VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH OPTIMALIZACE A MONITORINGU INFRASTRUKTURY SERVEROVNY PODNIKU

ENTERPRISE SERVER ROOM INFRASTRUCTURE OPTIMALIZATION AND MONITORING

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Tomáš Hink**
AUTHOR

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

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Tomáš Hink**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Viktor Ondrák, Ph.D.**
Akademický rok:	2018/19

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

Návrh optimalizace a monitoringu infrastruktury serverovny podniku

Charakteristika problematiky úkolu:

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

Cíle, kterých má být dosaženo:

Navrhnout optimalizaci infrastruktury serverovny a její monitoring.

Základní literární prameny:

BUYTAERT, Kris. Best damn server virtualization book period: including Vmware, Xen, and Microsoft Virtual Server. Oxford: Elsevier Science, 2007. ISBN 978-1-59749-217-1.

JORDÁN, Vilém a Viktor ONDRÁK. Infrastruktura komunikačních systémů II: kritické aplikace. Brno: CERM, Akademické nakladatelství, 2015. ISBN 978-80-214-5240-4.

JORDÁN, Vilém a Viktor ONDRÁK. Infrastruktura komunikačních systémů III: integrovaná podniková infrastruktura. Brno: CERM, Akademické nakladatelství, 2015. ISBN 978-80-214-5241-1.

RUEST, Danielle a Nelson RUEST. Virtualizace: podrobný průvodce. Brno: Computer Press, 2010. ISBN 978-802-5126-769.

TAKEMURA, Chris a Luke S. CRAWFORD. The book of Xen: a practical guide for the system administrator. San Francisco: No Starch Press, 2010. ISBN 15-932-7186-7.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2018/19

V Brně dne 28.2.2019

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Diplomová práce se zabývá problematikou návrhu a realizace optimalizace a také monitoringu serverovny podniku. Optimalizace spočívá v návrhu přístupového systému a měření teploty serverovny, dále návrhu systému řízení napájení a automatických startů infrastruktury, serverovou a síťovou optimalizací infrastruktury, managementem vizualizačního řešení a monitoringem sítě.

Abstract

This master's thesis deals with the design and implementation of optimization and monitoring of the server room. Optimization consists in designing access system and server room temperature measurement, automatic infrastructure start-up and power management, server and network infrastructure optimization, server virtualization management and network monitoring.

Klíčová slova

MikroTik, The Dude, Siemens LOGO, UniPi Neuron, Virtualizace, XCP-ng, Xen Orchestra, IT infrastruktura, Konsolidace serverů, Microsoft 365, Linux, Windows Server, Monitoring, Přístupový systém, Serverovna, Teplota

Keywords

MikroTik, The Dude, Siemens LOGO, UniPi Neuron, Virtualization, XCP-ng, Xen Orchestra, IT infrastructure, Servers consolidation, Microsoft 365, Linux, Windows Server, Monitoring, Access control system, Server room, Temperature

Citace

HINK, Tomáš. *Návrh optimalizace a monitoringu infrastruktury serverovny podniku* [online]. Brno, 2019 [cit. 2019-05-08]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/118967. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Viktor Ondrák.

Návrh optimalizace a monitoringu infrastruktury serverovny podniku

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně pod vedením pana doktora Viktora Ondráka. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

.....
Tomáš Hink
8. května 2019

Poděkování

Rád bych poděkoval mému vedoucímu panu doktoru Viktoru Ondrákovi za jeho cenné rady. Své poděkování bych chtěl věnovat také kolegovi Luďku Bukovskému za rady při řešení otázek analýzy společnosti. Dále bych chtěl vyjádřit poděkování panu jednateli inženýru Kochovi ze společnosti SPOLEČNOST-24, s.r.o. za poskytnutý hardware, důvěru a možnost testovat v reálném prostředí.

Obsah

Kapitola 1

Úvod

Počítačové sítě jsou nyní základním stavebním kamenem každé společnosti. Pro téměř všechny se staly nepostradatelnou součástí při každodenních činnostech. Nedostupnost počítačové sítě ve společnosti, která se zabývá poskytováním podpory pro IT infrastruktury jiných společností, znamená výpadek její vlastní infrastruktury vážný problém. Společnost není schopna vykonávat svou činnost, je ohrožen její zisk a snižuje se její produktivita, a dokonce i postavení na trhu. Pokud nebude síť fungovat správně ve společnosti, která dělá podporu pro IT, tak od ní pravděpodobně nebude chtít nikdo poskytovat služby. Firmě se tak může poškodit veřejný obraz.

Aby nenastávaly výpadky v počítačových sítích, je potřeba provádět proaktivní monitoring všech klíčových částí počítačové sítě. Před zavedením monitoringu, je více než vhodné IT infrastrukturu nejprve optimalizovat. Optimalizace IT infrastruktury podniku a její monitoring bude hlavní náplní této diplomové práce. Optimalizace je proces hledání řešení, které je nejvhodnější, má nejkratší cestu k jeho dosažení při nákupu co možná nejlevnějšího a současně nejkvalitnějšího zboží. Při procesu optimalizace měníme stavové proměnné optimalizovaného objektu a zjišťujeme, jaký má vliv změna těchto tzv. proměnných na výsledné parametry. Například pokud připravujeme pokrm, mohou hrát roli tzv. stavových proměnných (jež určují stav jídla) hmotnosti jednotlivých použitých ingrediencí. Námi sledovaným parametrem pokrmu pak může být jeho chuť. Optimalizátorem v tomto případě může být kuchařka, ta tak dlouho mění množství přísad, dokud nedosáhne požadované chuti [18].

V současné době existuje široká nabídka virtualizačních řešení informační infrastruktury pro podniky. Ve své diplomové práci bych se rád na tuto problematiku zaměřil a ihned realizoval své poznatky v praxi v podniku ve kterém pracuji. Práce bude realizována pro SPOLEČNOST-24, s.r.o.

Kapitola 2

Cíle práce

Hlavním cílem diplomové práce je zoptimalizovat infrastrukturu serverovny a navrhnout řešení monitoringu sítě. Návrh výsledného řešení je proveden na základě komplexní analýzy informační infrastruktury s ohledem na požadavky analyzované společnosti.

Cíle práce jsou rozděleny na hlavní cíl a dílčí postupové cíle, kterými bude dosaženo cíle hlavního. Dílčí cíle na sebe těsně navazují a využívají předchozích výstupů. Závěrečná kapitola hodnotí splnění cílů.

Pro naplnění hlavního cíle práce byly vytvořeny následující postupové cíle:

- Navrhnout výběr vhodných technologií.
- Navrhnout rozmístění technologií v serverovně, ať již na fyzické úrovni tak i virtuální.
- Navrhnout konsolidaci technologií.
- Navrhnout rozdělení technologii do takzvaných náběhových skupin.
- Navrhnout řešení pro postupné náběhy technologií při obnově elektrického napětí ve správném pořadí.
- Navrhnout systém monitoringu teploty serverovny.
- Navrhnout systém monitoringu síťových služeb.
- Navrhnout přístupový systém do serverovny.
- Navrhnout optimalizaci konfigurace jednotlivých technologických prvků.
- Implementovat navržené řešení.
- Ověřit funkci systémů, zhodnotit jeho vlastnosti a diskutovat možná rozšíření.
- Posoudit ekonomické zhodnocení návrhu řešení.

Výsledkem této diplomové práce bude funkční a komplexní řešení informačních technologií v podniku SPOLEČNOST-24 s.r.o. Jelikož tato společnost poskytuje IT podporu dalším společnostem, je potřeba, aby infrastruktura byla stabilní, spolehlivá, jednoduchá a monitorovaná. Před optimalizací se společnost potýkala s vysokou složitostí infrastruktury a neměla zavedený proaktivní monitoring ani dokumentaci sítě.

Kapitola 3

Teoretická východiska práce

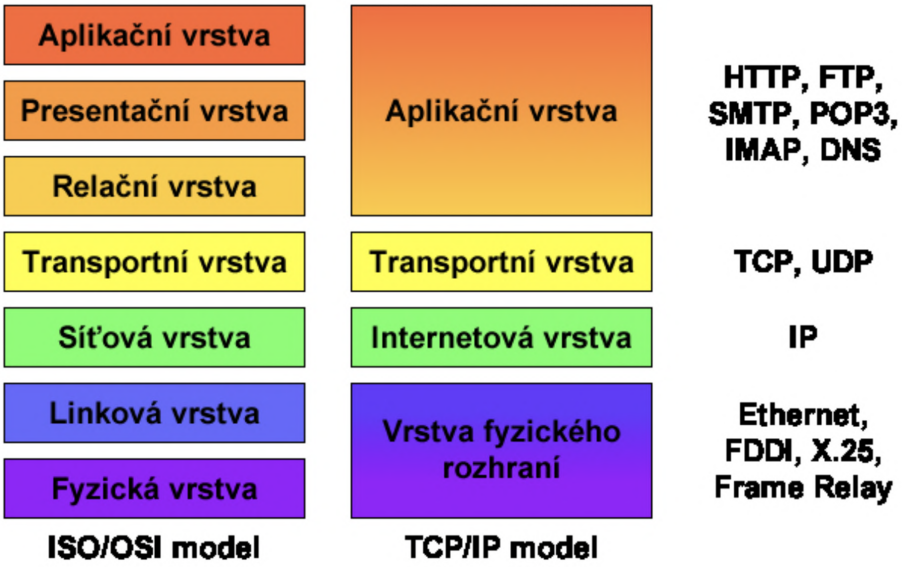
V následujících částech této kapitoly bych vás rád obeznámil s technologiemi, jež byly použity k realizování této diplomové práce. Budou zde objasněna teoretická východiska práce, jejichž znalost je nutná k pochopení dané problematiky, a na základě kterých je možné provést analýzu současného stavu informační infrastruktury podniku.

3.1 Architektura TCP/IP

V literaturách bývá často označována architektura TCP/IP jako Internetový model. Síťová architektura oproti síťovému modelu obsahuje navíc konkrétní představu o fungování jednotlivých vrstev. Model je více obecný a je zjednodušeným obrazem reality. Architektura TCP/IP je zjednodušením referenčního modelu ISO/OSI, model ISO/OSI tvoří 7 vrstev, některé vrstvy nebyly nikdy plně implementovány a je tak příliš složitý pro praxi. Implementace každé vrstvy modelu ISO/OSI samostatně se později ukázalo jako příliš náročné, často implementace funkcionality jedné vrstvy zajišťovala funkcionalitu i vrstev dalších. Architektura TCP/IP obsahuje pouze 4 vrstvy a to konkrétně vrstvu fyzického rozhraní, internetovou vrstvu, transportní vrstvu a aplikační vrstvu, kdy některé z vrstev modelu ISO/OSI jsou sloučeny do jediné v architektuře TCP/IP. Na obrázku 3.1 je zobrazeno porovnání vrstev modelu ISO/OSI a architektury TCP/IP, včetně uvedení příkladů protokolů nad jednotlivými vrstvami. Z obrázku je taktéž patrné mapování vrstev modelu ISO/OSI na vrstvy architektury TCP/IP. Hlavní zjednodušení architektury TCP/IP spočívá ve sloučení vrstev aplikační, prezentační a relační do jediné aplikační vrstvy. Dalším zjednodušením je sloučení vrstev linkové a fyzické do vrstvy fyzického rozhraní [7].

Pochopení architektury TCP/IP je kritické pro správnou konfiguraci a správu sítě. Je také důležité pro analýzu a řešení problémů při komunikaci mezi jednotlivými počítači a aplikacemi. Architektura TCP/IP řeší ve své podstatě jen vrstvy L3 (síťovou vrstvu) a L4 (transportní vrstvu). Vrstvu síťového (fyzického) rozhraní a aplikační vrstvu nedefinuje, jen přejímá jiné existující architektury. Například architekturu Ethernet, která řeší jen L1 (fyzická vrstva) a L2 (linková vrstva). Každá z vrstev architektury TCP/IP poskytuje a zajišťuje v síti jiné služby:

- **Vrstva síťového (fyzického) rozhraní** popisuje standardy pro fyzické médium a elektrické signály. Tato vrstva definuje funkce pro přístup k fyzickému médiu a zajišťuje zabalování datagramů do tzv. rámců, příkladem může být Ethernet rámec, jež je zobrazen na obrázku 3.2. Architektura TCP/IP pouze přejímá architekturu Ethernet.



Obrázek 3.1: Porovnání modelů ISO/OSI a TCP/IP s protokoly jednotlivých vrstev [7]

Ethernet rámec

Preamble	SFD	MAC D	MAC S	LT	Payload	FCS	IG
7× oktet 10101010	1× oktet 10101011	6 oktetů	6 oktetů	2 oktety	46-1500 oktetů	4 oktety	12 oktetů

Ethernet rámec rozšířený o VLAN

Preamble	SFD	MAC D	MAC S	TF		LT	Payload	FCS	IG
7 oktetů 10101010	1× oktet 10101011	6 oktetů	6 oktetů	ETPID 2 oktety	PCP/CFI/VID 2 oktety	2 oktety	42-1500 oktetů	4 oktety	12 oktetů

Obrázek 3.2: Standartní Ethernet rámec a rozšířený Ethernet rámec o VLAN [10]

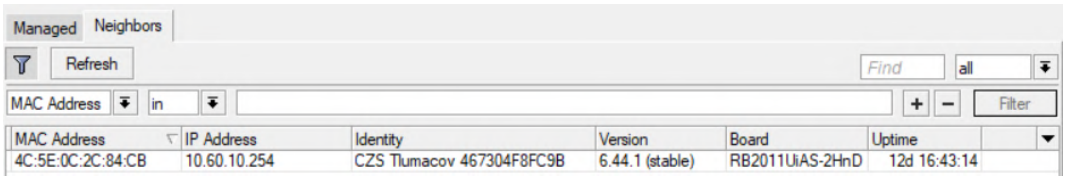
Ethernetový rámec se skládá z Preambule, která má velikost 7 oktetů, střídavě 1 a 0 a slouží k synchronizaci hodin příjemce, další částí rámce je SFD (Start of frame delimiter), jež označuje začátek rámce (oktet 10101011). Další částí rámce je MAC (Media Access Control) adresa cílového síťového rozhraní (MAC destination) a MAC adresa zdrojového síťového rozhraní (MAC source) cílová MAC adresa. Dále následuje část identifikující délku pole dat[1] nebo typ (LT - Length/Type). Následuje Payload nebo též Data Field (DF),jež může mít například pro Ethernet II délku 46 až 1500 oktetů[2]. Další částí je FCS (Frame Check Sequence), jenž je 32bitovým kontolním kódem (CRC32), který se počítá ze všech polí rálce s vyjímkou Preambule a FCS. Posledním polem Ethernetového rámce je IG (Interpacket Gap), která je mezerou mezi rámci [10].

[1] LT v Ethernetovém rámci udává délku pole dat pro IEE 802.3 [10].

[2] Pokud je posílaných dat méně než minimální délka pole, tak je doplněno do minimální délky. Minimální délka je důležitá pro správnou detekci kolizí v rámci segmentu

VLAN (Virtual LAN) je virtuální lokální sítí. Využívá se k vytvoření několika logických nezávislých sítích na jedné fyzické síti. Cílem je usnadnit správu sítě a zvýšit její bezpečnost. VLAN bývá zpravidla realizována switchi nebo routery. Porty se rozdělí na několik logicky samostatných částí. Oddělení sítě pomocí VLAN je realizováno na úrovni Linkové vrstvy modelu ISO/OSI (L2) [10].

LLDP (Link Layer Discovery Protocol) je standardizovaným protokolem (IEEE[3] 802.1AB-2009) Linkové vrstvy modelu ISO/OSI (L2). Protokol slouží k zjišťování aktuální topologie, tj. k způsobu propojení aktivních prvků. Jedná se o jednocestný protokol, který pouze vysílá informace a nedochází k žádnému potvrzování přijaté informace nebo k navazování spojení. Aktivní prvek odesílá přes své porty informace o sobě ostatním LLDP zařízením v síti. K odesílání dochází periodicky nebo při změně na aktivním prvku. Discovery protocol je obecným protokolem, který umožňuje mapovat L2 vrstvu a to konkrétně zjištěním připojených zařízení v síti. Ukázka zjištěných zařízeních v síti na je zobrazena na snímku 3.3. Aby mohly být zařízení v síti zjistitelná musí podporovat tento protokol. Discovery protocol umožňuje přiřadit parametry IP na zařízení pomocí Ethernetu přes SNMP nebo CLI (Command Line Interface) - příkazovou řádku. Tento protokol pracuje nad LLDP. Podmínkou funkce je, aby na všech zařízeních bylo LLDP aktivní [10].



Obrázek 3.3: Ukázka zjištěných zařízeních v síti pomocí Discovery protocolu

- **Internetová vrstva** vytváří logické spojení mezi zařízeními. Základním protokolem této vrstvy je protokol IP, který bude popsán v kapitole 3.2. Protokoly Internetové vrstvy směrují zabalené IP pakety tzv. datagramy, na místo určení na základě cílové adresy. IP paket je na vrstvě L3 uložen konkrétně do pole Payload Ethernetového rámce nebo jiného rámce a obsahuje IP adresu příjemce, velikost IP paketu, IP kontrolní součet a IP payload (data). Pokud není obsah IP paket tak krátký, že se i se celý vleze do pole Payload Ethernetového rámce, musí být rozdělen na více částí. Toto rozdělení lze provádět pouze na úrovni vrstvy L3, data jsou na 3. vrstvě rozdělena a doplněna o veškeré IP služební informace. Z pohledu Vrstvy L2 se jedná pouze o přenášená data, která nijak neanalyzuje. Zařízení pracující na L3 musejí tato data z rámce přečíst, dekódovat a provést s nimi patřičné operace. Časová náročnost zpracování je důvodem proč mají zařízení pracující na L3 větší zpoždění při průchodu dat než zařízení pracující na L2. Internetová vrstva se snaží doručit data nejvhodnější cestou, tzv. doručení s největším úsilím (best-efford delivery) [7].

ICMP Protokol ICMP neboli Internet Control Message Protocol se řadí mezi nejdůležitější protokoly počítačových sítí. ICMP slouží pro přenos řídících a chybových

[3]Institute of Electrical and Electronics Engineers (IEEE).

zpráv mezi uzly a směrovači sítě TCP/IP. Jedním ze základních diagnostických nástrojů pro analýzu stavu zařízení v síti je odeslání ICMP Echo Reguest po zadání příkazu ping a druhé dotazované zařízení pokud podporuje protokol ICMP odpoví zprávou ICMP Echo Reply. Dalším užitečným příkazem pro zjištění přes která zařízení prochází pakety je traceroute, ten přenáší UDP datagram se speciálně upravenou hlavičkou a to konkrétně částí s IP TTL. Pro řízení zahlcení počítačové sítě a toku paketů slouží zprávy ICMP Source Quench. Další funkcí je aktualizace směrovacích tabulek uzlů od směrovačů pomocí zpráv ICMP Redirect a odesílání masky podsítě zprávami ICMP Address Mask Reguest a ICMP Address Mask Reply [16].

- **Transportní vrstva** vytváří logické spojení mezi koncovými body[4]. Transportní protokoly rozdělují aplikační data na menší jednotky, tzv. pakety (TCP paket a UDP paket). Mezi základní protokoly transportní vrstvy patří:

  TCP (Transmission Control Protocol) je spojově orientovaný protokol pro přenos na transportní vrstvě (L4) pro spolehlivý přenos dat.Použitím TCP mohou aplikace na počítačích připojených do sítě vytvořit mezi sebou spojení , přes které mohou přenášet data. Protokol zajišťuje správné pořadí zasílaných paketů[5], potvrzování přijet paketů druhou stranou a také řízení toku a zahlcení. Než se mohou data posílat, je potřeba ustanovit spojení mezi koncovými uzly. TCP také rozlišuje data pro vícenásobné, současně běžící aplikace (například webový a e-mailový server), běžící na stejném počítači podle portu (čísla). TCP využívá služby IP protokolu. Opakovaným odesíláním paketů při jejich ztrátě zajišťuje spolehlivost a seřazením přijatých paketů zajišťuje správné pořadí [10].

  UDP (User Datagram Protocol) pro nespolehlivý přenos dat. Tento protokol slouží k rychlému (rychlejšímu než u TCP) přenosu dat, bez zaručení spolehlivého doručení. Pakety nejsou při přenosu protokolem UDP očíslovány a jsou zasílány samostatně, cílový koncový uzel tedy nemá jak zjistit, zda se některé pakety po cestě ztratily či nikoliv. Tento protokol je alternativní k TCP a pracuje taktéž na Transportní vrstvě L4. Na rozdíl od TCP tento protokol nenavazuje přímé spojení mezi komunikujícími počítači. Odesilatel pouze odešle paket, ale již se nestará o to, zda byl paket úspěšně doručen či nikoliv. V případě potřeby doručování paketů ve správné pořadí nebo zajištění spolehlivého doručení musí tuto funkcionalitu zajistit sám zdrojový koncový uzel například dodatečnou implementací na vyšší úrovni kupříkladu na úrovni aplikačního protokolu. Stejně jako TCP identifikuje aplikace na počítačích pomocí tzv. portu. Data jsou zabaleny do IP datagramu. U protokolu UDP se nedoporučuje fragmentace dat, i když je možná. Výhodou protokolu UDP oproti protokolu TCP je to že adresátem nemusí být pouze jednoznačná IP adresa, ale i skupina adres. Pomocí tohoto protokolu můžeme posílat broadcast nebo multicast pakety, tj. rozesílat data více počítačům najednou. UDP se nejčastěji používá při přenosech dat v reálném čase (real-time přenos). Příkladem takového přenosu může být streamování videa nebo

[4]Koncovým bodem se rozumí proces či aplikace, která vytváří nebo zpracovává aplikační data. Zařízení jenž data pouze příjme a pošle dále (případně analyzuje nebo modifikuje hlavičky), tedy jemuž nejsou tato data určena, není koncovým bodem [7].

[5]Cílový koncový uzel vždy čte zaslané pakety ve správném pořadí, ale dorazit mohou tyto pakety v různém pořadí, může dokonce dojít ke ztrátě některých paketů při přenosu, ty pak musejí být zaslány znovu [7].

poslech hudby online. Přenáší se totiž vždy velký objem dat a jejich potvrzování by bylo pro síť opravdu náročné (platí pro protokol TCP) [10].

- **Aplikační vrstva** zajišťuje komunikaci na nejvyšší úrovni, tedy komunikaci mezi samotnými procesy a aplikacemi, které běží na počítači. Tato vrstva také řeší samotnou reprezentaci dat[6] a řízení dialogu tzv. vytváření a udržování relací (sessions), jenž vyjadřují kontext komunikace [7].

SNMP Protokol SNMP neboli Simple Network Management Protocol slouží pro monitorování a správu informačních sítí a služeb. Umožňuje sbírat důležité údaje o stavu jednotlivých zařízení nebo služeb, případně přenášet požadavky na změnu konfigurace. SNMP je jedním z nejužívanějších řídících protokolů počítačových sítí. SNMP je asynchronní transakčně orientovaný protokol založený na modelu typu klient/server. Tento protokol poskytuje prostředky pro správu a monitorování aktivních prvků sítě, stejně tak umožňuje i řízení a změny konfigurací těchto zařízení. Protokol SNMP se skládá ze tří základních prvků a těmi jsou SNMP Manažer, MIB (Mangement Information Base) - databáze uložená v aktivním prvku a SNMP Agent - aktivní prvky - switche, routery, LAN adaptéry a podobně. Manažer je monitorujícím zařízením, jež posílá požadavky a následně sbírá i zpracovává získaná data. Funkcí agenta, který je také monitorovacím zařízením je odpovídat na dotazy od manažera a posílat informace o stavu svých služeb, statistiky a vytvářet TRAPy[7]. Na aktivních prvcích sítě (SNMP Agentech) běží programové vybavení, jež monitoruje stav zařízení a tyto data ukládá do informační databáze MIB jenž obsahuje informace objektech identifikovaných pomocí OID (Object Identifier) a jejich stavech. SNMP zprávy jsou přenášeny pakety UDP [10].

Telnet Protokol telnet je zkratkou z „teletype network“ a pracuje na aplikační vrstvě TCP/IP architektury. Typicky se používá v IP sítích pro spojení typu klient/server přes protokol TCP, přičemž přenáší osmibitové znaky oběma směry, zajišťuje tedy duplexní spoj. Serverová část protokolu Telnet standardně naslouchá na portu 23. Praktické použití tohoto protokolu spočívá v použití stejnojmenného klienta, které slouží uživatelům pro připojení ke vzdálenému počítači pomocí textového uživatelského rozhraní. Jelikož nejsou přenášená data ani spojení šifrováno, tak se v dnešní době příliš často tento protokol nepoužívá a je postupně nahrazován protokolem SSH. Nástroj Telnet je také možné použít pro ruční navázání spojení s otevřenými porty a tím i službami serveru jako jsou SMTP, HTTP a podobně. Dále se protokol Telnet využívá pro nastavování různých síťových zařízení například spravovatelných switchů, podnikových routerů případně modemů a podobně. [17].

SSH Protokol SSH neboli Secure Shell je určen pro bezpečnou a šifrovanou komunikaci mezi dvěma zařízeními. Umožňuje jak přenos textu tak i dat. SSH jakožto zabezpečený komunikační protokol vznikl v reakci na špatně zabezpečené až přímo nebezpečné protokoly a příslušné služby typu Telnet [1].

[6] Aplikační vrstva řeší reprezentaci dat a to konkrétně kódování aplikačních dat pro přenos, převod dat do tohoto kódování a zpět [7].

[7] SNMP TRAP zpráva je asynchronní nevyžádaná zpráva od agenta pro manažera, je to reakce na událost, například výpadek služby [4].

Implementace architektury TCP/IP je rozdělena do tří částí. Nejnižší část, vrstva fyzického rozhraní, je implementována přímo v síťové kartě a jejím ovladači. Vyšší vrstvy internetová a transportní jsou součástí síťových modulů operačních systémů (TCP/IP stack), jež bývají v instalaci operačního systému implicitně implementovány. Poslední vrstva a to aplikační je implementována buď přímo v aplikacích (například webový prohlížeč nebo e-mailový klient) nebo jako systémové služby (například DHCP klient nebo DNS klient) [7].

3.2 Internet Protocol (IP)

IP (Internet protokol) je základním protokolem z hlediska správy sítí pracujícím na síťové vrstvě modelu ISO/OSI a na internetové vrstvě architektury TCP/IP. Protokol IP poskytuje službu přenosu (směrování) datagramů (paketů) v síti celé skupině protokolů TCP/IP. Tento protokol sám o sobě neposkytuje záruky na přenos dat. Pomocí IP adresy rozlišujeme pouze jednotlivá síťová rozhraní. IP je zodpovědný za směrování datagramů (paketů) ze zdrojového počítače do cílového zařízení přes jednu nebo více IP sítí. Existují dvě verze tohoto protokolu, starší ale značně rozšířená IPv4 a novější IPv6. Obě tyto verze jsou od sebe velice odlišné [10].

IP adresa slouží k jednoznačnému identifikování síťového rozhraní (konkrétního zařízení) v rámci dané sítě nebo podsítě. Každý jednotlivý datagram obsahuje adresy zdrojového a cílového koncového uzlu. Internetová vrstva se snaží doručit takový datagram od zdroji k cíli [7].

3.2.1 Internet Protocol verze 4 (IPv4)

IPv4 je starší, ale značně rozšířenou verzí protokolu IP. Většina stávajících interních sítí a podstatná část sítě Internet používá IPv4 jako komunikační protokol internetové vrstvy [7].

IPv4 adresy jsou 32bitová čísla, jež se zapisují v dekadickém formátu s tečkovou notací po osmi bitech. Každá adresa je ve tvaru `X.X.X.X`, kde X je číslo od 0 do 255. Z hlediska struktury se dělí IPv4 adresa na tři základní části a to na adresu sítě, adresu podsítě a adresu rozhraní vizte obrázek 3.4 [7].

Obrázek 3.4: Struktura IPv4 adresy [7]

Dříve byla IPv4 adresa tvořena pouze adresou sítě a rozhraní, toto členění se ale ukázalo jako příliš hrubé a docházelo tak ke zbytečnému plýtvání adres. Protože adresa sítě byla tvořena vždy pouze prvními osmi bity a zbylé bity tvořily adresy rozhraní, kterých bylo 16 milionů pro každou síť a byly využívány jen minimálně. Z tohoto důvodu došlo k rozdělení IPv4 adres do tříd. Tyto třídy se odlišovaly velikostmi částí pro adresu sítě. Tímto způsobem se vytvořilo podstatně více sítí pro méně rozhraní. Nakonec se i toto členění ukázalo jako nevhodné a došlo k rozdělení adresy rozhraní na část adresy podsítě a část rozhraní.

Adresu sítě pro danou koncovou síť přiděluje vždy poskytovatel připojení (přesněji lokální registrátor). Jak bude rozdělena lokální část adresy, tedy jaká část bude vyhrazena pro adresy podsítí a jaká část pro adresy rozhraní, určuje již správce konkrétní sítě [7]. Pro určení hranice mezi adresami podsítě a rozhraní se využívají masky podsítě (subnet mask). Stejně jako v případě IPv4 adresy tak i maska podsítě je 32bitové číslo zapsané ve stejném formátu jako IPv4 adresa. V binárním tvaru obsahuje jedničky na všech pozicích, kde se v IPv4 adrese nachází adresa sítě i podsítě a nuly tam, kde je adresa rozhraní. Na základě toho, že část obsahující adresu podsítě může být různě velká, musí být vždy součástí konfigurace síťového rozhraní i maska podsítě [7].

Třída	Prefix sítě	1. bajt	Maska	Bitů sítě	Bitů počítače	Počet sítí	Počet stanic v síti
A	0	0 - 127	255.0.0.0	7	24	126	16 777 214
B	10	128 - 191	255.255.0.0	14	16	16 384	65 534
C	110	192 - 223	255.255.255.0	21	8	2 097 152	254
D	1110	224 - 239	Skupinové vysílání (*multicast*)				
E	1111	240 - 255	Rezervováno pro pozdější využití				

Obrázek 3.5: Třídy IPv4 adres [7]

V tabulce na obrázku 3.5 je znázorněno rozdělení IPv4 adres do jednotlivých tříd spolu s informací jaká část je vyhrazena pro identifikaci sítě a jaká část je vyhrazena pro identifikaci rozhraní. Dnes se již rozdělení do tříd prakticky nevyužívá, protože bylo nahrazeno rozdělením podle CIDR (Classless Inter-Domain Routing).

Směrování IPv4 adres slouží k dopravě datagramů (paketů) ze zdrojového koncového uzlu do cílového koncového uzlu. Směrování se provádí na základě směrovacích tabulek, jež mohou být nastaveny staticky správcem sítě nebo dynamicky pomocí směrovacích protokolů jako jsou RIP (Routing Information Protocol) nebo OSPF (Open Shortest Path First) [7].

CIDR adresový blok	Popis
0.0.0.0/8	Aktuální síť (pouze pro zdrojové adresy)
10.0.0.0/8	Privátní síť
127.0.0.0/8	Loopback
169.254.0.0/16	Privátní síť (**APIPA**)
172.16.0.0/12	Privátní síť
192.88.99.0/24	IPv6 to IPv4 překlad
192.168.0.0/16	Privátní síť
224.0.0.0/4	Multicast (skupinové vysílání, předchozí třída D)
240.0.0.0/4	Rezervováno (předchozí třída E)
255.255.255.255	Broadcast (všesměrové vysílání)

Obrázek 3.6: Speciální rozsahy IPv4 adres [7]

Směrovací tabulky nejčastěji obsahují informace o tom, kterými porty směrovače nebo skrz jaké síťové rozhraní se má dostat do sítě, ve které leží koncový uzel s cílovou adresou. V dnešní době se pro směrování používá nejčastěji beztřídní mezidoménové směrování CIDR, jež umožňuje explicitně specifikovat předěl mezi částí s adresou sítě a částí s adresou počítače (rozhraní). Adresy se při použití CIDR zapisují ve formátu `X.X.X.X/Y`, kde část před / je

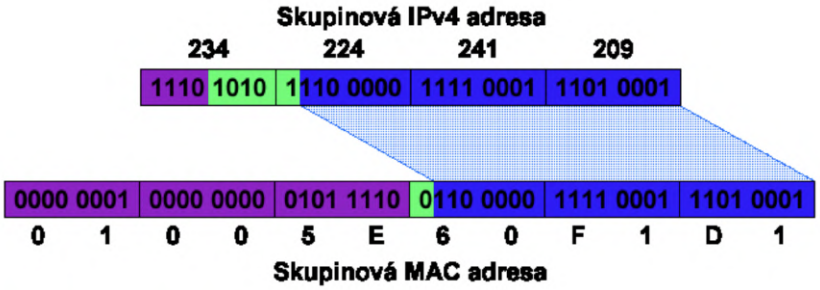
IPv4 adresa a Y je počet bitů adresy sítě. Pokud routeru dorazí datagram, podívá se do směrovací tabulky a zjistí, skrz jaké porty se dá dostat do sítě, do které náleží cílová IPv4 adresa v datagramu (paketu). V případě, že přípustných rozhraní je více, podívá se router na další metriky. Aby nedocházelo k cyklické závislosti, kdy datagram přijde na port, který vede do sítě, kam tento datagram směřuje, tak dojde k zahození tohoto paketu. Další situací kdy může být paket cíleně zahozen je když router odděluje interní síť od sítě Internet a cílová adresa paketu by obsahovala interní adresu jež náleží privátní síti. Tyto datagramy jsou nesměrovatelné v síti Internet. Posledním případem cíleného zahození datagramu je, pokud cílová adresa je adresou pro všesměrové vysílání (broadcast) a ostatní porty směrují do jiných podsítí, takové datagramy nikdy nesmějí překročit hranice podsítě [7].

3.2.2 Přenos dat na linkové vrstvě

Při přenosu dat na linkové vrstvě (vrstvě fyzického rozhraní) nedochází k žádnému směrování. Data jsou na linkové vrstvě reprezentována rámci (frames) a pro identifikaci zdrojových a koncových cílových uzlů se využívá MAC adresa. Fyzická MAC (Media Access Control) adresa je 48bitové číslo, které se zapisuje v hexadecimálním formátu s pomlčkovou notací po osmi bitech, často se však zapisuje také s dvojtečkovou notací po osmi bitech. Každá MAC adresa je tedy ve formátu `X-X-X-X-X-X` nebo `X:X:X:X:X:X`, kde X je hexadecimální číslo od 00 do FF [7].

Samotný přenos dat se dá přirovnat k všesměrovému vysílání v IPv4. Data jsou v rámci dané linky zaslána všem uzlům. Každé rozhraní příjme tento rámec a porovná svou MAC adresu s MAC adresou cílového koncového uzlu obsaženou v přijatém rámci v poli MAC D, pokud se tyto adresy shodují, jsou data předána vyšší vrstvě, jinak jsou data zahozena. Výjimkou je případ, kdy cílová MAC adresa koncového uzlu je přímo FF-FF-FF-FF-FF-FF, v tomto konkrétním případě každé rozhraní data takového rámce příjme. Tato adresa slouží pro všesměrové vysílání na linkové vrstvě. Jedno rozhraní může mít více než jednu MAC adresu, ovšem pouze jedna může být individuální, ostatní jsou pak vždy skupinové. Skupinové MAC adresy se vytvářejí automaticky na základě IP adres. V případě IPv4 se připojí k prefixu MAC adresy 01-00-5E nižších 23 bitů z 28 bitů, jenž identifikují skupinu u skupinové IP IPv4 adresy. Skupinové MAC adresy pro IPv4 jsou vždy v rozsahu 01-00-5E-00-00-00 až 01-00-5E-7F-FF-FF. Příklad převodu IPv4 skupinové adresy na odpovídající skupinovou MAC adresu je zobrazen na obrázku 3.7 [7].

Z příkladů skupinových adres výše vyplývá, že u protokolu IPv4 je počet skupinových IP adres větší než počet skupinových MAC adres, každá skupinová MAC adresa je tedy sdílena více skupinovými IP adresami při přenosech na linkové vrstvě (L2). Tento problém se řeší až na síťové (internetové) vrstvě (L3) ověřením skupinové IP adresy [7]. V případě všesměrové



Obrázek 3.7: Převod skupinové IPv4 adresy na odpovídající skupinovou MAC adresu [7]

IP adresy je odpovídající MAC adresa známá, MAC adresy pro skupinové IP adresy lze získat převody zmíněnými výše, ostatní (individuální) IP adresy mohou odpovídat obecně jakékoliv MAC adrese. K zajištění překladu IP adres na MAC adresy se používá protokol ARP (Address Resolution Protocol) u IPv4, jenž udržuje v paměti překladové tabulky mapující IP adresy na odpovídající MAC adresy. Záznamy v těchto ARP tabulkách mají omezenou dobu platnosti a jsou pravidelně mazány v periodách [7].

3.3 Systém DNS

DNS (Domain Name System) je systémem jež slouží pro překlad doménových jmen (DN, Domain name) na IP adresy a opačně. Umožňuje jednoznačně identifikovat počítač v lokální síti nebo na internetu pomocí textového názvu (jména), namísto hůře zapamatovatelné IP adresy. V dnešní době se často používají různá rozšíření doménových jmen jako například e-mailová adresa, jež není nic jiného než doménové jméno obohacené o identifikaci konkrétní osoby [7].

Systém DNS lze použít také pro flexibilní práci s IP adresami, kdy změna IP adresy počítače znamená pouze opravu mapování doménového jména na odpovídající novou IP adresu. Ze strany klienta nejsou potřeba žádné další úpravy. Lze díky tomu realizovat například load balancing (rozložení zátěže), kdy jedno doménové jméno identifikuje více počítačů (serverů), které poskytují specifickou službu. Klientovi je pak poskytnuta IP adresa pouze jednoho z těchto počítačů, ideálně takového, který je nejméně vytížený. Doménová jména se taktéž používají k rozlišení služeb, například doménové jména začínající prefixem www nejčastěji označují webové servery [7].

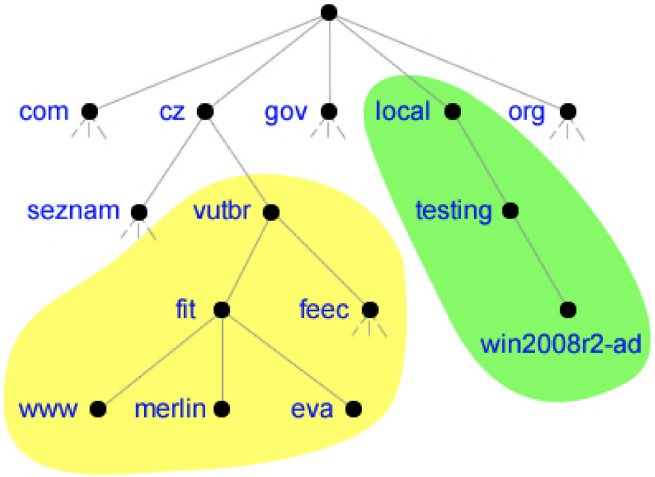
Systém DNS patří mezi decentralizované klient/server systémy. DNS záznamy jsou rozprostřeny po více serverech a je potřeba lokalizovat ty servery, které obsahují požadované informace. Výhodou takového decentralizovaného systému je jeho robustnost, pokud dojde k výpadku několika serverů, stále by mělo existovat dosti dalších, jež jsou schopny poskytnout požadované informace. Robustnost je pro systém DNS klíčová vlastnost [7].

3.3.1 Hierarchie DNS

Systém DNS je hierarchický prostor doménových jmen (Domain Name Space), jenž tvoří obecný strom. Příklad části stromu DNS je zobrazen na obrázku 3.8. Kořenem stromu (označovaný taktéž jako root) je prázdný, nepojmenovaný uzel. Ostatní uzly stromu jsou pojmenovány textovými řetězci o délce maximálně 63 znaků. Název nesmí obsahovat tečky, protože tečky slouží jako oddělovače jednotlivých úrovní stromu. Podle specifikace systému DNS může mít strom až 127 úrovní.

