Univerzita Hradec Králové
Fakulta informatiky a managementu
katedra informačních technologií

Dohled síťové infrastruktury v podnikovém prostředí

Krokový tutoriál

Bakalářská práce

Autor: Matěj Hromádka
Studijní obor: Informační managment

Vedoucí práce: Ing. Ph.D. Tomáš Svoboda

Hradec Králové Duben 2023

Prohlášení:

Prohlašuji, že jsem bakalářskou/diplomovou práci zpracoval/zpracovala samostatně a s použitím uvedené literatury.

vlastnoruční podpis

V Hradci Králové dne 25.4.2023 Matěj Hromádka

Poděkování:

Rád bych touto cestou vyjádřil své upřímné poděkování všem, kteří mi pomohli s napsáním této bakalářské práce.

Především bych rád poděkoval svému vedoucímu práce Ing. Ph.D. Tomášovi Svobodovi, za jeho cenné rady, trpělivost, obětavou pomoc, jeho konstruktivní kritiku a ochotu, kterou mi svým časem věnoval. Dále bych rád poděkoval i kolegům, kteří mi pomohli, když jsem byl ve svízlivé situaci.

Anotace

Bakalářská práce se zabývá se seznámením se s informacemi potřebnými k monitoringu síťové infrastruktury v podnikovém prostředí. Základní přehled o počítačových sítích, její historii, dělení a využití. Měla by nás uvést do základní terminologie a popisu dvou hlavních modelů ISO/OSI a TCP/IP. Vysvětlení funkčnosti jejich vrstev a popsání rozdílů mezi nimi. Obsahuje průvodce mezi základními pojmy „Network monitoring“ jaké jsou jeho možnosti a proč se v dnešní době aktivně využívá k monitoringu síťové infrastruktury v podnikovém prostředí. Bude popsáno, jak pomáhá „Change managment“ k bezpečnějšímu a pohodlnějšímu administrátorství sítě. Níže jsou uvedeny přímo vlastnosti vybraných programů jako je např.: „PRTG, Nagios“. Praktická část má za cíl vytvořit „step by step“ manuál, jak si takovou monitorovací síť, pomocí nástroje PRTG nakonfigurovat. V práci jsou uvedeny základní nastavení podle definovaných use case případů.

Annotation

Title: Network infrastructure monitoring in an enterprise environment

The bachelor thesis deals with getting acquainted with the information needed to monitor the network infrastructure in a corporate environment. Basic overview of computer networks, its history, division and use. It should introduce us to the basic terminology and description of the two main models ISO/OSI and TCP/IP. Explain the functionality of their layers and describe the differences between them. It includes a guide between the basic concepts of "Network monitoring" what its capabilities are and why it is actively used today to monitor network infrastructure in the enterprise environment. It will describe how Change management helps to make network administration more secure and convenient. Below are directly listed the features of selected programs such as "PRTG, Nagios". The practical part aims to create a "step by step" manual on how to configure such a monitoring network using the PRTG tool. The basic settings according to the defined use cases written below.

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Žijeme v době, kdy se Internetová síť (z angl. „Network“) stala aktivní a běžnou součástí života. Více než osmdesát procent lidí, kteří žijí v České republice, běžně využívá přímo nejznámější síť, kterou je internet [1]. Stává se tedy nutností, aby firmy, které chtějí uspět na trhu, začlenili používání internetu, jako sítě takové, taktéž do běžného užívání. Proto je monitorování sítě je důležitým aspektem správy IT, protože pomáhá organizacím zajistit stabilitu, výkon a bezpečnost jejich sítí. Průběžným monitorováním sítě a jejích součástí mohou organizace včas identifikovat a řešit problémy, a tím zlepšit celkovou spolehlivost a efektivitu sítě.

V posledních letech došlo k výraznému nárůstu složitosti a významu monitorování sítí, protože organizace spoléhají na sítě při podpoře široké škály aplikací a služeb. V důsledku toho roste poptávka po odbornících, kteří mají zkušenosti s monitorováním sítí a kteří mohou organizacím pomoci efektivně spravovat a optimalizovat jejich sítě.

Postupně bakalářská práce seznámí se základem v počítačových sítích a uvede do problematiky Network monitoringu. Nastíní a podrobně vylíčí k čemu zde slouží change managment a vysvětlí pojem incident. Vysvětlí, proč je dobré incidentům předcházet a jak minimalizovat riziko výpadku celé sítě.

2 Cíl práce

Cílem této bakalářské práce je prozkoumat současný stav monitorování sítí a identifikovat osvědčené postupy a trendy v této oblasti. Představit si některé možnosti programů, které bychom mohli k monitorování sítí použít. Ukázat si jejich výhody a nevýhody, případné doporučení. Vytvořit fyzickou lokální síť, která bude přes nejvhodnější program monitorována. V daném nástroji si definovat pět use casů, podle kterým se nadále bude praktická část řídit, aby dosáhla svého řešení.

3 Teoretická část

3.1 Úvod do počítačových sítí

Počítačová síť (z angl. computer network) se v informatice označuje spojení, které realizuje výměnu informací mezi jednotlivými počítači. Podle určitých pravidel a předem určených standardů protokolů umožňuje komunikaci uživatelům. Ti pak mohou pomocí zpráv komunikovat mezi sebou navzájem.

3.1.1 Vznik Internetu

První pokusy o komunikaci mezi dvěma počítači se začaly objevovat na v polovině 20. století. Vývoj tohoto odvětví zařídila armáda. Vůbec první oficiálně vzniklá síť byla pojmenována ARPANET. Psal se rok 1969 a armáda při rozvoji vůbec poprvé rozvíjí síť, která se v dnešní době označuje za předchůdce, dnes dobře známé sítě, internetu. Původně to byla pouze a jen experimentální síť americké armády. Její účel bylo propojit radarové stanice.

3.1.2 Formování Internetu (ARPANETu)

V roce 1983 se od ARPANETu oddělila vojenská síť MILNET (tzv. military network). Od té doby se pomalu začala formovat více než jako vojenská síť, síť veřejná/civilní. Největším milníkem pro tento rok byl ovšem byl vznik do dnes známého a aktivně využívaného protokolu TCP/IP. Jeho tvůrci se rozhodli původní implementaci protokolu rozdělit na dva samostatné protokoly TCP a IP, které se dodnes aktivně používají. Protokol IP se stará o samotný přenos dat, nicméně neručí za jejich ztrátu. Proto se používá ve spojení s TCP protokolem, jehož pravidla garantují kompletnost přenosového toku. Jako alternativa byl vyvinut protokol UDP, jenž pro přenos dat využívá taktéž protokolu IP. Oproti TCP protokolu je ale založen na rychlosti komunikace navzdory případné ztrátovosti. Obsahoval už služby jako jsou např. e-mail, či online přenos souborů (FTP). S tímto pokrokem se začíná objevovat i služba WWW „World Wide Web“. Jeho základy se objevily sice už v roce 1980, ale to byly začátky, kdy se přecházel ze stránky na stránku pomocí hypertextového odkazu. V 90. letech se dotvořily dnešní známe protokoly jako je HTML, FTP, a dokonce i jazyk HTML. [2]

3.1.3 Vznik sítě NFSNET

Jednou tehdy z největších institucí na podporu vědy a výzkumu, která se podílela na vývoji Internetu, byla agentura NSF (National Science Foundation). Skrze neshody se s vedením ARPANET vytvořila vlastní síť s názvem NSFNET. Tato síť se později stala součástí Internetu. Velkou zásluhou byl přísun finančních prostředků, protože instituce rozpoutala masové připojování akademických institucí. Z tohoto důvodu postupem času převzal roli páteřní sítě, přes kterou probíhala největší část provozu v rámci Internetu. Vše pak vyvrcholilo v roce 1990, kdy ARPANET byla v tichosti odstavena a zrušena. NSFNET tedy mezitím přebral kompletní úlohu páteřní sítě, která tvořila Internet.

Sám NSFNET přitom také prošel určitým vývojem, který nezahrnoval pouze změny technické. Šlo především o to, že NSFNET byl původně koncipován jako výzkumná síť, ale s postupem času se stal především provozní sítí, zajišťující spíše rutinní přenosy velkých objemů dat. Nikoli ale přenosy, sloužící ryze komerčním účelům, kterým se NSFNET nadále brání. 2 Provozovatel NSFNETu (agentura NSF) si změněnou roli své páteřní sítě uvědomil, a rozhodl se NSFNET pozvolna odstavit - s tím, že jeho přenosové funkce postupně převezmou jiné sítě, fungující již plně na komerčním základě. Tím vlastně NSF jen vzala na vědomí a přizpůsobila se trendu, který sama vyvolala svým omezením komerčního provozu po NSFNETu, a který dal vzniknout čistě komerčním páteřním sítím, schopným již dnes zcela se vyhnout NSFNETu (podrobněji viz článek: "Pro koho je Internet?"). Páteřní síť NSFNET tedy bude v následujících letech postupně odstavována. [2]

3.2 Počítačová síť

Počítačovou sítí je chápáno komunikační spojení umožňující vzájemnou komunikaci a výměnu dat propojených minimálně dvěma počítači. Jde o souhrnné označení pro:

- Hardware – tj. síťové prvky, kabely, switche, routery, servery apod.
- Software – tj. síťový operační systém, protokoly umožňující vzájemnou komunikaci, výměnu dat mezi počítači apod.

3.2.1 Dělení sítí

Dělení dle velikosti:

- **PAN** (Personal Area Network) – malá osobní síť sloužící pro propojení malého počtu zařízení. Příklad takové sítě v dnešním světě můžeme nazvat třeba Bluetooth.
- **LAN** (Local Area Network) – malá počítačová síť. Například v domácnosti nebo v jedné budově. Vstupuje do rozlehlé sítě přes jednu IP adresu.
- **MAN** (Metropolitan Area Network) – městská síť propojující větší množství zařízení v městské zástavbě.
- **WAN** (Wide Area Network) – rozlehlá širší síť spojující LAN a MAN sítě (např. Internet)

Dělení dle typu propojení:

- **peer-to-peer sítě** – počítače v síti jsou si rovny, např. sdílení souborů v síti nebo na internetu
- **klient-server** – síť, kde jsou počítače rozlišeny na servery, poskytující služby, a klientské počítače, které je využívají (podniková síť, web, apod.).

Dělení dle vlastnictví:

- **Veřejná síť** – to jsou např. telekomunikační sítě, veřejné WiFi, apod. Provozovateli jsou spojové organizace nebo jiné subjekty, které nabízejí své služby veřejnosti.
- **Privátní síť** – využívá speciální IP adresy podle daných standardů. Běžně se používají pro domácí, kancelářské a podnikové lokální sítě (LAN). Privátní sítě byly definovány jako nástroj pro spomalení ubývání IPv4 adres.
- **Virtuální síť** – umožňuje propojení několika počítačů prostřednictvím veřejné nedůvěryhodné sítě. Z angl. VPN. Díky této sítě lze dosáhnout stavu, kdy spojené počítače budou komunikovat mezi sebou jako by byly propojeny v rámci jedné společné sítě. Před začátkem spojení je totožnost

obou uzlů ověřována pomocí certifikátů. Poté co dojde k ověření platnosti, komunikace je zašifrována a putuje k příjemci, který ji může dešifrovat.

3.3 Síťová zařízení

3.3.1 Aktivní prvky

- **Switch** – přepínač, propojuje ostatní prvky sítě a umožňuje rozdělit síťový signál mezi více zařízení
- **Hub** – funguje na podobném principu jako switch, s rozdílem že nerozděluje kolizní doménu a data odesílá na všechny porty jako opakovač
- **Router** – počeštěle směrovač, přeposílá datové packety (balíčky) směrem k jejich cíli, umožňují vytvořit lokální síť propojenou s vnější sítí pod jednou fyzickou IP adresou

3.3.2 Pasivní prvky

- **Kabely** – fyzicky přenášejí data mezi počítači, např.: koaxiální dvojlinka, kroucená dvojlinka, optické, vlákno apod. [3]

3.4 Model ISO/OSI

Model OSI byl v roce 1979 oficiálně upraven jako norma ISO. Někdo by mohl říct, že je to starý standard. Ano, opravdu je starý. Ale to, co tento model udrželo při životě tak dlouho, je jeho schopnost rozšiřovat se podle vyvíjejících se potřeb. Většinu práce, která vytvořila základ modelu OSI, odvedla skupina ve společnosti Honeywell Information Systems. Vedoucím této skupiny byl Mike Canepa. V roce 1995 byl model OSI revidován, aby pokryl potřeby vyplývající z rychlého vývoje v oblasti počítačových sítí. Dnes každá vrstva zpracovává data způsobem, který se liší od ostatních vrstev. Jednotka, ve které určitá vrstva zpracovává data, se nazývá datová jednotka protokolu (PDU). Některé vrstvy přidávají k datům informace specifické pro danou vrstvu. Tyto informace přidané protokoly vrstev mohou mít podobu hlavičky, návěští nebo obojího. Informace v záhlaví se přidávají na začátek PDU, zatímco informace v traileru se přidávají na konec PDU. Tato hlavička nebo upoutávka obsahuje informace, které jsou užitečné při řízení komunikace mezi dvěma entitami.

Model OSI pracuje ve strategii vrstevníků. Tato strategie znamená, že řídicí informace přidané do PDU jednou vrstvou jsou určeny k tomu, aby se dostaly k vrstevnické vrstvě v přijímající entitě. Například informace v záhlaví přidané v síťové vrstvě v odesílajícím hostiteli jsou použity síťovou vrstvou v přijímajícím hostiteli a tyto informace jsou pro ostatní vrstvy nepodstatné. Proto musí být na obou koncích komunikace použity kompatibilní protokoly, aby se podařilo doručit uživatelská data správným způsobem.

Obrázek 1 - Model ISO/OSI Zdroj: Vlastní zpracování, inspirováno [10]

3.4.1 Fyzická vrstva

Fyzická vrstva v podstatě zpracovává data jako surové bity. To znamená, že PDU pro fyzické vrstvy je bit. Primární povinností fyzické vrstvy je poskytovat transparentní přenos bitů z vrstvy datového spoje odesílatele do vrstvy datového spoje příjemce. Toho se dosahuje definováním mechanických, elektrických, funkčních a procedurálních prostředků pro aktivaci, udržování a deaktivaci datového toku.

Kromě dat přenášených z jedné fyzické entity do druhé je třeba přenášet také řídicí informace. Tyto řídicí informace mohou být přidány k a transformovat ve

stejném kanálu, ve kterém jsou data přenášena, a to se nazývá in-line signalizace. Nebo mohou být řídicí informace přenášeny prostřednictvím kanálu. Samostatným řídicím kanálem, což se nazývá off-line signalizace nebo out-of-line signalizace. Volba způsobu přenosu řídicích informací je ponechána na protokolu. Protokoly fyzické vrstvy se liší podle typu fyzického média a typu signálu, který se na něm přenáší. Signál může být elektrické napětí přenášené po kabelu, světelný signál přenášený vláknovým spojem nebo dokonce elektromagnetický signál.

Funkce fyzické vrstvy:

a) Aktivace a deaktivace fyzického spojení.
b) Zajištění přenos bitů ze zdroje do cíle.
c) Multiplexování a demultiplexování
d) Zajištění sekvenčního příjmu bitů
e) Detekce chyb na fyzickém médiu

3.4.2 Linková vrstva

PDU linkové vrstvy je rámec, což znamená, že zpracovává data jako rámce. Tyto rámce mohou mít rozsah od několika set bajtů do několika tisíc bajtů. Dále přidává své řídicí informace ve formě záhlaví a hlavičky. Datová vrstva má ve srovnání s ostatními vrstvami mnoho složitých funkcí.

