	10 min	20 x	varování	x	x
sdílené disky	stav služby sdílených disků	stopped (6) running (0)	stav služby = 6	5 min	10 x	varování	x	x
aktualizace	stav služby Update	stopped (6) running (0)	stav služby = 6	60 min	120 x	informace	x	x
dostupnost zařízení	ICMP ping	up (1) down (0)	icmp ping = 0	5 minut	15 x	informace	x	x
Skupina počítačová místnost								
CPU	zatížení CPU	[%]	zatížení větší než 80 %	3 min	5 x	informace	x	x
fyzická paměť	využití paměti	[%]	využití větší než 80 %	20 min	2 x	informace	x	x
RAM	využití operační paměti	[%]	využití větší než 80 %	3 min	3 x	informace	x	x
zabezpečení	stav služby antiviru	stopped (6) running (0)	stav služby = 6	5 min	2 x	varování	x	x
aktualizace	stav služby Update	stopped (6) running (0)	stav služby = 6	60 min	2 x	informace	x	x
správa úloh	stav služby Task manager	stopped (6) running (0)	stav služby = 6	30 min	2 x	informace	x	x
dostupnost zařízení	ICMP ping	up (1) down (0)	icmp ping = 0	10 min	3 x	informace	x	x
Skupina servery								
RAM	využití operační paměti	[%]	využití větší než 75 %	3 min	3 x	problém	4 x časové okno	Vs,Vn
CPU	zatížení CPU	[%]	zatížení větší než 75 %	3 min	3 x	problém	4 x časové okno	Vs,Vn
fyzická paměť	využití paměti	[%]	využití větší než 75 %	5 min	3 x	varování	5 x časové okno	Vs,Vn
propustnost rozhraní	odeslaná data	[Mb/s]	*	3 min	3 x	problém	3 x časové okno	Vs,Vn
propustnost rozhraní	přijatá data	[Mb/s]	*	3 min	3 x	problém	3 x časové okno	Vs,Vn
propustnost rozhraní	využití šířky pásma	[%]	využití větší než 90 %	3 min	3 x	problém	3 x časové okno	Vs,Vn
dostupnost zařízení	ICMP ping	up (1) down (0)	icmp ping = 0	1 min	3 x	vážný problém	x	x
kvalita datového přenosu	čas odpovědi ICMP	[ms]	průměr > 40 ms	3 min	3 x	problém	3 x časové okno	Vs,Vn
Skupina tiskárny								
dostupnost zařízení	ICMP ping	up (1) down (0)	icmp ping = 0	5 min	3 x	informace	2 x časové okno	Vs
spotřební materiál	stav materiálu	[%]	zásoba materiálu < 10 %	30 min	4 x	informace	x	x

Příloha 2 Program využitý při analýze dat metodou shlukování [8]

```
clear,clc,close(winsid()),mode(0)
//Definice funkcí

function Lf=factLn(n)
  // Definování funkce log faktoriálu
  m=length(n)
  for i=1:m
    Lf(i)=sum(log(1:n(i)));
  end
endfunction

function pr=poiss(x, lam)
  // Pravděpodobnost Poissonova rozdělení
  x=x(:);
  Lp=-lam*ones(x)+x*log(lam)-factLn(x);
  pr=exp(Lp);
endfunction

function [f, sm]=histc(x, n, r)
  // histogram of x
  // x    data
  // n    počet sloupců
  if argn(2)<3, r=.8; end
  if argn(2)<2, n=20; end
  minx=min(x);
  maxx=max(x);
  h=(maxx-minx)/(n);
  s=minx:h:maxx;
  for i=1:n
    f(i)=length(find((x>=s(i))&(x<s(i+1))));
  end
  k=find(x==s(n));
  if ~isempty(k)
    f(n)=f(n)+length(k);
  end
  for i=1:n
    sm(i)=(s(i)+s(i+1))/2;
  end
  if r>0, bar(sm,f); end
endfunction

////////////// Počáteční podmínky
nd=440; //Počet naměřených dat
nc = 2; //Počet shluků
i=2;//Počátek indexu
////// Vložení vlastních dat
y = []

////// Zobrazení dat
scf(1);
plot(y);
title('využitá data pro shlukování');
xlabel('Čas [h]');ylabel('Velikost přijatých/odchozíchdatových toků
[Mbit/s]');

scf(2);
histc(y);
title('Histogram');
xlabel('Velikost datových toků [Mbit/s]');ylabel('Četnost');
```

```
///////// Inicilizace směsi dat
S=[1 10]'; /// počet sloupců histogramu
ka=ones(nc,1);/// sčítač
nu=rand(nc,1,'uniform'); /// statistika ukazovátka
LaE=S./ka; /// odhad parametru modelu komponenty
alE=nu./sum(nu);/// bodový odhad ukazovátka

//////// Předpověď směsi chování
for t=1:nd
    for i=1:nc
          m(i)=poiss(y(t),LaE(i));///blízkost poisson. roz. komponetám
    end
    tildew=m.*alE;
    w=tildew./sum(tildew);  /// normalizovaný šířkový vektor
    [nic,cE(t)]=max(w);   /// předpověď ukazovátka
    wt(:,t)=w;
    /////Aktualizace statistiky
    for i=1:nc
       S(i)=S(i)+w(i)*y(t);
       ka(i)=ka(i)+w(i);/// počítač komponent
    end
    nu=nu+w; /// aktualizace statistiky ukazovátka

    ////Body odhadu
    LaE=S./ka; /// bodový odhad komponent
    alE=nu./sum(nu);///bodový odhad ukazovátka
    //// Predikce
    bb=grand(1, 1, "poi", LaE(cE(t))); ///gen. vysledného Poissonova roz.
    yp(t)=bb;


end

///////Výsledky

scf(3);
plot(cE,'r.');
title('Předpověď ukazovátka');
set(gca(),"data_bounds",[nd-300 nd 0 nc+0.1]);
legend('simulace', 'předpověď',4);
xlabel('čas');ylabel('výsledky');

//// Přesnost
//ep=sum(c(:)~=cE(:));
PE=(ep*100)/nd;
disp('Procenta vyjadřující špatnou předpověď',PE)

///// Chyba odhadu
RMSE = sqrt(mean((y(:) - yp(:)).^2));
// Relativní chyba predikce
RPE=variance(y(:)-yp(:))/variance(y(:));
disp(['RMSE RPE'],[RMSE RPE]);
```