

Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií



Diplomová práce

Počítačová síť v hotelovém zařízení

Michal Plzák

© 2018 ČZU v Praze

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Michal Plzák

Informatika

Název práce

Počítačová síť v hotelovém zařízení

Název anglicky

Computer network at hotel facilities

Cíle práce

Cílem diplomové práce je návrh počítačové sítě v hotelové zařízení. Vzhledem k existující síti v daném zařízení a jejímu stáří, bude navržena nová síť s novými prvky, kdy bude kladen důraz na jednoduchost, funkčnost a účinnost nové sítě vůči stávající. Dílčí cíle:

- Definice počítačových sítí a základní charakteristika
- Analýza stávající sítě hotelu a návrh nové
- Výběr nových prvků
- Analýza měření Wi-Fi signálu
- Finanční analýza
- Závěry a doporučení

Metodika

Metodika teoretického hlediska diplomové práce je založena na analýze a zkoumání bibliografických a elektronických zdrojů, kde v teoretické části bude uvedena definice počítačových sítí a základní charakteristika. Hlavní důraz bude kladen na kapitoly aplikace a služby, zabezpečení počítačové sítě a samotná správa počítačové sítě.

Ve vlastní práci bude provedena analýza stávající sítě a návrh nové sítě, který bude vycházet ze syntézy získaných poznatků. V nákresech budovy, bude vyobrazená kabeláž nové počítačové sítě a její náležitosti. Pro výběr prvků v síti byla zvolena vícekritériální analýza, která určí vybrané prvky pro daný návrh nové sítě. Dále bude provedena analýza měření Wi-Fi signálů s určenou tolerancí ve vybrané softwarové aplikaci. V neposlední řadě bude provedena finanční analýza více návrhů možných realizací nové sítě.

Na základě výsledků vlastní práce budou generována doporučení a formulován závěr této diplomové práce.

Doporučený rozsah práce

50 – 60 stran

Klíčová slova

Počítačová síť, Wi-Fi, PC, Hotel, Restaurace, Server, Kamery, VoIP, Zabezpečení

Doporučené zdroje informací

Horák, J; Keršlanger, M. (2008). Počítačové sítě pro začínající správce. Brno: Computer Press

Horák, J. (2013). Počítačové sítě. Brno: Computer Press.

Sosinsky, B. (2010). Mistrovství – počítačové sítě. Brno: Computer Press.

Šubrt, T. (2011). Ekonomicko-matematické metody 2.vyd. Praha: Vydavatelství a nakladatelství Aleš Čeněk

Předběžný termín obhajoby

2017/18 LS – PEF

Vedoucí práce

Ing. Jiří Vaněk, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 22. 5. 2017

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 24. 5. 2017

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 31. 03. 2018

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Počítačová síť v hotelovém zařízení" jsem vypracoval(a) samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 31. 3. 2018

Poděkování

Rád(a) bych touto cestou poděkoval(a) Ing. Jiřímu Vaňkovi, Ph.D. za vedení mé diplomové práce. Dále bych rád poděkovat Ing. Rostislavu Kopeckému, majiteli hotelu DAR, který souhlasil s provedením analýzy hotelu, svěřením důvěry k volnému pohybu po budově a poskytnutím potřebných materiálů k vypracování této diplomové práce.

Počítačová síť v hotelovém zařízení

Abstrakt

Tato diplomová práce pojednává o počítačové síti v hotelovém zařízení a určitých požadavcích sítě v tomto prostředí. Napříč teoretickou prací jsou popsány definice počítačových sítí, jejich dělení až po moderní trendy v počítačových sítích. Jsou zde vysvětlovány moderní komunikační protokoly jednotlivých služeb, ať už se jedná o protokoly, které využijí v praktické části či nikoliv. Dále jsou v teoretické části popsány aktivní a pasivní prvky sítě. V neposlední řadě jsou zde popsány síťové služby a jakým způsobem je lze kontrolovat či spravovat.

V praktické části je provedena charakteristika hotelového zařízení, na kterém byla provedena stávající analýza sítě, která byla zaznamenána do půdorysů jednotlivých podlaží. Dále byly vytvořeny návrhy nového síťového řešení s ohledem na budoucí rozvoj budovy nebo při stávající velikosti budovy. V praktické části byly stanoveny požadavky na novou síť a pomocí vícekritériální analýzy byly vybrány jednotlivé prvky, které byly určeny tímto principem výběru. Výstupem práce je návrh nové sítě pro hotelové zařízení DAR a kdy tento návrh může být vzorovým řešením pro objekty podobné velikosti. Tento návrh je vytvořen i s finanční analýzou na pořizovací náklady a také s náklady v průběhu příštích let.

V závěru bude zhodnocen průběh praktické části, výsledné řešení a možné další využití sítě nebo jednotlivých prvků.

Klíčová slova: Počítačová síť, Wi-Fi, PC, Hotel, Restaurace, Server, Kamery, VoIP, Zabezpečení

Computer network at hotel facilities

Summary

This diploma thesis describes specific computer network and its requirements, which is used in a hotel. Computer networks and their definition are described at the start of the thesis, computer networks used in the past, and computer networks that we use nowadays. There are also described communication protocols, which can be used in the practical part. At the end of the theoretical part are described active and passive networking hardware, also network services, their controlling and managing.

In the practical part we can see analysis of the computer network used in hotel including all floors. New proposals of the computer network if the organisation grows, or if the organisation stays the same. There are also described requirements for the new computer network and new active/passive networking hardware, which was chosen via the multicriterial analysis. The output of this thesis is proposal for the new computer network for hotel facilities DAR, also can be used for other companies with the same or similar size. Proposal includes financial analysis of the initial costs and the future costs.

At the end of the practical part is described how tough was the realisation and the final solution of the computer network.

Keywords: Computer network, Wi-Fi, PC, Hotel, Restaurant, Server, Cameras, VoIP, Security

Obsah

2 Úvod.....	13
3 Cíl práce a metodika	14
3.1 Cíl práce	14
3.2 Metodika	14
4 Teoretická východiska	16
4.1 Definice počítačových sítí	16
4.2 Taxonomie počítačových sítí	17
4.3 Druhy přenosů a topologie počítačových sítí	19
4.3.1 Druhy přenosů.....	19
4.3.2 Topologie	20
4.4 Přenosová média	23
4.4.1 Kabelová média	23
4.4.2 Bezdrátové sítě.....	25
4.5 Přístupové metody	26
4.5.1 Metody statického přidělování.....	26
4.5.2 Metody centrálního přidělování.....	26
4.5.3 Metody náhodného přidělování	27
4.5.4 Metody distribuovaného přidělování	27
4.6 Hardwarové prvky počítačové sítě	28
4.6.1 Sběrnice pro síťové karty.....	29
4.6.2 Zařízení první a druhé vrstvy.....	29
4.6.3 Směrovače.....	31
4.6.4 Brány.....	31
4.7 Síťový zásobník	32
4.7.1 Model ISO/OSI.....	32
4.7.2 Model TCP/IP	35
4.8 Protokoly TCP/IP.....	36
4.8.1 Internet protokol	36
4.8.2 Protokoly TCP a UDP.....	36
4.8.3 Aplikační protokoly	37
4.9 Aplikace a služby.....	38
4.9.1 Síťové operační systémy.....	38
4.9.2 Domény a adresářové služby	40
4.9.3 Souborové systémy	44

4.9.4	Webové služby.....	47
4.9.5	Poštovní protokoly.....	48
4.9.6	Telefonie a VoIP.....	50
4.10	Zabezpečení počítačové sítě.....	52
4.10.1	Bezpečnostní protokoly a služby.....	52
4.10.2	Firewally, brány a proxy servery.....	55
4.10.3	VPN.....	57
4.11	Správa počítačové sítě.....	59
4.11.1	Správa sítě.....	59
4.11.2	Příkazy pro diagnostiku.....	62
4.11.3	Vzdálený přístup.....	64
5	Vlastní práce.....	67
5.1	Charakteristika podniku.....	67
5.1.1	Analýza stávající sítě hotelu a návrh nové.....	68
5.1.2	Požadavky na nové síťové řešení.....	84
5.1.3	Nové síťové řešení.....	86
5.2	Výběr nových prvků.....	99
5.2.1	Výběr síťových prvků.....	100
5.2.2	Výběr – UPS.....	103
5.2.3	Výběr – NAS.....	105
5.2.4	Výběr – Server.....	107
5.2.5	Výběr – PC (zákazníci).....	109
5.2.6	Výběr – PC (zaměstnanci).....	111
5.2.7	Výběr – Notebook.....	114
5.2.8	Poskytnuté prvky.....	115
5.3	Analýza měření Wi-Fi signálu.....	117
5.4	Finanční analýza.....	122
5.4.1	Náklady na pořízení síťového zařízení.....	123
5.4.2	Náklady na pořízení ostatního zařízení.....	123
5.4.3	Náklady na software.....	124
5.4.4	Náklady na práci.....	125
5.4.5	Celkové náklady.....	125
5.4.6	Provozní náklady v dalších letech.....	126
6	Výsledky a diskuse.....	130
6.1	Výsledky praktické části.....	130
6.2	Diskuse.....	132

7 Závěr.....	134
8 Citovaná literatura.....	136

Seznam obrázků

Obrázek 1 - Půdorys PP1 (autor)	70
Obrázek 2 - Půdorys NP1 (autor)	71
Obrázek 3 - Půdorys NP2 (autor)	72
Obrázek 4 - Půdorys NP3 (autor)	73
Obrázek 5 - Půdorys NP4 (autor)	74
Obrázek 6 - Analýza PP1 se stávajícími prvky (autor).....	75
Obrázek 7 - Analýza NP1 se stávajícími prvky (autor)	77
Obrázek 8 - Analýza NP2 se stávajícími prvky (autor)	78
Obrázek 9 – Analýza rozvaděče (autor)	79
Obrázek 10 – Analýza rozvaděče (autor)	80
Obrázek 11 - Analýza NP3 se stávajícími prvky (autor)	82
Obrázek 12 - Analýza NP4 se stávajícími prvky (autor)	83
Obrázek 13 - Hodnocení hotelu DAR na booking.com (autor)	84
Obrázek 14 - Hodnocení uživatele na booking.com (autor).....	84
Obrázek 15 - Návrh nového řešení s novými prvky v PP1 (autor).....	88
Obrázek 16 - Návrh nového řešení s novými prvky v NP1 (autor)	90
Obrázek 17 - Návrh nového řešení s novými prvky v NP2 (autor)	92
Obrázek 18 - Návrh nového řešení s novými prvky v NP3 (autor)	93
Obrázek 19 - Návrh nového řešení s novými prvky v NP4 (autor)	95
Obrázek 20 - Návrh "Řešení 1" v rozvaděči (autor).....	97
Obrázek 21 - Návrh "Řešení 2" v rozvaděči (autor).....	98
Obrázek 22 - Analýza Wi-Fi signálu v restauraci (autor).....	119
Obrázek 23 - Analýza Wi-Fi signálu ve vinárně (autor)	119
Obrázek 24 - Analýza Wi-Fi signálu na recepci (autor).....	120
Obrázek 25 - Pozice měření v druhém nadzemním podlaží (autor)	120
Obrázek 26 - Pozice měření ve třetím nadzemním podlaží (autor)	121

Obrázek 27 - Analýza Wi-Fi signálu v pokoji druhého nadzemního podlaží (autor)..... 121

Obrázek 28 - Analýza Wi-Fi signálu v pokoji třetího nadzemního podlaží (autor) 122

Seznam tabulek

Tabulka 1 - Charakteristika slabých míst	53
Tabulka 2 - Legenda prvků (autor)	87
Tabulka 3 - Náklady na "Řešení 1" v rozvaděči (autor)	98
Tabulka 4 - Náklady na "Řešení 2" v rozvaděči (autor)	99
Tabulka 5 - Výběr UPS - základní tabulka (autor)	104
Tabulka 6 - Výběr UPS - bodovací metoda (autor)	104
Tabulka 7 - Výběr UPS - metoda váženého součtu (autor)	105
Tabulka 8 - Výběr NAS - základní tabulka (autor)	106
Tabulka 9 - Výběr NAS - bodovací metoda (autor)	106
Tabulka 10 - Výběr NAS - metoda váženého součtu (autor)	107
Tabulka 11 - Výběr serveru - základní tabulka (autor).....	108
Tabulka 12 - Výběr serveru - bodovací metoda (autor).....	108
Tabulka 13 - Výběr serveru - metoda váženého součtu (autor).....	109
Tabulka 14 - Výběr PC pro zákazníka - základní tabulka (autor)	110
Tabulka 15 - Výběr PC pro zákazníka - bodovací metoda (autor)	110
Tabulka 16 - Výběr PC pro zákazníka - metoda váženého součtu (autor)	111
Tabulka 17 - Výběr PC pro zaměstnance - základní tabulka (autor).....	112
Tabulka 18 - Výběr PC pro zaměstnance - bodovací metoda (autor).....	113
Tabulka 19 - Výběr PC pro zaměstnance - metoda váženého součtu (autor).....	113
Tabulka 20 - Výběr notebooku - základní tabulka (autor).....	114
Tabulka 21 - Výběr notebooku - bodovací metoda (autor)	115
Tabulka 22 - Výběr notebooku - metoda váženého součtu (autor).....	115
Tabulka 23 - Kvalita Wi-Fi signálu (autor)	118
Tabulka 24 - Náklady na "Řešení 1" v rozvaděči (autor)	123
Tabulka 25 - Náklady na pořízení ostatního zařízení (autor)	124
Tabulka 26 - Náklady na software (autor)	125
Tabulka 27 - Celkové náklady na "Řešení 1" (autor)	125

Tabulka 28 - Přehled spotřeby stávajícího řešení (autor)	127
Tabulka 29 - Výpočet výsledné ceny za energie stávajícího řešení (autor).....	127
Tabulka 30 - Přehled spotřeby po rozšíření hotelu (autor)	128
Tabulka 31 - Výpočet výsledné ceny za energie po rozšíření hotelu (autor)	128
Tabulka 32 - Náklady na software v následujících letech (autor)	129

1 Úvod

21. století je stoletím digitálních technologií, které stále více zasahují nejen do životů běžných lidí, ale stále více do výrobních procesů firem, ať už malých podniků nebo nadnárodních korporací. Komunikace v digitálních technologiích probíhá za pomoci 1 a 0, která jsou přenášena po drátovém spojení, ať už po měděném nebo optickém spoji, anebo za pomoci bezdrátových technologií. Počítačové sítě urychlují, usnadňují komunikaci a jsou schopny ukládat jejich výsledky.

Téma diplomové práce „Počítačová síť v hotelovém zařízení“ bylo zvoleno z důvodu zájmu o znalosti z oblasti počítačových sítí a využití těchto znalostí na praktickém příkladu. V teoretické části budou popsány hierarchie počítačových sítí, které jsou nezbytné pro vybudování počítačové sítě jako takové. Důraz v teoretické části bude kladen na taxonomii počítačových sítí, druhy přenosů, topologii sítí a hardwarových prvků počítačových sítí. Ostatní kapitoly budou popsány z důvodu možného využití ve vlastní práci. V této diplomové práci je hlavním cílem a účelem tvorba kabelového a bezdrátového připojení, které v poslední době zaznamenává největší rozmach v historii lidstva.

Vlastní práce je hlavním bodem této diplomové práce. Zde budou využity poznatky z teoretické části práce, které budou přeneseny do praktického prostředí, tedy k vytvoření nové počítačové sítě v hotelovém zařízení. Hlavní částí bude analýza stávající sítě v hotelovém zařízení a konstrukce nové počítačové sítě. V tomto bodě bude provedena analýza hardwarových prvků, které budou využity pro nový návrh počítačové sítě. Za pomoci softwarových prvků bude provedena analýza měření Wi-Fi signálů v budově a budou vyznačeny pozice do půdorysu budovy, ze kterých byla analýza provedena. V neposlední řadě bude vypracována finanční analýza, která bude předložena majiteli hotelu s náklady na údržbu při stávajícím velikosti sítě, popřípadě po rozšíření velikosti sítě o další prvky. Z důvodu rozsáhlosti návrhu nejspíš nebude možné provést fyzickou realizaci sítě.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem diplomové práce je návrh počítačové sítě v hotelové zařízení. Vzhledem k existující síti v daném zařízení a jejímu stáří, bude navržena nová síť s novými prvky, kde bude kladen důraz na jednoduchost, funkčnost a účinnost nové sítě vůči stávající. Dílčí cíle:

- Definice počítačových sítí a základní charakteristika
- Analýza stávající sítě hotelu a návrh nové
- Výběr nových prvků
- Analýza měření Wi-Fi signálu
- Finanční analýza
- Závěry a doporučení

2.2 Metodika

Metodika teoretického hlediska diplomové práce je založena na analýze a zkoumání bibliografických a elektronických zdrojů, kde v teoretické části bude uvedena definice počítačových sítí a základní charakteristika. Hlavní důraz bude kladen na kapitoly aplikace a služby, zabezpečení počítačové sítě a samotná správa počítačové sítě.

Ve vlastní práci bude provedena analýza stávající sítě a návrh nové sítě, který bude vycházet ze syntézy získaných poznatků. Nákresey budovy budou získány ve formátu dwg, které lze otevřít v softwarové aplikaci AutoCAD od společnosti Autodesk. V nákresech budovy budou vyobrazeny stávající prvky sítě a bude provedena jejich krátká charakteristika. Následně bude vyobrazená kabeláž nové počítačové sítě a dalších prvků v síti. Pro výběr prvků v síti byla zvolena vícekritériální analýza, která určí vybrané vhodné prvky podle stanovených kritérií. Bude použita metoda „bodovací“ s intervalem 1-10 (10 – nejlepší, 1 – nejhorší) a metoda „váženého součtu“, která pracuje s ideálními a bazálními hodnotami. K porovnávání vlastností prvků byly stanoveny váhy, které poukazují na důležitost vlastnosti. Dále bude provedena analýza měření Wi-Fi signálů s určenou tolerancí ve vybrané softwarové aplikaci v areálu budovy. V neposlední řadě bude

provedena finanční analýza více návrhů s náklady na údržbu při stávající velikosti sítě, popřípadě po rozšíření velikosti sítě o další prvky. Bude proveden výpočet ceny elektřiny při stanoveném časovém horizontu jeden rok.

Na základě výsledků vlastní práce budou generována doporučení a formulován závěr této diplomové práce.

3 Teoretická východiska

3.1 Definice počítačových sítí

Existuje spousta definic popisující počítačovou síť, mezi nejjednodušší definici patří ta, která popisuje spojení dvou a více počítačů, které jsou navzájem vyměňují data a jsou navzájem propojené jedním nebo sadou spojení, pomocí kterých se vyměňují zmíněná data. Nelze říci, že by existoval univerzální model pro každou síť, každá má svoje uspořádání, velikost a architekturu, podle kterých se dělí, ovšem každá počítačová síť se musí skládat z těchto komponent, aby se za ni dala považovat:

- Propojené systémy
- Propojovací software
- Síťový software
- Fyzická přenosová media
- Adresní systém pro všechny výše uvedené komponenty

Tyto komponenty dávají dostatečně široké pole působnosti, aby se nedalo mluvit pouze o počítačové síti skládající se pouze z počítačových systémů, ale o síti, která obsahuje také systémy typu mobilních telefonů, paměťových zařízení, široko pásmových spojení a mnoha dalších systémů, které mohou být už z jednoho, či jiného důvodu patřit do počítačové sítě.

Jedním ze základních stavebních prvků síťové komunikace je síťový hardware, bez kterého zařízení není schopné výměny dat v dané počítačové síti. Tento síťový hardware je součástí operačního systému, v síťovém hardware, v zákaznický integrovaných síťových obvodech, ale také už i v přenosových mediích. Aby mohla probíhat komunikace v rámci počítačové sítě, je potřeba tzv. fyzické přenosové medium, které je schopné přenášet elektromagnetický signál. Signálem je rozuměna amplituda frekvence nebo napětí, které se stále mění v čase. Mění se signál představuje hodnotu přenášených informací, které jsou rozpoznávány přijímačem. Signály mohou být trvale proměnlivé (analogové) nebo omezené na jistou sadu (digitální). V této diplomové práci se budou využívat binární systémy, které využívají digitální signál.

Binární systém je systém, který využívá pouze dvou stavů: Zapnuto nebo Vypnuto, Ano nebo Ne, 1 nebo 0, napětí 1 nebo napětí 2. Digitální počítače využívají právě binární signál a tzv. Booleovskou algebru z důvodů snadného a rychlého přenosu. Jednoduchá reprezentace dvou stavů binárního signálu umožňuje reprezentovat jakýkoliv znak nebo matematickou vlastnost, pomocí kterých lze řešit téměř všechny matematické rovnice.

Přenos datových toků nemusí nutně probíhat prostřednictvím fyzického datového přenašeče jakými jsou kabely nebo dráty, ale k přenosu dat lze využít jakoukoliv složku elektromagnetického spektra. Typickým příkladem v této době může být notebook. Pokud na notebooku otevřete webový prohlížeč, počítač získává potřebná data k načtení webové stránky pomocí rádiové frekvence. Tyto buněčné sítě přenášejí data na větší vzdálenost pomocí mikrovlnných vysílačů. Bezdrátové sítě Wi-Fi fungují na standardu 802.11. Tento standard je dalším příkladem přenosu pomocí radiových vln.

Pokud mikrovlnná trouba pracuje na frekvenci 2,4 GHz, ruší bezdrátovou síť postavenou na standardu 802.11g.

Do definice počítačových sítí nespádají případy, kdy se data nepřenášejí automaticky. Takovým příkladem může být kopírování souboru z jednoho počítače na USB flash disk a následného přenosu na jiný počítač. V tomto případě se nejedná o počítačovou síť. (Sosinsky, 2010) (Horák & Keršlágner, 2016)

3.2 Taxonomie počítačových sítí

Počítačové sítě se mohou třídit podle své velikosti, uspořádání a architektury. Mohou existovat sítě o velikosti jednoho sériového, paralelního nebo USB kabelu, který propojuje dva počítače (vztah typu P2P). Tyto sítě jsou často pouze jednoúčelové, jsou vytvořeny a nakonfigurovány dle aktuální potřeby. Často spousta lidí toto propojení nepovažuje za typ sítě. Pokud by však bylo několik systémů spojeno do jedné pracovní skupiny, která by bylo propojena rozbočovačem, už by to představovalo většinovou představu o zapojení typu peer-to-peer. Pracovní skupina je kolekcí počítačů, které využívají nebo nabízejí služby dle potřeby.

Nejmenší sítě jsou označovány za personální počítačové sítě, které jsou označovány PAN. Jedná se o skupinu periférií připojených k jedinému počítačovému systému.

Typickým příkladem může být technologie Bluetooth, kdy se zařízení spojují radiovými vlnami se skokovými změnami frekvence. Datové toky jsou rozděleny do 75 různých frekvencí s dosahem 10 metrů. I když se jedná o malou síť, její možnosti jsou velice pokročilé. Automatická konfigurace, zabezpečení, propagace možností a služeb každého zařízení, to všechno technologie Bluetooth umožňuje.

Nejspíše nejvíce používaným pojmem v počítačových sítích je zkratka LAN. LAN označuje místní síť, ovšem tento pojem je velice subjektivní. LAN je skupina propojených systémů, které se mohou nacházet v jedné místnosti, patře nebo budově. Hlavní charakteristikou pro síť jsou adresní schémata a komunikační pravidla či protokoly. Z toho důvodu se AppleTalk a Netware považují na různé síť LAN i když běží na stejném hardwaru a po shodných komunikačních spojích. Snadno se narazí na LAN se sítí Windows včetně Windows Serveru a servery Netware. Hovoříme tedy o heterogenních sítích.

Síť typu LAN přestává být v okamžiku, kdy se podstatně liší adresace nebo když obsahuje přemostovací prvek, který dvě nebo více sítí propojuje. Uvažme možnost, kdy pro jednu skupinu zvolíme sadu adres 192.168.1.1 až 192.168.1.99 a pro druhou skupinu zvolíme sadu adres 192.168.1.100 až 192.168.1.199. V tomto případě se jedná o tutéž síť LAN, pokud mezi ně vložíme jeden nebo více směrovačů nebo mostů, které jsou inteligentními internetovými přepínači, pak se jedná o dvě různé síť typu LAN. Tato skutečnost je více patrná z fyzické vzdálenosti prvků, nebo když jsou mezi ně vloženy přepínače.

WAN je pojem, který popisuje síť na velké vzdálenosti a propojení více sítí. Jedná se o označení libovolní sítí sítí. Internet je nejznámější sítí WAN. Síť WAN lze dále dekomponovat na menší celky, například na síť CAN a MAN, kdy síť CAN popisuje propojení sítí v rámci budov a síť MAN popisuje propojení sítí v rámci měst. Tyto velké a geograficky rozptýlené síť využívají optická vlákna se zesilovači signálu k přenosu dat. (Horák & Keršláger, 2016) (Sosinsky, 2010)

3.3 Druhy přenosů a topologie počítačových sítí

3.3.1 Druhy přenosů

V počítačových sítích se v zásadě používají dva druhy přenosů: bodová komunikace od uzlu k uzlu a všesměrová komunikace.

3.3.1.1 Bodová komunikace

Komunikace point-to-point, neboli přímá komunikace mezi uzly je založena na jednoznačné identifikaci propojení dvou systémů sítě. Jsou zde známe prvky jako vysílací a přijímací systémy. Nemusí se jednat pouze o propojení dvou systémů, ale také zde může existovat jeden či více mezilehlých systémů, které využívají a zpracovávají datový tok na zamýšlené trase. Drtivá většina sítí point-to-point obsahuje nadbytečné trasy, které jsou často rozdílné délky, a proto pro efektivní využívání toků jsou nezbytné směrovače.

K realizaci bodových sítí se používají různé technologie, typickým příkladem může být propojení mezi více podsítěmi pomocí linky, jako je tomu například u sítě WAN. (Sosinsky, 2010)

3.3.1.2 Všesměrová komunikace

Příkladem všesměrové komunikace může být satelitní síť. Ta přijme zprávy od vysílajícího zařízení a rozešle všem ostatním systémům v síti. Pokud se v síti objeví určitá konfigurace o zaslání signálů určité množení uzlů, pak se jedná o proces zvaný vícesměrové vysílání (multicasting). Tento obvyklý způsob je používat pro zasílání mediálních toků, jelikož je zde uplatněn princip, kdy více koncových zařízení přijímá stejný datový tok.

Pakety, které všesměrová komunikace zasílá, obsahují adresu systému, nebo skupiny systému, kterým je komunikace určena. Cílovým uzlem může být jediný počítač, nebo skupina počítačů. V tomto druhu komunikace každý přijme paket, který dále zkoumá, pokud se adresa systému shoduje s adresou příjemce v packetu, pak je nadále packet zpracováván, v opačném případě je ignorován a zahozen. (Sosinsky, 2010)

3.3.2 Topologie

Dalším faktorem, pomocí kterých se klasifikuje síť, je topologie. Topologie nám popisuje seskupení či seřazení síťových prvků, a to nejen zařízení, ale také jejich propojení. Vše, co obsahuje síťovou adresu, je považováno za síťový element, který je potřeba zahrnout do popisu topologie.

Síť může být posuzována ze dvou hledisek, z fyzické topologie a logické topologie. Fyzická topologie se zabývá vztahy mezi fyzickými zařízeními, naopak logická topologie se zabývá popisem jednotlivých vztahů nebo hierarchie funkčních složek. Dále existuje kombinace těchto dvou topologií, která se nazývá hybridní topologie.

3.3.2.1 Fyzická topologie

Fyzická topologie nám popisuje fyzické vztahy mezi zařízeními. Z hlediska fyzické topologie jsou zařízeními myšleny nejen uzly, nebo koncové prvky sítě, ale také jednotlivé spoje a propojení. Sítě nejsou striktně daného typu, ve skutečnosti jsou sítě kombinací různých topologií.

Fyzické topologie jsou:

- **Topologie sběrnice** – Topologie sběrnice funguje na principu jednoho spojení mezi dvěma koncovými uzly. Právě na tomto spojení jsou připojené ostatní uzly. Paket putuje po této trase od jednoho uzlu k následnému uzlu v případě, pokud paket nenašel svůj cílový uzel. Pokud ho již našel, uzel ho neposílá dále. Toto chování má za následek zpožděného doručení paketu, ale v moderních sítích je zpoždění nepatrné. V této topologii existují prvky zvané terminátory, které napomáhají logickému odlišení uzlů. Terminace je proces, při kterém je signál ze sítě pohlcen a již se neposílá dále.
- **Topologie hvězdy** – Tato topologie je v praxi velice využívána. V této topologie je centrální prvek, ze kterého odbočují jednotlivé spoje k ostatním uzlům. Centralizace této topologie má za následek průchod všech dat právě centrálním prvkem, který rozhoduje, jakým směrem se data vydají. Topologie rozšířené hvězdy a distribuované hvězdy je spojení více hvězd

v jednu topologii. Nelze zde zcela určit centrální spojení, proto jsou si všechny hvězdy rovnocenné.

- **Topologie kruhu** – Principem topologie kruhu je uzavřená smyčka. Tento efekt má za následek, že každý uzel je jak počátečním, tak i koncovým uzlem datových přenosů. Přenos datových toků probíhá pouze jedním směrem, pokud by byla obousměrná komunikace, mělo by to za následek kolize paketů a interference. Topologie dvojitého kruhu nabízí obousměrnou komunikaci, ale také druhý kruh se dá využít jako řídicí kanál nebo jako záložní kanál.
- **Topologie spleti** – V této topologii může být uzel propojen s libovolným počtem jiných uzlů. Tato topologie může být buď částečně propojena, tzn. že každý uzel nemá fyzické propojení se všemi uzly, nebo úplně propojena, kdy naopak každý uzel má fyzické spojení se všemi ostatními uzly, ovšem toto propojení je velice nákladné. V této topologii je nutné inteligentní směrování z důvodů mnoha cest z počátečního uzlu ke koncovému uzlu. Na této topologie funguje Internet.
- **Topologie stromu a hierarchické sítě** – Ve stromové topologii je uzel (kořen) nejvyšší úrovně, k tomu jsou připojeny uzly druhé úrovně. K uzlům druhé úrovně jsou následně připojeny uzly třetí úrovně a ty mohou být koncové nebo se mohou dále rozšiřovat. Musí existovat minimálně tři úrovně dělení, pokud by neexistovali, pak by se jednalo o topologii hvězdy. (Bouška, 2007) (Horák & Keršláger, 2016)

3.3.2.2 Hybridní topologie

Uvedené topologie v kapitole 3.3.2.1 se nadále mohou kombinovat a prolínat, proto název hybridní topologie. V jediném uspořádání dostáváme více složitosti, ale také flexibility, jak nejeфекtivněji využívat výhody jednotlivých topologií.

Příklady hybridních topologií jsou:

- **Hvězdicová sběrnice** – principem této topologie je připojení jedné, nebo více hvězdic k jedné sběrnici. Řetěz uzlů je zakončen dvěma, nebo více

rozbočovači, pomocí kterých probíhá spojení s jiným rozbočovačem v jiné hvězdici.

- **Hierarchická hvězda** – hlavní myšlenka této hybridní technologie je ta, že každý uzel stromové struktury se stává rozbočovačem, ze kterého se odvětvují další periferní spojení, které tvoří hvězdy. Neexistuje žádná sběrnice, která by spojovala hvězdy, existuje zde pouze bodová výše jednotlivých hvězd. Kořenový uzel je často propojen vysokorychlostním páteřním spojem.
- **Hvězdicový kruh** – tato hybridní síť se skládá z rozbočovače a periférií, které jsou připojené k tomuto rozbočovači. Signály jsou šířeny na všechny dostupné periferie, tím je simulována topologie kruhu.
- **Hybridní splet'** – jedná se o kombinaci spleti s jedním nebo více uzly spleti, připojených k jiným topologiím. (Sosinsky, 2010)

3.3.2.3 Logická topologie

Logická topologie nezohledňuje fyzické zapojení jednotlivých prvků sítě, ale mapuje trasu, kterou musí datové pakety překonat od jednoho uzlu k druhému uzlu. Logickou topologii lze sestavit v případě, kdy jsou uzly v síti dostupné pomocí protokolů určených k výměně dat. Každý prvek v síti tedy musí mít jednoznačné identifikační číslo, které zajišťuje dostupnost prvku v síti. Jedná se o MAC adresu, která umožňuje daný uzel v síti rozpoznat. Virtuálním síťovým rozhraním se také přiděluje MAC adresa. Příklady logických topologií:

- **Logická topologie řetězu** – Tato topologie řetězu může být realizována dvěma způsoby, buď jako přímý nebo jako uzavřený kruh. Pokud přidáme nový systém do přímého řetězu, pak nově přidaný systém musí obsahovat jak vysílač, tak i přijímač, kdežto koncová zařízení mají jen jednu z těchto dvou vlastností. V kruhovém řetězu se data mezi uzly posílá pouze jedním směrem, tedy všechna zařízení si vystačí s jedním vysílačem a jedním přijímačem.
- **Logická topologie hvězdy** – Tvar hvězdy neexistuje pouze ve fyzické topologii, ale také v logické, kdy centrální uzel všesměrově vysílá signál,

který prochází jedním uzlem do všech uzlů v dané síti. Potvrzení signálu cílovým zařízením umožňuje pak samotný přenos dat. Hvězdy se dále dělí na aktivní a pasivní. V pasivní hvězdě musí být vysílací zařízení schopné rozpoznat odraz svého vlastního signálu, v aktivní hvězdě je centrální uzel vybaven obvody, které zabraňují odrazu signálů zpátky vysílajícímu zařízení. Existence směrové tabulky zjednodušuje přenos dat přímo do cílové destinace.

- **Logická topologie spleti** – základní charakteristikou této topologie jsou vícečetné trasy mezi dvojicí uzlů. Mřížkové sítě jsou vysoce distribuované spletité sítě, které jsou uspořádané do přímých nebo kruhových útvarů. Logická topologie spleti může být jako u fyzické spleti buď úplně nebo částečně propojená. V praxi se využívají částečně propojené z důvodů vysokých nákladů na úplné propojení. (Sosinsky, 2010)

3.4 Přenosová média

V této kapitole budou popsány tři typy přenosových spojení: měděnými dráty, optickými kabely a bezdrátovými spoji. Tato spojení se používají k propojení jednotlivých komponent sítě.

3.4.1 Kabelová média

Fyzické vrstvě sítě není tolik věnována pozornost, avšak životnost kabelů, která se pohybuje mezi 10 až 15 lety, je tedy nutné uvažovat i o vhodnosti media v budoucnosti. Běžně se používají tyto čtyři kabelová média: kroucená dvojlinka, koaxiální kabel, ethernet a optická linka. Tyto media budou dále popsána v jednotlivých podkapitolách. Základním rozdílem mezi těmito kabely je jejich rychlost spojení, šířka pásma a možnost použití v dané topologii. (Klimeš, 2003)

3.4.1.1 Kroucená dvojlinka

V této době je kroucená dvojlinka nejvíce využívanou kabeláží k propojení počítačové sítě. Lze přenášet jak analogový signál, tak i digitální. Principem je dvojice zakroucených párů, kdy k přenosu se využíval pouze jeden kabel u telefonních linek, druhý nevyužívaný kabel umožnil zavést technologie typu ADSL nebo ISDN. Kroucený drát má tu výhodu, že průměruje vliv externích magnetických a elektrických polí, čím snižuje riziko interferencí signálů. Výhodou jsou nízké pořizovací náklady.

Jsou dva základní typy kabelů: STP (stíněná kroucená dvojlinka) a UTP (nestíněná kroucená dvojlinka). V kabelech typu STP jsou pouze dva páry drátů, které jsou obtočeny kolem sebe a stínění se skládá buď z folie (označení FTP) nebo pleteného drátu. UTP kabel je sestaven z páru měděných drátů, které jsou kolem sebe obtočené, ale jednotlivé páry nejsou izolované. Právě tento kabel je používán v ethernetových sítích a telefonních linkách z důvodů nižších nákladů a lepší manipulace oproti STP. Nejvíce se používá UTP kabel CAT 5 (100 Mb/s–1 Gb/s) v síťových aplikacích a v telefonních linkách CAT 3 (16 Mb/s). (Roupec, 2002) (Koutná & Sochor, 2006)

3.4.1.2 Koaxiální kabel

Tento typ kabelu se využívá hlavně pro přenos televizního signálu. Jedná se o první typ kabelu, využívaný v ethernetových sítích, který vznikl v roce 1929 a stal se metodou pro přenos na dlouhé vzdálenosti. V 80. letech byly nahrazeny optickými vlákny. Jedná se o měděný drát (může být potažen stříbrem), kolem kterého je omotán dielektrický izolátor. K odstínění interferencí je využíván pletený drát nebo foliové balení. Vnější ochrana je tvořena pouzdrem z plastu nebo telefonu. (Roupec, 2002)

3.4.1.3 Ethernetový kabel

V ethernetových sítích má kabeláž zvláštní označení. Označení 100Base-T lze popsat takto. Zkratka BASE (anglicky baseband) je označení pro signál, který je šířen v rámci frekvenčního rozsahu, zkratka T označuje kroucenou dvojlinku (anglicky Twisted-Pair), kdy se používají čtyři páry, kterou jsou zakončené 8pinovým konektorem RJ-45. Osm pinů umožňuje 4 duplexní nebo 8 poloduplexních spojení. Původně byl Ethernet navržen pro

BASE-TX (TX je označení pro dvojitý koaxiální kabel). Zkratka 100 označuje ethernetovou technologii popsanou standart organizace IEEE, v tomto případě se jedná o standart 802.3.