Funkce linkové vrsty:

- Řízení propojení datových okruhů
  - Tato funkce poskytuje síťovým entitám možnost řídit propojení datových okruhů v rámci fyzické vrstvy.
- Identifikace a výměna parametrů
  - Každá entita se musí identifikovat vůči ostatním entitám a je třeba vyměňovat i některé parametry, jimiž se řídí komunikace. Příkladem těchto parametrů je datová rychlost.
- Detekce chyb a oprava
  - Některé fyzické kanály mohou být náchylné k faktorům, které brání správnému doručení dat. Těmito faktory mohou být

elektromagnetické rušení (EMI), teplota, déšť atd. v závislosti na typu média. Jednou z funkcí vrstvy datového spoje je detekce těchto chyb.

- Přeposílání
    - Některé konfigurace sítě vyžadují replying mezi jednotlivými místními sítěmi.
- Správa vrstvy datového spoje
    - Podobně jako správa fyzické vrstvy ponechává vrstva datového spoje některé operace správy na použitých protokolech.

3.4.3 Síťová vrstva

Síťová vrstva slouží k přenosu dat z jednoho hostitele na druhého, který se nachází v různých sítích. Stará se také o směrování paketů, tj. výběr nejkratší cesty pro přenos paketu z řady dostupných tras. IP adresy odesílatele a příjemce jsou umístěny v záhlaví síťovou vrstvou. Všechna data odesílaná přes Internet jsou rozdělena na menší části, kterým se říká "pakety". Když například Bob pošle Alici zprávu, jeho zpráva se rozdělí na menší části a poté se v Alicině počítači znovu složí. Paket má dvě části: záhlaví, které obsahuje informace o samotném paketu, a tělo, což jsou vlastní odesílaná data.

Na síťové vrstvě připojuje síťový software ke každému paketu hlavičku, když je paket odesílán přes internet, a na druhé straně může síťový software hlavičku použít k pochopení toho, jak s paketem zacházet.

Záhlaví obsahuje informace o obsahu, zdroji a cíli každého paketu (něco jako razítko na obálce s cílovou a zpáteční adresou). Například hlavička IP obsahuje cílovou IP adresu každého paketu, celkovou velikost paketu, údaj o tom, zda byl paket při přenosu fragmentován (rozdělen na ještě menší části), a počet sítí, kterými paket prošel.

Funkce síťové vrstvy:

- Směrování:
    - Protokoly síťové vrstvy určují, která trasa je vhodná od zdroje k cíli. Tato funkce síťové vrstvy se nazývá směrování.

- Logické adresování:
    - Aby bylo možné jednoznačně identifikovat každé zařízení v internetové síti, definuje síťová vrstva schéma adresování. Adresy IP odesílatele a příjemce jsou umístěny v záhlaví síťovou vrstvou. Taková adresa rozlišuje každé zařízení jednoznačně a univerzálně.

Protokoly na síťové vrstvě:

Protokol je dohodnutý způsob formátování dat tak, aby spolu dvě nebo více zařízení mohla komunikovat a vzájemně si rozumět. Připojení, testování, směrování a šifrování na síťové vrstvě umožňuje řada různých protokolů, včetně:

- IPv4, IPv6
- IPsec
- ICMP
- ICMPv6

3.4.4 Transportní vrstva

Transportní vrstva poskytuje služby aplikační vrstvě a přijímá služby od síťové vrstvy. Data v transportní vrstvě se označují jako segmenty. Je zodpovědná za doručení kompletní zprávy od konce ke konci. Transportní vrstva také zajišťuje potvrzení o úspěšném přenosu dat a v případě nalezení chyby data přenáší znovu.

- **Na straně odesílatele**

Na straně odesílatele přijímá transportní vrstva formátovaná data z vyšších vrstev, provádí segmentaci a také implementuje řízení toku a chyb, aby zajistila správný přenos dat. Do své hlavičky také přidá čísla zdrojového a cílového portu a předá segmentovaná data síťové vrstvě. Odesílatel musí znát číslo portu přiřazené aplikaci příjemce. Obecně je toto číslo cílového portu nakonfigurováno buď ve výchozím nastavení, nebo ručně. Například když webová aplikace zadává požadavek webovému serveru, obvykle použije číslo portu 80, protože je to

výchozí port přidělený webovým aplikacím. Mnoho aplikací má přiřazeny výchozí porty.

- **Na straně příjemce**

Transportní vrstva přečte číslo portu ze své hlavičky a předá data, která obdržela, příslušné aplikaci. Provádí také sekvencování a opětovné sestavení segmentovaných dat.

Funkce transportní vrstvy:

- *Segmentace a opětovné sestavení*:
  - Tato vrstva přijímá zprávu od vrstvy (relační) a rozděluje zprávu na menší jednotky. Ke každému vytvořenému segmentu je přiřazena hlavička. Transportní vrstva v cílové stanici zprávu znovu sestaví.
- *Adresování servisních bodů:*
  - Aby bylo možné doručit zprávu správnému procesu, obsahuje záhlaví transportní vrstvy typ adresy nazývaný adresa servisního bodu nebo adresa portu. Uvedením této adresy tak transportní vrstva zajistí, že zpráva bude doručena správnému procesu.

Služby poskytované transportní vrstvou:

A. Služba zaměřená na spojení: Jedná se o třífázový proces, který zahrnuje:
   - navázání spojení
   - přenos dat
   - Ukončení / odpojení

Při tomto typu přenosu odesílá přijímací zařízení po přijetí paketu nebo skupiny paketů zpět ke zdroji potvrzení. Tento typ přenosu je spolehlivý a bezpečný.

B. Služba bez spojení: Jedná se o jednofázový proces a zahrnuje přenos dat. Při tomto typu přenosu příjemce nepotvrzuje příjem paketu. Tento přístup

umožňuje mnohem rychlejší komunikaci mezi zařízeními. Služba orientovaná na spojení je spolehlivější než služba bez spojení.

3.4.5 Relační vrstva

Relační vrstva, která je pátou vrstvou modelu OSI, využívá služeb poskytovaných transportní vrstvou, umožňuje aplikacím navazovat a udržovat relace a synchronizovat relace.

Nyní je pro navázání spojení relace třeba dodržet několik věcí.

První věcí je, že bychom měli namapovat adresu relace na přepravní adresu. Druhou věcí je, že musíme zvolit požadované parametry kvality služby přenosu (označované také jako QoS). Další věcí je, že se musíme postarat o vyjednávání, které by mělo probíhat mezi parametry relace. Pak dále potřebujeme přenést omezená transparentní uživatelská data. A nakonec musíme správně monitorovat fázi přenosu dat. Schopnost odesílat větší množství datových souborů je nesmírně důležitá a také nezbytná věc.

Funkce relační vrstvy:

- Dialogový řadič
    - Relační vrstva funguje jako dialogový řadič, jehož prostřednictvím umožňuje systémům komunikovat v poloduplexním nebo plně duplexním režimu komunikace.
- Zajištění exkluzivity
    - Je také zodpovědná za správu tokenů, jejímž prostřednictvím zabraňuje současnému přístupu nebo pokusu dvou uživatelů o stejnou kritickou operaci.
- Synchronizace toku dat
    - Umožňuje synchronizaci tím, že umožňuje proces přidávání kontrolních bodů, které jsou považovány za synchronizační body k datovým tokům.
- Kontrola spolehlivosti
    - Je zodpovědná za kontrolní body relací a obnovu.

- Správa spojení
    - V podstatě poskytuje mechanismus otevírání, zavírání a správy relace mezi procesy aplikací koncového uživatele.
    - Synchronizace informací

Protokoly na relační vrstvě:

Relační vrstva používá některé protokoly, které jsou nutné pro bezpečnou, zabezpečenou a přesnou komunikaci mezi dvěma uživatelskými aplikacemi. Následují některé z protokolů, které poskytuje nebo používá vrstva relací.

- **Protokol AppleTalk Data Stream Protocol (ADSP**): ADSP je typ protokolu, který vyvinula společnost Apple Inc. a který obsahuje řadu funkcí umožňujících připojení k místním sítím bez předchozího nastavení.
- **Protokol RTCP (Real-time Transport Control Protocol):** RTCP je protokol, který poskytuje mimopásmové statistické a řídicí informace pro relaci RTP (Real-time Transport Protocol). Hlavní funkcí protokolu RTCP je poskytovat zpětnou vazbu o kvalitě služby (QoS) při distribuci médií pravidelným zasíláním statistických informací, jako jsou počty přenesených oktetů a paketů nebo ztráty paketů, účastníkům relace streamování multimédií.
- **Protokol PPTP (Point-to-Point Tunneling Protocol):** PPTP je protokol, který poskytuje metodu pro implementaci virtuálních privátních sítí. PPTP používá řídicí kanál TCP a tunel Generic Routing Encapsulation k zapouzdření paketů PPP (Point-to-Point Protocol) Tento protokol poskytuje úroveň zabezpečení a vzdáleného přístupu srovnatelnou s typickými produkty VPN (Virtual Private Network).

3.4.6 Prezentační vrstva

Prezentační vrstva se také nazývá překladová vrstva. Data z aplikační vrstvy jsou zde extrahována a upravena podle požadovaného formátu pro přenos po síti.

Funkce prezentační vrstvy:

- Překlad na odlišné kódování: Například ASCII na EBCDIC.
- Šifrování/dešifrování: Šifrování dat: Šifrování dat převádí data do jiné formy nebo kódu.
- Zašifrovaná data se nazývají šifrovaný text a dešifrovaná data se nazývají otevřený text. Pro šifrování i dešifrování dat se používá hodnota klíče.
- Komprese: Snižuje počet bitů, které je třeba přenést v síti.

3.4.7 Aplikační vrstva

Na samém vrcholu zásobníku vrstev referenčního modelu OSI se nachází aplikační vrstva, která je realizována síťovými aplikacemi. Tyto aplikace vytvářejí data, která je třeba přenášet po síti. Tato vrstva slouží také jako okno pro přístup aplikačních služeb k síti a pro zobrazení přijatých informací uživateli.
Příklad: Aplikace – prohlížeče, Skype Messenger atd.

Funkce aplikační vrstvy

Aplikační vrstva v modelu OSI obecně funguje pouze jako rozhraní, které je zodpovědné za komunikaci s hostitelskými a uživatelskými aplikacemi. To je rozdíl od protokolu TCP/IP, kde jsou vrstvy pod aplikační vrstvou, tj. relační a prezentační vrstva, spojeny dohromady a tvoří jednoduchou jedinou vrstvu, která je zodpovědná za plnění funkcí, mezi něž patří řízení dialogů mezi počítači, navazování a udržování i ukončování určité relace, zajišťování komprese a šifrování dat atd. Nejprve klient odešle příkaz serveru, a když server tento příkaz přijme, přidělí klientovi číslo portu. Poté klient odešle serveru požadavek na inicializaci spojení, a když server požadavek přijme, vydá klientovi potvrzení (ACK), že klient úspěšně navázal spojení se serverem, a proto má nyní přístup k serveru, jehož prostřednictvím může buď požádat server o zaslání jakýchkoli typů souborů nebo jiných dokumentů, nebo může sám nahrát nějaké soubory nebo dokumenty na server.

Protokoly na aplikační vrstvě:

Protokoly aplikační vrstvy: Aplikační vrstva poskytuje několik protokolů, které umožňují jakémukoli softwaru snadno odesílat a přijímat informace a prezentovat smysluplná data svým uživatelům.

Následují některé z protokolů, které poskytuje aplikační vrstva.

- **TELNET:** Telnet je zkratka pro telekomunikační síť. Tento protokol se používá pro správu souborů přes Internet. Umožňuje klientům Telnetu přistupovat ke zdrojům serveru Telnet. Telnet používá port číslo 23.
- **DNS:** DNS je zkratka pro Domain Name System (systém doménových jmen). Služba DNS překládá název domény (zvolený uživatelem) na odpovídající IP adresu. Například - pokud zvolíte název domény www.abcd.com, pak jej služba DNS musí přeložit jako 192.36.20.8 (náhodná IP adresa napsaná jen pro pochopení). Protokol DNS používá číslo portu 53.
- **DHCP:** Zkratka DHCP znamená Dynamic Host Configuration Protocol (protokol dynamické konfigurace hostitele). Poskytuje hostitelům IP adresy. Kdykoli se hostitel pokusí zaregistrovat u serveru DHCP o IP adresu, server DHCP poskytne příslušnému hostiteli mnoho informací. DHCP používá čísla portů 67 a 68.
- **FTP:** FTP je zkratka pro protokol pro přenos souborů. Tento protokol pomáhá přenášet různé soubory z jednoho zařízení do druhého. Protokol FTP podporuje sdílení souborů prostřednictvím vzdálených počítačových zařízení se spolehlivým a efektivním přenosem dat. FTP používá port číslo 20 pro přístup k datům a port číslo 21 pro řízení dat.
- **SMTP:** SMTP je zkratka pro Simple Mail Transfer Protocol (protokol pro jednoduchý přenos pošty). Používá se k přenosu elektronické pošty od jednoho uživatele k druhému. SMTP používají koncoví uživatelé ke snadnému odesílání e-mailů. SMTP používá čísla portů 25 a 587.
- **HTTP:** HTTP je zkratka pro Hyper Text Transfer Protocol. Je základem World Wide Webu (WWW). HTTP funguje na modelu klient-server. Tento protokol se používá k přenosu hypermediálních dokumentů, jako je HTML. Tento protokol byl navržen zejména pro komunikaci mezi webovými prohlížeči a webovými servery, ale tento protokol lze použít i pro několik dalších účelů. HTTP je bezstavový protokol (síťový protokol, ve kterém klient posílá požadavky serveru a server odpovídá zpět podle daného stavu), což

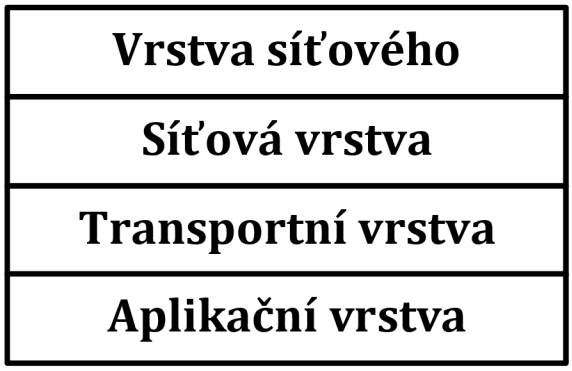
znamená, že server není zodpovědný za udržování předchozích požadavků klienta. HTTP používá port číslo 80.

- **SNMP:** SNMP je zkratka pro Simple Network Management Protocol. Tento protokol shromažďuje data dotazováním zařízení ze sítě na stanici pro správu v pevných nebo náhodných intervalech a vyžaduje od nich sdělení určitých informací. Protokol SNMP používá čísla portů 161 (TCP) a 162 (UDP). Později bude rozebrán podrobněji. [4]

3.5 Model TCP/IP

Model OSI, na který jsme se právě podívali, je pouze referenční/logický model. Byl navržen tak, aby popisoval funkce komunikačního systému rozdělením komunikačního postupu na menší a jednodušší součásti. Když však hovoříme o modelu TCP/IP, byl navržen a vyvinut ministerstvem obrany (DoD) v 60. letech 20. století a je založen na standardních protokolech. Je to zkratka pro Transmission Control Protocol/Internet Protocol. Model TCP/IP je stručnou verzí modelu OSI. Na rozdíl od sedmi vrstev modelu OSI obsahuje čtyři vrstvy.