Plně kvalifikované doménové jméno neboli FQDN (Fully Qualified Domain Name) je posloupností názvů jednotlivých uzlů na cestě ke kořeni oddělených tečkami. Například pro uzel win2008r2-ad ve stromu na obrázku 3.8 bude jeho plně kvalifikované doménové jméno win2008r2-ad.testing.local. (s tečkou na konci). Ukončující tečka vyplývá z existence prázdného kořenového uzlu, i ten je oddělen tečkou od názvu ostatních uzlů. V praxi se ovšem často poslední tečka vynechává, jelikož musí být vždy přítomná a může být doplněna automaticky při tvorbě požadavku pro překlad zadaného doménového jména. Maximální přípustná délka plně kvalifikovaného doménového jména je 255 znaků [7].

Relativní doménové jméno je doménové jméno bez ukončující tečky, je reprezentováno k relativní doméně, ve které se nachází. Například pokud v doméně TESTING zadáme relativní doménové jméno win2008r2-ad, bude primárně interpretováno jako win2008r2-



Obrázek 3.8: Část hierarchického stromu prostoru doménových jmen [7]

ad.testing.local., jelikož jsme v doméně testing.local., na relativní doménové jméno lze tedy nahlížet jako na prefix plně kvalifikovaného doménového jména [7].

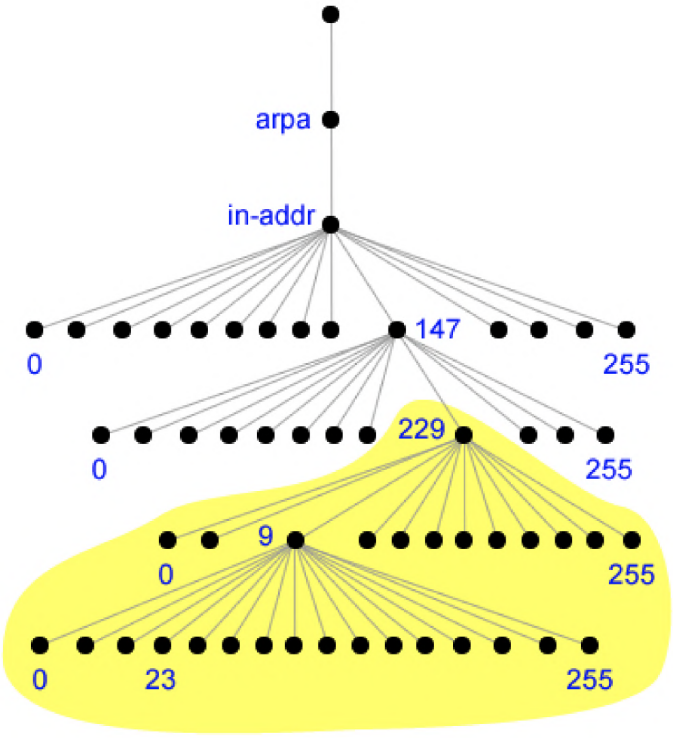
Doména je podstromem stromu doménových jmen. Název domény (Domain Name) je cesta mezi uzlem, jenž tvoří vrchol domény a kořenem celého stromu. Příkladem mohou být domény vutbr.cz. (vyznačena žlutě) a testing.local (vyznačena zeleně) ve stromu znázorněném na obrázku 3.8. Domény první úrovně jež mají vzdálenost 1 od kořene stromu, se často označují jako TLD (Top Level Domain) a jsou buď tématické[8] nebo státní[9]. Ostatní domény se označují podle vzdálenosti od kořene stromu jako domény druhého řádu, třetího řádu atd. nebo jako subdomény domén nižšího řádu. Často se jako domény chybně označují samotné uzly doménového stromu, ty tvoří ovšem jen prefixy konkrétních domén. Na rozdíl od doménových jmen u domén neexistuje žádný relativní zápis, každá doména musí být plně určena [7].

Výhodou stromové hierarchie DNS je možnost administrativního rozdělení jednotlivých domén, kdy konkrétní domény jsou spravovány samostatnými subjekty (buď organizacemi nebo soukromými osobami) [7].

Systém DNS však neslouží pouze pro překlad doménových jmen na IP adresy, ale i naopak. Tento překlad se označuje jako reverzní mapování a často se využívá k ověření překladu, kdy se kontroluje zda IP adresa počítače má v DNS odpovídající doménovou adresu. Pokud takovou adresu nemá lze ji vyhodnotit jako podvrženou nebo neplatnou. Takovýto typ ověření se často provádí u poštovních serverů. Informace pro tento druh překladu jsou uloženy ve speciální doméně jménem in-addr.arpa., kde v případě IPv4 adres tvoří jednotlivé uzly stromu osmibitová čísla v rozsahu 0 až 255, jež jsou vždy reprezentací osmi bitů IPv4 adresy.Strom pro reverzní mapování IPv4 adres na doménová jména je znázorněn na obrázku 3.9. Obdobně i pro IPv6 existuje speciální doména ip6.arpa., kde jednotlivé uzly tvoří čtyřbitová čísla [7].

[8] Příkladem tématické domény může být org pro organizace, gov pro vládní a edu pro vzdělávací instituce [7].

[9] Příkladem státní TLD domény může být cz pro Českou republiku nebo sk pro Slovenskou republiku [7].



Obrázek 3.9: Část stromu pro reverzní překlad IPv4 adres [7]

Například IPv4 adrese 147.229.9.23 ve stromu na obrázku 3.9 pro reverzní mapování odpovídá záznam 23.9.229.147.in-addr.arpa., kde in-addr.arpa. je speciální doménou druhého řádu [7].

3.3.2 Služba DNS

Služba DNS je typu klient/server a lze ji proto rozdělit na dvě části. První část tvoří DNS server[10], který obsahuje jednotlivé záznamy potřebné pro překlad doménového jména na IP adresu a zpět. Druhou částí systému DNS je klient, jenž je často označován jako resolver, který zprostředkovává překlad doménových jmen aplikacím. Pro komunikaci využívá systém DNS protokol, jež běží nad protokoly TCP i UDP na portu 53. Vetšinou se využívá pro přenos na transportní vrstvě (L4) protokol UDP, a to protože poskytuje vyšší rychlost přenosu. Vyšší rychlost je je v případě DNS klíčová. Protokol TCP se ve službě DNS používá výhradně pro přenos zónových souborů[11] mezi DNS servery [7].

[10] DNS server může být buď autoritativní nebo neautoritativní. Autoritativní server poskytuje odpovědi, jež jsou vždy aktuální a neautoritativní server poskytuje odpovědi,které mohou být již neplatné [7].

[11] Zóna obsahuje záznamy pro danou doménu nebo více domén. Zóna může být primární (obsahuje veškeré záznamy pro danou doménu a jako jediná umožňuje tyto záznamy přímo modifikovat), sekundární (obsahuje stejně jako primární veškeré záznamy pro danou doménu, tyto záznamy jsou ale pouze pro čtení a nelze je přímo modifikovat, pouze přenosem zóny) nebo stub (obsahuje pouze informace potřebné pro kontaktování nějakého autoritativního serveru) [7].

3.3.3 DNS záznamy

DNS server ukládá informace, jež jsou potřebné pro překlad doménových jmen a IP adres ve formě DNS záznamů. Existují různé typy DNS záznamů, každý typ poskytuje specifické informace. Mezi nejčastěji používané patří tyto typy DNS záznamů:

- **A** (Address) záznam obsahuje mapování doménového jména na odpovídající IPv4 adresu ve formátu `<doménové jméno> IN A <IPv4 adresa>` [7].
- **AAAA** (IPv6 Address) záznam obsahuje mapování doménového jména na odpovídající IPv6 adresu ve formátu `<doménové jméno> IN AAAA <IPv6 adresa>` [7].
- **CNAME** (Canonical Name) je záznam označovaný jako alias. Obsahuje mapování jednoho doménového jména na jiné. Tento typ záznamu umožňuje flexibilní pojmenování jednoho serveru více doménovými jmény. Stejného efektu jako použití záznamu CNAME lze dosáhnout i použitím více A nebo AAAA záznamů, ovšem v případě změny je nutné změnit všechny A nebo AAAA, kdežto u použití záznamu typu CNAME postačí pouze změnit jediný A nebo AAAA záznam a tím dojde ke změně mapování všech CNAME záznamů. Formát CNAME záznamu je `<zdrojové doménové jméno> IN CNAME <cílové doménové jméno>` [7].
- **MX** (Mail exchange) záznam obsahuje adresu a prioritu serveru pro příjem elektronické pošty pro danou doménu (zónu) ve formátu `<doména> IN MX <priorita> <doménové jméno>`, kde <doména> identifikuje cílovou doménu, <doménové jméno> cílový poštovní server a <priorita> je nezáporné číslo určující prioritu daného serveru. Čím je menší číslo, tím má server vyšší prioritu [7].
- **TXT** (Text) záznam obsahuje libovolný textový řetězec. TXT záznam se využívá například pro ověření vlastníka domény, kdy Vás poskytovatel hostingových či jiných služeb požádá o vložení TXT záznamu s určitým textem do DNS. Dalším příkladem použití záznamu TXT je pro SPF (Sender Policy Framework)[12]. Záznam TXT bývá zapsán ve formátu `<doménové jméno> IN TXT <text>`, kde <text> identifikuje požadovanou hodnotu (text) záznamu [7].
- **NS** (Name Server) záznam obsahuje doménové jméno autoritativního DNS serveru pro danou doménu ve formátu `<doména> IN NS <doménové jméno>`. Autoritativních serverů může být pro jednu doménu více [7].
- **PTR** (Pointer) záznam mapuje IP adresu počítače na odpovídající doménové jméno, slouží k reverznímu mapování. Tento záznam je obdobou A záznamu pro reverzní zóny. Formát je ve tvaru `<arpa doménové jméno> IN PTR <doménové jméno>`, kde <arpa doménové jméno> je IP adresa zapsaná ve formě doménového jména z domény in-addr.arpa. (pro IPv4) nebo ip6.arpa. (pro IPv6), tedy z domény pro reverzní mapování [7].
- **SOA** (Start of Autority Server) záznam obsahuje základní informace pro danou zónu, přesněji jméno primárního DNS serveru, elektronickou adresu správce zóny (v elektronické adrese správce se zavináč nahrazuje tečkou) a několik dalších údajů. Dalšími údaji SOA záznamu je Serial (obsahuje informace o sériovém čísle dané zóny, při každé

[12] SPF je speciální DNS záznam, pro definování, které SMTP servery (IP adresy) jsou pro danou doménu autorizované při odesílání e-mailů [7].

změně se inkrementuje o jedna), Refresh (je číslo určující v jakém intervalu se bude sekundární server dotazovat na změny zóny primárního serveru), Retry (je číslo určující za jak dlouho se má sekundární server dotazovat na změny zóny primárního serveru v případě, že se nepodařilo primární server kontaktovat), Expire (je číslo určující za jak dlouho sekundární server označí své záznamy za neaktuální a přestane vyřizovat příchozí požadavky na překlad) a TTL (Time To Live je číslo určující implicitní dobu platnosti jednotlivých DNS záznamů). Formát SOA záznamu je ve tvaru `<doména> IN SOA <primární DNS server> <e-mail> (<serial> <refresh> <retry> <expire> <ttl>)` [7].

Typ záznamu	Překlad	Formát
A	Doménové jméno (DN) → IPv4 adresa (IPv4)	*<DN>* **IN A** *<IPv4>*
AAAA	Doménové jméno (DN) → IPv6 adresa (IPv6)	*<DN>* **IN AAAA** *<IPv6>*
CNAME	Doménové jméno (DN) → Doménové jméno (DN)	*<DN>* **IN CNAME** *<DN>*
MX	Doména (D) → Doménové jméno serveru (DN)	*<D>* **IN MX** *<priorita>* *<DN>*
PTR	IP adresa (IP) → Doménové jméno (DN)	*<IP>* **IN PTR** *<DN>*
NS	Doména (D) → Doménové jméno serveru (DN)	*<D>* **IN NS** *<DN>*
SOA	Doména (D) → Doménové jméno serveru (DN) Elektronická adresa správce (MAIL) Informace o zóně (viz výše)	*<D>* **IN SOA** *<DN>* *<MAIL>* **(** *<serial>* *<refresh>* *<retry>* *<expire>* *<ttl>* **)**

Obrázek 3.10: Nejužívanější typy DNS záznamů [7]

Na obrázku 3.10 je znázorněna tabulka s nejužívanějšími typy DNS záznamů spolu s informace o překladu, jenž daný záznam provádí a formátu zápisu tohoto záznamu v zónovém souboru.

3.4 Systém DHCP

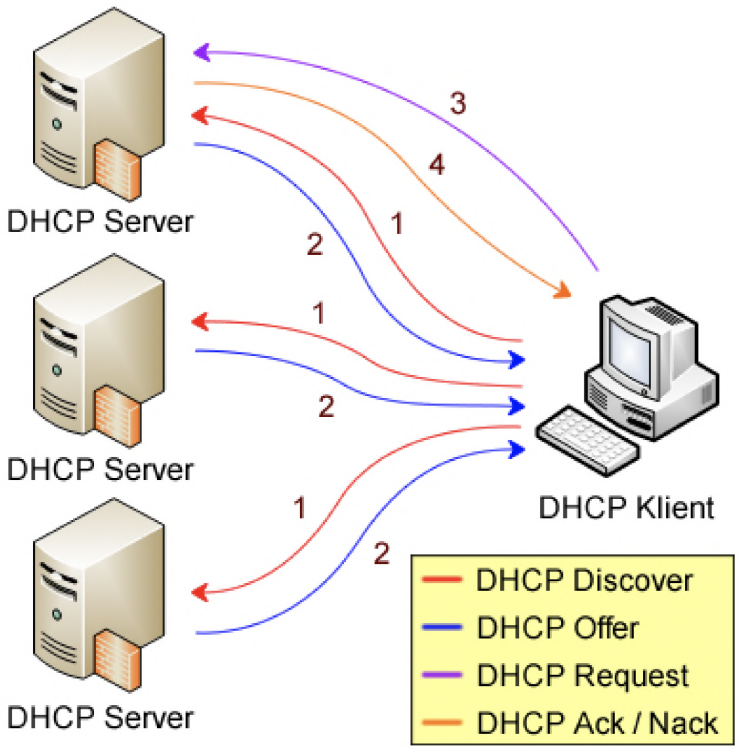
K zajištění konektivity mezi počítači v malé síti nám postačí manuálně nastavit jednotlivá síťová rozhraní. Často to není ani nutné, protože ve většině operačních systémů je k dispozici funkce pro automatické přidělení IPv4 adres pomocí systému APIPA. Pokud ovšem pracujeme v rozsáhlejší síti, kde jsou dokonce i servery, nejsou předchozí možnosti příliš použitelné. Manuální konfigurace IP adres je pracná a náchylná na chyby způsobené uživatelem, například chybným zadáním nezbytných údajů. Použití systému automatického přidělení IPv4 adres APIPA je nepřijatelné protože pravděpodobnost, že se podaří každému počítači vygenerovat do deseti pokusů unikátní IPv4 adresu je v tomto počtu nízká [7].

Systém DHCP slouží k automatické konfiguraci síťových rozhraní. Umožňuje nastavit IPv4 adresy, masky podsítě, výchozí brány, adresy DNS i WINS serverů a další informace. Konfigurace jednotlivých síťových rozhraní je realizována pomocí protokolu DHCP (Dynamic Host Configuration Protocol), jež vzniknul jako rozšíření protokolu BOOTP, který sloužil pro bootování bezdiskových stanic. Protokol BOOTP byl schopen pouze přidělovat IPv4 adresu, masku podsítě, adresu TFTP (Trivial File Transfer Protocol) serveru, na němž byl umístěn bootovací obraz a cestu k tomuto obrazu. Protokol DHCP je s BOOTP zpětně kompatibilní [7].

3.4.1 Služba DHCP

Služba DHCP je typu klient/server a lze ji proto rozdělit na dvě části. První část tvoří DHCP server, jenž obsahuje informace o IP adresách přidělených jednotlivým rozhraním. Druhou částí je DHCP klient, který od DHCP serveru zjišťuje informace potřebné pro konfiguraci jednotlivých síťových rozhraní. Pro komunikaci využívá DHCP protokol, jež běží na transportní vrstvě (L4) nad protokolem UDP na portech 67 (server) a 68 (klient). Komunikace je vždy realizována pomocí všesměrového vysílání (broadcast), protože jen to lze využít v případě, kdy rozhraní ještě nemá přidělenou IP adresu [7].

3.4.2 Přidělování IPv4 adres pomocí DHCP



Obrázek 3.11: Průběh přidělování IPv4 adres pomocí DHCP (DORA) [7]

Základní princip přidělování IPv4 adres je znázorněn na obrázku 3.11. Postup přidělování IPv4 adres DHCP serverem lze shrnout do následujících kroků:

1. DHCP klient zašle všesměrovou (broadcast) zprávu **DHCP Discover** všem DHCP serverům v dané síti, touto zprávou žádá o přidělení IPv4 adresy [7].

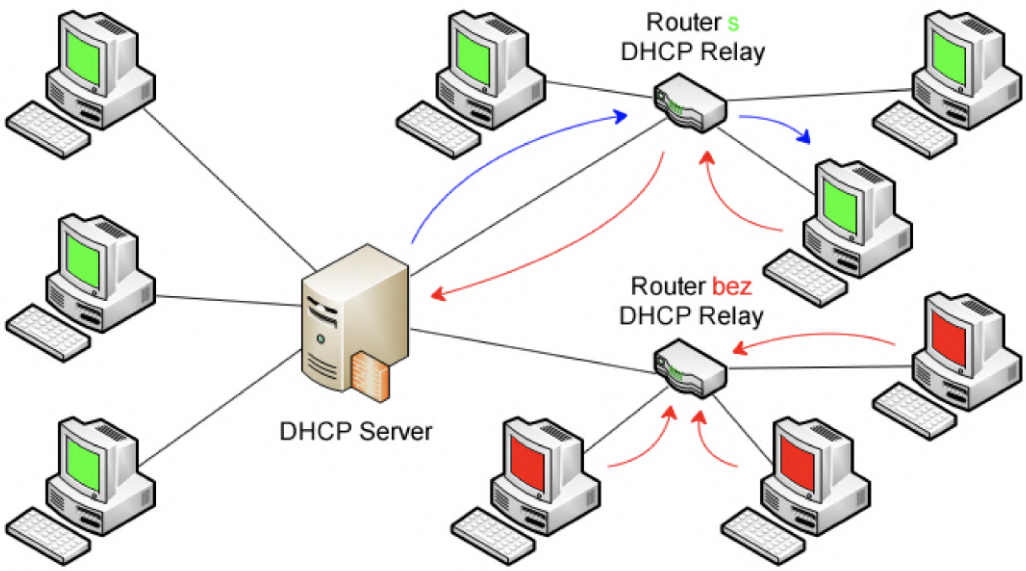
2. Každý jednotlivý DHCP server zašle zpět všesměrovou zprávu**DHCP Offer**, jež obsahuje IPv4 adresu, kterou server nabízí k použití. V případě, že DHCP server již nemá k dispozici ze svého adresního rozsahu (poolu) žádné volné IPv4 adresy pro zapůjčení, nijak na žádosti nereaguje [7].

3. DHCP klient čeká na nabídky od DHCP serverů, z přijatých nabídek vybere jedinou (nejčastěji je implementace realizována tak, že klient použije první příchozí) a

odpoví na ni všesměrovou (broadcast) zprávou **DHCP Request**, kterou potvrzuje svůj zájem o použití nabízené IPv4 adresy [7].

4. DHCP server jež IPv4 adresu nabídnul ověří, zda je možné opravdu tuto IPv4 adresu zapůjčit a v případě, že ano, zašle zpět všesměrovou (broadcast) zprávu **DHCP Ack**, kterou potvrzuje zapůjčení této IPv4 adresy. V případě, že požadovaná adresa již není k dispozici k zapůjčení (byla již někomu jinému zapůjčena), odpoví DHCP server všesměrovou (broadcast) zprávou **DHCP Nack**. DHCP klient po obdržení zprávy **DHCP Nack** musí zažádat znovu o (jinou) IPv4 adresu [7].

Tento postup přidělování IPv4 adres se označuje jako DORA (Discover, Offer, Request, Ack) a slouží klientům, kteří ještě nemají přidělenou žádnou IPv4 adresu. Adresa je vždy DHCP serverem přidělována jen na konkrétní (určitou) dobu, jež určuje DHCP server. DHCP klient musí pravidelně tuto dobu prodlužovat zasláním žádosti o prodloužení výpůjčky (lease renewal) [7].



Obrázek 3.12: Znázornění funkce routeru s DHCP s relay a routeru bez DHCP relay [7]

Po vypršení poloviny doby platnosti výpůjčky IPv4 adresy se začne DHCP klient pokoušet prodloužit dobu její platnosti. Žádost o prodloužení je realizována zasláním běžné (unicast) zprávy **DHCP Request** DHCP serveru, který zapůjčil danou IPv4 adresu. Tento DHCP server buďto prodloužení výpůjčky potvrdí pomocí zprávy **DHCP Ack** nebo zamítne zprávou **DHCP Nack**. V případě, že je prodloužení výpůjčky IPv4 adresy zamítnuto, klient si ponechá IPv4 adresu do konce doby její platnosti a poté zažádá o novou. V případě, že se DHCP klientovi nepodaří do prodloužit výpůjčku do 7/8 doby její platnosti, pokusí se klient kontaktovat jakýkoliv DHCP server, který ji může prodloužit. Prodloužení se provede stejným způsobem jako v předchozím případě, jen **DHCP Request** je zaslán všesměrově (broadcast) všem DHCP serverům. Pokud se DHCP klientovi vůbec nepodaří prodloužit výpůjčku do vypršení její doby platnosti, tak v tomto případě znovu zažádá po vypršení o novou IPv4 adresu [7].

3.4.3 DHCP relay

Hlavní nevýhodou systému DHCP je jeho závislost na všesměrovém vysílání (broadcast). DHCP zprávy nelze standardně šířit za hranice směrovačů do jiných sítí nebo podsítí. Funkce DHCP relay slouží k přeposílání DHCP zpráv do jiných sítí respektive k směrování DHCP zpráv z dané sítě nebo podsítě na DHCP server v jiné síti nebo podsíti a naopak. Schéma funkce DHCP relay je znázorněno na obrázku 3.12 [7].

3.5 Active Directory

Active Directory nyní přesněji doménové služby Active Directory (AD DS, Active directory Domain Services) je implementací adresářových služeb společností Microsoft. Slouží jako úložiště informací o uživatelích, počítačích i službách, zajišťuje autentizaci uživatelů včetně počítačů a umožňuje také vyhledávání i přístup ke zdrojům, případně distribuci politik včetně konfigurace počítačů nebo instalaci programového vybavení. Tato funkcionalita se též označuje často jako řešení identity a přístupu (IDA, Identity and Access). Hlavním úkolem IDA je zajistit bezpečnost podnikových zdrojů (souborů, aplikací, databází...) a to díky uložení informací(o uživatelích, skupinách, počítačích a jiných identitách), autentizaci identit, řízení přístupu a auditování. Jak již bylo zmíněno výše Active Directory je adresářová služba obsahující informace o uživatelích, počítačích a dalších entitách. Tyto entity jsou reprezentovány objekty příslušného typu a informace o těchto entitách jsou uloženy ve formě atributů daného objektu. Ze všech typů entit lze vyzdvihnout tři nejpoužívanější a to jsou uživatelé, skupiny a počítače [7].

V Active Directory, jakožto řešení IDA je uživatel hlavní komponentou identity, proto je nutné dobře se vyznat v jak uživatelských účtech tak v úkonech, které se jich týkají. Efektivní práce s uživatelskými účty má výrazný vliv na celkovou produktivitu. Active Directory může mít velikost i tisíce uživatelských účtů, a proto je vhodné vytváření účtů automatizovat a to například pomocí ADUC (Active Directory Users and Computers), použitím šablon účtů (account templates), příkazy Windows PowerShell nebo VBSkriptem (Vbscript) [7].

Dalším důležitým typem objektů jsou skupiny. Hlavním úkolem skupiny je umožnit jednoduchou správu kolekcí objektů, nejčastěji uživatelů nebo počítačů. Další využití skupiny je závislé na jejím typu. Existují celkem dva typy skupin:

- **Distribuční** (Distribution) skupiny jsou určeny primárně pro e-mailové aplikace. Zpráva jež je adresována distribuční skupině je doručena všem členům takové skupiny. Jelikož distribuční skupiny nemají SID (Security Identifier), nelze jim nastavovat oprávnění pro přístup ke zdrojům [7].

- **Bezpečnostní** (Security) skupiny mají SID a lze jim přidělovat oprávnění pro přístup ke zdrojům. Přesněji mohou být tyto skupiny použity jako záznamy oprávnění (permission entries) v ACL (Access Control List). Bezpečnostní skupiny mohou být použity taktéž jako distribuční skupiny, což se ovšem nedoporučuje. SID všech bezpečnostních skupin, kterých je uživatel členem, se totiž přidávají do jeho security access tokenu. Náhrada distribučních skupin bezpečnostními znamená, že zbytečně naroste SID v security access tokenu daného uživatele [7].

3.6 Virtualizace

Virtualizace je fenoménem dnešní doby. Virtualizace nám umožňuje spustit jeden či více virtuálních stanic nad jedním fyzickým hostitelem. S virtualizací se nejen v serverovnách podniků můžeme setkat na několika úrovních. Typem virtualizace, kterým se zabývá tato diplomová práce je virtualizace operačního systému hosta nebo virtualizace serveru. Virtualizace operačního sytému umožňuje zpřístupnit prostředky fyzického serveru několika různým virtuálním počítačům současně. Technologie virtualizace operačního systému existují ve dvou podobách a to v podobě softwarové vrstvy nad stávajícím operačním systémem, která se používá k simulaci fyzického počítače s hardwarem hostitele nebo v podobě softwarového jádra, jež běží přímo nad fyzickým hardwarem a eliminuje režii mít nad hardwarem další operační systém [20].

Virtualizace je technologie, která je na trhu již poměrně dlouho. Historie virtualizace se datuje až na konec 60. let minulého století ke společnosti IBM. Virtualizace je stará již 50 let, ale její hlavní myšlenkové koncepty se příliš nezměnily. Virtualizace u serverových operačních systémů odstraňuje závislost na hardwaru fyzického serveru, což umožňuje snadnější nasazení a přesunutí. Všechny nové servery se již v dnešní době nasazují formou virtuálních počítačů (VM), pokud neexistuje opodstatněný racionální důvod proč podpořit instalaci serveru na fyzickém hardware bez virtualizace. Při údržbě není potřeba dělat odstávku virtualizovaných serverů, ale pouze jejich migraci nejlépe v reálném čase do jiného fyzického serveru. Po dokončení migrace mohou správci fyzický server vypnout a provést hardwarovou údržbu, která nemusí být jako dříve plánovaná na víkend nebo pozdní večerní či ranní hodinu, ale může být realizována ve standardní pracovní době [20].

Virtualizace odstranila tradiční složitosti při testech zotavení po haváriích v produkčním prostředí. Díky virtualizaci je tak možné testovat zotavení po havárii častěji než kdy dříve a to dodává patřičnou míru důvěry IT oddělení v plán obnovy pro případ havárie serverové infrastruktury [20].

3.6.1 Definice virtualizace

Software virtualizace vytvoří jednu či více virtuálních pracovních stanic nebo serverů ve fyzickém systému. Virtualizace je závislá na tom jaké zdroje jsou k dispozici na skutečném počítači, například místo na disku, možnosti procesoru, síťové karty, velikost operační paměti RAM a podobně [20].

Základním předpokladem pro virtualizaci je vytváření oddílů na fyzických počítačích (partitioning). Tato možnost je v počítačích od šedesátých let minulého století, kdy začala společnost IBM vytvářet oddíly na svých sálových počítačích, aby hostily více instalací jejich operačního systému. V případě sálových počítačů společnosti IBM byla technologie vytváření oddílů použita ke spouštění více systémů, nebo lépe ke spouštění více paralelních instancí jednoho operačního systému. Navzdory tomu, že byla společnost IBM s představením vytváření oddílů první, tak se tento typ začal používat až v 90. letech století minulého, kdy byl přestaven u procesorů architektury x86. V této době se také vytváření oddílů přejmenovalo na virtualizaci. Tento první typ virtualizace byl představen z toho důvodu aby uživatelům provozovat operační systémy Windows na jiných platformách například na Apple Macintosh. V roce 2003 společnost Microsoft provedla akvizici francouzské společnosti Connectix, která se specializovala na vytváření softwaru pro virtuální počítače, určeného ke spouštění operačních systémů Microsoft Windows na počítačích Apple Macintosh, čímž byl uživatelům platformy Macintosh umožněn přístup k tisícům aplikací dostupných na

platformě Windows. Další společností, která se zabývala virtualizací již od 90. let minulého století je VMware Corporation. Společnost VMware si uvědomovala potenciál virtualizace a přišla s možností virtualizace serverů, čímž začal rozkvět virtualizace, jehož jsme svědky i dnes [20].

Aktuální stav virtualizace je takový, že se technologie natolik vyvinula a je ji proto možné použít nejen v datovém centru na více vrstvách. Pro správné použití virtualizace na různých vrstvách je potřeba jejich dobré porozumění. Mezi základní vrstvy virtualizace patří:

- Serverová virtualizace (SerV) - tento typ virtualizace se zaměřuje na rozdělení fyzické instance operačního systému na virtuální instanci nebo přímo virtuální počítač. Produkty skutečné serverové virtualizace umožňují virtualizovat libovolný operační systém platformy x86 nebo x64. Techniky virtualizace této vrstvy budou blíže popsány v kapitole 3.6.2.

- Virtualizace úložišť (StoreV) - používá se pro sloučení fyzického datového úložiště z více zařízení, tak aby se jevilo pro okolí jako jeden fond úložišť. Úložiště v tomto fondu může být buď přímo připojené (DAS), síťové připojené úložiště (NAS, Network Attached Storage) nebo sítě úložišť SAN (Storage Area Network) a lze je propojit pomocí několika protokolů. Příkladem propojovacího protokolu pro připojení fondu úložišť může být Fibre Channel, Internet SCSI (iSCSI), Fibre Channel on Ethernet, nebo dokonce prostřednictvím protokolu NFS (Network File System). Virtualizace síťových úložišť není pro serverovou virtualizaci nezbytná. Jedna z klíčových výhod použití virtualizace úložišť je použití thin provisioningu nebo přiřazení logické jednotky (LUN) úložiště o určité velikosti. Přidělení prostoru funguje na bázi přidělování podle skutečné potřeby. Například pokud vytvoříme logickou jednotku o kapacitě 1 TB a používáme pouze 360 GB tak bude poskytnuto pouze 360 GB aktuálního úložiště. Tím se značně sníží náklady na úložiště, neboť se platí jen za skutečně využívaný prostor [20].

- Virtualizace sítí (NetV) - umožní řídit dostupnou šířku pásma jejím rozdělením na nezávislé kanály, jež lze přiřadit konkrétním zdrojům. Nejjednodušším způsobem virtualizace sítí je virtuální lokální síť (VLAN), která vytváří logické oddělení na fyzické vrstvě sítě. Produkty serverové virtualizace dnes již v základu nabízejí podporu pro vytváření virtuálních síťových vrstev v samotném produktu. Použití této integrované virtuální síťové vrstvy nám umožňuje umístit hraniční síť na stejného hostitele jako ostatní virtuální provozní zátěž bez ovlivnění kterékoliv ze sítí nebo umožnění virtuálním počítačům mezi sebou vzájemně komunikovat (přistupovat) [20].

- Správa virtualizace (ManageV) - zaměřuje se na technologie, které spravují celé datové centrum, jak fyzické, tak i virtuální, a které poskytují jedinou a sjednocenou infrastrukturu pro poskytování služeb. Fyzická vrstva by měla používat silná hesla a měla by zaručovat šifrované spojení mezi servery konzolemi pro správu, a to protože jsou hesla posílána právě přes toto spojení [20].

- Virtualizace desktopů (DeskV) - umožňuje nám virtualizovat pracovní stanice uživatelů. Virtualizace desktopů má několik kladů z nichž nejvýznamnější je možnost centralizovaného nasazení desktopů a snížit náklady na distribuovanou správu a to díky tomu, že koncoví uživatelé přistupují ke svým virtualizovaným prostředím prostřednictvím různých tenkých klientů nebo nespravovaných zařízení [20].

- Virtualizace chytrých mobilních telefonů (MobileV) - umožňuje vytvořit virtuální vrstvu na mobilních telefonech, která umožňuje více (mobilních) operačních systémů na stejném chytrém mobilním telefonu. Příkladem může být platforma Samsung DeX, která umožňuje spouštět na chytrém telefonu s operačním systémem Android virtualizovaný Linux Ubuntu. Je tedy možné provozovat jednu platformu pro práci a druhou pro osobní použití [20].

- Virtualizace prezenční vrstvy (PresentV) - tato vstva byla označována dříve jako terminálové služby, jež nabízí uživatelům pouze prezentační vrstvu z centrálního umístění. Potřeba virtualizace prezenční vrstvy klesá díky zavádění nových technologií jako je virtualizace aplikací [20].

- Virtualizace aplikací (AppV) - virtualizace na této vrstvě využívá stejné principy jako softwarově založená serverová virtualizace. Funguje na základě oddělování aplikací od operačního systému. Virtualizace aplikací transformuje model správy distribuovaných aplikací, neboť virtualizovat určitou aplikaci je nutné pouze jednou [20].

K těmto aktuálně osmi vrstvám virtualizace je potřeba znát ještě další základní pojmy, jež jsou součástí jazyku používaného v prostředí datových center. Mezi základní pojmy patří:

Hostitelský server - fyzický server spouštějící příkazy virtuálních počítačů na svém hardware.

Hypervizor (Virtual Machine Monitor, Virtual Machine Manager, VMM) - software na hostitelském serveru, který se stará o správná běh virtuálního počítače včetně přidělování zdrojů. Hypervizory lze rozdělit do dvou tříd nativní (běží přímo na hostitelském hardware, hostovaný operační systém běží pod hypervizorem) a hostovaný (hypervizor běží v OS) [15].

Operační systém hosta - virtualizovaný operační systém běžící na hostitelském serverů.

Fond zdrojů - souhrn hardwarových zdrojů, zahrnující hostitelské servery, jež tvoří infrastrukturu datového centra [20].

3.6.2 Techniky serverové virtualizace

Téma serverová virtualizace je stěžejní částí této diplomové práce proto budou její techniky popsány podrobněji.

Úplná (plná) virtualizace S úplnou virtualizací neupravený operační systém[13] hostí prostor pro program, který emuluje počítač, v němž běží hostovaný operační systém. Plná virtualizace (hardwarová virtualizace) je ve zkratce emulace, ve které virtuální stroj je softwarovou simulací hardwaru a to reálného nebo smyšleného (musíme mít patřičné ovladače). Příkladem úplné virtualizace může být VMware a QEMU. Tento typ virtualizace je oblíbený, protože není nutné aby byl operační systém hosta jakkoliv upraven. Výhodou je, že virtualizovaná architektura může být kompletně odlišná od architektury hosta.

[13] nebo mírně upravený operační systém, například pro QEMU, jež má modul KQEMU do kernelu, který zrychluje emulovaný kód a to tak, že dovoluje aby byl spouštěn přímo na procesoru kdykoliv je to jen možné [22].

QEMU může například simulovat úplně odlišný typ procesoru. Nevýhodou tohoto řešení hardwarové nezávislosti je vysoká rychlostní penalizace. Neakcelerovaný QUMU je řádově pomalejší než nativní provádění instrukcí a akcelerovaný QEMU nebo VMware ESX server je schopen akcelerace instrukcí pouze pokud je emulovaný stroj stejné architektury jako fyzický hardware [22].

3.6.3 Virtualizace operačního systému

Na druhém straně extrému je virtualizace na úrovni operačního systému (softwarová virtualizace). Virtualizováno je v tomto případě jen operační prostřední namísto celého počítače. Příkladem může být FreeBSD jails a Solaris Containers. Virtualizace operačního systému se zakládá na tom, že již v základu umožňuje poskytovat všechny služby operačního systému pro virtuální počítač, který by mohl uživatel chtít použít. Operační systém hosta virtualizovaného počítače je při této technologii izolován a umožňuje uživateli instalovat software, aktualizovat knihovny bez ovlivnění operačního systému na fyzickém serveru. Tento přístup k virtualizaci používá principu toho, že neemuluje fyzický hardware, ale virtualizace operačního systému emuluje celé uživatelské prostředí operačního systému. FreeBSD jails a Solaris Containers (nebo Zones) patří mezi dvě oblíbené implementace technologie virtualizace operačního systému. Oba jsou deriváty klasického Unixového chroot jailu. Myšlenka je taková, že jailed (uvězněný) proces může pouze přistupovat k částem souborového systému, které patří pod danou složku (virtuální počítač). Zbytek souborového systému je pro tento proces nedostupný (neviditelný). Nevýhodou virtualizace operačního systému je může být sdílené jádro (Kernel), které v případě způsobení pádu ve virtuálním počítači způsobí pád i operačního systému hosta a tím i ostatních virtuálních počítačů běžících na stejném fyzickém serveru. Výhodou je naopak to, že není nutné virtualizovat žádný hardware a vykonávání instrukcí je tak stejně rychlé jako by bylo při zpracovávání přímo na fyzickém hardware [22].

3.6.4 Paravirtualizace

Tento typ virtualizace patří mezi hardwarovou virtualizaci a spoléhá na upravený operační systém, který spolupracuje s nadřazeným operačním systémem (hypervizorem) na fyzickém serveru. Předpokladem je, že nebude virtualizován celý hardware, ale že jsou některé komponenty společné jak pro fyzický server tak virtualizovaný server například procesor. Tento typ virtualizace tedy nepatří mezi plnou virtualizaci ani virtualizaci operačního systému. V případě paravirtualizace neběží operační systém hosta s plnými oprávněními. Jediný hypervizor má k dispozici plná oprávnění k nakládání s hardware. Hypervizor je navržen aby byl co nejjednodušší a nejmenší. Hypervizor (dom0) se stará pouze o nejzákladnější funkce. Spravuje procesorový času, přerušení, paměť, blokuje zařízení a síť. Hypervizor tedy funguje jako velmi malé jádro tradičních operačních systémů, rozděluje čas procesoru a zdrojů mezi operační systémy, které běží pod ním. Stejně jako moderní operační systémy mohou transparentně pozastavit proces, tak může hypervizor pozastavit celý operační systém hosta a předat kontrolu dalšímu operačnímu systému hosta (virtuálnímu počítači) a poté znovu zpět pozastavenému operačnímu systému hosta. Hypervizor má právo nakládat s fyzickou pamětí serveru (RAM) a tabulkou stránek, do nichž je fyzická paměť rozdělena. Každý jednotlivý virtuální počítač má přidělen unikátní adresní prostor. Nejznámějšími příklady paravirtualizace je Xen a VMware Workstation [22].

3.7 Konsolidace

Konsolidací se rozumí snížení počtu serverů. Rozlišujeme dva typy konsolidace a to konsolidaci serverů a fyzickou konsolidaci. Konsolidace serverů znamená snížení počtu serverů datovém centru, vytvoření větších serverů, jež hostí vetší míru pracovní zátěže. Cílem konsolidace by mělo být po jejím dokončení menší množství serverů, než na začátku před konsolidací. Mezi konsolidované servery by měly patřit i fyzické servery, které hostí virtuální počítače. Nejlepší dobou pro konsolidaci serverů je změna nebo migrace na novou virtualizační infrastrukturu. Procesu konsolidace fyzických hardwarových zařízení se nazývá fyzická konsolidace. Konsolidovat můžeme například i routery a switche [20].

Při procesu konsolidace bychom si měly položit následující otázky:

- Jaká je průměrná míra využití každého počítače (ať již fyzického tak virtualizovaného)
- Jsou v síťové infrastruktuře podniku nevyužívané zařízení nebo počítače?
- Existují v síti nějaké zastaralé počítače nebo zařízení?
- Je k dispozici nějaký způsob jak sloučit pracovní zátěž?
- Existuje nějaký způsob jak snížit počet hardwarových prvků nebo počítačů?