Standartní zapojení pinu v ethernetovém kabelu jsou odpovídající čísla na stejném pinu po obou stranách (přenosový drát navazuje na přijímací drát a ten zase na přenosový). Tomuto zapojení se říká přímé zapojení. Křížené zapojení se používá, pokud neodpovídají čísla na stejném pinu po obou stranách. Podle běžného schématu se signál z jednoho počítače přenáší na pinech 1 a 2 a přijímá na pinech 3 a 6.

Z praktického hlediska se pro propojení mezi počítači (nebo síťová zařízení) využívá křížená dvojlinka. Pokud ovšem nejsou počítače propojené křížovým kabelem a jsou tedy propojené přímým spojem, moderní síťové karty umí softwarově vytvořit záměnu příchozích a odchozích pinů. Této vlastnosti se říká MDI-X. (Klimeš, 2003)

3.4.1.4 Optický kabel

Optický kabel, nebo také optické vlákno, je médium vyrobené z oxidu křemičitého, skla nebo plastu. První patent byl podán v roce 1934 firmou AT&T. Jednovidové vlákno nese pouze jeden signál, vícevidové vlákno je schopno přenášet více signálů najednou, ale hlavním problémem vícevidového vlákna je nízký efekt dosahu z důvodů rozprostírání signálů v čase podle rychlosti šíření signálu, a to v různých videch (módech) přenosu.

Optický přenos se skládá ze zdroje světla, kabelu a detektoru. Zdroj vysílá pulzy, které jsou zachyceny detektorem. Absence signálu je 0 a zachycený signál je 1. Čím rychleji lze zdroj světla zapínat a vypínat, tím je větší obsah přenesených dat. Světlo cestuje skrz kabel, kdy se odráží od hranic mezi vrstvami s rozdílným indexem lomu.

Optické kabely neovlivňují elektromagnetické nebo radiové frekvence, ale z důvodů použití skla jsou tyto kabely velice křehké. Budování této sítě je velice obtížné a nákladné. (Donahue, 2009)(Sosinsky, 2010)

3.4.2 Bezdrátové sítě

Kabely a dráty nejsou jediným způsobem přenosu dat. Data lze posílat i vzduchem, které jsou převedeny do elektromagnetického záření pomocí tří druhů základní modulace:

- **Pulzní modulace** – signál se tvoří pouhým zapínáním a vypínáním zdroje.

- **Amplitudová modulace** – signál je tvořen změnami amplitudy, pokud je nad jistou prahovou hodnotou, pak je přenášena logická jednička.
- **Frekvenční modulace** – signál se skládá z proměnlivé frekvence vln, pokud je nad jistou prahovou hodnotou, pak je přenášena logická jednička.

Bez ohledu na použitou modulaci musí bezdrátový spoj obsahovat tyto tři složky: vysílač, přijímač a přenosové médium. Přenosové médium je prakticky ve všem případech vzduch nebo vakuum. Přijímač a vysílač musí být konstrukčně řešet tak, aby byly běžné použitelné a cenově dostupné. Vysílač emituje elektromagnetické záření s jistou frekvencí a energií. Amplituda vlny musí být tak velká, aby přijímač rozpoznal přenášený signál na požadovanou vzdálenost. (Zandl, 2003)

3.5 Přístupové metody

Z přehledu topologií v kapitole 3.3.2 tedy plyne, že neexistuje mezi každým párem počítače jedinečná cesta, která by byla k dispozici. S výjimkou topologie úplné spleti, kde každý počítač je propojen s každým. Z důvodů nepropojení všech počítačů se všemi, pak nastává situace, kdy jednu cestu budou muset využívat dva a více uzlů k vysílání. Je nutné vymyslet strategii pro přidělování přenosové kapacity, tyto metody se označují jako metody řízení přístupu. (Roupec, 2002)

3.5.1 Metody statického přidělování

Metoda statického přidělování pevně rozděluje přenosovou kapacitu pro jednotlivé účastníky komunikace. (Sosinsky, 2010)

3.5.2 Metody centrálního přidělování

V této metodě existuje zařízení, které má pravomoci přidělovat přenosovou kapacitu jednotlivým účastníkům komunikace za pomoci dvou metod. Metoda žádosti, kdy počítač musí vyslat žádost centrálnímu zařízení o využití přenosové cesty. Tato žádost se vysílá na služebním kanále. Druhou metodou je metoda výzvy, kdy se centrální prvek periodicky dotazuje účastníků komunikace, zda chtějí vysílat. (Horák & Keršláger, 2016)

3.5.3 Metody náhodného přidělování

Tato metoda je založena na obrovské pravděpodobnosti vytváření náhodných požadavků účastníků komunikace na využití přenosové komunikace. Je tedy výhodné poskytnout zařízení okamžité vysílání a nezdržovat se s řízením přístupu. V této metodě může docházet ke kolizím, kdy v jednom okamžiku mohou vysílat dva a více účastníků najednou. Používá se v síti, kdy se signál ve velice krátkém čase dostane ke všem účastníkům komunikace.

- CSMA/CD – Vysílající počítač stále sleduje signál v síti, zda je jeho či nikoliv. Pokud tomu tak není, vyhodnotí tuto situaci jako kolizi a upozorní na kolizi speciálním signálem nazývaným jam (charakter jako šum). Po tomto signálu každý uzel vyčká náhodnou dobu a poté se pokus o vysílání opakuje. Náhodné zpoždění se generuje algoritmem binárního exponenciálního odpočítávání. Pokud se opakovaně vyskytne kolize a nepodaří se data odvyšlat, další pokusy se nekonají a je ohlášena chyba spojení. Tato metoda se používá v síti Ethernet.
- CSMA/CA – tato metoda se nezabývá problémem kolizí. Je zde poslán paket před začátkem přenosu dat, který určitý čas poslouchá a sleduje, zda je přenosové medium volné. Pokud je přenosové medium volné, zahájí uzel vysílání, pokud není, počká na konec právě probíhajícího vysílání. Tato metoda se využívá například u bezdrátových sítí standardu 802.11, kdy zařízení při volném mediu vyčká po dobu náhodně zvoleného času. Po uplynutí této doby zkontroluje dostupnost přenosového media a pokud je volné, začne vysílat. (Roupec, 2002) (Sosinsky, 2010)

3.5.4 Metody distribuovaného přidělování

Vlastnosti tohoto přidělování lze ukázat na metodě Token Ring, která se využívá v kruhové topologii. V této topologii běhá tzv. token od jednoho uzlu k následujícímu. Pokud si uzel přeje vysílat, musí počkat na token a následně pak poslat rámec dat místo něj. Jediný token v tomto kruhu zabraňuje tvorbě kolizí. Po odvyšlání celého rámce je opět token vyslán. (Sosinsky, 2010)

3.6 Hardwarové prvky počítačové sítě

V této kapitole budou popsány jednotlivé propojovací zařízení v síti, které vytvářejí okruhy. Je nutné si vysvětlit dva základní typy sítí, které existují. Jsou to sítě na bázi přepínání okruhu a sítě na bázi přepínání paketu.

V prvním případě se jedná o stavový systém, kdy mezi počátečním a koncovým zařízením je definován fyzický nebo virtuální okruh (spoj). Okruh se může v závislosti na okolních podmínkách změnit a tím změnit na nový okruh, po kterém se pakety budou přenášet. Klasickým příkladem stavové komunikace je telefonní hovor, na kterém lze ukázat atributy, které stavová komunikace obsahuje. Ty jsou:

- Zdroj
- Cíl
- Trasa okruhu
- Náklady na trasu z hlediska času, výkonnosti nebo jiných atributů.

Naopak druhý případ je bezstavový, kdy každý paket vybírá cestu podle okolních podmínek ke svému cíli a hledá nejlepší trasu po které se má vydat. Využívá se to u nespolehlivé sítě, jelikož spojení jsou pouze přechodná. Pakety se mohou dostat do slepé uličky a budou ztraceny nebo vráceny ke zdroji. Pokud se dostanou ke svému cíli, nemusí být pakety správně seřazeny, je tedy nutné pakety číslovat. Je nutné doplnit mechanismy, které rekonstruuji data v případě nesprávného pořadí, či ztracení jisté části dat. Druhy přenosu bezstavové komunikace lze odvodit z těchto atributů:

- Zdroj
- Cíl
- Pozice paketu v řadě
- Životnost paketu

Přepínání paketů má své výhody a nevýhody oproti přepínání okruhů. V síti s přepínáním paketů daleko efektivněji využívají kapacitu sítě, naopak v sítích s přepínáním okruhů je jistota doručení celé zprávy a ve správném pořadí pakety. (Roupec, 2002)

3.6.1 Sběrnice pro síťové karty

Síťová rozhraní mají mnoho podob. Běžné síťové karty jsou dostupné v integrovaných obvodech umístěných na:

- Základní desce počítače
- Doplnkových kartách pro běžné rozšiřující sběrnice
- Předmětech s rozhraním pro periferní sběrnice (USB)
- Zařízeních schopných bezdrátového spojení, založeného na protokolu 802.11x nebo Bluetooth

Tyto integrované obvody tvoří hranici mezi počítačem a počítačovou sítí. Musí být schopna přijímat a odesílat signály. Síťové karty jsou buď elektrické nebo optické. Každá síťová karta má svůj jedinečný 48-bitový identifikátor, kterému se říká MAC adresa. Uživatelé v domácí prostředí se nejčastěji setkávají se síťovou kartou, která je vybavena ethernetovým konektorem RJ45. (Koutná & Sochor, 2006)

3.6.2 Zařízení první a druhé vrstvy

3.6.2.1 Pasivní rozbočovače

Jedná se o zařízení, které propojuje uzly ve stejném segmentu, často jen prostřednictvím kabelu z kroucené dvojlinky nebo optickým kabelem. Jedná se o fyzické propojení, pokud je již signál zesílen, pak se jedná o aktivní rozbočovač.

Síťové rozbočovače mají vlastnost větvení, mohou tedy vytvářet nové segmenty sítě. Jedinou vstupní linku lze propojit se čtyřmi, osmi a více spoji a každá tato cesta tvoří nový segment. Pokud pouze posílá signál dále, jedná se o pasivní rozbočovač, pokud ho zesiluje, jedná se pak o aktivní rozbočovač. (Horák & Keršláger, 2016)

3.6.2.2 Opakovače

Opakovače jsou aktivní rozbočovače. Jejich hlavním úkolem je rozšířit dosah fyzického média za pomoci zesílení a synchronizace signálů. Vytvoří nový signál ve stejné frekvenci a ten pak přešle dále. Nelze však propojovat různé sítě postavených na

různých architekturách a také nemohou filtrovat informace. Ethernet umožňuje dostatečnou vzdálenost vedení, proto není nutný v sítích LAN.

Naopak bezdrátové sítě mají pouze omezený dosah svého působení, zde je nutnost použití opakovačů, které šíří bezdrátový signál dále. Pak se jedná ve skutečnosti o přístupový bod v takzvaném opakovacím režimu. (Koutná & Sochor, 2006)

3.6.2.3 Přepínače

Přepínač nebo také switch je aktivní zařízení, které spojuje dvě sítě na jedné nebo více vrstvách síťového modelu. Na rozdíl od mostu (je kodifikován standardem IEEE 802.1D) není žádná pevná definice přepínače. Jedná se více méně o marketingový tah a často se používá jako rozbočovač, opakovač nebo most. Přepínače rozdělují komunikaci mezi segmenty sítě. Každý segment na svoji vlastní šířku pásma a tím i svoji kolizní doménu. Z důvodů neexistence definice vlastností přepínače, existují také přepínače, které pracují od druhé (linkové) vrstvy až po sedmou (aplikační) vrstvu síťového modelu OSI. (Klimeš, 2003)

3.6.2.4 Mosty

Nebo také bridge je zařízení, které spojuje dva síťové segmenty na druhé linkové vrstvě OSI. Mosty se zabývají fyzickou adresou (MAC adresa) síťového provozu. Most funguje jako adaptivní zařízení tzn., že porovnává MAC adresu z hlavičky paketu a porovnává ji s interní tabulkou MAC adres. Pokud nalezne záznam, pošle ho danému zařízení. Pokud záznam nenalezne, pošle packet všesměrově a čeká na odpověď, po doručení odpovědi most aktualizuje svoji interní tabulku MAC adres. Dnes všechny prodávané prvky typu most, jsou ve skutečnosti přístupovými body k bezdrátové síti, které jsou schopny přemostit dva nebo více segmentů. V standartních kabelových sítích současné přepínače fungují na druhé vrstvě v módu bridging mode, tedy opět je zde patrné sjednocení pojmu most a přepínač, kdy v tomto smyslu jsou synonymem. (Horák & Keršláger, 2016) (Sosinsky, 2010)

3.6.3 Směrovače

Směrovač je zařízení v počítačové síti, které pracuje na třetí (síťové) vrstvě modelu OSI, velice často je označován za přepínač na třetí vrstvě. Rozdělují kolizní doménu, filtrují, blokují všesměrové vysílání a zajišťují nejlepší trasy pro posílání paketů. V angličtině se využívá slovo *brouter*, kdy se jedná spojení slova *bridge* a *router* do jednoho z důvodu fungování směrovače. Pokud do směrovače přijdou pakety TCP/IP, pak *brouter* s nimi bude zacházet jako směrovač, pokud dorazí pakety založené na nesměrovaném protokolu, pak s nimi *brouter* naloží jako most.

Nyní budou popsány dvě operační úrovně, na které směrovač pracuje. Jedná se o úroveň řídicí a doručovací.

Řídicí úroveň obsahuje směrovací tabulka adres, která se vytváří dvěma způsoby. Doplňit cestu staticky nebo ve většině případů se využívá dynamický režim, kdy směrovače si navzájem vyměňují logické informace síti navzájem.

Doručovací úroveň má na starost kontrolu vstupních paketů, které pak následně pošle na správném odchozím rozhraní. Při tomto procesu se hledá v tabulce záznam, který obsahuje daný síťový identifikátor nebo adresu MAC. (Sosinsky, 2010)

3.6.4 Brány

Síťová brána je zařízení nebo program, pomocí které mohou komunikovat různé typy sítí, protože překládají adresy, síťové protokoly i samotná data. Jedná se buď o hardwarové zařízení nebo o software, které se nainstaluje na daný počítač, ten pak bude fungovat jako brána. Příkladem takové brány je *firewall* nebo *proxy server*. V TCP/IP je pro každé rozhraní definována brána. Hlavní odlišností brány od ostatních síťových zařízení je její působnost, kde brána pracuje. V referenčním modelu OSI se brány vyskytují buď ve čtvrté (transportní) vrstvě nebo častěji až v sedmé (aplikační) vrstvě. (Horák & Keršláger, 2016) (Sosinsky, 2010)

3.7 Síťový zásobník

Pod síťovým zásobníkem rozumíme model a architekturu, která popisuje transakce mezi dvěma systémy. Důvodem vzniku těchto modelů je standardizace. Právě tato možnost umožňuje vzájemné komunikaci mezi síťovými komponentami pracujícími na různých úrovních. V této kapitole budou popsány dva nejdůležitější síťové modely současnosti: první model je OSI od společnosti ISA a TCP/IP neboli internetový model. (Sosinsky, 2010)

3.7.1 Model ISO/OSI

Tento model je sám o sobě ten nejdůležitější ze všech síťových modelů, rozděluje komunikaci v síti do sedmi různých vrstev, které si mezi sebou vyměňují data. Každá vrstva, v průběhu odesílání dat, obaluje dalšími operaci a při přijímání naopak. Tento model definuje sedm vrstev číslovaných 1 až 7 v tomto pořadí: fyzická, linková, síťová, transportní, relační, prezentační, aplikační. Tyto vrstvy budou popsány v dalších podkapitolách.

V praxi je velice vzácné setkat se sítí postavenou přesně na tomto modelu, avšak se jedná o nejpoužívanější model k popisu síťových technologií. Například většina moderních zařízení je vybavena modelem TCP/IP, ten vychází z modelu OSI.

Při jakékoliv komunikaci musí být zajištěno, že data určená k odeslání projdou celým modelem od shora dolů. Tato akce se vyvolá určitým příkazem z I/O zařízení, nebo jiným druhem události. Tento požadavek začíná v aplikační vrstvě, který se postupně dostane na vrstvu fyzickou, která data pošle do jiného systému. Je důležité říct o komunikaci mezi vrstvami, kdy každá vrstva komunikuje se svým „sousedem“ tzn. třetí vrstva komunikuje se čtvrtou a druhou vrstvou. Pro korektní odeslání dat příjemci, musí být s daty připojena hlavička s dalšími informací, mluvíme o metadatech (data o datech). V každé vrstvě se připojí hlavička obsahující informace z dané vrstvy. Postupnému připojování hlaviček se říká zapouzdření. Na data se aplikují kontrolní algoritmy CRC. Při dosažení dat ke svému cíli je tento algoritmus spuštěn pro kontrolu správnosti přenosu dat. V případě nekorektnosti dat, jsou data poslána znovu. V každé vrstvě je sada protokolů, které je schopna komunikovat v horizontálním směru se stejnou vrstvou v jiném systému.

Technicky lze říci, že vrstvy nevědí, co dělají protokoly na ostatních vrstvách, už jen z důvodů, protože vrstva nepřečte hlavičku určenou jiné vrstvě. (Sosinsky, 2010) (Horák & Keršláger, 2016)

3.7.1.1 Fyzická vrstva

Fyzická vrstva s číslem 1 je nejnižší vrstvou v OSI modelu. Tato vrstva je odpovědná za přenos informací z jednoho systému do druhého. V této vrstvě je nutné nastavit formu pro reprezentaci dat při přenosu. K tomu se využívá booleovské hodnoty 1 a 0. Zařízení musí obsahovat potřebné elektrické komponenty k přenosu dat. Nejpoužívanější média na fyzické vrstvě jsou měděné kabely, optické kabely nebo forma radiové komunikace. (Peterka, Referenční model ISO/OSI - sedm vrstev, 1992)

3.7.1.2 Linková vrstva

Linková vrstva s číslem 2 obsahuje algoritmy pro určení cest komunikace, kterými budou data putovat. Na této vrstvě probíhá segmentace dat na menší kousky (tvoření rámců pro přenos) a jsou zde označovány začátky a konce segmentů. Jednotlivé segmenty vytvoří sekvence rámců. Linková vrstva musí zajistit správné seřazení těchto rámců pro přijímací zařízení. Linková vrstva řeší problémy duplicity rámců, jejich poškození, popřípadě jejich ztracení. Z přijímacího zařízení jsou odesílateli zaslány potvrzovací rámce o správnosti komunikace. Tato vrstva také spravuje využití rychlosti sítě. (Peterka, Referenční model ISO/OSI - sedm vrstev, 1992)

3.7.1.3 Síťová vrstva

Síťová vrstva s číslem 3 obsahuje funkce k řízení a směrování tras mezi jednotlivými sítěmi. Je zde také správa datového toku, které zabraňuje zahlcení sítě příliš mnoha pakety. Logika toků je závislá na směrovacích trasách, které jsou výsledkem směrování.

V přepínacích sítích má směrování stěžejní úlohu, možnost dynamicky měnit trasu paketu je výhodou, která se přizpůsobuje změnám v síti. Směrovače si nechávají trasy ve směrovacích tabulkách a podle toho se rozhodnout najít tu nejoptimálnější cestu. Tuto vrstvu nalezneme jak v modelu OSI ale i na Internetu, v případě broadcastu (všesměrového

vysílání) není tato vrstva potřebná. (Peterka, Referenční model ISO/OSI - sedm vrstev, 1992)

3.7.1.4 Transportní vrstva

Transportní vrstva s číslem 4 má za úkol propojovat síťovou vrstvu s relační vrstvou. Relační vrstva má za úkol předat data ve správném formátu a velikosti síťové vrstvě. V opačném směru zajistí korektní seřazení přijatých a rekonstrukci relačních informací. Na této vrstvě rozpoznáváme spojované (protokol TCP) a nespojované (protokol UDP) zasílání. Role této vrstvy spočívá v oddělení síťové a relační vrstvy z důvodu jejich charakteru. Zatímco síťová je hardwarového charakteru, relační je již softwarová.

- TCP protokol – je spojový způsob zasílání dat, kde pracuje s virtuálními okruhy. Předpokládá tedy spojení mezi odesílatelem a příjemcem. Každá spojení obsahuje svoje ID.
- UDP protokol – je nespojový způsob zasílání dat, kde jednotlivé datagramy se přenášejí nezávisle na ostatních datagramech. (Peterka, Referenční model ISO/OSI - sedm vrstev, 1992)

3.7.1.5 Relační vrstva

Relační vrstva s číslem 5 obsahuje prostředky pro vytvoření a udržení relací mezi koncovými účastníky komunikace. Na této vrstvě se k datům připojují kontrolní body nebo oddělovače. Za pomoci těchto vlastností není nutné opakovat přenos dat v případě přerušení komunikace a obnovit komunikaci v bodě přerušení. Také je zde prováděna synchronizace dat mezi komunikujícími zařízeními. Na této vrstvě se provádí autentifikace uživatelů a zabezpečuje přístup k zařízení. (Peterka, Referenční model ISO/OSI - sedm vrstev, 1992)

3.7.1.6 Prezentační vrstva

Prezentační vrstva s číslem 6 obsahuje algoritmy pro formátování a šifrování dat z aplikační vrstvy. Tyto algoritmy jsou nutné z důvodu různorodosti datových typů z aplikační vrstvy. Algoritmy převedou data do takové podoby, mohla být předána jiným

standardizovaným systémům. Jsou zde použity protokoly pro překonání rozdílů mezi operačními systémy.

Při opačné komunikaci jsou data dekomprimována a dešifrována pro aplikační vrstvu. (Peterka, Referenční model ISO/OSI - sedm vrstev, 1992)

3.7.1.7 Aplikační vrstva

Aplikační vrstva s číslem 7 a je nejvyšší vrstvou v modelu OSI. Jedná se o vrstvu, která je v přímém styku s uživatelem. Jedná se například o webové prohlížeče, e-maily, CLI apod., ale není pravidlem, že každý program pracuje na aplikační vrstvě (např. Microsoft Word má moduly pracující i na jiných vrstvách – síťový tisk). Software na aplikační vrstvě je často označován ze terminál, z důvodu přístupu uživatelům k jednotlivým systémům, jeho informacím, spouštění příkazů apod.

Právě na aplikační vrstvě se vyskytuje nejvíce síťových protokolů, kterými jsou:

- HTTP – protokol pro webové prohlížeče a webové servery.
- FTP – protokol na stahování a nahrávání souborů.
- SMTP – protokol pro přijímání e-mailové pošty.
- POP – protokol pro odesílání e-mailové pošty.

Toto je výčet příkladů protokolů na aplikační vrstvě. (Sosinsky, 2010)

3.7.2 Model TCP/IP

Alternativou pro model OSI je druhý nejznámější model TCP/IP, který je v dnešní době nejvíce používaný a rozšířený model síťového zásobníku. Tento model se používá ve všech sítích LAN. V tomto modelu jsou obsaženy tři protokoly na přenos dat. Protokol TCP, který se používá pro spojové zasílání dat. Protokol UDP, kterým se zajišťuje nespojovaná komunikace, a konečně nový protokol IP, který definuje formát paketů při přenosu. TCP a UDP protokol jsou obsaženy v transportní vrstvě a protokol IP v síťové vrstvě. Rozdíl oproti modelu OSI je v počtu vrstev. V tomto modelu jsou čtyři vrstvy oproti sedmi v modelu OSI. První a druhá vrstva v modelu OSI přibližně korespondují s vrstvou Hostitelské rozhraní v modelu TCP/IP. Síťová vrstva v modelu OSI odpovídá Internetové vrstvě v TCP/IP. Čtvrtá vrstva modelu OSI existuje i v TCP/IP ovšem je sdružena s relační vrstvou do jediné. Stejně tomu je se šestou a sedmou vrstvou z modelu

OSI, které jsou v TCP/IP modelu spojené do jedné, které se říká Aplikační vrstva. (Libor dostálek, 2000)

3.8 Protokoly TCP/IP

V tomto modelu se víceméně nezabývá první a druhou vrstvou. Tyto dvě vrstvy využívají protokoly z modelu OSI.

3.8.1 Internet protokol

Dále se bude označovat jako IP-protokol, je obsažen v síťové vrstvě. Tento protokol má za úkol přenášet IP datagramy mezi vzdálenými počítači, kdy každý datagram obsahuje adresu příjemce, jinak řečeno, datagram obsahuje úplnou směrovací informaci adresáta. Z tohoto důvodů může síť sama přenášet IP-datagramy. Tento samostatný přenos má nevýhodu, datagramy mohou příjemci dorazit v jiném pořadí.

Jsou zde určitá pravidla, ale jedno z nejdůležitějších je, že každá stanice musí mít originální číslo v daném segmentu sítě. Tato adresa se skládá ze čtyř segmentů oddělených tečkou obsah těchto segmentů je složen z čísel dvojkové abecedy (např. 192.168.1.1). tato adresa se skládá z dvou částí:

- Adresa sítě – první část adresy, kterou odděluje správce IP adres (např. 192.168.x.x)
- Adresa uzlu – druhá část adresy, přidělena správcem sítě (např. x.x.1.1)

Velikost těchto dvou částí nám udává tzv. maska sítě, která rozděluje síť na jednotlivé podsítě. Jedné se o 32-bitové číslo, které obsahuje jedničky z levé strany, až do čísla síťového rozhraní. V této době existují dva protokoly, IPv4 a modernější IPv6, které má za úkol nahradit IPv4 z důvodů blízkého vyčerpání adres z tohoto protokolu. Dělí se na dvě části: prefix a identifikátor rozhraní. (Libor dostálek, 2000)

3.8.2 Protokoly TCP a UDP

Protokol TCP je protokolem vyšší vrstvy na rozdíl od protokolu IP. TCP protokol přebere data od vyšší vrstvy, rozdělí je na segmenty, očísluje a seřadí podle pořadí v jakém

se mají odeslat. Samotný protokol IP přenáší data mezi počítači v Internetu, kdežto protokol TCP přenáší data mezi konkrétními aplikacemi. Jak již bylo řečeno v kapitole 3.7.1.4, protokol TCP je spojovanou službou, tzn. vytvoření virtuálního spojení mezi dvěma běžícími aplikacemi, které si mohou duplexně vyměňovat data. Každý jednotlivý bajt je číslován, a integrita dat je kontrolována kontrolním součtem. V případě poškození nebo ztracení dat jsou data vyžádána znovu. O samotný přenos dat se stará síťová vrstva.

Protokol UDP je alternativou protokolu TCP. Má na starost ty samé činnosti s tím rozdílem, že se jedná o nespojovanou službu, tzn. že nenavazuje spojení. Odesílatel odešle příjemci UDP datagram, ale už se nestará, zdali datagram došel či nikoliv. O tento problém se stará aplikační vrstva. (Libor dostálek, 2000) (Sosinsky, 2010)

3.8.3 Aplikační protokoly

3.8.3.1 Protokol HTTP

Je protokol, které se využívá pro komunikaci mezi WWW server a jejich klienty (browser). Tento protokol je určen pro přenos hypertextových dokumentů v tom samém formátu v nezabezpečeném prostředí. Obvykle je pro tento protokol vybrán port 80 naopak port 443 je pro HTTPS, který komunikuje v zabezpečeném prostředí. Jedná se o protokol http, který spolupracuje s protokolem SSL nebo TLS. (Peterka, 1998)

3.8.3.2 Protokol SMTP

Protokol SMTP je určen pro přenos elektronické zprávy a MTA (program pro přepravu elektronické pošty v Internetu), jako je například Microsoft Exchange Server. Protokol zajišťuje přímé spojení mezi odesílatelem zprávy a adresátem zprávy. V praxi to znamená, že zpráva je doručena do jeho poštovní schránky, ke které pak přistupuje pomocí protokolů POP nebo IMAP. (Peterka, 1998)

3.8.3.3 Protokol IMAP

Vychází z protokolu POP. Tento protokol je jeho nadstavbou. Užívá se pro komunikaci a přenos elektronické pošty. Tento protokol podporuje on-line komunikaci na

rozdíl od protokolu POP, který je určen pro práci s poštou a poštovním serverem. (Sosinsky, 2010)

3.8.3.4 Protokol FTP

Protokol FTP zajišťuje přenos souborů mezi jednotlivými stanicemi sítě za předpokladů existence FTP serverů. V praxi to znamená, že FTP server může být každý počítač, který umožňuje přístup do jejich souborového systému jiným uživatelům ze vzdálených počítačů. Podle přístupových práv jednotlivých uživatelů. Uživatel je oprávněn buď stahovat nebo nahrávat soubory na daný FTP server. (Peterka, 1998)

3.8.3.5 Protokol DNS

Tento protokol zajišťuje překlad adres stanic na doménová jména a naopak. Tento překlad zajišťuje DNS server, kteří přijímá zprávy v síti od jiných stanic a posílá jim adekvátní odpověď. (Peterka, DNS, 1998)

3.8.3.6 Protokol DHCP

Protokol DHCP zajišťuje dynamické přidělování IP adres logickým stanicí. Každá nově přidaná stanice pošle požadavek na přidělení IP adresy a DHCP přidělí IP adresu této stanice. IP adresu vybere ze zvoleného poolu IP adres. IP adresa se váže na MAC adresu stanice, která si o ni zažádala. (Droms & Lemon, 2004) (Sosinsky, 2010)

3.9 Aplikace a služby

V následujících podkapitolách budou popsány aplikace a služby, které budou součástí řešení nebo úzce souvisí s jeho vypracováním.

3.9.1 Síťové operační systémy

Existuje nepřeberné množství síťových operačních systémů, ale budou zde popsány pouze základní představitelé těchto systémů. Nejdříve je potřeba popsat, co je to síťový operační systém.

Síťový operační systém je systém, který je uzpůsobený a optimalizovaný pro poskytování síťových služeb. Musí poskytovat podporu pro hardware, spouštět protokoly a služby a následně tyto služby poskytovat klientským systémům. Mimo těchto základních služeb nabídnou nástroje pro správu, adresářové služby, zabezpečení a jiné. Takové to síťové operační systémy se označují za platformy. Klasickým příkladem platforem jsou UNIS, Linux a Microsoft Windows, které budou v následujících kapitolách popsány. Každý z těchto síťových operačních systémů musí zvládat následující funkce:

- Poskytovat podporu operačního systému pro hardware, na kterém běží.
- Provozovat různé síťové protokoly a služby, jako například adresování.
- Spouštět klientské aplikace, k nimž mohou přistupovat klientské systémy.

Tyto základní funkce musí každý síťový systém splňovat. Zatím zde byla řeč pouze o obecných síťových systémech, ale je vhodné poukázat i na ty specializované, kterým je například IOS společnosti Cisco Systems, který běží na všech směrovačích této společnosti, který obsahuje specializované funkce pro řízení síťové komunikace. (Stanek, Mistrovství v Microsoft Windows Server 2008, 2011) (Sosinsky, 2010)

3.9.1.1 Unix

Jedná se o víceúlohový, víceuživatelský, v čase sdílený operační systém, který byl postaven na jádru, který mohl využívat jakoukoliv počítačovou architekturu. Hlavní filozofií bylo vytvoření modulárního a opakovaně použitelného síťového operačního systému. Většina distribucí UNIX podporuje provoz bez monitoru a klávesnice, tento režim byl i přidán do Microsoft Windows Serveru 2008. Systémy odvozených z konceptů systému UNIX, ale nevyhovují specifikaci SUS (Single UNIX Specification), jsou považovány za tzv. „UNIX-like“ systémy – různé distribuce Linuxu. (Matyska, 1991)

3.9.1.2 Linux

Jedná se o Open Source systém, který může být tím nejrozšířenějším serverovým systémem. Organizace Netcraft (www.netcraft.com/), mluví až o 50% serverů běžících na různých verzích tohoto síťového operačního systému. Linux byl navržen z principů UNIX. Obsahuje monolitické jádra, které obsahuje správu procesů a paměti, ovladače a moduly

I/O zařízení, souborový systém a další funkce podporující uživatelský prostor (shell nebo GUI).

Jednotlivé verze běží od malých, integrovaných zařízení až po superpočítače (88% superpočítačů běží na některé verzi systému Linux uvedených na stránkách TOP 500 Supercomputer Sites (www.top500.org/)). Například Amazon, Google nebo Yahoo! Také běží na flotile linuxových serverů.

Jednotlivé distribuce nebudou dále popisovány, jen zde bude popsán balíček LAMP, který je často nasazován na hardware pro linuxový server. Jedná se o balíček skládající se z těchto komponent:

- Linux
- Apache
- MySQL
- P - Jeden z programovacích nebo skriptovacích jazyků. (Nemeth, Snyder, & Hein, 2008)

3.9.1.3 Microsoft

Jedná se o operační systém, který má nejširší podporu síťových aplikací ze všech síťových operačních systémů. Dalším nedílným faktem je, že Microsoft ovládá 90% celosvětového trhu desktopových počítačů. Tyto čísla naznačují jistou synchronizaci mezi Windows Serverem a desktopovým OS. Dále Microsoft nabízí jistou množinu serverových aplikací, pomocí kterých lze rozšířit funkčnost daného serveru a soběstačnost společnosti jako takové, kde je využit síťový systém od společnosti Microsoft. Dominantní postavení na trhu podnikové pošty zaujímá Microsoft Exchange, dále nejprodávanějším komerčním, podnikovým, databázovým serverem je SQL Server. (Russel & Crawford, 2009)

3.9.2 Domény a adresářové služby

Každý informační systém je uspořádán kolem konkrétní základní jednotky, v databázi je touto jednotkou záznam a v adresářové službě je touto základní jednotkou doména.

Síťová doména jako taková představuje množinu systémů, které sdílejí stejnou databázi zabezpečení neboli pole působení jejich zásad. Domény mohou být různých typů a obsahovat i různé objekty, jako jsou organizační jednotky, uživatelské účty, účty počítačů a jiné objekty, které lze adresovat pomocí jedinečného názvu objektu.

K uspořádání typů domén se používá mnoho schémat nebo jejich vzájemnými kombinacemi:

- Centrální hlavní doména s větví doménové struktury
- Struktura s více hlavními doménami
- Domény prostředků
- Vzdálené domény, kde jsou spojení reprezentována buď vztahem důvěryhodnosti nebo replikací
- Domény specifické pro aplikace.

Počítačový systém obsahující adresářovou službu se nazývá server domény pro danou síť, nebo případně doménový řadič. Z bezpečnostních důvodů si adresářové uchovávají svá data a bezpečnostní informace na stejném serveru domény. (Sosinsky, 2010) (Stanek, Mistrovství v Microsoft Windows Server 2008, 2011)

3.9.2.1 Adresářové služby

Adresářová služba jako taková uchovává metadata, tedy data o datech, které jsou uloženy v objektové databázi. Schéma adresáře pak určuje množinu tříd objektů, ke kterým jsou přiřazena množina požadovaných a volitelných atributů. Metadata poskytují mapu k systémovým prostředkům.

Adresářová služba je abstraktní vrstvou, která odděluje fyzickou realitu klientů, serverů a prostředků od logických přiřazení v daném schématu.

Adresářovou službu aplikujeme, pokud v síti potřebujeme:

- Centralizovanou správu síťových prostředků.
- Definované zásady zabezpečení.
- Možnost auditování síťových událostí.
- Rozšíření vaší sítě za účelem podpory více uživatelů.
- Podpory různých klientů a operačních systémů.

Tyto požadavky nejsou často splněny v kancelářských sítích o počtu menším než 20 připojených systémů. Adresářová služba poskytuje spoustu výhod, ale za cenu vyšších nákladů, složitosti sítě a nemluvě o znalosti IT pracovníků. (Stanek, Active Directory, 2009)

Synchronizace a replikace

Za účelem odolnosti proti chybám a zvýšení výkonu, jsou adresářové služby replikovány na různé servery s různým umístěním. Replikace je proces, kdy jsou data přenášena na jiný systém a jsou velice často aktualizována. Samotná replikace neuchovává záznam o stavu systému, pouze jeho aktuální podobu.