Vrstvy jsou následující:



Obrázek 2 - Model TCP/IP Zdroj: Vlastní zpracování, inspirováno [10]

3.5.1 Vrstva síťového rozhraní

Tato vrstva odpovídá kombinaci vrstvy linkové a fyzické vrstvy modelu OSI. Zajišťuje hardwarové adresování a protokoly přítomné v této vrstvě umožňují fyzický přenos dat.

Právě jsme hovořili o tom, že ARP je protokol internetové vrstvy, ale existuje rozpor ohledně jeho prohlášení za protokol internetové vrstvy nebo přístupové vrstvy sítě. Je popsán jako sídlící ve vrstvě 3, přičemž je zapouzdřen protokoly vrstvy 2.

3.5.2 Síťová vrstva

Tato vrstva má obdobné funkce jako síťová vrstva OSI. Definuje protokoly, které jsou zodpovědné za logický přenos dat v celé síti.

Hlavní protokoly na této vrstvě jsou:

IP – zkratka pro internetový protokol, který je zodpovědný za doručování paketů od zdrojového hostitele k cílovému hostiteli na základě IP adres v hlavičkách paketů. IP má dvě verze:
IPv4 a IPv6. IPv4 je ta, kterou v současné době používá většina webových stránek. IPv6 však roste, protože počet adres IPv4 je v porovnání s počtem uživatelů omezený.
ICMP - zkratka pro Internet Control Message Protocol (protokol řídicích zpráv internetu). Je zapouzdřen v datagramech IP a je zodpovědný za poskytování informací hostitelům o problémech v síti.
ARP - zkratka pro Address Resolution Protocol (protokol pro rozlišení adres). Jeho úkolem je zjistit hardwarovou adresu hostitele ze známé adresy IP. ARP má několik typů: Reverzní ARP, proxy ARP, bezdůvodný ARP a inverzní ARP.

3.5.3 Transportní vrstva

Tato vrstva je obdobou transportní vrstvy modelu OSI. Je zodpovědná za komunikaci mezi koncovými body a bezchybné doručování dat. Chrání aplikace vyšší vrstvy před složitostí dat. Dva hlavní protokoly přítomné v této vrstvě jsou:

Protokol TCP (Transmission Control Protocol) - zajišťuje spolehlivou a bezchybnou komunikaci mezi koncovými systémy. Provádí sekvencování a segmentaci dat. Má také funkci potvrzování a řídí tok dat pomocí mechanismu řízení toku. Je to velmi efektivní protokol, ale díky těmto funkcím má velkou režii. Zvýšená režie vede ke zvýšení nákladů.

Protokol UDP (User Datagram Protocol) - na druhé straně žádné takové funkce neposkytuje. Je vhodným protokolem, pokud vaše aplikace nevyžaduje

spolehlivý přenos, protože je velmi úsporný. Na rozdíl od protokolu TCP, který je orientován na připojení, je protokol UDP bez připojení.

3.5.4 Aplikační vrstva

Tato vrstva plní funkce horních tří vrstev modelu OSI: Vrstvy aplikační, prezentační a relační. Je zodpovědná za komunikaci mezi uzly a řídí specifikace uživatelského rozhraní. Některé z protokolů přítomných v této vrstvě jsou: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD.

Popis některých vybraných protokolů této vrstvy:

HTTP a HTTPS – HTTP je zkratka pro Hypertext transfer protocol. Používá se v síti World Wide Web ke správě komunikace mezi webovými prohlížeči a servery. HTTPS je zkratka pro HTTP-Secure. Jedná se o kombinaci protokolu HTTP s protokolem SSL (Secure Socket Layer). Je účinný v případech, kdy prohlížeč potřebuje vyplňovat formuláře, přihlašovat se, ověřovat a provádět bankovní transakce.

SSH – SSH je zkratka pro Secure Shell. Jedná se o software pro emulaci terminálu podobný Telnetu. Důvodem, proč je SSH preferovanější, je jeho schopnost udržovat šifrované spojení. Vytváří zabezpečenou relaci přes připojení TCP/IP.

NTP – NTP je zkratka pro Network Time Protocol (síťový časový protokol). Používá se k synchronizaci hodin v našem počítači s jedním standardním zdrojem času. Je velmi užitečný v situacích, jako jsou bankovní transakce. Předpokládejme následující situaci bez přítomnosti NTP. Předpokládejme, že provádíte transakci, při níž váš počítač odečítá čas ve 14:30, zatímco server jej zaznamenává ve 14:28. To znamená, že se na serveru zobrazí čas ve 14:28. Server se může velmi vážně zhroutit, pokud není synchronizován. [4]

3.6 Schematické srovnání modelu TCP/IP a OSI:

Obrázek 3 - Srovnání TCP/IP a OSO/OSI Zdroj: vlastní zpracování

3.7 Rozdíl mezi TCP/IP a modelem OSI:

Tabulka 1 - Rozdíl ve vlastnostech ISO/OSI a TCP/IP Zdroj: vlastní zpracování

TCP/IP MODEL OSI A ROZDÍL MEZI TCP/IP A OSI	
TCP znamená Transmission Control Protocol (protokol řízení přenosu).	OSI označuje Open Systems Interconnection (standardizace v počítačových sítích).
TCP/IP má 4 vrstvy.	OSI má 7 vrstev.
TCP/IP je spolehlivější.	OSI je méně spolehlivé.
TCP/IP nemá příliš přísné hranice.	OSI má přísné hranice.
TCP/IP se řídí horizontálním přístupem.	OSI uplatňuje vertikální přístup.

TCP/IP používá jak relační, tak prezentační vrstvu v samotné aplikační vrstvě.	OSI používá různé vrstvy relační a prezentační.
TCP/IP vyvinul protokoly a poté model.	OSI vyvinulo model a pak protokol.
Transportní vrstva v TCP/IP nezajišťuje doručení paketů.	V modelu OSI zajišťuje transportní vrstva doručení paketů.
Síťová vrstva v modelu TCP/IP poskytuje pouze méně služeb pro připojení.	V modelu OSI poskytuje síťová vrstva jak služby zaměřené na méně spojení, tak služby zaměřené na spojení.
Protokoly v modelu TCP/IP nelze snadno nahradit.	Zatímco v modelu OSI jsou protokoly lépe pokryty a lze je snadno nahradit při změně technologie.

3.8 Network monitoring

V dnešním světě je pojem monitorování sítě rozšířen v celém odvětví IT. Monitorování sítě je kritický proces IT, při kterém jsou všechny síťové komponenty, jako jsou směrovače, přepínače, brány firewall, servery a virtuální počítače, monitorovány z hlediska poruch a výkonu a průběžně vyhodnocovány s cílem udržet a optimalizovat jejich dostupnost. Jedním z důležitých aspektů monitorování sítě je, že by mělo být proaktivní. Proaktivní vyhledávání problémů s výkonem a úzkých míst pomáhá identifikovat problémy v počáteční fázi. Účinné proaktivní monitorování může zabránit výpadkům nebo poruchám sítě.

Chybná síťová zařízení ovlivňují výkon sítě. Včasnou detekcí lze tento problém eliminovat, a proto je monitorování síťových zařízení nesmírně důležité. Při efektivním monitorování sítě je prvním krokem identifikace zařízení a souvisejících výkonnostních metrik, které je třeba monitorovat. Druhým krokem je určení intervalu monitorování. Zařízení, jako jsou stolní počítače a tiskárny, nejsou kritická

a nevyžadují časté monitorování, zatímco servery, směrovače a přepínače plní kritické obchodní úlohy, ale zároveň mají specifické parametry, které lze selektivně monitorovat.

3.8.1 Proč použít network monitoring?

Proč zavést do naší podnikové sítě network monitoring může mít hned několik důvodů. Některé z nich si zde vysvětlíme.

- **Zlepšený výkon sítě:** Monitorování sítě může pomoci identifikovat a řešit problémy, které mohou mít vliv na výkon sítě, jako jsou úzká místa, latence a ztráta paketů. To může pomoci zajistit, aby síť fungovala efektivně a účinně.
- **Zvýšená bezpečnost:** Monitorování sítě může pomoci identifikovat a předcházet bezpečnostním hrozbám, jako jsou úniky dat, útoky malwaru a neoprávněný přístup do sítě. To může pomoci chránit síť a data, která jsou v ní uložena.
- **Lepší využití zdrojů:** Díky analýze síťového provozu a vzorců využití může monitorování sítě pomoci identifikovat příležitosti k optimalizaci využití zdrojů, jako je šířka pásma a úložiště. To může pomoci snížit náklady a zvýšit efektivitu.
- **Včasné odhalení problémů:** Monitorování sítě může pomoci identifikovat problémy s konkrétními zařízeními nebo aplikacemi v síti dříve, než se z nich stanou závažné problémy. To může pomoci zabránit výpadkům a udržet hladký chod sítě
- **Lepší dodržování předpisů:** V některých odvětvích mohou existovat regulační požadavky týkající se monitorování sítě. Monitorování sítě může pomoci zajistit, aby organizace tyto požadavky splňovala, a v případě potřeby může poskytnout potřebnou dokumentaci.

3.8.2 Možnosti network monitoringu

Existuje několik možností monitorování sítě, včetně:

- **Monitorování výkonu sítě:** Tento typ monitorování se zaměřuje na výkonnost sítě a jejích různých součástí, jako jsou směrovače, přepínače a servery. Může pomoci identifikovat problémy, jako jsou úzká místa, latence a ztráta paketů."
- **Monitorování bezpečnosti sítě**: Tento typ monitorování pomáhá identifikovat a předcházet bezpečnostním hrozbám, jako jsou úniky dat, útoky malwaru a neoprávněný přístup do sítě.
- **Monitorování síťového provozu:** Tento typ monitorování zahrnuje analýzu dat přenášených po síti s cílem pochopit vzorce používání, identifikovat trendy a optimalizovat výkon.
- **Monitorování dostupnosti sítě:** Tento typ monitorování zajišťuje, aby byla síť vždy dostupná a správně fungovala. Může upozornit správce na problémy s dostupností sítě.
- **Monitorování síťových zařízení:** Tento typ monitorování se zaměřuje na stav a výkon jednotlivých zařízení v síti, jako jsou směrovače, přepínače a servery. Může pomoci identifikovat problémy s konkrétními zařízeními a přijmout nápravná opatření.
- **Monitorování síťových aplikací:** Tento typ monitorování se zaměřuje na výkon a dostupnost konkrétních aplikací běžících v síti, jako jsou e-mailové a webové servery a databáze.
- **Monitorování síťových událostí:** Tento typ monitorování zahrnuje sledování konkrétních událostí nebo činností v síti, jako jsou změny konfigurace, přihlášení uživatelů nebo přenosy dat. Může pomoci identifikovat neobvyklé nebo podezřelé aktivity.
- **Monitorování syslog zpráv:** Tento typ monitorování zahrnuje sledování zpráv, které jsou vypisovány přímo zařízením, které je monitorováno. Tyto zprávy se pak pomocí SNMP nebo ICMP odesílají na monitorovací server.

3.9 Network change managment

Network change managment je proces, kterým organizace standardizují způsob provádění změn v síti. Cílem je vytvořit takový přístup, aby provádění nezbytných změn síťových zařízení co nejméně narušovalo stávající systémy. Change management v network monitoringu je důležitý pro zajištění bezpečnosti, spolehlivosti a výkonu sítě. Pomáhá zajistit, že změny v síti jsou provedeny řádně a bez zbytečného rizika pro síť nebo její uživatele.

Změny v síti mohou být proaktivní snahou o zlepšení sítě nebo reaktivní reakcí na problémy v systému. Proces řízení síťových změn má zajistit standardizované přístupy a snížit četnost a dopad souvisejících incidentů způsobených změnou, aby změny byly rychlé a efektivní. Tyto základní principy platí pro jakýkoli druh change managmentu. Protože change managment v síti úzce souvisí se správou konfigurace sítě, proces řízení změn v síti se více zaměřuje na monitorování a správu změn konfigurace než na správu aktualizací a oprav softwaru. Konfigurace sítě definují její tok, provoz a řízení. Tyto konfigurace mají zásadní význam pro fungování součástí sítě. Změny konfigurace mohou být autorizované nebo neautorizované a mohou buď fungovat, nebo způsobovat chyby. Change managment v síti pomáhá zajistit, aby provedené změny konfigurace byly autorizované a fungovaly bez problémů. Stejně jako u běžného change managmentu je cílem řízení síťových změn nulový výpadek a žádné přerušení funkcí síťového systému. [5]

3.9.1 ITIL (Information Technology Infrastructure Library)

ITIL je soubor osvědčených postupů pro správu a poskytování služeb IT. Poskytuje rámec, kterým se organizace mohou řídit, aby zlepšily účinnost a efektivitu svých IT operací.

ITIL vyvinul a spravuje Úřad pro vládní obchod (Office of Government Commerce, OGC) vlády Spojeného království. Používají jej organizace po celém světě ke zlepšení poskytování a řízení služeb IT a je všeobecně uznáván jako přední postup v této oblasti. ITIL se skládá z řady knih, které poskytují návod k různým aspektům řízení služeb IT, včetně strategie, návrhu, přechodu, provozu a zlepšování služeb.

ITIL je navržen tak, aby byl flexibilní a přizpůsobivý, a lze jej upravit tak, aby vyhovoval konkrétním potřebám a cílům organizace. Často se používá ve spojení s dalšími rámci, jako jsou COBIT a TOGAF, a poskytuje tak komplexní přístup ke správě služeb IT. Některé texty už zde byly citovány, a některé budou.[6]

3.10 Network Incident

Incident v systému monitorování sítě může znamenat jakoukoli neočekávanou nebo nežádoucí událost, ke které dojde v systému nebo v monitorované síti. Může jít o problémy s hardwarem nebo softwarem, narušení dat nebo jiné bezpečnostní hrozby. Může se také jednat o problémy se samotným monitorováním, například výpadek systému nebo problémy s výkonem.

Pro řešení incidentu v systému monitorování sítě je důležité nejprve identifikovat hlavní příčinu problému. To může zahrnovat shromažďování informací z různých zdrojů, jako jsou protokoly, systémová upozornění nebo hlášení od správců sítě. Po zjištění hlavní příčiny lze podniknout kroky k odstranění problému a zabránit výskytu podobných incidentů v budoucnu. To může zahrnovat aplikaci záplat nebo aktualizací, konfiguraci bezpečnostních opatření nebo zavedení nových monitorovacích postupů. [6]

3.10.1 Kroky k vyřešení incidentu

Pokud dojde k incidentu v systému monitorování sítě, je možné podniknout několik kroků k vyřešení problému:

1. **Shromáždění informací:** Prvním krokem je shromáždit co nejvíce informací o incidentu. To může zahrnovat přezkoumání protokolů, systémových výstrah a zpráv od správců sítě.
2. **Identifikace hlavní příčiny:** Jakmile shromáždíte dostatek informací, je důležité pokusit se identifikovat hlavní příčinu incidentu. To vám pomůže pochopit, co problém způsobilo a jak jej odstranit.
3. **Vypracování akčního plánu:** Jakmile víte, co incident způsobilo, můžete vypracovat akční plán, jak problém vyřešit. Ten může zahrnovat aplikaci záplat nebo aktualizací, konfiguraci bezpečnostních opatření nebo zavedení nových monitorovacích postupů.