3.7.1 Kategorie serverů podle zdrojů

Role serverů nebo můžeme rozdělit do následujících skupin:

- Fyzické servery a servery síťové infrastruktury - tyto servery poskytují základní síťové funkce, příkladem může být přidělování IP adres (DHCP server), překlad doménových jmen na IP adresy (DNS server), poskytování služeb virtuální privátní sítě (VPN server) a směrování. Služby těchto serverů jsou většinou nezbytné pro provoz dalších serverů a prvků klientských zařízeních v podnikové síti.
- Servery pro správu identit (adresářové služby) - tyto servery jsou hlavními správci identit pro podnikovou síť, obsahují a spravují databázi s daty identit pro všechny uživatele ve firemní síti. Příkladem adresářových služeb může být protokol LDAP (Lightweight Directory Access Protocol) nebo v případě Windows služby AD DS (Active Directory Domain Services). Správa identit by neměla být sdílena s jinou funkcí, pokud se nejedná o klíčovou síťovou funkci například DNS (Domain Name System).
- Souborové a tiskové servery - úkolem těchto serverů je poskytování služeb datového úložiště a strukturovaných dokumentů v síti. Tyto servery tvoří základ pro sdílení informací v podniku.
- Aplikační servery - tyto servery poskytují služby aplikací uživatelům v podnikové síti. Příkladem může být e-mailový server, SQL server atd.
- Terminálové servery - tyto servery pro připojení přes vzdálenou plochu z terminálových klientů poskytují jednotné centrální prostředí pro spouštění aplikací. Uživatelé potřebují mít jen minimální infrastrukturu pro přístup k těmto serverům, protože celé spouštěcí prostředí se nachází a běží ze serveru samotného.

- Kolaborační servery - cílem těchto serverů je poskytovat infrastrukturu pro spolupráci uvnitř podniku. Příkladem může být Microsoft SharePoint, služby pro streamování médií nebo sjednocená komunikace v podniku.

Servery lze dále kategorizovat podle jejich umístění a typu serveru. Servery v kancelářích jsou běžně typu `tower`, kdežto v datovém centru se využívají převážně servery typu `rack` nebo blade serverů pro umístění do datových rozvaděčů [20].

Rovněž lze aplikace nebo pracovní zátěž rozdělit do skupin:

- kritické aplikace,
- aplikace klíčové pro obor podnikání,
- aplikace pro podporu podnikání,
- aplikace infrastruktury,
- aplikace zastaralé nebo aktualizované,
- komerční aplikace nebo vnitropodnikové aplikace.

Každá z těchto skupin aplikací je při konsolidaci důležitá a je vhodné servery do těchto kategorií rozdělit [20].

Kapitola 4

Analýza současného stavu

V této kapitole bude přestaven podnik SPOLEČNOST-24 s.r.o., kapitola taktéž bude obsahovat analýzu současného stavu informačních technologií v analyzované společnosti. Prostředí ve společnosti znám velmi dobře, protože v ní již déle než tři roky pracuji.

4.1 Představení společnosti

4.1.1 Základní informace o společnosti

Společnost byla založena 26. března 2014, je evidována pod spisovou značkou C 82582 vedenou u Krajského soudu v Brně. Její celý obchodní název je SPOLEČNOST-24 s.r.o. a sídlí na adrese Mezírka 775/1, Veveří, 602 00 Brno [21].

Obrázek 4.1: Firemní logo - SPOLEČNOST-24 s.r.o. [21]

Identifikační číslo: 028 20 358
Právní forma: Společnost s ručením omezeným
Předmět podnikání: Výroba, obchod a služby neuvedené v přílohách 1 až 3 živnostenského zákona.
Klasifikace ekonomických činností podle CZ-NACE:

- 461: Zprostředkování velkoobchodu a velkoobchod v zastoupení.
- 68: Činnosti v oblasti nemovitostí.
- 749: Ostatní profesní, vědecké a technické činnosti j. n.
- 7729: Pronájem a leasing ostatních výrobků pro osobní potřebu a převážně pro domácnost.

- 8129: Ostatní úklidové činnosti.
- 8211: Univerzální administrativní činnosti.
- 855: Ostatní vzdělávání.

Zařazení podniku do institucionálního sektoru podle ESA2010 11003: Nefinanční podniky soukromé pod zahraniční kontrolou.

Statutární orgán – jednatel: Ing. Miroslav Koch

Společníci: COMPANY-24 LTD. se sídlem Londýn, 207 Regent Street, Spojené království Velké Británie a Severního Irska (100% podíl)

Základní kapitál: 20 000,- Kč

4.1.2 Popis společnosti

Společnost bude popsána pomocí rámce 7S společnosti McKinsey[1], jež slouží k analýze interního prostředí.

Strategie Hlavní strategií společnosti je zaměření na poskytování lepší služby než konkurent za stejnou cenu (strategie diferenciace neboli odlišení). SPOLEČNOST-24 s.r.o. se zaměřuje na poskytování outsourcingových služeb v oblasti správy pohledávek pro právnické osoby i fyzické osoby, advokáty a insolvenční správce.

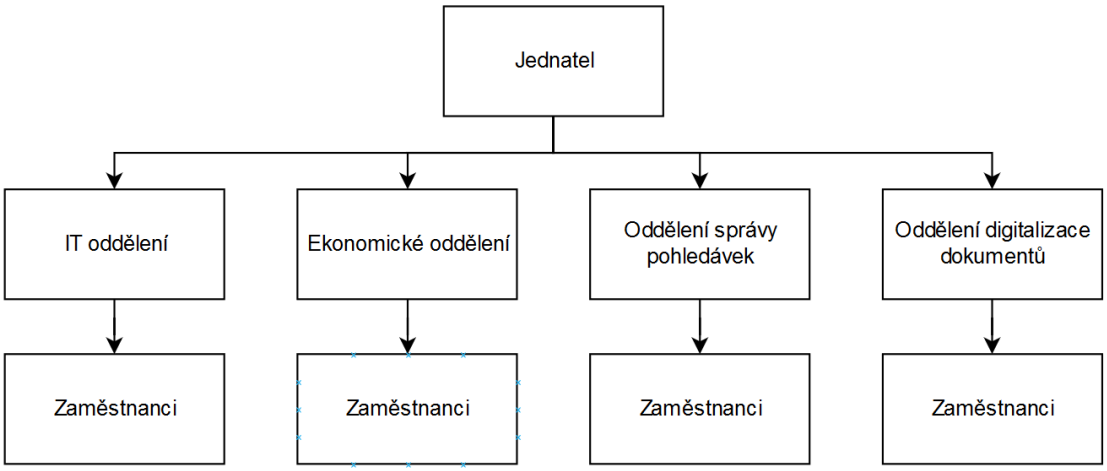
Poskytuje také podporu pro IT infrastrukturu a koncové uživatele. Nabízí také administrativní služby pro ostatní společnosti. V oblasti informačních technologií společnost programuje vlastní systém na měření a regulaci inteligentní elektroinstalace v administrativních budovách. Vlastní systém měření a regulace se používá ať již pro chytrou elektro-instalaci tak pro vytápění.

Společnost také poskytuje komplexní služby v oblasti digitalizace papírových dokumentů. Nejčastěji zpracovávané dokumenty jsou: smlouvy, formuláře, faktury, platební příkazy a běžné firemní dokumenty. Brněnské pracoviště je vybaveno skenovacími zařízeními značky KODAK. Oddělení informačních technologií se skládá pouze z vedoucího a jednoho podřízeného pracovníka. Celé oddělení má na starost přibližně 300 uživatelských pevných počítačů včetně přenosných pracovních stanic.

Struktura Společnost zaměstnává 10 pracovníků a řadí se tak mezi malé podniky. Firma dosáhla v roce 2017 obratu 14 mil. Kč. Její organizační struktura je znázorněna na obrázku 4.2. Organizační struktura společnosti je velmi jednoduchá a to konkrétně divizionální. Společnost se skládá z relativně samostatných divizí, které spolu navzájem spolupracují. Divize jsou rozděleny podle typu služby, jež poskytují. Odborné činnosti jsou rozděleny mezi jednotlivé divize, což umožňuje pružné a operativní jednání divizí. Hlavní činností je správa pohledávek, dále správa informačních technologií, digitalizace dokumentů a podpůrné ekonomické oddělení. Všechny tyto divize spadají pod jednatele.

Systémy Ve společnosti se používá převážně kancelářský balík Microsoft Office, ve kterém je spravována ekonomika a účetnictví společnosti. Soubory jsou poté ukládány na centrální síťové úložiště. Infrastruktura a její systém použití bude popsán v části 4.2 této práce.

[1] Rámec 7S řadí mezi faktory úspěchu strategii a strunkturu firmy, její spolupracovníky ve firmě a schopnosti těchto jednotlivých pracovníků, dále styl řízení společnosti, systémy a procesy ve firmě, sdílené hodnoty a podnikovou kulturu [19].



Obrázek 4.2: Organizační struktura podniku SPOLEČNOST-24 s.r.o.

Společnost plánuje do konce roku 2019 zavedení informačního systému Microsoft Dynamics AX.

Styl řízení Podnik je řízen převážně demokratickým stylem, který je spojen s vyšší mírou participace podřízených pracovníků na vedení společnosti. Jednatel dává svým podřízeným možnost vyjádřit se, deleguje značnou část svých pravomocí, avšak ponechává si svou odpovědnost v konečných rozhodnutích. Komunikace ve společnosti je v tomto ohledu dvousměrná.

Spolupracovníci Lidé jsou hlavním zdrojem zvyšování produktivity a výkonnosti firmy, proto si SPOLEČNOST-24 s.r.o. své budoucí zaměstnance před přijetím vybírá ve výběrových řízeních. Je kladen vysoký důraz na proškolování zaměstnanců společnosti.

Sdílené hodnoty Firemní kultura je silně spjata se sdílenými hodnotami. Společnost dbá na vysokou kvalitu provedené práce. V analyzované společnosti panuje velmi přátelský a uvolněný způsob komunikace. Tento uvolněný způsob komunikace odlehčuje někdy vypjatou atmosféru při řešení problémů.

Schopnosti Pro společnost jsou dovednosti jejich zaměstnanců velmi důležité, společnost dbá na zdatnost pracovníků při efektivní práci s informačními technologiemi. Schopnost pracovníků dobře pracovat s počítačem a informačními technologiemi umožňuje rychlejší, kvalitnější a jednodušší dosahování cílů.

4.2 Analýza současného stavu řešené oblasti

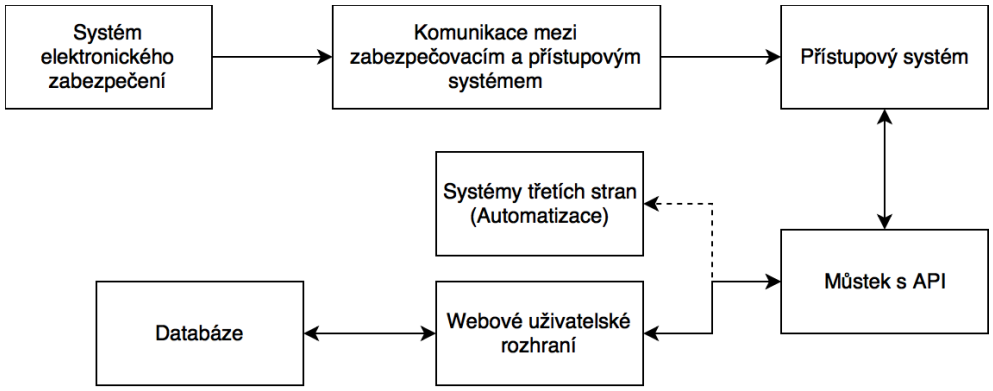
4.2.1 Budova

Analyzovaná společnost provádí svou činnost jak ve svém sídle tak i provozovně, obě lokality jsou poblíž centru Brna. Ve svém sídle má společnost kancelářské prostory v rámci jednoho

patra. Sídlo je umístěno ve čtvrtém nadzemním podlaží, kde si společnost pronajímá kancelářské prostory. Tyto prostory jsou zabezpečeny mechanickým klíčem. V prostorách sídla vykonává společnost podpůrnou administrativní činnost.

Hlavní provozovna, ve které společnost vykonává svou činnost se skládá z více pater a to konkrétně z původních v přízemí umístěných kancelářský prostor, jež jsou nyní využívány jako sklad, případně archiv, dále společnost působí v 6. a 7. nadzemním podlaží stejné administrativní budovy. V horních prostorách se nachází hlavní administrativní část. Společnost nemá budovu ani patra sama pro sebe, ale sdílí ji s ostatními firmami. Budova provozovny, ve které má společnost pronajata kancelářské prostory prochází aktuálně kompletní rekonstrukcí, jež bude ještě přibližně dva roky trvat a pravidelně při ní dochází k výpadkům elektrické energie.

Přístup do administrativních prostor společnosti je z vedlejší cesty. V přízemí je vrátnice s obsluhou, která hlídá vstup nepovolaných osob do budovy, ohlašuje a směruje návštěvníky. Pro přístup do administrativních prostor společnosti je možné využít schodiště nebo výtah. Výtah je zabezpečen čipovou kartou. Po přiložení čipové karty umožní výtah jízdu až do 5. nadzemního poschodí, jež je posledním patrem kam se dá výtahem dopravit. Z pátého nadzemního podlaží je nutné vyjít ještě jedno patro po schodech. Prostor mezi administrativní částí analyzované společnosti a chodbou je dělen bezpečnostními skleněnými dveřmi. Na tyto dveře je třeba přes dveřní hlásek zazvonit a následně jsou dveře otevřeny paní recepční. Zaměstnanci nemusejí na recepci zvonit a použijí přístupový systém autorizací čipem na čtečku, která následně sepne zámek a otevře dveře. Vedle vstupních dveří je umístěn terminál docházkového systému. Recepce společně se zasedačkami je v šestém nadzemním podlaží oddělena od kancelářských prostor skleněnými posuvnými dveřmi a chodbou. Pro otevření posuvných dveří se musí zaměstnanec ověřit na čtečce čipem. Z administrativní chodby v šestém nadzemním je možné se dostat do všech kanceláří, kuchyňky, serverovny A i přes schodiště do kanceláří v sedmém nadzemním podlaží. Všechny kanceláře mají vedle svých dveří čtečku a je možné se do nich dostat pouze s oprávněnou kartou nebo čipem.



Obrázek 4.3: Blokové schéma celého řešení zabezpečovacího a přístupového systému administrativních prostor včetně jeho obsluhy z webového rozhraní [8]

Pro docházkový a přístupový systém využívá společnost systém řady Jablotron 100[2]. Prostory společnosti jsou rozděleny zabezpečovacím a přístupovým systémem na sekce: re-

[2] Jablotron 100 je platforma pro realizaci elektronického zabezpečení objektů. Skládá se z ústředny a periferií, které rozšiřují funkcionalitu celého systému (například pohybová čidla, detektory kouře, magnetické detektory...).

cepce, kanceláře a technologie. Docházkový a přístupový systém společnosti je blíže popsán v mé bakalářské práci, jež byla realizována taktéž pro analyzovanou společnost vizte [8].

Administrativní prostory jsou vybaveny zabezpečovacím a kamerovým systém. Na obrázku 4.3 je znázorněno blokové schéma zabezpečovacího a přístupového systému administrativních prostor včetně jeho obsluhy z webového rozhraní. Společnost ve svých kancelářských prostorách používá pro systém měření a regulace vlastní systém.

4.2.2 Serverovny

Společnost má k dispozici dvě serverovny (A a B) i pronajatý prostor v datacentru. Pro vstup jak do serverovny B tak serverovny A, jež je jedinou místností v administrativní části bez přístupového systému, je nutný mechanický klíč. Klíče od obou serveroven jsou uloženy na recepci ve skříni s klíči. Předání klíčů je evidováno a vede se záznam kdo v kolik hodin a za jakým účele klíč použil.

Datacentrum Analyzovaná společnost využívá hostingových služeb od firmy Faster CZ, spol. s r.o., kde má pronajat prostor 2U pro vlastní server SuperMicro. Pracovníci interního IT oddělení mají non-stop přístup k fyzickému serveru pro případnou výměnu komponent. Zabezpečení a prostředí datacentra je v kompetenci samotné společnosti Faster. Datacentrum rovněž nabízí nezávislé okruhy napájení, redundantní chlazení, bezpečnost, úklid, monitoring a v případě potřeby možnost kontaktovat pracovníka datacentra pro lokální vizuální kontrolu serveru. Hostingové služby podporují chod vlastní infrastruktury a je díky tomu stabilnější. Parametry sjednané hostingové služby jsou:

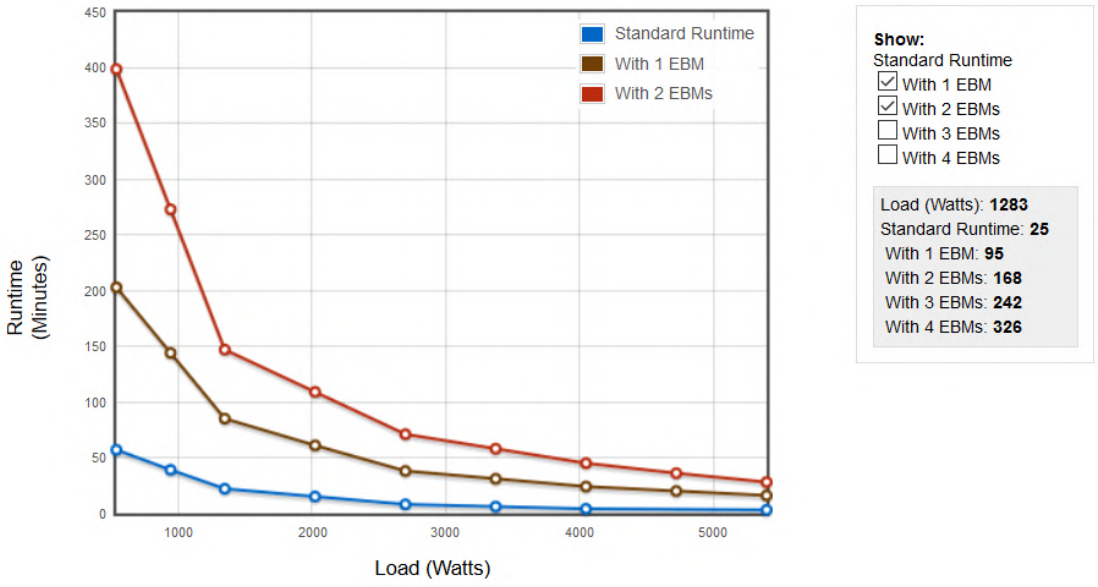
- Symetrické připojení do sítě Internet rychlostí 1 Gb/s.
- Datové omezení přenesených dat do NIX 100 TB / měsíc.
- Datové omezení přenesených dat pro Tranzit 2 TB / měsíc.
- Datově neomezené symetrické spojení mezi serverovnou A a datecentrem rychlostí 1 Gb/s bez limitu přenesených dat.
- Dva nezávislé napájecí okruhy.
- Blok čtyř veřejných IPv4 adres.

Serverovna A Prostory serverovny jež je hlavní serverovnou jsou od zbytku administrativní části odděleny dveřmi. Do serverovny A se dá dostat ze dvou stran. Z přední strany skleněnými dveřmi a ze zadní strany dveřmi dřevěnými. Oba vchody jsou osazeny klikou a běžným mechanickým zámkem na klíč. Vstup do serverovny A podniku není nijak regulován a dveře jsou osazeny běžnou klikou a vstoupit může do serverovny každý, kdo si požádá na recepci o klíč od serverovny. Prostory serverovny jsou střeženy elektronickým zabezpečovacím systémem a kamerovým systémem. Serverovna A nemá žádné okna, které by umožňovali pasivní chlazení. Prostory serverovny jsou chlazeny dvěma aktivními redundantními klimatizačními systémy. Prostor serverovny je rozdělen na teplou a studenou uličku. Celý prostor serverovny A je klimatizován na 16°C. Serverovna nedisponuje žádným systémem monitoringu teploty.

V serverovně A jsou umístěny tři datové rozvaděče Triton o velikosti 42U a čtvrtý menší rozvaděč Triton o velikosti 9U. Rozvaděče jsou z přední strany uzamykatelné a mají bočnice.

Průchod do zadní části serverovny je oddělen uzamykatelnými dvířky z 42U rozvaděče Triton. Ze zadní části jsou rozvaděče přístupné plně a nejsou osazeny dvířky. Menší rozvaděč Triton 9U je uzamykatelný a ve správě poskytovatele připojení k Internetu Faster.

Napájení serverovny A je řešeno z elektrického okruhu objektu budovy bez dalšího zálohování například motor generátorem. Hlavní jistič pro celou společnost má charakteristiku 40D. Přívodní jistič do serverovny má charakteristiku nižší a to 32D. Z tohoto jističe vychází napájecí 230V větev pro zařízení označena jako okruhu 1. Na tuto větev je připojen jednofázový záložní zdroj UPS EATON 9SX 6000. Tento záložní stroj je vybaven dvěma bateriovými moduly EATON 9SX EBM. Záložní zdroj má dvojitou on-line konverzi se systémem PFC (korekce účiníku), zvládne zátěž až 6000 VA nebo 5400 W. UPS disponuje pokročilými technologiemi pro nabíjení s teplotní kompenzací, automatickým testováním baterie, ochranou proti hlubokému vybití a automatickou detekcí externích modulů baterie. UPS lze ovládat přes vícejazyčný LCD displej, USB port, port sériové linky RS232 (port USB a RS232 nemohou být použity současně), 4 bezpotenciálové kontakty (DB9), 1 miniaturní svorkovnici se svorkami pro dálkový start a odstavení nebo svorkovnicí pro dálkové vypnutí. Při aktuální průměrné zátěži v době analýzy vydrží UPS po výpadku napájení přibližně 162 minut (2 hodiny a 42 minut), výdrž samotné UPS a bateriových modulů je možné vidět z grafu na obrázku 4.4. UPS je připojena USB kabelem pouze do jednoho serveru s kterým komunikuje [5]. Většina zařízení v serverovně A je připojena na zálohovaný okruh včetně PoE napájených IP telefonů a IP kamerového systému.



Obrázek 4.4: Graf výdrže UPS EATON 9SX 6000 a bateriových modulů 9SX EBM [5]

Serverovna B Serverovna B je umístěna v přízemních prostorách provozovny stejné budovy. Serverovna se nachází vedle vrátnice a je v prostorách archivu společnosti, konkrétně v oddělené uzamykatelné místnosti, která je sdílena se skladem IT techniky. Přízemní prostory nejsou střeženy elektronickým zabezpečovacím systémem, ale jsou střeženy kamerovým systémem a to konkrétně třemi PoE napájenými IP kamerami. Serverovna B není klimatizována. Jediný způsob chlazení serverovny B je pasivní a to otevřením okna do nádvoří, které se v místnosti nachází.

Serverovna B je vybavena jediným datovým rozvaděčem Triton o velikosti 24U. Tento datový rozvaděč má zepředu zamykatelná dvířka a ze stran je uzavřen. Zadní strana je zcela otevřená.

Rozvaděč je osazen záložním zdrojem napájení APC Smart-UPS C1000, jež je napájen z nezálohovaného okruhu. Z této UPS jsou napájeny všechny zařízení v rozvaděči včetně kamerového systému.

4.2.3 Pasivní vrstva kabeláže

Kabeláž neboli pasivní vrstva počítačové sítě je v administrativních prostorách společnosti tažena hvězdicovou topologií. Každá stanice je připojena vlastním kabelem do aktivního prvku (switche). Společnost má ve svých kancelářských prostorech v 6. a 7. podlaží rozvedenu strukturovanou kabeláž kategorie CAT 7A s frekvenčním rozsahem 1000 MHz. Kabeláž je vedena z patch panelů ze serverovny A do jednotlivých zásuvek v kancelářích. Pasivní vrstva byla projektovaná pro přenosové rychlosti 10 Gb/s včetně patch panelů a zásuvek, ale reálně se ve společnosti využívá rychlost 1 Gb/s a to díky tomu, že počítače mají pouze 1 Gb/s síťové karty a propoj od zásuvek je realizován patch kabely kategorie CAT 5E. Rozvody od patch panelů k zásuvkám využívají kabeláž, která má individuální stínění párů kabelu i celkové stínění kabelu. Kabeláž v přízemí u ze serverovny B je vedena hvězdicovou topologií strukturovanou kabeláží obdobným způsobem, avšak pouze nestíněnou kabeláží kategorie CAT 5E.

Jednotlivé prvky vlastního systému měření a regulace jsou připojeny od zařízení (kotle, klimatizace, vzduchotechnika, osvětlení...) do patch panelů v serverovně A nestíněnou kabeláží kategorie CAT 5E.

Přenosná zařízení jsou k infrastruktuře připojeny bezdrátovou technologií WiFi pracující na frekvenci 2,4 GHz nebo 5 GHz.

Serverovny B s A jsou mezi sebou propojeny opticky single modovým vláknem. Tento propoj je realizován přímo ze serverovny B do rozvaděče poskytovatele připojení k Internetu v serverovně A.

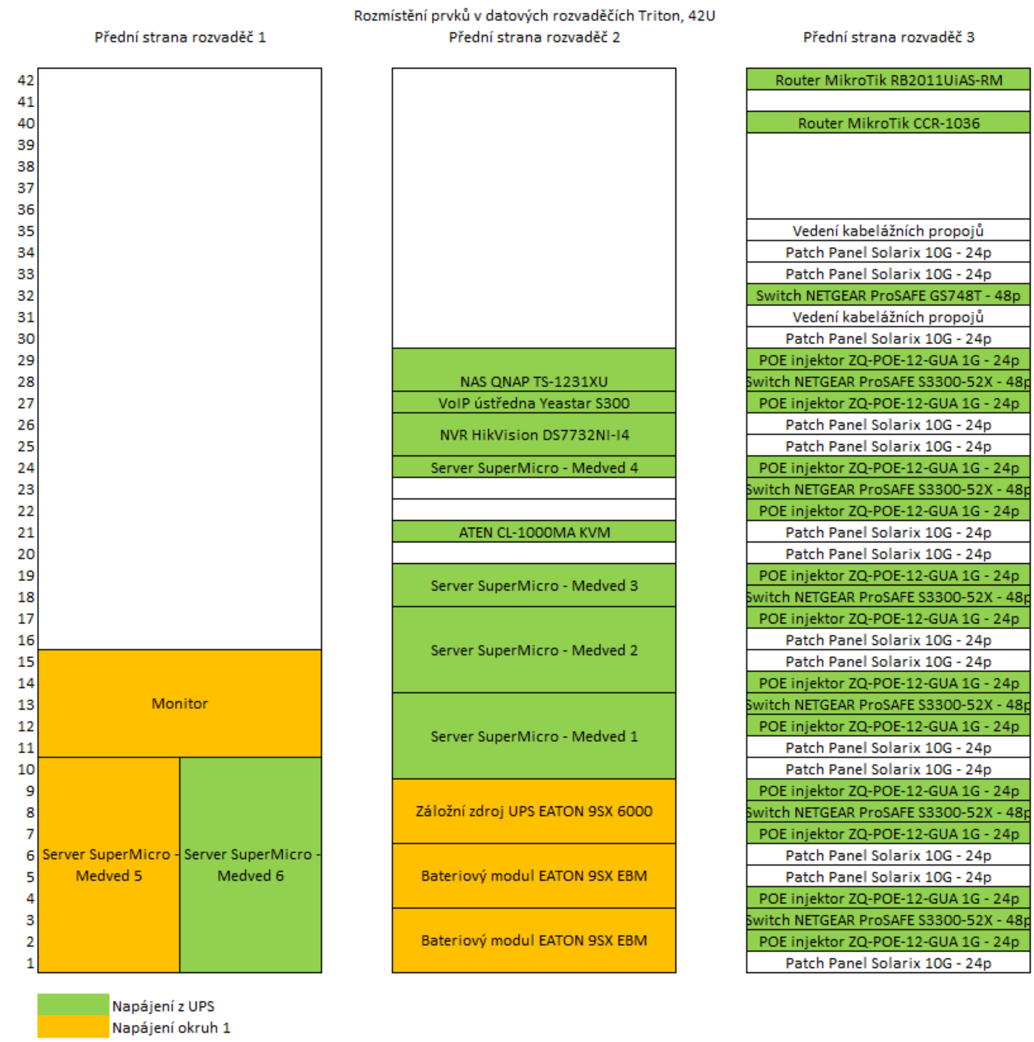
Dále je serverovna A z rozvaděče poskytovatele připojení k Internetu propojena single modovým vláknem s datacentrem společnosti Faster.

4.2.4 Fyzická topologie

V datových rozvaděčích jsou umístěny servery, bateriové UPS záložní zdroje, PoE injektory, patch panely a aktivní prvky. Na obrázku 4.5 je znázorněno rozmístění vlastních technologií v serverovně A, na obrázku 4.7 je znázorněno uspořádání technologií v rozvaděči určeného pro zařízení v majetku poskytovatele připojení k Internetu v serverovně A a na obrázku 4.8 je vyobrazeno rozmístění prvků serverovny B. Propoj mezi serverovnou A a B je realizován do switchů s propustností 1 Gb/s.

Serverovna A V rozvaděči 3 serverovny A je v horní pozici umístěn router MikroTik (`RB2011UiAS-RM`), do kterého jsou připojeny dva samostatné WiFi přístupové body MikroTik `cAP`. Pod tímto routerem je umístěn hlavní router (GATE) Mikrotik `CCR-1036`. Na dalších pozicích jsou poté dva dvacetičtyř portové patch panely. Pod těmito patch panely je umístěn samostatný čtyřicetiosmi portový switch NETGEAR `ProSAFE GS748T`. Dále je rozvaděč osazen 6x stejnou sestavou technologických prvků a to konkrétně:

- Patch panel Solarix 10G - 24 portů.

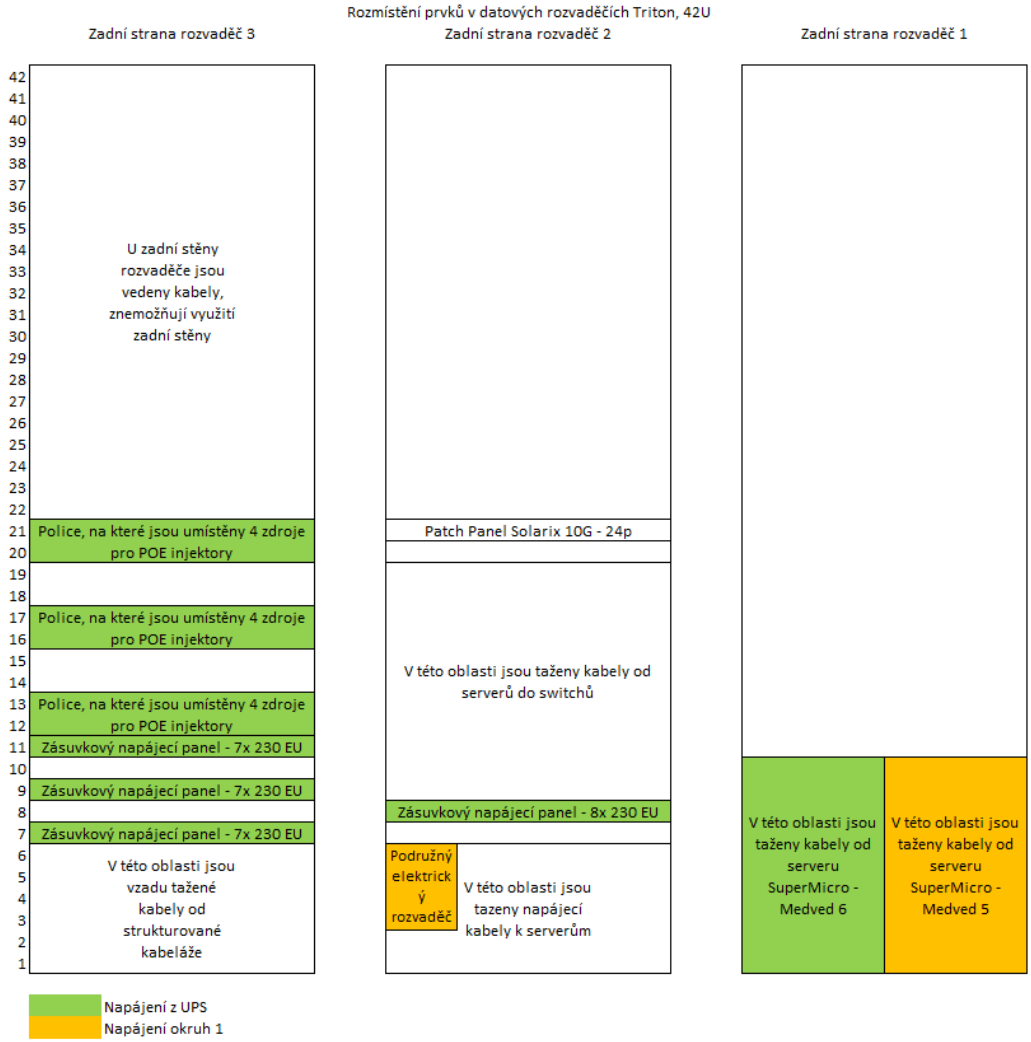


Obrázek 4.5: Rozmístění prvků v datových rozvaděčích Triton, 42U - Serverovna A - pohled zepředu

- POE injektor ZQ-POE-12-GUA 1G - 24 RJ45 portů.
- Switch NETGEAR ProSAFE S3300-52X - 48 RJ45 portů
- POE injektor ZQ-POE-12-GUA 1G - 24 RJ45 portů.
- Patch panel Solarix 10G - 24 RJ45 portů.

V rozvaděči 2 serverovny A jsou umístěny fyzické servery. Nejvýše je umístěno síťové diskové úložiště QNAP `TS-1231XU`. Pod diskovým úložištěm je umístěna VoIP telefonní ústředna Yeastar `S300`. Dále IP kamerové záznamové zařízení NVR HikVision `DS7732NI-I4`. Níže je umístěn KVM (klávesnice, video, myš) panel od značky ATEN `CL-1000MA` a čtyři servery SuperMicro. V nejnižších pozicích rozvaděče je umístěn bateriový záložní zdroj EATON `9SX 6000` a pod ním dva bateriové moduly `9SX EBM` také značky EATON.

Rozvaděč 3 serverovny A slouží pro hostování fyzických zařízení pro ostatní společnosti. V současné době jsou v rozvaděči umístěny dva klientské servery SuperMicro a jeden přehledový monitor.

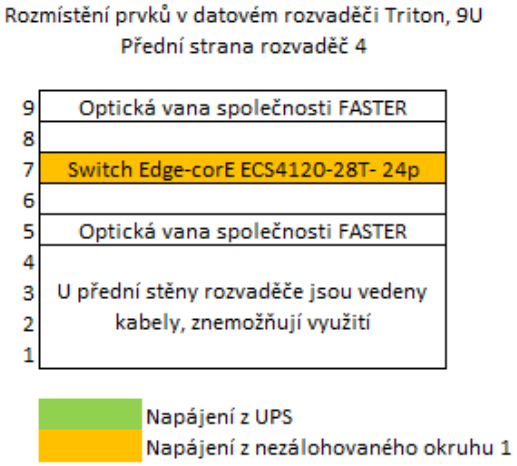


Obrázek 4.6: Rozmístění prvků v datových rozvaděčích Triton, 42U - Serverovna A - pohled zezadu

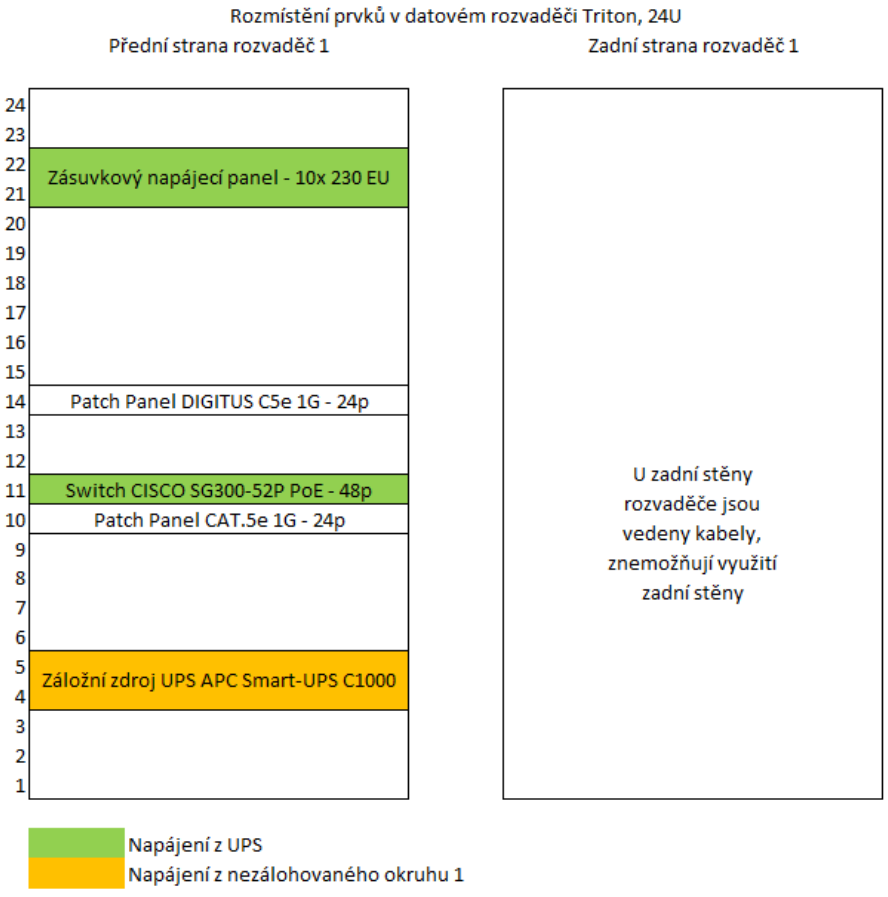
V rozvaděči 4 taktéž v serverovně A je umístěn switch a optická vana od poskytovatele připojení k Internetu. Switch je ve vlastnictví společnosti Faster CZ, spol. s r.o.

Serverovna B Rozmístění prvků v rozvaděči v serverovně B je znázorněno na obrázku 4.8. Rozvaděč je osazen záložním zdrojem APC `Smart-UPS C1000`. Nad záložním zdrojem je umístěn dvaceti čtyř portový patch panel. Patch panel je propojen se čtyřiceti osmi portový PoE switchem CISCO `SG300-52P PoE`. Nad switchem je umístěn a propojen patch panel DIGITUS kategorie s dvaceti čtyřmi porty. Nejvýše je umístěn zásuvkový napájecí panel s deseti zástrčkami pro zapojení napájecích vidlic.

Propojení zařízení Switche NETGEAR `ProSAFE S3300-52X` jsou mezi sebou propojeny 10 Gb/s linkou do kruhové topologie. Přímo do routeru GATE je připojen taktéž 1 Gb/s linkou Mikrotik 2011. Do tohoto routeru jsou 1 Gb/s linkami přes PoE injektor připojeny čtyři přístupové body MikroTik cAP. Do stohovatelného switche NETGEAR je připojen taktéž 1 Gb/s linkou nestohovatelný switch NETGEAR. Do nestohovatelného switche jsou



Obrázek 4.7: Rozmístění prvků v datových rozvaděčích Triton, 9U - Serverovna A - pohled zepředu na rozvaděč 4



Obrázek 4.8: Rozmístění prvků v datových rozvaděčích Triton, 24U - Serverovna B

přes PoE injektor připojeny IP kamery. Dále jsou do nestohovatelného switche NETAGER připojeny prvky systému měření a regulace. Do stohovatelného switche je připojen switch CISCO ze serverovny B. Do switche v serverovně B jsou připojeny a napájeny přes PoE pouze tři IP kamery. V současné době všechny klientské stanice, diskové úložiště, telefonní ústředna, kamerový server a NVR jsou připojeny do stohovatelného switche 1 Gb/s linkou. Do stejného switche jsou přes PoE napaječe připojeny i IP telefony.

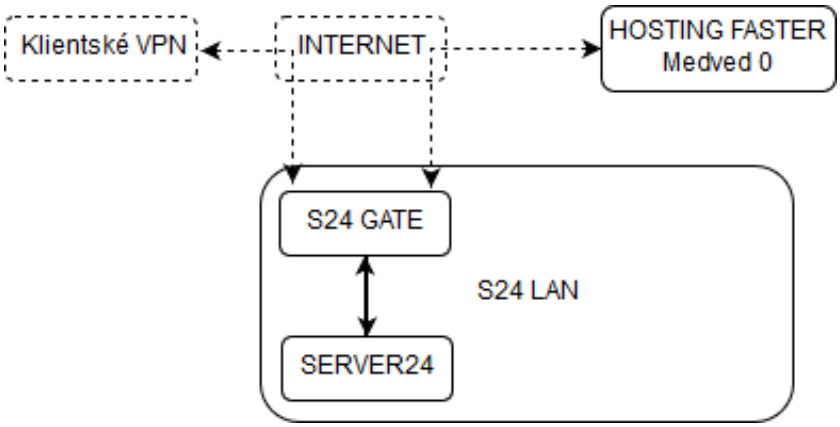
Notebooky a jiné přenosné zařízení jsou do sítě připojeny převážně prostřednictvím firemní WiFi nebo pevné (drátové) síti stejně tak jako stolní pracovní stanice.

Propojení serverů Server Medved 1 je propojen dvěma 1 Gb/s linkami se serverem Medved 2, Medved 2 je propojen dvěma 1 Gb/s linkami se serverem Medved 3 a server Medved 3 dvěma 1 Gb/s linkami se serverem Medved 1. Linka mezi servery je ralizována pomocí protokolu LACP[3]. Díky tomuto propoji vzniká kruhová topologie s teoretickou přenosovou rychlostí až 2 Gb/s pro interní komunikaci mezi servery navzájem. Všechny servery servery jsou spojeny se stohovatelným switchem NETGEAR linkou s propustností 1 Gb/s.

Komunikace UPS Fyzická topologie připojení UPS je taková, že záložní zdroj UPS komunikuje sériovou linkou USB. Tato komunikační linka je zapojena do serveru Medved 3 a komunikuje pouze s tímto serverem.

Připojení k Internetu Společnost Faster CZ, spol. s r.o. dodává do podniku optické připojení k Internetu o přenosových rychlostech 100 Mb/s pro stahování a 100 Mb/s pro nahrávání. Připojení k Internetu není časově ani datově omezeno a je poskytováno s agregací 1:1. Switch poskytovatele připojení k Internetu je propojen metalickým kabelem s hlavním routerem GATE.

4.2.5 Logická topologie



Obrázek 4.9: Schéma připojení VPN a hostovaného serveru Medved 0 do firemní sítě

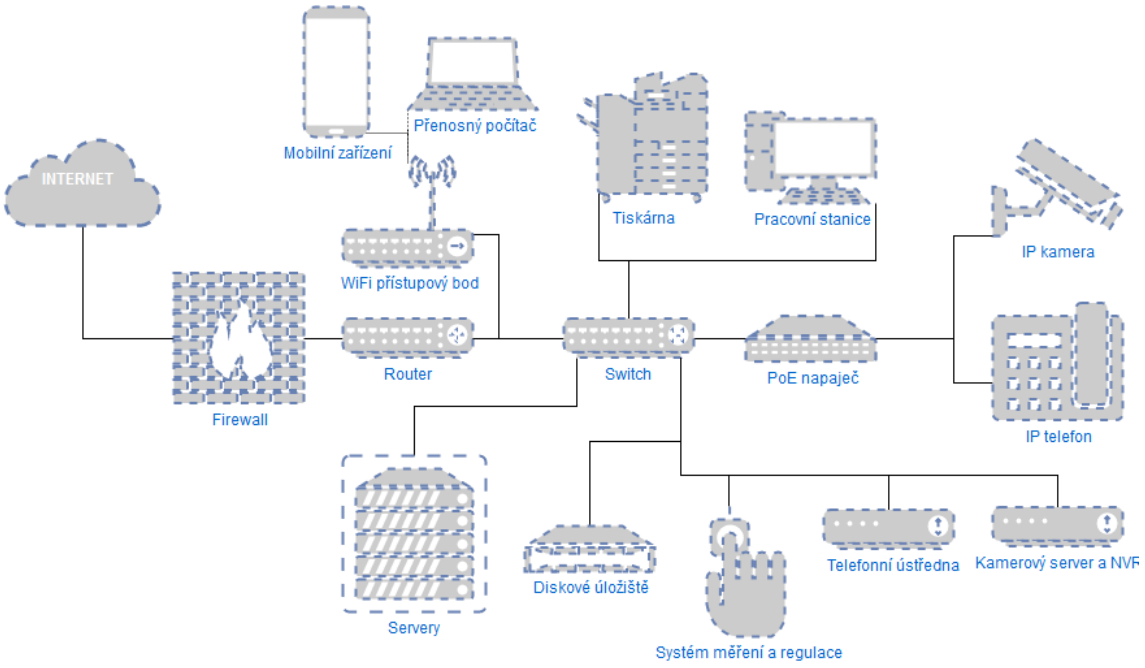
Síťová infrastruktura má logickou topologii tvořenou jednou hlavní sítí z privátního rozsahu X.X.X.0/24 (S24 LAN), ve které jsou umístěny jak pracovní stanice, tiskárny, IP

[3]Link Aggregation Control Protocol (LACP) je síťovým protokolem pro dynamické sloučení fyzických linek do jednoho komunikačního kanálu [10].

kamery, IP telefony, servery, systém měření a regulace, diskové úložiště, routery a switche. Další síť X.X.X.0/24 (S24 WLAN) je vyhrazena pro privátní WiFi, síť X.X.X.0/24 (S24 HOST) je taktéž vyhrazena pro hostovskou bezdrátovou síť a poslední síť X.X.X.0/24 (S24 VPN) je vyhrazena pro adresaci VPN tunelů. Přes VPN je připojeno sídlo společnosti. V sídle je taktéž separátní lokální síť X.X.X.0/24. Konkrétní adresní rozsahy privátních sítí analyzované společnosti nejsou záměrně v práci uvedeny a to z důvodu bezpečnosti. Na obrázku 4.9 je znázorněno logické schéma připojení VPN a hostovaného serveru Medved 0 do firemní sítě.

Od poskytovatele má společnost k dispozici souvislý blok čtyř veřejných IPv4 adres a dvě samostatné veřejné IPv4 adresy. Všechny veřejné adresy jsou nasměrovány do hlavním routeru GATE. Hlavní MikroTik zastává také funkci brány do sítě Internet, hlavního firewallu společnosti a VPN koncentrátoru pro zaměstnanecké VPN tunely. Na hlavním routeru jsou realizovány taktéž překlady portů z veřejné IP adresy na vnitřní IP adresu a port. Tyto překlady jsou pro servery Backoffice, Portal, Kerio1, Kerio2, kamerový server, telefonní ústřednu a diskové úložiště.

Logické schéma topologie sítě S24 LAN je znázorněno na obrázku 4.10. Lokální síť S24 LAN je plochá na L2 vrstvě ISO/OSI modelu.



Obrázek 4.10: Logická topologie lokální sítě S24 LAN

Sítě S24 LAN a S24 WLAN je adresována DHCP serverem SERVER24. Všechny zařízení v síti krom fyzických hardwarových serverů včetně IPMI jsou adresovány staticky. Privátní síť pro VPN tenuly S24 VPN a hostovská S24 HOST WiFi síť jsou adresovány DHCP serverem z routeru GATE. Stejně tak DNS server pro tyto sítě se nachází na routeru GATE.

Zaměstnancům společnosti je umožněno přistupovat do lokální sítě (S24 LAN) z Internetu přes SSTP (Secure Socket Tunneling Protocol) VPN tunel, schéma je znázorněno na obrázku 4.9. Tento VPN tunel je terminován v hlavním routeru GATE. Uživatelé jsou autorizováni do VPN přes přístupové údaje ověřené doménovým řadičem SERVER24.

Na provozovně společnosti jsou dvě bezdrátové sítě (2,4 GHz i 5 GHz) a obě mají veřejné SSID[4], první slouží pro připojení uživatelů do firemní sítě a druhá pro případné návštěvy společnosti, kdy je nutný přistup k Internetu. Hostovská síť je oddělena od privátní sítě. Obě sítě jsou zabezpečeny před sdíleným WPA2[5] klíčem. V sídle společnosti jsou propagovány logicky stejné WiFi sítě jako na provozovně.

Logická topologie e-mailové komunikace Společnost používá jako hlavní nástroj komunikace e-maily. MX záznam na veřejném DNS serveru je směrován na veřejnou IPv4 adresu směrovanou routerem GATE na lokální poštovní server server Kerio1. Zprávy jsou následně protokolem IMAP vybírány e-mailovým klientem a přes stejný server odesílány protokolem SMTP.

4.2.6 Aktivní prvky

Ve společnosti je síťová infrastruktura realizována pomocí aktivních prvků značek Mikrotik, CISCO a NETGEAR. Níže budou popsány pouze zařízení v majetku analyzované společnosti, nebudou popisovány aktivní prvky v rozvaděči poskytovatele připojení k Internetu. Všechny popisované aktivní prvky jsou v provedení do rozvaděče a mají velikost 1 U.

Všechny routery a switche v analyzované společnosti podporují VLAN, SNMP i IEEE 802.1ab (LLDP).

Routery Operačním systémem všech používaných routerů je MikroTik RouterOS v různých verzích.

- **MikroTik Cloud Core CCR1036-12G-4S** je 36-ti jádrový router s taktem 1,2 GHz a se 4 GB operační paměti RAM. Tento router má 12 x (RJ-45) 10 Mb / 100 Mb / 1 Gb Ethernet a 4 x SFP port (1 Gb). Celková propustnost tohoto routeru je až 16 Gb/s a dokáže zpracovat až 8 milionů paketů za sekundu.
- **MikroTik RB2011UiAS-RM** je jedno-jádrový router s taktem procesoru 600 MHz a se 128 MB operační paměti RAM. Router je osazen 5 x Gb Ethernet, 5 x 100 Mb Ethernet a 1 x Gbit SFP portem. Router má vstup pro napájení z PoE. Router disponuje taktéž 1 x PoE výstupem na 100 Mb Ethernet portu a má stejné napětí jako použitý zdroj či PoE napájení. PoE lze z tohoto zařízení použít pro napájení od 8 do 28 V s maximálním proudem 580 mA.
- **MikroTik cAP ac** je router, konkrétně přístupový bod vybavený čtyř-jádrovým procesorem s taktem 716 MHz a 128 MB operační paměti RAM. Router je osazen 2 x 10 Mb / 100 Mb / 1 Gb Ethernet portem a je možně jej napájet pomocí PoE. Tento přístupový bod pracuje na frekvenci 2,4 GHz i 5 GHz a podporuje standardy IEEE 802.11 a/b/g/n/ac.

Switche

- **NETGEAR ProSAFE S3300-52X** je stohovatelný, spravovatelný a pracuje na vrstvě L3 ISO/OSI modelu, poskytuje 48 x (RJ-45) 10 Mb / 100 Mb / 1Gb Ethernet, 2 x 10Gb Ethernet a 2 x SFP+ (10 Gb). Tento switch má výkon 176 Gb/s a lze stohovat až do počtu šesti jednotek.

[4]SSID (Service Set Identifier neboli identifikátor) bezdrátové sítě [10].
[5]WPA2 (Wi-Fi Protected Access II) je zabezpečovacím protokolem technologie bezdrátových sítí [10].

- **NETGEAR ProSAFE GS748T** je spravovatelný, pracuje na vrstvě L3 ISO/OSI modelu, poskytuje 48 x (RJ-45) 10 Mb / 100 Mb / 1 Gb Ethernet a 4 x sdílený SFP port (1 Gb). Výkon switche je až 96 Gb/s.
- **Cisco SG300-52P PoE** je spravovatelné, pracuje na vrstvě L3 ISO/OSI modelu, poskytuje 52 x (RJ-45) 10 Mb / 100 Mb / 1 Gb Ethernet a 2 x SFP port (1 Gb). Prvních 48 portů má schopnost napájet zařízení přes PoE. Tento switch nabízí celkový výkon 375 W pro napájená zařízení. Výkon switche je až 104 Gb/s.

4.2.7 Servery

Ve společnosti je v současné době v provozu celkem sedm fyzických serverů, z nichž jsou všechny značky SuperMicro a obsahují integrované rozhraní IPMI pro vzdálené ovládání. Všechny servery jsou umístěny v datových rozvaděčích vizte výše. Servery jsou staré přibližně tři roky. Servery ve společnosti jsou označovány jako `Medved 0 - Medved 6`, servery `Medved 5 a 6` jsou v majetku klientů společnosti. Na všech serverech je provozován aktuálně souborový systém ZFS[6] Na fyzických serverech podniku je nainstalován virtualizační software QEMU KVM.

Medved 0 Tento server je hostován v datacentru Faster a slouží primárně k zálohování virtuálních serverů. Hardwarové specifikace jsou následující:

- **CPU:** Intel(R) Xeon(R) CPU E3-1220 v3 @ 3.10GHz
- **RAM:** 4x DDR3 8GB 1600MHz ECC (32 GB)
- **Řadič:** LSI Logic / Symbios Logic SAS2308 PCI-Express Fusion-MPT SAS-2
- **HDD:** 12x Raid Edition 4TB, 3,5", SATA 600, 7200RPM, 64MB (48 TB)

Medved 1 Hardwarové specifikace jsou následující:

- **CPU:** 2x Intel(R) Xeon(R) CPU E5-2650L v2 @ 1.70 GHz
- **RAM:** 4x DDR3 16 GB 1866 MHz ECC (64 GB)
- **Řadič:** LSI Logic / Symbios Logic MegaRAID SAS 2108
- **SSD:** 2x 600GB, 2.5", SATA 6 Gb/s, 20 nm, MLC (1,2 TB)
- **HDD:** 5x Raid Edition 4 TB, 3,5", SATA 600, 7200 RPM, 64 MB (20 TB)
- **LAN:** 4x Intel Corporation I350 Gigabit Network Connection

Medved 2 Hardwarové specifikace jsou následující:

- **CPU:** 2x Intel(R) Xeon(R) CPU E5-2650L v2 @ 1.70 GHz
- **RAM:** 16x DDR3 4 GB 1600 MHz ECC (64 GB)
- **Řadič:** LSI Logic / Symbios Logic MegaRAID SAS 2108

[6] ZFS (Zettabyte File System) je kombinovaný souborový systém a správce logických svazků [3].

- **SSD:** 2x 600 GB, 2.5", SATA 6 Gb/s, 20nm, MLC (1,2 TB)
- **HDD:** 5x Raid Edition 4 TB, 3,5", SATA 600, 7200 RPM, 64 MB (20 TB)
- **LAN:** 4x Intel Corporation I350 Gigabit Network Connection

Medved 3 Hardwarové specifikace jsou následující:

- **CPU:** 4x Intel(R) Xeon(R) CPU E5-4627 v2 @ 3.30 GHz
- **RAM:** 32x DDR3 8 GB 1866 MHz ECC (256 GB)
- **SSD:** 2x 800 GB, 2.5", SATA 6 Gb/s, 20nm, MLC (1,6 TB)
- **HDD:** 4x Raid Edition 4 TB, 3,5", SATA 600, 7200 RPM, 64 MB (16 TB)
- **LAN:** 4x Intel Corporation I350 Gigabit Network Connection

Medved 4 Tento server byl nejstarším ze serverů společnosti a byl dodán společně s Linuxovým řešením doménového řadiče (Zentyal) a během analýzy vypověděl službu a již není dále provozu schopný.

Hostovaný server Medved 5 a Medved 6 Hardwarové specifikace obou serverů jsou shodné a to konkrétně následující:

- **CPU:** Intel(R) Xeon(R) CPU E3-1220 v3 @ 3.10 GHz
- **RAM:** 4x DDR3 8 GB 1866 MHz ECC (32 GB)
- **SSD:** 240 GB, 2.5", SATA 6 Gb/s, 20nm, MLC (240 GB)
- **HDD:** 2x 3 TB, 3,5", SATA 600, 7200 RPM, 64 MB (6 TB)

Diskové úložiště Dalším serverem v analyzované společnosti je diskové úložiště QNAP. Má dvanáct slotů na disky, z nichž osazeno je osm. V diskovém úložišti je 5x 4 TB, 3,5", SATA 600, 7200 RPM, 64 MB. čtyři z těchto disků tvoří RAID 5[7] pole a jeden disk je připraven k zapojení do pole v případě selhání jednoho z disků (hot spare). V diskovém poli jsou také 3x 120 GB SSD disky, z nichž dva jsou zapojeny v RAID 1[8] (zrcadlo), jež slouží jako vyrovnávací paměť pro pomalejší HDD disky a třetí 120 GB SSD disk je připraven jako hot spare pro tento RAID 1. Celková kapacita úložiště pro data je 12 TB.

4.2.8 Aplikační servery

Jednotlivé softwarové servery a jejich umístění je vyobrazeno na obrázku 4.11.

Server Portal (16 GB RAM, 4 CPU, 600 GB HDD) je hlavním kolaboračním serverem podniku, na němž je nainstalovaná aplikace Bitrix a je dostupný ze sítě Internet. Tento

[7] RAID 5 (Redundant Array of Independent Disks) je vícenásobné diskové pole nezávislých disků, které má kapacitu n-1 disků, kde n je počet disků. Kapacitu jednoho členu (disku) zabírají samoopravné kódy, které jsou uloženy na členech (discích) střídavě [23].

[8] RAID 1 (Redundant Array of Independent Disks) je vícenásobné diskové pole nezávislých disků, kdy se obsah současně zaznamenává na dva disky. V případě výpadku jednoho disku umožňuje RAID 1 práci s kopií, která je okamžitě dostupná [2].

Umístění	Název serveru	Role	Operační systém
Medved 1	Portal	Bitrix - Intranet	CentOS 7
Medved 1	Kerio1	E-mailový server	Debian 9.4
Medved 1	Synopsis	Pohledávkový systém	Ubuntu 12.04 LTS
Medved 1	Synopsis02	Pohledávkový systém	Ubuntu 12.04 LTS
Medved 2	Backdomain	Záložní - Zentyal AD na linuxu	Ubuntu 14.04 LTS
Medved 2	Epodatelna	Archiv datových zpráv	Windows 10 Pro
Medved 3	Terminal24	RDS server	Windows Server 2016
Medved 3	Terminal	Spisová služba - produkce	Windows Server 2012
Medved 3	Server24	AD, DNS, DHCP, Profily	Windows Server 2016
Medved 3	Optimidoc	Tiskový server	Windows Server 2012
Medved 3	Backoffice	Zentyal AD na linuxu	Ubuntu 14.04 LTS
Medved 3	ESS	Spisová služba - testovací	Windows Server 2012
Medved 5	Synopsis01	Klientský pohledávkový systém	Ubuntu 12.04 LTS
Medved 6	Kerio2	Klientský e-mailový server	Debian 9.4

Obrázek 4.11: Servery podniku

server slouží k interní komunikaci a výměně souborů a vizuálnímu prohlížení dat docházky. Dalším serverem je Kerio1 (5 GB RAM, 2 CPU, 500 GB HDD), jež slouží jako hlavní interní e-mailový server společnosti a je dostupný ze sítě Internet. Server Synopsis (8 GB RAM, 2 CPU, 300 GB HDD) je aplikačním serverem, jež hostuje stejnojmenný informační systém na správu pohledávek SynopsIS. Server Synopsis02 (4 GB RAM, 2 CPU, 300 GB HDD) je pouze testovací verzí výše zmíněného aplikačního serveru.

Server Backdomain (4GB RAM, 1 CPU, 200 GB HDD) je Linuxovým adresářovým serverem a slouží jako záložní linuxový doménový kontroler AD (aplikační software Zentyal). Epodatelna (4 GB RAM, 2 CPU, 500 GB HDD) je aplikačním serverem pro stahování a archivaci datových zpráv.

Terminálový server Terminal24 (128 GB RAM, 24 CPU, 800 GB HDD) slouží jako centralizované uživatelské prostředí pro zaměstnance, jež se připojují skrz přenosné počítače prostřednictvím VPN. Na aplikačním serveru Terminal (16 GB, 4 CPU, 3 TB HDD) běží software FormFlow od společnosti Software602, jež aktuálně slouží jako spisová služba společnosti a je na ní postaven koloběh dokumentů. Dalším serverem je Server24 (4 GB RAM, 2 CPU, 2 TB HDD), který obstarává více funkcí, je hlavním doménovým kontrolerem služeb AD DS, DNS serverem, DHCP serverem a úložištěm pro uživatelské profily a data. Na tiskovém serveru OptimiDoc (12 GB RAM, 4 CPU, 150 GB) běží stejnojmenná aplikace, která se stará o tiskárny Xerox ve společnosti. Umožňuje uživatelům po autorizaci na tiskárně čipovou kartou vytisknout nebo naskenovat požadovaný dokument. Server Backoffice (4 GB, 1 CPU, 1 TB HDD) slouží jako adresářový server a proxy server společnosti (stejné aplikační vybavení jako server Backdomain). Veškerý příchozí datový provoz ze sítě internet je distribuován na cílové servery přes proxy server na tomto aplikačním serveru. Aplikační server ESS (4 GB RAM, 1 CPU, 300 GB) hostuje testovací instanci spisové služby FormFlow od společnosti Software602.

Server Synopsis01 (16 GB RAM, 4 CPU, 500 GB HDD) je aplikačním serverem na správu pohledávek hostovaný pro klienta. E-mailový server Kerio2 (16 GB, 4 CPU, 1 TB HDD) je taktéž hostován pro klienta a je dostupný ze sítě Internet.

4.2.9 Pracovní stanice

Všechny pracovní stanice ve společnosti běží s operačním systémem Microsoft Windows 10 Pro. Ve společnosti nejsou počítače unifikované. Pracovní stanice uživatelů jsou různého stáří a různé výkonnosti. Každá pracovní stanice má nainstalovaný lokálně spravovaný a licencovaný antivirový program ESET AntiVirus. Na pracovních stanicích je hlavním pracovním nástrojem balík Microsoft Office 2007. Ke své e-mailové schránce přistupují uživatelé jen přes webové rozhraní. Ostatní systémy nutné k práci jsou k dispozici přes webové rozhraní. Všechny počítače splňují alespoň minimální hardwarové požadavky pro běh 64 bitové verze operačního systému. Procesor musí mít takt alespoň 1 GHz s architekturou 64 bit (x64) splňovat alespoň, operační paměť minimálně 2 GB, pevný disk s dostupnou kapacitou 20 GB a grafickou kartu s podporou technologie DirectX 9 [7].

Ve společnosti převládá počet stolních počítačů nad přenosnými notebooky, kdy notebook mají zhruba čtyři zaměstnanci, kteří jej využívají při práci z domu či na poradách. U každé pracovní stanice se nachází IP telefon. Každému zaměstnanci je při nástupu do zaměstnání založen účet v Active Directory, předán zabezpečovací, přístupový a docházkový čip.

Tisk probíhá ve společnosti přes tiskový server OptimiDoc. Tento tiskový server spravuje a komunikuje s firemními tiskárnami Xerox. Ve společnosti jsou celkem čtyři barevné laserové tiskárny Xerox, dvě formátu A4 a dvě formátu A3. Uživatel, který zadá dokument k tisku může přijít k jakékoliv tiskárně, na ní se přihlásit a vytisknout požadovaný dokument. Po přihlášení na tiskárnu je možné také skenovat a to buď do osobní složky nebo do e-mailové schránky prostřednictvím SMTP serveru.

4.2.10 Monitoring a management

Monitoring síťové infrastruktury Společnost v současné době žádným způsobem nemonitoruje stav své síťové infrastruktury. Monitorováno není ani prostředí serverovny A (například teplota). Aktuálně ve společnosti nejsou definované pravomoci, zodpovědnost, směrnice, procesy, postupy ani pravidla jak se o infrastrukturu podniku starat a přistupovat k ní.

Management infrastruktury O ICT analyzované společnosti se stará interní oddělení IT a externí společnost. Správa o interní hardwarové servery společnosti je outsourcována externí společnosti, externí firma má dále na starost správu celého virtualizačního řešení včetně virtuálních stanic a zálohování i správy síťových prvků. O správu virtuálních serverů se operačním systémem Microsoft Windows se stará interní IT oddělení, které má dva členy. Jedním z těchto členů jsem i já, pracuji na pozici vedoucího IT oddělení a mám pod sebou kolegu, jež vypomáhá se správou infrastruktury. Interní oddělení IT se stará o požadavky uživatelů, správu uživatelských zařízení a konfiguraci Active Directory Domain Services. Dále se interní IT stará o kompletní ICT infrastrukturu klientů analyzované společnosti.

Zálohy dat Pracovní stanice ve společnosti nemají nastavený pravidelný cyklus záloh dat. Uživatelé pracovních stanic přistupují na data ze sdílených složek umístěných na diskovém úložišti QNAP.

Zálohování diskového úložiště je realizováno jak lokálně tak i do serveru Medved 0 v datacentru. Zálohování na server Medved 0 probíhá každý den v nočních hodinách. Lokální zálohování v rámci zařízení QNAP uchovává vždy zálohu hodinu starého stavu dat, verzi dat za každý den posledních sedm dnů, osm posledních týdenních verzí a deset posledních měsíčních verzí. Tyto zálohy jsou automaticky přepisovány zálohami novými.

Virtuální servery z fyzického serveru Medved 3 a Medved 1 jsou zálohovány na server Medved 2. Virtuální servery z Medved 2 jsou zálohovány na Medved 1. Každý den v noci jsou zálohy virtuálních serverů přenášeny na server Medved 0 v datacentru FASTER.

4.3 Požadavky investora

Návrh systému byl proveden s ohledem na následující klíčové požadavky vedení společnosti SPOLEČNOST-24 s.r.o., jejichž podrobnější popis je součástí této kapitoly.

Klíčové požadavky vedení:

- Provést inventarizaci (dokumentaci) a analýzu používaných technologií v serverovně.
- Posoudit vhodnost použitých technologií.
- Optimalizovat infrastrukturu tak, aby byla její správa efektivní pro interní pracovníky IT.
- Vstup do serverovny společnosti bez mechanických klíčů.
- Navrhnout řešení jak monitorovat teplotu serverovny - odeslání upozornění na nepříznivý stav.
- Jednoduchá uživatelská obsluha dohledového panelu nad sítí a technologií.
- Odolnost infrastruktury vůči výpadku napájení.
- Zajištění bezproblémového náběhu celého systému.
- Možnost rozšíření infrastruktury a realizace za přiměřenou cenu.

Jedním ze základních požadavků je optimalizovat serverovou infrastrukturu společnosti, tak aby její obsluha byla pro interní pracovníky IT oddělení efektivní. Ideální by pro podnik bylo, kdyby byla sestavena dokumentace. Dokumentace serverovny prozatím nikdy nebyla vytvořena.

Aktivně používané fyzické servery by měly být omezeny jen na nezbytně nutnou část. Bylo by vhodné zvážit i případnou změnu virtualizační technologie a to za takovou, která by byla pro interní pracovníky relativně snadno spravovatelná a nebyli tak odkázáni na závislost na externích dodavatelích IT podpory.

Dalším požadavkem je, aby se mohli zaměstnanci vstupovat do serverovny podniku bez nutnosti mít u sebe mechanické klíče, jen za pomocí RFID klíčenky a nebo případně karty, stejně tak jako je to v ostatních prostorách společnosti. Cílem je tedy využít elektromagnetický zámek dveří namísto konvenčních mechanických zámků na klíč.

Požadavkem na optimalizaci serverovny je také pravidelné monitorování teploty serverovny, aby nedocházelo k výkyvům teplot a zbytečnému snížení životnosti umístěné technologie.

Je nutné také vyřešit problém se startováním serverů po výpadku elektrické energie a vybití bateriové zálohy. Pokud dojde k takovému výpadku, tak serverovna nenastartuje.

Dalším důležitým požadavkem je přiměřená cena. Nesmíme opomenout ani bezpečnost celého systému. Celý systém by měl používat zabezpečenou šifrovanou komunikaci, všude tam, kde je to jen možné.

4.4 Zhodnocení analýzy

Ve společnosti jsem na základě analýzy zjistil, že je serverovna A špatně fyzicky zabezpečená a může se k infrastruktuře uvnitř dostat i jakákoliv nepovolaná osoba, která má přístup do administrativních prostor společnosti.

Jako další zjištěný problém je, že často nastává situace kdy nefunguje správně klimatizace a je potřeba objednat servis. O této nepříznivé situaci se však IT oddělení doví až když vnímavý zaměstnanec jdoucí kolem serverovny slyší vyšší hluk než obvykle a dá vědět některému z pracovníků interního IT oddělení.

Budova, ve které má společnost pronajata kancelářské prostory prochází aktuálně kompletní rekonstrukcí, jež bude ještě přibližně dva roky trvat a pravidelně při ní dochází k výpadkům elektrické energie. Za rok 2018 byla serverovna zasažena třiceti osmi různě dlouhými výpadky napájení serverovny. Některé z těchto výpadků (za rok 2018 konkrétně jedenáct) elektrické energie jsou dostatečně dlouhé na to, že vybijí záložní zdroj UPS i bateriové moduly a při opětovném zprovoznění přívodu elektrické energie zapříčiní velký špičkový odběr a ten způsobí, že jistič před UPS tento nápor nevydrží a vypne. Největší měrou dle mého názoru do špičkového odběru proudu vstupují spínané síťové zdroje Mean Well AD-155C s krytem o výkonu 151,55 W 54/53,5 V. Tyto spínané zdroje napájí přes PoE telefony a kamery. Tento výpadek jističe má za následek celkovou nefunkčnost celé infrastruktury, a to až do doby než se o výpadků správci IT od zaměstnanců o problému dozvědí. Obvyklý nepopsaný interní proces zprovoznění serverovny je následující: poté co se fyzicky dostaví pracovnici oddělení IT do prostor serverovny A nevidí žádnou světelnou indikaci provozu. Pracovník vyhledá patřičný jistič a pokusí se serverovnu znovu zprovoznit. Tato snaha je však bez úspěchu, protože špičkový proud odběru UPS je vyšší než je schopen jistič udržet a proto opět padá. Dále pracovníci musejí ručně odpojit všechny zařízení od UPS a zapnout pouze samotnou UPS a jistič. Poté co UPS běží bez problémů mohou teprve pracovníci IT postupně připojovat technologii k napájení z UPS. Postupné zapojování a zprovoznění serverovny po výpadku ve společnosti trvá až 3 hodiny. Společnost nemá nastaveny postupy pro řešení těchto havarijních situací. Při analýze bylo taktéž zjištěno, že rozvaděč 4 se zařízením poskytovatele připojení k Internetu není připojen na zálohovaný okruh. U záložního zdroje UPS byl zjištěn ještě jeden problém a to je ten, že UPS komunikuje pouze se serverem Medved 3, ostatní zařízení se o stavu záložního zdroje nedozví a při výpadku se nekontrolovaně vypínají, což může vést k nezvratnému poškození hardware nebo dat.

Dalším zásadním problémem je monitoring síťových rozsahů a správa jednotlivých koncových bodů. Společnost taktéž nedisponuje žádnou dokumentací sítě či infrastruktury. Interní oddělení IT nemá úplné oprávnění do všech síťových prvků společnost a je pro ni správa vlastní infrastruktury složitá. Systém měření a regulace potřebuje pro svou činnost

vlastní rozsah kdy budou jednotlivé komponenty tohoto systému mezi sebou komunikovat na druhé vrstvě ISO/OSI modelu.

Správci informační technologie společnosti nemají úplnou kontrolu nad všemi servery podniku. Servery Medved 0 - Medved 6 jsou spravovatelné pouze prostřednictvím operačního systému Linux a není aktuálně žádná jiná alternativa například webové rozhraní či klient pro Windows.

Tiskové řešení přes tiskový server OptimiDoc taktéž není pro podnik ideální a to z toho důvodu, že uživatelé na první pohled nevidí v jakém stavu je tiskárna a nedozví se tak, že například v tiskárně došel toner, papír nebo jiný spotřební materiál. Nevýhodou tohoto řešení v tomto konkrétním případě je taktéž rychlost, kdy se na zařazení dokumentu do tiskové fronty čeká až minutu a po příchodu k tiskárně, přihlášení a odeslání úlohy k vytištění nastává až dvou minutová prodleva.

Kapitola 5

Vlastní návrhy řešení

Tato kapitola je nosnou částí diplomové práce, budou zde navržena nejen technická řešení problémů odhalených při analýze infrastruktury společnosti.

5.1 Přístupový systém a měření teploty serverovny

5.1.1 Návrh funkčnosti a specifikace požadavků

Návrh funkčnosti přístupového systému serverovny A Navrhuji, aby do serverovny A měly přidělen přístup pouze zaměstnanci oddělení IT, jednatel a případně poskytovatel připojení k Internetu. Všechny přístupy ať již platné či neplatné (pokusy o přístup) by měly být ukládány do historie ústředny stejně tak jako tomu je i u ostatních místností provozovny.

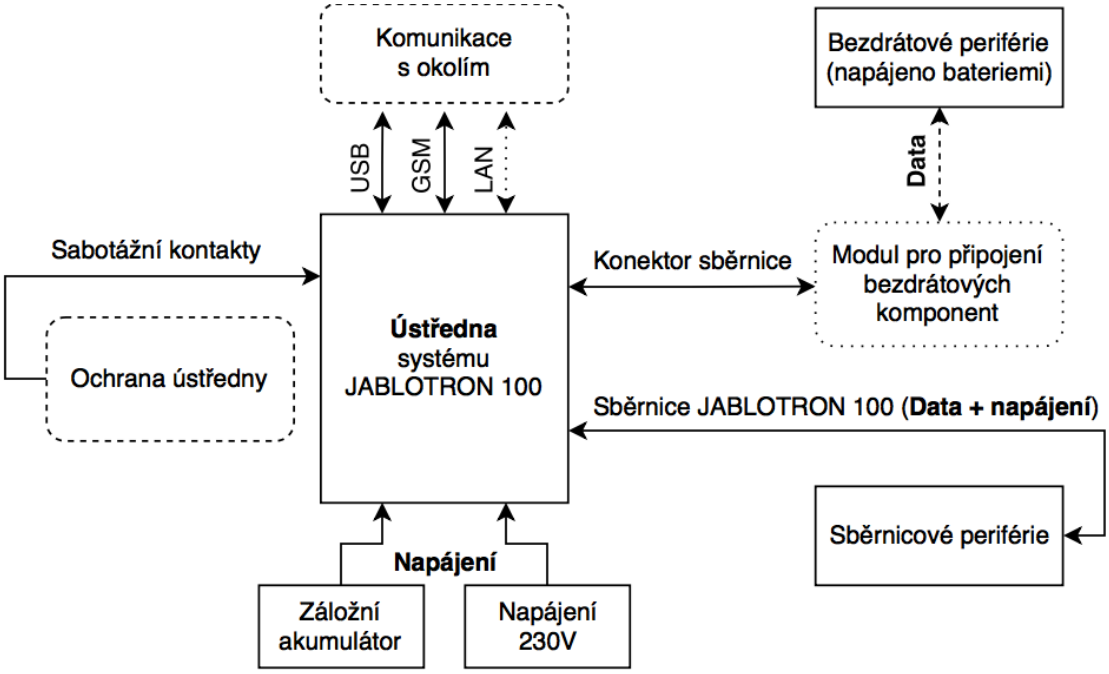
Návrh funkčnosti pro systému monitoringu prostředí serverovny A Na základě toho, že je celý prostor serverovny A klimatizován na 16°C navrhuji, aby byl systém monitoringu teploty serverovny nakonfigurován tak, že bude při překročení hranice 25°C odesílat SMS zprávu zaměstnancům oddělení IT a automaticky založí požadavek k řešení problému. IT oddělení bude mít také přes webové rozhraní přístup k jak aktuální teplotě serverovny tak i historickým hodnotám.

5.1.2 Realizace

Jako přístupový systém do serverovny A podniku bude použit Jablotron 100, jež je platforma pro realizaci elektronického zabezpečení objektů, která je použita i pro ostatní místnosti. Skládá se z ústředny a periferií, které rozšiřují funkcionalitu celého systému (například pohybová čidla, detektory kouře, magnetické detektory...). Monitoring teploty bude realizován přidáním bezdrátového teploměru do systému Jablotron 100.

Na obrázku 5.1 je znázorněna architektura systému Jablotron 100, do kterého budou přidány sběrnicové periférie. Jedná se o sběrnicový systém, který je možné relativně jednoduše rozšiřovat o další prvky. Mezi periferie systému patří detektory, komponenty pro ovládání a výstupní prvky. Pro tento systém jsem v minulosti navrhl přístupový a docházkový systém vizte [8].

Zařízení z produktové řady Jablotron 100 od společnosti JABLOTRON ALARMS a. s. jsou evolucí řady Jablotron 80. Společnost JABLOTRON ALARMS a. s. působí na českém trhu již od roku 1990. Za tuto dobu se stali významným poskytovatelem alarmů v České



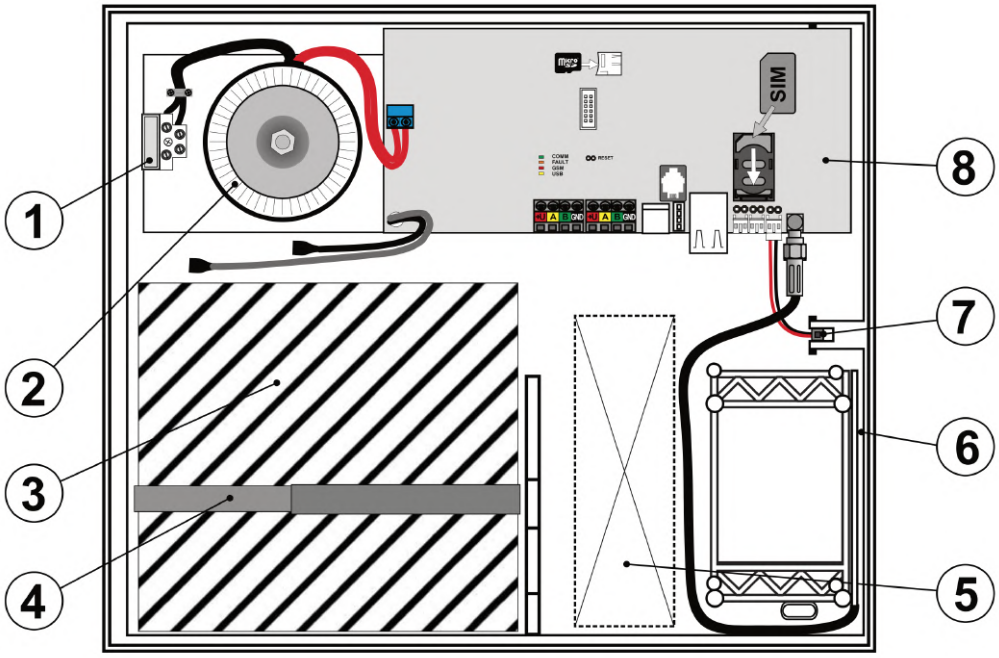
Obrázek 5.1: Architektura systému Jablotron 100 [8]

Republice. Produkty značky Jablotron jsem pro realizaci elektronického zabezpečovacího systému zvolil na základě vysoké spolehlivosti produktů o čemž svědčí jejich sedmiletá záruka na všechny produkty v nabídce, jejich progresivní technologický postup a v neposlední řadě velmi vkusné grafické zpracování. EZS Jablotron 100 se skládá z ústředny (hlavní řídicí jednotky) a dílčích periferií. Hlavní výhodou elektronického zabezpečovacího systému Jablotron 100 je to, že celý systém je hybridní. To znamená, že je možné kombinovat jak drátové (sběrnicové) tak i bezdrátové komponenty. Vlastnosti jednotlivých drátových a bezdrátových prvků jsou stejné. Díky této vlastnosti se dají jednotlivé komponenty plnohodnotně nahradit za drátovou nebo bezdrátovou verzi [8].

Ústředna Ústředna je základním stavebním kamenem celé realizace přístupového systému na platformě Jablotron 100. Je také mozkem celého systému a potřebuje dostatek informací z periferií, aby mohla rozhodnout, kdy a jakou událost provede. Celá ústředna by měla být připojena do síťového napájení přes nezávislý jistič elektrického rozvodu v objektu.

Ústředna *JA-106KR-LAN* Periférie budou přidány do již použité ústředny *JA-106KR-LAN*, vizte obrázek 5.2, jež je plnou verzí ústředny zabezpečovacího systému Jablotron 100. Tento typ ústředny je také největší z nabízených ústředen a umožňuje tak možnost připojení nejvíce periferií. Tato ústředna ve variantě s písmenem R je doplněna o rádiový modul (vizte kapitola 5.1.2) pro připojení bezdrátových periferií.

Periférie Zde budou navrženy všechny potřebné periférie pro rozšíření přístupového systému Jablotron 100. Všechny komponenty použité k rozšíření systému jsou adresované v ústředně a zabírají tak pozici v systému.



Obrázek 5.2: Ústředna zabezpečovacího systému JA-106KR-LAN [9]

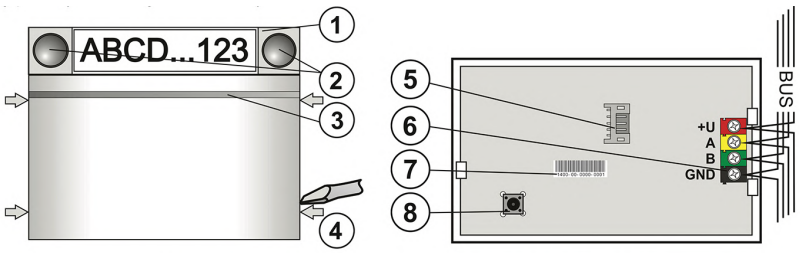
Sběrnicový modul pro bezdrátové připojení - *JA-110R* Tento sběrnicový modul k bezdrátovému připojení periferií do systému Jablotron 100 je již připojen přímo do základní desky ústředny (konektorem RJ11). Modul umožňuje obousměrnou rádiovou komunikaci s bezdrátovými periferiemi řady Jablotron 100 na frekvenci 868,1 MHz. Při bezdrátovém přenosu dat je využíván vlastní šifrovaný protokol Jablotron [9].

Obrázek 5.3: Bezdrátový detektor teploty - *JA-151TH [9]*

Bezdrátový detektor teploty - *JA-151TH* Na základě změřené teploty umožňuje tento bezdrátový detektor teploty (obrázek 5.3) ovládat topení pomocí programovatelného

výstupu ústředny. Všechny funkce se nastavují v MyJABLOTRON[1], uživatel může kdykoliv a odkudkoliv vše sledovat a ovládat. Pro komunikaci je nutné využívat služeb portálu MyJABLOTRON a využívat připojení jak přes GSM síť, tak i LAN komunikátor. Funkce spínání programovatelného výstupu není garantovaná v případě poruchy externí komunikace nebo výpadku serverů. K jedné ústředně lze připojit až 2 teploměry, které mohou vzdáleně ovládat programovatelný výstup. Dále je možné zasílat notifikace při přetečení nebo podtečení nastavených teplot. Teplotní rozsah měření je v rozmezí od -20°C do 70°C. Odchylka měření teploměru je 0,5°C. Výdrž baterie v detektoru je cca 2 roky [9].

Sběrnicový přístupový modul RFID - *JA-112E* Sběrnicový modul RFID složí k ovládání systému Jablotron 100 (obrázek 5.4). Přístupový modul může být ve variantě s klávesnicí a nebo také i s dvouřádkovým displejem. Jednotlivé ovládací segmenty jdou nad sebe zapojovat do série a je možné tak ovládat až 20 sekcí nebo programovatelných výstupů ústředny. Umožňuje také indikovat stav dané sekce nebo programovatelného výstupu. V neposlední řadě je modul osazen RFID čtečkou na frekvenci EM 125 kHz [9].



Obrázek č. 1: 1 – ovládací segment; 2 – tlačítka segmentu; 3 – prosvětlené aktivační tlačítko s RFID čtečkou; 4 – západky pro otevření modulu;

Obrázek č. 2: 5 – konektor pro připojení ovládacích segmentů; 6 – svorkovnice sběrnice; 7 – sériové číslo; 8 – sabotážní kontakt

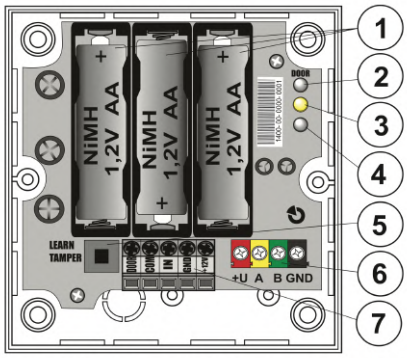
Obrázek 5.4: Sběrnicový přístupový modul RFID - *JA-112E [9]*

Sběrnicový modul pro obsluhu elektrického zámku - *JA-120N* Tato komponenta slouží k ovládání a napájení elektromagnetických zámků a propouštěcích systému ze sběrnice Jablotron 100 (obrázek 5.5). Obsahuje akumulátory, které dodávají počáteční proudový impuls potřebný pro otevření elektromagnetických zámků. Modul reaguje na programovatelný výstup ústředny nebo jej lze aktivovat vybavovacím tlačítkem zapojeným do vstupu IN [9].

Elektronický otevírač BeFo - DUAL - *2611 MB* Tento elektromagnetický zámek (elektronický otevírač dveří) byl zvolen především díky tomu, že disponuje mechanickou blokádou, která umožňuje přepnou zámek do režimu volného průchodu. Zámek je vyobrazen na obrázku 5.6.

Zámek nabízí také odolnost proti vylomení a to konkrétně až silou 2900 N (285 kg). Je také vyroben ze zinku a má stavitelnou západku (4 mm). Zámek bude napájen z komponenty *JA-120N*, vizte sekce 5.1.2 [11].

[1]MyJABLOTRON je webovým portálem výrobce pro ovládání ústředen Jablotron 100 prostřednictvím sítě Internet. Komunikace mezi servery Jablotron a ústřednou je šifrována [9].



Obrázek 1: 1 – akumulátory; 2 – signalizace výstupu DOOR, 3 – signálka komunikace sběrnice JA-100; 4 – signálka aktivace vstupu IN; 5 – tamper; 6 – svorkovnice sběrnice; 7 – svorkovnice vstupů a výstupů

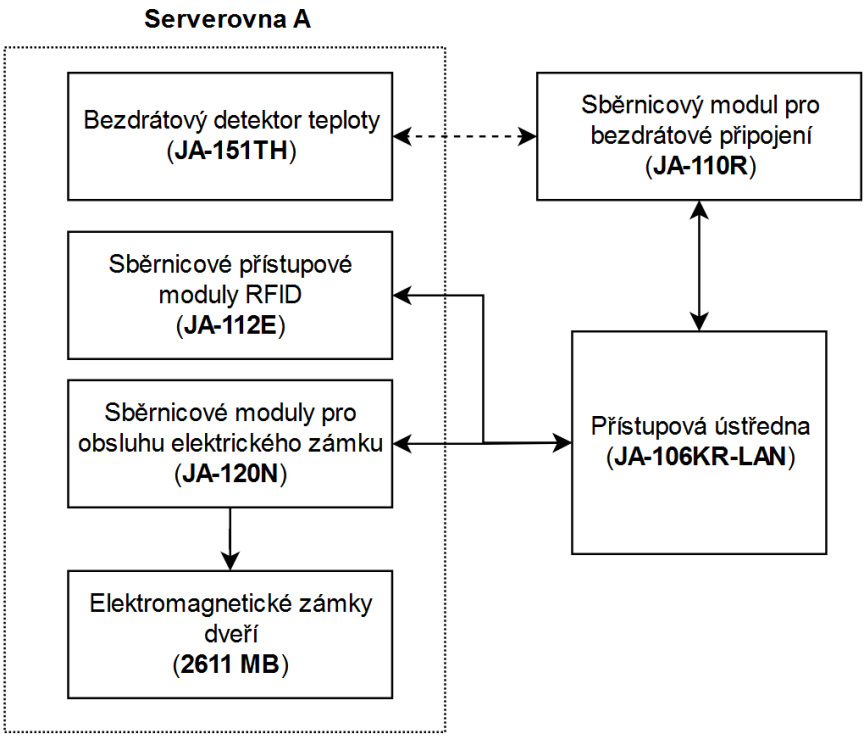
Obrázek 5.5: Sběrnicový modul pro obsluhu elektrického zámku - *JA-120N [9]*

Obrázek 5.6: Elektronický otevírač BeFo - DUAL - *2611 MB [11]*

Samotné rozšíření Pro realizaci výměny zámků serverovny A navrhuji koupit dva sběrnicové přístupové moduly RFID, dva sběrnicové modulu pro obsluhu elektromagnetického zámku a dva elektrické otevírače. Navrhuji pro systém monitoringu teploty serverovny A použít bezdrátový detektor teploty. Všechny nové komponenty budou integrovány se stávající přístupovou ústřednou Jablotron 100. Kabeláž pro propojení sběrnicových technologií bude použita ze zbytků po předchozích instalacích. Navržené schéma rozšíření je znázorněno na obrázku 5.7.

Instalaci komponent a výměnu mechanického zámku za elektrický otevírač provedou pracovníci IT a rozsah prací je odhadován na jeden pracovní den. Interní pracovníci IT provedou nejprve odpojení a demontáž stávajících zámků dveří, dále nainstalují nový elektrický otevírač, propojí jej se sběrnicovým modulem pro obsluhu elektronického zámku a ten následně připojí na sběrnici ústředny Jablotron 100. Jako další namontují sběrnicovým přístupový modul RFID, který taktéž připojí na sběrnici přístupové ústředny Jablotron 100. Dále pracovníci vhodně umístí bezdrátový detektor teploty a spárují jej s ústřednou. Po úspěšné montáži všech komponent naprogramují pracovníci IT přístupovou ústřednu Jablotron 100, aby bylo možné ovládat zámky za pomocí RFID čipu a zařadí dveře do přístupového systému společnosti.

Na obrázku 5.8 je vytvořená tabulka s na základě nejlepší cenové nabídky od poptaných dodavatelů. Celková cena realizace by dle nejlepší nabídky měla činit 6955 Kč bez DPH a bez započtení práce při montáži a konfiguraci. Montáž a konfiguraci doplnění přístupového systému a systému pro monitoring teploty serverovny A provedou pracovníci oddělení IT.



Obrázek 5.7: Schéma rozšíření přístupového systému

Kód	Název	Cena	Množství	Celkem
JA-151TH	Bezdrátový detektor teploty	595 Kč	1	595 Kč
JA-112E	Sběrnicový přístupový modul RFID	1148 Kč	2	2 296 Kč
JA-120N	Sběrnicový modul pro obsluhu elektrického zámku	898 Kč	2	1 796 Kč
	Elektrický otvírač Befo DUAL 2611 MB	1134 Kč	2	2 268 Kč
	Celkem bez DPH			**6 955 Kč**
	DPH 21.00 %			**1 461 Kč**
	Cena celkem s DPH			**8 416 Kč**

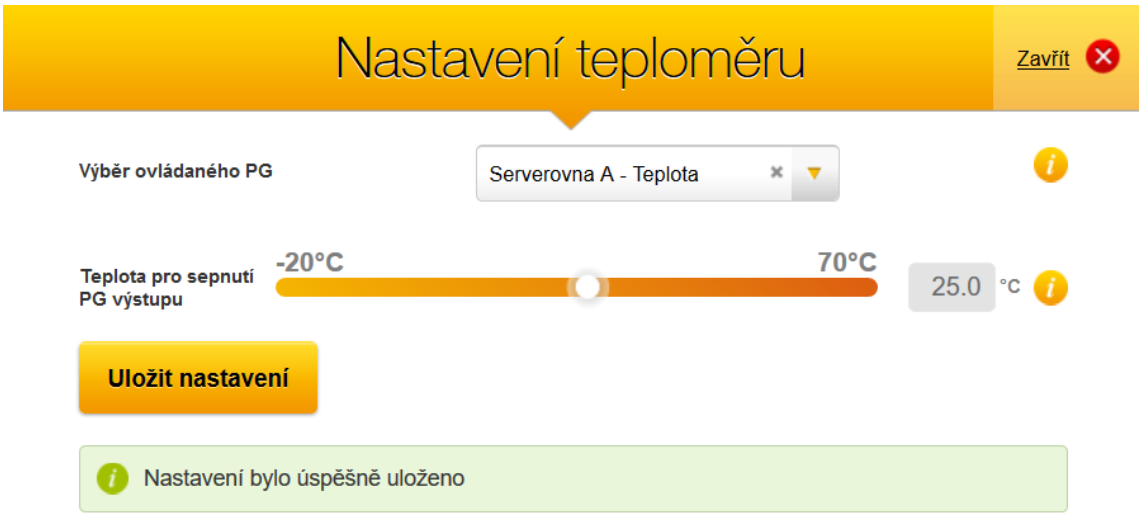
Obrázek 5.8: Cenová nabídka komponent za rozšíření přístupového systému

Konfigurace rozšíření přístupového systému do serverovny A Pro rozšíření konfigurace bude nutné naprogramovat na přístupové ústředně ústředně Jablotron 100 dva nové programovatelné výstup (PG), které je nutné navázat na sepnutí relé sběrnicového modulu pro obsluhu elektronického zámku z předních a zadních dveří. Sepnutí relé bude probíhat ověřením uživatele na sběrnicové přístupovém modulu RFID. Nastavení a způsob organizace ústředen jsem podrobně popsal ve své bakalářské práci [8].

Konfigurace systému monitoringu prostředí serverovny A Pro dosažení výše navrženého je nutné nejprve vytvořit v přístupové ústředně programovatelný výstup (PG). Logika programovatelného výstupu bude spínací a funkce zapni/vypni (dojde k trvalému zapnutí nebo vypnutí). Na základě změny stavu programovatelného výstupu bude ústředna nakonfigurována, aby odesílala upozornění oddělení IT prostřednictvím SMS. SMS upozornění zapnutí programovatelného výstupu bude mít text následující: `Upozorneni: Teplota serverovny A je prilis vysoka!`, zpráva nebude obsahovat diakritiku, protože ústředna

není schopna odeslat tak dlouhou SMS s diakritikou. Text SMS upozornění pro vypnutí programovatelného výstupu bude: `Upozorneni: Teplota serverovny A je jiz v tolerance!`.

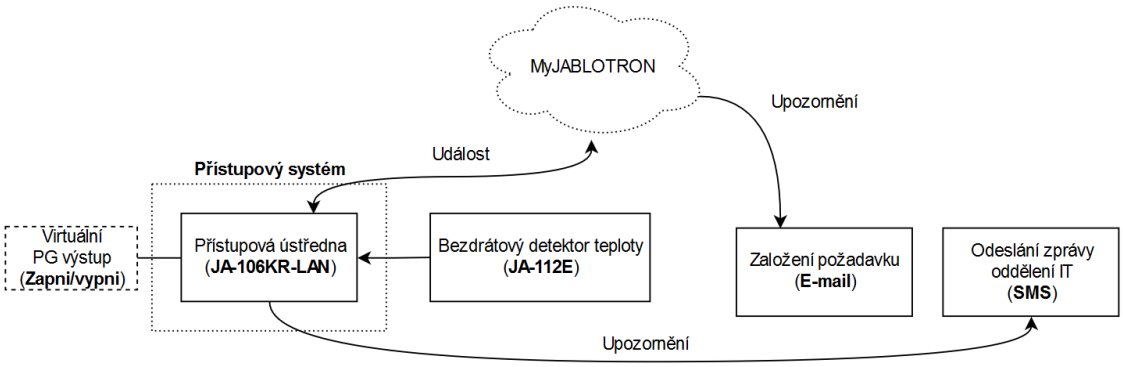
Na základě toho, že přístupová ústředna již je napojena na portál MyJABLOTRON, nebude s ústřednou nutno činit žádné další operace. Všechny další konfigurace se budou provádět na portálu MyJABLOTRON. K navázání bezdrátového detektoru teploty na programovatelný výstup je nutné mít přístupové oprávnění montážníka a provést nastavení přes tento přístup. Abych mohl tuto navrhované řešení realizovat musel jsem se zúčastnit školení a složit závěrečný test. Certifikát o úspěšném absolvování kurzu je přiložen v příloze této diplomové práce A. Po absolvování školení mi byl vygenerován přístup pro montážníka. Montážník má v modulu pro správu instalovaných zařízení možnost dodatečně nastavit funkce bezdrátového detektoru teploty. Nastavení spočívá ve specifikaci ovládaného programovatelného výstupu (musí být funkce zapni/vypni). Dále je nutné specifikovat teplotu pro sepnutí programovatelného výstupu. Tuto teplotu jsem nastavil dle návrhu na 25°C. Pokud naměřená teplota klesne pod hodnotu 25°C, tak se programovatelný výstup sepne. K vypnutí programovatelného výstupu dojde opět po dosažení teploty 25°C. Implementované navržené nastavení je znázorněno na obrázku 5.9.



Obrázek 5.9: Implementace navrženého nastavení teploměru v portálu MyJABLOTRON

Díky propojení bezdrátového detektoru teploty a virtuálního programovatelného výstupu, bude ústředna schopna na základě změny stavu tohoto výstupu odesílat SMS s upozorněním. Aby bylo možné vytvářet požadavky na řešení případného problému s teplotou v serverovně A, je nutné zprovoznit odesílání upozornění E-mailem. Ústředna sama neumožňuje odesílat e-maily, navrhuji pro tento úkol odesílat e-maily na základě událostí o změně stavu programovatelného výstupu portálem MyJABLOTRON. Portál dovoluje nastavit upozornění na zapnutí či vypnutí programovatelného výstupu a toto upozornění odeslat e-mailem na požadovanou adresu. Oznámení o vypnutí virtuálního programovatelného výstupu bude odesílat e-mail na adresu interní podpory společnosti. Odeslaný přijatý e-mail automaticky založí požadavek pro řešení IT oddělením.

Na obrázku 5.10 je znázorněn navržený systém monitoringu teploty serverovny A a následně proces zasílání upozornění ať již prostřednictvím SMS tak i e-mailem.



Obrázek 5.10: Schéma systému monitoringu teploty serverovny A

5.2 Systém řízení napájení

Z provedené analýzy infrastruktury společnosti vyplývá, že oblastí, která společnost trápí nejvíce je problematika nepříznivých stavů serverovny A po výpadku elektrické energie. Před návrhem řešení tohoto problému navrhuji aby byly všechny zařízení, jež jsou součástí infrastruktury servervny A připojeny na záložní zdroj. Navrhuji aby se tak k UPS připojil rozvaděč poskytovatele připojení k Internetu a server Medved 5.

5.2.1 Návrh funkčnosti a specifikace požadavků

Automatické postupné zapínání Navrhuji problematiku řízení napájení i náběhu serverů vyřešit a to připojením zařízení, které bude umístěno za záložním zdrojem UPS a bude řídit automatické postupné zapínání zařízení infrastruktury serverovny A (zátěže). Cílem je aby bylo zajištěno opětovné obnovení plné funkčnosti serverovny podniku po výpadku napájení. Navrhuji aby po obnovení elektrické sítě a sepnutí výstupu na UPS (230 V) došlo v určité časové posloupnosti ke spouštění určitých spotřebičů (zátěží), tak aby nedocházelo k velkým proudovým náběhům (špičkám proudů), které vytvářejí jednotlivé spínané zdroje v těchto zařízeních. Navrhuji rozdělit zařízení infrastruktury do náběhových skupin, které budou postupně v časových rozestupech po obnovení napájení zapínány. Navrhuji rozdělení do čtyř náběhových skupin a to konkrétně:

1. Skupina - **Zařízení v rozvaděči poskytovatele připojení k Internetu** - 15 sekund po obnově napájení UPS
2. Skupina - **Routery a telefonní ústředna** - 2 minuty po obnově napájení UPS
3. Skupina - **Switche** (jak s PoE tak i bez) - 3 minuty po obnově napájení UPS
4. Skupina - **Servery a ostatní zařízení** - 5 minut po obnově napájení UPS

Po detekci obnovy elektrického napájení navrhuji, aby systém nestartoval ihned. Dle mého názoru bude ideální, když systém setrvá 15 sekund bez odezvy a poté sepne první skupinu, následně po 1 minutě a 45 sekundách druhou skupinu, dále po 1 minutě třetí skupinu a na konec po 2 minutách poslední čtvrtou skupinu.

Úvodní prodleva, je navržena protože velmi často se po obnovení přívodu elektrické energie (do nejčastěji 5 sekund) znovu dodávka přeruší. Výše navržené časy byly zjištěny při pokusných startech jednotlivých zařízení skupin infrastruktury.

Dále od záložního zdroje navrhuji odpojit spínané síťové zdroje Mean Well, jež napájí PoE injektory, které mají největší dopad na špičkový odběr.

Specifikace automatického postupného zapínání Základním požadavkem na systém je jednoduché přeprogramování časových intervalů mezi sepnutím jednotlivých skupin. Dalším požadavkem je ovládání výstupů minimálně pro oddělení čtyř skupin. Výhodou by byla možnost rozšíření na více náběhových skupin. Důležité specifikum je i oddělení jednotlivých náběhových skupin jističem. Toto oddělení vyřadí pouze jednu větev a nikoliv celý systém napájení. Požadavkem je také umístění celého řešení na DIN lištu do rozvaděče 2 serverovny A. Zařízení by mělo mít možnost být napájeno 24 V.

Navrhuji, aby byly pro realizaci použity:

- **Jističe** - chrání jednotlivé obvody a zvyšuje spolehlivost, tím, že odstaví vadný obvod a neselže celý systém.
- **Stykače** - zvyšují výkon přenosu proudu a zvyšují odolnost k vyšší četnosti spínání. Například zařízení umí implicitně na výstupu posílat proud 10 A, po použití stykače může na kontaktu být 25 A.
- **Relé** - Slouží ke spínání nebo rozpínání obvodů.

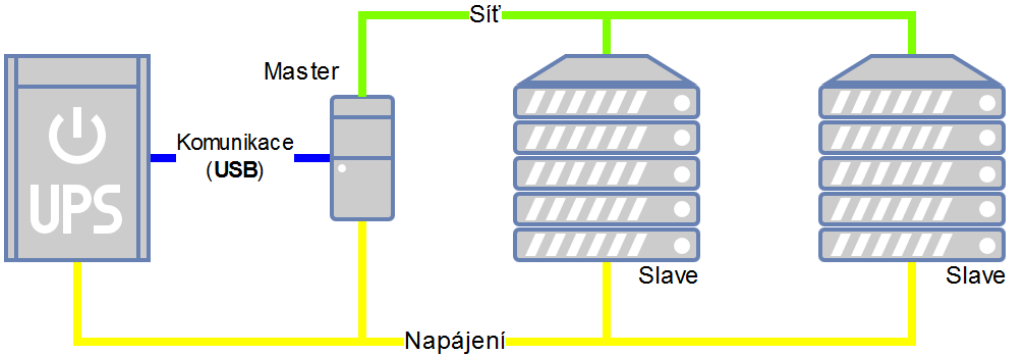
Navrhuji, aby byl systém zapojen následujícím způsobem. Výstup z UPS bude připojen do řídicí jednotky systému, která bude detekovat obnovu napájení z UPS. Na výstupy pro jednotlivé náběhové skupiny řídicí jednotky systému navrhuji připojit jistič, za jistič stykač a na kontakty stykače rozvodný zásuvkový panel konkrétní skupiny.

Pro jednotlivé náběhové skupiny budou vyhrazeny zásuvkové panely, do kterých budou připojeny zařízení infrastruktury podle typu zařízení.

Komunikace s UPS Cílem optimalizace komunikace s UPS v serverovně A udělat síťový záložní zdroj, který předává informace o svém stavu přes infrastrukturu sítě ostatním zařízením v síti. Na základě analýzy se jedná o záložní zdroj EATON 9SX 6000 s dvěma bateriovými moduly, který umožňuje komunikaci přes USB pouze s jedním zařízením.

V úvahu při návrhu připadají tři varianty. Prvním z nich je rozšířit záložní zdroj EATON o síťovou komunikační LAN kartu. Tato varianta ovšem neumožní připojení UPS ke všem zařízením a to konkrétně diskovému úložišti, které kompatibilní s výše uvedenou UPS při komunikaci jiným způsobem než přímo přes USB. Druhým řešením je výměna za UPS značky APC, jež si ale vedení společnosti nepřeje. Třetí variantou a i nejvhodnější je připojení záložního zdroje do zařízení, které bude zpřístupňovat UPS a informace o jejím stavu po síti a to i zařízením, které přímo nepodporují konkrétní používaný záložní zdroj.

Navrhuji, aby informace o stavu UPS měly i ostatní zařízeni serverovny A. Záložní zdroj navrhuji připojit přes USB k master zařízení, které bude předávat informace o stavu UPS. Ostatní zařízení (slave) připojené k napájení z UPS budou informace o stavu záložního zdroje zdroje získávat přes IP protokol od zařízení master. Blíže je návrh komunikace UPS s master zařízením a komunikace master se slave zařízeními znázorněn na obrázku 5.11. Master zařízení by mělo posílat při vybití baterií na úroveň, kdy zbývá pouze 1/5 kapacity baterií příkaz k vypnutí slave zařízení. Ponechání části kapacity v bateriích záložního zdroje je navrženo z toho důvodu, že k výpadkům může dojít opakovaně i více krát po sobě a je nutné ponechat dostatek energie pro čas než se korektně vypnou všechna napájená zařízení. Master zařízení by mělo být schopno taktéž poslat upozornění prostřednictvím SMS internímu IT oddělení o výpadku elektrického proudu v serverovně A.



Obrázek 5.11: Návrh komunikace UPS s master zařízením a komunikace master se slave zařízeními

Specifikace komunikace s UPS Navrhuji, aby byl pro systém komunikace s UPS použit jako master spolehlivé zařízení, schopné běhu operačního systému Debian Linux. Zařízení by mělo mít minimálně 1 GHz procesor a 1 GB operační paměti a kapacitu 4 GB. Dále by mělo být schopno komunikovat prostřednictvím sítě Ethernet a GSM. GSM modem je nutnou podmínkou jelikož je požadováno, aby zařízení bylo schopné odesílat SMS upozornění IT administrátorům. Master zařízení by stejně tak jako programovatelný automat pro ovládání automatických náběhů mělo být schopno provozu na napájení z 24 V. Master zařízení by mělo být taktéž umístitelné na DIN lištu.

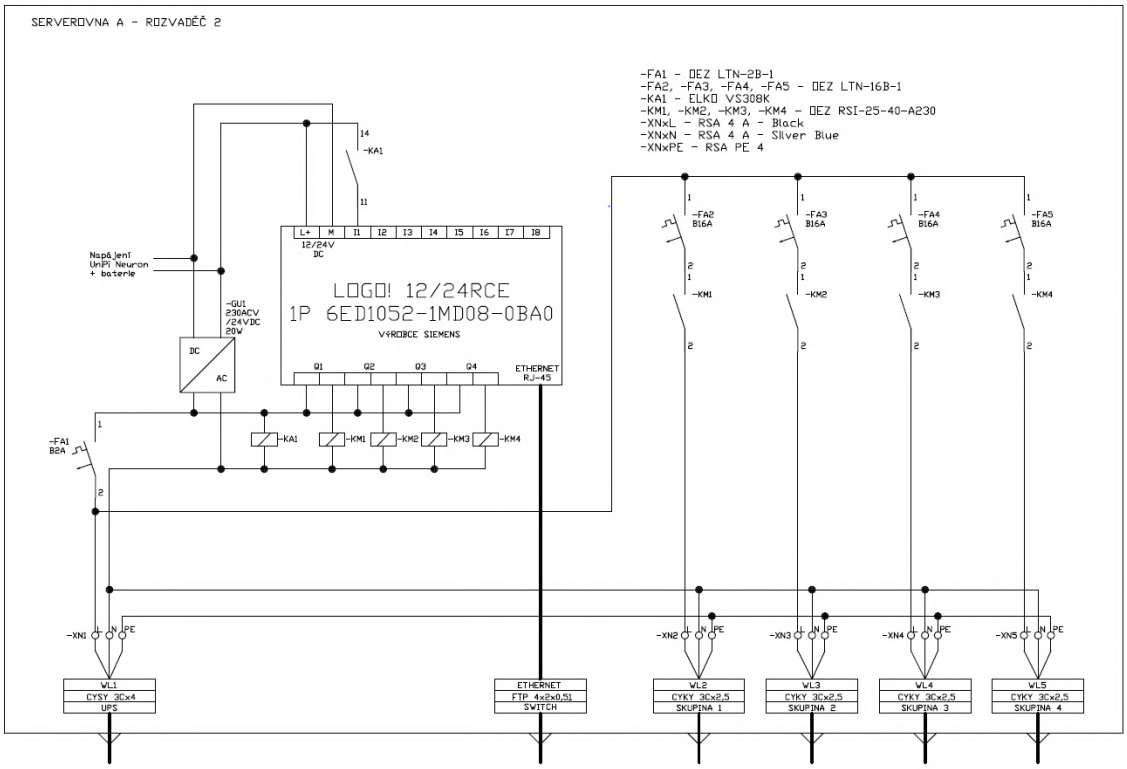
5.2.2 Realizace

Automatické postupné zapínání Jedním z řešení dle návrhu výše by bylo použití časových relé, které ale nesplňují základní požadavek na možnost jednoduše upravit časy spouštění jednotlivých zapínacích skupin. U časových relé by bylo nutné pro úpravu časů provést i fyzické předrátovaní. Proto navrhuji, aby bylo k automatickému spínání skupin použito multifunkční programovatelný automat PLC (Programmable Logic Controller). Doporučuji použít programovatelný automat Siemens LOGO!. V úvahu pro řešení přicházely taktéž inteligentní rozvodné panely PDU, které jsou ale výrazně dražší a nenabízí možnost rozšíření o jističe. Zařízení Siemens volím na základě dobrých referencí od kolegů spravujících solární elektrárny, na kterých jsou hlavní jednotky právě Siemens LOGO! funkční již déle než 15 let. Výhodou programovatelného automatu Siemens je jeho modulárnost, možnost rozšíření o další výstupy a relativně jednoduché programování, které se dá realizovat pomocí logických bloků.

Zapojení systému bude následující dle schématu 5.12. Do digitálního vstupu PLC Siemens LOGO! bude přiveden výstup z relé, jež je napojeno na výstup z UPS 230 V. Siemens LOGO! bude detekovat. že je přítomen proud z UPS. Na základě přivedeného napětí a časové prodlevy se budou postupně spínat čtyři stykače, do kterých budou přes čtyři jističe připojeny rozvodné zásuvkové panely jednotlivých náběhových skupin podle návrhu. Před zařízením LOGO! bude taktéž pojistka, aby bylo taktéž chráněné.

Pro řešení navrhuji použít konkrétně tyto komponenty dle návrhu na schématu 5.12 :

- 1 x PLC - **Siemens LOGO! 12/24RCE (6ED1052-1MD08-0BA0)** - programovatelný automat na DIN lištu se čtyřmi programovatelnými výstupy, osmi digitálními vstupy, integrovaným webovým serverem a Ethernet portem. Celá jednotka splňuje



Obrázek 5.12: Realizace zapojení systému automatického postupného zapínání infrastruktury Serverovny A s PLC Siemens LOGO

certifikaci CE[2], zkoušky EMC[3] a také stupeň krytí IP20[4] - cena za kus 3200 Kč bez DPH.

- 1 x jistič - **OEZ LTN-2B-1** - jedno-pólový jistič na DIN lištu, jmenovitý proud tohoto jističe je 2 A, vypínací charakteristika B - cena za kus 200 Kč bez DPH.
- 4 x jistič - **OEZ LTN-16B-1** - jedno-pólový jistič na DIN lištu, jmenovitý proud tohoto jističe je 16 A, vypínací charakteristika B - cena za kus 90 Kč bez DPH.
- 4 x stykač - **OEZ RSI-25-40-A230** - 25 A stykač na DIN lištu s vizuální indikací při zapnutí - cena za kus 410 Kč bez DPH.
- 15 x svorkovnice - **OEZ RSA 4** - Řadová svorkovnice na DIN lištu pro kabely (různé barvy) - cena za kus 10 Kč bez DPH.

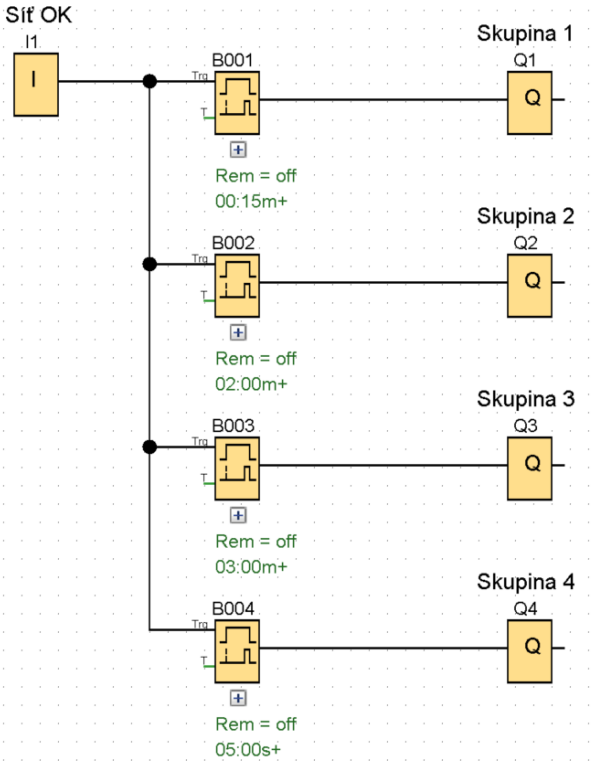
Celková cena součástek řešení potřebných pro realizaci automatického postupné zapínání je 5550 Kč bez DPH. Relé a kabeláž pro propojení komponent bude použita ze skladových zásob společnosti. Pro programovatelný automat jsem vytvořil program v oficiálním nástroji LOGO!Soft Comfort, který je znázorněn na obrázku 5.13. Program byl napsán aby detekoval

[2]CE certifikát je nezávislým ověřením posouzení shody výrobku s požadavky příslušných nařízení vlády, které provádí výrobce [6].

[3]Elektromagnetickou kompatibilitou (EMC) je nazývána schopnost elektrického zařízení nerušit jiná elektrická zařízení a odolávat jejich případnému rušení [6].

[4]IP20 znamená že, zařízení je chráněno před vniknutím pevných cizích těles o průměru 12,5 mm a větších a před dotykem prstem. Není chráněno proti vodě[13].

stav elektrické sítě na výstupu z UPS a po časové prodlevě 15 sekund spustil sepnul výstup, který je připojena skupina 1. Následně spustil v čase dvou minut od detekce, že je síť v pořádku spustil sepnul výstup skupiny 2, dále v čase tří minut výstup se skupinou 3 a v čase pět minut výstup se skupinou 4. Následně zůstanou výstupy sepnuté, až do přerušení detekce napájení z UPS.



Obrázek 5.13: Program chování v PLC LOGO

Komunikace s UPS Jedním z nejlevnějších spolehlivých zařízení jež jsou schopné plnohodnotného běhu operačního systému Debian je Raspberry Pi, konkrétně Raspberry Pi 3[5]. Toto zařízení ovšem není vybaveno krytem a nedá se tak umístit na DIN lištu. Navrhuji jako master jednotku pro realizaci systému komunikace s UPS použít UniPi Neuron S103-G. Toto zařízení s cenou 6500 Kč bez DPH je vybaveno GSM modemem a je vhodné pro umístění na DIN lištu. Toto zařízení splňuje všechny specifické požadavky a navíc jej volím, protože tento typ zařízení používá společnost ve svém řešení systému měření a regulace. Společnost má s tímto zařízením již dlouholeté zkušenosti a důvěru.

UniPi Neuron je programovatelnou logickou jednotkou, která je vybavena řadou vstupů a výstupů. Tato jednotka vychází z mikropočítače Raspberry Pi 3 doplněného o rozšiřující obvody od společnosti UniPi.technology. Je také zapouzdřena do hliníkového krytu, který je umístitelný na DIN lištu a zabírá na ní 4 pozice. Výrobek je určen pro průmyslové použití a proto se vyznačuje vysokou spolehlivostí bez nutností restartu. Řídící jednotka používá operační systém Debian Linux. Další výhodou je velká rychlost vnitřní komunikace a tím minimální zpoždění při provádění příkazů.

[5]Raspberry Pi 3 model B https://www.raspberrypi.org/products/raspberry-pi-3-model-b/

Obrázek 5.14: UniPi Neuron - *S103-G [24]*

Jako master zařízení systému komunikace s UPS byla zvolena jednotka S103-G (obrázek 5.14). Tato jednotka je nejmenším a nejlevnějším produktem z řady Neuron, která je vybavena GSM modemem. Výběr tohoto produktu také zapadá do celkové koncepce společnosti SPOLEČNOST-24, s.r.o.

Klíčovými vstupy a výstupy jednotky UniPi Neuron S103 jsou:

- GSM/GPRS modem pro připojení k GSM síti a odesílání SMS,
- 4x USB 2.0,
- napájecí zdroj (24 V DC).

Jednotka je osazena čtyř-jádrovým procesorem o taktu 1,2 GHz. Nabízí 1 GB operační paměti. Pro připojení do počítačové sítě slouží síťová karta 10/100 Mb/s, případně WiFi standardu b/g/n. Jednotka je napájena pomocí stejnosměrného 24 V adaptéru a je možné ji připevnit na DIN lištu. Výhodou této jednotky je také její rychlost. Celá jednotka splňuje certifikaci CE, zkoušky EMC a také stupeň krytí IP20 [24].

Na jednotku bude nainstalován software Network UPS Tools[6], který pracuje na principu z návrhu řešení a zpřístupňuje lokálně připojenou UPS přes síť ostatním slave zařízením přes protokol SNMP. Dále bude software NUT nakonfigurován tak, aby při výpadku napájení odesílal interním administrátorům SMS s upozorněním o výpadku elektrického proudu. SMS upozornění při výpadku napájení bude mít text následující: `Upozorneni: Napajeni serverovny A bylo preruseno!`, zpráva nebude obsahovat diakritiku, protože modem není schopen odeslat tak dlouhou SMS zprávu s diakritikou. Text SMS upozornění při obnovení napájení serverovny A bude: `Upozorneni: Napajeni serverovny A je jiz`

[6]Network UPS Tools (NUT) https://networkupstools.org/

`obnoveno!`. Pro odesílání SMS bude použit již existující mobilní tarif systému měření a regulace. V neposlední řadě bude master zařízení (Neuron) odesílat slave zařízením požadavek na vypnut při vybití baterií na úroveň, kdy zbývá pouze 1/5 kapacity baterií UPS.

Obě řídící jednotky systému napájení (Siemens LOGO!) a komunikace s UPS (UniPi Neuron) budou zálohovány baterií a napájeny jedním stejnosměrným 24 V zdrojem. Díky tomu, že budou obě jednotky napájeny z jednoho zdroje se zvýší jejich spolehlivost a sníží se chybovost. V rámci zvýšení stability a snížení špičkových proudů při náběžích navrhuji odpojit i všechny spínané síťové zdroje Mean Well, jež napájí PoE injektory, které mají největší dopad na špičkový odběr. Jeden z těchto zdrojů včetně PoE injektoru navrhuji přemístit do serverovny B pro napájení IP kamer přes PoE.

5.3 Serverová infrastruktura

5.3.1 Návrh funkčnosti a specifikace požadavků

Na základě analýzy má společnost k dispozici sedm serverů, diskové úložiště, telefonní ústřednu, kamerový server a NVR. Společnosti v současné době vyhovují hardwarové parametry serverů a nabízí ještě dostatečný rezervní výkon. Nenavrhuji tedy žádnou aktualizaci komponent serverů, ani sloučení fyzických zařízení. Navrhuji aby kamerový server, NVR a telefonní ústředna zůstaly beze změn, vyhovují kompletně aktuálním požadavkům společnosti V průběhu analýzy vypověděl službu server Medved 4. Tento server navrhuji rozebrat a uschovat pevné disky, operační paměť RAM a procesor. Zbytek serveru navrhuji ekologicky zlikvidovat, není důvodu proč by měl server zabírat místo v racku serverovny A. Dále navrhuji vyčištění serverů od prachu vyfoukáním vzduchem. Prostory provozovny prošly rekonstrukcí v roce 2016 a v době nastěhování fyzických serverů do serverovny A neměla serverovna dveře a byla v ní tedy zvýšená prašnost.

Z analýzy infrastruktury společnosti vyplývá, že má společnost celkem 14 virtuálních serverů, které provozuje na 5 fyzických serverech. V rámci optimalizace a minimalizace infrastruktury podniku navrhují část infrastruktury, zrušit, přesunout do cloudu nebo archivovat. Cílem je, aby se interní IT oddělení nemuselo starat o zbytečně příliš mnoho serverů, které nepřináší žádný vyšší komfort uživatelům a taktéž je tento návrh motivován snahou o zajištění vysoké dostupnost služeb nejen z prostředí provozovny nebo sídla, ale jakékoliv lokality s přístupem k Internetu.

Další problematikou, na kterou bych se chtěl zaměřit je umístění uživatelských dat a dat oddělení. Uživatelé ukládají svá data lokálně do počítačů například na plochu nebo do dokumentů. Tyto uživatelské složky, ale dle analýzy nejsou nijak zálohována. Situace s daty je rozdílná, kdy data jsou umístěna na síťovém diskovém serveru. Pro přístup k datům oddělení mimo prostředí společnosti je možné pouze přes VPN, kterou ale nemají všichni uživatelé. Navrhuji aby byly data uživatelů i skupin v jedné platformě (řešení) a byly trvale zálohována a přístupná z Internetu i bez VPN. V rámci optimalizace celkové koncepce a směrování IT navrhuji aby společnost začala využívat veřejný cloud. Bezpečnost samotného datového centra je vždy vyšší než bezpečnost lokální serverovny.

Společnost používá již nepodporovaný kancelářský balík Microsoft Office 2007 a z důvodu zjednodušení předávání informací navrhuji používat předplatné Microsoft Office, které zajistí vždy aktuální verzi kancelářského balíku Microsoft Office. Navrhuji aby uživatelé měli možnost používat kancelářský balík ve stejné verzi i na svém domácím počítači, což bude mít pozitivní dopad na produktivitu zaměstnanců. V rámci zvýšení produktivity a snížení

prostojů navrhuji aby zaměstnanci tiskli přímo přes síťové tiskárny tiskárny a byl vynechán tiskový server.

Specifikace požadavků Navrhuji aby bylo množství lokálně provozovaných serverů sníženo, zrušením již nepotřebných serverů. Při změně části stávající infrastruktury na cloud požaduji, aby dodavatel cloudového řešení nabízel komplexní služby od ověřování identit, ukládání dat, e-mailové komunikace až po kancelářský balík a kolaborační software. Dále by měla všechna uživatelská a firemní data na lokálních počítačích zálohována a přístupná bez VPN z cloudu.

5.3.2 Realizace

Konsolidace serverů Na základě specifikace jsem navrhl konsolidaci virtuálních serverů. Na obrázku 5.15 je znázorněno co se stane s každým konkrétním serverem infrastruktury. Na obrázku není znázorněn server Medved 0 a diskové úložiště QNAP. Tyto dva servery budou složit k zálohám a archivaci dat.

Kolaborační server Portal navrhuji v budoucnu zrušit a místo něj pro ukládání souborů a komunikaci nad jednotlivými úkoly přesunout na službu Microsoft 365, konkrétně na SharePoint Online. Server bude nadále provozován na serveru Medved 1 ve formě archivu a bude přepnut do režimu jen pro čtení. E-mailový server Kerio1 zůstane zachován ve stejném stavu na serveru Medved 1, jen bude předávat E-mailovou poštu i na cloudový server Exchange Online. Server Kerio1 i nadále zůstane funkční pro odesílání zpráv pro interní systém měření a regulace. Dále bude server Synopsis přesunut do soukromého cloudu společnosti SynopsIS Technologies a.s., která je zároveň i tvůrcem tohoto softwarového řešení. Server Synopsis tak bude přístupný přes Internet a bude pod správou přímo samotného výrobce, což urychlí zpracování případných požadavků na úpravu funkcionality software. Cena hostování pohledávkového systému v soukromém cloudu by měla být v řádu jednotek tisíc Kč měsíčně. Server Synopsis02 již po migraci hlavního pohledávkového serveru nebude potřebný, protože testovací instance bude zpřístupněna přímo jako další instance cloudového serveru Synopsis.

Původní umístění	Nové umístění	Co se stane	Název serveru	Role	Operační systém
Medved 1	Archiv	Bude zrušen a archivován	Portal	Bitrix - Intranet	CentOS 7
Medved 1	Medved 1	Bude zachován	Kerio1	E-mailový server	Debian 9.4
Medved 1	Cloud SynopsIS	Bude přemístěn	Synopsis	Pohledávkový systém	Ubuntu 12.04 LTS
Medved 1		Bude zrušen	Synopsis02	Pohledávkový systém	Ubuntu 12.04 LTS
Medved 2		Bude zrušen	Backdomain	Záložní - Zentyal AD na linuxu	Ubuntu 14.04 LTS
Medved 2	Archiv	Bude zrušen a archivován	Epodatelna	Archiv datových zpráv	Windows 10 Pro
Medved 3	Medved 2	Bude přemístěn	Terminal24	RDS server	Windows Server 2016
Medved 3	Medved 3	Bude zachován	Terminal	Spisová služba - produkce	Windows Server 2012
Medved 3		Bude zrušen	Server24	AD, DNS, DHCP, Profily	Windows Server 2016
Medved 3		Bude zrušen	Optimidoc	Tiskový server	Windows Server 2012
Medved 3		Bude zrušen	Backoffice	Zentyal AD na linuxu	Ubuntu 14.04 LTS
Medved 3		Bude zrušen	ESS	Spisová služba - testovací	Windows Server 2012
Medved 5	Medved 5	Bude zachován	Synopsis01	Klientský pohledávkový systém	Ubuntu 12.04 LTS
Medved 6	Medved 6	Bude zachován	Kerio2	Klientský e-mailový server	Debian 9.4

Obrázek 5.15: Návrh konsolidace serverů v infrastruktuře podniku

Ze serveru Medved 2 bude záložní linuxový doménový řadič Backdomain bez archivace zrušen. Server Epodatelna s archivem datových zpráv bude nadále provozován ve formě archivu a bude přepnut do režimu pouze pro nahlížení. Na Medved 2 se přemístí terminálový

server Terminal24, na který bude nainstalován kancelářský balík Office 365 a umožní přihlašování uživatelů pomocí AzureAD. Přihlašování uživatelů přes AzureAD bude na serveru Terminal24 specifické, protože v infrastruktuře nebude k dispozici žádný lokální doménový kontroler Active Directory, který by ověřil identitu uživatele i instanci terminálového serveru.

Server se spisovou službou Terminal zůstane zachován ve stejném fyzickém umístěni i funkčnosti jako doposud. Hlavní doménový řadič Server24 bude zrušen. Přesun služeb DNS a DHCP bude popsán v kapitole 5.4. Místo ověřování a správy uživatelů v lokální adresářové službě Active Directory Domain Services bude společnost používat ověřování identit uživatelů a počítačů cloudovou alternativu AzureAD, jež je součástí řešení Microsoft 365, které je popsáno níže v této kapitole. Profily uživatelských účtů budou umístěny lokálně na pracovních stanicích nebo na terminálovém serveru Terminal24. Tiskový server Optimidoc bude bez náhrady zrušen. Tisky jednotlivých uživatelů budou směrovány přímo na konkrétní síťové tiskárny bez prodlevy tiskového serveru. Skenování dokumentů z tiskáren bude probíhat do e-mailových schránek nebo do cloudového souborového úložiště SharePoint Online. Historický linuxový doménový kontrolér a proxy server Backoffice bude taktéž zrušen. Přístup z veřejného Internetu na servery již nebude realizován skrz proxy server, ale skrz hlavní router, blíže popsáno v kapitole 5.4. Testovací virtuální server se spisovou službou ESS bude zrušen. Testovací instance spisové služby bude integrována do produkčního serveru Terminal, integrace umožní rychlejší tvorbu obrazu produkční verze do testovací instance.

S klienty podniku byl diskutován záměr konsolidace a případný přesun do cloudu, který byl ale ze stran klientů zamítnut a přejí si, aby jejich servery zůstaly hostovány v nezměněné formě. Server Synopsis01 i Kerio2 zůstanou umístěny na původních serverech bez jakékoliv změny.

Umístění	Název serveru	Role	Operační systém
Medved 1	Portal	Bitrix - Intranet	CentOS 7
Medved 1	Kerio1	E-mailový server	Debian 9.4
Medved 2	Epodatelna	Archiv datových zpráv	Windows 10 Pro
Medved 2	Terminal24	RDS server	Windows Server 2016
Medved 3	Terminal	Spisová služba - produkce	Windows Server 2012
Medved 5	Synopsis01	Klientský pohledávkový systém	Ubuntu 12.04 LTS
Medved 6	Kerio2	Klientský e-mailový server	Debian 9.4

Plnohodnotný server
Server jen pro čtení

Obrázek 5.16: Stav serverů ve společnosti po konsolidaci

Stav po konsolidaci popsané výše bude takový, že na lokálních serverech poběží pouze sedm virtuálních serverů, z nich dva jsou klientské, jež mají pro svůj chod vyhrazen celý fyzický server a dva servery pouze v režimu archivu s přístupem pro čtení vizte obrázek 5.16. Samotná společnost bude po konsolidaci pro svůj chod potřebovat pouze tři provozní virtuální servery z původních dvanácti.

Řešení cloudové infrastruktury Pro realizaci návrhu ukládání dokumentů navrhuji přejít na cloudové řešení Microsoft 365 v edici E3. Microsoft 365 je kompletní inteligentní

řešení, které zahrnuje Office 365, Windows 10 a sadu Enterprise Mobility + Security, jenž umožňuje všem bezpečně a kreativně spolupracovat. Edici E3 volím z toho důvodu, že umožňuje používat kancelářský balík Microsoft Office 365 i na terminálovém serveru (RDS, Remote Desktop Services), jedná se konkrétně o možnost aktivace software na sdíleném počítači. Řešení Microsoft 365 obsahuje přístup k základním produktům a funkcím společnosti Microsoft, které umožňují zvýšení produktivity a bezpečnosti. Celé řešení Microsoft 365 používá při přenosu dat šifrování a skládá se z těchto částí:

- Licence pro operační systém Windows v edici Enterprise.
- Přístup ke klientským aplikacím Office (Word, Excel, PowerPoint, OneNote a Access) nainstalovaných až na 5 počítačích, 5 tabletech a 5 mobilních telefonech s Office 365 v edici ProPlus. Dále budou mít uživatelé přístup k Office Mobile a webovému Office Online.
- E-mail a kalendář bude k dispozici přes cloudový E-mailový server Exchange Online s možností používat klient Outlook.
- Portál Teams pro kolaboraci, přístup k dokumentům a hlasovou i video komunikaci. K řízení úkolů je možné použít aplikaci Planner nebo To-Do.
- Soubory a obsah jsou uloženy v SharePoint Online a poskytuje neomezené úložiště OneDrive pro skupiny a kapacitu 1 TB dat pro uživatelské soubory.
- Ochrana před internetovými útoky a viry.
- Správa identit a přístupů - Azure Active Directory.
- Správa zařízení a aplikací pomocí portálu Microsoft Intune.
- Další komponenty řešení jsou dostupné na webových stránkách společnosti Microsoft[7].

Cena řešení Microsoft 365 v edici E3 je přibližně 31,5 EUR bez DPH za uživatele za měsíc. Řešení obsahuje téměř všechny aplikace a služby Microsoftu, se službou nejsou spojeny žádné další poplatky ani více náklady.

Všechny uživatelská data budou z lokálních počítačů zmigrována na SharePoint Online konkrétně do služby OneDrive. Následně budou na všech klientských stanicích přesměrovány složky plocha, dokumenty a obrázky na cloudové úložiště SharePoint Online přístupné z Internetu bez VPN. Přístup k souborům bude skrz zabezpečenou infrastrukturu společnosti Microsoft s přihlašováním přes AzureAD.

Klientské počítače budou připojeny do cloudové domény AzureAD a uživatelé budou používat jednotné přihlašování na všech svých zařízeních ať již telefonech nebo tabletech i na domácích počítačích. Přihlašování a přístup k dokumentům bude tak závislé pouze na připojení k Internetu a ne na stavu serverů podniku.

5.4 Síťová infrastruktura

Na základě návrhu přesunu části serverové infrastruktury do cloudu Microsoft 365, je nutné přizpůsobit této změně i síťovou infrastrukturu podniku. Dle konsolidace serverů bude třeba dále navrhnout, které zařízení bude poskytovat služby DHCP a DNS serveru. Zároveň je nutné optimalizovat síť i z toho důvodu, že je aktuálně plochá a vše je v jedné síti.

[7] Webové stránky společnosti Microsoft s porovnáním plánů řešení Microsoft 365 jsou dostupné na adrese: https://www.microsoft.com/cs-cz/microsoft-365/compare-all-microsoft-365-plans.

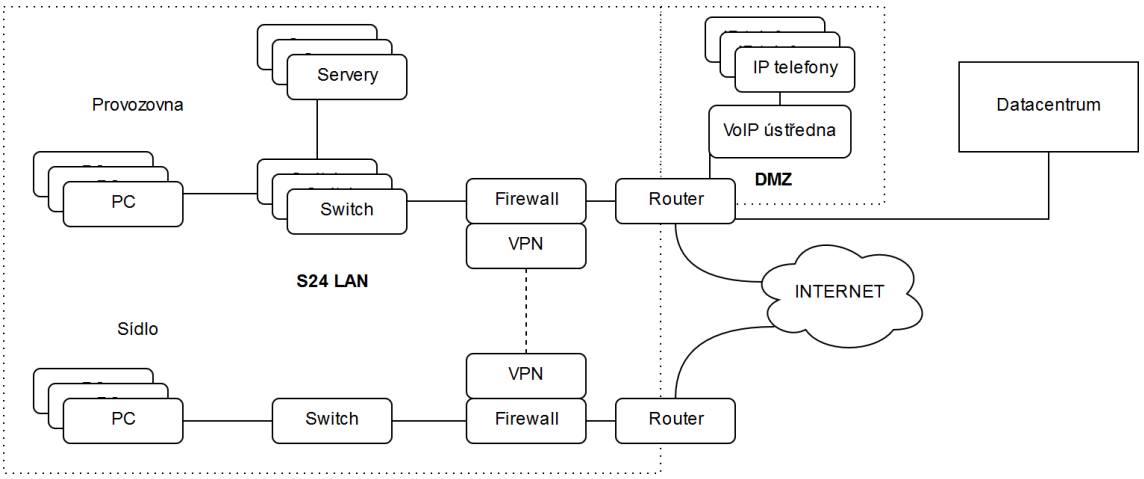
Požadavky na síť Používání Microsoft cloudu nenese žádné významné zásahy do síťové infrastruktury, jedinou prerekvizitou pro optimalizaci rychlosti je používaní nejbližších DNS serverů. Kromě změny bude potřeba vytvořit DNS záznamy pro automatickou konfiguraci cloudových služeb Microsoft pro uživatele a příjem pošty. Ze strany vedení společnosti se klade požadavek na oddělení lokální sítě, alespoň části se systémem měření a regulace a hostovaných serverů. Z důvodu automatické konfigurace IP telefonů je nutné oddělit taktéž síť, do které jsou připojeny IP telefony. Navrhuji aby byly WiFi přístupové body spravovány centrálně.

5.4.1 Logická topologie

Navrhuji síťovou infrastrukturu podniku rozdělit na čtyři základní oddělené celky:

- **S24 LAN** - lokální síť podniku, která bude obsahovat všechnu technologii podniku a bude dále logicky rozdělena do VLAN.
- **S24 TEL LAN** - vyhrazená lokální síť pouze pro VoIP telefonní ústřednu a IP telefony, jenž bude umístěna v DMZ.
- **S24 HOSTING LAN** - lokální síť s klientskými hostovanými servery.
- **S24 PODPORA LAN** - síť pro interní oddělení IT, která bude mít neomezený přístup do všech sítí.

Spojení sídla a pobočky navrhují v rámci zjednodušení infrastruktury na druhé vrstvě ISO/OSI modelu pomocí VPN tunelu a v něm zapouzdřeného EoIP tunelu. Schéma navrhované sítě S24 LAN je znázorněno na obrázku 5.17.



Obrázek 5.17: Logická topologie sítě S24 LAN

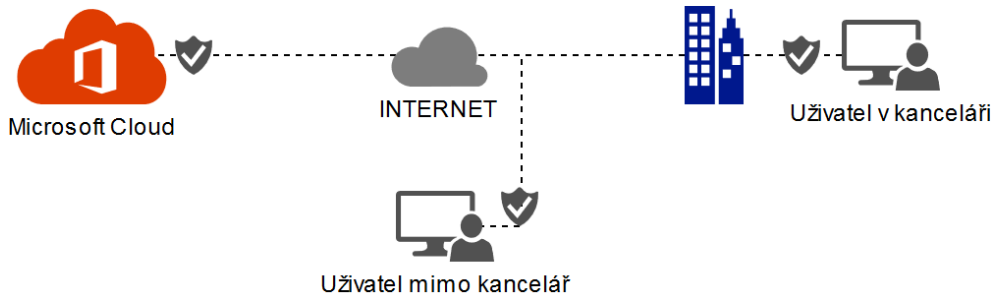
Lokální síť S24 LAN navrhuji dále logicky rozdělit do 5 VLAN (konkrétní navrhované rozsahy nebudou z důvodu bezpečnosti zveřejněny):

- **VLAN 1** - privátní síť pro připojení stolních počítačů, přenosných zařízení a tiskáren s přístupem do serverové sítě. Pro privátní síť navrhuji použít rozsah X.X.0.0/23.
- **VLAN 2** - hostovská síť pro návštěvy společnosti s přístupem pouze k internetu. Pro hostovskou síť navrhuji použít rozsah X.X.X.0/24.

- **VLAN 4** - serverová síť pro interní servery a hypervizory. Pro serverovou síť navrhuji použít rozsah X.X.4.0/24.
- **VLAN 5** - technická síť pro zařízení, které jsou spojena s provozem budovy. Do této VLAN budou přidány zařízení systému měření a regulace (PLC, metostanice, kotle, vzduchotechnika, klimatizace...), IP kamery a navrhovaný systém monitoringu napájení. Pro technologickou síť navrhuji použít rozsah X.X.5.0/24.
- **VLAN 6** - správcovská VLAN, z této VLAN budou přístupné všechny spravovatelné síťové prvky (routery a switche). Pro správcovskou síť navrhuji použít rozsah X.X.6.0/24.

VLAN 3 je záměrně vynechána, protože bude ponechána rezerva v číslování pro potřeby ještě podrobnějšího členění sítě.

Přístup k souborů a serverům mimo privátní síť S24 LAN Na základě návrhu a zrušení proxy serveru bude nutné, aby byly původně veřejně přístupné servery z Internetu dostupné i nadále. Navrhuji, aby hlavní router překládal porty z jednotlivých veřejných IPv4 adres na lokální IPv4 adresy a porty serverů. Pro přístup ke službám, komunikačním nástrojům a souborům navrhuji aby zaměstnanci nepoužívali VPN ale přistupovali k serverům Microsoftu přímo. Při komunikaci s cloudovými servery je velmi důležitá odezva a ta by při použití VPN a směrování datového toku přes připojení k Internetu společnosti byla zbytečně zvyšována. Navíc by použití VPN pro uživatele nepřineslo žádné výhody ani v zabezpečení, protože přenos z Microsoft Cloudu až po uživatele je zabezpečen, konkrétně šifrován. Navrhované logické schéma při komunikaci na Microsoft cloud je znázorněno na obrázku 5.18.



Obrázek 5.18: Návrh logické topologie při komunikaci na Microsoft cloud

5.4.2 Požadavky na jednotlivé prvky

Jednotlivé prvky infrastruktury by měly disponovat podporou pro protokol SNMP a podporovat VLAN. Výběr nových přepínacích prvků by měl zohledňovat a podporovat technologii STP[8], aby nevznikaly smyčky. Nasazované přepínače by také v nejlepším případě měly být managované, pracovat na vrstvě L3 ISO/OSI modelu a nejlépe používat stejný operační systém jako hlavní router tedy RouterOS[9] nebo kompatibilní. V případě, že prvek má jiný

[8]Spanning Tree Protocol pracuje na principu teorie grafů. Síť představuje ohodnocený graf a algoritmus hledá v kostře tohoto grafu nejkratší cesty mezi uzly (switchi) [10].

[9]RouterOS je operačním systémem v zařízeních od společnosti MikroTik.

operační systém je potřeba posoudit vhodnost a přijmout případné riziko potíží. Pokud by byl v infrastruktuře použit nemanagovaný switch, tak případu použití nevyhovuje a mohl by způsobit potíže, které nikde nebudeme vidět. Zároveň by na obsluhu konfigurace měla být aplikovatelná jednotná správa a napojení na systém zálohování konfigurace. Při posouzení vhodnosti by mělo být brána v patrnost i chlazení (směr proudění vzduchu), vzhledem k ostatní infrastruktuře v serverovně. Navrhuji aby hlavní komunikační páteř mezi switchi byla realizována 10 Gb/s linkou.

5.4.3 Realizace

Na základě specifikací a logické topologie navrhuji aby se do rozvaděče 3 umístily nové routery a switche. Na základě výše zmíněných požadavků jsem zvolil tyto nové zařízení:

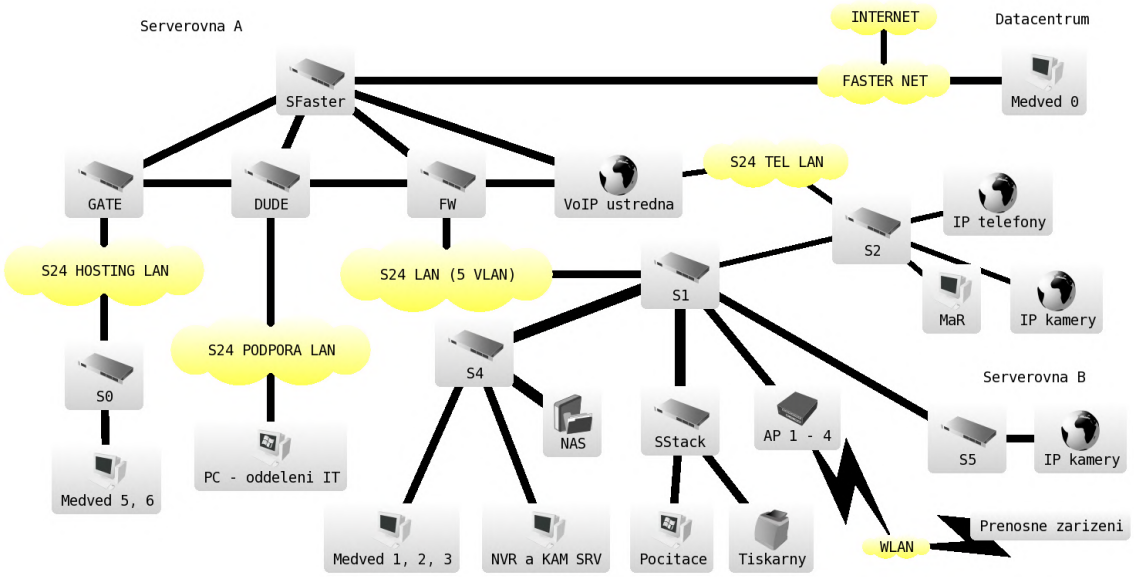
- **1 x Router MikroTik RB1100AHx4 Dude Edition (DUDE)** - tento router bude sloužit k monitoringu infrastruktury a bude popsán níže v kapitole monitoringu infrastruktury vizte 5.6.
- **1 x Router MikroTik CCR-1036 (FW)** - následující zařízení bylo zvoleno nejen díky tomu že splňuje požadavky, ale i na základě toho, že byl tento nepoužívaný router umístěn ve skladu společnosti. Dodatečné pořizovací náklady na tento router jsou tedy nulové.
- **1 x Switch MikroTik CRS328 (S1)** - je dvaceti čtyř portovým PoE switchem, který disponuje čtyřmi porty SFP+ (přenosová rychlost až 10 Gb/s). Pořizovací cena tohoto switche je dle nabídky 7385 Kč bez DPH.
- **2 x Switch MikroTik CRS 326 (S0 a S4)** - tento switch je dvaceti čtyř portový a nabízí dva porty SFP+ (přenosová rychlost až 10 Gb/s). Nabídková cena prvku je 3799 Kč bez DPH za kus.
- **3 x Propojovací kabel MikroTik S+DA0003** - 3 metry dlouhý propojovací SFP+ kabel (přenosová rychlost až 10 Gb/s). Nabídková cena kabelu je 693 Kč bez DPH za kus.

Další síťové prvky nebude nutné kupovat a využijí se již vlastněné zařízení. Na již použitých síťových prvcích bude upravena konfigurace dle návrhu.

Výsledná topologie, která vychází z návrhu logické topologie sítě je znázorněna na obrázku 5.19.

S24 LAN Hlavní privátní sítí bude S24 LAN, hlavním routerem této lokální sítě bude router MikroTik CCR-1036 (FW). Router bude propojen metalicky se switchem poskytovatele připojení SFaster. Hlavní router FW bude plnit funkci firewallu i VPN koncentrátoru. Na routeru bude nakonfigurován SSTP VPN server pro připojení sídla společnosti a případně i dalších lokalit společnosti. Router FW bude provádět překlad portů z veřejných IPv4 adres na adresy a porty lokálních firemních serverů. Na routeru FW bude používána technologie cApsMan pro hromadnou správu přístupových bodů značky MikroTik a veškerá komunikace bude terminována z přenosných zařízení až v samotném hlavním routeru FW (bez lokálního předávání).

Router FW bude taktéž routovat síťový provoz z VLAN a poskytovat pro všechny jednotlivé VLANy služby DHCP a DNS serveru. Hostovská VLAN 2 bude mít přístup



Obrázek 5.19: Návrh topologie síťové infrastruktury serverovny

pouze do Internetu a bude používána pouze interně v routeru FW pro potřeby routování přenosů z hostovské sítě.

Do nového switche S1 bude z routeru FW posílána netagovaná VLAN 1, tagovaná VLAN 4, 5 a 6. Konkrétní konfigurace VLAN pro switch S1 je znázorněna na obrázku 5.20. Do switche S1 budou do netagovaných VLAN 6 portů připojeny metalicky PoE napájené centrálně spravované WiFi přístupové body, jež budou komunikovat pouze s routerem FW a všechna komunikace bude řízena přes tento router.

```
[podpora@6NP S1] > interface vlan print
Flags: X - disabled, R - running
 #    NAME                                MTU ARP             VLAN-ID INTERFACE
 0 R ;;; Privatni LAN - PC, tiskarny, priv WiFi
     vlan1                              1500 enabled                1 bridge1
 1 R ;;; Privatni serverova LAN
     vlan4                              1500 enabled                4 bridge1
 2 R ;;; System mereni a regulace i kamery
     vlan5                              1500 enabled                5 bridge1
 3 R ;;; Spravcovska LAN
     vlan6                              1500 enabled                6 bridge1
```

Obrázek 5.20: Konkrétní konfigurace VLAN pro switch S1

Uživatelské počítače a tiskárny budou připojeny do původního stohovatelného switche NETGEAR (SStack). Switch SStack bude opticky spojen 10 Gb/s se switchem S1. Linka bude obsahovat netagovanou VLAN 1 a tagovanou VLAN 6 pro správu switche.

Interní systém měření a regulace včetně PoE napájených IP kamer bude připojeno přímo do CISCO switche (S2), jenž byl původně umístěn v serverovně B. Switch S2 bude interně rozdělen pomocí lokálních VLAN na 3 separátní logické switche po 16, 32 a 6 portech. Switch S2 bude spravován přes propoj s netagovanou VLAN 6 do interního switche se 6 porty. Skupina 32 portů bude vyhrazena pro připojení systému měření a regulace i PoE napájených IP kamer. Do tohoto interního switche bude metalicky připojena i netagovaná

linka s VLAN 5 ze switche S1. Využití poslední skupiny s 16 PoE napájenými porty bude popsáno níže v odstavci S24 TEL LAN.

Opticky 10 Gb/s linkou s netagovanou VLAN 5 bude spojen nový serverový switch S4 se switchem S1. Do switche S4 budou připojeny všechny všechny fyzické servery (Medved 1, 2, 3), NVR, kamerový server a síťové úložiště. Krom síťového úložiště, které bude spojeno opticky 10 Gb/s linkou budou všechny linky ze serverů do switche S2 realizovány metalicky s rychlostí 1 Gb/s.

Do serverovny B bude umístěn Router MikroTik 2011 (S5), který bude používán pouze jako switch. Tento switch S5 bude opticky propojen se switchem S1. Linka bude obsahovat netagovanou VLAN 5 a tagovanou VLAN 6 pro správu. Všechny fyzické porty na tomto zařízení budou switchovány a propagovat netagovanou VLAN 5. Do portů budou připojeny PoE injektorem napájené IP kamery.

Připojení sídla k provozovně a síti S24 LAN doporučuji realizovat pomocí SSTP VPN a nad ní vytvořit EoIP tunel. Realizace konfigurace EoIP tunelu je znázorněna na obrázku 5.21. Tento EoIP tunel je termínován do VLAN 1. Díky tomuto spoji je možné adresovat sídlo společnosti hlavním routerem FW s DHCP serverem a dokonce přes vrstvu L2 zobrazovat síťové tiskárny. Nebude tak nutné použít ani DHCP relay.

```
[tomas@S24 FW] > interface eoip print
Flags: X - disabled, R - running
 0  R name="eoip-tunnel-mezirka" mtu=1500 actual-mtu=1500 l2mtu=65535
      mac-address=02:60:AC:01:70:0F arp=enabled arp-timeout=auto
      loop-protect=default loop-protect-status=off
      loop-protect-send-interval=5s loop-protect-disable-time=5m
      local-address=0.0.0.0 remote-address=192.168.160.30 tunnel-id=0
      keepalive=10s,10 dscp=inherit clamp-tcp-mss=yes dont-fragment=no
      allow-fast-path=yes
```

Obrázek 5.21: Realizace konfigurace EoIP tunelu mezi sídlem a provozovnou

S24 TEL LAN Pro telefony a telefonní ústřednu bude vytvořena samostatná lokální síť. Samotná telefonní ústředna bude WAN portem připojena přímo do switche poskytovatele připojení k Internetu SStack do DMZ a bude mít přidělenu veřejnou IPv4 adresu. Telefonní ústředny bude nakonfigurován, aby propagovala na výstupu LAN portu přes DHCP server síť S24 TEL LAN a své služby. Port LAN bude připojen do switche S2 do interního podswitche se skupinou 16 portů. Do těchto portů budou přímo připojeny IP telefony, které budou využívat PoE k napájení.

S24 HOSTING LAN Původní router GATE bude sloužit jako firewall s překladem portů, DHCP a DNS server pro lokální síť S24 HOSTING LAN. Router bude připojen metalicky přímo do switche SFaster poskytovatele připojení k Internetu. Za router GATE bude připojen nový switch S0, do kterého budou připojeny síťové karty klientských hostovaných serverů Medved 5 i 6.

S24 PODPORA LAN Další a poslední separátní část infrastruktury bude tvořit síť S24 PODPORA LAN. Tato síť bude sloužit pro interní pracovníky oddělení IT k neomezenému přístupu ke správě nejen vlastních aktivních prvků sítě. Hlavním routerem sítě bude MikroTik RB1100AHx4 Dude Edition (DUDE). Tento router bude propojen do všech ostatních lokálních sítí jako klient a taktéž přímo do swithce SFaster. Router bude mít k dispozici ve-

řejnou statickou IPv4 adresu. Router bude sloužit kromě monitoringu i jako firewall a VPN koncentrátor. IT podpora bude používat SSTP VPN pro vzdálené připojení a správu infrastruktury. Lokální stolní počítače IT oddělení budou přímo připojeny do routeru DUDE bez potřeby dalšího switche.

Nastavení konkrétních DNS záznamů pro služby Microsoft 365 Pro automatickou konfiguraci služeb a doručování e-mailů je nutné přidat veřejné DNS záznamy. Konkrétně pro správnou funkčnost doručování e-mailů do Exchange Online je nutné nastavit záznam tyto záznamy:

- @ 3600 IN MX 20 spolecnost24-cz02e.mail.protection.outlook.com.
- @ 3600 IN TXT "v=spf1 include:spf.protection.outlook.com -all"
- autodiscover 3600 IN CNAME autodiscover.outlook.com.

Záznamu MX Microsoft doporučuje nastavit prioritu 0, což však v případě mého scénáře není možné, protože pošta bude primárně doručována na lokální poštovní server Kerio a z něj bude pošta předávána na servery Microsoftu. Z toho důvodu jsem u lokálního mail serveru zvolil prioritu 10 a pro cloudový e-mailový server Exchange Online prioritu 20.

Ke správné funkčnosti komunikace kolaboračního serveru Microsoft Teams je nutné nastavit následující DNS záznamy:

- sip 3600 IN CNAME sipdir.online.lync.com.
- lyncdiscover 3600 IN CNAME webdir.online.lync.com.
- _sip._tls.spolecnost-24.cz. 3600 IN SRV 100 1 443 sipdir.online.lync.com.
- _sipfederationtls._tcp.spolecnost-24.cz. 3600 IN SRV 100 1 5061 sipfed.online.lync.com.

Poslední dva DNS záznamy slouží ke vzdálené správě a přidávaní zařízení pod správu v prostředí Microsoft 365 a jsou to následující:

- enterpriseregistration 3600 IN CNAME enterpriseregistration.windows.net.
- enterpriseenrollment 3600 IN CNAME enterpriseenrollment.manage.microsoft.com.

Poslední neméně důležitou částí realizace optimalizace sítě je umístění prvků do rozvaděčů a jejich připojení. V neposlední řadě propoj označit štítky stejnou metodikou jako všechny ostatní hlavní síťové technologické spoje. Navrhuji aby byly všechny propoje jež spojují významné síťové prvky označeny. Označení by mělo obsahovat označení názvu zařízení a portu z a do něhož je propoj veden. Navrhované fyzické umístění prvků je znázorněno v příloze B.

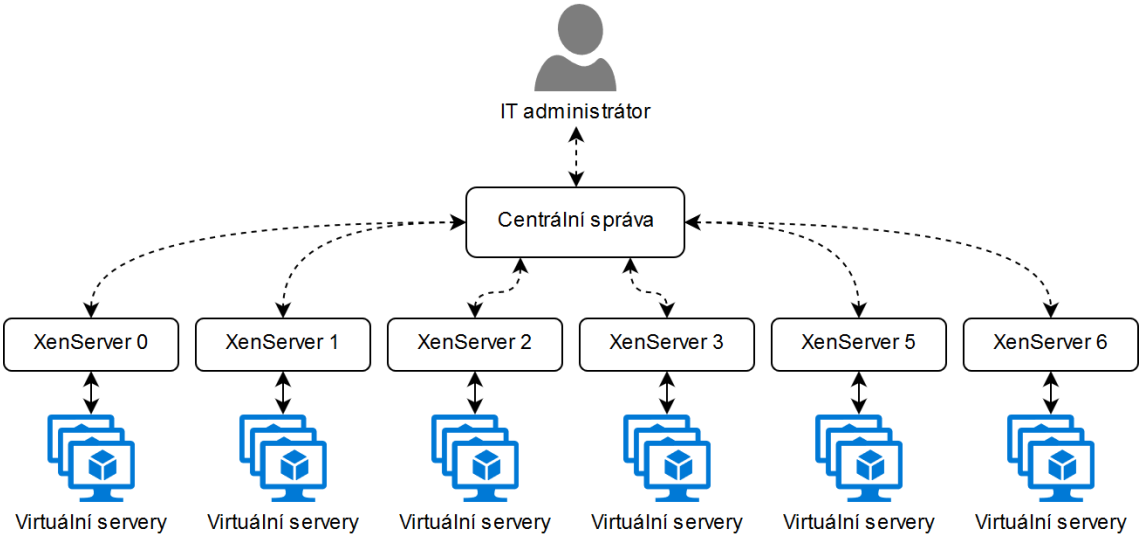
5.5 Management

5.5.1 Návrh a specifikace požadavků

Na základě analýzy bylo zjištěno, že lokální oddělení IT nemá přímý přístup ke správě hypervizorů fyzických serverů, které jsou provozovány na virtualizační technologii QEMU

KVM a spravováno externí společnosti. V rámci optimalizace navrhuji tento pro společnost nepříznivý stav změnit a provést výměnu virtualizační technologie za takovou, která bude umožňovat jednoduchou a intuitivní správu hypervizorů a virtuálních serverů interním oddělením IT.

Navrhuji aby byl na fyzické servery nainstalován XenServer případně jiné Xen řešení, které je dostupné zdarma. Dále navrhuji aby bylo možné systém ovládat pomocí webového uživatelského rozhraní. Požadavkem je aby nebylo nutné ovládat každý server jednotlivě, ale přes centrální správu jako je zobrazeno na obrázku 5.22.



Obrázek 5.22: Návrh centrální správy hypervizorů XenServer

Navrhuji také, aby byl v maximální možné míře využíván při fyzické správě serverů již přítomný panel KVM, namísto separátního monitoru, klávesnice a myši.

5.5.2 Realizace

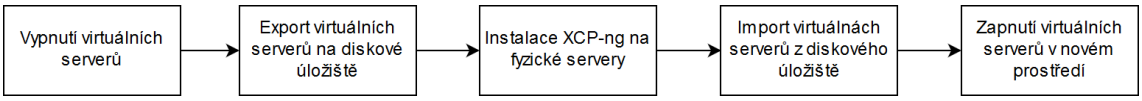
Realizace bude spočívat ve změně virtualizační technologie, nebude se zabývat parametry jednotlivých serverů, ty budou při řešení považovány jako fakt. Na fyzické servery, jež budou hostovat virtuální servery bude na základě návrhu a specifikace nainstalován hypervizor zdarma s otevřeným zdrojovým kódem XCP-ng v poslední verzi. Hypervizor XCP-ng jsem vybral z toho důvodu, že oddělení IT již má zkušenost se správou tohoto paravirtualizačního řešení i stejným typem hypervizoru u jiných klientů.

Hypervizor XCP-ng je založen na XenServeru[10] a je výsledkem masivní spolupráce mezi jednotlivci a firmami, kterým se podařilo vytvořit produkt, který nemá licenční omezení. XCP-ng tak nemá žádné omezení týkající se funkcí a každý jednotlivý bit zdrojového kódu je dostupný na portálu GitHub[11]. Hypervizory, na kterých je nainstalován XCP-ng se dají spravovat buď přímo na serveru přes textové uživatelské rozhraní, dále vzdáleně pomocí grafického rozhraní Xen Center a nebo přes grafické webové uživatelské rozhraní Xen Orchestra. Právě webové rozhraní Xen Orchestra bude součástí realizace [25].

[10] Citrix XenServer je komerční platformou pro virtualizaci serverů a operačních systémů. Umožňuje provoz většího množství operačních systémů na jednom fyzickém hardwaru [14].

[11] GitHub je webová služba od společnosti Microsoft, která podporuje vývoj softwaru za pomoci verzovacího nástroje Git. Portál GitHub nabízí bezplatný hosting nejen pro zdrojové kódy open source projektů.

Proces migrace hypervizoru a virtuálních serverů Změna virtualizační technologie bude realizována dle znázorněného procesu migrace na obrázku 5.23. Migrace se nebude provádět automaticky ale ručně. Nejdříve budou všechny virtuální servery korektně vypnuty. Následně bude proveden export virtuálních serverů do formátu XVA na diskové úložiště. Po úspěšném exportu na diskové úložiště bude na fyzické servery nainstalován virtualizační software XCP-ng v poslední verzi. Jakmile bude operační systém nainstalován a provedena počáteční nastavení budou do serverů naimportovány virtuální servery z diskového úložiště. Nakonec bude provedeno zapnutí virtuálních serverů a ověření funkčnosti.



Obrázek 5.23: Proces migrace virtuálních serverů na nové řešení virtualizace

Centrální webová správa hypervizorů Pro efektivnější správu hypervizorů a virtuálních strojů v nich jsem zvolil open source řešení zdarma Xen Orchestra. Toto webové uživatelské rozhraní umožňuje centrální správu skupin hypervizorů, jednotlivých hypervizorů i virtuálních strojů z jakéhokoliv zařízení v síti. Součástí jsou všechny potřebné funkce pro efektivní správu virtualizačního řešení, od vytvoření virtuálních strojů, jejich úpravu až po metriky a statistiky. Xen Orchestra umožňuje také vytvářet automatizované úlohy pro rychlé zálohování a krizovou obnovu poškozeného virtuálního stroje. Mezi podporované zálohovací metody patří:

- Plné zálohy - jsou nejnáročnější na diskový prostor, ale zato umožňují velmi jednoduchou obnovu. Výsledný soubor se zálohou obsahuje všechny disky virtuálního stroje a potřebné informace. Plné zálohy využívají nativní možnosti exportu virtuálního stroje z XCP-ng do formátu XVA.

- Přepisující snímky (snapshoty) - tato funkce je podobná zálohám, ale vytváří pouze snímky disku podle plánovače a zároveň odmazává starší snímky podle retenční politiky. Tato funkce přináší nejrychlejší obnovu do konzistentního stavu po havárii virtuálního stroje. Nevýhodou je však to, že snímky jsou uloženy na stejném disku nebo úložišti jako zálohovaný virtuální stroj a díky tomu nelze toto řešení považovat za regulérní metodu zálohování, protože při selhání fyzického disku, kde je virtuální stroj uložen tak ztrácíme i snímky.

- **Nepřetržité rozdílové zálohy** - umožňují exportovat pouze rozdíly mezi aktuálním stavem disků virtuálního stroje a stavu dat v předchozím snímku. Nazývají se nepřetržité z toho důvodu, že se nikdy neexportuje další plná záloha po provedení první plné zálohy. Po vytvoření určitého limitního množství rozdílových snímků se nejstarší rozdílový snímek sloučí s původní plnou zálohou a vznikne místo pro nový rozdílový snímek. Tato technologie zálohování kombinuje flexibilitu snímkových záloh a sílu plných záloh, protože rozdílové snímky jsou uloženy na jiném fyzickém disku než je uložen virtuální stroj, rozdílové zálohy jsou malé, rychle se vytvářejí a jsou relativně snadno obnovitelné.

- **Zotavení po havárii** - zahrnuje všechny dostupné způsoby obnovy po ztrátě hypervizoru, nebo skupiny úložišť, na kterém byly uložen virtuální stroje. Z důvodu, aby

se dal obnovit funkční stav infrastruktury s virtuálními servery v relativně krátkém čase a zamezilo se dlouhým časům importního procesu byla implementována funkce streamování. Tato funkce spočívá v tom, že umožňuje v reálném čase exportovat a importovat virtuální stroje. Hlavním cílem zotavení po havárii je mít startu schopné stroje připravené na funkčním hypervizoru obnovené ze záloh. Díky technologii streamování není nutné mít pro obnovu virtuálních strojů dodatečné diskové úložiště a exportování i importování se zkrátilo na polovinu původního času bez streamování.

- **Nepřetržitá replikace** - tato funkce nepřetržité replikace virtuálních strojů není závislá na konkrétních výrobcích hypervizorů, na kterých je XCP-ng nainstalován. Replikovat můžeme virtuální stroj každých `X` minut nebo hodin do jakéhokoliv úložiště. Může to být vzdálený hypervizor XCP-ng nebo jednoduše jakékoliv lokální úložiště. Tato funkce zahrnuje nezávislost na výrobci úložiště nebo fyzického stroje, na kterém je nainstalován hypervizor XCP-ng, žádnou dodatečnou konfiguraci či nutnost aby byl přítomný agent, rychlou obnovu zotavení od 10 minut do 24 hodin a více, flexibilitu. Pro nepřetržitou replikaci není nutné mít žádnou mezipaměť, zároveň je zajištěna atomičnost replikace, což znamená, že transakce (replikace) je buď provedena celá nebo žádná z operací, která replikaci tvoří. Tato metoda je velmi efektivním zotavením po havárii. V případě, že infrastruktura ztratila celý pool[12] tak můžeme začít kopírovat virtuální stroje do jiného poolu či jednoho konkrétního hypervizoru s velmi nedávnými daty.

- **Obnovení na úrovni souborů** - díky této metodě můžeme obnovit určité soubory a adresáře uvnitř virtuálního stroje. Můžeme jej použít se všemi existujícími rozdílovými zálohami. Aktuální technologickou nevýhodou tohoto typu obnovy je to, že nelze obnovit soubory ze vzdálených úložišť a použít pro obnovu lze pouze rozdílové zálohy.

Xen Orchestra je možné jednoduše používat na všech zařízeních, které podporují moderní webové technologie HTML[13], JS[14] a CSS[15], což může být například mobilní telefon, tablet nebo stolní počítač [26].

Na základě shrnutí podporovaných zálohovacích metod navrhuji používat nepřetržité rozdílové zálohy a ukládat je na server Medved 0 do datacentra Faster.

Instalace centrální správy Xen Orchestra Ve společnosti bude nasazeno webové řešení pro centrální správu hypervizorů a to konkrétně Xen Orchestra v komunitním sestavení. Nejprve je nutné připravit linuxový virtuální stroj s operačním systémem Debian. Xen Orchestra vyžaduje minimálně 2 GB operační paměti a 1 jádro procesoru, 10 GB volného místa na disku a síťovou kartu. Po instalaci operačního systému stačí spustit následující příkaz pro instalaci:

- sudo curl https://raw.githubusercontent.com/Jarli01/xenorchestra_installer/master/xo_install.sh | bash

Pro aktualizaci Xen Orchestra na nejnovější verzi je možné použít následující příkaz:

[12] Seskupení fyzických hypervizorů do jednoho kompaktního funkčního celku [26].

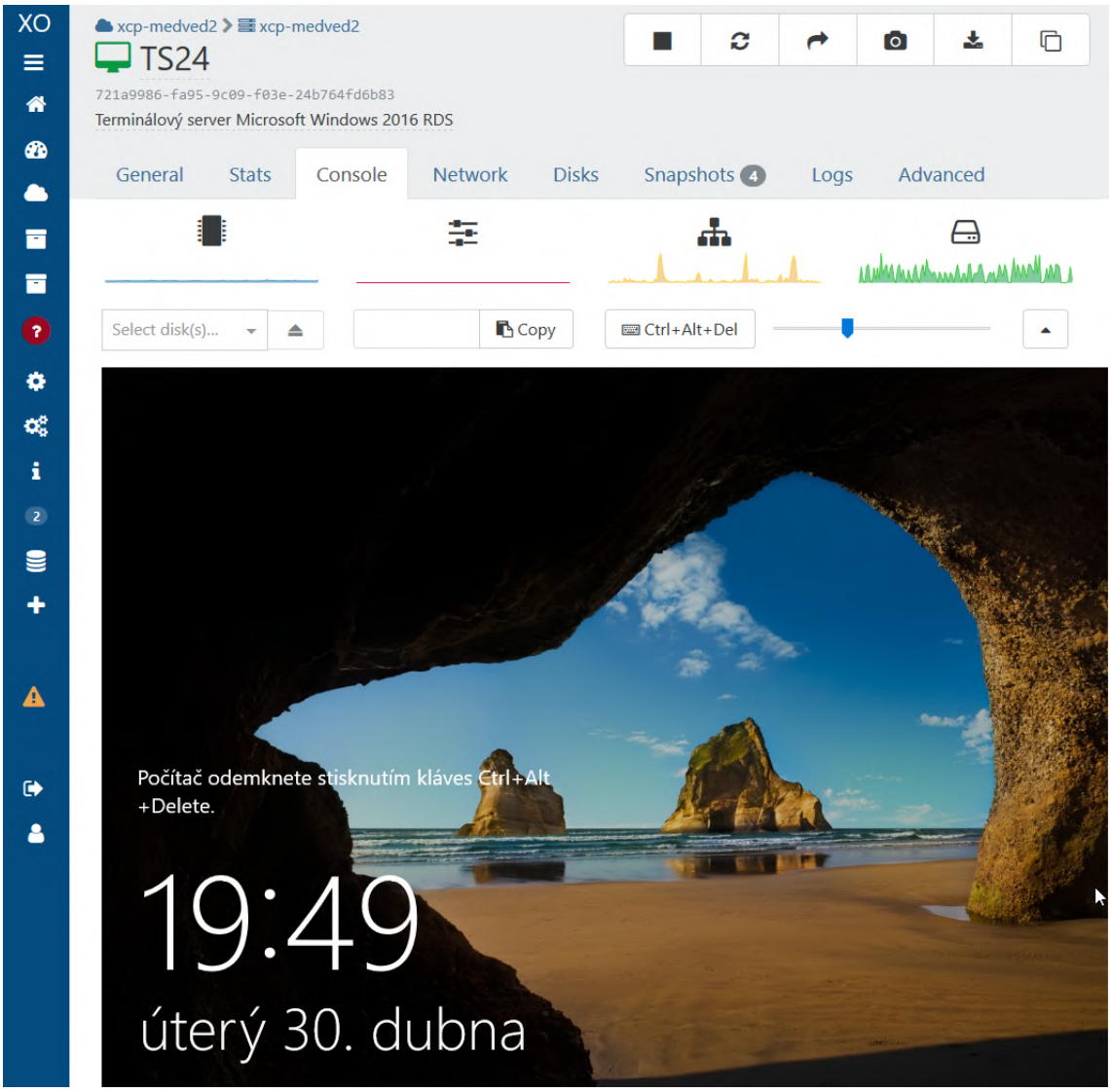
[13] HyperText Markup Language je značkovacím programovacím jazykem https://www.w3.org/standards/webdesign/htmlcss

[14] JavaScript je objektově orientovaný skriptovací jazyk https://www.javascript.com/

[15] Cascading Style Sheets slouží k definování způsobu zobrazení elementů na stránce https://www.w3.org/standards/webdesign/htmlcss

- sudo curl https://raw.githubusercontent.com/Jarli01/xenorchestra_updater/master/xo-update.sh | bash

Výše zmíněné příkazy[16] za nás automaticky přeloží zdrojové kódy, zkompiluje a nainstaluje, případně aktualizuje všechny potřebné součásti. Na obrázku 5.24 je vidět snímek obrazovky pořízený z nástroje centrální správy Xen Orchestra v komunitní verzi.



Obrázek 5.24: Snímek obrazovky z řešení centrální správy hypervizorů Xen Orchestra v komunitní verzi

Fyzická správa serverů V rámci zkvalitnění obsluhy fyzických serverů a jejich případné lokální diagnostiky budou dále servery Medved 5 a 6 připojeny k ostatním serverům na panel KVM. Připojením na panel KVM bude možné z rozvaděče odstranit již nepotřebný monitor.

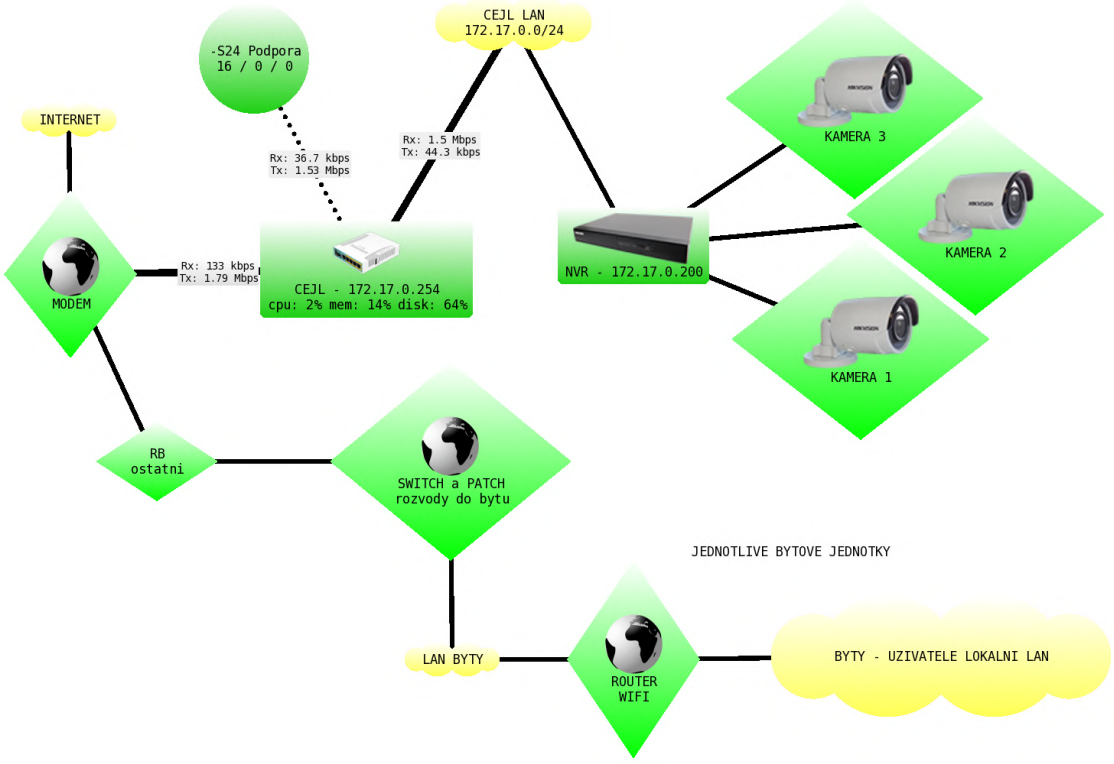
[16] Příkazy pro aktualizaci a instalaci Xen Orchestra byly získány z adresy: https://github.com/Jarli01/.

5.6 Monitoring sítě

Cílem nasazení monitoringu a centrální správy síťové technologie je také udržení aktuálních verzí a bezpečnostních aktualizací operačních systému routerů a switchů. Vedení společnosti si také přeje minimalizovat počet výpadku síťové infrastruktury na minimum a toho můžeme dosáhnout například použitím monitorovacího systému.

V mé diplomové práci se budu věnovat klient/server technologii The Dude od společnosti MikroTik. The Dude je nový síťový monitorovací nástroj, který umožňuje dramaticky zefektivnit správu síťových zařízení. Umožňuje automaticky skenovat všechny zařízení ve specifikovaném subnetu, nakreslit a rozvrhnout strukturu počítačové sítě. Dále umožňuje monitorovat jednotlivé služby na zařízeních a oznamovat jejich výpadek. Na jednotlivé výpadky lze reagovat zasláním upozornění anebo automatickým spuštěním vlastního příkazu. Na obrázku 5.25 je možné vidět, jak se dá rozvrhnout dokumentace sítě.

Technologii The Dude jsem vybral, protože je distribuován s routerboard od MikroTiku zdarma a také díky jeho téměř neomezeným možnostem programování vlastních sond například přes protokoly: SNMP, ICMP, SSH, telnet a další.

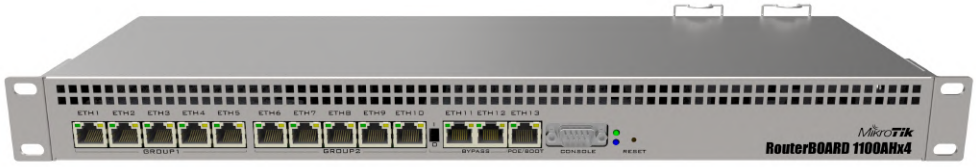


Obrázek 5.25: Ukázka ze systému The Dude

5.6.1 Specifikace požadavků

Pro nasazení technologie The Dude je více než vhodné, aby prostředí, ve kterém chceme nasadit tuto technologii bylo vytvořeno převážně z produktů značky MikroTik. Což společnost splňuje. Spravovat se dají také zařízení, které podporují technologii SNMP. Technologii SNMP podporují všechny aktivní prvky ve firmě. Samotný běh serverové části aplikace je

nyní vyžadován podporovaný hardware, přičemž aplikace je dodávána zdarma. Společností MikroTik je doporučen router RB1100AHx4 Dude Edition vizte obrázek 5.26.



Obrázek 5.26: Router RB1100AHx4 Dude Edition [12]

Tento router je aktuálně nejvýkonnější gigabytový routerboard s podporou The Dude v rack verzi osazený 13 x RJ45 10 / 100 / 1000 Mbps. Procesor se čtyřmi jádry na frekvenci 1400 MHz dokáže zpracovat až 5,5 milionů packetů za sekundu. Disponuje integrovaným 64 GB SSD diskem a redundantním zdrojem. Kromě dvojího napájení má ještě DC vstup a podporuje jak pasivní, tak i aktivní PoE napájení ve standardu 802.3at. Router disponuje také slotem pro microSD kartu. Pro nasazení serveru The Dude jsem navrhl právě tento router [12].

5.6.2 Realizace

Postup instalace v reálném prostředí Instalační proces instalace serverové části monitorovacího systému The Dude obnáší stažení `NPK` serverového balíku aplikace The Dude z webových stránek společnosti MikroTik `http://www.mikrotik.com/download`. Důležité je vybrat verzi odpovídající architektuře routeru. V případě routeru RB1100AHx4 Dude Edition je to architektura ARM. Po stažení je nutné nahrát balíček `.npk` do RouterOS a rebootovat router.

Příkaz pro zapnutí The Dude serveru:

```
/dude set enabled=(yes/no)
```

K ověření zda server běží slouží příkaz:

```
[admin@MikroTik] > /dude print
enabled: yes
data-directory: dude
status: running
```

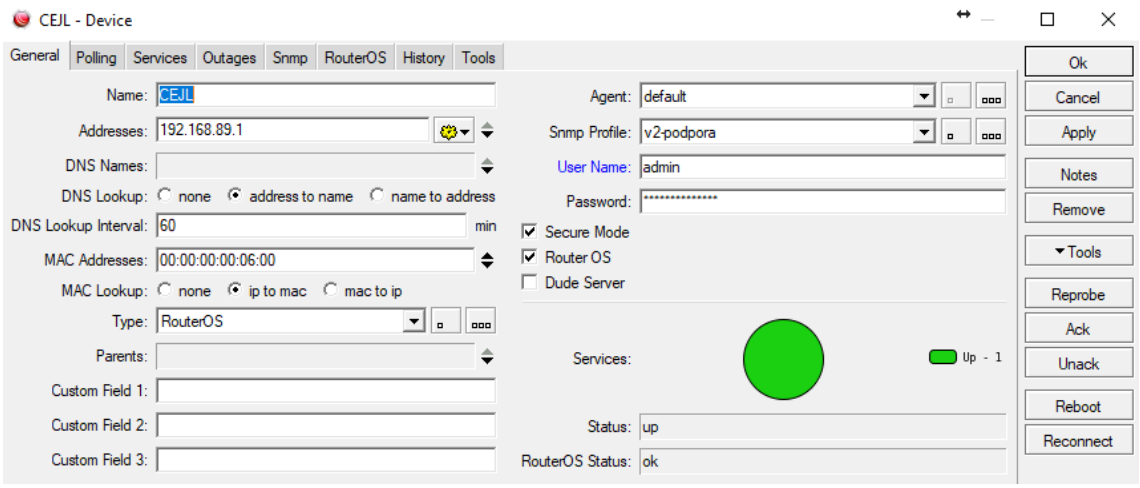
Ve výchozím nastavení se nainstaluje The Dude na systémový disk, což není v našem případě vůbec vhodné, protože máme k dispozici 64GB SSD disk (systémové paměti nevyhovuje velký počet zápisů). Proto přesměrujeme datovou část na SSD disk, konkrétně disk2.

```
/dude set data-directory=disk2/dude
```

Nyní máme nainstalovánu serverovou část a můžeme začít s instalací klientské části do operačního systému Windows 10. Instalační software klientské části je ke stažení taktéž volně ze stránek společnosti MikroTik. Klienta nainstalujeme pomocí průvodce instalace. Zástupce aplikace bude přidán do nabídky start.

Po spuštění klienta musíme zadat IP adresu nebo doménové jméno routeru, na který jsme nainstalovali serverovou část. Po specifikaci IP adresy je nutné specifikovat port, výchozím portem je 8291. Dále je nutné zadat uživatelské jméno s plným přístupem do routeru a heslo, poté kliknout na tlačítko `Connect`. Po přihlášení do aplikace můžeme začít tvořit mapu počítačové sítě. Můžeme buď využít `Device Discovery` nebo manuálně přidávat zařízení. Pro přidání zařízení do mapy klikneme pravým tlačítkem do okna aplikace a zvolíme

`Add Device`, vybereme požadované monitorované služby a zadáme přihlašovací údaje a způsob komunikace SNMP. Příklad zařízení po vyplnění požadovaných údajů, specifikaci monitorovaných služeb a nastavené komunikaci přes SNMP je znázorněn na obrázku 5.27



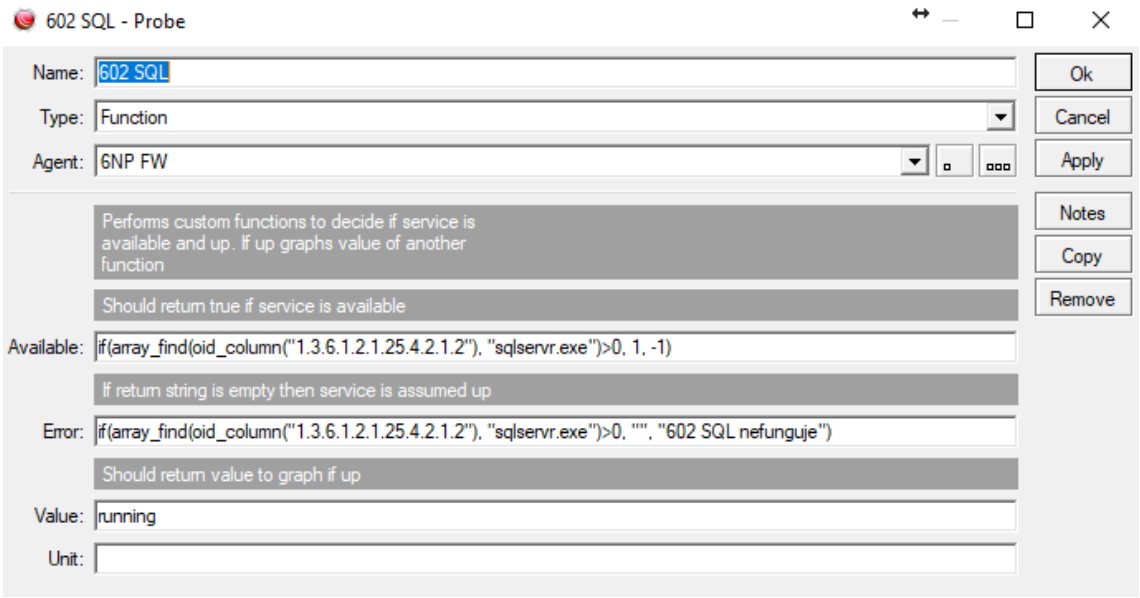
Obrázek 5.27: Ukázka zobrazení nakonfigurovaného zařízení v systému The Dude

Návrh konkrétních nastavení konkrétních parametrů SPOLEČNOST-24, s.r.o. využívá server s operačním systémem Windows Server 2012 a nad ním provozuje aplikaci FormFlow od společnost Software602, a.s. Pro potřeby monitorování této spisové služby bylo nutné na Windows server nainstalovat službu SNMP a následně v monitorovacím software The Dude vytvořit sondy pro monitoring specifických služeb FormFlow. K vytvoření této sondy jsem využil znalostí protokolu SNMP a OID. MIB soubor je možné stáhnout ze stránek výrobce monitorovaného produktu a ten následně implementovat do softwaru The Dude. Na obrázku 5.28 je možné vidět příklad sondy, kterou jsem vytvořil pro monitoring stavu databázového SQL serveru spisové služby FormFlow.

Na všech aktivních prvcích bylo nastaveno přeposílání událostí do syslogu v The Dude. Dotazování na funkčnost jednotlivých služeb jsem navrhl nastavit každých třicet sekund, kdy timeout bude nastaven na deset sekund a počet opakování při neúspěchu na pět pokusů. Při nefunkčnosti se událost zaznamená do syslogu a podle typu události odešle upozornění e-mailem.

Aspekty managementu Technologie The Dude je velice mocný nástroj, který umožňuje nastavovat každý aspekt RouterOS, proto je potřeba nastavit odpovědnost a pravomoci při používání tohoto software. Odpovědnost za nasazení technologie bude mít vedoucí interního IT oddělení. Přístup k náhledu budou mít všichni pracovníci interního IT oddělení.

Vedoucí interního IT oddělení ponese odpovědnost za sestavení implementačního týmu. Implementační tým se bude zodpovídat vedoucímu IT oddělení. Vedoucí interního IT oddělení může pověřit dílčími úkoly členy implementačního týmu, je však povinen zkontrolovat odvedenou práci členů týmu. Instalaci serveru The Dude provede sám vedoucí IT, asistovat mu budou na lokalitách mimo hlavní provozovnu ostatní členové týmu ať již lokálně v místě umístění aktivních prvků tak vzdáleně. Vedoucím IT oddělení byl přidělen časový plán dvaceti člověkodnů na počáteční implementaci monitorovacího systému The Dude. Odpovědnost za dodržení časového plánu nese vedoucí implementačního týmu.



Obrázek 5.28: Ukázka sondy monitorující stav databáze SW602 v systému The Dude

Po počáteční implementaci bude probíhat měsíční zkušební provoz, jehož cílem bude odhalit nedokonalosti systému a jednotlivých vytvořených sond pro zařízení i služby. Zkušební provoz bude prohlášen za ukončený vedoucím IT oddělení. Po úspěšném zkušebním provozu bude spuštěn ostrý provoz, který bude generovat oznámení na e-mail. Na tyto oznámení budou povinni operátoři podpory reagovat v pracovní době do třiceti minut od obdržení oznámení. Každá akce vykonaná uživatelem bude v technologii The Dude zaznamenána do protokolu událostí. Do směrnic společnosti budou muset být zakomponovány kritéria zálohování a krizových scénářů provozu technologie na monitoring sítového provozu The Dude. Bude nutné vytvořit seznam úkonů, které je nutné provést při přidání nové lokality do monitorovacího řešení. V neposlední řadě je nutné vymezit kritéria bezpečnosti provozu, protože v systému budou uloženy i hesla do jednotlivých prvků počítačové sítě. Zaměstnanec bude moci využívat monitorovací nástroj pouze pro pracovní účely.

Ekonomické aspekty Nasazení tohoto řešení obnáší nákup routeru RB1100AHx4 Dude Edition, který aktuálně stojí 6600 Kč bez DPH. Další náklady na nákup hardware nebo software nejsou. Je potřeba počítat s vyčleněním pracovní síly, protože nasazení této technologie zabere poměrně dost času v závislosti na rozsáhlosti sítě a počtu monitorovaných služeb a množství vytvářených sond. Přínosem pro firmu je jednoznačně stále aktuální dokumentace celé počítačové sítě. Velkou výhodou je také centrální správa všech aktivních prvků a jejich aktualizace. Monitoring SLA s možností vyhodnocovat statistik. Umožňuje identifikovat často poruchovou část sítě až na úroveň konkrétního aktivního prvku a služby. Neposledním přínosem je záznam všech monitorovaných událostí v síti. Dle mého názoru patří The Dude na špičku monitorovacích nástrojů a pokud společnost používá převážně routery značky MikroTik, tak v tom případě je nasazení této technologie téměř nutností. Díky tomu, že je The Dude zdarma tak je náklad na nákup hardware opodstatněn jako VPN server pro správu klientských sítí, který je nutné koupit ať již monitoring bude použit či nikoliv.

Kapitola 6

Rozšíření

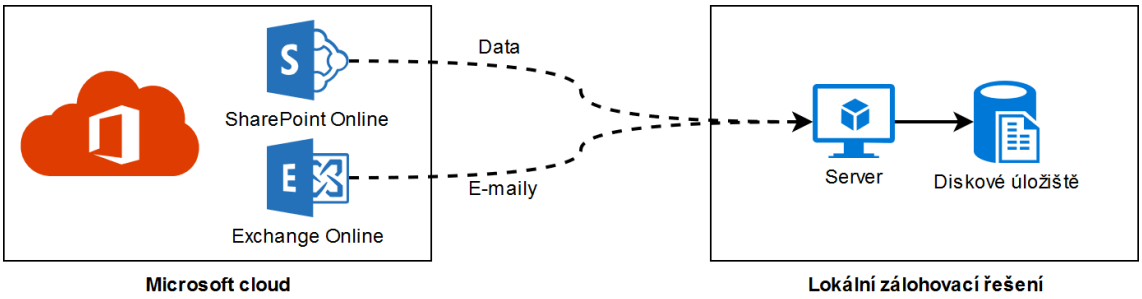
6.1 Exit strategie z Cloudu

6.1.1 Návrh a specifikace

Po úspěšném návrhu řešení všech dílčích cílů jsem se rozhodl navrhnout i strategii opuštění cloudového řešení (exit strategii). Základními aktivy podniku jsou data a e-mailová komunikace. Ty se dle předchozího návrhu v rámci konsolidace serverů v kapitole 5.3 přesunou na cloudové řešení Microsoftu.

Navrhuji, aby byla data vždy jako záloha i offline na diskovém úložišti společnosti. Navrhuji jako hlavní požadavek, aby byla všechna data (i soubory pracovních skupin) neustálé přístupná jako lokální záloha, pro případnou nedostupnost cloudové služby či jinou neočekávanou situaci. Požadavkem je, aby byla lokálně zálohovaná i veškerá e-mailová komunikace realizovaná přes navržené cloudové řešení společnosti.

Základní koncepci exit strategie zálohování e-mailů a dat z cloudu navrhuji následující. Lokální server s přístupem k Internetu bude neustále synchronizovat data ze služby SharePoint Online a ukládat je jako zálohu na lokální síťové úložiště. Podobnou koncepci navrhuji i s E-maily, kdy server bude každou hodinu periodicky vyčítat E-mailové schránky ze služby Exchange Online a ukládat e-maily do archivu na lokální diskové úložiště. Schéma základní koncepce zálohování dat z cloudu je znázorněno na obrázku 6.1.



Obrázek 6.1: Základní koncepce exit strategie z cloudu

6.1.2 Řešení

Na základě specifikace navrhuji aby pro řešení byl vytvořen virtuální server s operačním systémem Windows Server 2016 Standard. Po konsolidaci serverů bude mít společnost právě potřebnou licenci k dispozici. Na tento server navrhuji nainstalovat zdarma dostupného klienta Microsoft OneDrive, který umožňuje synchronizaci dokumentů na lokální úložiště. Lokální úložiště pro OneDrive bude přesměrováno do sdílené složky síťového diskového úložiště QNAP. Pro lokální zálohování E-mailů bude na virtuální server nainstalován komerční software MailStore[1]. Cena archivačního řešení je 12080 Kč bez DPH, která je vypočtena z ceny za uživatele pro kategorii 10-24 uživatelů, kdy cena za jednoho uživatele je 1208 Kč bez DPH. K nákupu licence je dodávána automaticky podpora a aktualizace pro následující rok. Po vypršení podpory software poběží dál, pouze nebude nárok na aktualizace. Server MailStore bude nainstalován na stejný server, který bude synchronizovat i data. Výchozí úložiště archivu bude přesměrováno taktéž do sdílené složky síťového diskového úložiště QNAP. Běžní uživatelé nebudou mít přístup k lokálnímu zálohovacímu řešení.

V klientovi Microsoft OneDrive bude v parametrech synchronizace dat nakonfigurována možnost vždy přístupné na lokálním zařízení pro všechny firemní skupiny ve službě Exchange Online. Server MailStore bude nakonfigurován, aby se periodicky každou hodinu připojoval šifrovanou komunikací k serveru Exchange Online s využitím administrátorského účtem a stahoval všechny nově příchozí i odchozí zprávy společnosti.

Virtuální server by měl disponovat 4 jádry CPU, 8 GB operační paměti RAM a 80 GB místa na pevném disku. Parametry virtuálního serveru jsou zvoleny na základě požadavků použité technologie a software. Virtuální server bude konkrétně umístěn na fyzickém serveru Medved 2. Předpokládaná pracnost implementace a otestování navrženého řešení je odhadována na 4 člověkodny práce jednoho člena interního IT oddělení a předpokládaná cena se skládá pouze s pořízení licencí archivačního systému MailStore, jenž by konkrétně činilo 12080 Kč bez DPH za celou společnost bez dalších nutných investic.

[1] Mailstore je komplexní archivační řešení pro e-mailovou komunikaci, dostupný pouze pro operační systém Microsoft Windows - https://www.mailstore.com/.

Kapitola 7

Ekonomické zhodnocení a projektová realizace

Tato kapitola je věnována ekonomickému zhodnocení a projektové realizaci řešení pro podnik SPOLEČNOST-24, s.r.o., které konkrétně řeší optimalizaci infrastruktury serverovny.

Ekonomické zhodnocení Celkové jednorázové náklady na projekt realizace optimalizace infrastruktury serverovny podniku činí 42667 Kč bez DPH. Soupis včetně cen jednotlivých komponent navrhovaných řešení je znázorněn v tabulce na obrázku 7.1.

Typ	Položka	Počet	Cena za jednotku	Celkem
Hardware	Bezdátový detektor teploty (JA-151TH)	1	595,00 Kč	595,00 Kč
Hardware	Sběrnicový přístupový modul RFID (JA-112E)	2	1 148,00 Kč	2 296,00 Kč
Hardware	Sběrnicový modul pro obsluhu elektrického zámku (JA-120N)	2	898,00 Kč	1 796,00 Kč
Hardware	Elektrický otevírač Befo DUAL 2611 MB	2	1 134,00 Kč	2 268,00 Kč
	Náklady celkem za přístupový systém a měření teploty serverovny			**6 955,00 Kč**
Hardware	PLC Siemens LOGO! 12/24RCE (6ED1052-1MD08-0BA0)	1	3 200,00 Kč	3 200,00 Kč
Hardware	Jistič OEZ LTN-2B-1	1	200,00 Kč	200,00 Kč
Hardware	Jistič OEZ LTN-16B-1	4	90,00 Kč	360,00 Kč
Hardware	Stykač OEZ RSI-25-40-A230	4	410,00 Kč	1 640,00 Kč
Hardware	Svorkovnice OEZ RSA 4	15	10,00 Kč	150,00 Kč
Hardware	PLC UniPi Neuron S103-G	1	6 500,00 Kč	6 500,00 Kč
	Náklady celkem za systém řízení napájení serverovny			**12 050,00 Kč**
	Náklady celkem za optimalizaci serverové infrastruktury			**0,00 Kč**
Hardware	Switch MikroTik CRS328	1	7 385,00 Kč	7 385,00 Kč
Hardware	Switch MikroTik CRS326	2	3 799,00 Kč	7 598,00 Kč
Hardware	Propojovací kabel Mikrotik S+DA0003	3	693,00 Kč	2 079,00 Kč
	Náklady celkem za optimalizaci síťové infrastruktury			**17 062,00 Kč**
Software	XCP-ng - Serverová virtualizační technologie	6	0,00 Kč	0,00 Kč
Software	Xen Orchestra (CE) - centrální webová správa hypervizorů	1	0,00 Kč	0,00 Kč
	Náklady celkem za optimalizaci managementu infrastruktury			**0,00 Kč**
Hardware	MikroTik RB1100AHx4 Dude Edition	1	6 600,00 Kč	6 600,00 Kč
Software	Monitorovácí software The Dude	1	0,00 Kč	0,00 Kč
	Náklady celkem za monitoring sítě			**6 600,00 Kč**
	Náklady celkem za všechny navrhované řešení			**42 667,00 Kč**

Obrázek 7.1: Celkové jednorázové náklady za navrhované řešení

Uskutečnění všech navrhovaných optimalizací si vyžádá 487 člověkohodin. Práci záměrně neohodnocuji, protože se bude vykonávat v rámci interních požadavků na správu

IT. Věnovat se navrhované problematice budou interní pracovníci IT i ve volných časech, kdy zrovna nejsou přiděleny žádné prioritněji požadavky. Pracovníci interního IT oddělení i ostatní zainteresovaní zaměstnanci (například pracovník údržby - elektrikář) jsou ohodnocováni pevnou mzdou a společnost realizace nebude stát na práci nic navíc.

1. **Přístupový systém a měření teploty serverovny** - Celková cena potřebných komponent pro realizaci přístupového systému a monitoringu teploty serverovny A je 6995 Kč bez DPH. V celkové ceně není započtena práce při montáži a konfiguraci řešení, protože bude provedena interními pracovníky IT oddělení. Očekávaná pracnost jsou 3 člověkodny[1] (24 člověkohodin[2]) interního pracovníka oddělení IT.

2. **Systém řízení napájení** - Celková cena součástek pro řešení potřebných pro realizaci automatického postupného zapínání napájení infrastruktury je 5500 Kč bez DPH. Systém řízení napájení je složen ještě z monitoringu a komunikace se záložním zdrojem, které stojí 6500 Kč bez DPH. Celkové jednorázové náklady obou podsystémů je 12050 Kč bez DPH. Realizaci provedou opět pracovníci IT společně s interním pracovníkem údržby - elektrikářem. Předpokládaná pracnost je odhadována na 44 člověkohodin. Pro systém řízení napájení byl zpracován ukázkový podrobný projektový plán změny vizte 7.3.

3. **Serverové infrastruktura** - Realizace optimalizace serverové infrastruktury nebude vyžadovat žádné jednorázové náklady. Naopak společnosti zbudou bez využití dvě licence Microsoft Windows Server 2012 Standard a jedna licence Microsoft Windows Server 2016 Standard. Přechod na cloudové řešení přinese společnosti měsíční náklad na jednoho uživatele 31,5 EUR (809,55 Kč[3]) bez DPH. Společnost bude mít celkové měsíční náklady za cloudové služby všech svých deseti zaměstnanců 8095,5 Kč, což činí 97146 Kč ročně bez DPH. Realizaci řešení provedou rovněž pracovníci interního IT oddělení. Předpokládaná pracnost je odhadována na 120 člověkohodin.

4. **Síťová infrastruktura** - Síťová optimalizace si vyžádá jednorázové náklady ve výši 17062 Kč bez DPH převážně za nákup nových síťových prvků značky MikroTik. Realizace bude provedena interními pracovníky IT oddělení a předpokládaná pracnost realizace je 56 člověkohodin.

5. **Management** - Optimalizace managementu infrastruktury nebude vyžadovat žádné jednorázové náklady a to z toho důvodu, že budou použity programy s otevřeným zdrojovým kódem, které jsou k dispozici zdarma. Realizace změny virtualizační technologie a zavedení centrální správy hypervizorů bude provedena interními pracovníky IT oddělení a předpokládaná pracnost realizace je v rozsahu 64 člověkohodin.

6. **Monitoring sítě** - Realizace monitoringu sítě si vyžádá jednorázový nákup 6600 Kč bez DPH za hlavní monitorovací router. Monitorovací software je dodávám k routeru v ceně, nepředstavuje tak žádný další jednorázový náklad. Realizaci provedou opět pracovníci interního IT oddělení. Předpokládaná pracnost realizace je 180 člověkohodin.

[1] Člověkoden znamená čas odpovídající práci jednoho pracovníka po dobu jednoho pracovního dne. Zpravidla odpovídá osmi člověkohodinám.

[2] Člověkohodina znamená čas odpovídající práci průměrného pracovníka po dobu jedné hodiny.

[3] Cena při kurzu 25,7 Kč za 1 EUR.

Z ekonomického hlediska celá optimalizace infrastruktury serverovny podniku nebude pro společnost nijak zásadně nákladná. Ovšem byl kladen důraz na kvalitu a přiměřenou cenu při jednotlivých výběrech komponent. Hlavním přínosem práce je zvýšení spolehlivosti a zefektivnění práce lokálních administrátorů.

7.1 Přínosy řešení

Zavedením optimalizace může společnost výrazně zvýšit dostupnost a to až o 33 hodin ročně. Výpočet byl proveden na základě analýzy, kdy společnost postihlo za rok jedenáct dlouhých výpadků napájení serverovny a po obnovení napájení trvalo internímu IT oddělení průměrně tři hodiny než dokázali serverovnu uvést do provozu.

Cena výpadku lze u podniku SPOLEČNOST-24, s.r.o. jen velmi těžko vyčíslit, ale pokud společnosti nepojede serverová infrastruktura tak firemní zaměstnanci nebudou vědět co mají dělat a firma nebude generovat výkon.

Řešení bude přínosné i z hlediska správy infrastruktury, jenž bude oceněno převážně interním IT oddělením. Celá správa infrastruktury se stane jednodušší, rychlejší a přehlednější oproti původnímu stavu.

Budoucí vývoj může spočívat v zavedení řešení, jakým způsobem mít data lokálně zálohována pro nenadálé situace. Řešení pro lokální zálohování dat a e-mailové komunikace jsem navrhl v kapitole 6.1 (Rozšíření), konkrétně v podobě exit strategie z cloudu. V případě, že by se podnik rozhodl tuto exit strategii použít, tak by se zvýšily jednorázové náklady o 12080 Kč bez DPH za licence archivačního řešení. Celkové náklady za navrhované řešení rozšíření exit strategie z cloudu jsou znázorněny v tabulce na obrázku 7.2. Realizaci navrženého řešení by stejně tak jako u ostatních realizací činili pracovníci IT oddělení a předpokládaný rozsah prací by byl 32 člověkohodin.

Typ	Položka	Počet	Cena za jednotku	Celkem
Software	Archivační řešení MailStore - licence za uživatele	10	1 208,00 Kč	12 080,00 Kč
Software	Synchronizační klient Microsoft OneDrive	1	0,00 Kč	0,00 Kč
	Náklady celkem za exit strategii z cloudu			**12 080,00 Kč**

Obrázek 7.2: Celkové náklady za navrhované rozšíření exit strategie z cloudu

7.2 Projekt realizace

Projekt realizace navržených optimalizací bude řízen jako změnový projekt. Všechny navržené technologie jsou k mání. Navržené řešení jsou proveditelná jak technicky, technologicky, tak i finančně.

- **Síly inicializující proces změny** - Opakované výpadky elektrického proudu, nedostatečné zabezpečení serverovny, složitá správa lokální infrastruktury a neexistence monitoringu sítě, to jsou základní síly působící pro změnu. Tyto důvody vedly vedení společnosti k rozhodnutí, že je potřeba tyto problémy řešit. Proti zavedení změny působí mírné omezení provozu serverovny během realizace a neochota zaměstnanců učit se nové postupy.
- **Nositel změny** - U nositele změny se dá předpokládat, že rozumí potřebám a procesům společnosti. Nositelem změny v tomto procesu bude takzvaný product owner

neboli agent změny, kterým bude vedoucí interního oddělení IT, jenž je schopen nadefinovat dílčí cíle změny. Agent změny bude podporován přímo jednatelem společnosti a bude koordinovat přidělování lidských zdrojů při procesu provádění změny. Změny při realizaci řešení sebou nesou odstávku provozu jednotlivých komponent, je proto nutné zajistit součinnost s uživateli.

- **Intervenční oblasti** - Samotná realizace projektu změny není primitivní záležitostí a je potřeba, aby jí byla věnována dostatečná pozornost. To hlavně z toho důvodu, že každý pracovník společnosti pracuje s nějakou částí infrastruktury, která bude projektem zasažena. Změny se dotknou převážně interního oddělení IT a jeho chodu. Před zavedením bude nutká koordinace s vedením společnosti, které bude na projekt dohlížet. Při zavádění změn bude vytížen převážně vedoucí IT oddělení, který dohlíží a provádí realizaci. IT oddělení bude muset dohlédnout na správné zaškolení obsluhy. Změna se projeví také v chodu společnosti, při jejím zavádění, jelikož bude muset být minimálně omezen provoz v době instalace.

- **Realizace změny** - K realizaci bude vytvořen samostatný projekt, ve kterém budou pomocí WBS[4] rozloženy úkoly na podúkoly (podprojekty). Vedoucím projektu bude projektový manažer, konkrétně vedoucí interního IT oddělení. Projektový manažer na základě podúkolů vytvoří harmonogram změn, ve kterém bude zřejmá priorita (pořadí) jednotlivých úkolů. Po dokončení všech úkolů bude nutné výsledné řešení důkladně otestovat. Na základě řádného otestování bude sestavena dokumentace, která bude ověřena vedoucím IT oddělení a dalšími spolupracovníky, jež se podíleli na procesu změny a jsou schopni nalézt případné neshody dokumentace s reálným stavem. Případné nesrovnalosti by měly být v konečné verzi dokumentace napraveny.

Časový plán začíná v květnu a to realizací přístupového systému a měření teploty serverovny, dále systémem řízení napájení. Plán je dodržován, část prací je v době odevzdání diplomové práce již hotova. Tato diplomová práce bude sloužit podniku SPOLEČNOST-24, s.r.o. jako dokumentace k navrženým optimalizacím a bude tyto optimalizace v průběhu roku 2019 postupně v daném pořadí po etapách realizovat.

7.3 Plán projektu optimalizace řízení napájení

7.3.1 Analýza rizik projektu

Tento projekt stejně tak jako jakýkoliv jiný obsahuje řadu rizik, které jej mohou ovlivnit ať již pozitivním tak negativním směrem. Tyto rizika je však vhodné dobře analyzovat a mít je pod kontrolou, nejhorším stavem je jejich neznalost. Nikdy ovšem nemůžeme snížit pravděpodobnost rizika na nulu.

Identifikace rizik Pro analyzovaný projekt změny bylo nalezeno těchto sedm rizik:

1. **Nedostatečná kapacita přívodního jističe** - Toto riziko má velký vliv na úspěch celého řešení. Pokud nebude dostatečně vhodná charakteristika jističe na přívodu elektrické energie do serverovny, tak může celé řešení zkrachovat, protože bude selhávat jistič nikoliv v serverovně podniku, ale přímo před přívodem.

[4] Work Breakdown Structure (WBS).

2. **Neočekávané fyzické rozměry řešení** - Rizikem může být, že by se nové řešení ovládání s PLC nevlezlo do aktuálního rozvaděče v serverovně podniku a bylo by nutné volit alternativní umístění.

3. **Nesprávné zvolení technologií pro realizaci** - Díky nesprávnému zvolení technologií by mohlo dojít k nekompatibilitě jednotlivých prvků. Příkladem by mohlo být chybné vyčítání hodnoty zbývajícího běhu záložního zdroje na baterie.

4. **Nedostatek finančních prostředků** - V případě nedostatku financí na projekt musí společnost tyto nedostatky odstranit. Podnik bude muset žádat například o úvěr. Nedostatek finančních prostředků může ohrozit dokončení nebo jej minimálně zbrzdit.

5. **Nedostatečné proškolení zaměstnanců** - Toto riziko má velký vliv na práci s novou technologií, na situace ohledně výpadku napájení bude třeba reagovat, zjistit, zda se jedná o plánovaný výpadek nebo o neplánovaný, zda vypínat servery nebo nechat běžet na záložní zdroj.

6. **Časové zpoždění projektu oproti plánu** - Nedodržení časového plánu by mohlo mít negativní vliv na provozování jak lokální infrastruktury tak infrastruktury hostované pro klienty společnosti.

7. **Poškození technologie infrastruktury serverovny** - Díky nesprávnému zapojení silových komponent, může dojít k nevratnému poškození hardwarové infrastruktury podniku. Na těchto serverech jsou umístěny virtuální produkční servery s daty.

Kvantifikace rizik Uvedená rizika je nutné posoudit a kvantifikovat. Dále je potřeba je posoudit, a to konkrétně jejich dopad spolu s pravděpodobností vzniku rizika. Součinem těchto dvou hodnot získáme celkový význam rizika. Na základě vypočteného významu se budeme dále rozhodovat, zdali riziko přijmeme nebo provedeme návrh na zavedení opatření, jež sníží pravděpodobnost rizika na přijatelnou úroveň.

č.	Riziko	Pst	Dopad	Hodnota
1	Nedostatečná kapacita přívodního jističe	4	8	32
2	Neočekávané fyzické rozměry řešení	3	2	6
3	Nesprávné zvolení technologií pro realizaci	2	6	12
4	Nedostatek finančních prostředků	1	2	2
5	Nedostatečné proškolení zaměstnanců	7	4	28
6	Časové zpoždění projektu oproti plánu	2	8	16
7	Poškození technologie infrastruktury serverovny	7	9	63

Obrázek 7.3: Kvantifikovaná rizika optimalizace řízení napájení

Rizika v tabulce na obrázku 7.3 byla ohodnocena na stupnici od 1 do 10 dle pravděpodobnosti vzniku a dopadu, kde 1 představuje nejnižší a 10 nejvyšší hodnotu. Výsledná hodnota rizika se pak pohybuje v rozmezí od 1 do 100.

Z kvantifikovaných rizik vyplývá, že nejkritičtější hrozbou je poškození technologie infrastruktury serverovny, převážně na tuto hrozbu je nutné se při návrhu opatření zaměřit. Mírně významná rizika jsou dále nedostatečná kapacita přívodního jističe a nedostatečné proškolení zaměstnanců.

Identifikace opatření Na rizika je možné použít opatření z tabulky na obrázku 7.4.

č.	Opatření	Náklady	Pst	Dopad	Hodnota
1	Provést průzkum charakteristiky přívodních jističů	0,00 Kč	1	8	8
2	Získat podrobné rozměry jednotlivých komponent	0,00 Kč	3	2	6
3	Provést předimplementační poradu	0,00 Kč	1	6	6
4	Vyhledat dodavatele, který nabídne odloženou splatnost	0,00 Kč	1	2	2
5	Realizovat školení pracovníků vedením IT oddělení	0,00 Kč	2	4	8
6	Naplánovat větší časové rezervy při nahlášení výpadku	0,00 Kč	1	8	8
7	Zajistit důkladné jištění všech prvků serverovny	360,00 Kč	1	9	9

Obrázek 7.4: Identifikovaná opatření optimalizace řízení napájení

Obrázek 7.5: Pavučinový graf rizik optimalizace řízení napájení

Navržená opatření v tabulce na obrázku 7.5 budou realizována stejně tak jako samotný projekt změny interními pracovníky IT a proto, není do nákladů započtena cena práce. Pro rizika byla navržena taková opatření, aby byly sníženy na přijatelnou hranici. Důkladné jištění všech prvků (náběhových skupin) serverovny spočívá v osazení jističů před každou ze čtyř náběhových skupin zařízení.

7.3.2 Časový harmonogram řízení projektu

Doby trvání projektu pro optimalizaci řízení napájení serverovny není možné přesně odhadnout. Důvodem proč nelze doby jednoduše odhadnout je fakt, že serverovna není nijak typizovaná, ale je svého druhu unikátní a ve společnosti ještě nebyla provedena optimalizace této rozsáhlosti. Na základě těchto skutečností bude pro sestavení časového harmonogramu použita metoda PERT.

Metoda PERT pracuje s hranově orientovanými síťovými grafy, kde je trvání každé činnosti považováno za náhodnou veličinu s určitým rozdělením pravděpodobnosti. Síťový graf je tedy ohodnocen stochasticky. Při ohodnocování se používají tyto tři časové odhady:

- Optimistický odhad doby trvání činnosti - značíme písmenem a.
- Nejpravděpodobnější odhad doby trvání činnosti - značíme písmenem m.
- Pesimistický odhad doby trvání činnosti - značíme písmenem b.

Pro převod na deterministický model je nutné každé činnosti síťového grafu přiřadit ohodnocení, jenž je dáno očekávaným trváním činnosti. K převodu na deterministický odhad je možné použít vzorec pro vážený průměr (t_e).

$$t_e = \frac{a + 4m + b}{6}$$

Označení	Činnost	Následník	a	m	b	t_e
A	Inventarizace vybavení a rozdělení do náběhových skupin	B	3	5	8	5,17
B	Výběr prvků pro optimalizaci napájení	C	4	5	6	5,00
C	Kontrolované vypnutí všech zařízení připojených na zálohované větve	D	1	2	4	2,17
D	Demontáž zařízení, jenž nebudou v novém řešení potřeba	E	3	4	7	4,33
E	Úklid a vyčištění zadní strany rozvaděčů	F	1	2	4	2,17
F	Instalace nových prvků	G	3	4	5	4,00
G	Propojení nových a stávajících prvků technologie (PLC, jističe, stykače)	H, I	4	5	6	5,00
H	Konfigurace postupných náběhu jednotlivých napájecích větví v PLC LOGO!	J	2	3	4	3,00
I	Konfigurace monitoringu UPS v PLC Neuron	J	3	5	7	5,00
J	Zapojení zařízení na jednotlivé nakonfigurované zálohované větve	K	1	2	3	2,00
K	Simulovaný start zařízení pro ověření správně funkčnosti řešení	L	1	2	3	2,00
L	Důkladné testování a proškolení obsluhy	M	3	4	7	4,33
M	Ukončení a vyhodnocení projektu	-	1	2	3	2,00

Obrázek 7.6: Časový harmonogram optimalizace řízení napájení

Na obrázku 7.6 je znázorněn časový harmonogram optimalizace řízení napájení včetně časových odhadů, které jsou uvedeny v člověkohodinách.

Většina z činností leží na kritické cestě. Pokud by se zpozdila jakákoliv činnost ležící na kritické cestě došlo by ke zpoždění celého zavádění změny systému řízení napájení. Kritická cesta je tvořena těmito činnostmi:

$$A - B - C - D - E - F - G - I - J - K - L - M$$

Kritická cesta je tvořena dvanácti činnostmi z celkových třinácti. Střední doba trvání zavádění změny optimalizace řízení napájení je 43,17 člověkohodin. Tato doba byla zaokrouhlena nahoru na 44 člověkohodin.

Kapitola 8

Závěr

Cílem této diplomové práce práce bylo navrhnout optimalizaci infrastruktury a monitoring serverovny podniku. Konkrétně byla práce zaměřena na infrastrukturu podniku SPOLEČNOST-24, s.r.o., jehož vedení souhlasilo i s nasazením v reálném prostředí serverovny společnosti. Tento cíl byl úspěšně splněn.

K dosažení výsledků bylo nutné nastudovat problematiku sítí, konkrétně architektury TCP/IP a virtualizace. Po seznámení se s teoretickými východisky byla provedena analýza reálné společnosti, ve které bude optimalizace probíhat. Na základě zhodnocení analýzy a respektování požadavků investora byly vytvořeny vlastní návrhy řešení.

Výsledkem práce jsou vlastní návrhy přístupového systému a měření teploty serverovny. Přístupový systém byl navržen pomocí elektronického zabezpečovacího systému Jablotron 100 stejně tak jako systém měření teploty serverovny. Dalším výsledkem práce je návrh systému řízení napájení. Tento systém spočívá v automatických startech infrastruktury serverovny a komunikace záložního zdroje s jedním serverem, který předává informace dál zařízením v síti. V rámci optimalizace jsem dále řešil serverovou infrastrukturu a to její konsolidaci. Dále byla navržena optimalizace síťové infrastruktury, která byla zjednodušena a vytvářena s ohledem na fakt, že bude spravována interním IT oddělením. Byla navržena změna systému managementu serverů a to konkrétně nasazení virtualizační technologie XCP-ng a centrální webové správy Xen Orchestra. V neposlední řadě byl navrhnut systém monitoringu síťové infrastruktury.

Vyhotovování návrhů bylo pro mne velice zajímavé a přínosné. Navržené řešení byla hodnocena vedením společnosti pozitivně a bylo uděleno povolení realizovat řešení v praxi, na kterém se budu nadále podílet. Tato diplomová práce bude sloužit podniku SPOLEČNOST-24, s.r.o. jako dokumentace k navrženým optimalizacím a bude tyto optimalizace v průběhu roku 2019 postupně v daném pořadí po etapách realizovat. Část navržených řešení byla v době tisku práce již nasazována.

V budoucnu by společnost mohla využít i navrženého rozšíření v podobě exit strategie z cloudu. Dále pro budoucí řešení problematiky infrastruktury serverovny navrhuji, aby si společnost dokoupila motor generátor (diesel agregát například 8kW) s nádrží na 40 litrů paliva. Motor generátor pomůže infrastruktuře společnosti překonat i výpadky delší než 8 hodin.

Seznam zkratek

DIN — Deutsches Institut für Normung
DMZ — Demilitarized Zone
EoIP — Ethernet over IP
EZS — Elektronický zabezpečovací systém
FW — Firewall
GSM — Groupe Spécial Mobile
IP — Internet Protocol
IS — Information System
IT — Information Technology
LAN — Local Area Network
MAC — Media Access Control
MIB — Mangement Information Base
NVR — Network Video Recorder
OID — Object Identifier
PG — Programovatelný výstup
PLC — Programmable Logic Controller
PoE — Power over Ethernet
RDS — Remote Desktop Services
RFID — Radio Frequency Identification
SLA — Service Level Agreement
SMS — Short Message Service
SNMP — Simple Network Management Protocol
SSH — Secure Shell
SSTP — Secure Socket Tunneling Protocol
TCP — Transmission Control Protocol
Telnet — Teletype network
UDP — User Datagram Protocol
UPS — Uninterruptible Power Supply
USB — Universal Serial Bus
VLAN — Virtual LAN
VM — Virtual Machine
VPN — Virtual Private Network

Literatura

[1] ADSL s.r.o.: *SSH – bezpečné používání vzdáleného počítače a kopírování dat.* [Online; navštíveno 14.01.2019].
URL https://www.dsl.cz/jak-na-to/jak-na-ssh

[2] BANDERA, D. Q.; LEGBAND, D. A.: Hot spare light weight mirror for raid system. 2001, uS Patent 6,223,252.

[3] BONWICK, J.; MOORE, B.: ZFS. In *LISA*, 2007.

[4] CASE, F.; SCHOFFSTALL, D.: *Request for Comments: 1157, SNMP.* [Online; navštíveno 14.01.2019].
URL https://tools.ietf.org/html/rfc1157

[5] Eaton: *Eaton 9SX 6000i RT3U (9SX6KiRT).* [Online; navštíveno 15.03.2019].
URL http://powerquality.eaton.com/9SX6KiRT.aspx?cx=68&GUID=3683B1D0-DDAA-4B46-9EC5-F341D50E89E3

[6] Elektrotechnický zkušební ústav, s.p.: *Elektrotechnický zkušební ústav.* [Online; navštíveno 05.03.2019].
URL http://ezu.cz/

[7] FIEDOR, J.; SOLÁR, P.: *Studijní materiály předmětu Serverové systémy Microsoft Windows(IW2/XMW2).* [Verze 2019].

[8] HINK, T.: *Přístupový systém podniku s EZS Jablotron 100.* Brno, 2017. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Bidlo Michal.

[9] Jablotron security a. s.: *Materiály získané ze školení (Jablotron - Základy elektronického zabezpečení objektů).* [Verze 2016/02].

[10] JORDÁN, V.; ONDRÁK, V.: *Infrastruktura komunikačních systémů II.* Brno: CERM, Akademické nakladatelství, 2015, ISBN 978-80-214-5240-4.

[11] KOVOTECHNIKA, spol. s r.o.: *Elektrický otvírač Befo-DUAL 2611 MB.* [Online; navštíveno 04.03.2019].
URL https://www.kovotechnika.cz/elektricky-otvirac/Befo-DUAL-2611MB

[12] MikroTik: *MikroTik Routers and Wireless.* [Online; navštíveno 14.01.2019].
URL https://mikrotik.com/

[13] MINAŘÍKOVÁ, A.: *Tabulka krytí IP (popis stupňů).* [Online; navštíveno 03.04.2019].
URL http://elektrika.cz/data/clanky/krip030918

[14] NetWin CZ, s.r.o.: *Citrix XenServer*. [Online; navštíveno 16.01.2019].
URL http://www.netwin.cz/citrix-xenserver/

[15] ONDRÁK, V.; SEDLÁK, P.; MAZÁLEK, V.: *Problematika ISMS v manažerské informatice*. Brno: Akademické nakladatelství CERM, vyd. 1 vydání, 2013, ISBN 978-80-7204-872-4.

[16] POSTEL, J.: *Request for Comments: 792, ICMP*. [Online; navštíveno 14.01.2019].
URL https://tools.ietf.org/html/rfc792

[17] POSTEL, J.: *Request for Comments: 854, Telnet*. [Online; navštíveno 14.01.2019].
URL https://tools.ietf.org/html/rfc854

[18] RAIDA, Z.: *Základní pojmy*. [Online; navštíveno 11.01.2019].
URL http://www.urel.feec.vutbr.cz/~raida/optimalizace/pojmy/pojmy_a.htm

[19] RAIS, K.; DOSKOČIL, R.: *Risk management: studijní text pro kombinovanou formu studia*. Brno: Akademické nakladatelství CERM, 2007, ISBN 978-80-214-3510-0.

[20] RUEST, D.; RUEST, N.: *Virtualizace*. Brno: Computer Press, vyd. 1 vydání, 2010, ISBN 978-802-5126-769.

[21] SPOLEČNOST-24 s.r.o.: *Webové stránky podniku*. [Online; navštíveno 04.02.2019].
URL https://www.spolecnost-24.cz

[22] TAKEMURA, C.; CRAWFORD, L. S.: *The book of Xen*. San Francisco: No Starch Press, c2010, ISBN 15-932-7186-7.

[23] THOMASIAN, A.; MENON, J.: RAID5 performance with distributed sparing. *IEEE Transactions on Parallel and Distributed Systems*, ročník 8, č. 6, 1997: s. 640–657.

[24] UniPi.technology, dceřiná společnost Faster CZ spol. s r.o.: *Unipi*. [Online; navštíveno 17.01.2019].
URL https://www.unipi.technology/cs/

[25] XCP-ng: *XCP-ng documentation*. [Online; navštíveno 16.01.2019].
URL https://github.com/xcp-ng/xcp/wiki

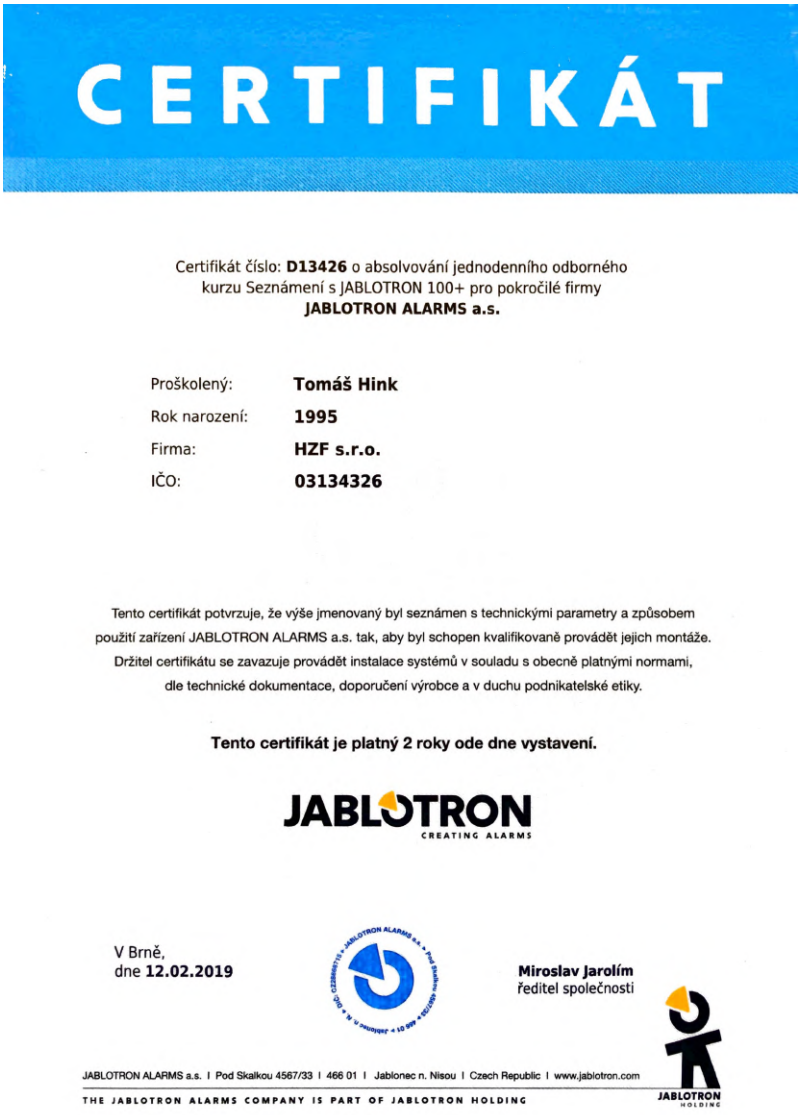
[26] Xen Orchestra: *Web interface for XCP-ng*. [Online; navštíveno 16.01.2019].
URL https://xen-orchestra.com/

Seznam obrázků

Přílohy

Příloha A

Certifikát ze školení



CERTIFIKÁT

Certifikát číslo: **D13426** o absolvování jednodenního odborného kurzu Seznámení s JABLOTRON 100+ pro pokročilé firmy
JABLOTRON ALARMS a.s.

Proškolený:	**Tomáš Hink**
Rok narození:	**1995**
Firma:	**HZF s.r.o.**
IČO:	**03134326**

Tento certifikát potvrzuje, že výše jmenovaný byl seznámen s technickými parametry a způsobem použití zařízení JABLOTRON ALARMS a.s. tak, aby byl schopen kvalifikovaně provádět jejich montáže. Držitel certifikátu se zavazuje provádět instalace systémů v souladu s obecně platnými normami, dle technické dokumentace, doporučení výrobce a v duchu podnikatelské etiky.

Tento certifikát je platný 2 roky ode dne vystavení.

JABLOTRON
CREATING ALARMS

V Brně,
dne **12.02.2019**

Miroslav Jarolím
ředitel společnosti

JABLOTRON ALARMS a.s. I Pod Skalkou 4567/33 I 466 01 I Jablonec n. Nisou I Czech Republic I www.jablotron.com
THE JABLOTRON ALARMS COMPANY IS PART OF JABLOTRON HOLDING

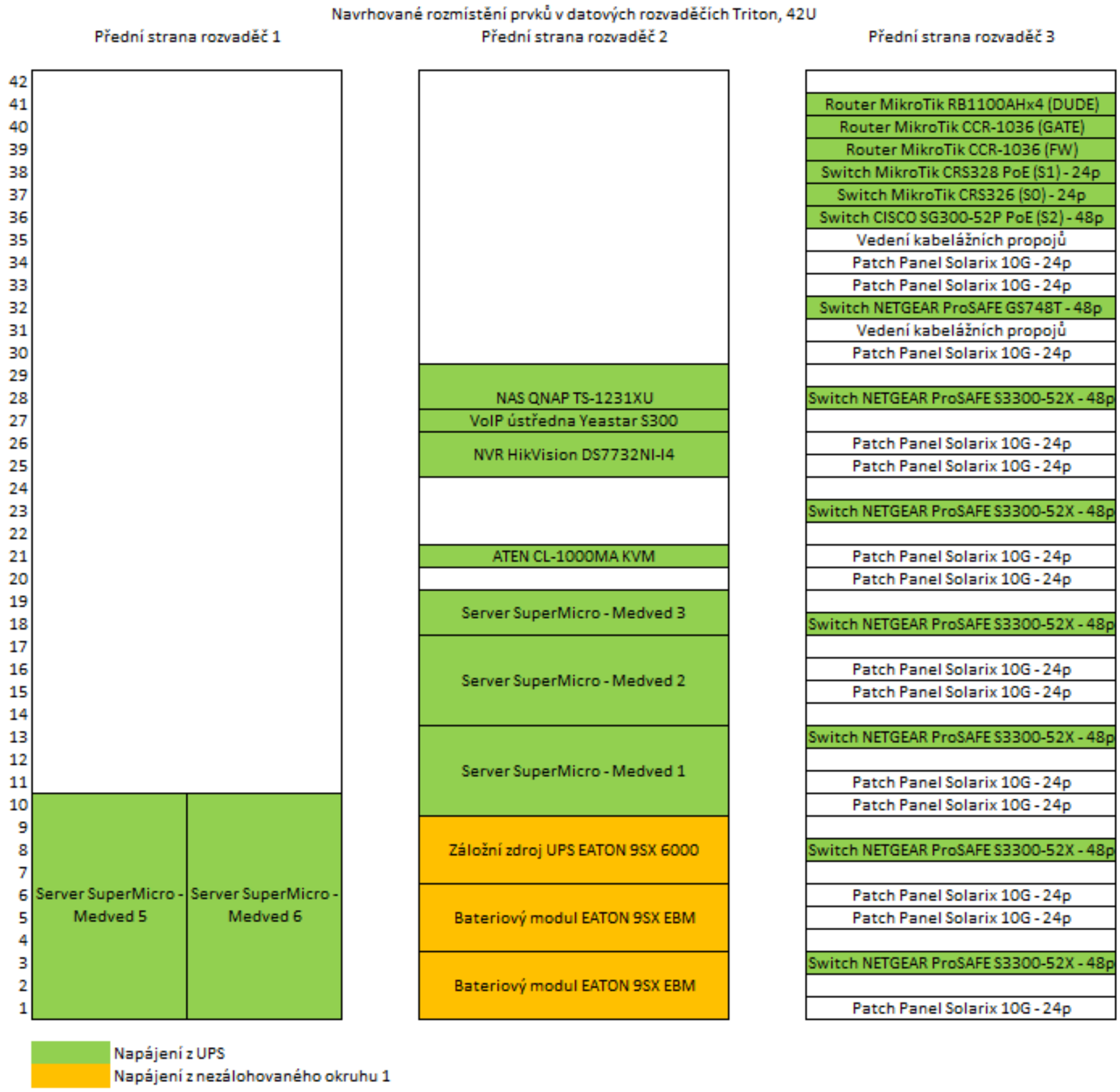
JABLOTRON HOLDING

Obrázek A.1: Certifikát ze školení Jablotron - *Tomáš Hink*

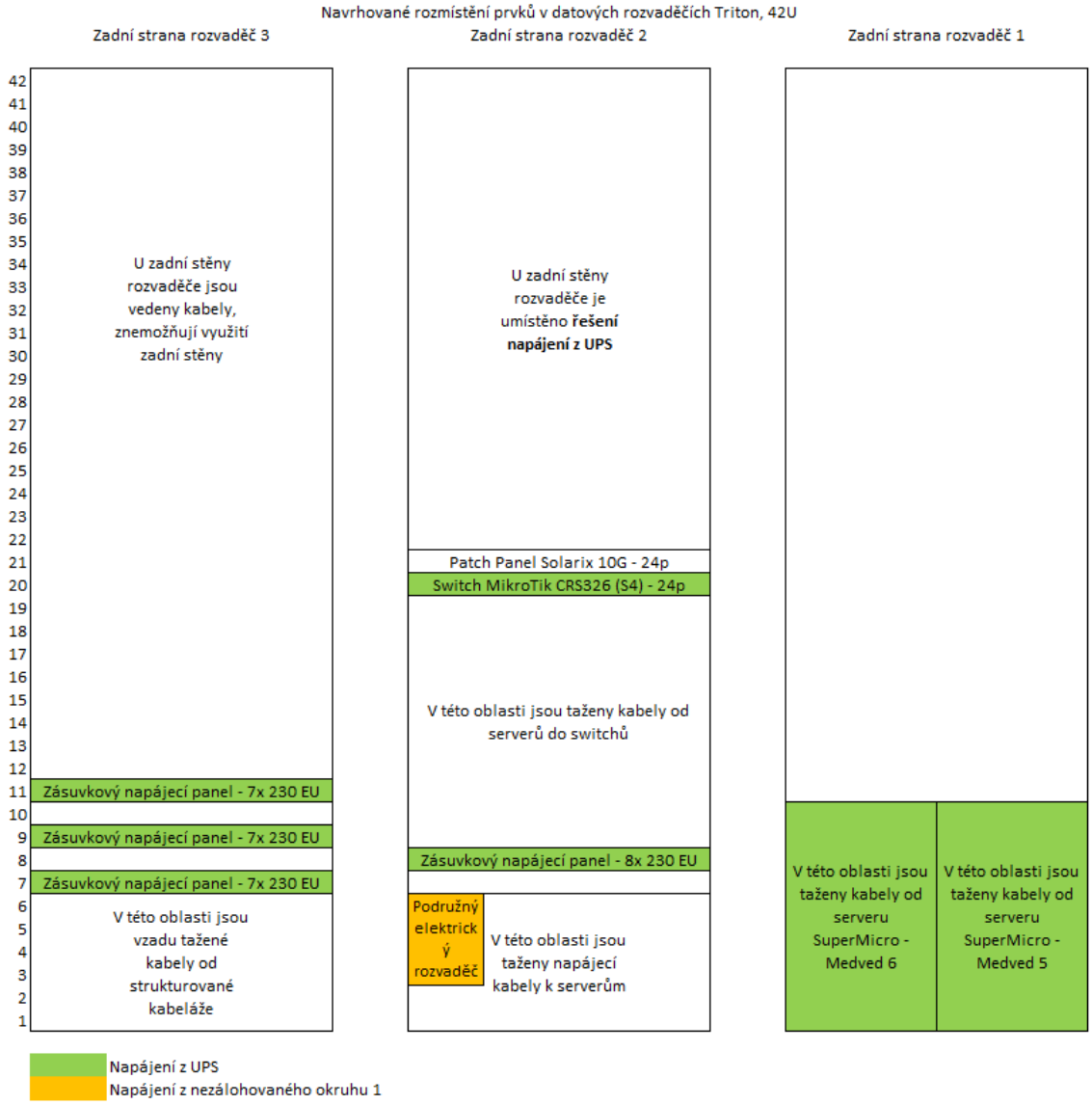
Příloha B

Fyzické rozmístění zařízení v rozvaděčích po optimalizaci

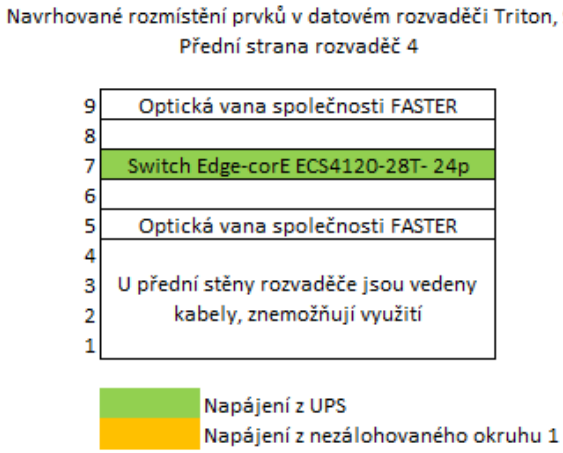
V této příloze bude znázorněno a popsáno navrhované fyzické rozmístění zařízení po provedení optimalizací infrastruktury podniku. Dle obrázku B.1 (rozvaděče serverovny A - pohled zepředu) a obrázku B.2 (rozvaděče serverovny A - pohled zezadu) bylo navrhnuto, aby byl odebrán již nepotřebný monitor z rozvaděče 1, server Medved 4 z rozvaděče 2 a dvanáct PoE injektorů z rozvaděče 3. Tyto zařízení již nadále nebudou v infrastruktuře třeba. Dále bylo navrhnuto umístění řešení pro ovládání napájení do horní části rozvaděče 2, přesun routeru MikroTik RB2011 i jednoho PoE injektoru včetně jeho zdroje do Serverovny B a ze serverovny B přesunout čtyřiceti osmi portový PoE switch CISCO. Navrhované schéma rozmístění infrastruktury rozvaděče v serverovně B je znázorněno na obrázku B.4. V rozvaděč poskytovatele připojení dle mého uvážení není třeba nijak měnit umístění prvků, jedinou optimalizaci, kterou si dovoluji navrhnout je připojit switch pro připojení k Internetu (SFaster) na zálohovanou větev napájenou z UPS. Umístění prvků v rozvaděči 4 serverovny A je znázorněno na obrázku B.3. V rámci optimalizace proudění vzduchu navrhuji, aby v budoucnu byly všechny nepoužívané pozice v rozvaděčích vyplněny fólií nebo záslepkami.



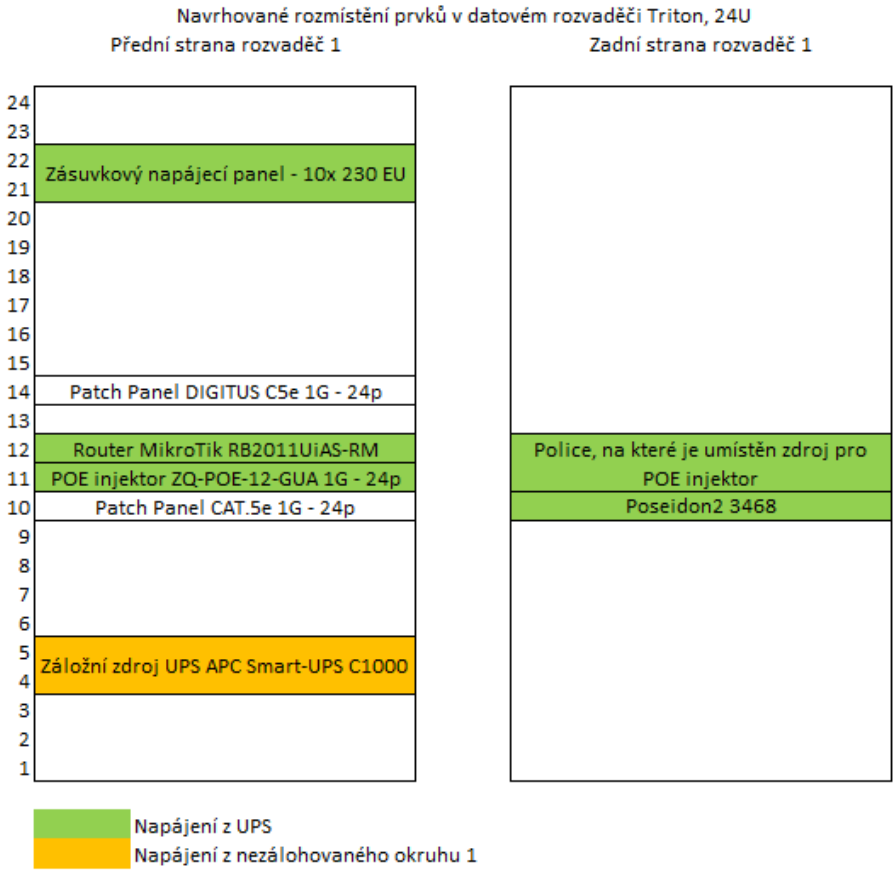
Obrázek B.1: Návrh rozmístění prvků po optimalizaci v datových rozvaděčích Triton, 42U - Serverovna A - pohled zepředu



Obrázek B.2: Návrh rozmístění prvků po optimalizaci v datových rozvaděčích Triton, 42U - Serverovna A - pohled zezadu



Obrázek B.3: Návrh rozmístění prvků po optimalizaci v datových rozvaděčích Triton, 9U - Serverovna A - pohled zepředu na rozvaděč 4



Obrázek B.4: Návrh rozmístění prvků po optimalizaci v datových rozvaděčích Triton, 24U - Serverovna B