Pokud je jediná kopie označena jako hlavní kopie (master copy), topologie replikace funguje na principu master/slave. Replikace typu multimaster může trpět nekonzistencemi dat a také latencí sítě, protože se jedná o asynchronní přenos. (Stanek, Active Directory, 2009)

Jednotné přihlášení

Uživatelům je nepříjemné se mnohokrát přihlašovat (přihlašování na různé webové stránky), proto adresářová služba řeší tento problém jednotným přihlášením do své domény a jsou tedy jeho pověření předána i ostatním objektům zabezpečení ve formě, kterou mohou akceptovat. Velice elegantní řešení, ale velice složité z důvodů způsobů autentizace pro různé systémy, které mohou být značně odlišné. (Stanek, Mistrovství v Microsoft Windows Server 2008, 2011)

Moduly zásad

Pokud jsou do databáze uložena informace o síťovém objektu, pak lze vytvořit množinu pravidel, jak mají být tyto objekty použity. Tyto moduly jsou oddělené od modulu zabezpečení operačního systému, i když se mohou značně překrývat. Tyto zásady mohou ovlivňovat chod sítě, včetně následujících:

- konfigurace desktopu klienta;
- frekvence aktualizací nebo oprav;
- složitost hesla;
- akce přihlášení/odhlášení.

Nejnámějším modulem zásad jsou zásady skupin od společnosti Microsoft. Group Policies (Zásady skupin) jsou uloženy ve službě Active Directory. (Sosinsky, 2010)

3.9.2.2 Protokol LDAP

Pro vzájemnou spolupráci různých adresářů musel být vytvořen protokol označován jako DAP (Directory Access Protocol) standardu X.500. Tento protokol je použitelný pro libovolný typ sítě a je schopen uchovávat informace o objektech z jakékoliv vrstvy ISO/OSI. Pro zavedení sítě typu TCP/IP byl vytvořen nový protokol nazývaný se LDAP (Lightweight Directory Access Protocol). Slovo „Lightweight“ je opravdu neodpovídající, protože protokol LDAP je velice složitým protokolem. (Sosinsky, 2010)

3.9.2.3 Novel eDirectory

Jedná se o objektově orientovanou hierarchickou databázi, která podporuje uživatele a skupiny, role, systémy, aplikace a služby s globálními a lokálními vlastnostmi. Globální a lokální vlastnosti vymezují pole působnosti (například zásady skupin) na doménu nebo jednotlivé počítače. Novel eDirectory je hlavním konkurentem Microsoft Active Directory, který bude více popsána v další podkapitole. Jedná se o verzi NDS, která ve své době předběhla AD a proto je používána v některých největších sítích využívající adresářové služby.

Databáze eDirectory se vyznačuje vysokou interoperabilitou (schopnou vzájemné spolupráce různých systémů), a to s klienty i servery různých systémů. (Focus, 2018)

3.9.2.4 Microsoft Active Directory

Active Directory je nejčastěji používanou adresářovou službou dnešní doby, která se poprvé objevila v systému Windows Server 2000 a je stále aktualizována. Active Directory je doména množinou systémů, které jsou vzájemně propojené v logickém seskupení založeném na modelu zabezpečení, který je aplikován na všechny sdružené systémy v rámci stejné místní sítě, v rámci WAN nebo na vzdálené systémy, které se občas přihlašují k doméně.

Službu Active Directory tvoří široká škála objektů, které lze spravovat. Uživatelé nebo skupiny, jsou objekty a kolekce vlastností, práva a oprávnění lze transformovat na uživatelské účty a skupinové účty. Počítače a jiné periferie jsou rovněž objekty, které jsou uspořádané podle jejich účtů.

Množina domén může být sloučena do jedné doménové struktury, kdy každá doména má svou vlastní databázi zabezpečení. Aby pak mohli uživatelé komunikovat mezi těmito doménami, je nutné vytvořit vztahy důvěryhodnosti, kdy pak řadiče obsahují informace o ostatních doménách v doménové struktuře prostřednictvím replikace.

Společnost Microsoft rozkouskovala služby Active Directory pro různé edice systému, tzn. že takový SQL Server může běžet na serveru bez nutnosti vytváření doménového serveru a stejném serveru. (Stanek, Active Directory, 2009)

3.9.3 Souborové systémy

Přístup k souborům je jedním z nejdůležitějších služeb, kterou mohou být za pomoci sítě poskytovány. Jedná se o jeden z největších datových toků po síti. Proto existuje mnoho způsobů, jak přenášet data po síti, jak zabezpečit jeho obsah a zajištění jeho ochrany.

Každý souborový systém lze nakonfigurovat tak, aby poskytoval soubory klientům, ovšem za podmínky, že tyto systémy nebudou optimalizovány pro síťové služby. jedním takovým příkladem může být třída serverů specializována na sdílení souborů, nazývají se NAS (Network Attached Storage). (Sosinsky, 2010)

3.9.3.1 NAS

Takovéto uložisko se skládá ze souborových serverů, které poskytují klientům přístup k datům v síti. Zařízení NAS mohou nabývat různých velikostí, ať už od velikosti jednoho externího disku, až po velké diskové pole. Na oblíbenosti těchto uložišť značně napomáhá jednoduché nastavení, kdy stačí k NAS serveru připojit ethernetový kabel, zapnout server a o vše ostatní je již postaráno. Pomocí webového prohlížeče lze nakonfigurovat sdílené složky, uživatele a skupiny nebo nastavování přístupových práv souvisejících se serverem. NAS servery jsou vytvořeny jako promiskuitní zařízení, obsahují různé protokoly zajišťující komunikaci s různými operačními systémy.

Velké servery a podniková zařízení jsou dodávána s různými výkonnými programy pro zálohování, replikaci a dalšími funkcemi pro práci se soubory a zajišťující jejich bezpečnost.

Souborový systém vyžaduje:

- Optimalizovanou funkci vstupu/výstupu sítě;
- Optimalizovanou funkci vstupu/výstupu disků;
- Výkonný systém souborů;
- Velkou kapacitu diskového pole, pokud možno v chránění podobě (RAID)

Zařízení NAS podporuje:

- Široké spektrum protokolů zajišťující připojení ke klientům v heterogenní síti.
- SW/HW diskové pole RAID (RAID 0, 1, 0+1 a 5).
- Pokročilé diskové nástroje (formátování nebo vytváření oddílů).
- Nástroje pro správu systému, obvykle za pomoci webového prohlížeče.
- Integraci služby Active Directory, stejně jako integraci služby NIS do adresářů systémů UNIX/Linux. (WDC)

NAS vs. síť SAN

Hlavním rozdílem je způsob prohlížení souborů, u NAS serveru si klient prohlíží soubory uložené na NAS serveru a na základě požadavku jsou nebo nejsou přeneseny na jeho operační systém. SAN (Storage Area Network) úložiště obsahuje stejné součásti jako úložiště NAS, ale klient si prohlíží soubor na svém souborovém systému svého operačního systému. Pokud si klient zažádá o soubor, mapovací tabulka namapuje tento požadavek na množinu bloků na konkrétní sadě disků, následně jsou tyto bloky přeneseny na systém klienta.

Klient nepozná rozdíl ve způsobu prohlížení, ale z hlediska architektury systému je rozdíl mezi NAS a SAN systémem podstatný. (Sosinsky, 2010)

3.9.3.2 Protokoly

Existuje spousta protokolů souborových služeb, ale budou popsány pouze dva a to NFS, který je populární v systémech UNIX a Linux, a protokol SMB/CIFS. Účelem těchto protokolů je poskytovat klientovi vzdálený přístup k uložení.

Protokol NFS

Tento protokol je populární v systémech UNIX a Linux, který umožňuje přístup k síťovým sdíleným složkám. NFS protokol je podporován téměř všemi síťovými operačními systémy (Microsoft Windows, Novell Network, Mac OS apod.), i když se nepoužívá tolik jako protokol CIFS/SMB.

Tento protokol je implementován na 7. vrstvě, tedy aplikační vrstvě. Ve skutečnosti protokol pracuje od 5. až po 7. vrstvu, protože tento protokol obsahuje jazykovou sadu XDR (External Data Representation), která se používá pro definování typů dat, která lze přenášet po síti. Tento protokol je konfigurován na straně serveru, kde se nachází sdílená složka, ale také na straně klienta. Značná většina NAS serveru to udělá automaticky. (Peterka, NFS, 1993)

Protokol SMB/CIFS

Protokol SMB je protokolem aplikační vrstvy využívaný ke sdílení souborů, tiskáren, sériových portů a dalších síťových prostředků, ale také zároveň zahrnuje přístup k síťovým aplikačním rozhraním (API).

Tento protokol vytváří spojení mezi prostředky na jednom hostiteli a druhým hostitelem mechanismu žádostí/odpovědí typu klient/server. Tedy při žádosti klienta o prostředek, například o přístup k souboru na serveru, protokol uzamkne daný prostředek na dobu nezbytnou k jeho užití. Protokol obsahuje dva režimy zabezpečení – úroveň sdílení a uživatelskou úroveň.

Společnost Microsoft, společně s SCO Group a dalšími subjekty, vytvořili protokol CIFS, který je rozšířenou verzí protokolu SMB, který je podporován téměř všemi síťovými operačními systémy. (Sosinsky, 2010)

3.9.4 Webové služby

V této kapitole budou představeny základy webových služeb, a to z jednoduchého důvodu, protože moderní technologie stále více využívají internetové prostředí a toto prostředí bude v budoucnosti stále důležitější.

Klasická webová služba se skládá z poskytovatele služby (server) a žadatele o službu (klienta). Protokolem pro předání zpráv je SOAP protokol, který data formátuje v jazyce XML, který má svoje výhody a nevýhody. Zprávy jazyka XML jsou čitelné a upravitelné pomocí prostého textového editoru, ale jsou schopny vysoce zatížit webovou službu, na rozdíl od binární reprezentace dat.

Zprávy SOAP mohou být přenášeny prostřednictvím protokolů HTTP, HTTPS nebo SMTP. HTTP protokol bude blíže popsán v následující podkapitole.

3.9.4.1 HTTP

Jedná se o nativní protokol aplikační vrstvy, který využívají webové servery a webové prohlížeče klientů ke vzdálenému přenosu informací. Tento protokol pracuje na mechanismu požadavků a odpovědí, kdy požadavek je tvořen textem v kódování ASCII a obsahuje jeden nebo více příkazů akcí. Odpověď je naopak naformátovaný text podle standardů.

Protokol HTTP je bezstavový, informace jsou potřebné k relaci jsou obsaženy v samotných zprávách. Díky tomu nemusí klient ani server uchovávat a spravovat uživatelské informace. Za tímto účelem se přizpůsobuje uživatelské prostředí pomocí jiných metod. Nejčastěji využívanými metodami je zapisování a změna souborů cookies, autentizovaná přihlášení pro jednotlivé relace a relace na straně serveru. Ačkoli se používá v sítích TCP/IP, tento protokol nevyžaduje protokol TCP pro přenos dat, stačí jen ověřená integrita příchozích dat. Odchozí a příchozí port tohoto protokolu je 80.

Protokol HTTPS je zabezpečený protokol, který využívá protokol HTTP spolu s protokolem SSL nebo TLS. Tento protokol zajišťuje autentizaci, důvěryhodnost přenášených dat a jejich integritu. Na rozdíl od protokolu HTTP, pracuje HTTPS na portu 443. (David, 2002)

Stavové kódy protokolu HTTP

Tyto kódy se využívají v případě naskytnutí problému. Následně webový server vrátí klientovi jednořádkový stavový kód. Příkladem takového stavového kódu může být chyba „404 – Nenalezeno“. Jednotlivé stavové kódy nebudou dále vysvětleny, pouze jejich třída.

Třídy stavových kódů:

- 1xx – Informační
- 2xx – Úspěch
- 3xx – Přesměrování
- 4xx – Chyba klienta
- 5xx – Chyba serveru

3.9.4.2 SOA

Jedná se o architekturu orientovanou na služby a představuje rámec pro vytváření distribuovaných síťových aplikací z množiny služeb, které jsou schopny vzájemně komunikovat. Jinými slovy je architektura SOA platformou využívanou k vytváření distribuovaných aplikací a bude sloužit jako metoda budoucnosti, pomocí které budou aplikace doručovány jako služby na požádání. (Sosinsky, 2010)

3.9.5 Poštovní protokoly

Poštovní protokoly tvoří systém, který jsou základem pro přijímání a odesílání e-mailových zpráv prostřednictvím e-mailových aplikačních serverů. E-mail jako takový je jednou z nejstarších existujících služeb počítačových sítí. Existovala před vznikem sítě Internet a Internetu jako takovému se přizpůsobila.

Obecný postup zasílání e-mailu:

1. E-mailový klient odesílatele odešle zakódovanou zprávu ve formátu SMTP serveru odchozí pošty SMTP.
2. Server SMTP zjistí e-mailovou adresu příjemci (v záhlaví SMTP), vyhledá symbol @, aby zjistil název domény, poté kontaktuje DNS server této domény za získáním MX záznamu (Mail eXchange). DNS vrátí záznam MX serveru SMTP s umístěním POP3 serveru pro danou doménu.

3. Zpráva SMTP je odeslána agentem MDA (Mail Delivery Agent) přes Internet serveru POP3 (nebo IMAP).
4. Server POP3 (nebo IMAP) odešle zakódovanou zprávu SMTP poštovnímu příjemci nebo klientovi příjemci, kde je e-mail dekodován a vhozen do poštovní schránky.

Je zde patrný vztah k DNS službě, kdy každý server DNS musí obsahovat MX záznam, který definuje, kam musí být odeslána pošta pro danou doménu. (Sosinsky, 2010)

3.9.5.1 SMTP

Jedná se o protokol používaný k posílání e-mailové zprávy mezi servery v síti protokolem IP. Většina e-mailových klientů odesílá za pomoci protokolu SMTP, ačkoli přijímá za pomoci jiných protokolů (POP3 nebo IMAP). Protokol komunikuje se server odchozí pošty na protokolu 25. Mezi nejznámější poštovní servery SMTP jsou UNIX sedmail (který byl jako první), Microsoft Exchange, Novell GroupWise a mnoho dalších. (Stanek, Microsoft Exchange Server 2010, 2010)

3.9.5.2 POP3

Protokol POP3 je nejnovější verzí protokolu POP. Tento protokol je jedním ze dvou běžných e-mailových protokolů, které přijímají poštu ze serverů v síti IP do klientských aplikací. Tento protokol pracuje na portu 110.

Hlavním rozdílem oproti protokolu IMAP je ten, že protokol POP3 obsahuje nastavení, zda po přijetí klientskou aplikací má zanechat i zprávu na serveru. Implicitně je nastaveno, že se má zpráva na severu odstranit a uživatelé ve většině případu nemění. (Stanek, Microsoft Exchange Server 2010, 2010)

3.9.5.3 IMAP

Protokol IMAP je programem pošty založeným na serveru. Na rozdíl od protokolu POP3, který byl popsán v předchozí podkapitole, protokol IMAP vytváří uložisko dat na serveru elektronické pošty, ke kterým je uživatel schopen přistupovat odkudkoliv prostřednictvím IMAP klienta. Klasickým příkladem takového serveru a klienta je

Microsoft Exchange a klient Outlook. Nespornou výhodou, oproti protokolu POP3, je možnost nahlédnout do své e-mailové schránky kdykoliv a synchronizovat zprávy, které se neodeslaly z klientské aplikace například z důvodu odpojení systému od sítě IP. Zároveň tento protokol umožňuje, aby se e-mail objevil na dvou či více systémech prostřednictvím synchronizace. (Stanek, Microsoft Exchange Server 2010, 2010) (Sosinsky, 2010)

3.9.6 Telefonie a VoIP

Telefonie představuje spojení počítačů a telefonů za pomoci dvou různých sítí. Telefonie pokrývá široké spektrum multimediálních aplikací, včetně hlasu, videa, obchodních a zábavních aplikací. Telefonie jako taková je množina služeb, která umožňuje přenášet analogový zvuk po sítí jako digitální data. V některých případech je přenášena za pomoci nespojitě služby (jako zvukový soubor), ale stále více se způsob přenosu zvuku a okamžitého streamování příjemci.

Telefonní aplikace v počítačových systémech spojených do sítě spadají do následujících kategorií:

- Hlasová volání po telefonní síti s přepínáním okruhů
- PBX (simulace pobočkových ústředen)
- Pořádání konferencí po sítí s protokolem IP
- Hlasové odpovídací systémy
- VoIP hovory
- Systémy pro spolupráci, sdílené tabule a systémy vzdálené plochy
- Technologie automatického volání)

3.9.6.1 PBX

Jedná se o telefonní síť, která se obecně instaluje na všechny středně až velké kanceláře. K této ústředně je připojena veřejná síť, která poskytne jednu nebo více telefonních linek. Hovory pak přicházejí do ústředny, které jsou podle zvolené linky distribuovány ke konkrétnímu příjemci. Nebudou zde vybrány PBX a nebudou popsány. (Sosinsky, 2010)

3.9.6.2 VoIP

Jedná se o název protokolu pro přenos hlasové komunikace po sítích s přepínáním paketů. Tento protokol používá co nejmenší soubory pro tento přenos, tyto soubory jsou protokolem TCP rozděleny na pakety a odeslány přijímajícímu zařízení. Služby VoIP jsou implementovány jedním z následujících způsobů:

- Softwarové řešení, jako je například aplikace Skype.
- Připojení telefonu k internetovému připojení prostřednictvím analogového telefonního adaptéru.
- Připojení prostřednictvím kabelového modemu
- Použití VoIP systému PBX k síti TCP/IP.

Primární motivací pro použití VoIP byly značně klesající náklady na dálková spojení, ale hlavní nevýhodou je, že VoIP slučuje telefon a Internet do jedné linky, v případě přerušení internetové spojení, uživatel přijde o obě možnosti komunikace. (Wallace, 2017) (Sosinsky, 2010)

3.9.6.3 Videotelefonie

Tato technologie umožňuje vzájemný hovor dvou uživatelů a současně sledovat synchronizovaný video stream. Opět hlavní ikonou je zde aplikace Skype, která je celosvětově nejoblíbenějším médiem pro tento způsob komunikace. Tato aplikace také podporuje rychlé zasílání zpráv a také přenos souborů.

V průběhu času byla představena řada přenosných počítačů, které jsou vybaveny kamerami a tím umožňují VoIP komunikaci z jakéhokoliv místa za předpokladu, že je uživatelé připojen do sítě. Tyto webové kamery nejsou jen používány v rámci komunikace, ale také jako bezpečnostní prvek, který lze připojit k ethernetové síti a zasílat tak real-time obraz uživatelů, ať už se jedná o soukromé využití, jakou je ochrana objektu, nebo veřejné přístupné, jakou je například online stream kamer skiareálu Klínovec. (Wallace, 2017)

3.10 Zabezpečení počítačové sítě

3.10.1 Bezpečnostní protokoly a služby

Kvalitní bezpečnost sítě funguje na bázi vzájemně překrývajících se technologií, které běží na různých vrstvách. Budou zde uvedeny místa sítě, na které se dá zaútočit a tím kompromitovat síťové systémy. Dále v této kapitole bude sepsán seznam aktivit, které by měly být podniknuty ke správnému zabezpečení sítě.

3.10.1.1 Přehled síťové bezpečnosti

Každý den jsou vytvářeny nové způsoby, jak napadnou počítačovou síť a systémy obsažené v ní. Z digitalizace všech dostupných informací jsou tyto útoky stále propracovanější a správci sítě se snaží odradit útočníky stále propracovanější obranou. Ovšem je nutné se smířit se skutečností, že neexistuje jednoduchý návod, jak zabezpečit síť. Každý systém je dříve či později prolomitelný a pokud ne zvenčí, tak zcela určitě zevnitř. Nejlepší metodou je zavedení několika bezpečnostních vrstev. (Zeltser, Winters, Frederick, Ritchey, & Northcutt, 2005)

Zranitelná místa v síti

Zranitelné místo může být použito k neoprávněnému přístupu do sítě nebo systému. Existuje spousta způsobů, jak se do takového systému proniknout: uhodnutí hesla, prostřednictvím viru, softwarové chyby, spustitelnému programu apod. V případě zjištění této zranitelnosti se systém stane cílem útočníků. Chyby vzniklé v systému jsou opravovány aktualizacemi, ale za rizika, že mohou vzniknout další trhliny v systému, jedná se o nekonečný koloběh, kdy opravením jedné chyby vzniká další. Odhalení síťových zranitelností lze zajistit prověrkami sítě nebo pomocí softwaru pro analýzu rizik sítě. Po skončení průzkumu sítě skener sestaví mapu sítě a vytvoří výstupní zprávu. (Zeltser, Winters, Frederick, Ritchey, & Northcutt, 2005)

Slabá místa k napadení

Nejčastější způsob prolomení sítě je z externí sítě směrem dovnitř, kdy útoky se snaží zacílit na zranitelná místa v síti. Tento způsob je zcela neefektivnější, protože se může odehrávat nepozorovaně.

Nejslabší slabá místa jsou:

Zvenku
Dostupnost systému – Přetížení prvků v síti ICMP paketem, jehož výsledkem je velké množství odpovědí na systém oběti.
Odepření služby – Služba je zahlcena požadavky útočníka.
Distribuované útoky – Koordinované útoky s větším množstvím napadajících prvků.
Zvenku/zevnitř
Autentizace – Útočník se vydává za jiného uživatele.
Data při přenosu – Data mohou být zachyceny a pozměněny, ale také mohou být pouze odposlouchána.
Zevnitř
Zadní vrátka – útočník je schopen ovládat systémy uvnitř sítě formou spustitelných programů nebo algoritmů, které mohou obcházet autentizaci v síti.
Přímý přístup – Útok pomocí přenosného média.

Tabulka 1 - Charakteristika slabých míst

Principy bezpečného návrhu sítí

Správce sítě by se měl soustředit na tři základní úrovně zabezpečení:

- Ohodnocení rizik a prevence – neefektivnější preventivní technologiemi pro ošetření rizik jsou řízení přístupu uživatelů, kryptografie a firewally.
- Detekce hrozeb – antivirové skenery, rozpoznání škodlivého softwaru, audit událostí a jejich analýza.
- Reakce na incidenty – v případě útoku je nutné správně reagovat.

Dalším důležitým principem je minimalizace útočného povrchu systému nebo sítě. Čím méně existuje cestiček do systému nebo sítě, tím nižší jsou bezpečnostní rizika. V další kapitole „Čtrnáctero přikázání“ budou sepsána doporučení vycházející z praxe. (Sosinsky, 2010)

Čtrnáctero příkázání

1. Používání firewall
2. Vynucování silných hesel
3. Instalace antivirových programů a anti-spywaru
4. Zavedení odolných zásad zálohování
5. Aktualizace softwaru
6. Rozdělení sítě na segmenty a podsítě
7. Šifrování všech citlivých dat a pro datové přenosy použít bezpečnostní protokoly
8. Vyvarování se stahování obsahu, hyperlinků a nevyžádaných e-mailů
9. Zmenšení útočného povrchu
10. Vyvarování sdílených složek a poskytování plného přístupu k nim
11. Omezení mobilních systému a přenosových medií
12. Bezpečnost je bezpečnost (spojení budou prováděna v jejich zabezpečené formě)
13. Být zásadoví a nekompromisní
14. Být vlídní ke svým rodičům, dětem, zvířátkům a ostatním síťovým administrátorům, s nimiž se setkáváte. (Sosinsky, 2010)

3.10.1.2 Technologie NLA a NAP

Jak již bylo řečeno, každý den vznikají nové způsoby, jak proniknout do počítačové sítě, není možné tedy zabezpečit síť pomocí administrátorovi pracovní kapacity a je tedy nutné se spolehnout na adaptivní bezpečnostní strategie. Tyto technologie vyvinula společnost Microsoft, které integrovala do svých systémů. NLA (Network Location Awareness) je schopnost detekovat systém, spojení a stavy relací a tím přizpůsobit odpovídajícím způsobem zásady klienta. Systém NAP (Network Access Protection) má definované zásady, které při vznikajícím síťovém spojení zjišťují, zda tyto zásady nejsou porušeny (např. zda má klient zapnutý firewall a antivirový program). V případě nesplnění zásad je počítač v karanténě do doby, dokud nesplní stanovené zásady. (Sosinsky, 2010)

3.10.2 Firewally, brány a proxy servery

3.10.2.1 Firewall

Tento způsob zabezpečení je na bázi jak softwarové, tak i hardwarové aplikace na síťové služby. Jedná se o další úroveň bezpečnosti, která zamezuje neoprávněnému autorovi přístup do zabezpečené sítě. Firewally jako takové sledují provoz na síti a rozhodují se, kterou komunikaci pošlou dále a kterou naopak zablokují a vrátí zpět. Kritériem, pro tento způsob rozhodování, je filtr, který čte hlavičku paketu a nejčastěji se rozhoduje na základě zdrojové a cílové adresy komunikace. Vlastnosti, které firewally vyhodnocuje:

- Filtrování paketů – čtou data ze záhlaví IP paketu a na základě stanovených pravidel je komunikace povolena nebo zakázána.
- Vstupní filtr na síťovém rozhraní – blokuje dat na základě rozsahu IP adres, čísel portů a protokolů.
- NAT – pro firewally je důležité skrývání IP adres interních počítačů před veřejností, tuto možnost zprostředkovává služba NAT.
- Stavová inspekce – kontrolují odchozí pakety a zaznamenávají se tyto cíle stavové tabulky, příchozí pakety se pak kontrolují podle aktuální stavové tabulky.
- Inspekce okruhů – tento filtr se zabývá celými relacemi, kterou inicializuje uzel za firewallem. Tyto filtry zamezují útokům typu IP spoofing (podvržení a odposlech IP adresy).
- Proxy firewall – jedná se o mezičlánek, se kterým veřejná síť komunikuje jako s jediným možným koncovým uzlem. Tento firewall zavádí dvě oddělené komunikace mezi privátní a veřejnou sítí.
- Aplikační filtry – jedná se o nejpomalejší způsob filtrování, jelikož tyto filtry zkoumají pakety i data, která obsahují. a dokonce je mohou i modifikovat na aplikační vrstvě.

Pokročilejší firewally se mohou podívat do paketu na aplikační vrstvě. Firewally často využívají překladu adres (NAT), kdy adresy v privátní síti jsou anonymní veřejné

síti. Bude zde jednoduše popsány firewally, které se vyskytují. (Zeltser, Winters, Frederick, Ritchey, & Northcutt, 2005)

Personální firewally

Tento firewall jistě každý zná, jedná se o firewall zabudovaný v operačním systému osobních počítačů. Jeho hlavním úkolem je tedy chránit koncové stanice v počítačové síti. Typickým příkladem této integrace je firewall od společnosti Microsoft (Microsoft Windows Firewall), který je velice jednoduchý, ale je i velice účinný. Jeho integrace do systému měla za následek zvýšení bezpečnosti tohoto systému a zvýšení odolnosti vůči externím útokům. Filtrovat lze pomocí zdrojové a cílové IP adresy, zdrojových a cílových TCP/UDP portů a také na základě identifikace uživatele, některé firewally filtrují i na základě MAC adresy. (Zeltser, Winters, Frederick, Ritchey, & Northcutt, 2005)

Firewally ve směrovačích

Ve směrovačích se také nachází firewall, ovšem není tak agilní jako například personální firewall. Směrovače podporují blokování adres a portů a jistý způsob překladu adres. Pokročilejší směrovače obsahují nejen pokročilejší a propracovanější firewall, ale mohou do nich být instalovány i antivirové programy. Tyto směrovače jsou u správců velice oblíbené, jelikož nabízejí správu směrovače a firewallu pomocí jednoho rozhraní. (Zeltser, Winters, Frederick, Ritchey, & Northcutt, 2005)

Hardwarové firewally

Jedná se o firewally vyšší kategorie, kde jejich vlastností je neproniknutelnost, vysoký výkon, vysoká míra dostupnosti a obsahují záložní systémy, které v případě výpadku automaticky přeberou provoz. Jedná se o velice složité systémy a také jsou velice drahé, proto jsou aplikovány ve velkých firmách, které si to mohou dovolit.

Serverové firewally

Na rozdíl od hardwarových firewallů, které jsou dodávány s vlastním operačním systémem a s vlastním hardwarem, jsou serverové firewally implementovány přímo do serverového operačního systému. Z hlediska funkčnosti jsou velice malé rozdíly mezi serverovým firewallem od hardwarovým firewallem. Výhodou firewallu na serveru je

integrace do sítě, která je daleko snazší nežli u jeho oponenta, naopak nejsou vyladěné na hardware a je potřeba silnější hardware pro dodržení výpočetního standardu. (Zeltser, Winters, Frederick, Ritchey, & Northcutt, 2005)

3.10.2.2 Brána

Brána hraje roli rozhraní mezi dvěma nebo více sítěmi. Její hlavním úkolem je konverze jednotlivých protokolů pro správnou komunikaci mezi odlišnými sítěmi. Mohou převádět jeden typ souboru na druhý na aplikační vrstvě nebo v prezenční vrstvě mohou měnit způsob šifrování. Brána je obecný termín pro zařízení fungující na libovolné vrstvě OSI. (Zeltser, Winters, Frederick, Ritchey, & Northcutt, 2005) (Sosinsky, 2010)

3.10.3 VPN

VPN neboli Virtual Private Networks jsou základním stavebním kamenem pro zabezpečenou komunikaci mezi sítěmi, které se tvoří přes poskytovatele veřejných linek, jakou jsou veřejné přepínané telefonní sítě nebo Internet.

3.10.3.1 Technologie VPN

Technologie VPN vytváří bezpečné prostřední (linky) v nezabezpečeném prostředí. Tyto bezpečné linky (VPN linky) propojují privátní datovou síť s uživateli nebo lokalit, prostřednictvím pomocí tunelovacích a šifrovacích protokolů. V dnešní době lze VPN linky rozdělit na tyto čtyři typy:

- **Interní linky v místní síti LAN** – VPN spojení mezi dvěma počítači v jedné síti.
- **Linky mezi místními sítěmi LAN** – VPN síť propojuje dvě různé místní sítě LAN.
- **Externí linky prostřednictvím WAN** – Spojení mezi dvěma vzdálenými LAN sítěmi prostřednictvím sítě WAN.
- **Linka pro vzdálený přístup** – Přechodná spojení pomocí sítě WAN, kterou se připojuje vzdálený klient k místnímu serveru nebo počítači.

Obecně lze VPN spojení rozdělit na ty, které zprostředkovávají přístup uživatelům a na VPN spojení mezi sítěmi. Sítě VPN se mohou implementovat v hardwaru nebo softwarově, zřídka je možné narazit na kombinaci obou.

Softwaru, který se používá pro VPN, je velice mnoho jako je například OpenVPN nebo LogMeIn Hamachi, který velice často využívali/využívají hráči pro hraní počítačových her. Mimo jiné je VPN služba také implementována v systémech od společnosti Microsoft.

Mezi nejznámější společnosti, která vytvářejí hardwarové virtuální privátní sítě jsou Cisco Systems a Juniper Networks. Cisco nabízí komplexní VPN řešení pro všechny možné situace, které mohou v sítích nastat. Jejich směrovače mají zabudovanou VPN službu přímo v sobě a mohou také fungovat jako firewally. Standardy a testy hardwarových prvků provádí konsorcium VPNC (Virtual Private Network Consortium), který zároveň na svých stránkách uvádí seznam svých členů, které jejich testy a standardy splňují. (Sosinsky, 2010)

3.10.3.2 Šifrování

V koncových bodech VPN spojení je VPN komunikace šifrována a dešifrována. K šifrování dat se využívají symetrické šifry, kdy odesílatel a příjemce nejčastěji využívají Diffie-Hellman algoritmus. Princip tohoto algoritmu spočívá ve vygenerování veřejného klíče/privátního klíče a veřejné klíče si navzájem vymění. Dále k šifrování dat se mohou využívat asymetrické šifry, kde se pracuje s páry klíčů, kdy je jeden veřejný, který slouží k šifrování dat, zatímco privátní slouží k jejich dešifrování.

Je zde provedena úvaha, kdy mohou být zašifrované jednotlivé segmenty trasy:

1. Z PC A na Server A
2. Ze Serveru A na Směrovač A
3. Ze směrovače A na Firewall A
4. Z Firewallu A přes síť WAN na Firewall B
5. Z Firewallu B na Směrovač B
6. Ze Směrovač B na Server B
7. Ze Serveru B na PC B

Z jednotlivých segmentů je zřejmé nutné šifrování dat v segmentu 4, kdy data cestují po rozsáhlé veřejné síti. (Zeltser, Winters, Frederick, Ritchey, & Northcutt, 2005) (Sosinsky, 2010)

3.10.3.3 Tunelování

Tunelování je proces, kdy je paket obalen (zapouzdřen) do jiného paketu. Zašifrovaný paket se pak nazývá *pasážérský paket* a jeho obalující paket se nazývá *přepravní paket*, který není šifrován, protože obsahuje informace o adresaci. Koncové body se nazývají *tunelová rozhraní*. Jsou zde sady protokolů, které mají různé způsoby využití. Jedny jsou určeny k samotnému zapouzdření zašifrovaných paketů, další mají za úkol transport dat v síti přes vytvořený tunel (např. TLS/SSL), nebo také skupina protokolů, které se používají v záhlaví šifrovacího protokolu a obsahuje adresní informace. Tyto protokoly nebudou dále popsány. (Sosinsky, 2010)

3.11 Správa počítačové sítě

Správa sítě je nedílnou součástí ať už malých, domácích sítí, nebo velkých, firemních. Na velikosti sítě nezáleží, ovšem je důležité, aby každá část sítě fungovala správně a nenastaly potíže, které by vedly k pádu části sítě (např. finanční oddělení firmy) nebo pádu celé vnitropodnikové sítě firmy. (Horák & Keršlágér, 2016)

3.11.1 Správa sítě

Správa sítě je velikým oříškem, jelikož potenciální zdroj chyb roste exponenciálně s rostoucím počtem uzlů v dané síti. Existuje hranice množství počítačů v síti, kdy náklady na práci s její údržbou budou větší než za pomoci automatizovaných systémů. Správce sítě musí umět pracovat ve všech spektrech správy sítě, které budou v následujících podkapitolách popsány. (Horák & Keršlágér, 2016)

3.11.1.1 Správa chyb

Je nutné si definovat, co je to chyba. Chybou je myšlena jak hardwarová, tak softwarová chyba, která vede k nežádoucím výsledkům. Cílem správy chyb je chybu najít, izolovat, poskytnout informace o chybě a navrhnout její řešení. Princip, jak nalézt chybu, je využitím určité množiny událostí, na kterých moderní počítačové stroje pracují. Počítače tedy jsou ve stavu pohotovosti, dokud neobdrží událost, na kterou mohou reagovat. Některé události jsou v množině údržby, jiné zase v množině, která kontroluje integritu paměti aj. Důležité události jsou zaznamenávány do protokolů událostí, který bude představen v následujícím odstavci.

Protokol událostí zaznamenává důležité události do paměti a tím umožňuje správci sítě si tyto události procházet. Taková událost je často ve tvaru: ID události nebo referenční typ, datum a čas, zdroj a název souboru protokolu, kde byla událost zaznamenána. Pro zachytávání události jsou používány čítače nebo agenti. Čítače jsou integrovány do systému vývojáři, naopak agenti jsou spustitelné soubory, které jsou instalovány za účelem sledování hodnot čítačů.

Korelace událostí rozpoznávají duplicitu totožných událostí a interpretují je uživateli jako smysluplná data. Příkladem může být chybové hlášení, kdy subsystém vyžaduje připojení k zařízení pomocí USB, ovšem toto zařízení připojené není. Systém opakovaně kontroluje připojení tohoto zařízení, ale s negativním výsledkem. Tímto způsobem mohou vznikat duplicitní události. (Sosinsky, 2010)

3.11.1.2 Správa konfigurace

Cílem správy konfigurace je nastavení systému tak, aby automatizovaně prováděly události, které se opakují, aktivně sledovaly stavy systému a tím snížily složitost správy sítě jako celku. Pomocí centrální konzole lze sledovat všechny možné konfigurace, které jsou ručně nastaveny uživatelem, nebo jsou nastaveny pro automatizované provádění událostí. Úlohy, které spadají pod správu patří:

- Nastavení počítačů a síťových zařízení,
- Instalace a konfigurace softwaru,
- Dokumentace konfigurace,

- Správa uživatelů a skupin,
- Vyžadované aktualizace a opravy softwaru.

Bude zde popsán životní cyklus softwaru a jeho nasazení, protože cílem správy konfigurace je zajištění užitečnosti softwaru a maximalizace využití softwaru během jednotlivých etap jeho nasazení. Etapy budou představeny bodově a dále nebudou více popsány.