4. **Implementace plánu:** Dodržujte plán opatření, který jste vypracovali, abyste problém odstranili a zabránili podobným incidentům v budoucnu.
5. **Komunikace se zúčastněnými stranami:** Je důležité informovat zúčastněné strany o incidentu a o všech opatřeních, která jsou přijímána k jeho řešení. To může zahrnovat komunikaci se zaměstnanci, zákazníky nebo dalšími stranami, kterých se incident týká.
6. **Zhodnocení incidentu a poučení se z něj:** Po vyřešení incidentu je důležité přezkoumat, co se stalo, a poučit se z této zkušenosti. To vám pomůže identifikovat případné nedostatky ve vašem monitorovacím systému a přijmout opatření, která v budoucnu zabrání výskytu podobných incidentů.

3.11 Budoucnost network monitoringu

Je obtížné předpovědět přesný budoucí vývoj monitorování sítí, protože bude záviset na řadě faktorů, včetně technologického pokroku, průmyslových trendů a konkrétních potřeb a cílů organizací.

Je však pravděpodobné, že monitorování sítí se bude i nadále vyvíjet a časem se stane sofistikovanějším. Mezi potenciální vývojové trendy, které mohou ovlivnit budoucnost monitorování sítí, náleží:

- **Zvýšená automatizace:** Nástroje a systémy pro monitorování sítí se mohou více automatizovat, což umožní účinnější a efektivnější monitorování sítí a systémů. Pokročilá analytika a algoritmy strojového učení mohou například sloužit k identifikaci vzorců a trendů v síťových datech a upozornit správce na potenciální problémy dříve, než se z nich stanou problémy velké. Automatizace může také umožnit rychlejší a přesnější reakci na incidenty, což pomůže minimalizovat prostoje a narušení provozu.
- **Větší integrace:** Monitorování sítě může být těsněji integrováno s dalšími IT systémy a procesy, jako je správa incidentů a bezpečnostní operace. To může umožnit plynulejší a koordinovanější reakce na

problémy a události a zlepšit celkovou efektivitu a účinnost provozu IT.

- **Zvýšená bezpečnost:** Monitorování sítě se může více zaměřit na bezpečnost a detekci incidentů a zahrnovat pokročilou analytiku a strojové učení k identifikaci potenciálních hrozeb a zranitelností. To může organizacím pomoci proaktivně odhalovat narušení bezpečnosti a předcházet mu, stejně jako rychleji a efektivněji reagovat na incidenty, pokud k nim dojde.
- **Zlepšená uživatelská zkušenost:** Nástroje a systémy pro monitorování sítí se mohou stát uživatelsky přívětivějšími a intuitivnějšími, což usnadní jejich používání a pochopení pro netechnické uživatele. To může zahrnovat vývoj intuitivnějších rozhraní a začlenění funkcí, jako je kontextová nápověda a pomoc při zavádění.
- **Monitorování v cloudu:** Nástroje a systémy pro monitorování sítí mohou přejít na model založený na cloudu, což umožní flexibilnější a škálovatelnější monitorování sítí a systémů. To může organizacím umožnit snadnější monitorování a správu distribuovaných a vzdálených sítí a také využití úspor z rozsahu a dalších výhod cloud computingu.
- **Integrace internetu věcí (IoT):** Monitorování sítí může být těsněji integrováno s internetem věcí (IoT), což umožní monitorovat širokou škálu připojených zařízení a systémů. To může organizacím umožnit získat komplexnější přehled o svých sítích a systémech a také rychleji a efektivněji identifikovat a řešit problémy.
- **Větší využívání umělé inteligence (AI) a strojového učení:** Nástroje a systémy pro monitorování sítí mohou zahrnovat pokročilejší funkce umělé inteligence a strojového učení, což umožní sofistikovanější analýzu a předvídání chování sítě. To může organizacím umožnit proaktivně identifikovat a řešit problémy dříve, než se stanou závažnými, a zlepšit tak spolehlivost a výkonnost jejich sítí a systémů.

3.12 Programy dostupné pro network monitoring

Pro monitorování sítě je k dispozici celá řada programů a nástrojů, od jednoduchých nástrojů až po složité systémy na podnikové úrovni. Mezi příklady programů a nástrojů, které se běžně používají pro monitorování sítě, náleží sem:

- **Software pro monitorování sítě:** Tento typ softwaru je určen speciálně pro monitorování a správu sítí. Může poskytovat celou řadu funkcí a možností, například monitorování výkonu, upozorňování a vytváření zpráv. Mezi příklady softwaru pro monitorování sítě patří:
  → *SolarWinds Network Performance Monitor*
  → *Nagios*
  → *PRTG Network Monitor*
- **Software pro monitorování systému:** Tento typ softwaru je určen k monitorování a správě výkonu jednotlivých systémů, jako jsou servery nebo pracovní stanice. Může poskytovat funkce, jako je sledování výkonu, upozorňování a vytváření zpráv. Příklady softwaru pro monitorování systému:
  → *SolarWinds Server & Application Monitor*
  → *Zabbix*
  → *Datadog.*
- **Síťové analyzátory a analyzátory protokolů:** Tyto nástroje jsou určeny k analýze síťového provozu a identifikaci problémů nebo problémů s výkonem sítě. Mohou poskytovat funkce, jako je zachytávání paketů, analýza protokolů a analýza provozu. Příklady síťových analyzátorů a analyzátorů protokolů:
  → Wireshark
  → NetworkMiner
  → NetFlow Analyzer
- **Nástroje pro mapování a zjišťování sítě:** Tyto nástroje jsou určeny k vytváření map topologie sítě a k identifikaci zařízení a systémů v síti. Mohou poskytovat funkce, jako je automatické zjišťování zařízení, mapování síťových připojení a identifikace typu zařízení a

operačního systému. Mezi nástroje pro mapování a zjišťování sítě patří například:

→ SolarWinds Network Topology Mapper
→ Spiceworks Network Mapper
→ Lansweeper

3.12.1 PRTG Network Monitor

PRTG Network Monitor je softwarový program určený pro monitorování a správu sítí. Poskytuje řadu funkcí a možností, včetně monitorování výkonu, upozorňování a vytváření zpráv. Zde jsou uvedeny některé potenciální výhody a nevýhody používání programu PRTG Network Monitor:

Výhody:

⊕ Široká škála možností monitorování: PRTG Network Monitor dokáže monitorovat širokou škálu síťových zařízení a protokolů, včetně směrovačů, přepínačů, serverů, pracovních stanic a dalších. Je možnost monitorovat až do 100 senzorů zdarma.

⊕ Přizpůsobitelné upozorňování: PRTG Network Monitor umožňuje uživatelům konfigurovat vlastní výstrahy na základě konkrétních podmínek a prahových hodnot, což pomáhá zajistit rychlou identifikaci a řešení potenciálních problémů.

⊕ Podrobné hlášení: PRTG Network Monitor poskytuje podrobné reporty o výkonu sítě a dalších metrikách, které pomáhají organizacím identifikovat trendy a oblasti pro zlepšení.

⊕ Škálovatelnost: PRTG Network Monitor je navržen tak, aby byl škálovatelný, což mu umožňuje přizpůsobit se potřebám organizací různých velikostí a složitosti.

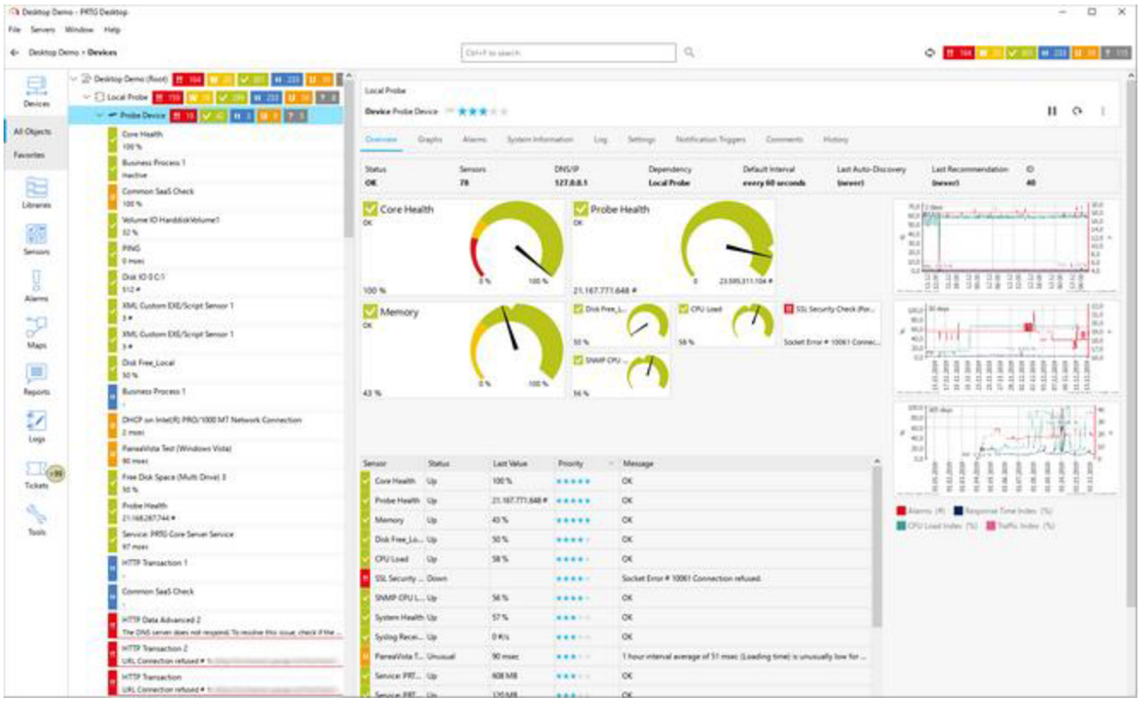
Nevýhody:

⊖ Složitost: Zejména pro uživatele, kteří nejsou obeznámeni s monitorováním sítě, může být nastavení a konfigurace nástroje PRTG Network Monitor složitá.

- Náklady: Problémem je, že síť PRTG je schopna zajistit, aby se v budoucnu mohla rozšířit: PRTG Network Monitor je komerční produkt a jeho nákup a údržba mohou být pro organizace nákladné.
- Kompatibilita: PRTG Network Monitor nemusí být kompatibilní se všemi typy síťových zařízení a protokolů a pro podporu určitých typů zařízení může vyžadovat další software nebo konfiguraci.

Shrnutí:

Celkově lze říct, že PRTG Network Monitor je výkonný a funkčně bohatý nástroj pro monitorování sítě, který může být užitečný pro organizace s komplexními potřebami monitorování sítě. Nemusí však být nejlepší volbou pro všechny organizace, a to kvůli faktorům, jako jsou náklady, složitost a kompatibilita. [7]



Obrázek 4 - Program PRTG Zdroj: upraveno dle [7]

3.12.2 SolarWinds Network Performance Monitor

SolarWinds je softwarová společnost, která nabízí řadu programů a nástrojů pro správu IT včetně monitorování sítě. Zde jsou uvedeny některé potenciální výhody a nevýhody používání produktů SolarWinds pro monitorování sítě:

Výhody:

- ⊕ Široká škála možností monitorování: Společnost SolarWinds nabízí řadu produktů pro monitorování sítě, včetně Network Performance Monitor, Network Topology Mapper a Network Configuration Manager. Tyto produkty jsou schopny monitorovat širokou škálu síťových zařízení a protokolů, včetně směrovačů, přepínačů, serverů, pracovních stanic a dalších.
- ⊕ Přizpůsobitelné upozorňování: Mnoho produktů SolarWinds nabízí přizpůsobitelné funkce výstrah, které uživatelům umožňují konfigurovat výstrahy na základě konkrétních podmínek a prahových hodnot. To pomáhá zajistit rychlou identifikaci a řešení potenciálních problémů.
- ⊕ Podrobný reporting: Mnoho produktů SolarWinds poskytuje podrobné reporty o výkonu sítě a dalších metrikách, které pomáhají organizacím identifikovat trendy a oblasti pro zlepšení.
- ⊕ Škálovatelnost: Produkty SolarWinds jsou navrženy tak, aby byly škálovatelné, což jim umožňuje přizpůsobit se potřebám organizací různých velikostí a složitosti.

Nevýhody:

- ⊖ Náklady: Produkty SolarWinds jsou komerční produkty a jejich nákup a údržba mohou být pro organizace nákladné.
- ⊖ Složitost: Některé produkty SolarWinds mohou být složité na nastavení a konfiguraci, zejména pro uživatele, kteří nejsou obeznámeni s monitorováním sítě.

- Kompatibilita: Produkty SolarWinds nemusí být kompatibilní se všemi typy síťových zařízení a protokolů a pro podporu určitých typů zařízení mohou vyžadovat další software nebo konfiguraci.

Obrázek 5 - Program SolarWinds Network Performance Monitor Zdroj: upraveno dle [8]

Shrnutí:

Celkově lze říct, že společnost SolarWinds je uznávaným a funkčně bohatým poskytovatelem nástrojů a programů pro monitorování sítě. Její produkty však podobně jako u PRTG nemusí být nejvhodnější pro všechny organizace, a to kvůli faktorům, jako jsou náklady, složitost a kompatibilita. Menší firmy pro tyto programy své využití nenajdou. [8]

3.12.3 Nagios

Nagios je open-source program pro monitorování sítě, který je hojně využíván organizacemi všech velikostí. Zde jsou uvedeny některé potenciální výhody a nevýhody používání programu Nagios pro monitorování sítě:

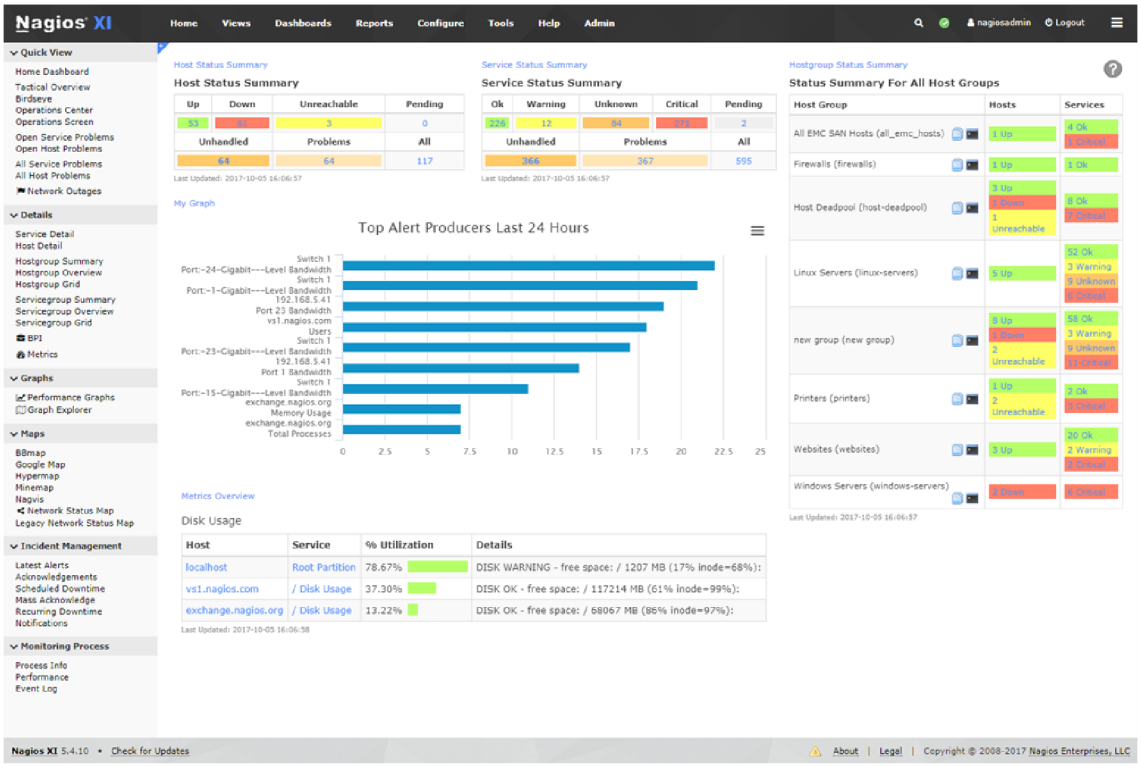
Výhody:

- ⊕ Široká škála možností monitorování: Nagios je schopen monitorovat širokou škálu síťových zařízení a protokolů, včetně směrovačů, přepínačů, serverů, pracovních stanic a dalších.
- ⊕ Přizpůsobitelné upozorňování: Nagios umožňuje uživatelům konfigurovat vlastní výstrahy na základě konkrétních podmínek a prahových hodnot, což pomáhá zajistit rychlou identifikaci a řešení potenciálních problémů.
- ⊕ Podrobný reporting: Nagios poskytuje podrobné reporty o výkonu sítě a dalších metrikách, které pomáhají organizacím identifikovat trendy a oblasti pro zlepšení.
- ⊕ Otevřený zdrojový kód: Nagios je open-source software, který může kdokoli volně používat a upravovat. Díky tomu může být jeho používání a údržba pro organizace cenově dostupnější ve srovnání s komerčními nástroji pro monitorování sítě.

Nevýhody:

- ⊖ Složitost: Nagios může být složitý na nastavení a konfiguraci, zejména pro uživatele, kteří nejsou obeznámeni s monitorováním sítě.
- ⊖ Omezená podpora: Nagios jako program s otevřeným zdrojovým kódem nenabízí stejnou úroveň podpory jako komerční produkty. Uživatelé se možná budou muset spolehnout na komunitní fóra nebo jiné zdroje pomoci.

- Kompatibilita: Nagios nemusí být kompatibilní se všemi typy síťových zařízení a protokolů a pro podporu některých typů zařízení může vyžadovat další software nebo konfiguraci.



Obrázek 6 - Program Nagios Zdroj: upraveno dle [9]

Shrnutí:

Celkově je Nagios výkonný a funkčně bohatý nástroj pro monitorování sítě, který může být užitečný pro organizace s komplexními potřebami monitorování. Nemusí však být nejlepší volbou pro všechny organizace, a to kvůli faktorům, jako je složitost, kompatibilita a podpora. [9]

3.12.4 Porovnání všech tří programů pro střední firmu

Je obtížné určit, který z těchto tří programů – PRTG Network Monitor, SolarWinds a Nagios – je pro středně velkou firmu tou nejlepší volbou, protože při výběru nejvhodnějšího řešení budou hrát významnou roli konkrétní potřeby a cíle společnosti. Zde je několik faktorů, které je třeba při porovnávání těchto programů zvážit:

Možnosti monitorování:

Všechny tyto tři programy nabízejí širokou škálu možností monitorování, ale mohou se lišit z hlediska konkrétních typů zařízení a protokolů, které podporují. Pro určení nejvhodnějšího programu je důležité vzít v úvahu konkrétní potřeby a cíle společnosti v oblasti monitorování.

Upozorňování a hlášení:

Všechny tři programy nabízejí přizpůsobitelné upozornění a podrobné hlášení, ale mohou se lišit z hlediska konkrétních funkcí a možností, které nabízejí. Je důležité projít si možnosti upozorňování a vykazování jednotlivých programů, aby bylo možné určit, který z nich je nejvhodnější.

Náklady:

Náklady na tyto programy mohou být významným faktorem při rozhodování o tom, který z nich je nejlepší volbou. PRTG Network Monitor a SolarWinds jsou komerční produkty, které mohou být dražší než Nagios, což je program s otevřeným zdrojovým kódem. Je však důležité zvážit dlouhodobé náklady jednotlivých programů, včetně nákladů na údržbu a podporu, aby bylo možné určit, který z nich je nákladově nejefektivnější.

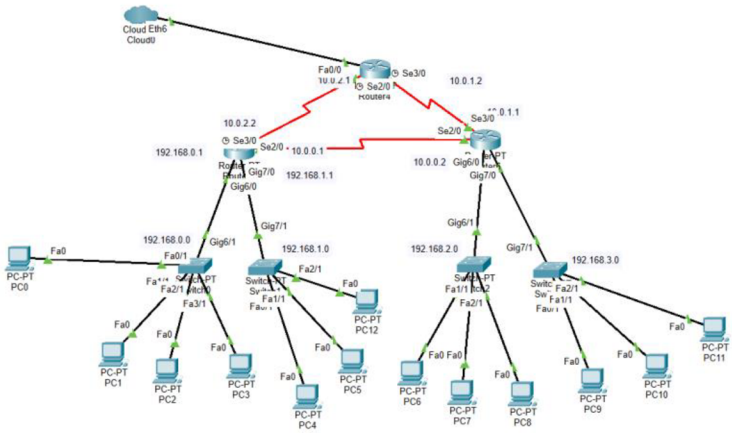
Kompatibilita a integrace:

Je důležité zvážit kompatibilitu těchto programů se zařízeními a systémy, které již společnost používá, a také jejich schopnost integrace s dalšími nástroji a systémy. To může pomoci zajistit, že program bude schopen efektivně monitorovat síť a systémy společnosti.

4 Praktická část – návodný tutoriál

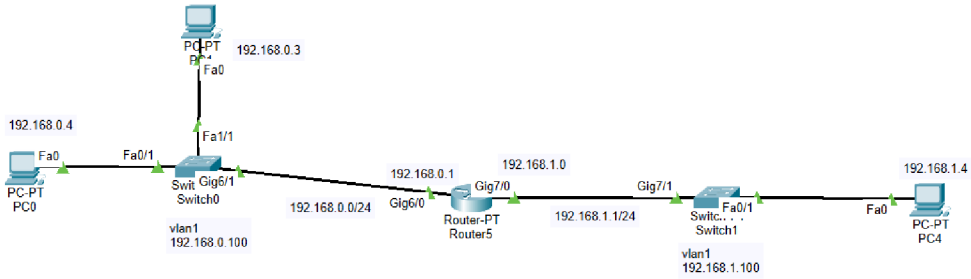
4.1 Návrh/modelování počítačové sítě

Pro návrh počítačové sítě k monitorování byl použit nástroj Cisco Packet Tracer - Network Simulation Tool od společnosti Cisco Systems.



Obrázek 7 - Topologie sítě Zdroj: vlastní zpracování

V síti byly použity 2 topologie. Kruhová topologie byla využita pro zapojení routerů. Každý router měl dvě sériové rozhraní, která byla propojena s rozhraními sousedních routerů. Tato konfigurace umožňuje vytvořit redundanci a zlepšit dostupnost sítě. Pokud dojde k výpadku jednoho z routerů, zbývající dva routery si stále mohou vyměňovat informace. Síť se poté rozrůstala jako stromová topologie, aby se simulovalo odvětví ve společnosti, které potřebuje oddělenou kolizní doménu a v ní určitý počet počítačů připojených pomocí ethernetového kabelu. Vzhledem k opakujícím se nastavujícím parametrům pro ostatní prvky byla k monitoringu využita pouze jedna větev.



Obrázek 8 - Topologie k monitoringu Zdroj: vlastní zpracování

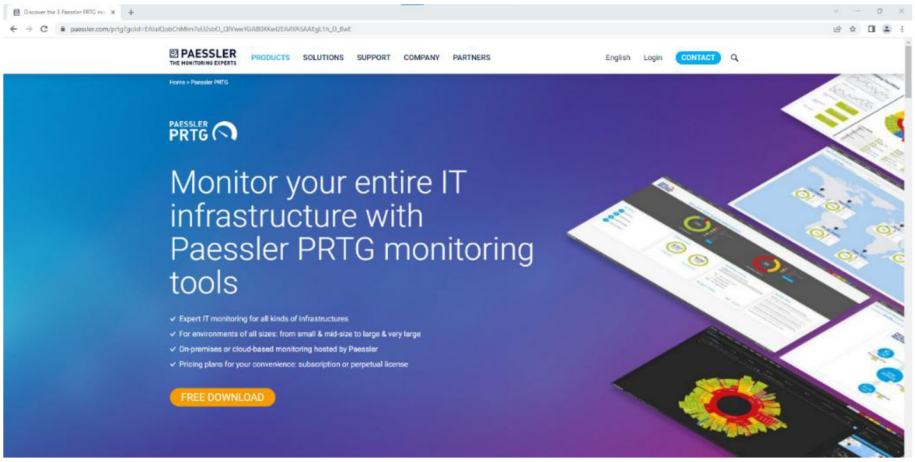
Topologie měla 2 sítě: 192.168.0.1/24 a druhou 192.168.1.0/24. Síť byla monitorována ze zařízení PC1 s IP adresou 192.168.0.3, maskou sítě: 255.255.255.0 a výchozí branou na router 192.168.0.1.

4.2 Fyzická konfigurace prvků

Konfigurace switchů byla obdobná. První switch SW1 obsahuje 24 portů FastEthernet a 2 porty GigabitEthernet. Vlany jsou přidělovány automaticky. Switch používá protokol Spanning-Tree s režimem pvst a rozšiřuje systémové ID. Switch má jednu rozhraní Vlan s IP adresou 192.168.0.100 a maskou sítě 255.255.255.0. Výchozí brána je 192.168.0.1. Switch má zapnutou HTTP a HTTPS službu, i když využita v tomto modelu nebude. Byla použita SSH verze 2, protokol SNMP a služba syslog. Konfigurace obsahuje také příkazy pro logování, správu uživatelů a port security. Příkladná konfigurace SW1 je umístěna v příloze.

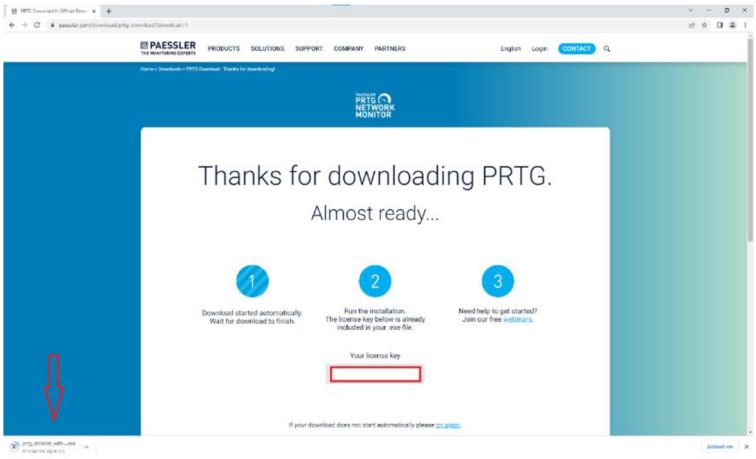
4.3 Instalace PRTG

Poslední dostupná verze PRTG je k dispozici ke stažení a další aktualizace budou instalovány automaticky. Odkaz na stažení je zde: https://www.paessler.com/manuals/prtg/download.



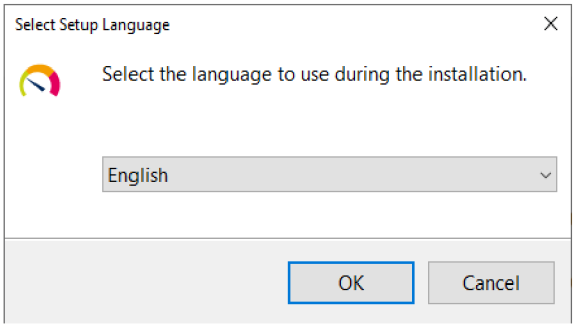
Obrázek 9 - Stránka PRTG Zdroj: vlastní zpracování

Trial verze je k dispozici na 30 dní, po vypršení se verze stává zdarma s omezením na 100 senzorů. Při začátku stahování bude zobrazena nabídka licence.



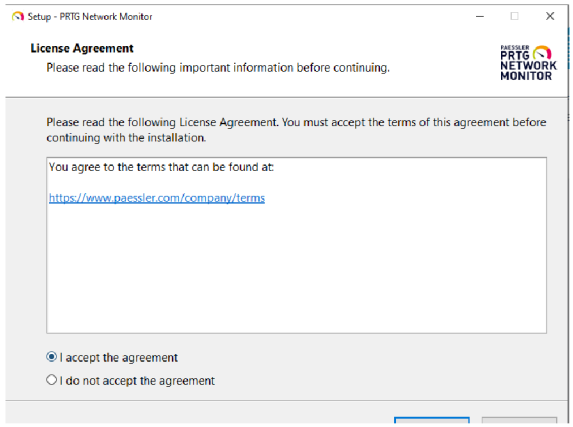
Obrázek 10 - Stažení PRTG Zdroj: vlastní zpracování

Instalace PRTG je prováděna podobně jako u ostatních aplikací založených na Windows. Stažený soubor se otevře kliknutím na "run", což spustí instalační program. Pro instalaci jsou potřeba administrátorská práva. Po potvrzení instalace se spustí samotná instalace, kde se nejprve vybere jazyk.

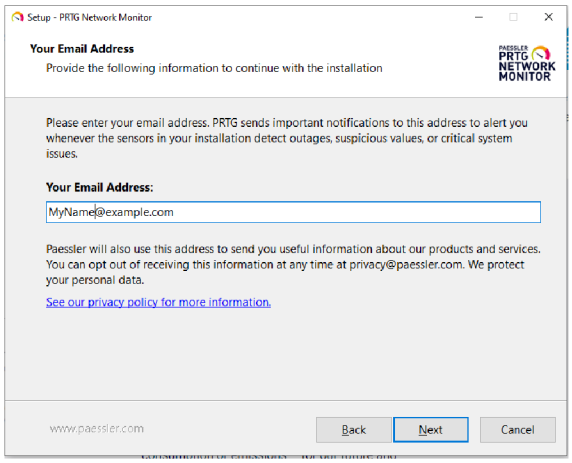


Obrázek 11 - Jazyk aplikace Zdroj: vlastní zpracování

Další okno odkazuje na obchodní podmínky a podmínky užívání aplikace.