Životní cykly softwaru a jeho vývoje jsou:

1. Software je nově pořízen a je aktuální.
2. Software je nasazen.
3. Software zastarává a je třeba ho monitorovat.
4. Software vyžaduje opravu nebo je nutný dílčí update.
5. Software je zastaralý a je třeba podstatný upgrade.
6. Software je zastaralý a je potřeba jej vyměnit. (Sosinsky, 2010)

3.11.1.3 Účtování a správa

Funkce účtování se týká měření využití dat pro účely fakturace zákazníkům nebo oddělením. Tato funkce spoléhá na údaje poskytované nástroji pro správu výkonu, konkrétně pro nástroje, které sledují provoz v síti. Příkladem síťových funkcí, které se měří za účelem fakturace jsou:

- Objem dat posílané přes určité spojení,
- Konkrétní události s určitou aktivitou (např. vytváření vzdáleného připojení),
- Počet spotřebovaných síťových prostředků,
- Hodnoty špičkového využití.

Mnohé sítě tuto správu nepotřebují, tedy nejsou hlavní součástí operačních systémů, nebo softwarových prostředků pro správu sítě od třetích stran.

3.11.1.4 Správa výkonu

Cílem této správy je zajistit správné fungování prostředků sítě ve standardních podmínkách. V případě snížení standardu sítě nabídne optimální řešení, jak zlepšit výkon

síťových prostředků. Tento monitoring sítě, který probíhá pomocí čítačů, shromažďuje data, pomocí kterých může správce sítě detekovat nebo vyloučit místo chyby, popřípadě zamezit potencionálním chybám v síti. Tyto čítače nezachytávají události v síti, ale také měří jejich frekvenci, trvání, hodnotu nebo jiný parametr, které nejlépe vyhodnotí funkčnost subsystému, na kterém je čítač nastaven. Každý operační systém obsahuje aplikaci pro sledování výkonu. Typickým příkladem je *Správce úloh* v operačním systému Windows, kde je možné si zobrazit real-time informace (viz. obrázek). Tento nástroj slouží pro sledování hardwaru sítě, ale existují také programy, které sledují výkon sítě jako takové a sledují komunikaci probíhající v síti. Paketové sniffery, jak se jim také říká, jsou nejpoužívanější nástroje pro sledování výkonu. Tento nástroj zachycuje data v síti, je schopen je přečíst a analyzovat jejich obsah. Neumí pouze číst data, ale také analyzovat chyby sítě, detekovat porušení zabezpečení, vytvářet reporty o výkonu, zjišťování použitých protokolů a filtrovat pakety podle pravidel a v neposlední řadě zachytávat relace v síti. (Horák & Keršláger, 2016)

3.11.1.5 Správa zabezpečení

Správa zabezpečení umožňuje uživatelům nebo skupinám uživatelů sítě povolit přístup, nebo ho zamítnout, k jednotlivým síťovým prostředkům nebo službám. Tato správa je nedílnou součástí operačních systémů, bez které by nebylo možné nastavovat práva a omezení pro uživatele. Správa sítě spoléhá na dvě důležité funkce, autentizaci uživatelů a na systém ochrany dat při jejich přenosu po síťových prostředcích. (Sosinsky, 2010)

3.11.2 Příkazy pro diagnostiku

V této podkapitole se dozvíme o užitečných možnostech příkazového řádku, pomocí kterého lze spustit příkazy sloužící ke zjištění stavu sítě a jejího testování a v případě problému lokalizovat nefunkční část sítě nebo systém. Se vznikem prvních počítačů a jejich operačních systémů byli příkazové shelly nedílnou součástí počítačové technologie. Budou zde vybrány nejznámější příkazové shelly a následně popsány. (Kretchmar, 2005)

3.11.2.1 Diagnostika sítě

Identifikace problému v síti může být velice obtížná a vyžaduje jisté znalosti. Síťové operační systémy do sebe integrovali široké spektrum technologií, které pomohou vyhodnotit funkčnost sítě a předat relevantní data uživateli. Ať už se jedná o utility, které se spouští pomocí příkazového řádku, nebo utility, které své funkce nabízí prostřednictvím grafického rozhraní.

Zde je sepsán metodický postup, jak řešit problémy v síti.

1. Dokumentace problému a stanovení hypotézy.
2. Shromáždit informace týkající se souvisejících systému a připojení.
3. Zvolit vhodný diagnostický nástroj a ověřit výsledky.
4. Postupně zužovat rozsah problému.
5. Segmentace, izolace a testování možné chyby pomocí testovacích procesů, náhrady a/nebo výměny.
6. Potvrzení hypotézy odstraněním chyby. (Sosinsky, 2010)

3.11.2.2 Nástroje příkazového řádku

Shell nebo CLI je textové rozhraní, které přijímá uživatelský vstup a překládá jej na příkazy. Na tyto příkazy pak operační systém reaguje. Rozhraní příkazového řádku se používají už od konce 60. let 20. století. Nebyly vytvořeny žádné standardy pro jejich formu zápisu, tedy výrobci si do svých síťových operačních systémů integrovaly příkazové řádky používající různé programovací jazyky. Tato integrace způsobila rozmanitost syntaxe síťových příkazů.

Bude zde sepsán seznam příkazových shellů, které autor zvolil na základě jejich nabídky množiny síťových funkcí. Mezi tyto shelly patří:

- CMD.COM – Nástroj zodpovědný za příkazový řádek v systémech společnosti Microsoft.
- SH, BASH, CSH a KSH – Toto jsou unixové shelly, které jsou integrovány v závislosti na verzi systému UNIX nebo Linuxu. Tyto systémy mohou využívat jeden a více těchto shellů.

- PowerShell – Skriptovací jazyk, který je implementován jako příkazový řádek pro systémy rodiny Microsoft
- REXX – Shell společnosti IBM.
- PHPsh – Shell jazyka PHP.
- Python – Interpret jazyka Python.
- JavaScript a BeanShell – JS je interaktivním rozhraním skriptovacího jazyka JavaScript a BS je shellem pro jazyk Java. (Kretchmar, 2005) (Sosinsky, 2010)

3.11.3 Vzdálený přístup

Jedná se o software typu klient-server, který připojuje klienta k serveru pro vzdálený přístup. Jsou dva základní softwary, pomocí kterých se lze vzdáleně připojit. První software připojuje klienty prostřednictvím veřejné telefonní sítě, nicméně moderním trendem se připojování vzdálených klientů pomocí služby VPN přes Internet.

Software vzdálené plochy umožní klientovi se připojit na hostitelského systému tak, že plocha hostitelského systému je promítána na ploše připojeného vzdáleného klienta. Tato možnost, tedy využití vzdálené plochy, lze využít k provedení vzdálených výpočtů, správě vzdálených systému, aplikace technické podpory nebo aplikace vzdálené výuky.

Hlavním smyslem vzdáleného přístupu je zapůsobit na klienta tak, aby měl pocit, že skutečně ovládat server/počítač, ke kterému se vzdáleně připojil. Pro vytvoření takového dojmu není jen potřeba dostatečné šířky pásma, pro kvalitní přenos dat, ale je nutné uživatele autentizovat, autorizovat a zabezpečit vzdálené připojení. K dosažení těchto vlastností jsou standardizovány tyto nejčastěji používané protokoly, které dále nebudou popsány:

- SLIP
- PPP
- PPPoE
- PPTP
- L2TP

Protokoly SLIP, PPP a PPPoE se používají pro vzdálený přístup prostřednictvím telefonického připojení, naopak protokoly PPTP a L2TP jsou přidruženy k protokolům služby VPN. Pro autentizaci a autorizaci klienta je nutné, aby klient prošel autorizační službou. Touto službou vybavila společnost Microsoft svoje operační systémy Windows Server službou, která se nazývá NPS.

3.11.3.1 Služba vzdáleného přístupu

Tato služba přijímá příchozí připojení od vzdálených uživatelů, ověřuje jejich ověření, následně po úspěšném ověření vytváří zabezpečené připojení, pomocí kterého uživatel dostane přístup k síťovým prostředkům. Servery pro vzdálený přístup jsou stavěny tak, aby přijímaly některé z těchto typu připojení:

- PPP nebo SLIP protokolu využívají DSL modemy
- Směřovaný provoz přes síť s protokolem IP
- Pomocí služby VPN
- Širokopásmové připojení ATM
- Asynchronní terminálové připojení využívají například protokol Telnet

Většina serverů vzdáleného přístupu využívají kombinaci těchto možností a v případě potřeby často umožňují překlad mezi různými použitými protokoly.

3.11.3.2 Vzdálená plocha

Je software, který umožňuje graficky znázornit prostředí, ke kterému se vzdálený uživatel připojuje. Ačkoli na první pohled není rozdíl mezi vzdálením přístupem a vzdálenou plochou, opak je však pravdou. Zatímco vzdálený přístup zajišťuje přístup k síťovým prostředkům, zatímco vzdálená plocha umožňuje klientovi zobrazit a řídit serverový systém tak, jako by seděl přímo za ním. Tomuto připojení se říká relace, tak jako se toto označení používá pro připojení k terminálovému serveru.

Technologie vzdálené plochy se využívá pro:

- Vzdálené výpočty
- Vzdálenou správu systému
- Technickou podporu

- Vzdálenou výuku

Klienti vzdálené plochy se připojují k systému pomocí protokolů pro připojení VPN. Tento způsob připojení je optimalizován pro přenos vstupů klávesnice a myši klienta a přenos výstupu na klientovo zobrazovací zařízení. (Sosinsky, 2010)

4 Vlastní práce

4.1 Charakteristika podniku

Je nutné provést základní charakteristiku hotelu DAR pro podrobnější analýzu jeho sítě a následného návržení nové sítě dle jeho potřeb.

Hotel se nachází na Starém městě na Praze 1, v ulici Kožná, který byl v roce 2006 zrekonstruován do dnešní podoby. Hotel obsahuje 5 podlaží obsahujících pokoje, kancelářské prostory a restaurační zařízení. Dále obsahuje terasu na střeše budovy, terasu v prvním nadúrovňovém podlaží a vinárnu, která je k dispozici v suterénu. Prostory vinárny jsou v ranních hodinách využívány pro snídani hotelových hostů. V přízemí se nachází recepce, s 24 hodinovým provozem. Prostředí restauračního zařízení je inspirováno dobou za císaře Rudolfa II., který byl posedlí alchymií. Všechny tyto patra jsou propojeny jediným výtahovým zařízením a točným schodištěm. Hotel DAR je podle jednotné klasifikace hotelů ohodnocen třemi hvězdičkami, spadá do kategorie Komfort. Splňuje tato kritéria, některé však přesahuje:

- **Minimální velikost 75 % pokojů:** Jednolůžkový 9 m², dvoulůžkový 13 m²
- **Vybavení pokoje:** Lůžko, šatník, koš na odpadky, 1 sedací možnost na 1 lůžko, stůl/psací stůl/deska, stolek na kufr, osvětlení pokoje, noční lampička, uzamykatelná skříň/zásuvka
- **Hygienický komfort:** 100 % pokojů má tekoucí studenou a teplou vodu, krom toho je k dispozici na 10 lůžek bez sprchy/WC na poschodí 1 koupelna/WC, 90 % pokojů je vybaveno sprchou/vanou a WC.
- **Vybavení koupelny a WC:** Froté ručník a froté osuška na 1 hosta, zrcadlo nad umyvadlem, osvětlení nad umyvadlem, odkládací prostor/polička, velké zrcadlo (min. 0,4 m²), předložka před umyvadlem nebo před sprchou/vanou, krytý odpadkový koš, 1 pohárek na osobu
- **Bezplatný drobný artikl:** Hygienický pytlík, 1 mýdlo na hosta, dopisní papír, psací potřeby, hotelová dokumentace
- **Doplňkový artikl:** Lžice na obuv, kartáč na oděv, kartáč/hadřík na obuv, 1 nápojové sklo na hosta, otvírač lahví

- **Rozhlasový a televizní příjem:** 90 % pokojů má rozhlas a televizor (má 100%)
- **Telefon:** 75 % pokojů je vybaveno telefonním přístrojem včetně návodu pro jeho použití (příchody a odchody hovorů mohou být realizovány přes recepci), noční hovory umožněny (má 100%)
- **Telefax, On-line, Internet:** Telefax v objektu
- **Možnost úschovy, trezor:** Trezor na recepci
- **Recepce:** Obsazena 12 hodin denně a dosažitelnost zvonkem/telefonem (má obsazenost 24 hodin)
- **Společenské místnosti pro hotelové hosty:** 1 společenská místnost/prostor (např. místnost pro podávání snídaní či restaurace), 1 společenská místnost/prostor (např. sedací kout v prostoru příjmu hosta)
- **Snídaňový servis:** Rozšířená snídaňová nabídka
- **Jídelní servis:** Oběd 2 hodiny, večere 3 hodiny
- **Nápojový servis:** Minibar/nápojový automat/lednička na recepci
- **Restaurace:** 1

Od dob vzniku hotelu, nebyly v budově prováděny rozsáhle obměny počítačového zařízení a tím hotel DAR ztrácí krok s moderními technologiemi, například v oblasti Wi-Fi technologií, které jsou nyní považovány za standardní vybavení a hotelu DAR nejsou dostačující. Dále se zde nacházejí bezpečnostní kamery, které nejsou schopné nahrávat v rozlišení HD a zároveň obsahují úzké zorné pole ani noční vidění. V následujících kapitolách bude provedena analýza současného stavu infrastruktury počítačové sítě v budově. Od majitelů hotelu byly získány půdorysy budovy, do kterých budou zanášeny sledovaná a navrhovaná řešení. (Hotel Fontána)

4.1.1 Analýza stávající sítě hotelu a návrh nové

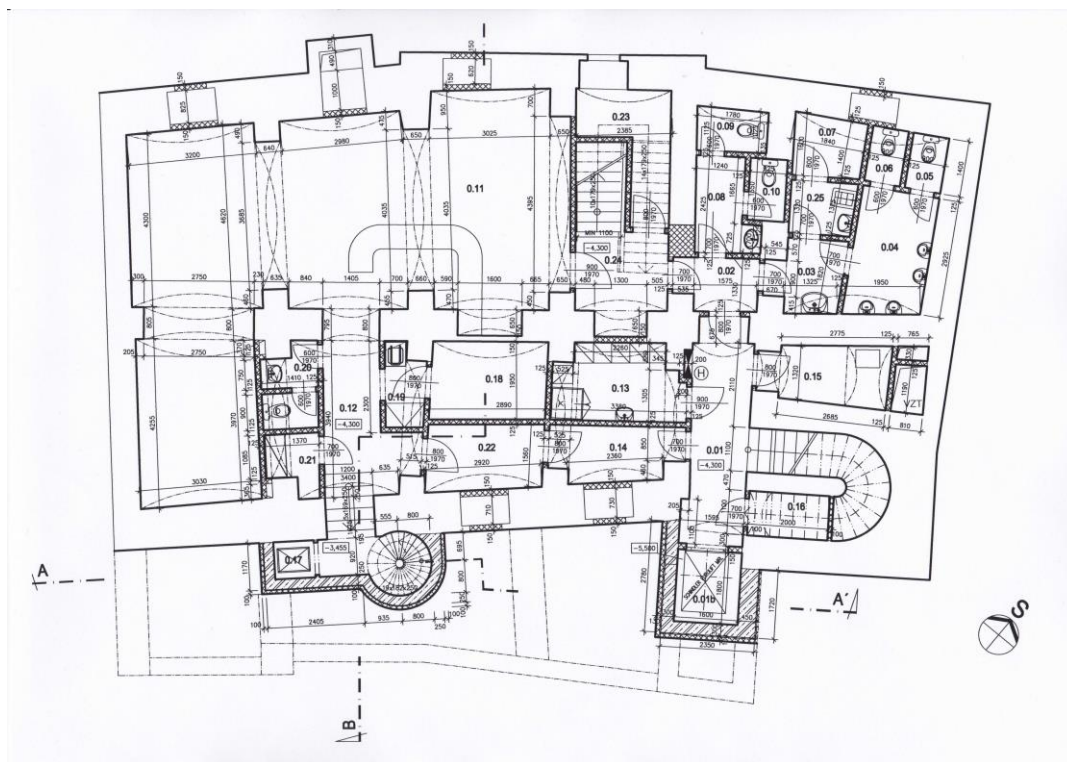
4.1.1.1 Půdorys budovy

V této kapitole budou vyobrazeny půdorysy budovy podle jednotlivých podlaží a jejich krátká charakteristika. Tyto půdorysy vznikly v programu AutoCAD. Jedná se o populární software určený pro 2D a 3D modelování. Součástí výkresů jsou i popisová pole

a legendy jednotlivých půdorysů, ale protože nejsou zde zcela potřeba, proto jsou vyobrazené pouze půdorysy samotné. Všechny výkresy uvedené v této práci, jsou v měřítku 1:90 a tisknuté na papíře formátu A4. Po vložení obrázků do programu Microsoft Word byly upraveny velikosti obrázků a neodpovídají tedy velikosti formátu papíru A4. Autor těchto nákresů si nepřál být zveřejněn.

PP1

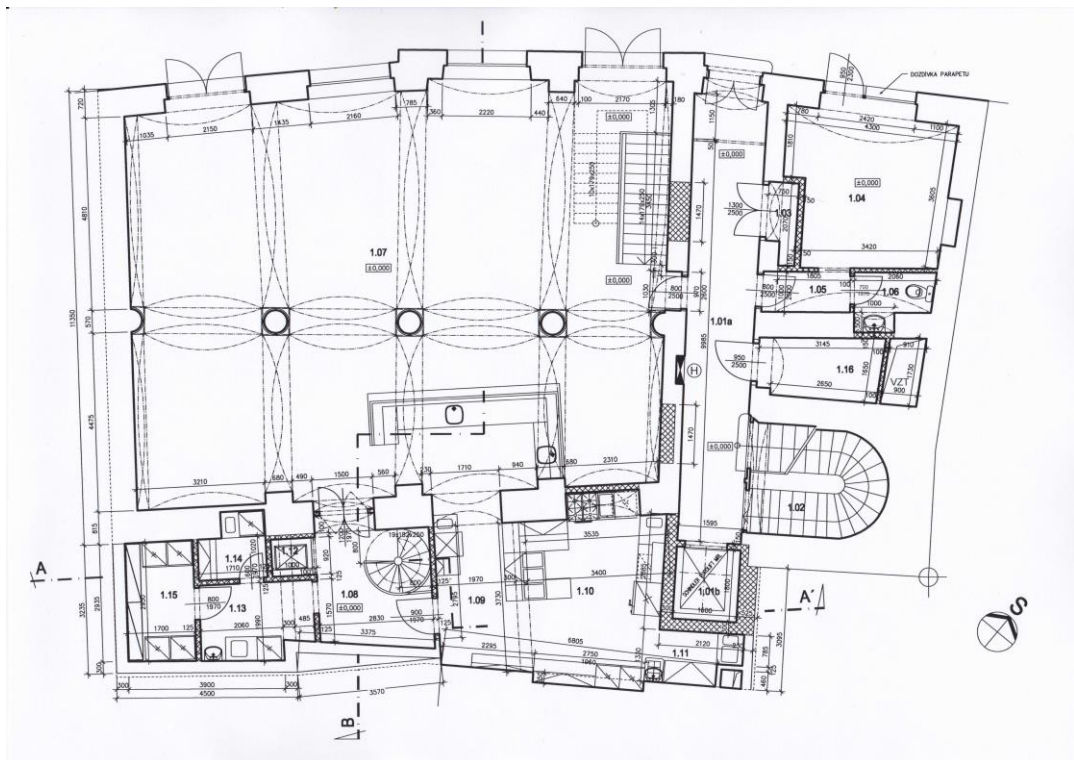
Tento půdorys vyobrazuje jediné podúrovňové podlaží nacházející se v hotelovém zařízení. V tomto podlaží se nenachází žádné obytné jednotky. V podlaží se nachází vinárna (0.11), která je v ranních hodinách využívána na snídani pro hotelové hosty. Dále se zde nachází toaletní zařízení, jak pro dámy, tak i pány. Schodiště spojující vinárnu s restauračním zařízením. Dále se zde nachází točité schodiště a výtah, která spojují vinárnu se všemi patry hotelového zařízení. V neposlední řadě jsou zde prostory určené jako hotelové zázemí a skladovací prostory určené ke skladování trvanlivého materiálu. V době realizace zde bylo přistavěno točité kovové schodiště a servisní výtah, které propojují toto patro s kuchyní restaurace, pro lepší zásobování podúrovňového podlaží. Nosné stěny jsou cihelného charakteru s betonovými překlady.



Obrázek 1 - Půdorys PP1 (autor)

NP1

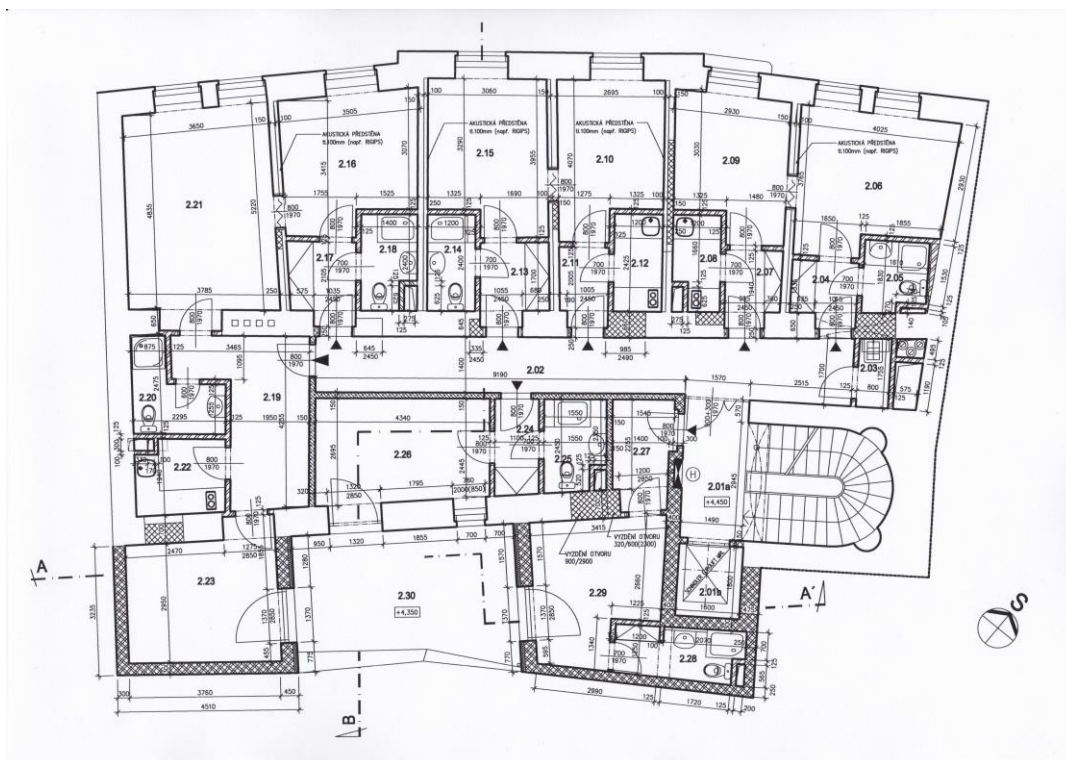
Tento půdorys vyobrazuje první nadúrovňové podlaží, které je rozdělené v přibližném poměru 70:30 na restaurační zařízení a hotelové zařízení. Tyto dvě samostatné jednotky jsou propojené dvěma zabezpečené pomocí čipového terminálu, kde mohou z hotelové zařízení vstupovat zákazníci, nebo personál, do restauračního zařízení a naopak. Na tomto patře se nachází recepční sál (1.04), kde zaměstnanci vstupují do interakce se zákazníky z důvodů check-in, check-out služeb, plateb a podobných služeb související s ubytováním. Za recepcí se nachází místnost k úschově zavazadel. Na tomto patře se nenachází žádné ubytovací prostory. Dále se zde nachází točité schodiště a výtah, která spojují recepci se všemi patry hotelového zařízení. V restauračním zařízení se nachází jídelní sál (1.07) o přibližné kapacitě 80 lidí, dále je zde kuchyň, skladovací prostory potravin a chladicí místnost. V době realizace zde bylo přistavěno točité kovové schodiště a servisní výtah, která propojují toto patro se zázemím vinárny, pro lepší zásobování podúrovňového podlaží. V neposlední řadě se zde nachází schodiště pro přístup veřejnosti do vinárny a toaletních zařízení v podúrovňovém podlaží. Nosné stěny jsou cihelného charakteru s betonovými překlady.



Obrázek 2 - Půdorys NP1 (autor)

NP2

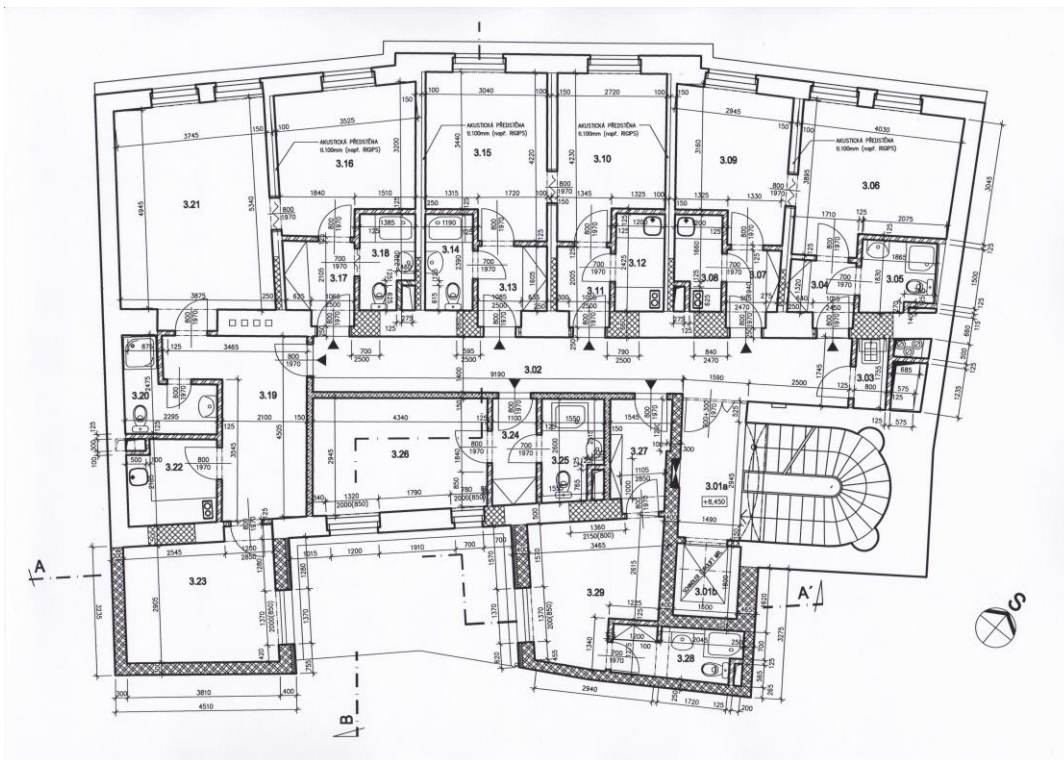
Tento půdorys vyobrazuje druhé nadúrovňové podlaží, které již není rozdělené na restaurační a hotelové zařízení, ale je pouze hotelového charakteru. Na tomto patře se nachází stěžejní místnost této diplomové práce, tedy pracovna (2.29) pro vedení hotelu, kde bude umístěné potřebné vybavení pro realizaci nové sítě. Na tomto patře se nachází 6 samostatných pokojů a 1 apartmá obsahující 2 pokoje a 2 koupelny pro větší skupiny. Všechny pokoje obsahují standartní vybavení odpovídající 3 hvězdičkovému hotelu. Teresa (2.30) je přístupná z pokojů 2.23, 2.30 a 2.29 (pracovna) a ostatní pokoje mají výhled do ulice Kožná. V neposlední řadě se zde nachází točité schodiště a výtah, která spojují toto patro se všemi patry hotelového zařízení. Nosné stěny jsou cihelného charakteru s betonovými překlady.



Obrázek 3 - Půdorys NP2 (autor)

NP3

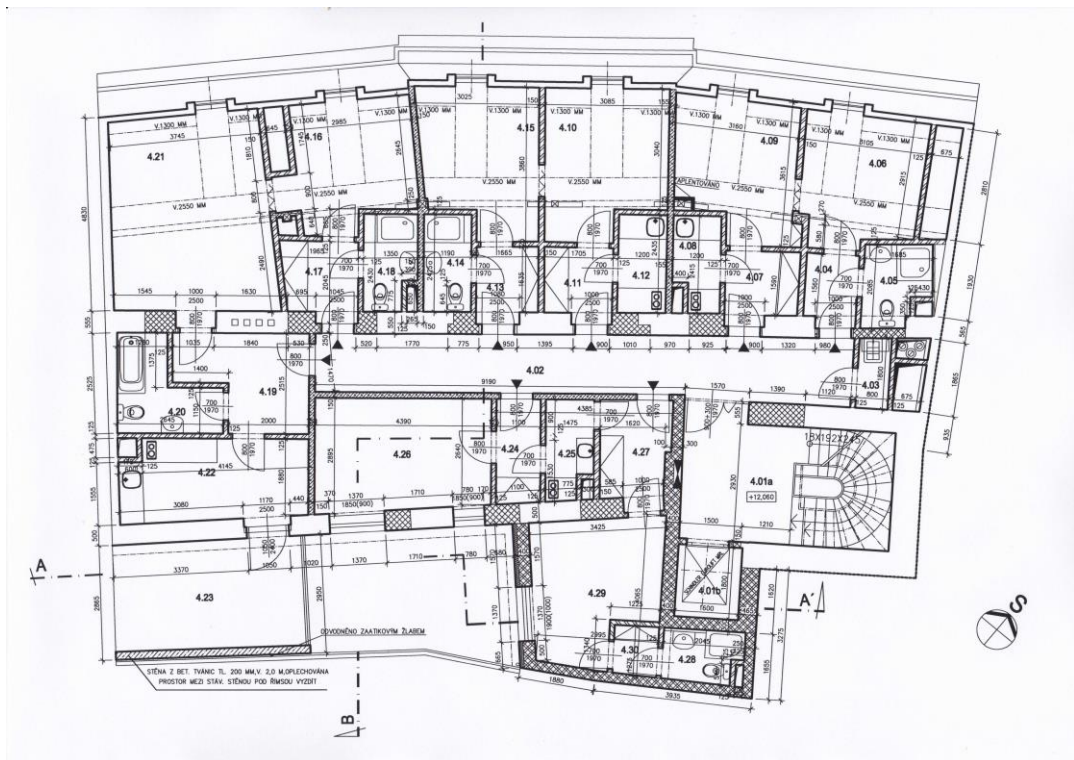
Tento půdorys vyobrazuje třetí nadúrovňové podlaží hotelového zařízení, kde se nenachází žádné prostory pro hotelové vedení. V místě pracovny je vybudován další samostatný pokoj pro hotelové hosty. Na tomto patře se tedy nachází 7 samostatných pokojů a 1 apartmá obsahující 2 pokoje a 2 koupelny pro větší skupiny. Všechny pokoje obsahují standartní vybavení odpovídající 3 hvězdičkovému hotelu. Pokoje 3.23, 2.26, 3.29 mají výhled do atria hotelu a ostatní pokoje mají výhled do ulice Kožná. V neposlední řadě se zde nachází točité schodiště a výtah, která spojují toto patro se všemi patry hotelového zařízení. Nosné stěny jsou cihelného charakteru s betonovými překlady.



Obrázek 4 - Půdorys NP3 (autor)

NP4

Tento půdorys vyobrazuje čtvrté nadúrovňové podlaží hotelového zařízení, kde se nenachází žádné prostory pro hotelové vedení, ale jeden z pokojů (4.09) je využit pro vytvoření adekvátního a pohodlného zázemí pro potřeby personálu hotelu. Na tomto patře se tedy nachází 6 samostatných pokojů a 1 apartmá obsahující 2 pokoje a 2 koupelny pro větší skupiny. Všechny pokoje obsahují standartní vybavení odpovídající 3 hvězdičkovému hotelu. Pokoje 4.23, 4.26, 4.29 mají výhled do atria hotelu a ostatní pokoje mají výhled do ulice Kožná. V neposlední řadě se zde nachází točité schodiště a výtah, která spojují toto patro se všemi patry hotelového zařízení. Toto patro je poslední zastávkou hotelového výtahu, které spojuje patra od prvního podúrovňového podlaží až do čtvrtého nadúrovňového podlaží. V tomto patře pokračuje točité schodiště na střešní terasu hotelu. Nosné stěny jsou cihelného charakteru s betonovými překlady.



Obrázek 5 - Půdorys NP4 (autor)

4.1.1.2 Půdorys budovy s původním zařízením

Pro popis jednotlivých pozic zařízení byly použity zjednodušené plány budovy, na kterých jsou vyobrazena stěžejní zařízení pro chod hotelu.

PP1

Kamery a Wi-Fi antény

Na tomto patře se nachází celkem 2 kamery pro vnitřní použití. Jedna kamera je osazena tak, aby zaznamenávala pohyb kolem barového pultu vinárny. Druhá kamera je osazena tak, aby zaznamenávala pohyb v chodbě od výtahu a schodišti propojující ostatní patra. Všechny kamery jsou osazené na svislé zdi ve výšce 2,8 metrů nad podlahou.

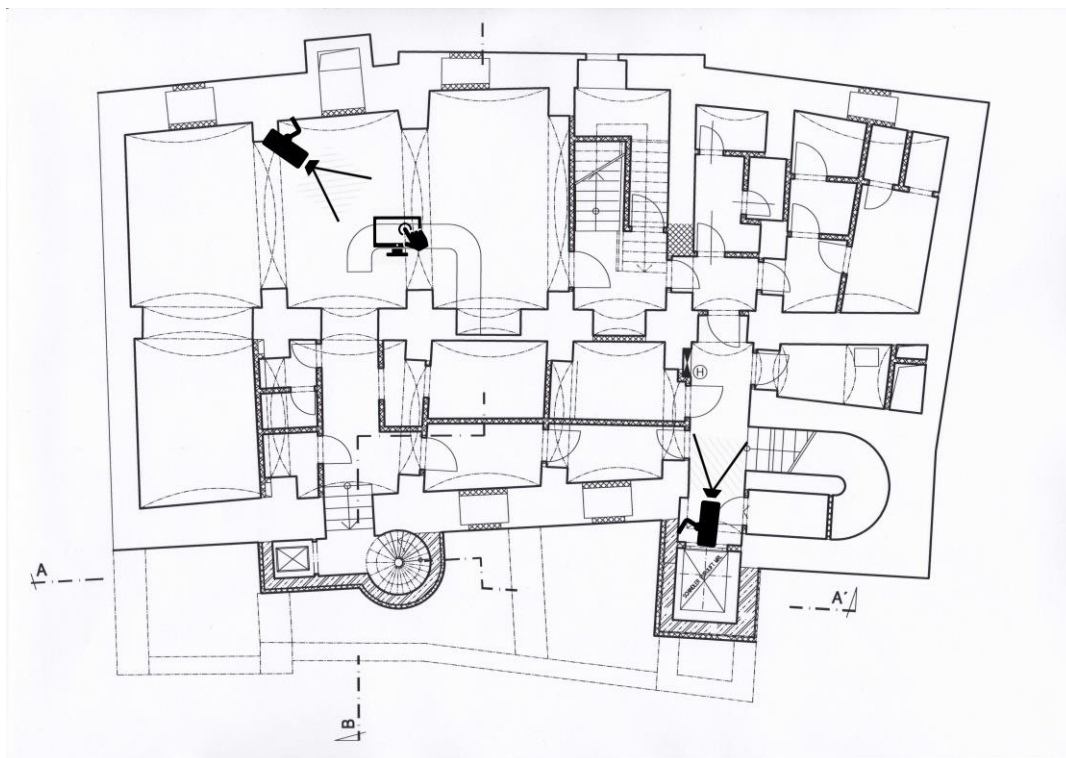
Nenachází se zde žádná Wi-Fi anténa.

Počítače a tiskárny

Ve vinárně je instalován dotykový All-in-one počítač obsahující aplikaci EET, k tomuto počítači je připojena tiskárna na tisk účtenek.

Ostatní zařízení

Nenachází se zde žádný analogový telefon.



Obrázek 6 - Analýza PP1 se stávajícími prvky (autor)

Závěr

Nedostatečný počet kamer zajišťující pokrytí celého prostoru tohoto patra včetně prostor zázemí vinárny. Kamery jsou zastaralé, nenahrávají ani nestrreamují v rozlišení HD ani neobsahují noční vidění. Výrobce kamer nebyl uveřejněn. Absence Wi-Fi antény nezajišťuje pokrytí patra internetem. Personál vinárny není schopen komunikovat s pracovníky hotelu z důvodu absence telefonního spojení.

NP1

Kamery a Wi-Fi antény

Na tomto patře se nachází celkem 4 kamery pro vnitřní použití a 1 kamera pro venkovní použití. Všechny kamery jsou osazené na svislé zdi ve výšce 2,8 metrů nad

podlahou. Dvě kamery se nachází v restauračním sále, které jsou osazené v protilehlých rozích, vzhledem na jejich staří nemají takovou kvalitu, aby dostatečně pokryly celý prostor restauračního sálu. Další kamera se nachází v recepčním sále a poslední vnitřní kamera se nachází v chodbě od recepce k výtahu a schodišti propojující ostatní patra. Poslední, venkovní kamera je osazena na vnější zdi a její zorné pole směřuje na hlavní vchod a vchod do recepce. V zázemí restaurace se nenachází žádná kamera.