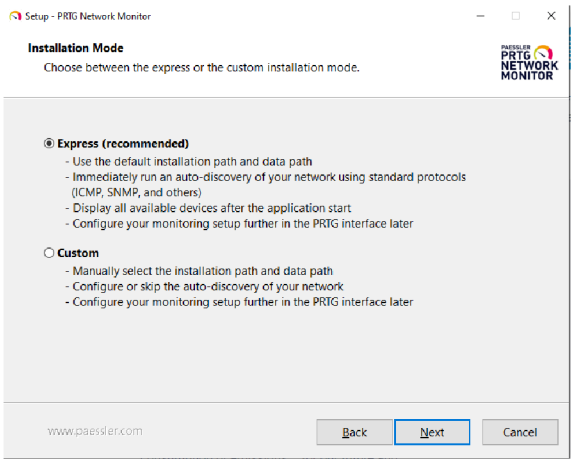


Obrázek 12 - Obchodní podmínky Zdroj: vlastní zpracování



Obrázek 13 - Zadání emailu Zdroj: vlastní zpracování

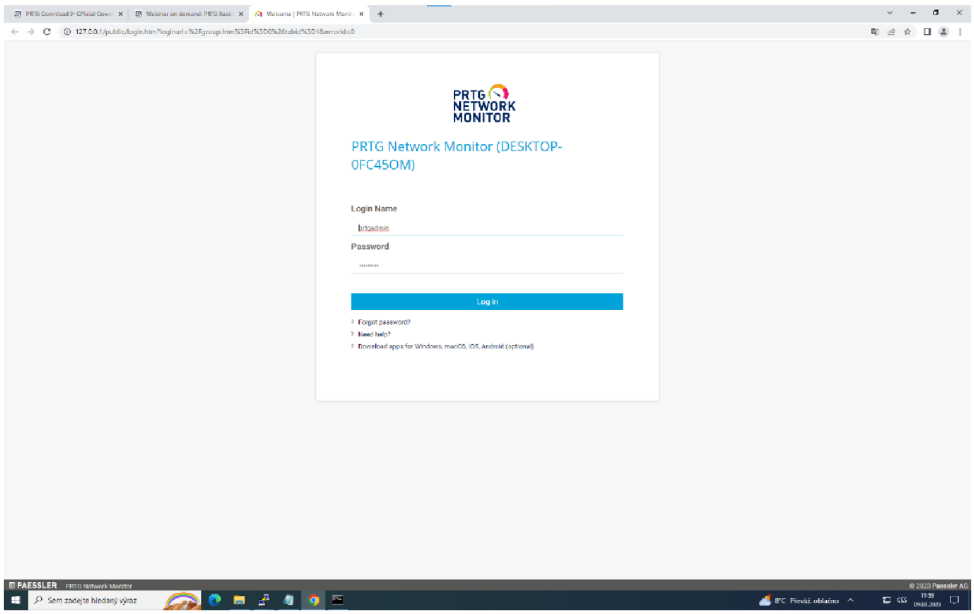
Po odsouhlasení podmínek se dostaneme k dialogovému oknu pro zadání e-mailu. Tento e-mail bude použit pro oznámení o sledované síti.



Obrázek 14 - Instalační mód Zdroj: vlastní zpracování

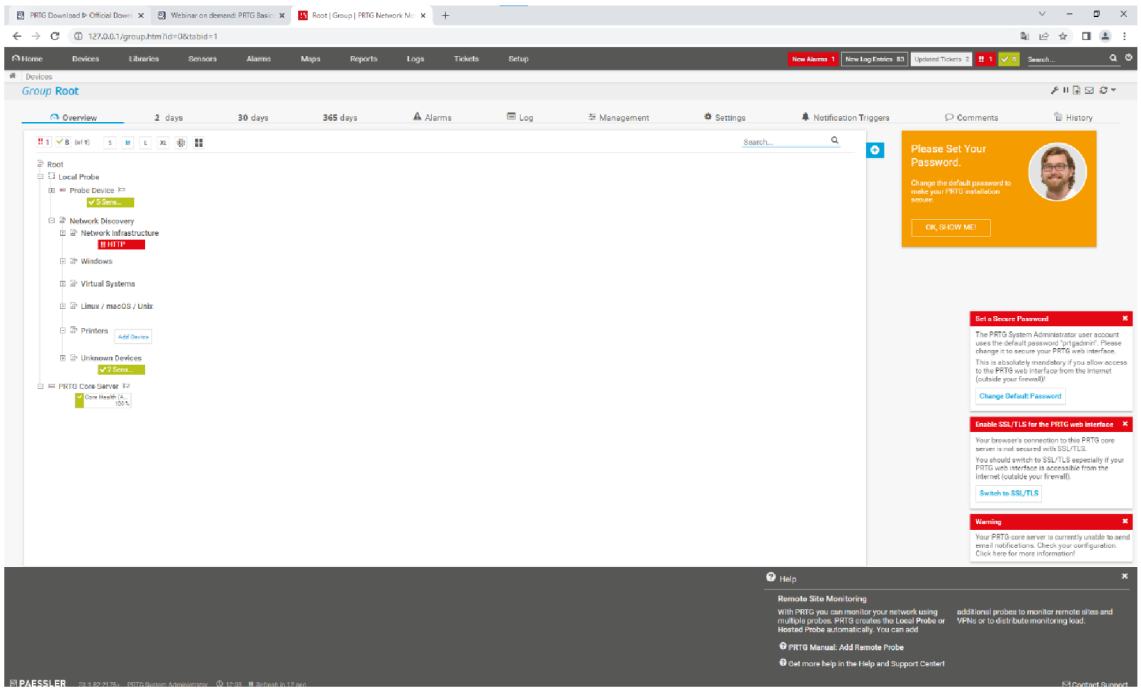
Instalační mód má dvě možnosti. Express nabídne předem připravenou infrastrukturu, do které vám pomocí funkce auto-discovery přidá prvky objevené v dané síti. Defaultním režimem je Express, který umožňuje pozdější úpravy všech informací. Druhým řešením je Custom, ve kterém je možností nastavit si instalační cestu, nakonfigurovat auto-discovery a celkové interface a setup PRTG. V práci je zvolen mód Express.

Po úspěšné instalaci se v prohlížeči otevře okno, kde bude vyžadováno jméno a heslo pro přihlášení. Při prvním přihlášení je nutné změnit heslo.



Obrázek 15 - Přihlášení do PRTG Zdroj: vlastní zpracování

Po přihlášení se dostanete do grafického rozhraní aplikace PRTG, které nabízí tutoriál od PRTG pro první orientaci. Hierarchie zařízení se nachází ve stromové hierarchii a lze ji vytvořit a upravit podle potřeb. Tato hierarchie je definována jako defaultní, protože bylo použito Express nastavení při instalaci.

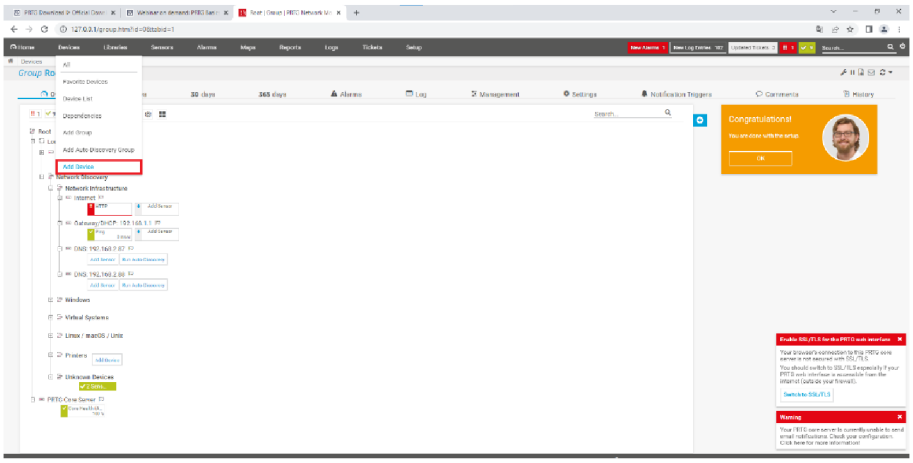


Obrázek 16 - Defaultní nastavení Zdroj: vlastní zpracování

4.4 Monitoring sítě

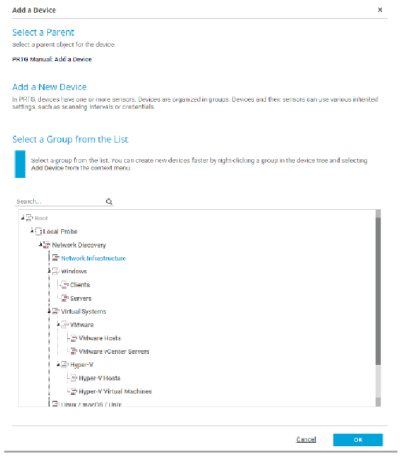
4.4.1 Dostupnosti sítě a prvků

Do PRTG nejdříve musí být přidány prvky jako tak samotné. Přes naváděcí menu, kde je popsáno Devices se nachází Add Device neboli přidání nového zařízení. Před přidáním je žádoucí si vytvořit si nového rodiče. Pro jednoduché monitorovací sítě ovšem tato struktura není nutná k rozšiřování.



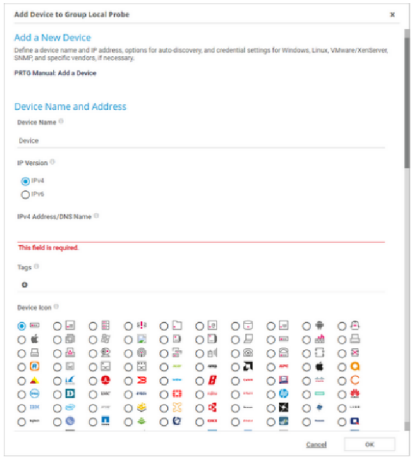
Obrázek 17 - Přidání nového prvku Zdroj: vlastní zpracování

Při kliknutí se objeví tabulka pro vybrání rodiče tohoto prvku. Prvek byl předán

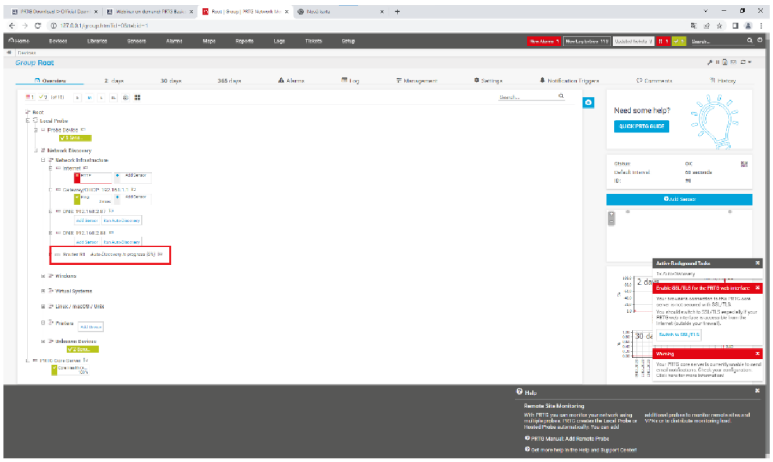


Obrázek 18 - Přidání zařízení rodiči Zdroj: vlastní

rodiči Network infrastructure a byl zaveden pod síťovou infrastrukturu. Zařízení bylo pojmenováno a byla přidána IP adresa pro komunikaci s monitorovacím serverem. U daného prvku byl zapnutý systém auto-discovery.

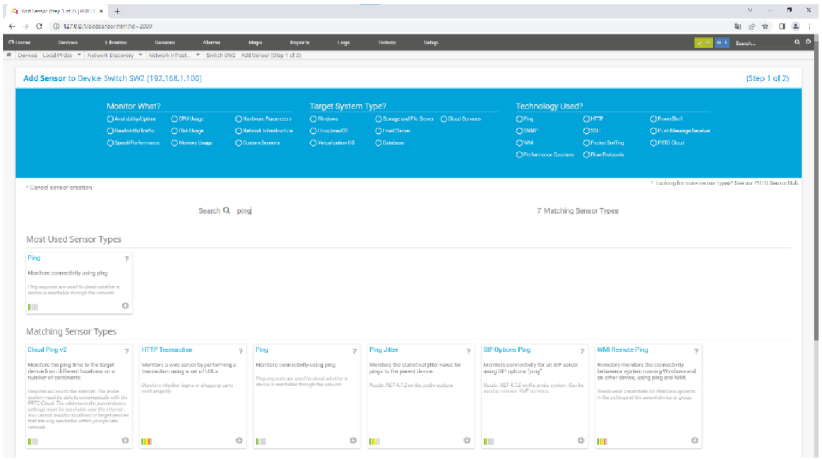


Obrázek 19 - Pojmenování zařízení Zdroj: vlastní zpracování



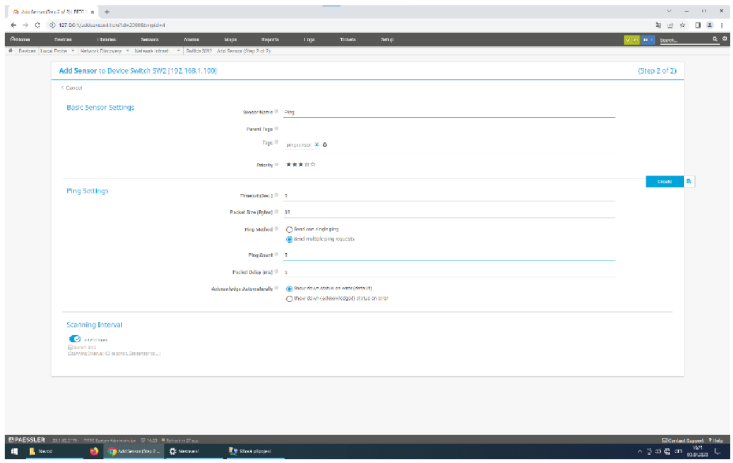
Obrázek 20 - Auto Discovery Zdroj: vlastní zpracování

Nyní bylo zařízení úspěšně přidáno. Jedno z mnoha senzorů, které byly přidány je PING. Tento sensor v návaznosti v textu na teoretickou část posílá packety a získává povědomí o tom, zda daný prvek dostupný je či nikoliv. Pokud Auto Discovery použito z určitých důvodů nebylo. Postup přidání senzoru PING je následující. Nejprve zvolte "Device Tree" a vyberte zařízení, ke kterému chcete přidat sensor Ping. Klikněte pravým tlačítkem myši na zařízení a vyberte "Add Sensor" a poté "Ping".



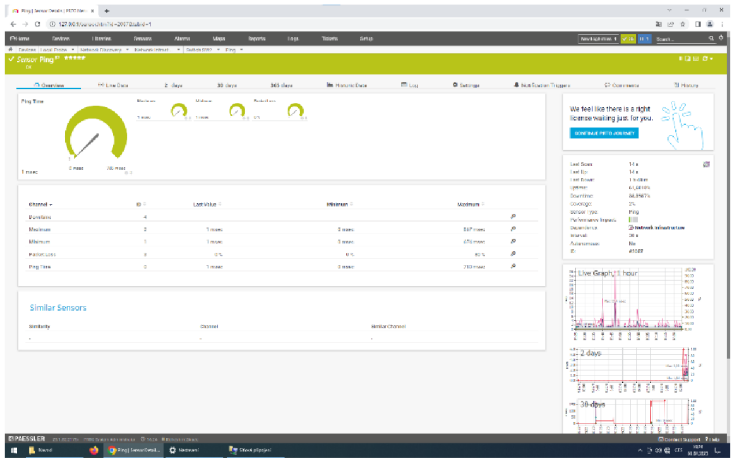
Obrázek 22 – Přidání senzoru Zdroj: vlastní zpracování

Následně stačí zadat název sensoru a vybrat typ IP adresy. Můžete také specifikovat



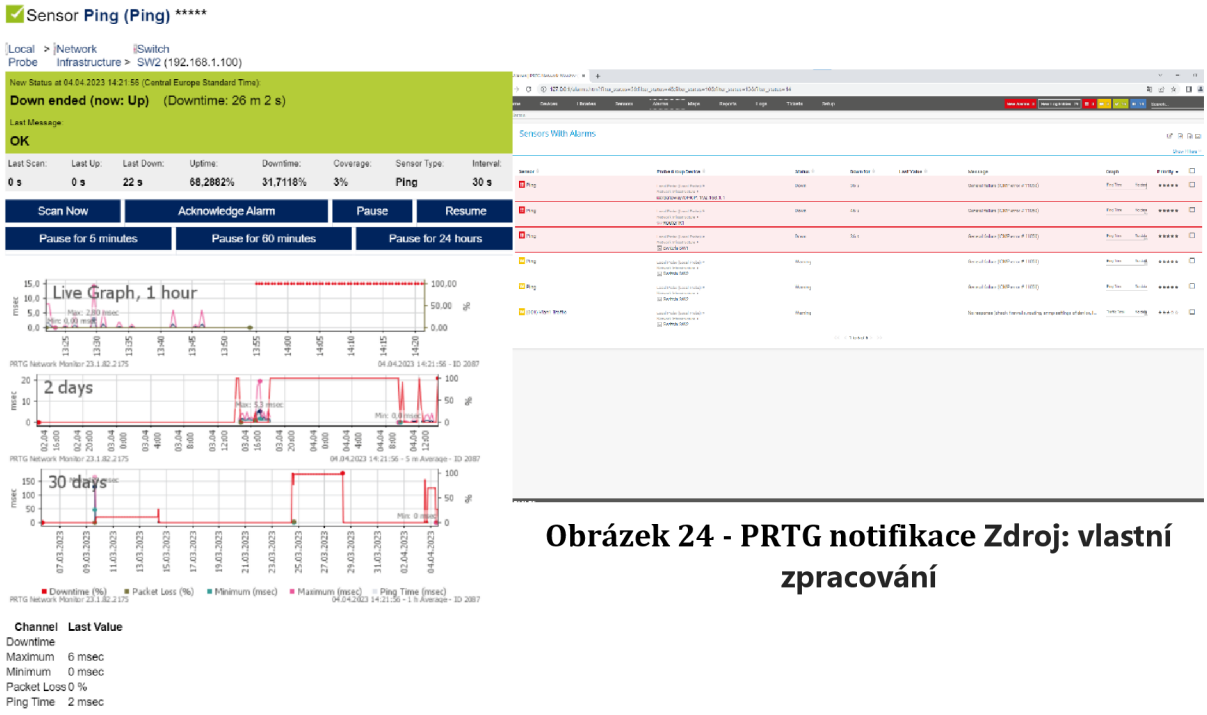
Obrázek 23 - Senzor Ping Zdroj: vlastní zpracování

rychlost pingů, jestli chcete použít IPv6 a také časový interval pro pingování. Poté stačí kliknout na tlačítko "Create" a sensor bude přidán k vašemu zařízení.



Obrázek 21 - Ping online Zdroj: vlastní zpracování

Pokud bude prvek nedostupný, nebo naopak zpátky naskočí a jeho dostupnost bude opět online. Mám zde několik druhů oznámení, které mohou být zasílány. Za prvé se mohou zasílat přímo na email, který byl uvádněn při instalaci. Nebo případně může



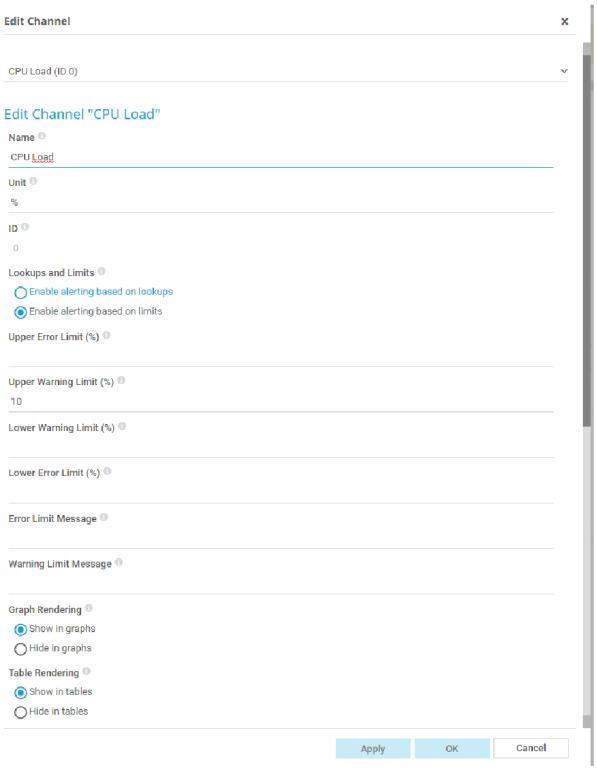
Obrázek 24 - PRTG notifikace Zdroj: vlastní zpracování

Obrázek 25 - Email notifikace Zdroj: vlastní zpracování

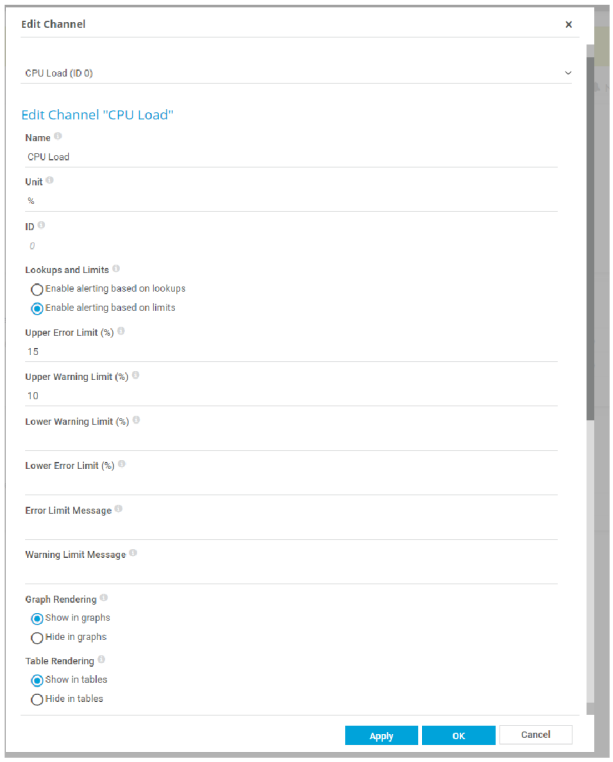
být oznámení posláno pouze do systému PRTG buď jako varování o nedostupnosti zařízení. Anebo při opakované nedostupnosti přímo jako error. V obou dvou případech je vidět graf prvku, kdy je/byl dostupný a s jakou odezvou, případně kdy byl nedostupný.

4.4.2 Monitoring výkonu zařízení

Pro monitorování výkonu zařízení na CPU v PRTG může být použito několik různých metod. Jednou z možností je aktivování senzoru CPU Load, který měří aktuální vytížení CPU v procentech. Dále je možné použít senzor SNMP CPU Load, který



Obrázek 26 - CPU nastavení1 Zdroj: vlastní zpracování



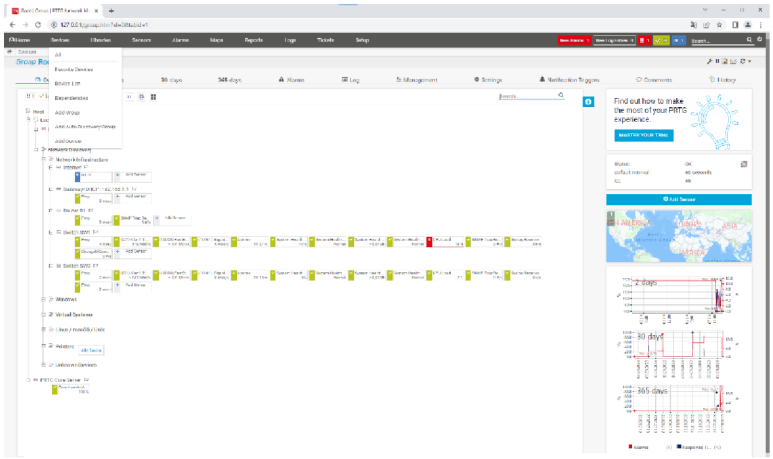
Obrázek 27 - CPU nastavení2 Zdroj: vlastní zpracování

získává informace o vytížení CPU pomocí protokolu SNMP.

V obou případech jsou tyto senzory pasivně monitorovány PRTG, což znamená, že PRTG pouze přijímá data z monitorovaného zařízení, aniž by ovlivňoval jeho výkon. Tyto senzory lze použít k monitorování výkonu CPU u různých zařízení v síti, jako jsou servery, směrovače, přepínače a další.

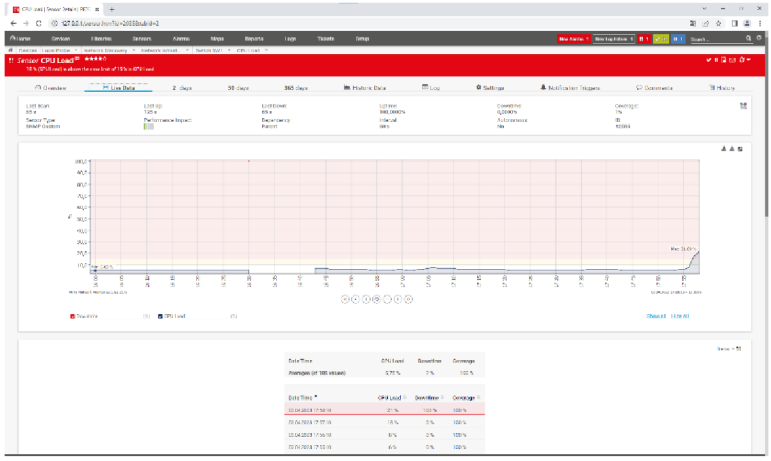
Při konfiguraci senzorů CPU Load v PRTG je možné nastavit různé prahové hodnoty, aby bylo možné sledovat výkon CPU v reálném čase a reagovat na případné problémy. Například lze nastavit prahovou hodnotu pro vysoké vytížení CPU, která upozorní administrátora na možnou hrozbu přetížení systému. Zde byly nastaveny

hodnoty pro jednoduché testování 10 % pro oznámení warning a 15% pro oznámení error.



Obrázek 28 - CPU test hierarchie Zdroj: vlastní zpracování

Celkově lze tedy říci, že pasivní monitorování výkonu CPU v PRTG je důležitou součástí správy sítě, která umožňuje administrátorům rychle reagovat na případné problémy a udržovat vysokou úroveň dostupnosti a výkonu sítě.

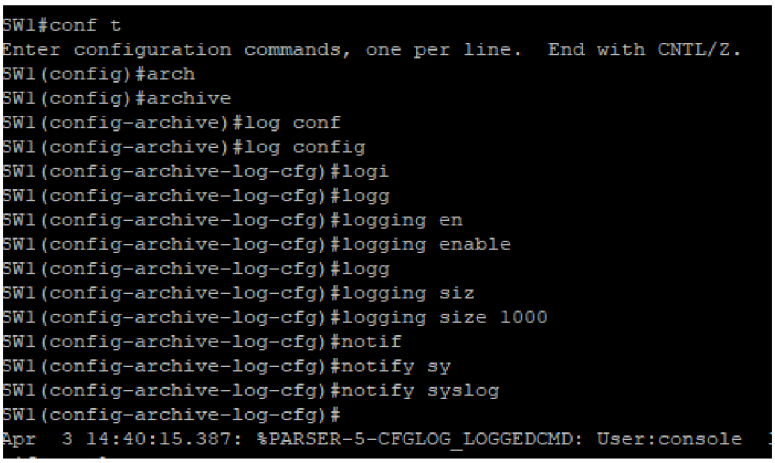


Obrázek 29 - Test přetížení CPU Zdroj: vlastní zpracování

4.4.3 Monitoring připojení uživatele k prvku přes SSH

Při monitoringu přihlášení uživatelů přes SSH na prvku je nutné přidat senzor buď "SSH v2 Sensor", který umožňuje monitorování SSH přihlášení. Senzor je třeba nastavit podle požadavků, například prahovou hodnotu pro maximální počet přihlášení nebo počet přihlášení za určitý interval.

Pro upozornění na přihlašování uživatele je nutné přidat notifikační pravidlo. Lze ho nastavit například na e-mail nebo SMS. Dále je možností využít syslog zpráv, které jsou nastaveny tak, že se odesílají na daný PRTG monitoring server. V tomto případě 192.168.0.3/24 PC.



Obrázek 30 – Logging konfigurace Zdroj: vlastní zpracování

Nejprve bylo nastaven syslog na samotném switchi.

logging host 192.168.0.3

logging trap informational

Pokud je třeba monitorovat, kdo se na zařízení přihlásil, je nutné povolit logování SSH přihlášení. Nejprve byl prvek pojmenován a nastaven hostname. Poté musel být přidán do domény, vygenerován SSH klíč a povolena podpora SSH na Vty0 lince. Doporučuje se mít vytvořeno přihlašovacího usera už na začátku před vytvářením RSA zabezpečovacího klíče. Veškeré kroky jsou v praktickém případě zaznamenány níže:

hostname SW1

ip domain name MyDomain.com

crypto key generate rsa general-keys modulus 1024

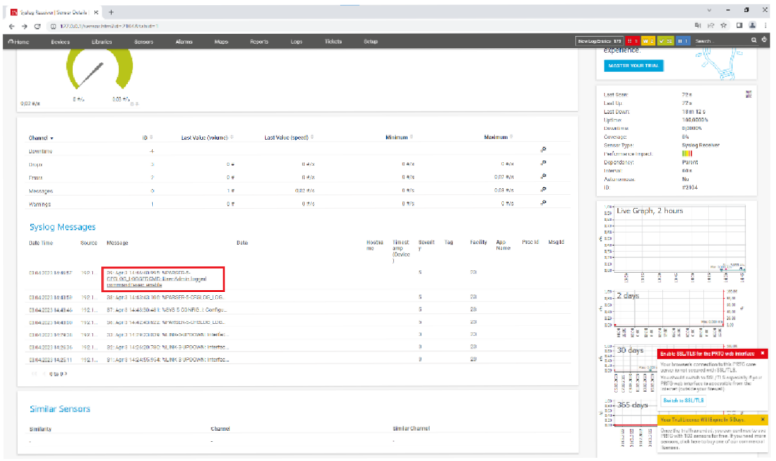
ip ssh version 2

line vty 0 4

login local

transport input ssh

Každé zařízení má své vlastní nastavení logování, které je nutné upravit. Po povolení logování lze sledovat přihlašování uživatele pomocí logování událostí. Tyto informace lze zobrazit v sekci "Event Log" v PRTG u konkrétního zařízení.



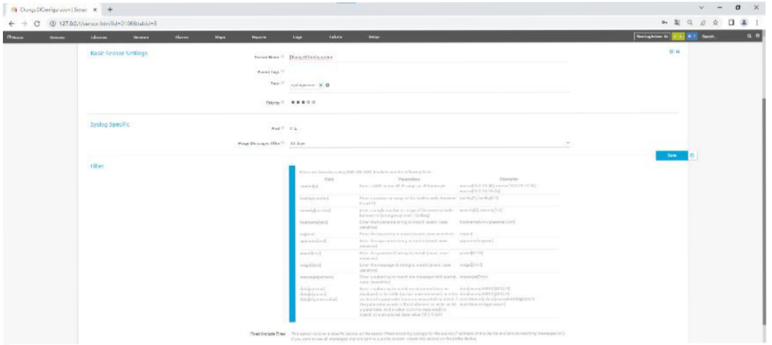
Obrázek 31 – Přihlášení SSH syslog Zdroj: vlastní zpracování

Celkově lze říci, že monitorování SSH přihlášení na zařízeních pomocí PRTG je důležitou součástí správy sítě. Díky této funkci lze snadno sledovat přihlašování uživatelů a v případě potřeby rychle reagovat na možné hrozby.