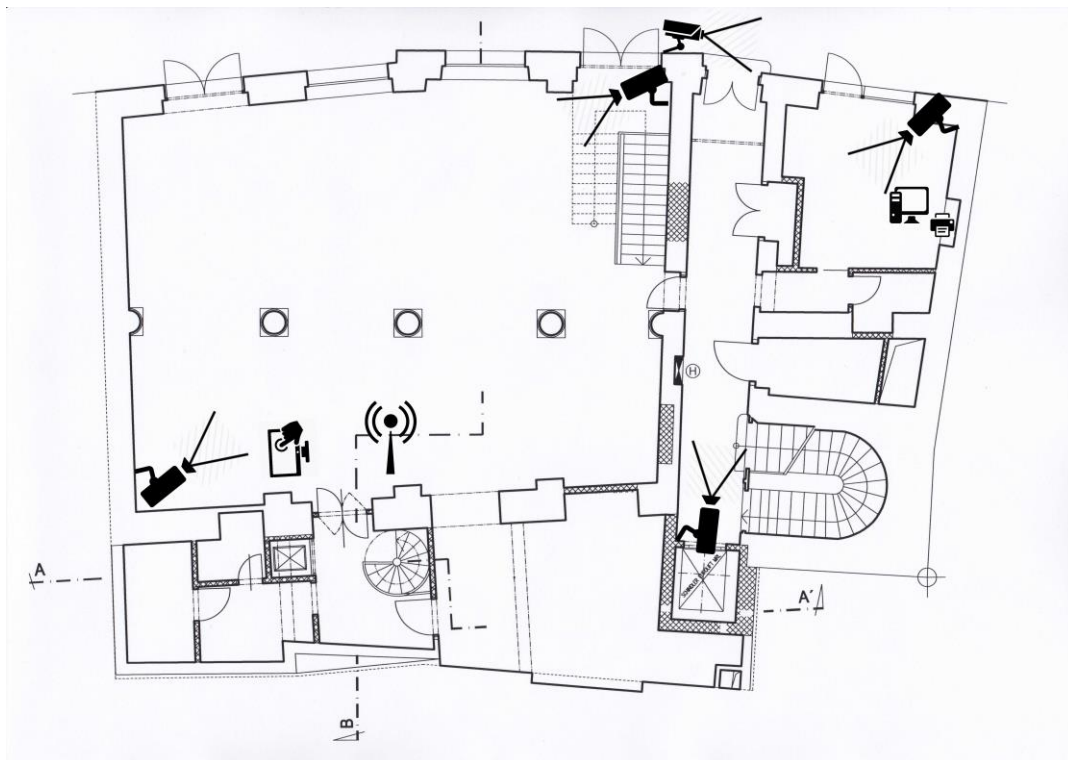
Wi-Fi anténa je položena na barovém stole ve výšce 1,2 metru.

Počítače a tiskárny

Na tomto patře se nacházejí celkem 2 počítače. Jeden počítač se nachází v recepčním sále a jen určen pro chod recepce a všechny administrativní úkoly s tím spojené. K tomuto počítači je připojena tiskárna pomocí USB portu, není tedy připojena do sítě a není sdílená. V restauračním sále je nainstalována dotykový All-in-one počítač obsahující aplikaci EET, k tomuto počítači je připojena tiskárna na tisk účtenek, ke které je přidružena tiskárna v kuchyňském zázemí pro správnou expedici objednávek a eliminaci chyb.

Ostatní zařízení

V recepčním sále se nachází analogový telefon pro potřeby recepce a je spojen s telefonní ústřednou hotelu.



Obrázek 7 - Analýza NP1 se stávajícími prvky (autor)

Závěr

Nedostatečný počet kamer zajišťující pokrytí celého prostoru tohoto patra, obzvláště venkovních vchodů nebo zázemí restaurace (kuchyň), zároveň jsou kamery zastaralé, nenahrávají ani nestreamují v rozlišení HD ani neobsahují noční vidění. Výrobce kamer nebyl uveřejněn. Jediná Wi-Fi anténa zcela nepokrývá celý prostor tohoto patra a je umístěna ve špatné pozici. Počítače jsou 8 let zastaralé s operačním systémem Vista. Tiskárna není síťová a není ani sdílená. Personál restaurace není schopen komunikovat s pracovníky hotelu z důvodu absence telefonního spojení.

NP2

Kamery a Wi-Fi antény

Na tomto patře se nachází celkem 3 kamery pro vnitřní použití. První kamera se nachází na chodbě od výtahu a schodiště, konkrétně nad dveřmi pracovny ve výšce 2,8 metru. Zbýlé dvě kamery se nachází v chodbě spojují ubytovací zařízení hotelů ve výšce

2,8 metru. Obě kamery svým zorným polem pokrývají celý prostor chodby, ale jejich velice malé rozlišení nespĺňuje plné pokrytí chodby.

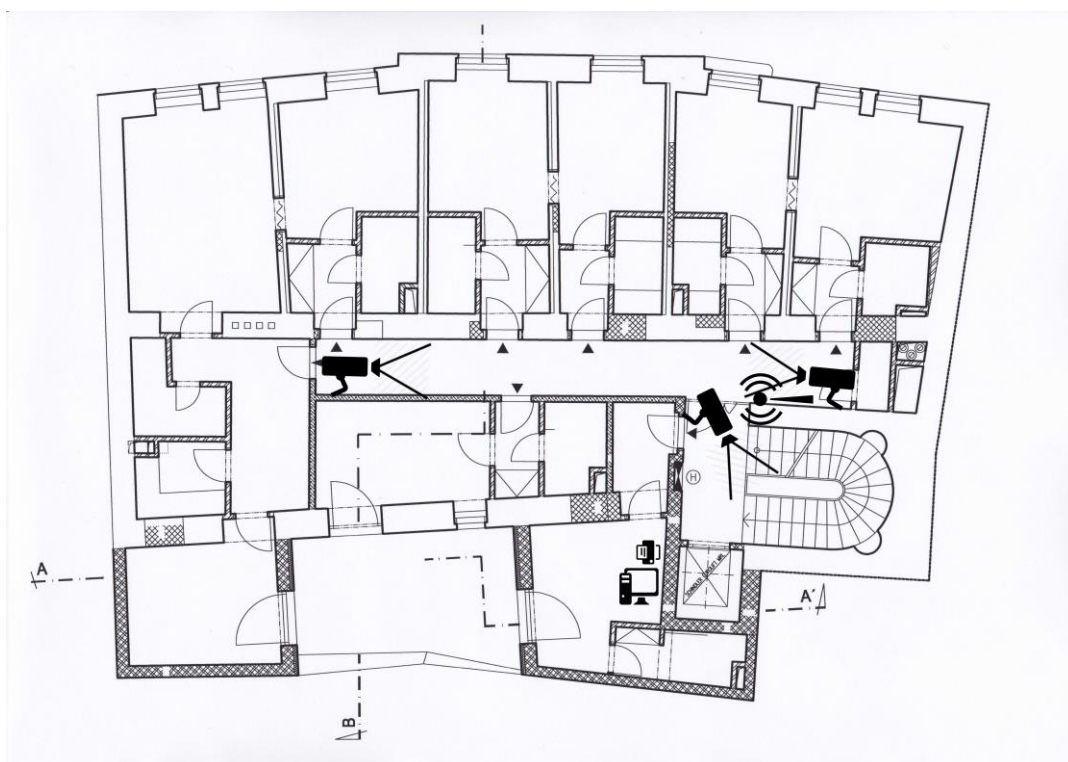
Na tomto patře se nachází 1 Wi-Fi anténa lokalizována nad vstupními dveřmi do chodby k ubytovacím zařízením ve výšce 3 metry.

Počítače a tiskárny

Na tomto patře se nachází 1 počítač v pracovně hotelu, ke kterému je připojena tiskárna pomocí USB portu, není připojena do sítě a není ani sdílená.

Ostatní zařízení

V každém pokoji a pracovně se nachází analogový telefon, který je propojen do telefonní ústředny hotelu. V každém pokoji se nachází datová zásuvka.

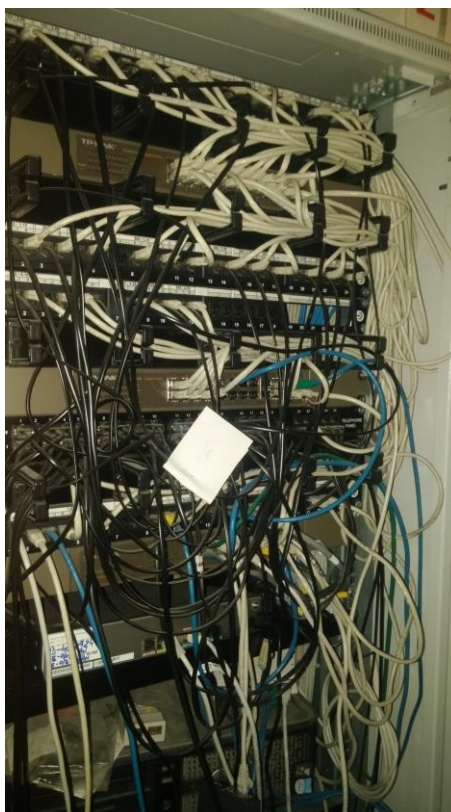


Obrázek 8 - Analýza NP2 se stávajícími prvky (autor)

Analýza rozvaděče

Během analýzy tohoto patra, proběhala také analýza současného rozvaděče. Dle obrázků je patrný chaos v datových kabelech a vysoký stupeň nečistot usazených na perifériích. Jsou zde patrné patch panely umístěné v horní části rozvaděče, které distribuují internet do pokojů a taky analogové telefony. Dále v rozvaděči se nachází switche, zálohovací jednotka pro kamery, UPS zařízení, nefunkční server a telefonní ústředna. Telefonní ústředna by bylo jediné zařízení, které by se zachovalo v nové síti.

Je zde jisté riziko nebezpečí požárů, protože na všem jsou značné vrstvy prachu, který velice rychle může vzplanout. Prach také velice zatěžuje chladicí systémy periférií a tím snižují jejich výkon. Nové řešení bude obsahovat cable management.



Obrázek 9 – Analýza rozvaděče (autor)



Obrázek 10 – Analýza rozvaděče (autor)

Závěr

Nedostatečný počet kamer zajišťující pokrytí celého prostoru tohoto patra, obzvláště venkovního prostoru terasy, který je přístupný ze tří stran, zároveň jsou kamery zastaralé, nenahrávají ani nestrámují v rozlišení HD ani neobsahují noční vidění. Výrobce kamer nebyl uveřejněn. Jediná Wi-Fi anténa zcela nepokrývá celý prostor tohoto patra a je umístěna ve špatné pozici. Počítač je 8 let starý s operačním systémem Vista. Tiskárna není síťová a není ani sdílená.

Rozvaděč obsahuje zastaralé a nefunkční periferie, které jsou pokryté značnou vrstvou nečistot, které mohou způsobit poškození hardwaru nebo dokonce požár. Chaos v kabelech znemožňuje efektivní orientaci v propojených periferiích.

NP3

Kamery a Wi-Fi antény

Na tomto patře se nachází celkem 3 kamery pro vnitřní použití. První kamera se nachází na chodbě od výtahu a schodiště ve výšce 2,8 metru. Zbylé dvě kamery se nachází v chodbě spojují ubytovací zařízení hotelů ve výšce 2,8 metru. Obě kamery svým zorným polem pokrývají celý prostor chodby, ale jejich velice malé rozlišení nespĺňuje plné pokrytí chodby.

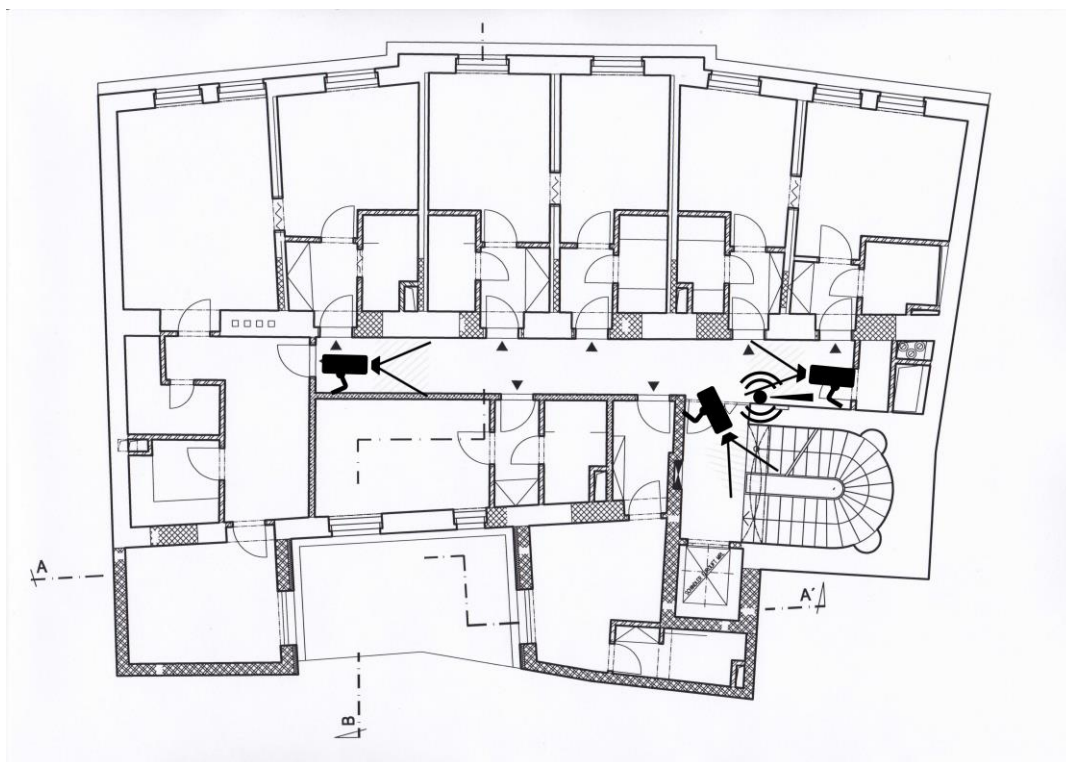
Na tomto patře se nachází 1 Wi-Fi anténa lokalizována nad vstupními dveřmi do chodby k ubytovacím zařizzením ve výšce 3 metry.

Počítače a tiskárny

Na tomto patře se nenachází žádný počítač ani tiskárna.

Ostatní zařizzení

V každém pokoji se nachází analogový telefon, který je propojen do telefonní ústředny hotelu. V každém pokoji se nachází datová zásuvka.



Obrázek 11 - Analýza NP3 se stávajícími prvky (autor)

Závěr

Nedostatečný počet kamer zajišťující pokrytí celého prostoru tohoto patra, zároveň jsou kamery zastaralé, nenahrávají ani nestreamují v rozlišení HD ani neobsahují noční vidění. Výrobce kamer nebyl uveřejněn. Jediná Wi-Fi anténa zcela nepokrývá celý prostor tohoto patra a je umístěna ve špatné pozici.

NP4

Kamery a Wi-Fi antény

Na tomto patře se nachází celkem 3 kamery pro vnitřní použití. První kamera se nachází na chodbě od výtahu, a schodiště ve výšce 2,8 metru. Zbylé dvě kamery se nachází v chodbě spojují ubytovací zařízení hotelů ve výšce 2,8 metru. Obě kamery svým zorným polem pokrývají celý prostor chodby, ale jejich velice malé rozlišení nespĺňuje plné pokrytí chodby.

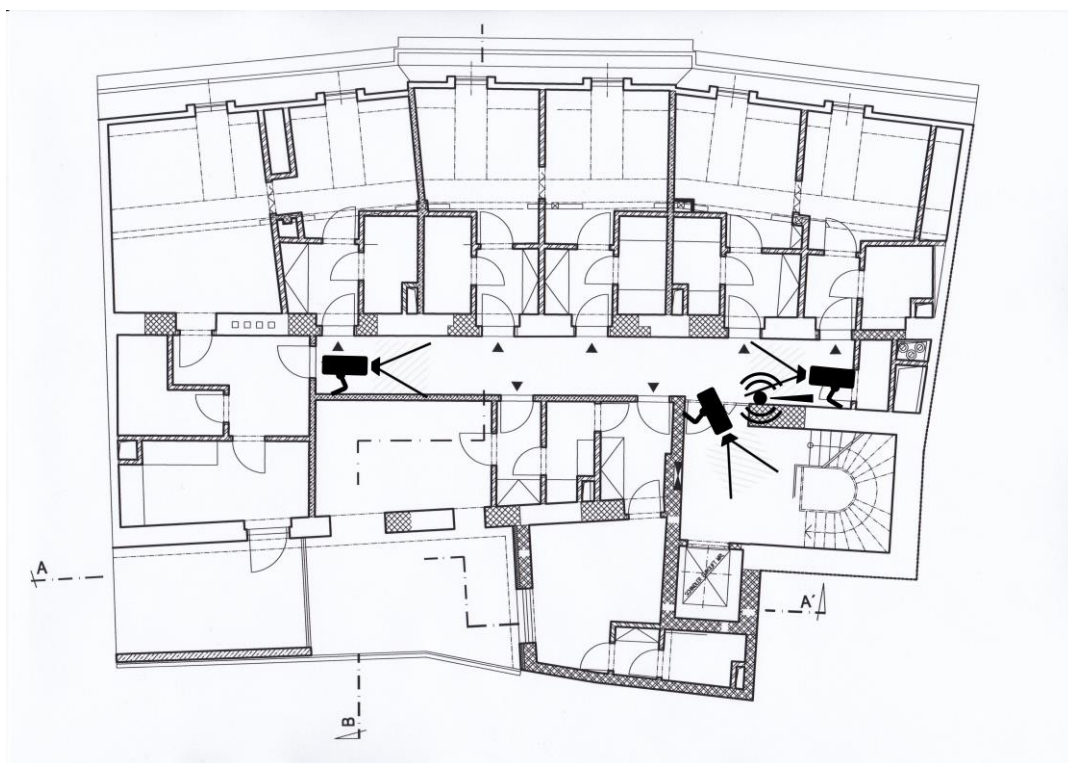
Na tomto patře se nachází 1 Wi-Fi anténa lokalizována nad vstupními dveřmi do chodby k ubytovacím zařízením ve výšce 3 metry.

Počítače a tiskárny

Na tomto patře se nenachází žádný počítač ani tiskárna.

Ostatní zařízení

V každém pokoji se nachází analogový telefon, který je propojen do telefonní ústředny hotelu. V každém pokoji se nachází datová zásuvka.



Obrázek 12 - Analýza NP4 se stávajícími prvky (autor)

Závěr

Nedostatečný počet kamer zajišťující pokrytí celého prostoru tohoto patra, zároveň jsou kamery zastaralé, nenahrávají ani nestrámují v rozlišení HD ani neobsahují noční vidění. Výrobce kamer nebyl zjištěn. Jediná Wi-Fi anténa zcela nepokrývá celý prostor tohoto patra a je umístěna ve špatné pozici.

4.1.1.3 Závěr této kapitoly

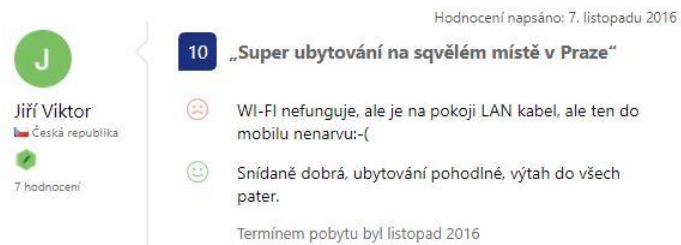
Z dílčích závěrů analýzy jednotlivých pater byl informován majitel hotelu, který tyto informace konzultoval se svými pracovníky, kteří se starají o jeho IT infrastrukturu v jiných objektech.

Částečným potvrzením výsledků dílčích závěrů mohou být i recenze uživatelů na portálu booking.com.



Obrázek 13 - Hodnocení hotelu DAR na booking.com (autor)

Z obrázku je patrné špatného hodnocení kolonky „Wi-Fi zdarma“, ve kterém uživatelé hodnotí i jeho pokrytí po prostorách hotelu. Příkladem může být i tato recenze.



Obrázek 14 - Hodnocení uživatele na booking.com (autor)

Z recenze je patrná nespokojenost s kvalitou Wi-Fi pokrytí signálu po hotelovém zařízení. Tato nespokojenost je zapříčiněna špatnou lokalizací Wi-Fi antén, které jsou vyobrazené v půdorysech budovy.

4.1.2 Požadavky na nové síťové řešení

Na základě předání výsledků analýzy stávajícího řešení, byly následně předány požadavky na nové síťové řešení. Tyto požadavky jsou generovány z konzultace majitele hotelu s jeho IT pracovníky. Jedním z požadavků je snaha využít prvky již stávající sítě.

4.1.2.1 Síťové řešení

Majitel hotelu požaduje vytvoření nové síťové infrastruktury zajišťující ochranu dat, ochranu objektu a plné pokrytí vnitřních prostor novou WLAN sítí. Požaduje vytvoření sítě, která je sestavena na síťových prvcích od společnosti Ubiquiti Networks. S těmito prvky pracují jeho IT zaměstnanci a přejí si sjednotit zařízení se kterými pracují v jiných objektech. Pomocí GUI bude správa velice jednoduchá, protože všechny prvky sítě od této společnosti je možné spravovat pomocí jediné aplikace (Unifi Console). Dalším kladem tohoto požadavku je synchronizovanost všech prvků této společnosti, ale jedná se i o jisté riziko v případě použití nového síťového prvku od jiné společnosti, kdy komunikace mezi prvky různých výrobců nemusí být tak „sladěná“, jako v případě prvků od stejné společnosti.

Byl kladen důraz na Wi-Fi pokrytí hotelu a nové bezpečnostní kamery zajišťující záznam a přehrávání v HD rozlišení.

4.1.2.2 Další infrastruktura

Dalšími požadavky majitele hotelu je z modernizování stávajících počítačů, vytvoření jednoduchého serveru pro správu dat a dokumentů, který poběží na operačním systému Windows, možnost vytvoření VPN a vzdálené správy. Dále je požadavek pro výběr počítače pro veřejnost, který se bude nacházet v recepčním zařízení pro hotelové hosty a také požadavek na výběr notebook pro majitele.

Prvky, které je třeba vybrat pomocí vlastního uvážení, ale za minimálních kritérií výběru stanovených zadavatelem:

- UPS
 - Záložní doba při zátěži 100%: 5,39-13,94 min
 - Záložní doba při zátěži 50%: 15,69-37,84 min
 - Počet výstupních zásuvek: 6-9
 - Rack UPS 2U
- NAS
 - Využití: Firemní
 - Provedení: Rack

- Podporovaný RAID 5
- Server
 - Bez minimálního kritéria
- PC (veřejnost)
 - Provedení All-in-one PC
 - Procesor Intel Core i5
 - Disk HDD
 - Kapacita disku: 1-1,5 TB
- PC (zaměstnanci)
 - Procesor Intel Core i5
 - Disk SSD
 - Kapacita disku: 128-500 GB
- Notebook
 - Procesor Intel Core i5
 - Disk SSD
 - Kapacita disku: 128-500 GB

Majitelem, a jeho IT správci, budou poskytnuty tyto prvky:

- Rack
- Tiskárny











Na základě těchto požadavků budou vytvořena řešení nové síťové infrastruktury, kde důraz bude kladen na nový kamerový systém a nové Wi-Fi, pokrytí všech hotelových a restauračních prostor.

4.1.3 Nové síťové řešení

Tato kapitola je rozdělena do 2 podkapitol, ve kterých se popisuje nové síťové řešení, které je zakreslené do půdorysu budovy. Řešení prvků v prostorách hotelu bylo vytvořeno pouze jedno, které částečně vychází z původního řešení, ale je doplněné o prvky, které jsou potřeba po pokrytí potřeb zákazníku a zároveň splní požadavky majitele hotelu.

4.1.3.1 Řešení prvků v prostorách hotelu

V následujících podkapitolách se bude popisovat rozvržení prvků v prostorách hotelu. Také zde bude vyobrazena legenda.

	Rozvaděč		Počítač (zaměstnanci)
	Počítač (zákazníci)		EET pokladna
	Guest Wi-Fi		Private Wi-Fi
	Kamera vnitřní		Kamera venkovní
	Tiskárna		VoIP telefon
	Kamerová kabeláž		Kabeláž Private
	Wi-Fi kabeláž (Guest)		VoIP kabeláž

Tabulka 2 - Legenda prvků (autor)

PP1

Kamery a Wi-Fi antény

V novém návrhu vzrostl počet vnitřních kamer na 5 kusů. Kamery jsou umístěny tak, aby pokrývaly co největší plochu tohoto patra. Zaznamenávají pohyb ve všech veřejných prostorách hotelu, s výjimkou toaletních prostor, kdy by tyto kamery narušovali soukromý zákazník hotelu. Dále byly přidány kamery do zázemí vinárny, konkrétně do chodby ke

kovovému točitému schodišti a servisnímu výtahu. Vnitřní kamery budou osazené na vodorovném stropě ve výšce 3,5 metrů.

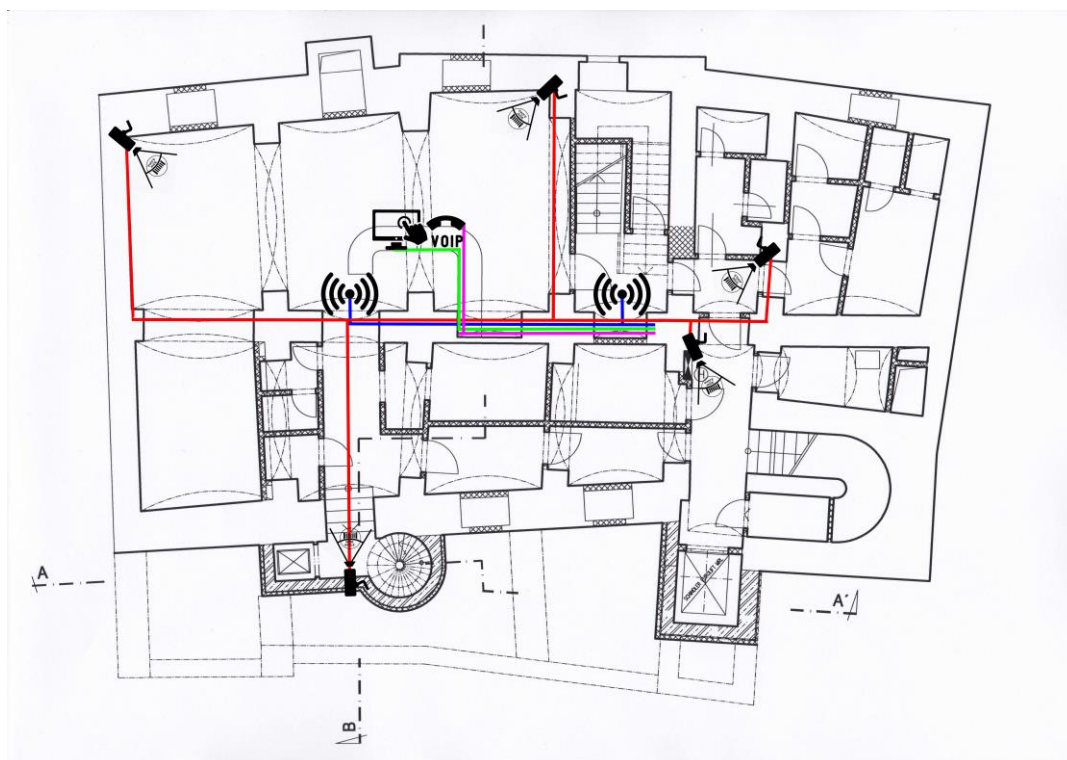
Na tomto patře se budou nacházet 2 Wi-Fi antény zajišťující pokrytí všech prostor na tomto patře. Obě antény budou určeny pro zákazníky hotelu. Wi-Fi antény budou osazené na vodorovném stropě ve výšce 3,5 metrů.

Počítače a tiskárny

V restauračním zařízení zůstane původní dotykový počítač All-in-one obsahující aplikaci EET, kdy k tomuto počítači je připojena tiskárny na tisk účtenek.

Ostatní zařízení

Nově zde bude zázemí vinárny obsahovat VoIP telefon, který se bude nacházet na barovém pultě pro potřeby vinárny a jeho personálu a zároveň umožní komunikace vinárny s hotelovým zařízením.



Obrázek 15 - Návrh nového řešení s novými prvky v PP1 (autor)

Závěr

V novém řešení je již dostatečný počet kamer zajišťujících pokrytí všech veřejných prostor hotelového zařízení s výjimkou toaletních prostor. Původní kamery budou nahrazeny moderními kamerami schopné nahrávat v rozlišení HD a budou mít schopnost nočního nahrávání.

Dostatečný počet Wi-Fi antén zajistí pohodlí zákazníkům hotelu. Wi-Fi antény budou síti Guest, nebudou mít přístup privátní síti hotelu. Na plánu je zřejmý bod, kde se sbíhají kabely z tohoto patra, v tomto místě bude vybudována stoupací šachta do patra se serverem (toto místo bylo vybráno, protože v tomto průsečíku budovy se nachází opěrná zeď).

NP1

Kamery a Wi-Fi antény

V novém návrhu vzrostl počet vnitřních kamer na 8 kusů a počet venkovních kamer vzrostl na 3 kusy. Kamery jsou umístěny tak, aby vzájemně pokrývaly svá zorná pole a zaznamenávaly pohyb ve všech veřejných prostorách hotelu. Nyní kamery zaznamenávají všechny vstupy a výstupy hotelu na ulici. Dále byly přidány kamery do zázemí restauračního zařízení, konkrétně do kuchyňských prostor a nad kovové točité schodiště. Vnitřní kamery budou osazené na vodorovném stropě ve výšce 3,5 metrů.

Wi-Fi antény zde budou celkem 3 (2 pro veřejnost a zákazníky hotelu, 1 pro privátní užití). Tento model byl zvolen z důvodů zvýšení bezpečnosti hotelových dat a omezení a větší kontroly přístupu veřejnosti z neznámých zařízení. Wi-Fi anténa bude mít skryté SSID a bude na ni aplikováno pravidlo, kdy se mohou připojit pouze zařízení uložené v databázi známých zařízení. Wi-Fi antény budou osazené na vodorovném stropě ve výšce 3,5 metrů.

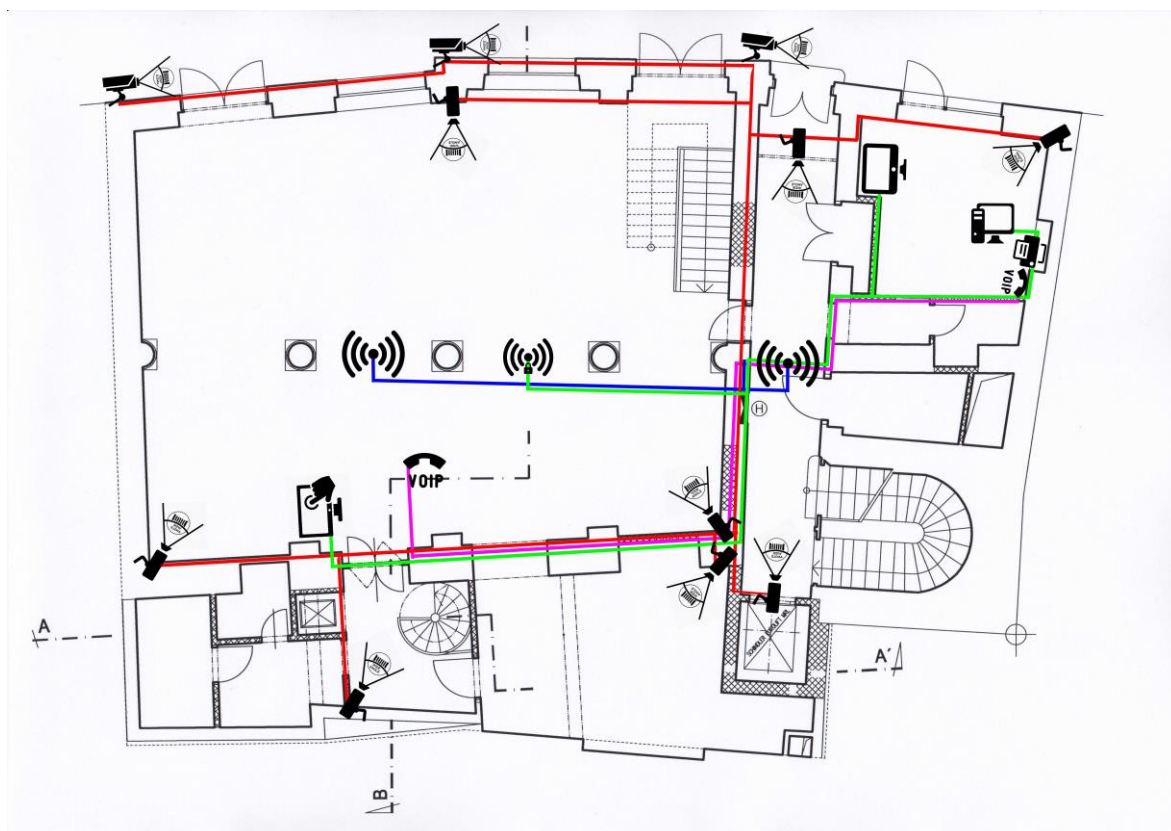
Počítače a tiskárny

Umístění počítačů a tiskáren bude stejné, budou nahrazené novými modely, které budou odpovídat požadavkům majitele. Dále tiskárny budou připojené do sítě a nebudou pouze místně nastavené. V recepčním sále přibude nový All-in-one počítač určený pro potřeby zákazníků hotelu. V restauračním zařízení zůstane původní dotykový počítač All-

in-one obsahují aplikaci EET, kdy k tomuto počítači je připojena tiskárny na tisk účtenek a tiskárna v kuchyňském zázemí, které je k tomuto počítači přidružená.

Ostatní zařízení

V recepčním sále bude analogový telefon nahrazen VoIP telefonem pro potřeby recepce, další VoIP telefon se bude nacházet na barovém pultě pro potřeby restaurace a zároveň zpřístupnění možnosti komunikace restauračního zařízení s hotelovým zařízením.



Obrázek 16 - Návrh nového řešení s novými prvky v NP1 (autor)

Závěr

V novém řešení je již dostatečný počet kamer zajišťujících pokrytí celého prostoru tohoto patra, obzvláště venkovních vchodů nebo zázemí restaurace. Původní kamery budou nahrazeny moderními kamerami schopné nahrávat v rozlišení HD a budou mít schopnost nočního nahrávání. Dostatečný počet Wi-Fi antén zajistí pohodlí zákazníkům hotelu a rozdělení Wi-Fi na Guest/Private zvýší bezpečnost síťových dat. Private Wi-Fi zde byla nainstalována z důvodu možných jednání v prostorách hotelu, ke kterým bude potřeba internetového připojení a přístupu ke sdíleným datům, zároveň tato Wi-Fi síť poběží na 5

GHz anténě. Nové počítače budou zajišťovat bezproblémový chod hotelových aplikací a pomohou hotelovým zaměstnancům v jejich práci. Počítače budou obsahovat operační systém Microsoft Windows 10 Pro a dalšími potřebnými aplikacemi k zajištění bezpečnosti a chodu pracovních stanic. Tiskárny budou nastaveny jako síťové. Nyní bude restaurační personál schopen komunikovat s pracovníky hotelu z důvodu nového VoIP telefonu. Na plánu je zřejmý bod, kde se sbíhají kabely z tohoto patra, v tomto místě bude vybudována stoupací šachta do patra se serverem (toto místo bylo vybráno, protože v tomto průsečíku budovy se nachází vždy opěrná zeď).

NP2

Kamery a Wi-Fi antény

V novém návrhu vzrostl počet vnitřních kamer na 4 kusy. Kamery jsou umístěny tak, aby vzájemně pokrývaly svá zorná pole a zaznamenávaly pohyb ve všech veřejných prostorách hotelu. Vnitřní kamery budou osazené na vodorovném stropě ve výšce 3,5 metrů. Zároveň bude zřízena 1 venkovní kamera pokrývající vnitřní atrium hotelu. Bude také ve výšce 3,5 metrů.

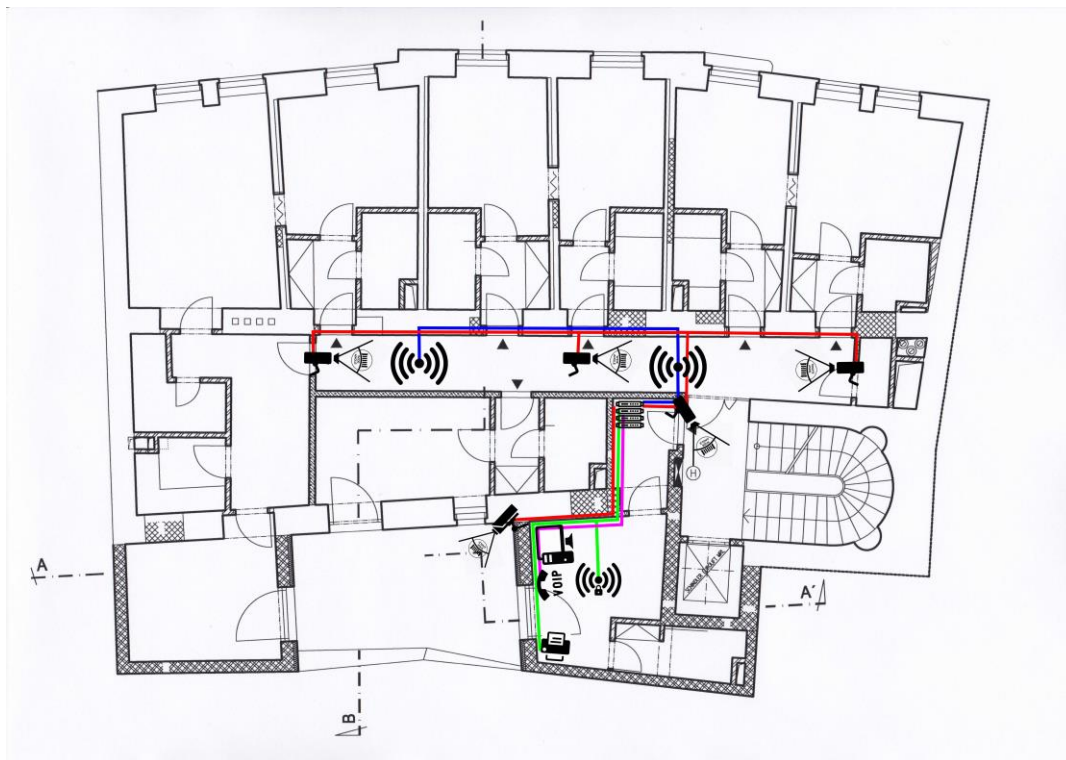
Wi-Fi antény zde budou celkem 3 (2 pro veřejnost a zákazníky hotelu, 1 pro privátní užití). Wi-Fi anténa bude mít skryté SSID a bude na ni aplikováno pravidlo, kdy se mohou připojit pouze zařízení uložené v databázi známých zařízení. Wi-Fi antény budou osazené na vodorovném stropě ve výšce 3,5 metrů.

Počítače a tiskárny

Umístění počítačů a tiskáren bude podobné, budou nahrazené novými modely, které budou odpovídat požadavkům majitele. Dále tiskárny budou připojené do sítě a nebudou pouze místně nastavené. V předsíni pracovny se bude nacházet nový Rack se všemi potřebnými komponentami zajišťující rychlý a bezpečný chod sítě.

Ostatní zařízení

V každém pokoji se budou nacházet stávající analogové telefony, které budou propojené do telefonní ústředny hotelu. V každém pokoji se nachází datová zásuvka. Stávající analogový telefon v pracovně bude nahrazen novým VoIP telefonem zajišťující komfortní komunikaci.



Obrázek 17 - Návrh nového řešení s novými prvky v NP2 (autor)

Závěr

V novém řešení je již dostatečný počet kamer zajišťujících pokrytí všech veřejných prostor hotelového zařízení. Původní kamery budou nahrazeny moderními kamerami schopné nahrávat v rozlišení HD a budou mít schopnost nočního nahrávání. Dostatečný počet Wi-Fi antén zajistí pohodlí zákazníkům hotelu a rozdělení Wi-Fi na Guest/Private zvýší bezpečnost síťových dat. Private Wi-Fi zde byla nainstalována z důvodu možných jednání v prostorách kanceláře a přístupu ke sdíleným datům, zároveň tato Wi-Fi síť poběží na 5 GHz anténě.

Počítače budou obsahovat operační systém Microsoft Windows 10 Pro a dalšími potřebnými aplikacemi k zajištění bezpečnosti a chodu pracovních stanic. Tiskárny budou nastaveny jako síťové. Ze stoupací šachty, do které bude vedena nová kabeláž, budou (přes stavební úpravu podlahy) kabely vedené k novému rozvaděči v předsáli pracovní.

NP3

Kamery a Wi-Fi antény

V novém návrhu vzrostl počet vnitřních kamer na 4 kusy. Kamery jsou umístěny tak, aby vzájemně pokrývaly svá zorná pole a zaznamenávaly pohyb ve všech veřejných prostorách hotelu. Vnitřní kamery budou osazeny na vodorovném stropě ve výšce 3 metrů.

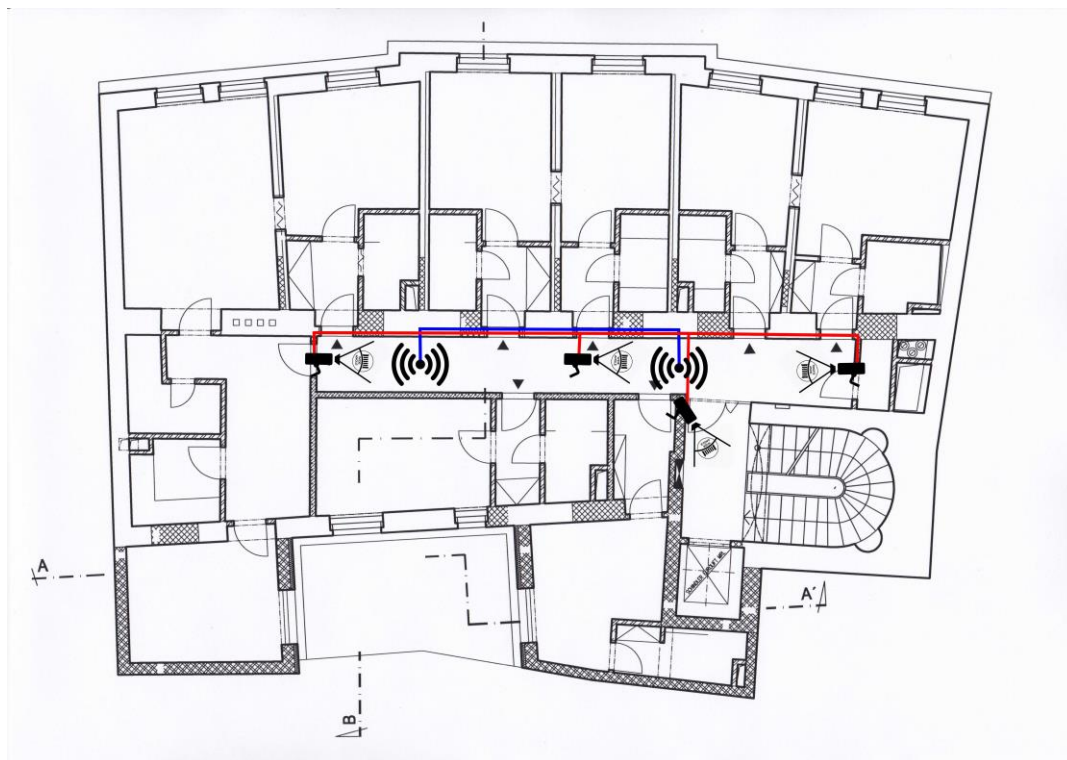
Na tomto patře se budou nacházet 2 Wi-Fi antény zajišťující pokrytí všech prostor na tomto patře. Obě antény budou určeny pro zákazníky hotelu. Wi-Fi antény budou osazeny na vodorovném stropě ve výšce 3 metrů.

Počítače a tiskárny

Na tomto patře nebude žádný síťový počítač ani tiskárna.

Ostatní zařízení

V každém pokoji se budou nacházet stávající analogové telefony, které budou propojené do telefonní ústředny hotelu. V každém pokoji se nachází datová zásuvka.



Obrázek 18 - Návrh nového řešení s novými prvky v NP3 (autor)

Závěr

V novém řešení je již dostatečný počet kamer zajišťujících pokrytí všech veřejných prostor hotelového zařízení. Původní kamery budou nahrazeny moderními kamerami schopné nahrávat v rozlišení HD a budou mít schopnost nočního nahrávání. Dostatečný počet Wi-Fi antén zajistí pohodlí zákazníkům hotelu. Wi-Fi antény budou v síti Guest, nebudou mít přístup k privátní síti hotelu. Na plánu je zřejmý bod, kde se sbíhají kabely z tohoto patra, v tomto místě bude vybudována stoupací šachta do patra se serverem (toto místo bylo vybráno, protože v tomto průřezu budovy se nachází opěrná zeď).

NP4

Kamery a Wi-Fi antény

V novém návrhu vzrostl počet vnitřních kamer na 4 kusy. Kamery jsou umístěny tak, aby vzájemně pokrývaly svá zorná pole a zaznamenávaly pohyb ve všech veřejných prostorech hotelu. Vnitřní kamery budou osazené na vodorovném stropě ve výšce 3 metrů.

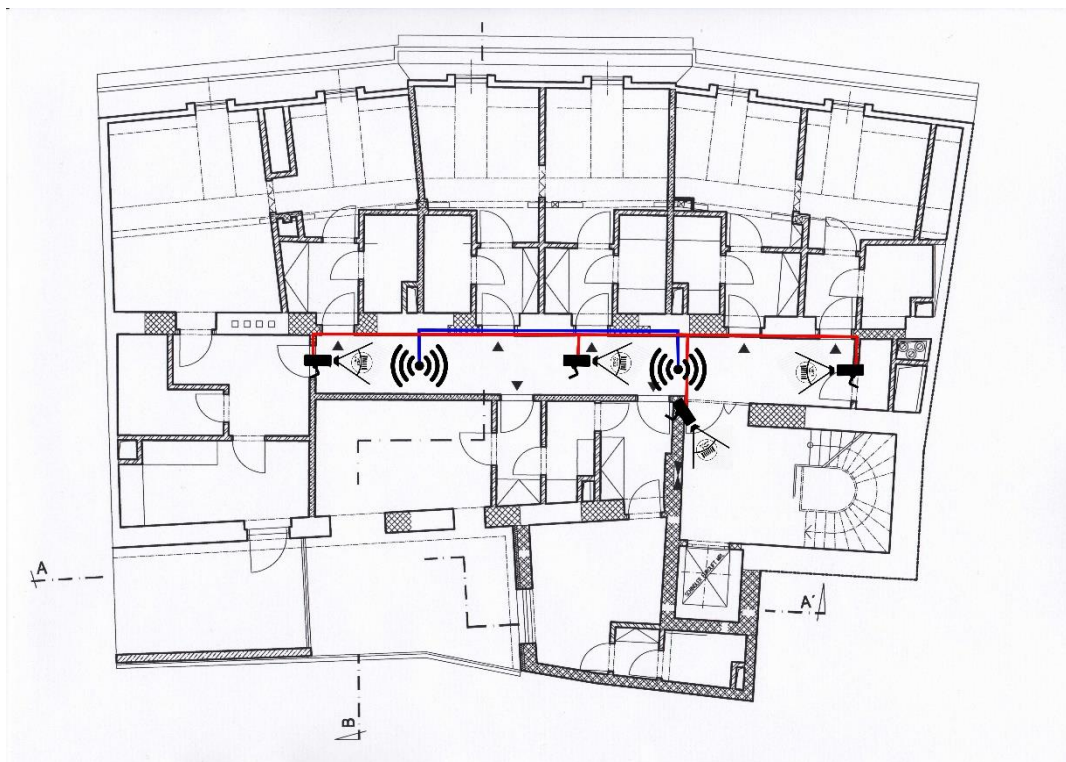
Na tomto patře se budou nacházet 2 Wi-Fi antény zajišťující pokrytí všech prostor na tomto patře. Obě antény budou určeny pro zákazníky hotelu. Wi-Fi antény budou osazené na vodorovném stropě ve výšce 3 metrů.

Počítače a tiskárny

Na tomto patře nebude žádný síťový počítač ani tiskárna.

Ostatní zařízení

V každém pokoji se budou nacházet stávající analogové telefony, které budou propojené do telefonní ústředny hotelu. V každém pokoji se nachází datová zásuvka.



Obrázek 19 - Návrh nového řešení s novými prvky v NP4 (autor)

Závěr

V novém řešení je již dostatečný počet kamer zajišťujících pokrytí všech veřejných prostor hotelového zařízení. Původní kamery budou nahrazeny moderními kamerami schopné nahrávat v rozlišení HD a budou mít schopnost nočního nahrávání. Dostatečný počet Wi-Fi antén zajistí pohodlí zákazníkům hotelu. Wi-Fi antény budou v síti Guest, nebudou mít přístup k privátní síti hotelu. Na plánu je zřejmý bod, kde se sbíhají kabely z tohoto patra, v tomto místě bude vybudována stoupací šachta do patra se serverem (toto místo bylo vybráno, protože v tomto průřezu budovy se nachází vždy opěrná zeď).

Řešení prvků v Racku

Byla navržena celkem 2 řešení podle kterých by byla realizována síť v hotelovém zařízení. Hlavním rozdílem je počet aktivních prvků v síti instalovaných do rozvaděče a jejich konfigurace. Funkčnost obou sítí je totožná, ale v druhém řešení je využíváno funkce VLAN, pomocí které je možné nastavit více sítí na jednom aktivním prvku a rozdělit tak

výstupy pro jednotlivé sítě. V prvním případě má každá síť svůj vlastní aktivní prvek, je tedy patrné, že mnoho výstupů bude prázdných a nevyužitých. Obě řešení mají svůj důvod vzniku. „Řešení 1“ je vytvořeno z důvodů možnosti rozšíření hotelové sítě, a to z důvodu rozšíření hotelu téměř o dvojnásobnou velikost. Z toho vyplývá velké rozšíření kamerové sítě nebo sítě pro Wi-Fi síť Guest. V „Řešení 2“ je menší počet aktivních prvků a je s maximální možným úsilím využití všech výstupů aktivních prvků pomocí VLAN. Toto řešení je méně nákladné, ale v případě rozšíření hotelu bude potřeba rekonfigurace sítě a koupě dalších aktivních prvků. Do návrhů nových sítí nebyla zakreslena PBX ústředna a switch, ke kterému jsou vedené datové zásuvky a s jejím využitím se počítá v novém řešení.

Základní princip fungování sítě

V této kapitole budou nastíněny základní principy fungování sítě, ale toto nastavení nebude možné vyzkoušet v praxi, protože fyzicky tato síť nebude realizována během tvorby diplomové práce.

V privátní síti, která bude mít adresaci 192.168.1.0/24, budou všechny prvky nutné k chodu sítě a její bezpečnosti. Dále zde bude instalována Wi-Fi síť pro privátní uživatele, kam se budou moci přihlásit pouze známá zařízení podle jejich MAC adres, SSID této Wi-Fi sítě bude skryté. Dále na serveru bude instalován pokročilý balíček od společnosti ESET, který podporuje vzdálenou správu. Na této síti bude nastavené DHCP v rozsahu 192.168.1.150 - 192.168.1.200. Autorizovaní uživatelé se mohou z veřejné sítě pomocí VPN přihlašovat na NAS server a tím mít přístup k sdíleným dokumentům. Počítač určený pro veřejnost bude obsahovat Guest profil, který bude náležitě omezen pro bezpečnost sítě.

V kamerové síti, která bude mít adresaci 192.168.2.0/24, budou všechny venkovní i vnitřní kamery a NVR zařízení. NVR zařízení obsahuje aplikaci umožňující vzdálený přístup autorizovaným uživatelům. V této síti nebude DHCP nastaveno.

V Wi-Fi síti pro zákazníky hotelu, která bude mít adresaci 192.168.3.0/24, budou všechny Wi-Fi antény, které budou distribuovat internet mezi zákazníky. Tato síť bude založena na DHCP, která zde bude aplikována v plném rozsahu.

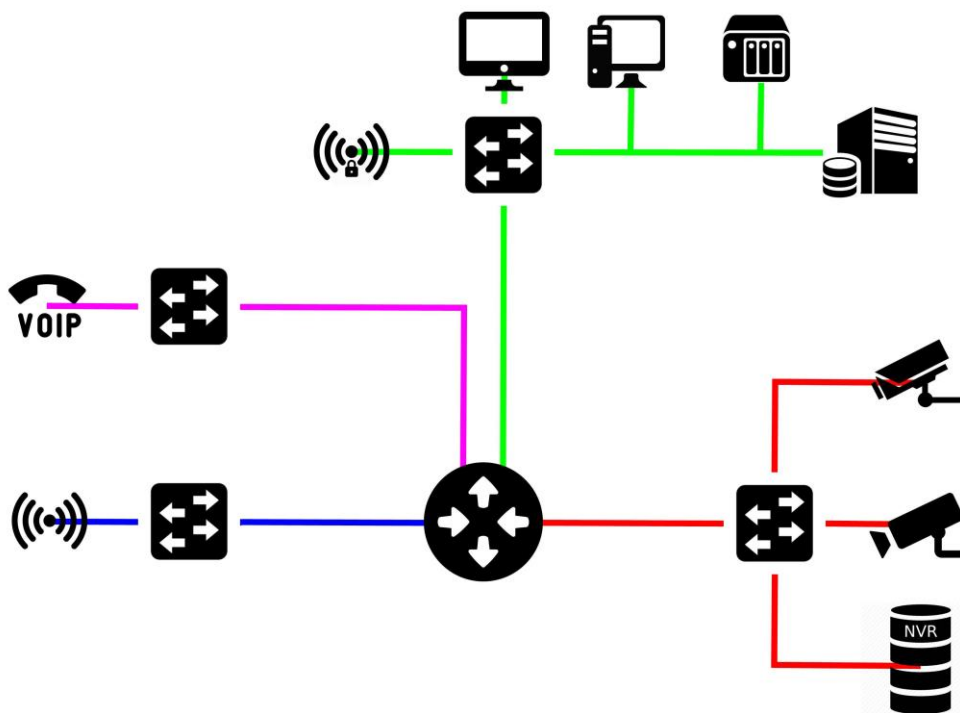
V síti pro VoIP telefony, která bude mít adresaci 192.168.4.0/24, budou umístěny IP telefony. IP telefony mohou komunikovat s vnějším prostředím, ale také budou pomoci

tunelu komunikovat s PBX ústřednou, do které jsou připojené analogové telefony. Toto spojení je zcela nutné například z důvodu komunikace hotelových zákazníků s recepcí, kde je VoIP telefon umístěn.

V síti, kde jsou připojené datové zásuvky, bude mít adresaci 192.168.5.0/24.

Pomocí ACL budou sítě nastaveny tak, aby nemohly mezi sebou komunikovat a nemohla vzniknout situace, kdy si zákazník ze sítě pro veřejnost připojí ke sdíleným souborům v privátní síti. Prvky ze sítě 192.168.1.0/24 budou moci přistupovat do ostatních sítí a tím kontrolovat její funkčnost a možnost její správy.

Řešení 1



Obrázek 20 - Návrh "Řešení 1" v rozvaděči (autor)

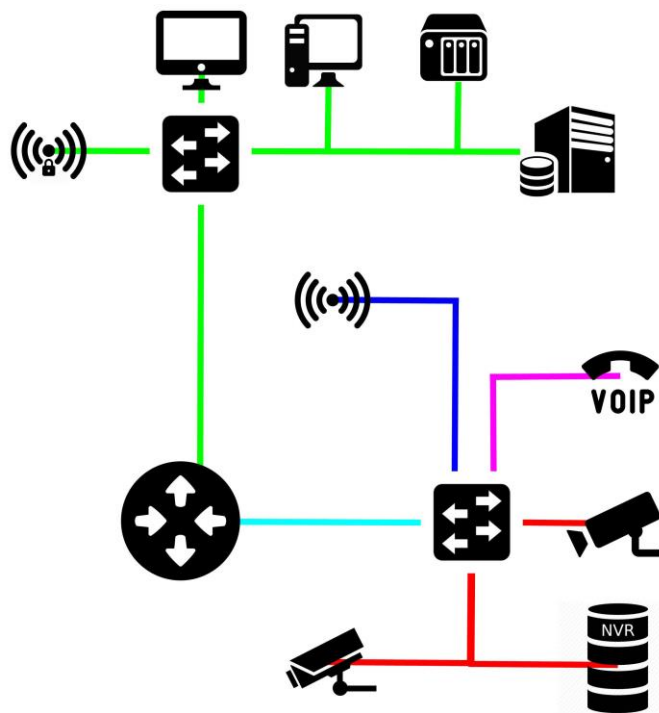
V následující tabulce jsou vyobrazeny prvky, jednotkovou cenu a množství, které bude potřeba k realizaci sítě tohoto typu.

Název	Cena za kus	Množství	Cena celkem
EdgeRouter	7 190,00 Kč	1	7 190,00 Kč
US-24-500W	12 824,00 Kč	3	38 472,00 Kč
US-48-750W	27 203,00 Kč	1	27 203,00 Kč
UniFi UAP-AC-PRO	3 515,00 Kč	12	42 180,00 Kč
UniFi Video Camera G3 Dome	3 373,00 Kč	25	84 325,00 Kč
UniFi Video G3 PRO	7 265,00 Kč	4	29 060,00 Kč
UniFi NVR Controller 2 TB	12 499,00 Kč	1	12 499,00 Kč
UniFi Voip Phone Executive	8 850,00 Kč	4	35 400,00 Kč
Cena celkem			276 329,00 Kč

Tabulka 3 - Náklady na "Řešení 1" v rozvaděči (autor)

Náklady na toto řešení činí 276 329,00 Kč včetně DPH. Více v kapitole „Finanční analýza“.

Řešení 2



Obrázek 21 - Návrh "Řešení 2" v rozvaděči (autor)

V této síti by byla definovaná síť 192.168.10.0/29, kde by v této síti bylo spojení mezi routerem a switchem, kde by byly definovány VLAN sítě. Byly zde zvolena rezerva pro další prvky, kvůli možnosti správy switche. Počet připojených prvků ke switchi, na kterém jsem definovány VLAN sítě je celkem 46. Další výstup bude sloužit k propojení switche a routeru, Zbývá poslední výstup k možné přímé správě tohoto switche.

V následující tabulce jsou vyobrazeny prvky, jednotkovou cenu a množství, které bude potřeba k realizaci sítě tohoto typu.

Název	Cena za kus	Množství	Cena celkem
EdgeRouter	7 190,00 Kč	1	7 190,00 Kč
US-24-500W	12 824,00 Kč	1	12 824,00 Kč
US-48-750W	27 203,00 Kč	1	27 203,00 Kč
UniFi UAP-AC-PRO	3 515,00 Kč	12	42 180,00 Kč
UniFi Video Camera G3 Dome	3 373,00 Kč	25	84 325,00 Kč
UniFi Video G3 PRO	7 265,00 Kč	4	29 060,00 Kč
UniFi NVR Controller 2 TB	12 499,00 Kč	1	12 499,00 Kč
UniFi Voip Phone Executive	8 850,00 Kč	4	35 400,00 Kč
Cena celkem			250 681,00 Kč

Tabulka 4 - Náklady na "Řešení 2" v rozvaděči (autor)

Náklady na toto řešení činí 250 681,00 Kč včetně DPH. Více v kapitole „Finanční analýza“.

4.2 Výběr nových prvků

Výběr síťových prvků je dán společností Ubiquiti Networks. Dále jsou zde prvky, které je potřeba vybrat dle vlastního uvážení. Jedná se o prvky:

- UPS
- NAS
- Server
- PC (veřejnost)
- PC (zaměstnanci)
- Notebook

Představitelé výše zmíněných prvků byly vybrány z internetového e-shopu společnosti Alza (<https://www.alza.cz>), kde byla nastavena filtrace podle minimálních kritérií stanovených majitelem. Po filtraci byl vygenerován seznam s největšími prodeji konkrétních prvků. Z toho seznamu byly vybrány první 4 prvky, které budou analyzovány pomocí metody vícekritériální analýzy. Bude použita metoda „bodovací“ s intervalem 1-10 (10 – nejlepší, 1 – nejhorší) a metoda „váženého součtu“, která pracuje s ideálními a bazálními hodnotami. K porovnáváním vlastnostem prvků byly stanoveny váhy, které poukazují na důležitost vlastnosti. Součet vah je roven 1. (Šubrt, 2015)

4.2.1 Výběr síťových prvků

Výběr síťových prvků je zúžen z portfolia prvků společnosti Ubiquiti Networks. Využití této společnosti si přeje majitel po konzultaci s jeho IT pracovníky. Prvky sítě budou vybrány na základě navrhovaných řešení (kap. 4.1.4.1 a 4.1.4.2).

4.2.1.1 Router

První prvek a stěžejní prvek, který je potřeba, je router. Protože společnost byla stanovena majitelem, výběr se velice zúžil a nebylo potřeba vybírat prvky pomocí vícekritériální analýzy, jejich prvky jsou z větší části naprosto totožné a odlišují se v počtu portů nebo podpoře PoE výstupů. Router byl vybrán z řady EdgeMax, konkrétně Ubiquiti EdgeRouter. Jedná se o výkonný rackový router od tohoto výrobce. Disponuje 8 ethernetovými porty (EdgeMax Pro obsahuje 6 ethernetových portů + 2 SFP porty, ale v tomto případě nejsou potřeba), tento počet je více než dostačující a volné porty budou fungovat jako záložní v případě rozšiřování sítě. Router garantuje vysokou propustnost až 2 miliony paketů za sekundu s 99,9% uptime. Tento výkon potvrzuje hardware, který tvoří dvoujádrový procesor s frekvencí 800 MHz, 2 GB operační paměti a 4 GB datového uložení. Prostřednictvím grafického rozhraní EdgeOS je vysoce stabilní systém, pomocí kterého je možné nastavovat služby jako jsou například ACL, NAT, OpenVPN, DHCP a podobně. Logování chodu, statistiky provozu, nastavování je možné pomocí webového prohlížeče nebo pomocí sériového portu a CLI, případně SSH. Tento prvek bude centrálním prvkem sítě, ze kterého bude dále nastavována síť.

Celkový počet routeru: 1 kus.

4.2.1.2 Switch

Dalším prvkem pro výběr je prvek switch, celkový počet switchů v této síti jsou 4. Switch pro privátní síť, switch pro Wi-Fi Guest, switch pro kamerovou síť a switch pro VoIP telefony. Vzhledem k charakteru prvků v hotelu (všechny prvky od této společnosti podporu PoE napájení), jsou tyto prvky vybírány podle této vlastnosti. Tuto vlastnost mají switche US-24-500W a US-48-750W. Podle jejich názvů je zřejmý počet gigabitových portů. PoE napájení má výhodu vedení napájecího kabelu a datového kabelu v jednom, proto byla tato možnost využita do tohoto řešení. Vzhledem k počtu současných prvků a možných budoucích prvků v případě rozšíření hotelu. Pomocí softwaru totožného jako u routeru je možné monitorovat chod sítě a využít jednoduchého a intuitivního nastavení. Počet potřebných switchů je:

- 1 switch US-24-500W pro síť s VoIP telefony. Celkový počet telefonů je 4 kusy.
- 1 switch US-24-500W určený pro Wi-Fi antény pro Guest síť. Celkový počet antén je 10 kusů.
- 1 switch US-24-500W určený pro privátní síť, která bude obsahovat: 2 Wi-Fi antény pro privátní určení, 2 počítače All-in-one pro aplikaci EET, 1 počítač All-in-one pro veřejnost, 2 počítače kancelářského charakteru, 2 tiskárny kancelářského charakteru, 1 server, 1 NAS. Celkový počet prvků je 11 kusů.
- 1 switch US-48-750W určený pro kamerovou síť, která se z hlediska prvků stala tou nejčetnější. Celkový počet venkovních kamer je 4, celkový počet vnitřních kamer je 25 a jeden port pro NVR server. Celkový počet prvků je 30 kusů.

Ve schváleném řešení (Řešení 1) je mnoho nevyužitých portů, které byly ve druhém řešení (Řešení 2) odstraněny pomocí VLAN, S budoucím rozšiřováním hotelu bylo zvoleno toto „Řešení 1“, kdy volné porty budou připraveny pro další prvky v rozšiřující se síti hotelu.

4.2.1.3 Wi-Fi anténa

Pro WLAN síť určenou pro hosty (Guest) byla vybrána anténa UniFi UAP-AC-PRO, která splňuje nejmodernější standardy 802.11ac a je schopna pracovat s pásmu 2,4 GHz nebo v pásmu 5 GHz. Pomocí velice snadného nastavení a jednoduché správy antény je vhodným prvkem do této sítě. Vyznačuje se vysokou stabilitou a nízké odezvě při připojení velkého počtu klientů. Rychlost přenosu Wi-Fi je až 1 300 MB/s (pokud je klient připojen na 5 GHz anténě) a na 2,4 GHz anténě se rychlost pohybuje okolo 450 MB/s. Tato anténa je vhodná i pro venkovní použití, proto bude možné ji instalovat i na terase hotelu. Anténa je napájena pomocí PoE.

Celkový počet Wi-Fi antén pro Guest síť: 10 kusů

Pro WLAN síť určenou pro pracovníky hotelu (Private) byla vybrána shodná anténa jako pro Guest Wi-Fi, tedy anténa UniFi UAP-AC-PRO.

Celkový počet Wi-Fi antén pro Private síť: 2 kusy

4.2.1.4 IP kamery

Pro vnitřní použití byla vybrána kamera UniFi Video Camera G3 Dome, jedná se o nejnovější kameru od této společnosti, která podporuje sledování prostoru jak ve dne, tak i v noci v kvalitě HD s plynulostí 30 snímků za sekundu. Obsahuje technologii PoE napájení, která odstraňuje další potřebu kabelových rozvodů. Pomocí dodávaného softwaru je velice jednoduchá správa těchto kamer a pomocí mobilní aplikace je možné sledovat přímý přenos odkudkoliv. Obsahuje také zabudovaný mikrofon. Nahrávání videa je možné jak kontinuálně, tak po detekci pohybu.

Celkový počet vnitřních kamer: 25 kusů.

Pro venkovní použití byla vybrána kamera obdobných vlastností. Kamera UniFi Video G3 PRO má prakticky totožné vlastnosti, ale je určena pro venkovní použití, zvládne náročnější podmínky a je hlavně voděodolná, další její vlastností je 3x optický zoom na rozdíl od kamery UniFi Video Camera G3 Dome.

Celkový počet venkovních kamer: 4 kusů.

4.2.1.5 NVR

Záznam z IP kamer je možný dvěma způsoby, buď je v síti server obsahující aplikace airVision, která umožňuje zaznamenávat data z kamer na úložiště serveru. Druhou možností je airVision NVR zařízení, které je možné koupit přímo u výrobce. Byla zvolena možnost NVR zařízení. Toto zařízení automaticky detekuje kamery v síti a je schopné zvládnout až 50 kamer (udává výrobce), dále výrobce udává, že Unifi NVR o velikosti 500 GB je schopné zaznamenat zhruba 1 200 nahrávacích hodin při rozlišení 480p nebo 400 nahrávacích hodin při rozlišení 720p. Z toho důvodu je vybrán Ubiquiti UniFi NVR Controller o kapacitě 2 TB, který zajistí dostatečný počet nahrávacích hodin (4x větší).

Celkový počet NVR zařízení: 1 kus.

4.2.1.6 VoIP telefony

Poslední IP prvkem v síti od této společnosti je VoIP telefon UniFi Voip Phone Executive, který je vybaven 7 palcovým dotykovým, barevným displejem s rozlišením 1024x600px a vestavěnou kamerou pro videohovory a 4 GB interním úložištěm určeným pro aplikace. Telefon je postaven na operačním systému Android.

Polkový počet VoIP telefonů: 4 kusy.

4.2.2 Výběr – UPS

Prvním prvkem určeným pro výběr je záložní zdroj UPS, který zajišťuje dostatečný čas pro bezpečné vypnutí všech periférií, které jsou k němu připojené. Podle minimálních kritérií, stanovených majitelem, byly zvoleny tyto 4 záložní zdroje ke vzájemnému porovnání na základě vlastností, které byly vybrány. Tyto vlastnosti jsou:

- Skutečný výkon
- Zdánlivý výkon
- Záložní doba při zátěži 100%
- Záložní doba při zátěži 50%
- Hmotnost
- Počet výstupních zásuvek
- Cena

- Přepěťová ochrana

Podle těchto vlastností, a jejich hodnot, byla sestavena následující tabulka, která je výchozí tabulkou k sestavení tabulky při procesu rozhodování, který nevhodnější záložní zdroj vybrat.

	APC Smart-UPS X 1000VA LCD	APC Smart-UPS 2200VA LCD RM	APC Smart-UPS X 1500VA LCD	APC Smart-UPS X 2200VA LCD
Skutečný výkon (W)	800	2200	1200	1980
Zdánlivý výkon (VA)	1000	1980	1500	2200
Při zátěži 100% (min)	7,94	5,39	5,78	9,61
Při zátěži 50% (min)	17,25	15,69	16,86	24,22
Hmotnost (kg)	22,86	42,3	24,82	37,32
Počet výstupních zásuvek (ks)	8	8	8	8
Cena (Kč)	17690	29690	26990	48590
Přepěťová ochrana (J)	600	375	645	645

Tabulka 5 - Výběr UPS - základní tabulka (autor)

Byla použita metoda „bodovací“ s intervalem 1-10 (10 – nejlepší, 1 – nejhorší) a metoda „váženého součtu“, která využívá nejlepší možné kombinace a nejhorší možné kombinace k eliminaci subjektivního hodnocení. K porovnávání vlastností prvků byly stanoveny váhy, které poukazují na důležitost vlastnosti. Největší důraz byl kladen na vlastnost „Záložní doba při zátěži 100%“, kdy tato vlastnost byla ohodnocena váhou 0,25. Nejmenší důraz byl kladen na vlastnost „Hmotnost“, která byla ohodnocena váhou 0,05. Součet vah je roven 1.

	APC Smart-UPS X 1000VA LCD	APC Smart-UPS 2200VA LCD RM	APC Smart-UPS X 1500VA LCD	APC Smart-UPS X 2200VA LCD	Váhy
Skutečný výkon (W)	2	10	4	8	0,1
Zdánlivý výkon (VA)	4	8	6	10	0,07
Při zátěži 100% (min)	8	5	6	10	0,25
Při zátěži 50% (min)	6	4	5	10	0,15
Hmotnost (kg)	10	2	9	6	0,05
Počet výstupních zásuvek (ks)	10	10	10	10	0,07
Cena (Kč)	10	6	7	2	0,16
Přepěťová ochrana (J)	7	3	10	10	0,15
	7,23	5,62	6,84	8,32	1

Tabulka 6 - Výběr UPS - bodovací metoda (autor)

	APC Smart-UPS X 1000VA LCD	APC Smart-UPS 2200VA LCD RM	APC Smart-UPS X 1500VA LCD	APC Smart-UPS X 2200VA LCD	Váhy	H	D
Skutečný výkon (W)	800	2200	1200	1980	0,1	2200	800
Zdánlivý výkon (VA)	1000	1980	1500	2200	0,07	2200	1000
Při zátěži 100% (min)	7,94	5,39	5,78	9,61	0,25	9,61	5,39
Při zátěži 50% (min)	17,25	15,69	16,86	24,22	0,15	24,22	15,69
Hmotnost (kg)	22,86	42,3	24,82	37,32	0,05	22,86	42,3
Počet výstupních zásuvek (ks)	8	8	8	8	0,07	8	8
Cena (Kč)	17690	29690	26990	48590	0,16	17690	48590
Přepětová ochrana (J)	600	375	645	645	0,15	645	375
					1		

	APC Smart-UPS X 1000VA LCD	APC Smart-UPS 2200VA LCD RM	APC Smart-UPS X 1500VA LCD	APC Smart-UPS X 2200VA LCD	Váhy
Skutečný výkon (W)	0	1	0,285714286	0,842857143	0,1
Zdánlivý výkon (VA)	0	0,816666667	0,416666667	1	0,07
Při zátěži 100% (min)	0,604265403	0	0,092417062	1	0,25
Při zátěži 50% (min)	0,182883939	0	0,137162954	1	0,15
Hmotnost (kg)	1	0	0,899176955	0,25617284	0,05
Počet výstupních zásuvek (ks)	1	1	1	1	0,07
Cena (Kč)	1	0,611650485	0,699029126	0	0,16
Přepětová ochrana (J)	0,833333333	0	1	1	0,15
	0,583498942	0,325030744	0,478220312	0,787094356	1

Tabulka 7 - Výběr UPS - metoda váženého součtu (autor)

Po aplikaci bodovací metody a metody váženého součtu, vychází nejvhodnějším záložním zdrojem APC Smart-UPS X 2200VA LCD v obou metodách.

Celkový počet UPS: 1 kus

4.2.3 Výběr – NAS

Druhým prvkem určeným pro výběr je NAS server, který slouží jako chráněné úložiště pro zálohu dat a následnému přístupu uživatelů k těmto datům napříč sítě. Podle minimálních kritérií, stanovených majitelem, byly zvoleny tyto 4 NAS servery ke vzájemnému porovnání na základě vlastností, které byly vybrány. Tyto vlastnosti jsou:

- Cena
- Počet pozic pro disk
- Podpora 2,5“ disků
- Kapacita paměti RAM
- Hmotnost
- Podpora sdílení souborů
- Podpora nahrávání z IP kamer
- Frekvence procesoru
- VPN

Podle těchto vlastností, a jejich hodnot, byla sestavena následující tabulka, která je výchozí tabulkou k sestavení tabulky při procesu rozhodování, který nejvhodnější NAS server vybrat.

	Synology RackStation RS2416RP+	Synology RackStation RS816	QNAP TS-873U-8G	QNAP TS-873U-RP-8G
Cena (Kč)	64263	15997	46490	54490
Počet pozic pro disk (ks)	12	4	8	8
Podpora 2,5" disků	Ano (redukce)	Ano (redukce)	Ano	Ano
Kapacita paměti RAM (GB)	2	1	8	8
Hmotnost (kg)	13,25	4,34	9,83	10,93
Podpora sdílení souborů	Ano	Ano	Ano	Ano
Podpora nahrávání z IP kamer	Ano	Ano	Ano	Ano
Frekvence procesoru (GHz)	2,4	1,8	2,1	2,1
VPN	Ano	Ano	Ano	Ano

Tabulka 8 - Výběr NAS - základní tabulka (autor)

Byla použita metoda „bodovací“ s intervalem 1-10 (10 – nejlepší, 1 – nejhorší) a metoda „váženého součtu“, která využívá nejlepší možné kombinace a nejhorší možné kombinace k eliminaci subjektivního hodnocení. K porovnávání vlastností prvků byly stanoveny váhy, které poukazují na důležitost vlastnosti. Největší důraz byl kladen na vlastnost „Cena“, kdy tato vlastnost byla ohodnocena váhou 0,35. Nejmenší důraz byl kladen na vlastnost „Podpora sdílení souborů“ a „Podpora nahrávání z IP kamer“, které byly ohodnoceny váhou 0,025. Tyto vlastnosti jsou podstatou NAS serveru, proto nebyl takový důraz na tyto vlastnosti. Součet vah je roven 1.

	Synology RackStation RS2416RP+	Synology RackStation RS816	QNAP TS-873U-8G	QNAP TS-873U-RP-8G	Váhy
Cena (Kč)	1	10	4	2	0,35
Počet pozic pro disk (ks)	10	4	7	7	0,15
Podpora 2,5" disků	4	4	10	10	0,05
Kapacita paměti RAM (GB)	4	2	10	10	0,05
Hmotnost (kg)	4	10	8	7	0,05
Podpora sdílení souborů	10	10	10	10	0,025
Podpora nahrávání z IP kamer	10	10	10	10	0,025
Frekvence procesoru (GHz)	10	6	8	8	0,1
VPN	10	10	10	10	0,2
	5,95	8	7,15	6,4	1

Tabulka 9 - Výběr NAS - bodovací metoda (autor)

	Synology RackStation RS2416RP+	Synology RackStation RS816	QNAP TS-873U-8G	QNAP TS-873U-RP-8G	Váhy	H	D
Cena (Kč)	64263	15997	46490	54490	0,35	15997	64263
Počet pozic pro disk (ks)	12	4	8	8	0,15	12	4
Podpora 2,5" disků	4	4	10	10	0,05	10	4
Kapacita paměti RAM (GB)	2	1	8	8	0,05	8	1
Hmotnost (kg)	13,25	4,34	9,83	10,93	0,05	4,34	13,25
Podpora sdílení souborů	10	10	10	10	0,025	10	10
Podpora nahrávání z IP kamer	10	10	10	10	0,025	10	10
Frekvence procesoru (GHz)	2,4	1,8	2,1	2,1	0,1	2,4	1,8
VPN	10	10	10	10	0,2	10	10
					1		

	Synology RackStation RS2416RP+	Synology RackStation RS816	QNAP TS-873U-8G	QNAP TS-873U-RP-8G	Váhy
Cena (Kč)	0	1	0,368230224	0,202482078	0,35
Počet pozic pro disk (ks)	1	0	0,5	0,5	0,15
Podpora 2,5" disků	0	0	1	1	0,05
Kapacita paměti RAM (GB)	0,142857143	0	1	1	0,05
Hmotnost (kg)	0	1	0,383838384	0,260381594	0,05
Podpora sdílení souborů	1	1	1	1	0,025
Podpora nahrávání z IP kamer	1	1	1	1	0,025
Frekvence procesoru (GHz)	1	0	0,5	0,5	0,1
VPN	1	1	1	1	0,2
	0,507142857	0,65	0,623072498	0,558887807	1

Tabulka 10 - Výběr NAS - metoda váženého součtu (autor)

Po aplikaci bodovací metody a metody váženého součtu vychází nejvhodnějším NAS serverem Synology RackStation RS816 v obou metodách.

Celkový počet NAS: 1 kus

4.2.4 Výběr – Server

Třetím prvkem určeným pro výběr je server, který slouží jako poskytovatel služeb klientům sítě, popřípadě jako centrální správa těchto služeb, uživatelů, práv přístupu apod. Podle minimálních kritérií, stanovených majitelem, byly zvoleny tyto 4 servery ke vzájemnému porovnání na základě vlastností, které byly vybrány. Tyto vlastnosti jsou:

- Cena
- Kapacita disku
- Model procesoru
- Frekvence procesoru
- Cash procesoru
- Počet jader procesoru
- Přídavné sloty
- USB 3.0

- Rack montáž
- Maximální kapacita RAM

Podle těchto vlastností, a jejich hodnot, byla sestavena následující tabulka, která je výchozí tabulkou k sestavení tabulky při procesu rozhodování, který nejhodnější server vybrat.

	Lenovo ThinkServer RS160	Dell PowerEdge R230	Fujitsu PRIMERGY TX1310 M	Dell PowerEdge T30
Cena (Kč)	32990	38590	19990	28990
Kapacita disku (GB)	2000	600	2000	2000
Model procesoru	Intel Xeon E3 1220 v5	Intel Xeon E3 1220 v5	Intel Xeon E3-1225 v6	Intel Xeon E3 1225 v5
Frekvence procesoru (GHz)	3	3	3,3	3,3
Cash procesoru (MB)	8	8	8	8
Počet jader procesoru (ks)	4	4	4	4
Přídavné sloty	Ne	Ano	Ano	Ano
USB 3.0 (ks)	4	2	4	6
Rack montáž	Ano	Ano	Ne	Ne
Maximální kapacita RAM (GB)	64	64	32	64

Tabulka 11 - Výběr serveru - základní tabulka (autor)

Byla použita metoda „bodovací“ s intervalem 1-10 (10 – nejlepší, 1 – nejhorší) a metoda „váženého součtu“, která využívá nejlepší možné kombinace a nejhorší možné kombinace k eliminaci subjektivního hodnocení. K porovnávání vlastností prvků byly stanoveny váhy, které poukazují na důležitost vlastnosti. Největší důraz byl kladen na vlastnost „Počet jader procesoru“, „Přídavné sloty“ a „Maximální kapacita RAM“, kdy tyto vlastnosti byly ohodnoceny váhou 0,2. Nejmenší důraz byl kladen na vlastnost „Model procesoru“ a „USB 3.0“, které byly ohodnoceny váhou 0,005. Součet vah je roven 1.

	Lenovo ThinkServer RS160	Dell PowerEdge R230	Fujitsu PRIMERGY TX1310 M	Dell PowerEdge T30	Váhy
Cena (Kč)	6	4	10	7	0,05
Kapacita disku (GB)	10	4	10	10	0,05
Model procesoru	6	6	10	8	0,005
Frekvence procesoru (GHz)	8	8	10	10	0,04
Cash procesoru (MB)	10	10	10	10	0,1
Počet jader procesoru (ks)	10	10	10	10	0,2
Přídavné sloty	0	10	10	10	0,2
USB 3.0 (ks)	8	5	8	10	0,005
Rack montáž	10	10	0	0	0,15
Maximální kapacita RAM (GB)	10	10	5	10	0,2
	7,69	9,275	7,49	8,34	1

Tabulka 12 - Výběr serveru - bodovací metoda (autor)

	Lenovo ThinkServer RS160	Dell PowerEdge R230	Fujitsu PRIMERGY TX1310 M	Dell PowerEdge T30	Váhy	H	D
Cena (Kč)	32990	38590	19990	28990	0,05	19990	38590
Kapacita disku (GB)	2000	600	2000	2000	0,05	2000	600
Model procesoru	6	6	10	8	0,005	10	6
Frekvence procesoru (GHz)	3	3	3,3	3,3	0,04	3,3	3
Cash procesoru (MB)	8	8	8	8	0,1	8	8
Počet jader procesoru (ks)	4	4	4	4	0,2	4	4
Přídavné sloty	0	10	10	10	0,2	10	0
USB 3.0 (ks)	4	2	4	6	0,005	6	2
Rack montáž	10	10	0	0	0,15	10	0
Maximální kapacita RAM (GB)	64	64	32	64	0,2	64	32
					1		

	Lenovo ThinkServer RS160	Dell PowerEdge R230	Fujitsu PRIMERGY TX1310 M	Dell PowerEdge T30	Váhy
Cena (Kč)	0,301075269	0	1	0,516129032	0,05
Kapacita disku (GB)	1	0	1	1	0,05
Model procesoru	0	0	1	0,5	0,005
Frekvence procesoru (GHz)	0	0	1	1	0,04
Cash procesoru (MB)	1	1	1	1	0,1
Počet jader procesoru (ks)	1	1	1	1	0,2
Přídavné sloty	0	1	1	1	0,2
USB 3.0 (ks)	0,5	0	0,5	1	0,005
Rack montáž	1	1	0	0	0,15
Maximální kapacita RAM (GB)	1	1	0	1	0,2
	0,717553763	0,85	0,6475	0,823306452	1

Tabulka 13 - Výběr serveru - metoda váženého součtu (autor)

Po aplikaci bodovací metody vychází a metody váženého součtu nejvhodnějším serverem Dell PowerEdge R230 na kterém bude instalován Microsoft Windows Server Standard 2016 v obou metodách.

Celkový počet serveru: 1 kus

4.2.5 Výběr – PC (zákazníci)

Čtvrtým prvkem určeným pro výběr je počítač určený pro zákazníky, kteří budou moci využívat v recepčním sále pro vyhledávání informací na internetu. Podle minimálních kritérií, stanovených majitelem, byly zvoleny tyto 4 počítače k vzájemnému porovnání na základě vlastností, které byly vybrány. Tyto vlastnosti jsou:

- Cena
- Kapacita disku
- USB 3.0
- Uhlopříčka
- Frekvence procesoru
- Počet jader procesoru
- Hmotnost
- Maximální kapacita RAM

Podle těchto vlastností, a jejich hodnot, byla sestavena následující tabulka, která je výchozí tabulkou k sestavení tabulky při procesu rozhodování, který nejlépe vyhovuje počítač pro zákazníky vybrat.

	iMac 21.5" CZ Retina 4K 2017	HP 24-e007nc	Lenovo IdeaCentre 520-24IKL Silver	Acer Aspire C24-860
Cena (Kč)	39990	19490	21499	19990
Kapacita disku (GB)	1000	1000	1000	1000
USB 3.0 (ks)	4	2	3	2
Uhlopříčka (palce)	21,5	23,8	23,8	23,8
Frekvence procesoru (GHz)	3	2,5	2,4	2,5
Počet jader procesoru (ks)	4	2	4	2
Hmotnost (kg)	5,66	6,46	8,83	5
Kapacita paměti RAM (GB)	8	8	4	8

Tabulka 14 - Výběr PC pro zákazníka - základní tabulka (autor)

Byla použita metoda „bodovací“ s intervalem 1-10 (10 – nejlepší, 1 – nejhorší) a metoda „váženého součtu“, která využívá nejlepší možné kombinace a nejhorší možné kombinace k eliminaci subjektivního hodnocení. K porovnávání vlastností prvků byly stanoveny váhy, které poukazují na důležitost vlastnosti. Největší důraz byl kladen na vlastnosti „Počet jader procesoru“ a „Frekvence procesoru“, kdy tyto vlastnosti byly ohodnoceny váhou 0,2. Počítač je orientován na rychlost. Nejmenší důraz byl kladen na vlastnost „Uhlopříčka“ a „Hmotnost“, která byla ohodnocena váhou 0,05. Součet vah je roven 1.

	iMac 21.5" CZ Retina 4K 2017	HP 24-e007nc	Lenovo IdeaCentre 520-24IKL Silver	Acer Aspire C24-860	Váhy
Cena (Kč)	5	10	8	9	0,15
Kapacita disku (GB)	10	10	10	10	0,1
USB 3.0 (ks)	10	4	7	4	0,15
Uhlopříčka (palce)	8	10	10	10	0,05
Frekvence procesoru (GHz)	10	7	6	7	0,2
Počet jader procesoru (ks)	10	5	10	5	0,2
Hmotnost (kg)	8	6	3	10	0,05
Kapacita paměti RAM (GB)	10	10	5	10	0,1
	9,05	7,3	7,6	7,35	1

Tabulka 15 - Výběr PC pro zákazníka - bodovací metoda (autor)

	iMac 21.5" CZ Retina 4K 2017	HP 24-e007nc	Lenovo IdeaCentre 520-24IKL Silver	Acer Aspire C24-860	Váhy	H	D
Cena (Kč)	39990	19490	21499	19990	0,15	19490	39990
Kapacita disku (GB)	1000	1000	1000	1000	0,1	1000	1000
USB 3.0 (ks)	4	2	3	2	0,15	4	2
Uhlopříčka (palce)	21,5	23,8	23,8	23,8	0,05	23,5	23,8
Frekvence procesoru (GHz)	3	2,5	2,4	2,5	0,2	3	2,5
Počet jader procesoru (ks)	4	2	4	2	0,2	4	2
Hmotnost (kg)	5,66	6,46	8,83	5	0,05	5	8,83
Kapacita paměti RAM (GB)	8	8	4	8	0,1	8	4
					1		

	iMac 21.5" CZ Retina 4K 2017	HP 24-e007nc	Lenovo IdeaCentre 520-24IKL Silver	Acer Aspire C24-860	Váhy
Cena (Kč)	0	1	0,902	0,975609756	0,15
Kapacita disku (GB)	1	1	1	1	0,1
USB 3.0 (ks)	1	0	0,5	0	0,15
Uhlopříčka (palce)	7,666666667	0	0	0	0,05
Frekvence procesoru (GHz)	1	0	-0,2	0	0,2
Počet jader procesoru (ks)	1	0	1	0	0,2
Hmotnost (kg)	0,82767624	0,618798956	0	1	0,05
Kapacita paměti RAM (GB)	1	1	0	1	0,1
	1,174717145	0,380939948	0,4703	0,396341463	1

Tabulka 16 - Výběr PC pro zákazníka - metoda váženého součtu (autor)

Po aplikaci bodovací metody a metody váženého součtu vychází nejvhodnějším počítačem pro zákazníky iMac 21.5" CZ Retina 4K 2017 v obou metodách, který výrazně předčil ostatní počítače určených k výběru. Nespornou výhodou je rozlišení (tato vlastnost nebyla zahrnuta) 4K (4096x2304px). Kvalita obrazu, rychlost a vůbec samotná značka přidá na hodnocení zákazníků hotelu.

Při srovnání s jinými špičkovými hotely (Hilton, Intercontinental Hotel Group, aj.), mají tyto hotely počítače, určené pro zákazníky, značky Apple.

Celkový počet PC pro zákazníky: 1 kus

4.2.6 Výběr – PC (zaměstnanci)

Dalším počítačem určeným pro výběr je počítač pro zaměstnance, na kterých budou aplikace potřebné k chodu hotelu. Podle minimálních kritérií, stanovených majitelem, byly zvoleny tyto 4 NAS servery ke vzájemnému porovnání na základě vlastností, které byly vybrány. Tyto vlastnosti jsou:

- Cena
- Kapacita disku
- Frekvence procesoru
- Počet jader procesoru
- Kapacita paměti RAM

- USB 3.0
- Digitální výstup
- Operační systém
- Optická mechanika
- Čtečka paměťových karet
- Hmotnost

Podle těchto vlastností, a jejich hodnot, byla sestavena následující tabulka, která je výchozí tabulkou k sestavení tabulky při procesu rozhodování, který nevhodnější počítač pro zaměstnance vybrat.

	Alza TopOffice 3040	Dell Vostro 3668 MT	HP ProDesk 400 G3 DM	Lenovo ThinkCentre M710t Tower
Cena (Kč)	17490	18890	18390	20490
Kapacita disku (GB)	240	256	256	256
Frekvence procesoru (GHz)	3,5	3,5	2,7	3
Počet jader procesoru (ks)	4	4	4	4
Kapacita paměti RAM (GB)	8	8	8	8
USB 3.0 (ks)	3	2	4	6
Digitální výstup	Ano	Ano	Ano	Ano
Operační systém	Windows 10 Pro	Windows 10 Pro	Windows 10 Pro	Windows 10 Pro
Optická mechanika	Ne	Ano	Ne	Ano
Čtečka paměťových karet	Ne	Ano	Ne	Ano
Hmotnost (kg)	3,8	6,3	1,3	6,5

Tabulka 17 - Výběr PC pro zaměstnance - základní tabulka (autor)

Byla použita metoda „bodovací“ s intervalem 1-10 (10 – nejlepší, 1 – nejhorší) a metoda „váženého součtu“, která využívá nejlepší možné kombinace a nejhorší možné kombinace k eliminaci subjektivního hodnocení. K porovnávaným vlastnostem prvků byly stanoveny váhy, které poukazují na důležitost vlastnosti. Největší důraz byl kladen na vlastnost „Cena“, kdy tato vlastnost byla ohodnocena váhou 0,25. Nejmenší důraz byl kladen na vlastnost „Hmotnost“, která byla ohodnocena váhou 0,03. Součet vah je roven 1.

	Alza TopOffice 3040	Dell Vostro 3668 MT	HP ProDesk 400 G3 DM	Lenovo ThinkCentre M710t Tower	Váhy
Cena (Kč)	10	7	8	5	0,25
Kapacita disku (GB)	8	10	10	10	0,15
Frekvence procesoru (GHz)	10	10	6	8	0,1
Počet jader procesoru (ks)	10	10	10	10	0,05
Kapacita paměti RAM (GB)	10	10	10	10	0,07
USB 3.0 (ks)	6	5	7	10	0,1
Digitální výstup	10	10	10	10	0,05
Operační systém	10	10	10	10	0,1
Optická mechanika	0	10	0	10	0,05
Čtečka paměťových karet	0	10	0	10	0,05
Hmotnost (kg)	7	5	10	4	0,03
	8,21	8,6	7,8	8,37	1

Tabulka 18 - Výběr PC pro zaměstnance - bodovací metoda (autor)

	Alza TopOffice 3040	Dell Vostro 3668 MT	HP ProDesk 400 G3 DM	Lenovo ThinkCentre M710t Tower	Váhy	H	D
Cena (Kč)	17490	18890	18390	20490	0,25	17490	20490
Kapacita disku (GB)	240	256	256	256	0,15	256	240
Frekvence procesoru (GHz)	3,5	3,5	2,7	3	0,1	3,5	2,7
Počet jader procesoru (ks)	4	4	4	4	0,05	4	4
Kapacita paměti RAM (GB)	8	8	8	8	0,07	8	8
USB 3.0 (ks)	3	2	4	6	0,1	6	2
Digitální výstup	10	10	10	10	0,05	10	10
Operační systém	10	10	10	10	0,1	10	10
Optická mechanika	0	10	0	10	0,05	10	0
Čtečka paměťových karet	0	10	0	10	0,05	10	0
Hmotnost (kg)	7	5	10	4	0,03	4	10
					1		

	Alza TopOffice 3040	Dell Vostro 3668 MT	HP ProDesk 400 G3 DM	Lenovo ThinkCentre M710t Tower	Váhy
Cena (Kč)	1	0,533333333	0,7	0	0,25
Kapacita disku (GB)	0	1	1	1	0,15
Frekvence procesoru (GHz)	1	1	0	0,375	0,1
Počet jader procesoru (ks)	1	1	1	1	0,05
Kapacita paměti RAM (GB)	1	1	1	1	0,07
USB 3.0 (ks)	0,25	0	0,5	1	0,1
Digitální výstup	1	1	1	1	0,05
Operační systém	1	1	1	1	0,1
Optická mechanika	0	1	0	1	0,05
Čtečka paměťových karet	0	1	0	1	0,05
Hmotnost (kg)	0,5	0,833333333	0	1	0,03
	0,66	0,778333333	0,645	0,6875	1

Tabulka 19 - Výběr PC pro zaměstnance - metoda váženého součtu (autor)

Po aplikaci bodovací metody a metody váženého součtu vychází nejvhodnějším počítačem pro zaměstnance Dell Vostro 3668 MT, na kterém je přinstalován operační systém Microsoft Windows 10 Pro a vybaven standartním kancelářským monitorem, klávesnicí a myší.

Celkový počet PC pro zaměstnance: 2 kusy

4.2.7 Výběr – Notebook

Posledním prvkem určeným pro výběr je notebook pro majitele hotelu, který má dlouhou výdrž baterie, spolehlivost a nízkou hmotnost. Podle minimálních kritérií, stanovených majitelem, byly zvoleny tyto 4 notebooky k vzájemnému porovnání na základě vlastností, které byly vybrány. Tyto vlastnosti jsou:

- Cena
- Kapacita disku
- Kapacita baterie
- Uhlopříčka
- Frekvence procesoru
- Počet jader procesoru
- Hmotnost
- Kapacita paměti RAM

Podle těchto vlastností, a jejich hodnot, byla sestavena následující tabulka, která je výchozí tabulkou k sestavení tabulky při procesu rozhodování, který nejvhodnější notebook vybrat.

	Dell Inspiron 13z (5000) Touch šedý	ASUS ZENBOOK UX430UN-GV033T	Lenovo Yoga 510-14IKB	MacBook Pro 13" Retina CZ 2017
Cena (Kč)	22990	25990	21999	45990
Kapacita disku (GB)	256	256	256	256
Kapacita baterie (Wh)	42	50	35	54,5
Uhlopříčka (palce)	13,3	14	14	13,3
Frekvence procesoru (GHz)	1,6	1,6	2,5	2,3
Počet jader procesoru (ks)	4	4	2	2
Hmotnost (kg)	1,62	1,3	1,75	1,37
Kapacita paměti RAM (GB)	8	8	8	8

Tabulka 20 - Výběr notebooku - základní tabulka (autor)

Byla použita metoda „bodovací“ s intervalem 1-10 (10 – nejlepší, 1 – nejhorší) a metoda „váženého součtu“, která využívá nejlepší možné kombinace a nejhorší možné kombinace k eliminaci subjektivního hodnocení. K porovnávaným vlastnostem prvků byly stanoveny váhy, které poukazují na důležitost vlastnosti. Největší důraz byl kladen na vlastnost „Kapacita baterie“, kdy tato vlastnost byla ohodnocena váhou 0,25. Nejmenší důraz byl kladen na vlastnost „Kapacita paměti RAM“, která byla ohodnocena váhou 0,04. Součet vah je roven 1.

	Dell Inspiron 13z (5000) Touch šedý	ASUS ZENBOOK UX430UN-GV033T	Lenovo Yoga 510-14IKB	MacBook Pro 13" Retina CZ 2017	Váhy
Cena (Kč)	9	7	10	4	0,1
Kapacita disku (GB)	10	10	10	10	0,08
Kapacita baterie (Wh)	6	8	4	10	0,25
Uhlopříčka (palce)	8	10	10	8	0,07
Frekvence procesoru (GHz)	5	5	10	8	0,25
Počet jader procesoru (ks)	10	10	5	5	0,06
Hmotnost (kg)	7	10	4	9	0,15
Kapacita paměti RAM (GB)	10	10	10	10	0,04
	7,06	7,95	7,3	8,31	1

Tabulka 21 - Výběr notebooku - bodovací metoda (autor)

	Dell Inspiron 13z (5000) Touch šedý	ASUS ZENBOOK UX430UN-GV033T	Lenovo Yoga 510-14IKB	MacBook Pro 13" Retina CZ 2017	Váhy	H	D
Cena (Kč)	22990	25990	21999	45990	0,1	21999	45990
Kapacita disku (GB)	256	256	256	256	0,08	256	256
Kapacita baterie (Wh)	42	50	35	54,5	0,25	54,5	35
Uhlopříčka (palce)	13,3	14	14	13,3	0,07	14	13,3
Frekvence procesoru (GHz)	1,6	1,6	2,5	2,3	0,25	2,5	1,6
Počet jader procesoru (ks)	4	4	2	2	0,06	4	2
Hmotnost (kg)	1,62	1,3	1,75	1,37	0,15	1,3	1,75
Kapacita paměti RAM (GB)	8	8	8	8	0,04	8	8
					1		

	Dell Inspiron 13z (5000) Touch šedý	ASUS ZENBOOK UX430UN-GV033T	Lenovo Yoga 510-14IKB	MacBook Pro 13" Retina CZ 2017	Váhy
Cena (Kč)	0,958692843	0,833645951	1	0	0,1
Kapacita disku (GB)	1	1	1	1	0,08
Kapacita baterie (Wh)	0,358974359	0,769230769	0	1	0,25
Uhlopříčka (palce)	0	1	1	0	0,07
Frekvence procesoru (GHz)	0	0	1	0,777777778	0,25
Počet jader procesoru (ks)	1	1	0	0	0,06
Hmotnost (kg)	0,288888889	1	0	0,844444444	0,15
Kapacita paměti RAM (GB)	1	1	1	1	0,04
	0,408946207	0,675672287	0,54	0,691111111	1

Tabulka 22 - Výběr notebooku - metoda váženého součtu (autor)

Po aplikaci bodovací metody a metody váženého součtu vychází nejvhodnějším notebookem pro majitele MacBook Pro 13" Retina CZ 2017, který o 0,06 porazil notebook Lenovo Yoga 510-14IKB. Při takto těsném výsledku je vybrán MacBook Pro 13" Retina CZ 2017, který má lepší vlastnosti i v těchto vlastnostech, které nebyly zahrnuté do rozhodovacího modelu. Tyto vlastnosti jsou:

- vyšší rozlišení (2460x1600px) oproti konkurenci
- vyšší Core Boost frekvence (3,6GHz) oproti konkurenci
- vyšší stabilita operačního systému Mac OS

Celkový počet notebooků: 1 kus

4.2.8 Poskytnuté prvky

Majitelem hotelu a IT jeho pracovníky byly poskytnuty tiskárny od společnosti OKI a rozvaděč (Rack). Nebylo odůvodněno proč tyto prvky byly poskytnuty, ale lze uvažovat

o skutečnosti, že tyto tiskárny jsou využívány pracovníky v jiných objektech. Po zjištění kvalit tiskáren se dá říci, že se jedná o tiskárny určené pro kancelářské využití, jsou tedy velice odolné, málo poruchové a jednoduché na obsluhu. Vzhledem k charakteru tiskárny, jedná se o laserové, jsou tonery obecně do tiskáren tohoto typu velice drahé. Z ekonomického hlediska je výhodné kupovat tiskárny od stejného, ověřeného výrobce, kdy tonery jsou vzájemně zaměnitelné. Podle velikosti objednávky lze aplikovat množstevní slevu od výrobce a lze tonery distribuovat do jednotlivých pracovišť dle potřeby.

4.2.8.1 Rozvaděč

Rozvaděč (Rack), byl poskytnut společností Triton, se kterou majitel hotelu spolupracuje a dodává mu rozvaděčové systému do jeho dalších projektů. Konkrétně model Triton ROA-27-A88-BAX-A1, jedná se o otočný rozvaděč se skleněnými dveřmi. Jeho výhodou je velikost, protože v útrokách rozvaděče je otočný skelet, do kterého jsou rackové prvky instalovány. Velikost racku je 800x800mm, není tedy problém projít standartní velikostí dveří. V horní a dolní části jsou ventilátory pro zajištění optimální teploty uvnitř rozvaděče. Rozvaděč je formátu 27U.

Do rozvaděče budou instalovány prvky, které jsou o velikosti 1U, kromě UPS, která je o velikosti 2U.

4.2.8.2 Tiskárny

Tiskárny byly poskytnuté majitelem od společnosti OKI a jejich vlastnosti budou v následujících podkapitolách více přiblížené.

Kancelářská tiskárna

Pro potřeby kanceláře, kde se předpokládá objemné množství tisknutých papírů, jako jsou jídelní lístky, denní nabídka, faktury aj., to vše se bude tisknout na tiskárně v kanceláři. Také je zde potřeba scanner, kdy bude potřeba dokumenty kopírovat nebo zálohovat v elektronické formě. Od této tiskárny se vyžaduje jednoduché a intuitivní ovládání, spolehlivost, rychlost, oboustranný tisk, tisk formátu A3 a možnost síťového připojení. Tiskárna OKI MC853dn tyto vlastnosti splňuje. Zde jsou její hlavní přednosti:

- Technologie tisku: Laser. barevná
- Rychlost tisku barevně/černobíle: 23 str./min /23 str./min
- Maximální měsíční vytížení: 60 000 str./měsíc
- Tisk A3 formátu

Tiskárnu je možné připojit pomocí portu USB, ale je vyžadováno LAN připojení. Tato tiskárna toto připojení také obsahuje. Mezi její další funkce je kopírování a skenování (v rozlišení 600dpi), které jsou nutné při kancelářské práci. Další výhodou je oboustranný tisk, kdy je možné šetřit množství spotřebovaného papíru. 60 000 stran za měsíc se zdá jako malé množství, ale pokud se tento počet převeden na dny, pak za den je maximální vytížení až 2 000 stránek. Tento počet je více než dostačující.

Recepční tiskárna

Potřeby recepce se nijak neliší od potřeb kanceláře. Ovšem na rozdíl od kancelářské tiskárny nepotřebuje recepce tisk A3 formátu nebo scanner ani kopírku. Tím bude velikost této tiskárny daleko kompaktnější a bude možné ji daleko lépe umístit v recepčním sále. Od této tiskárny se hlavně vyžaduje spolehlivost a rychlost tisku. Pro tyto potřeby byla majitelem zvolena tiskárna OKI C532dn. Toto jsou její vlastnosti:

- Technologie tisku: Laser. barevná
- Rychlost tisku barevně/černobíle: 30 str./min /26 str./min
- Maximální měsíční vytížení: 60 000 str./měsíc

Tiskárnu je možné připojit pomocí portu USB, ale je vyžadováno LAN připojení. Tato tiskárna toto připojení také obsahuje. Další výhodou je oboustranný tisk, kdy je možné šetřit množství spotřebovaného papíru. 60 000 stran za měsíc se zdá jako malé množství, ale pokud se tento počet převeden na dny, pak za den je maximální vytížení až 2 000 stránek. Tento počet je více než dostačující.

4.3 Analýza měření Wi-Fi signálu

Jako dílčím cílem této diplomové práce je analýza Wi-Fi signálu stávající sítě. Pro zjištění kvality Wi-Fi signálu byl použit Wi-Fi Analyzer dostupný pro mobilní zařízení se

systemem Android. Za pomoci tohoto testu zjistime, jakym zpusobem je hotelove zarizeni pokryto.

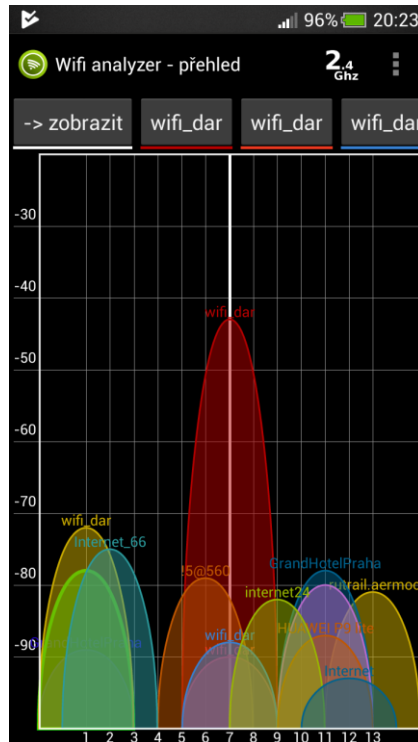
Po zkoumani site timto programem bylo zjisteno velice značne množství Wi-Fi siti v okolí a je zde značne riziko přehlcenosti frekvenčního pásma. V následující tabulce budou znázorněny jednotlivé stupně kvality signálů. Síla Wi-Fi signálu je měřena v dBm (decibel milliwatts) a vyjadřuje, jak moc je signál negativně ovlivněn.

Síla signálu	Očekávaná kvalita	Vyžadováno pro
-30 dBm	Maximální síla, pravděpodobně je analyzátor hned vedle zdroje.	
-50dBm	Velice silný a stabilní signál.	
-60 dBm	Dostačující síla signálu.	-67 dBm je minimum pro stabilní a silný signál pro uskutečnění hlasových telefonátů a sledování non-HD videa.
-70 dBm	Jedná se již o slabý signál ovlivněna počtem připojených zařízení.	Lehké prohlížení stránek a e-mailů.
-80 dBm	Nespolehlivá síla signálu a zároveň nedostatečné pro více uživatelů.	Připojení k internetu
-90 dBm	Minimální šance připojení zařízení k tomuto signálu.	

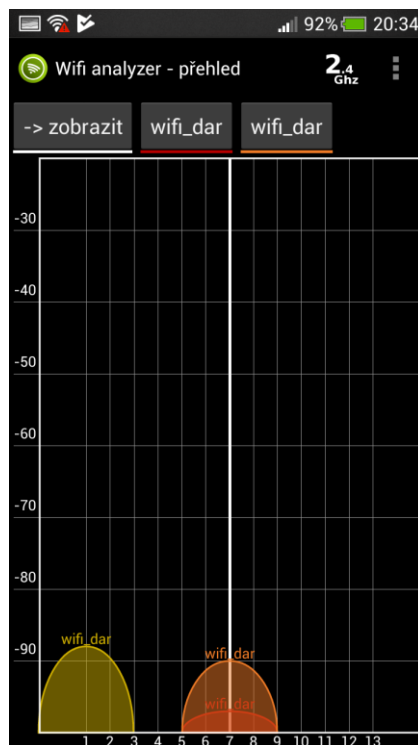
Tabulka 23 - Kvalita Wi-Fi signálu (autor)

Pro měření Wi-Fi signálu byly vybrány konkrétní pozice v prostorách hotelu, kde se očekává vysoký počet připojených zařízení. Jedná se o restaurační zařízení, recepční sál hotelu, vinárna a 2 pokoje. Následující obrázky byly zaznamenány v restauračním zařízení, recepčním sále a vinárně. Wi-Fi s SSID „wifi_dar“ běží na 7 kanále v tomto frekvenčním pásmě, k této Wi-Fi síti jsou přidružené další antény, které rozšiřují síť na další patra. Na

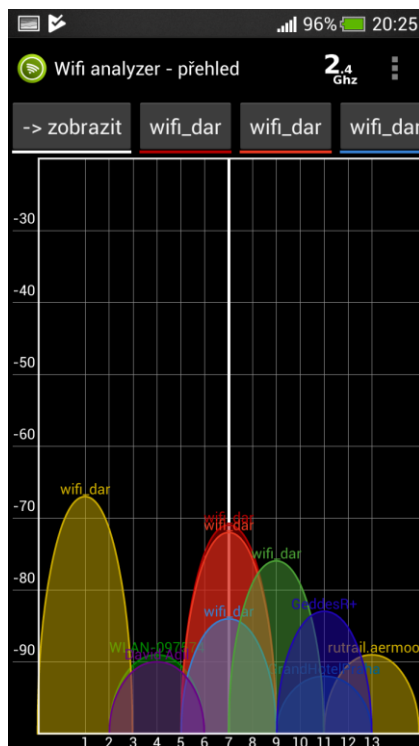
prvním a devátém kanále jsou totožné Wi-Fi sítě s SSID „wifi_dar“, která obsahuje vyšší stupeň šifrování hesla, tyto sítě jsou generované stejnou anténou.



Obrázek 22 - Analýza Wi-Fi signálu v restauraci (autor)

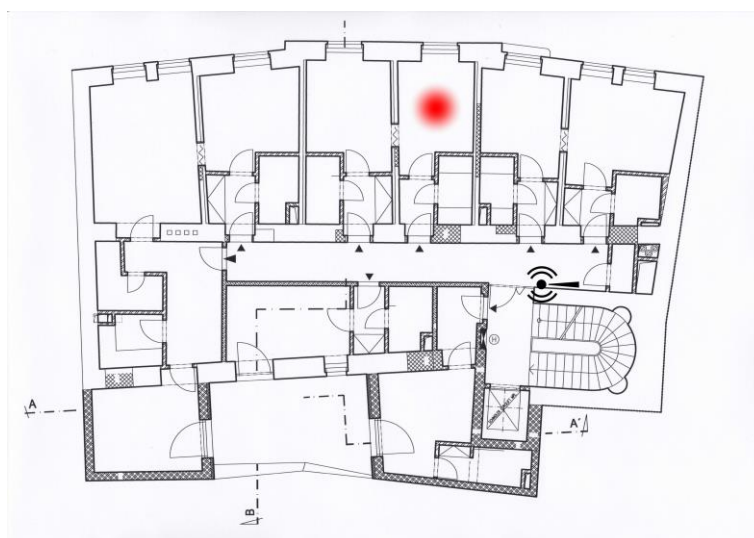


Obrázek 23 - Analýza Wi-Fi signálu ve vinárně (autor)

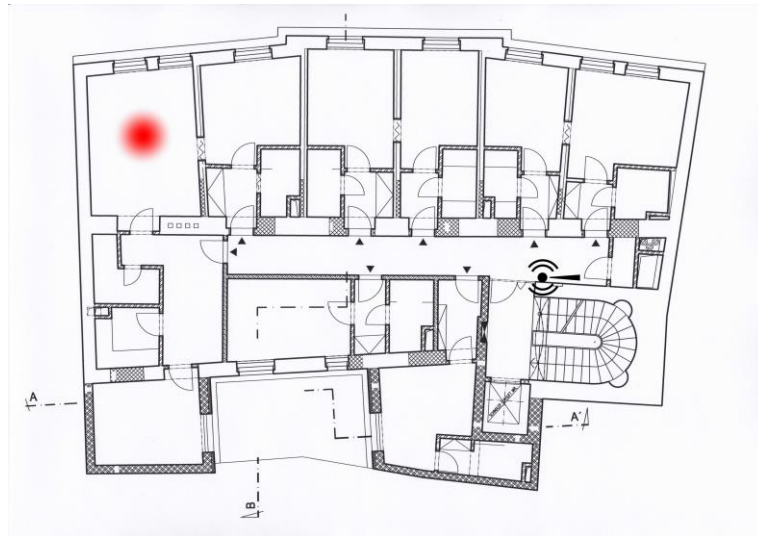


Obrázek 24 - Analýza Wi-Fi signálu na recepci (autor)

Následující snímky poukazují na analýzu Wi-Fi sítě provedenou v pokojích hotelového zařízení. Byly vybrány dva pokoje, první pokoj se nachází ve druhém nadzemním podlaží hotelu a druhý pokoj se nachází ve třetím nadzemním podlaží hotelu. Tyto dva pokoje jsou vyznačené v následujících obrázcích.

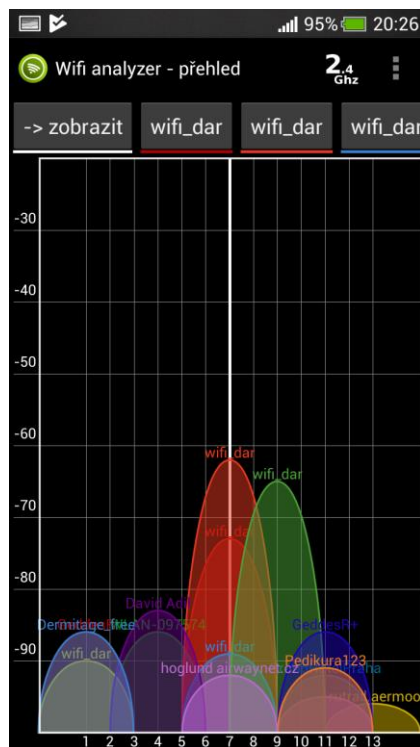


Obrázek 25 - Pozice měření v druhém nadzemním podlaží (autor)

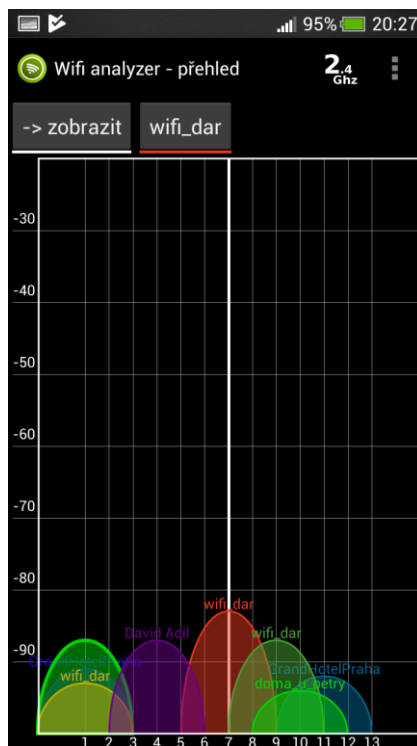


Obrázek 26 - Pozice měření ve třetím nadzemním podlaží (autor)

Zde jsou výsledky měření. Na obrázcích je patrná vzdálenost od vysílače signálu.



Obrázek 27 - Analýza Wi-Fi signálu v pokoji druhého nadzemního podlaží (autor)



Obrázek 28 - Analýza Wi-Fi signálu v pokoji třetího nadzemního podlaží (autor)

V průběhu měření ovlivňoval sílu signálu počet připojených zařízení. Analýza Wi-Fi potvrdila nejen závěr autora při analýze stávající sítě, ale také potvrdila špatné recenze uživatelů na internetu.

4.4 Finanční analýza

Pro majitele je důležité kvalitní Wi-Fi služby pro jeho zákazníky a nový kamerový systém, který by zajišťoval bezpečnost nemovitosti a nové síťové řešení. Majitel si zvolil „Řešení 1“ z důvodů předpokladu koupě sousední nemovitosti a tím možnost rozšířit hotel téměř na dvojnásobnou plochu (očekává se 2x větší počet IP kamer a 2x Wi-Fi antén). Z toho důvodu si majitel vybral toto řešení a přeje si mít kvalitně připravený rozvaděč v pracovně. Jedná se o nákladnější řešení, protože obsahuje více prvků. V Následujících podkapitolách budou vyčísleny jednotlivé náklady na realizaci návrhu „Řešení 1“. Ceny budou vyčísleny včetně DPH. Majitelova firma je plátcem DPH a bude schopna si o výši DPH snížit základ daně.

4.4.1 Náklady na pořízení síťového zařízení

Nákup síťových prvků od společnosti Ubiquiti Networks, by se uskutečnil na internetovém obchodě Senetic (<https://www.senetic.cz/>), která se specializuje na prodej síťových prvků.

Název	Cena za kus	Množství	Cena celkem
EdgeRouter	7 190,00 Kč	1	7 190,00 Kč
US-24-500W	12 824,00 Kč	3	38 472,00 Kč
US-48-750W	27 203,00 Kč	1	27 203,00 Kč
UniFi UAP-AC-PRO	3 515,00 Kč	12	42 180,00 Kč
UniFi Video Camera G3 Dome	3 373,00 Kč	25	84 325,00 Kč
UniFi Video G3 PRO	7 265,00 Kč	4	29 060,00 Kč
UniFi NVR Controller 2 TB	12 499,00 Kč	1	12 499,00 Kč
UniFi Voip Phone Executive	8 850,00 Kč	4	35 400,00 Kč
Cena celkem			276 329,00 Kč

Tabulka 24 - Náklady na "Řešení 1" v rozvaděči (autor)

Cena celkem činí 276 329,00 Kč včetně DPH.

4.4.2 Náklady na pořízení ostatního zařízení

Nákup ostatního zařízení potřebného k realizaci sítě proběhnou na internetovém obchodě Alza.cz (<https://www.alza.cz/>), kromě prvků poskytnutých majitelem. Tyto prvky ale byly zahrnuty do finanční analýzy pro lepší upřesnění finální ceny za realizaci. Do výpočtu nákladů byly zahrnuty i náklady za nákup kabeláže. Byl vybrán kabel (lanko) CAT5E v provedení UTP. Kabely budou koupeny v krabicích a bude provedena kabeláž na míru. Délka kabelu v krabici je 305 metrů. Počet RJ45 konektorů v jednom balení je 100 kusů.

Název	Cena za kus	Množství	Cena celkem
APC Smart-UPS X 2200VA LCD	48 590,00 Kč	1	48 590,00 Kč
Synology RackStation RS816	15 997,00 Kč	1	15 997,00 Kč
Dell PowerEdge R230	38 590,00 Kč	1	38 590,00 Kč
iMac 21.5" CZ Retina 4K 2017	39 990,00 Kč	1	39 990,00 Kč
Dell Vostro 3668 MT	18 890,00 Kč	2	37 780,00 Kč
Klávesnice	229,00 Kč	2	458,00 Kč
Myš	229,00 Kč	2	458,00 Kč
Monitor	3 290,00 Kč	2	6 580,00 Kč
MacBook Pro 13" Retina CZ 2017	45 990,00 Kč	1	45 990,00 Kč
Triton ROA-27-A88-BAX-A1	47 434,00 Kč	1	47 434,00 Kč
OKI MC853dn	30 990,00 Kč	1	30 990,00 Kč
OKI C532dn	7 190,00 Kč	1	7 190,00 Kč
Datacom, licna (lanko), CAT5E, UTP, 305m	1 899,00 Kč	3	5 697,00 Kč
RJ-45 konektor, 100-pack,Datacom	409,00 Kč	2	818,00 Kč
Cena celkem			326 562,00 Kč

Tabulka 25 - Náklady na pořízení ostatního zařízení (autor)

Cena celkem činí 326 562,00 Kč včetně DPH.

Pro rozvod kabeláže ke každému prvku v síti, bude celkem potřeba 3 kusů balení Datacom lanka, kdy v jednom balení je celkem 305 metrů lanka. Bylo vypočteno přibližné celkové množství lanka, kterého bude potřeba cca 708, metrů. Jedna se pouze o orientační výpočet na základě kotování a odhadu z půdorysů budovy. V posledním balení je dostatečná rezerva při chybě výpočtu a propojení prvků v rozvaděči. Při počtu 52 prvků, které jsou zakreslené v půdorysech budovy, bude tedy potřeba 104 RJ-45 konektorů, zbylé konektory budou potřeba při propojení prvků v rozvaděči, nebo budou použity jako rezerva.

4.4.3 Náklady na software

Náklady na software se skládají z antivirového programu od společnosti ESET, který zajistí bezpečnost stanic a sítě jako takové, dále z balíčku Microsoft Office pro podnikatele, které budou instalovány na všechny nové stanice a jako poslední je zde Microsoft Windows Server Standard 2016, který se bude instalovat na server Dell PowerEdge R230. Operační systém na stanice není potřeba, protože stanice jsou již vybaveny operačními systémy Microsoft Windows 10 Pro a MacOS. Antivirová programy

jsou formou roční licence. Tyto částky se následně promítnou do provozních nákladů v dalších letech.

Název	Cena za kus	Množství	Cena celkem
ESET Smart Security Premium (2 stanice)	2 390,00 Kč	1	2 390,00 Kč
ESET Cyber Security Pro (2 stanice)	1 935,00 Kč	1	1 935,00 Kč
ESET Secure Enterprise	6 950,00 Kč	1	6 950,00 Kč
Office 2016 pro podnikatele pro PC	7 699,00 Kč	2	15 398,00 Kč
Office 2016 pro podnikatele pro Mac	7 699,00 Kč	2	15 398,00 Kč
Microsoft Windows Server Standard 2016 x64	17 599,00 Kč	1	17 599,00 Kč
Cena celkem			59 670,00 Kč

Tabulka 26 - Náklady na software (autor)

Cena celkem činí 59 670,00 Kč včetně DPH.

4.4.4 Náklady na práci

Instalaci sítě budou provádět IT pracovníci majitele dle návrhu „Řešení 1“, proto nebude vypočtena cena za jejich práci, jedná se o práci v rámci jejich pracovní náplně, za kterou dostávají mzdu.

4.4.5 Celkové náklady

Náklady v prvním roce reprezentují součet těchto nákladů:

- Náklady na pořízení síťového zařízení
- Náklady na pořízení ostatního zařízení
- Náklady na software

Název	Cena celkem
Náklady na pořízení síťového zařízení	276 329,00 Kč
Náklady na pořízení ostatního zařízení	329 016,00 Kč
Náklady na software	59 670,00 Kč
Cena celkem	665 015,00 Kč

Tabulka 27 - Celkové náklady na "Řešení 1" (autor)

Celkové náklady na pořízení všech potřebných komponent a softwaru v prvním roce budou činit 665 015,00 Kč včetně DPH.

4.4.6 Provozní náklady v dalších letech

V následujících podkapitolách budou orientačně vypočítané náklady na udržení chodu tohoto nového síťového řešení v provozu a jeho bezpečnosti.

4.4.6.1 Spotřeba energie

Tyto náklady se velice často opomíjí, ale je velice vhodné vyčíslit spotřebu energie, které v tomto případě bude nemalá. Do výpočtu byly zahrnuty prvky, které jsou v provozu denně. Cena za energii byla vypočítaná na základě spotřeby jednotlivých prvků a průměrné ceny za energii 1 kWh, která je 3,50 Kč/KWh včetně DPH. Jsou zde simulovány 2 možné případy. První kalkulace je výpočet spotřeby elektřiny při zachování stávajícího počtu prvků. Druhá kalkulace je vypočtena v případě rozšíření budovy a tím rozšíření sítě. Pro výpočet byl použit Microsoft Excel.

Tyto kalkulace jsou pouze orientační, do kalkulací je zahrnuta skutečnost, že některé prvky, ač jsou v provozu 24 hodin, nespotřebovávají 100% elektrické energie. Příkladem mohou být kamery, které zcela určitě nebudou vytiženy ze 100% po celý den, ale pro stanovení ceny za energii bylo počítáno se 100% využitím po celý den. Je velice obtížné vypočítat skutečnou spotřebu, ale je velice pravděpodobné, že skutečná cena za energii bude nižší než ceny zde vypočítané.

Stávající počet prvků

V následující tabulce je souhrn všech prvků, které by byly v 24 hodinovém provozu.

Název	Spotřeba (W)	Počet zař.	Spotřeba celkem
EdgeRouter	35,00	1	35,00
US-24-500W (odhad)	40,00	3	120,00
US-48-750W (odhad)	40,00	1	40,00
UniFi UAP-AC-PRO	9,00	12	108,00
UniFi Video Camera G3 Dome	4,00	25	100,00
UniFi Video G3 PRO	12,50	4	50,00
UniFi NVR Controller 2 TB	65,00	1	65,00
UniFi Voip Phone Executive	26,00	4	104,00
APC Smart-UPS X 2200VA LCD (odhad)	40,00	1	40,00
Synology RackStation RS816	28,00	1	28,00
Dell PowerEdge R230	200,00	1	200,00
Spotřeba celkem			890

Tabulka 28 - Přehled spotřeby stávajícího řešení (autor)

Spotřeba v této variantě činí 890,00 W.

Výsledek		Použité vzorce
Cena za hodinu (Kč):	3,12	$890,00/1000*3,5$
Cena za měsíce(Kč):	2242,80	$890,00/1000*3,5*24*30$
Cena za rok(Kč):	26913,60	$890,00/1000*3,5*24*30*12$
Spotřeba za měsíc (kWh):	640,80	$890,00,00/1000*24*30$
Spotřeba za rok (kWh):	7689,60	$890,00/1000*24*30*12$

Tabulka 29 - Výpočet výsledné ceny za energii stávajícího řešení (autor)

Výsledná cena za spotřebu energie v této variantě je 26 913,60 Kč za rok vč. DPH.

Možný budoucí počet prvků

V následující tabulce je přibližný souhrn všech prvků, které by byly v 24 hodinovém chodu. Po rozšíření hotelu by bylo nutné dokoupit určité prvky, aby byla zachována bezpečnost hotelu a také zajistit Wi-Fi pokrytí sítě pro hotelové hosty. Následující počet prvků je pouze orientační. Počty nových prvků, pořízených do nových částí hotelu, se mohou lišit. Pro orientační výpočet byly přidány tyto prvky:

- US-48-750W: 1 kus
- UniFi UAP-AC-PRO: 8 kusů
- UniFi Video Camera G3 Dome: 25 kusů

- UniFi Video G3 PRO: 3 kusy
- UniFi Voip Phone Executive: 2 kusy

Název	Spotřeba(W)	Počet zař.	Spotřeba celkem
EdgeRouter	35,00	1	35,00
US-24-500W (odhad)	40,00	3	120,00
US-48-750W (odhad)	40,00	2	80,00
UniFi UAP-AC-PRO	9,00	20	180,00
UniFi Video Camera G3 Dome	4,00	50	200,00
UniFi Video G3 PRO	12,50	8	100,00
UniFi NVR Controller 2 TB	65,00	1	65,00
UniFi Voip Phone Executive	26,00	6	156,00
APC Smart-UPS X 2200VA LCD (odhad)	40,00	1	40,00
Synology RackStation RS816	28,00	1	28,00
Dell PowerEdge R230	200,00	1	200,00
Spotřeba celkem			1204,00

Tabulka 30 - Přehled spotřeby po rozšíření hotelu (autor)

Navýšení spotřeby v této variantě je oproti variantě se současným počtem prvků o 314,00 W větší.

Výsledek		Použité vzorce
Cena za hodinu (Kč):	4,21	$1204,00/1000*3,5$
Cena za měsíce(Kč):	3034,08	$1204,00/1000*3,5*24*30$
Cena za rok(Kč):	36408,96	$1204,00/1000*3,5*24*30*12$
Spotřeba za měsíc (kWh):	866,88	$1204,00/1000*24*30$
Spotřeba za rok (kWh):	10402,56	$1204,00/1000*24*30*12$

Tabulka 31 - Výpočet výsledné ceny za energie po rozšíření hotelu (autor)

V této variantě je patrné zvýšení spotřeby, tedy i zvýšení cen za energie. Cena za energie v této variantě je 36 408,96 Kč vč. DPH za rok. Rozdíl, mezi variantou s počtem prvků před rozšířením a variantou po rozšíření, činí 9 495,36 Kč vč. DPH za rok. Měsíčně to je 791,28 Kč vč. DPH.

4.4.6.2 Software

V následující tabulce jsou vyobrazené náklady na software v následujících letech. Tyto náklady se mohou měnit s měnícím se počtem počítačových stanic v budově.

Název	Cena za kus	Množství	Cena celkem
ESET Smart Security Premium (2 stanice) (rok)	2 390,00 Kč	1	2 390,00 Kč
ESET Cyber Security Pro (2 stanice) (rok)	1 935,00 Kč	1	1 935,00 Kč
ESET Secure Enterprise (rok)	6 950,00 Kč	1	6 950,00 Kč
Cena celkem			11 275,00 Kč

Tabulka 32 - Náklady na software v následujících letech (autor)

5 Výsledky a diskuse

V úvodu této kapitoly je potřeba zmínit, že závěry jsou odvozeny ze studie bibliografický a elektronických zdrojů a výsledků praktické části práce. V případě aplikace výsledků práce je nutné brát ohled na teoretická východiska a jejich aplikace a interpretaci praktické části práce, jejíž platnost může být ovlivněna řadou prvků.

5.1 Výsledky praktické části

Výsledkem diplomové práce je návrh nové počítačové sítě pro hotelové zařízení DAR, kde je kladen důraz na spokojenost zákazníků, tedy zabezpečit uspokojení jejich poptávky po internetu pomocí nové Wi-Fi sítě, ale také zajistit bezpečnost objektu jako takového pomocí instalace nového kamerového řešení. Je dobré podotknout, že bylo vybrané nákladnější řešení s ohledem na budoucí rozvoj hotelového zařízení, kdy se v příštích měsících očekává rozšíření hotelových prostor téměř o dvojnásobný počet pokojů, a to koupí a rekonstrukcí sousedního objektu. K návrhu nové sítě bylo zapotřebí několika dílčích cílů. Prvním cílem bylo analyzovat prostředí. Analýza prostředí proběhal za pomoci AutoCAD výkresů, které byly poskytnuty majitelem. Tyto výkresy jsou z roku 2006, tedy z doby, kdy bylo hotelové zařízení zkolaudováno. Po získání těchto materiálů bylo možné fyzicky analyzovat prvky sítě a jejich situování v rámci objektu a jejich následného zakreslení do půdorysu jednotlivých pater. Po této analýze bylo zcela evidentní nedostatečné pokrytí Wi-Fi sítí v prostorách hotelu. Toto tvrzení po potvrzení nejen analýzou Wi-Fi sítě, které je jedním z dílčích cílů, ale také špatným hodnocením zákazníků na internetových rezervačních portálech. Staří kamer, které je spojeno se stářím hotelu, již nevyhovuje stávajícím nárokům, neschopnost HD záznamu nebo nočního vidění nepracuje kamerový systém efektivním způsobem.

Pro návrh nové sítě bylo potřeba zajistit určité požadavky na novou síť, které byly získány od majitele a jeho IT pracovníků. Byl kladen důraz na Wi-Fi pokrytí hotelu a nové bezpečnostní kamery zajišťující záznam a přehrávání v HD rozlišení. Požadavky na nové prvky sítě byly celkem 3 různých typů, výběr síťových prvků od zadané společnosti, výběr dalších zařízení sítě a třetí typem prvků byly dodané prvky od majitele. K sestavení sítě bylo vyžadováno využít prvky od společnosti Ubiquiti Networks a to z důvodu tzv.

„sladěnosti“, kdy prvky od stejné společnosti pracují na vyšší úrovni, ale také sjednocení síťových prvků této budovy s administrativními budovami a jinými objekty majitele. Po výběru vhodných prvků od této společnosti byly vytvořeny 2 řešení sítě. „Řešení 1“ je vytvořeno s ohledem na možnost přidání dalších prvků a tím připravit síťové řešení na situaci, kdy bude hotelové zařízení rozšířeno o nové prostory pro hotelové hosty, pak bude potřeba zajistit rozšíření pokrytí Wi-Fi sítě pro hosty, ale také zabezpečit nové prostory dalšími kamerami do kamerové sítě. Odhadovaný počet prvků, které by se do sítě přidaly, je 39, z toho 28 prvků by byly kamerové zařízení. Jedná se o velice značný nárůst prvků a tím je potřeba dostatečně dimenzovat novou síť. Je patrné nevyužitelnost výstupů aktivních prvků, ale naopak nám ulehčí konfiguraci nových prvků sítě. „Řešení 2“ je postavené s maximálním využitím výstupů aktivních prvků pomocí VLAN. Toto řešení obsahuje o 2 aktivní prvky méně a jednotlivé výstupy aktivních prvků jsou přiřazeny k jednotlivým sítím. Toto řešení je méně nákladné, ale do budoucna by bylo potřeba dokoupit chybějící aktivní prvky a bylo by nutné z části rekonfigurovat síť hotelového zařízení. Z toho důvodu bylo rozhodnuto pro „Řešení 1“, kdy se počítá s rozšířením hotelového zařízení. Dalším důvodem je také skutečnost, kdy celkové náklady na realizaci nové sítě činí 665 015,00 Kč. Jedná se tedy o velice nákladné řešení. Cena druhého řešení by byla nižší o 2 ušetřené aktivní prvky, tedy o částku 25 648,00 Kč, které by bylo potřeba stejně dokoupit, když by se instalovali nové prvky do nových prostor hotelu. Po výběru prvků do sítě nastal výběr dalších zařízení sítě. Konkrétně se jedná o zařízení NAS, UPS, serveru, počítače pro zákazníky, počítače pro zaměstnance a notebooku pro majitele. Podle minimálních kritérií proběhl výběr prvků na internetovém portálu Alza.cz, kde byli vybrány vždy 4 zařízení reprezentující daný segment. Dále pak byly stanoveny kritéria a za pomoci vícekritériální analýzy byl vybrán nejvhodnější prvek. Z vícekritériální analýzy byly použity 2 metody, a to metoda bodovací, kdy jednotlivá kritéria byly ohodnoceny na stupnici od 1 do 10, kde 1 je nejhorší a 10 nejlepší. Dále byly stanoveny váhy pro jednotlivá kritéria s celkovým součtem 1. V této metodě mohou být jisté subjektivní preference. Proto byla dále zvolena metoda váženého součtu, která pracuje s ideální a bazální hodnotou. Výsledky metody bodovací byly potvrzeny výsledky metody váženého součtu za předpokladu využití stejných vah pro jednotlivá kritéria. Po výběru těchto prvků byly autorem představeny dodané prvky, a to tiskárny a rozvaděč. Jelikož jsou tyto prvky dodané a nepodléhají

žádnému výběru, byly v práci krátce popsány. Jsou zde uvedené z důvodu vypočtení celkových nákladů na vybudování sítě.

V poslední části praktické části se práce zabývá finanční analýzou nové sítě a jejími náklady v dalších letech. Celkové náklady na toto řešení činí 665 015,00 Kč, jedná se tedy o velice nákladné řešení, pro objekt této velikosti. Náklady na síťová zařízení od společnosti Ubiquiti Networks činí 276 329,00 Kč, je vhodné podotknout náklady na samotné kamery které činí 113 385,00 Kč. Dále náklady na ostatní zařízení jsou 326 562,00 Kč. V této části by se dalo velice značně ušetřit, v některých případech se jedná o profesionální zařízení, které využívají větší podniky, nebo výsledná cena může být ovlivněna produkty od společnosti Apple, které jsou více nákladné oproti konkurenci. Náklady na software činí 59 670,00 Kč. Zajímavou kapitolou jsou náklady v příštích letech, do té jsou započítané náklady na zajištění bezpečnosti sítě a zajištění administrativních prostředků, které činí 11 275,00 Kč. Byla zde vytvořena analýza náklady na spotřebu elektrické energie při stávajícím počtu prvků, ale také při budoucím počtu prvků, tedy v situaci, kdy je již objekt rozšířen. Současná spotřeba prvků, které by byly v 24 hodinovém provozu (je počítáno s maximální možnou spotřebou) je 890,00 W. Při průměrné ceně 3,50 Kč za 1 kWh by celkové náklady za energii činily 26 91,60 Kč za rok. Po rozšíření sítě, kde by byl současný počet prvků rozšířena o další prvky, orientačně o 39 prvků, by se zvýšila spotřeba na 1 204,00 W. Při stejné průměrné ceně za 1 kWh by celkové náklady na elektrickou energii činily 36 408,96 Kč za rok. Měsíčně to činí 791,28 Kč vyšší náklady než při stávajícím počtu prvků. Uváděné ceny jsou ceny vč. DPH,

Přínosem diplomové práce je reálné řešení pro hotel DAR, ale také navržení komplexní počítačové sítě pro hotelové zařízení podobného charakteru, popřípadě pro podniky střední velikosti, zde by síť byla daleko více orientovaná jako privátní síť s důrazem na bezpečnost. Tato navržená síť může být orientační sítí pro neznalé v tomto oboru a poukázat na nákladnost tohoto řešení a pomoci jim v jejich rozhodování a objemu jejich možností investovat do nové infrastruktury svého objektu.

5.2 Diskuse

V době vyhotovení práce se v hotelovém zařízení vyskytly problémy ohledně hotelových systémů, kdy zanikl poskytovatel tohoto softwaru. Bylo tedy rozhodnuto

o instalaci nového softwaru od nové společnosti, která poskytla nabídku zahrnující náklady na server, který by byl umístěn v síti hotelového zařízení. Jedná se v podstatě o jednoúčelový server, který by byl použitelný pouze pro daný software. Vzhledem k výkonu zvoleného serveru od společnosti Dell by bylo možné nový software instalovat na nový server a tím zmenšit náklady na nový hotelový systém. Vzhledem k výkonu serveru zde vznikají otázky jeho využití. O využití adresářové služby zde není pochyb nebo instalaci jednotlivých služeb od společnosti Microsoft, jako je například Microsoft Exchange Server 2016, pro hotelový e-mail, ale také virtualizace stanic, kde by běžel zmíněný nový hotelový software, který by byl oddělený od fyzického serveru jako takového, ale také možnost instalace dalších aplikací na virtuální server, jakou může být správa elektrifikovaných zámků a požárních hlásičů.

6 Závěr

Spousta hotelových zařízení se snaží soustředit na svoji primární činnost, kde se snaží zdokonalovat svoje procesy ve vedení zařízení tohoto typu, ale zapomínají na moderní technologie a nedrží krok s moderní dobou v oblasti informačních technologií. Nevěnují podpůrným činnostem tolik pozornosti, času a hlavně ani financí. Z toho důvodu mohou být hotelové sítě zastarale a mohou mít problémy s implementací nových technologií nebo adaptací na nové nařízení jakou je například nařízení Evropské unie GDPR, které slouží k ochraně osobních údajů. K tvorbě sítě je doporučeno vybírat prvky sítě, se kterými má administrátor již zkušenosti a jsou bezpečnými prvky a je možné jim důvěřovat. Z toho důvodu byli zvoleny prvky sítě od stanovené společnosti. Určitě je možné vytvořit levnější řešení od jiných zprostředkovatelů nebo kombinovat různé výrobce, nicméně je důležité rozlišovat funkce jednotlivých zařízení a pokládat si otázky, zda má takové zařízení smysl teď, ale i v budoucnosti. Výběr prvků od stejné společnosti může být nákladnější, ale zde mnohem větší jistota ve správnost fungování sítě jako celku.

Během nabytých znalostí v průběhu studia a studia teoretických podkladů se práce snažila navrhnout nejlepší, novou, počítačovou síť ve zvoleném hotelu. Rozsah a nákladnost tohoto projektu je velice značná na rozdíl od domácího prostředí, kde by bylo možné navrženou síť zrealizovat a ukázat její praktické využití v praxi.

V praktické části provedl autor analýzu stávajícího hotelové řešení, která byla vyhodnocena jako nedostatečná, kde se toto tvrzení potvrdilo z recenzí hotelových zákazníků. Po této analýze byl proveden návrh dvou nových síťových řešení. První řešení pracovalo se skutečností, kdy majitel hodlá rozšířit budovu téměř na dvojnásobnou velikost, toto řešení je navrženo tak, aby bylo již připravené na situaci, kdy se budou přidávat nové prvky. Druhé řešení pracuje s aktuální velikostí hotelu a všechny prvky jsou maximálně využity a je zde provedena jistá minimalizace oproti prvnímu řešení. V tomto řešení by byly využity VLAN sítě při konfiguraci switchů. Vzhledem k malému rozdílu nákladů obou řešení a záměrů majitele, bylo zvoleno první řešení. Prvky této sítě jsou od zvolené společnosti, kterou stanovil majitel se svým IT zázemím, a to z důvodů sjednocení prvků tohoto zařízení s prvky v jiných objektech majitele. Dále byly vybírány prvky pomocí vícekritériální analýzy variant, kde byla určena kritéria pro výběr a podle nich vyšla nejlepší možná varianta pro výběr konkrétního prvku. Jednou z kapitol

praktické části, byla provedena metodika pro testování stávající sítě, kde se potvrdily závěry autora a také se zde potvrdily tvrzení hotelových zákazníků o nedostatečném Wi-Fi pokrytí prostoru hotelu. Závěrem praktické části práce byla provedena finanční analýza prvního řešení, kdy náklady na a pořízení všech potřebných komponent a softwaru v prvním roce budou činit 665 015,00 Kč včetně DPH. Také byly vypočteny provozní náklady v příštích letech z pohledu na stávající velikost sítě a také z pohledu sítě po rozšíření hotelu. Příkladem je cena za energii při stávající velikosti, kde je spotřeba 890,00 W, která činí 26 913,60 Kč za rok. Po rozšíření sítě, kde by potřeba vzrostla o 314,00 W, by cena za energii na 36 408,96 Kč za rok. Je velice obtížné vypočítat skutečnou spotřebu, ale je velice pravděpodobné, že skutečná cena za energii bude nižší než ceny zde vypočítané, nejen z důvodů skutečné hodinové spotřeby prvků, protože prvky mohou fungovat ve spořicí režimu, ale také z důvodů proměnlivé ceny za 1 kWh.

Návrh této sítě může sloužit jako návrh pro hotelové řízení podobného charakteru a velikosti, popřípadě jiných podnikových objektů s jistými individuálními úpravami jako je velikost úložiště, počet připojených zařízení a finančních prostředcích podniku.

7 Citovaná literatura

1. **Focus, Micro.** Novell eDirectory 8.7.3 Administration Guide. *www.novell.com*. [Online] 2018.
<https://www.novell.com/documentation/edir873/?page=/documentation/edir873/edir873/data/h0000007.html>.
2. **Nožka, Ing. Marek.** Komunikační model vrstvy TCP/IP I. *http://mamut.spseol.cz*. [Online] 1999. http://mamut.spseol.cz/nozka/psk/134-tcpip_1/.
3. **Bouška, Petr.** Počítačové sítě - základní topologie. *Samuraj-cz.com*. [Online] 30. Července 2007. <https://www.samuraj-cz.com/clanek/pocitacove-site-zakladni-topologie/>.
4. **Koutná, Marcela a Sochor, Tomáš.** *Úvod do počítačových sítí*. Orlová : Obchodní akademie Orlová, 2006.
5. **Peterka, Jiří.** Aplikační protokoly TCP/IP. *earchiv.cz*. [Online] 1998.
<http://www.earchiv.cz/a98/a819k180.php3>.
6. **Matyska, Luděk.** Operační systém UNIX. *webserver.ics.muni.cz*. [Online] 1991.
<http://webserver.ics.muni.cz/bulletin/articles/395.html>.
7. **WDC.** SÍŤOVÉ ÚLOŽIŠTĚ. *wdc.com*. [Online] <https://www.wdc.com/cs-cz/solutions/what-is-network-attached-storage-nas.html>.
8. **Peterka, Jiří.** NFS. *earchiv.cz*. [Online] 1993. <http://www.earchiv.cz/a93/a341c110.php3>.
9. **Peterka, Jiří.** Referenční model ISO/OSI - sedm vrstev. *earchiv.cz*. [Online] 1992.
<http://www.earchiv.cz/a92/a213c110.php3>.
10. **Hotel Fontána, s.r.o.** Jednotná klasifikace hotelů, hotelů garni, motelů a penzionů. *cestovni-ruch.cz*. [Online] <http://www.cestovni-ruch.cz/kategorizace/jednotna.php>.
11. **Sosinsky, Barrie.** *Mistrovství počítačové sítě*. Brno : Computer Press, a.s., 2010. ISBN 9788025139165.
12. **Klímeš, Cyril.** *Úvod do počítačových sítí*. Ostrava : Ostravská univerzita v Ostravě, 2003. ISBN 8070428651.
13. **Stanek, William R.** *Mistrovství v Microsoft Windows Server 2008*. Brno : Computer Press, a.s., 2011. ISBN 9788025138717.
14. **Donahue, Gary A.** *Kompletní průvodce síťového experta*. Brno : Computer Press, a.s., 2009. ISBN 9788025122471.
15. **Horák, Jaroslav a Keršláger, Milan.** *Počítačové sítě pro začínající správce*. Brno : Computer Press, a.s., 2016. ISBN 8025143961.

16. **Libor, Dostálek a Alena, Kabelová.** *Velký průvodce protokoly TCP/IP a systémem DNS.* Praha : Computer Press, a.s., 2000. ISBN 8025138860.
17. **Russel, Charlie a Crawford, Sharon.** *Microsoft Windows Server 2008.* Brno : Computer Press, a.s., 2009. ISBN 9788025121153.
18. **Droms, Ralph a Lemon, Ted.** *DHCP Příručka administrátora.* Brno : Computer Press, a.s., 2004. ISBN 8025101304.
19. **Wallace, Kevin.** *VoIP.* Brno : Computer Press, a.s., 2007. ISBN 9788025114582.
20. **Nemeth, Evi, Snyder, Garth a Hein, Trent R.** *Linux.* Brno : Computer Press, a.s., 2008. ISBN 9788025124109.
21. **Stanek, William R.** *Active Directory.* Brno : Computer Press, a.s., 2009. ISBN: 978-80-251-2555-7.
22. **Šubrt, Tomáš.** *Ekonomicko-matematické metody.* Praha : Vydavatelství a nakladatelství Aleš Čeněk, 2015. ISBN 9788073805630.
23. **Kretchmar, James M.** *Administrace a diagnostika sítí.* Brno : Computer Press, a.s., 2005. ISBN 8025103455.
24. **Zeltser, Lenny, a další.** *Bezpečnost počítačových sítí.* Brno : Computer Press, a.s., 2005. ISBN 8025106977.
25. **Stanek, William R.** *Microsoft Exchange Server 2010.* Brno : Computer Press, a.s., 2010. ISBN 9788025133422 .
26. **Zandl, Patrick.** *Bezdrátové sítě WiFi.* Brno : Computer Press, a.s., 2003. ISBN 9788072266326.
27. **Roupec, Jan.** *Počítačové sítě.* Brno : VUT Brno, 2002.
28. **David, Gourley.** *HTTP.* Champaign : O'Reilly Media, Inc, USA, 2002. ISBN13 9781565925090.
29. **Peterka, Jiří.** DNS. *earchiv.cz.* [Online] 1998.
<http://www.earchiv.cz/a98/a816k180.php3>.