Obrázek 32 - SSH login Admin Zdroj: vlastní zpracování

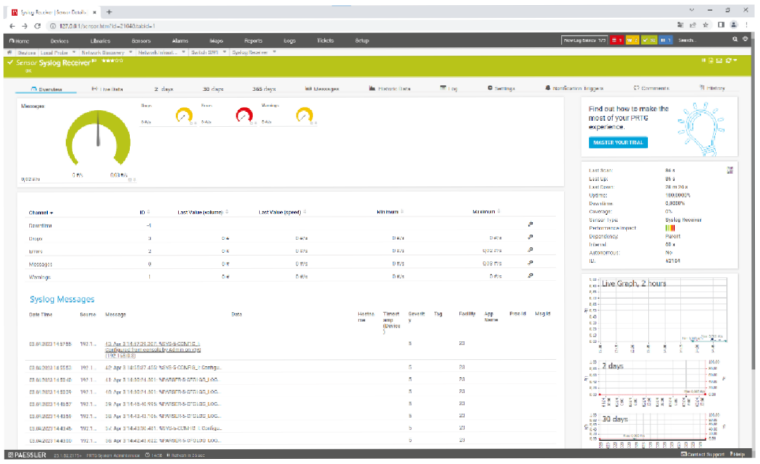
4.4.4 Monitoring změny konfigurace zařízení

Pro monitoring změny konfigurace byl přidán senzor Syslog Reciever. Tento senzor už byl na configurován v sekci Monitoring připojení uživatele přes SSH.

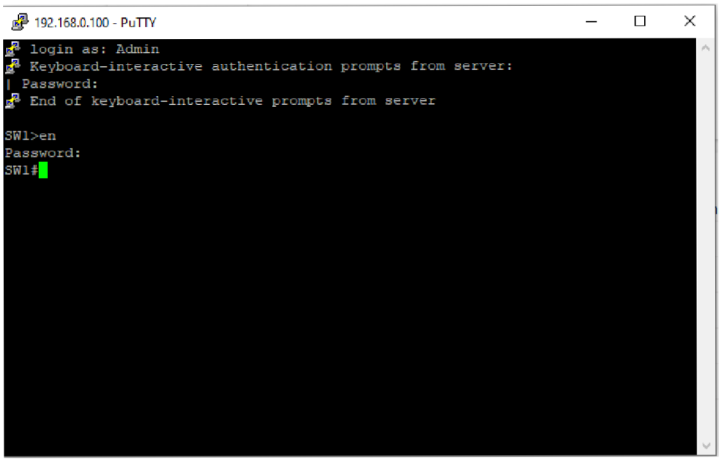


Obrázek 33 - Konfigurace fyzických portů PRTG Zdroj: vlastní zpracování

Tento senzor zachytí veškeré logy, které se dějí na zařízení, tudíž logy musí být filtrovány. Zpráva byla vyfiltrována pomocí hesel „Configured from console by“, které objevují ve zprávě od zařízení. Tento senzor byl pojmenován Změna



Obrázek 35 - Změna konfigurace zařízení Zdroj: vlastní zpracování



Obrázek 34 – PuTTY login Zdroj: vlastní zpracování

konfigurace u zařízení. Ze zprávy senzoru bylo získáno, jaký uživatel přistoupil do konfiguračního módu terminálu a z jaké linky. Práce testovala monitorování u uživatele Admin na lince vty0. Při přihlášení do konfiguračního módu na PRTG přišlo varování k tomuto senzoru.

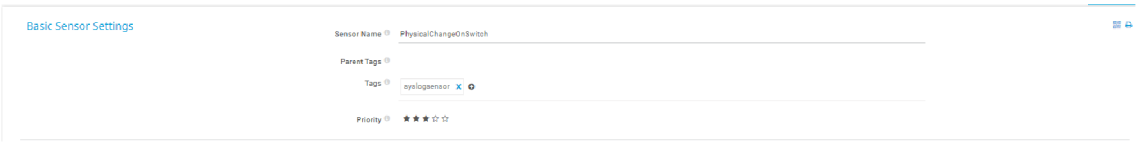
Obrázek 36 - SNMP Změna konfigurace Zdroj: vlastní zpracování

4.4.5 Monitoring portu při přepojení zařízení

Pro monitoring portů na switchi je důležité, aby bylo nastaveno portové zabezpečení na následující porty. V případě této práce, s jednoduchou sítí, bylo nastaveno pouze na prvních třech portech daného switche.

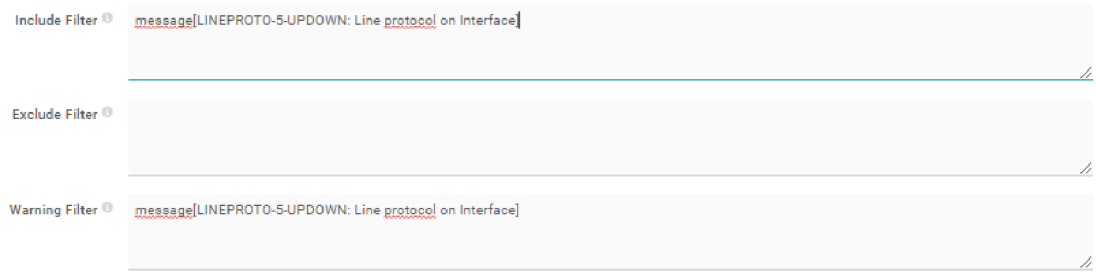
```
interface <název_portu>
switchport mode access
switchport port-security
switchport port-security violation restrict
```

Toto nastavení zabezpečí porty na switchi tak, aby mohly být používány pouze určitým zařízením (MAC adresám), které jsou dovoleny pomocí příkazu "switchport port-security mac-address". Po tomto nastavení jsou zprávy zasílány na nastevený syslog server (tento server byl nastavován výše v sekci Monitoring připojení uživatele k prvku přes SSH). Na PRTG byl přidán nový senzor. Senzor byl pojmenován “PhysicalChangeOnSwitch”, zde byly vyfiltrovány zprávy podle



Obrázek 38 - Pojmenování senzoru Zdroj: vlastní zpracování

“message[LINEPROTO-5-UPTODOWN]”. Tyto zprávy byly I přidány do warning, tudíž kdykoliv se změní fyzická conifigurace zařízení, přijde do PRTG varování o



Obrázek 37 - Filtrování zpráv Zdroj: vlastní zpracování

tomto stavu. V daném varování jsou uvedeny informace, který port byl zaměněn, v jakém čase apod. viz obrázek níže.

```
SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#arch
SW1(config)#archive
SW1(config-archive)#log conf
SW1(config-archive)#log config
SW1(config-archive-log-cfg)#logi
SW1(config-archive-log-cfg)#logg
SW1(config-archive-log-cfg)#logging en
SW1(config-archive-log-cfg)#logging enable
SW1(config-archive-log-cfg)#logg
SW1(config-archive-log-cfg)#logging siz
SW1(config-archive-log-cfg)#logging size 1000
SW1(config-archive-log-cfg)#notif
SW1(config-archive-log-cfg)#notify sy
SW1(config-archive-log-cfg)#notify syslog
SW1(config-archive-log-cfg)#
Apr  3 14:40:15.387: %PARSER-5-CFGLOG_LOGGEDCMD: User:console
```

Obrázek 39 - Konfigurace ukládání syslogů Zdroj: vlastní zpracování

Konfigurace byla testována na switchi 192.168.0.100. Zde byl odpojen počítač 192.168.0.4 a připojen počítač se stejnou IP adresou, ale s jinou mac adresou. V PRTG přišlo varovné oznámení o tom, že tento PORT byl změněn na stav DOWN. Ovšem ne kvůli dostupnosti, ale kvůli změně fyzické topologie zapojených zařízení. Jak je vidět na obrázku níže. K přepojení došlo na portu FastEthernet0/3.

03.04.2023 17:50:23	192.168.0.100	63: Apr 3 17:50:07.839: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

Obrázek 40 - Změna portu test Zdroj: vlastní zpracování

5 Shrnutí výsledků

Jedním z důvodů, proč byl výbrán program PRTG je jeho široká škála monitorovacích funkcí. PRTG Network Monitor dokáže monitorovat obrovské množství síťových zařízení a protokolů, včetně směrovačů, přepínačů, serverů, pracovních stanic a dalších. Díky tomu mohou organizace používat jediný nástroj pro monitorování celé sítě, místo aby musely používat více nástrojů pro monitorování různých typů zařízení a protokolů. Jeho ovládání je intuitivní, což dokazuje tato bakalářská práce, protože autor s tímto programem pracoval poprvé. Důležitým parametrem výběru hrála roli dlouhá zkušební verze a verze zdarma, která obsahuje plné funkční rozhraní se 100 senzory zdarma.

6 Závěry a doporučení

Závěr této bakalářské práce ukázal, že monitorování sítí je klíčovým prvkem pro správu infrastruktury v podnikovém prostředí. Tato funkce nám umožňuje včasnou detekci, maximalizaci výkonu a minimalizaci výpadků. Byly identifikovány osvědčené postupy a trendy v této oblasti a bylo představeno hned několik programů. Veškeré monitorování proběhlo v pořádku, a tedy program PRTG byl uznán vhodnou variantou pro tuhle bakalářskou práci. Pro monitorování bylo definováno 5 use casů, které jsou popsány výše i s uvedeným řešením a step-by-step návodem. S monitorováním use casů nebyl sebemenší problém a PRTG zvládlo všechny. Tyto use casy byly ovšem jen malinkým zlomkem toho, co opravdu tento program dokáže monitorovat. Proto z důvodu obsáhlosti nástrojů, které by se už do téhle práce nevešly, musely být ignorovány. Avšak samotný program nabízí velmi intuitivní rozhraní a jakékoliv další monitorovací nástroje by byly příležitostí k návaznosti na tuto práci. Kvalita ostatních programů byla hodnocena pouze na jejich testování a nemá nic dotyčného s praktickou částí této práce, otevírá se tedy možnost zkoumání dané problematiky a vhodnosti programů přímo na stejné use casy.

7 Seznam použité literatury

[1] Český statistický úřad. Czso.cz [online]. Český statistický úřad Na padesátém 81 Praha 10 100 82: Český statistický úřad, 2020 [cit. 2023-02-01]. Dostupné z: https://www.czso.cz/csu/czso/internet-pouziva-pres-80-obyvatel-ceska

[2] MACHALA, Miroslav. Historie Internetu a jeho budoucí využití: bakalářská práce. Brno: Masarykova univerzita, Fakulta pedagogická, Katedra technické a informační výchovy, 2007. Vedoucí diplomové práce Ing. Martin Dosedla.

[3] ZVÁROVÁ, Jana. Biomedicínská informatika I : Základy informatiky pro biomedicínu a zdravotnictví. 1. vydání. Praha : Karolinum, 2002. ISBN 80-246-0609-7.

[4] Alani, M.M. (2014). OSI Model. In: Guide to OSI and TCP/IP Models. SpringerBriefs in Computer Science. Springer, Cham. https://doi.org/10.1007/978-3-319-05152-9_2

[5] SUBRAMANIAN, Mani. Network Management: Principles and Practice. Addison-Wesley: Reading, Mass., 2000. ISBN 9780201357424, 0201357429.

[6] Majanoja, A. , Tervala, E. , Linko, L. and Leppänen, V. (2014) The Challenge of Global Selective Outsourcing Environment: Implementing Customer-Centric IT Service Operations and ITIL Processes. Journal of Service Science and Management, 7, 396-410. doi: 10.4236/jssm.2014.76037.

[7] Https://www.paessler.com/prtg. Paessler – The Monitoring Experts [online]. Thurn-und-Taxis-Str. 14, 90411 Nuremberg Germany: Paessler, 2023 [cit. 2023-02-01]. Dostupné z: https://www.paessler.com/prtg

[8] Solarwinds. Solarwinds [online]. 7171 Southwest Parkway Bldg 400 Austin, Texas 78735: SolarWinds Worldwide, LLC., 2023 [cit. 2023-02-01]. Dostupné z: https://www.solarwinds.com

[9] Nagios. Nagios [online]. 1295 Bandana Blvd N, Suite 165 Saint Paul, MN 55108: Nagios Enterprises, 2023 [cit. 2023-02-01]. Dostupné z: https://www.nagios.org/

[10] Internet a jeho služby. Internet a jeho služby [online]. Neznámé: Neznámé, Neznámé [cit. 2023-02-12]. Dostupné z: http://ijs2.8u.cz/images/Vrstvy2.jpg

8 Přílohy

Příloha č. 1

```
Current configuration : 3330 bytes
!
! Last configuration change at 11:45:18 UTC Tue Mar 14 2023 by
Admin
! NVRAM config last updated at 11:44:05 UTC Tue Mar 14 2023 by
Admin
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SW1
!
boot-start-marker
boot-end-marker
!
logging buffered warnings
logging monitor warnings
enable secret 5 $1$6M84$Vf9I/1P0jf8Sww472dy8O0
!
username Admin secret 5 $1$N8Yt$GI7cBrytWN2kS3QcvjSMn/
no aaa new-model
system mtu routing 1500
!
!
ip domain-name MyDomain.com
login on-failure log
login on-success log
!
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip ssh version 2
!
!
!
!
!
interface FastEthernet0/1
 switchport mode access
 switchport port-security violation restrict
```

```
!
interface FastEthernet0/2
 switchport mode access
 switchport port-security violation restrict
!
interface FastEthernet0/3
 switchport mode access
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.0.100 255.255.255.0
```

```
!
ip default-gateway 192.168.0.1
ip http server
ip http secure-server
logging history notifications
logging trap warnings
logging host 192.168.0.3
snmp-server community public RO
snmp-server enable traps snmp authentication linkdown linkup
coldstart warmstart
snmp-server enable traps transceiver all
snmp-server enable traps call-home message-send-fail server-fail
snmp-server enable traps tty
snmp-server enable traps cluster
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps dot1x auth-fail-vlan guest-vlan no-auth-
fail-vlan no-guest-vlan
snmp-server enable traps envmon fan shutdown supply temperature
status
snmp-server enable traps power-ethernet police
snmp-server enable traps fru-ctrl
snmp-server enable traps event-manager
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps energywise
snmp-server enable traps vstack
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps stpx inconsistency root-inconsistency
loop-inconsistency
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server enable traps errdisable
snmp-server host 192.168.0.3 version 2c public
!
vstack
!
line con 0
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login
!
end
```

UNIVERZITA HRADEC KRÁLOVÉ
Fakulta informatiky a managementu
Akademickj rok: 2021/2022

Studijní program: Informační management
Forma studia: Prezenční

Podklad pro zadání BAKALÁŘSKÉ práce studenta

Jméno a příjmení:	Matěj Hromádka
Osobní číslo:	I2000487
Adresa:	Jana Zajíce 961, Pardubice - Studánka, 53012 Pardubice 12, Česká republika
Téma práce:	Dohled síťové infrastruktury v podnikovém prostředí - tutoriál
Téma práce anglicky:	Network Infrastructure Monitoring in an Enterprise Environment - Tutorial
Jazyk práce:	Čeština
Vedoucí práce:	Ing. Tomáš Svoboda, Ph.D. Katedra informačních technologií

Zásady pro vypracování:

Cílem bakalářské práce je vytvořit podpůrné materiály v oblasti dohledu síťové infrastruktury v podnikovém prostředí v podobě tutoriálů. V teoretické části autor představí a podrobně popíše postupy a řešení dílčích úloh monitoringu síťové infrastruktury s důrazem na podnikovém prostředí a využití podnikovjch procesůincident a change managementu. V praktické části pak autor vytvoří praktická řešení dílčích úloh ve formě "step-by-step" tutoriálů.

Seznam doporučené literatury:

Wireshark for Security Professionals. Hoboken: John Wiley, 2017. ISBN 978-1-118-91821-0. KABELOVÁ, Alena a Libor DOSTÁLEK. *Velkj průvodce protokoly TCP/IPasystémem DNS*. 5., aktualiz. vyd. Brno: Computer Press, 2008. ISBN 978-80-251-2236-5.

Podpis studenta: Datum:

Podpis vedoucího práce: Datum: