



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

IMPLEMENTACE VOIP SYSTÉMU 3CX

IMPLEMENTATION OF VOIP SYSTEM 3CX

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE

AUTHOR

Vojtěch Sommer

VEDOUCÍ PRÁCE

SUPERVISOR

Ing. Viktor Ondrák, Ph.D.

BRNO 2018

Zadání bakalářské práce

Ústav: Ústav informatiky
Student: **Vojtěch Sommer**
Studijní program: Systémové inženýrství a informatika
Studijní obor: Manažerská informatika
Vedoucí práce: **Ing. Viktor Ondrák, Ph.D.**
Akademický rok: 2017/18

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

Implementace VoIP systému 3CX

Charakteristika problematiky úkolu:

Úvod
Cíle práce
Analýza současného stavu
Teoretická východiska práce
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Navrhnout implementaci VoIP systému.

Základní literární prameny:

BITTO, Ondřej. Základy VoIP [online]. [cit. 2017-03-06]. Dostupné z: <http://www.lupa.cz/clanky/jak-se-vola-pres-internet-zaklady-voip/>

JOHNSTON, Alan B. SIP: understanding the session initiation protocol. 3rd ed. Boston: Artech House, 2009. ISBN 978-1-60783-995-8.

PEREA, Rogelio Martínez. Internet multimedia communication using SIP: a modern approach including java practice. Amsterdam: Elsevier; Morgan Kaufmann, 2008. ISBN 978-0-12-374300-8.

PETERKA, Jiří. VoIP, IP telefonie. Praha: Univerzita Karlova, 2006.

SIP. CESNET [online]. 1122 [cit. 2017-03-05]. Dostupné z: <https://sip.cesnet.cz/cs/protokoly/sip>

WALLACE, Kevin. Cisco VoIP: autorizovaný výukový průvodce. Brno: Computer Press, 2009. 527 s. ISBN 978-80-251-2228-0.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2017/18

V Brně dne 28.2.2018

L. S.

doc. RNDr. Bedřich Půža, CSc.
ředitel

doc. Ing. et Ing. Stanislav Škapa, Ph.D.
děkan

Abstrakt

Cílem této bakalářské práce je vysvětlení VoIP a popis implementace ve firemním prostředí. Firma, která toto řešení zvolila, přechází na toto řešení ze zastaralých pevných linek. Práce je rozdělena na teoretické vysvětlení komunikace pomocí SIP a implementaci systému.

Abstract

The aim of this bachelor thesis is explanation of VoIP and description of implementation in company environment. Company which have choosen this solution is converting to this solution from old landline connections. Thesis is devided in theoretical explanation of SIP communication and implementation of the system.

Klíčová slova

VoIP, SIP, implementace, komunikace, systém

Key words

VoIP, SIP, implementation, communication, system

Bibliografická citace

SOMMER, V. *Implementace VoIP systému 3CX*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2018. 65 s. Vedoucí bakalářské práce Ing. Viktor Ondrák, Ph.D.

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 15. května 2018

podpis studenta

Poděkování

Rád bych poděkoval vyučujícímu Ing. Viktoru Ondrákovi, Ph.D. za pevné vedení mé bakalářské práce, díky kterému jsem získal znalosti, které mohu uplatnit i v pozdějších pracích. Dále bych chtěl poděkovat Ing. Martinovi Veselému, který mi umožnil provést implementaci systému ve společnosti Jonckers.

OBSAH

ÚVOD.....	11
1 CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ.....	12
2 TEORETICKÁ VÝCHODISKA PRÁCE	13
2.1 VoIP	13
2.2 Historie IP telefonie	13
2.3 Signalizace a přenos v telekomunikačních sítích	13
2.3.1 Signalizace	13
2.3.2 Vlastní přenos (RTP)	24
2.3.3 Kontrola přenosu (RTCP).....	26
2.3.4 Kódování.....	26
2.3.5 Možnosti realizace	27
3 ANALÝZA SOUČASNÉHO STAVU	30
3.1 Firma.....	30
3.2 Počítačová síť.....	32
3.2.1 Aktivní prvky	32
3.2.2 Kabeláž	34
3.2.3 Serverová infrastruktura	35
3.2.4 Bezpečnost sítě	36
3.3 Stav telefonie	39
3.3.1 PBX (telefonní ústředna)	39
3.3.2 Pevné telefony.....	40
3.3.3 Číselný plán linek	40

3.4	Požadavky ze strany zadavatele.....	40
3.5	SWOT analýza.....	41
3.6	Shrnutí analýzy	41
3.6.1	Negativní faktory	41
3.6.2	Pozitivní faktory	42
4	VLASTNÍ NÁVRHY ŘEŠENÍ	43
4.1	Logický návrh.....	44
4.1.1	Návrh požadavků na nový komunikační systém	44
4.1.2	Návrh signalizace.....	44
4.1.3	Umístění a způsob realizace ústředny.....	44
4.1.4	Výběr systému	45
4.1.5	Umístění ústředny	46
4.1.6	Číselný plán linek	46
4.1.7	Systém provoleb	46
4.1.8	Návrh logiky směrování a volacích skupin.....	47
4.1.9	Hlasové schránky	47
4.2	Vytvoření Virtual Machine	47
4.3	Instalace ústředny	48
4.3.1	Nastavení síťového rozhraní	48
4.3.2	Instalace virtuální ústředny	49
4.3.3	Instalace certifikátů	49
4.4	Nastavení ústředny.....	49
4.5	Nastavení výjimek na firewallu	49

4.6	Vytvoření uživatelských účtů	50
4.7	Získání potřebných informací od poskytovatele pro nastavení ústředny	50
4.8	Vytvoření směrovacích pravidel a reportovacích nástrojů	51
4.8.1	Vytvoření volacích skupin	51
4.8.2	Vytvoření směrovacích pravidel	51
4.8.3	Vytvoření reportovacích nástrojů	51
4.9	Instalace telefonní aplikace na uživatelská zařízení	52
4.10	Testovací provoz	53
4.11	Odstranění pevných linek a PBX	54
4.11.1	Pevné linky a kabeláž	54
4.11.2	Telefonní ústředna	54
4.12	Uvedení do provozu	54
4.13	Ekonomické zhodnocení	55
4.13.1	Návratnost investice	56
ZÁVĚR		58
SEZNAM POUŽITÝCH ZDROJŮ		59
SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ		61
SEZNAM GRAFŮ		62
SEZNAM OBRÁZKŮ		63
SEZNAM TABULEK		64
SEZNAM PŘÍLOH		65

ÚVOD

VoIP představuje zvukovou komunikaci, kterou lze přenášet pomocí internetového protokolu. Tato vlastnost umožňuje efektivní uplatnění ve firmách a domácnostech. Velkým rozdílem oproti klasickým pevným linkám je způsob přenosu. Zatímco pevné linky pracovali s analogovým signálem, VoIP pracuje s digitálním signálem. Přesnější specifikace pro přenos a způsob komunikace definují jednotlivé protokoly. V této práci bude dále popsán protokol SIP. Veškerou komunikaci lze tedy přenášet stejným médiem, jakým přenášíme internetové připojení. Tato vlastnost představuje výhodu pro firmu, kde systém implementují, neboť můžeme odstranit kabely pro dosud používanou pevnou linku.

VoIP systémy dnes nabízí většina poskytovatelů internetového připojení a komunikačních operátorů. Pro firmy představuje modernější, ve většině případů také, levnější alternativu pro pevné linky. Mezi jednu z mnoha výhod patří mobilita a volání v rámci sítě zdarma. Pro implementaci jsem si vybral systém 3CX, který nabízí firma UPC. Tato společnost primárně poskytuje internetové připojení.

1 CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Cílem této práce je navrhnout telefonní komunikační systém společnosti. Vedle návrhu samotné technologie, na základě které bude tento komunikační systém pracovat, se práce věnuje implementaci do prostředí mezinárodní firmy a řešení jednotlivých aspektů systému od administrace, přes koncového uživatele až po ekonomiku provozu.

V úvodů mé práce se věnuji představení VoIP, které je dále popsáno v teoretické části práce, kde bude rozebrán princip fungování možných technologií, které lze v daném oboru uplatnit. V práci bude rovněž popsána analýza současného stavu, kde bude rozebrán obor podnikání společnosti Jonckers, aktuální stav počítačové sítě, současný stav telefonie a požadavky, které zadavatel očekává. Na základě analýzy vypracuji vlastní návrh řešení, který by se měl dočkat skutečné implementace ve firemním prostředí. Výsledek tohoto návrhu bude doplněn ekonomickým zhodnocením.

Závěr práce bude obsahovat zhodnocení spolupráce účastníků a přínosy, které tato práce všem těmto subjektům přinesla.

2 TEORETICKÁ VÝCHODISKA PRÁCE

Důležitá teoretická východiska této práce je pochopení principu fungování komunikace v této síti. Tato znalost je důležitá pro pochopení dalšího kroku práce, kterým je implementace 3CX systému.

2.1 VoIP

VoIP v plném znění Voice over Internet Protocol je technologie pro přenos digitalizovaného hlasu. Tento hlas lze přenášet rodinou protokolů UDP/TCP/IP po veřejné síti Internet nebo privátní síti intranet. Na rozdíl od pevných linek využívá stejné přenosové médium jako internetové připojení (1). Využívá se zde protokol IP na třetí vrstvě a protokoly TCP a UDP na čtvrté vrstvě ISO/OSI modelu (7).

2.2 Historie IP telefonie

Za počátek IP telefonie je považován únor 1995, kdy izraelská společnost Vocaltec přišla s produktem Internet Phone. Nová technika zpracování hlasu, pomocí kodeky s lineární predikcí, umožnila redukovat hovorové pásmo při zachování kvality a jejich nasazení se uplatnilo právě v IP telefonii. Díky možnosti využití internetu jako infrastruktury pro telefonii se snižují náklady na telefonování. Dominantní se stalo kódování ITU-T G.729 a G.723.1. Povinnost pro všechna zařízení je schopnost dorozumět se na ITU-T G.711 (3).

2.3 Signalizace a přenos v telekomunikačních sítích

Problematika telefonie se především skládá ze signalizace, přenosu, řízení přenosu a kódování.

2.3.1 Signalizace

Signalizace je výměna informací týkajících se sestavování a řízení spojení v telekomunikačních sítích, a také výměna informací při dohlížení nad těmito sítěmi. Tato definice signalizace byla vypracována pro digitální síť integrovaných služeb (ISDN =

Integrated Services Digital Network) a byla zveřejněna v řadě I. doporučení ITU-T pod označením I.112 (03/93) "Názvosloví sítí ISDN" (Vocabulary of terms for ISDNs). Doporučení I.112 obsahuje definice pojmů používaných v sítích ISDN. Stejná definice byla převzata i do technické zprávy, kterou vypracoval technický výbor ETSI, pojmenovaný "Služby a protokoly pro zdokonalené sítě (SPAN)" (Services and Protocols for Advanced Networks (SPAN)). Tato zpráva, nazvaná "Pojmy a definice" (Terms and definitions), byla vydána ETSI v roce 2001 s označením ETSI TR 101 287 V1.2.1 (2001-09) (TR = Technical Report) (14).

Hlavním úkolem signalizace v telekomunikačních sítích je zajistit spojovací funkce systémů přenosem nezbytných informací pomocí stanoveného souboru řídicích signálů. V případě systémů přenosu komutovanými spoji slouží signalizace k sestavování, udržování a rušení příslušných spojení (14).

Podle účelu užívání se rozlišují tyto druhy signalizace:

- Signalizace na přípojných účastnických vedeních ústředen (účastnická signalizace). Koncové zařízení si vyměňují informace s ústřednou jako prvkem sítě, na kterou je připojeno v koncovém bodě sítě.
- Signalizace uvnitř ústředen k vyměňování informací mezi jednotlivými částmi ústředny (vnitřní signalizace). Vnitřní signalizace je řešena individuálně výrobcem spojovacího systému a závisí na interních specifikacích výrobce.
- Signalizace k připojení přístupových systémů (přístupová signalizace). Tato signalizace umožňuje výměnu informací mezi koncovým zařízením a obslužnou ústřednou pomocí tzv. přístupového systému v přístupové síti.
- Signalizace k výměně informací mezi ústřednami (meziústřednová signalizace, nazývaná také síťová signalizace).

Signalizace zajišťuje výměnu informací, přesněji řečeno výměnu řídicích signálů a zpráv. Podle definice zavedené v doporučení ITU-T Q.9 (88 a 93) Názvosloví spojování a signalizace (Vocabulary of switching and signalling terms), vydaném v rámci "Obecných doporučení pro telefonní spojování a signalizaci v mezinárodním automatickém a poloautomatickém styku", pojem signalizační systém (signalling system)

zahrnuje nejen stanovenou soustavu procedur pro interpretaci a užívání definované množiny řídicích signálů a zpráv, ale i příslušná zařízení a/nebo programová vybavení (software) potřebná pro generování, přenos a příjem těchto signálů a zpráv (14).

Signalizaci lze realizovat více způsoby. V klasických telekomunikačních sítích pracujících s komutací okruhů se v případě systémů s analogovým telefonním přenosem potřebné signalizační informace přenášely hovorovým kanálem, tzn. pro každý hovorový kanál zvlášť (individuálně). S nástupem digitálních spojovacích systémů byl k přenosu signalizace vytvořen oddělený signalizační kanál, zpravidla společný pro více hovorových kanálů (14).

2.3.1.1 SIP

SIP v plném znění Session Initiation Protocol je signalizační protokol, který je využíván k řízení multimediálních relací v IP sítích (2). Obsahuje zprávy pro sestavení, udržení a ukončení spojení. Jádrem protokolu je definováno v RFC 3261. RFC je soubor doporučení popisující internetové protokoly (4). Session Initiation Protocol se stal velkou silou v aplikačním inženýrství a sítích příští generace (6).

Protokol SIP je typu klient-server, takže komunikace probíhá výměnou dvou typů zpráv, požadavků a odpovědí. Klient i server jsou logickou částí jednoho prvku. Pokud je dále v textu zmiňován termín klient, je tím míněn telefon nebo softwarová aplikace u uživatele a pojmem server jsou označovány aplikační servery služby, které poskytují klientům další služby jako registrace, lokalizace, zpoplatňování atd. Protokol SIP lze použít i pro další účely například síťové hry, instant messaging a další (5).

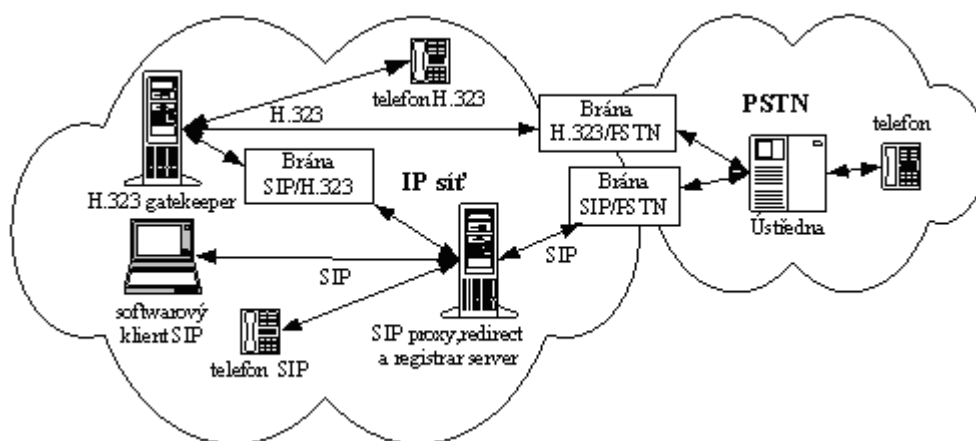
2.3.1.1.1 Historie SIP

Historie SIP se začala psát v roce 1996 (8, s. 12). V té době vznikly základy protokolu, který byl vyvinut pracovní skupinou MMUSIC (Multiparty Multimedia Session Control) v rámci IETF (Internet Engineering Task Force). Ve stejném roce vznikla pracovní skupina nazvaná SIP, která převzala vývoj hlavního jádra protokolu. Výsledný Session Initiation Protocol byl v roce 1999 přijat jako RFC 2543. O další vývoj protokolu se stará IETF a SIP Forum (16).

2.3.1.1.2 Způsob komunikace SIP

SIP je signalizační protokol pracující na aplikační vrstvě. Je navržen tak, aby byl snadno implementovatelný, rozšiřitelný a dostatečně flexibilní. Protokol je využíván pro navázání, modifikaci a ukončení spojení s protějšimi stranami. Pro komunikaci je zapotřebí dalších protokolů, nejčastěji RTP a SDP. RDP protokol slouží k přenosu multimédií v reálném čase. Tento protokol umožňuje přenos videa a hlasu v paketech pomocí IP. Dalším důležitým protokolem je SDP. SDP protokol se využívá k popisu vlastností účastníků spojení. Popis pak slouží k vyjednání parametrů spojení všech stran, které se účastní spojení (4).

SIP byl navržen v souladu s modelem Internetu. Veškerá logika je uložena v koncových zařízeních (kromě směrování SIP zpráv). Koncové uzly znají jednotlivé stavy komunikace, to zvyšuje odolnost komunikace vůči chybám. Tento koncept je rozdíl mezi SIP a veřejnou telefonní sítí. Úkolem SIP je zajistit stejnou funkcionalitu, ale jeho návrh umožňuje vyšší výkonnost a implementaci nových služeb, které nelze aplikovat na veřejné telefonní síť (15).



Obrázek č. 1: Pojmy a prvky architektury služby SIP

(Zdroj: 5)

2.3.1.1.3 SIP adresa

Každý uživatel je identifikován pomocí SIP URI (Uniform Resource Identifikator). SIP adresa funguje stejně, jako emailová adresa a obvykle bývá ve tvaru:

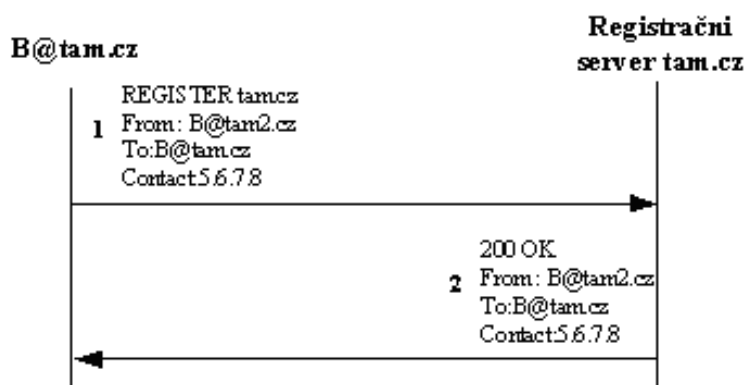
„sip:user@host“. Část „user“ může být jméno nebo telefonní číslo. V takovém případě má adresa předponu tel.: Za část „host“ se dosazuje doménové jméno nebo IP adresa. Adresa může dále obsahovat nepovinné parametry, jako například číslo portu. Běžně se používá port 5060. Výjimku pro tento port budeme dále nastavovat na firewallu (5).

2.3.1.1.4 SIP Server

SIP server odpovídá za uživatele v doméně. Může pracovat v proxy nebo redirect módu. V redirect módu sdělí informace o poloze volaného získané lokalizační službou zpět volajícímu a ten navazuje spojení přímo na novou adresu. V proxy módu pokračuje navazování spojení prostřednictvím serveru (5).

2.3.1.1.5 SIP Registrace

Úspěšná registrace se tvoří požadavkem REGISTER a odpovědí 200 OK. Adresa uvedená v položce To společně s aktuální adresou v položce Contact vytvoří časově omezený záznam v registračním serveru REGISTRAR, který je předán lokalizační službě. Tato informace umožňuje dosažení uživatele bez závislosti na poloze klienta (5).



Obrázek č. 2: Registrace

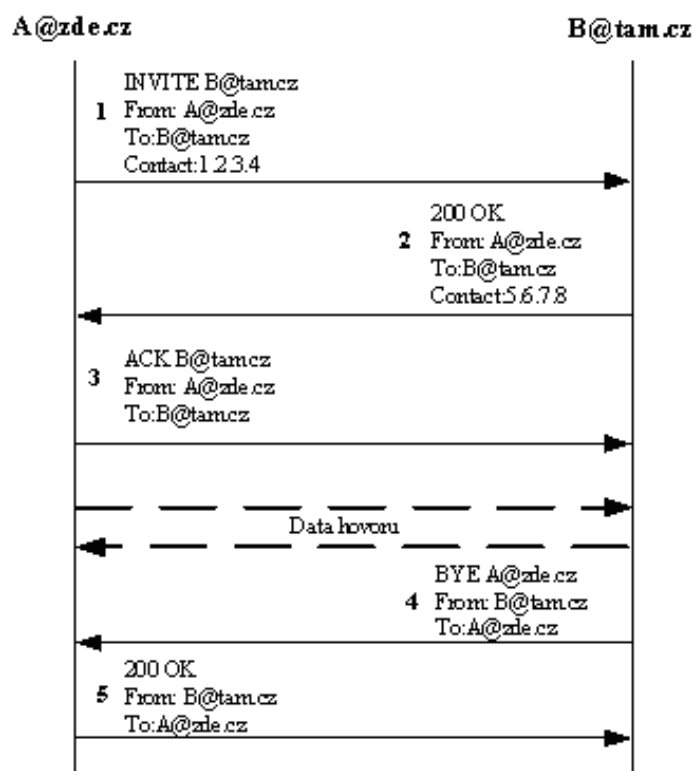
(Zdroj: 5)

2.3.1.1.6 Navázání a ukončení spojení v SIP

Procedura pro navazování spojení se nazývá „three-way handshake“. Klient A, který chce zavolat klientovi B, vyšle požadavek INVITE, který obsahuje popis nabízeného spojení. V případě, že zpráva došla, a byla pochopena správně, pošle klient B prozatímní odpověď. Tuto odpověď lze chápat jako vyzváněcí tón. Pokud klient B přijme hovor,

vyšle zpět odpověď OK s návratovou hodnotou 200. Odpověď 200 obsahuje kodeky, IP adresy a čísla portů, na kterých bude klient B očekávat data. Poslední krok je odeslání zprávy ACK klientem A klientovi B. Tímto potvrzuje přijetí odpovědi od klienta B. Proces navázání spojení je kompletní a může začít rozhovor (5).

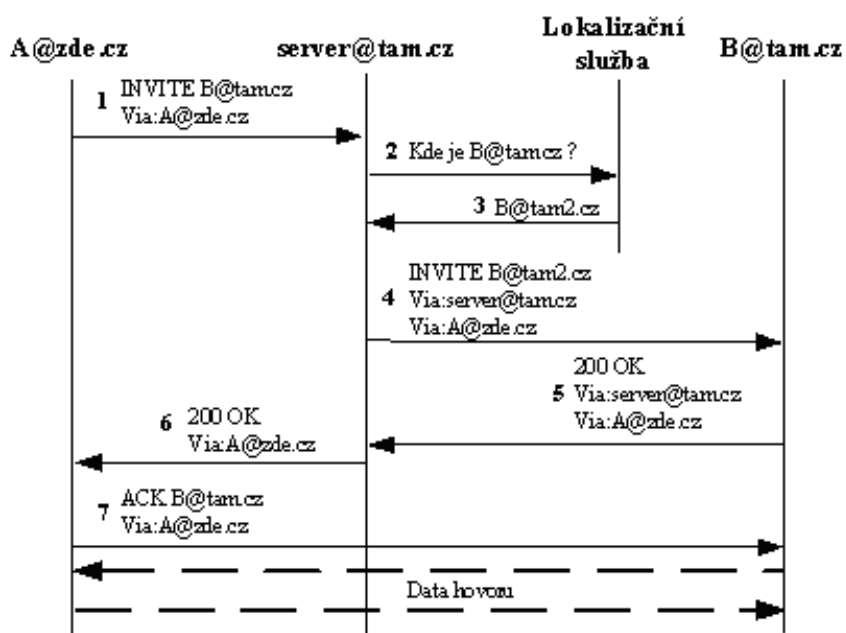
Pro ukončení hovoru musí jedna ze stran poslat protistraně požadavek BYE, který bude potvrzen odpovědí 200 OK (5) (5).



Obrázek č. 3: Navázání spojení
(Zdroj: 5)

Spojení většinou probíhá za účasti SIP serverů. Díky tomu uživatel nemusí znát aktuální adresy volaného. Volající se požadavkem INVITE dotazuje serveru SIP, ke kterému přísluší volaný. Tuto informaci získáme z adresy. Server se pokusí zjistit aktuální polohu volaného. Tuto informaci je možno zjistit pomocí dotazu do databáze kontaktů, která může být serverem spravována. Po obdržení informace o místě, kde by se klient B mohl nacházet, zašle SIP server tuto informaci zpět klientovi A a závisí na klientovi, zda naváže spojení. Nebo může server zprávu INVITE upravit a poslat směrem ke klientovi B sám (proxy mód). Přijetí hovoru 200 OK se vrací zpět na server a od něj pokračuje

k volajícímu. Pokud není použit mechanismus Record-Route putuje potvrzení ACK a všechny další zprávy mezi klienty A a B přímo (5).



Obrázek č. 4: Komunikace se SIP serverem

(Zdroj: 5)

SIP je textově orientovaný protokol a metody (příkazy) se v něm píší velkými písmeny. Tabulka níže zobrazuje základní rozdělení chybových hlášení (5).

Tabulka č. 1: Chybová hlášení protokolu SIP

(Zdroj: 5)

Číslo chyby	Proces	Popis
1xx	průběh	průběh bez problémů, ale ještě není ukončen
2xx	úspěch	krok ukončen bez problémů
3xx	přesměrování	krok probíhá, ale ještě něco očekává
4xx	chyba klienta	chybný požadavek, nemůže být serverem zpracován
5xx	chyba serveru	chyba na straně serveru
6xx	fatální chyba	fatální chyba, nelze jakkoliv zpracovat

2.3.1.1.7 Směrování SIP zpráv a mechanismus Record-Route

Základní směrovací mechanismus probíhá pomocí adresy Request-URI a položek Via. Každý prvek vysílající požadavek zaznamená svou adresu do položky Via a umístí ji před ostatní položky Via, pokud existují. Příjemce žádosti, ať už server nebo klient (UAS), by měl zkontrolovat, zda položka Via doplněná předchozím prvkem obsahuje správnou adresu IP vysílače. Pokud položka obsahuje doménové jméno nebo se adresy IP neshodují, měl by příjemce přidat parametr received, jehož hodnotou bude adresa IP, ze které požadavek přišel. Neshoda adres IP může nastat v případě, že vysílač má více rozhraní nebo je zakryt překladačem. Do adresy Request-URI je zapsán další příjemce požadavku a požadavek je odeslán. Prvek, který na požadavek odpovídá, zkopíruje všechny položky Via do odpovědi a odešle ji na adresu uvedenou v první položce Via v pořadí. Příjemce odpovědi odstraní první položku Via (svou) a odesílá odpověď na další adresu v pořadí. Takto postupně projde odpověď všemi prvky, kterými prošel požadavek (5).

Příchodem odpovědi klientovi došlo k vzájemné výměně adres v položkách Contact a je možné všechny další požadavky zasílat přímo mezi klienty bez prostřednictví serverů. Některé servery ale potřebují zůstat informovány o dalším průběhu signalizace. Takovými servery jsou například zpoplatňovací servery nebo servery zajišťující průchod firewalem atd.. V tomto případě je třeba použít mechanismus Record-Route, který zaručí, že přes vybrané servery bude procházet veškerá signalizace hovoru. Vybraný server přidá na konec položky Record-Route požadavku INVITE svoji adresu. Pokud položka neexistuje, vytvoří ji. Volaný klient zkopíruje položku Record-Route do odpovědi. Mimo to přidá na konec seznamu adresu volajícího z položky Contact a tento seznam (cestu) si uloží. Volající po příchodu odpovědi obrátí pořadí adres uvedených v položce Record-Route, vloží na konec adresu volaného z položky Contact a cestu si také uloží. Příchodem odpovědi jsou tedy oba klienti informováni o cestě, po níž budou zasílány všechny další požadavky tohoto hovoru (5).

V okamžiku odesílání nového požadavku, kterýmkoliv z klientů, je vložena první adresa z cesty do adresy Request-URI a zbytek cesty do položky Route. Via položka je vytvořena také. Příjemce požadavku vyjme první adresu seznamu v položce Route a запиše ji do adresy Request-URI. Doplní požadavek o svoji položku Via a pošle ho dál.

Takto doputuje požadavek až k cíli. Odpověď je zasílána jako předtím podle položek Via (5).

2.3.1.1.8 Bezpečnost a kvalita SIP

Většina řešení VoIP zatím nepodporuje šifrování. Proto platí totéž, co pro jiné datové přenosy. Tedy pro síťové uzly na cestě paketů mezi dvěma účastníky je odposlech velmi triviální. Aby mohlo být prováděno kryptování provozu, musí tuto operaci podporovat obě strany (resp. Všechny strany při konferenčních hovorech) (1).

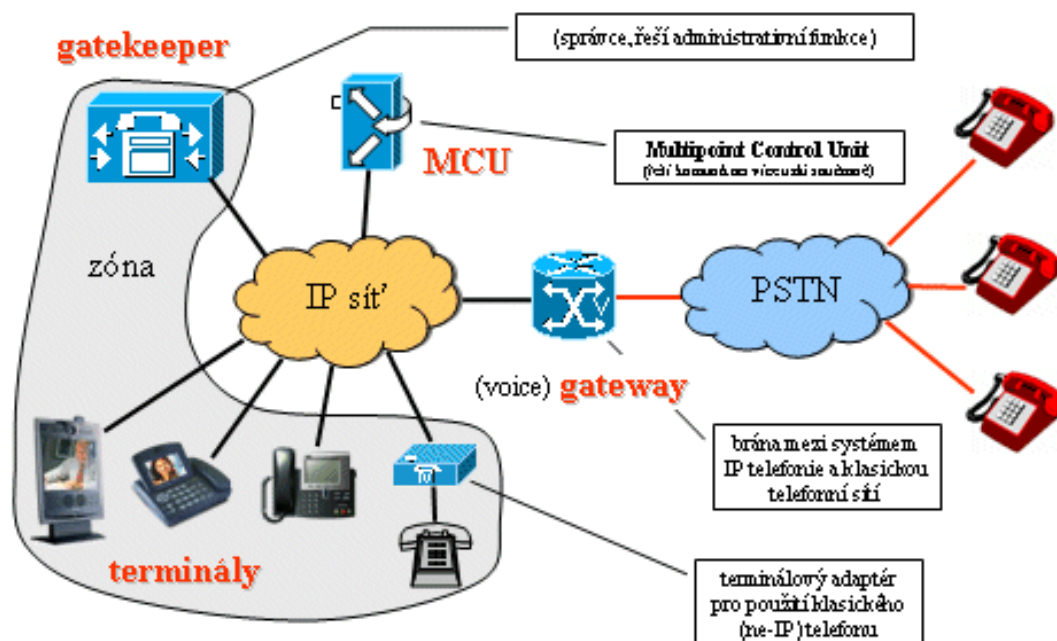
2.3.1.2 H.323

Jde o rozsáhlý a poměrně složitý standard, který kromě telefonie řeší například i videopřenosy, a zabývá se všemi aspekty, které s tím jsou spojeny. Samozřejmě pamatuje také na možnost propojení s klasickou veřejnou sítí, skrze příslušné brány (3).

2.3.1.2.1 Popis protokolu H.323

Standardy pro telefonní služby na bázi VOIP existují dva. Kromě SIP je zde i starší protkol H.323, a pochází "ze světa spojů" (od Mezinárodní telekomunikační unie, ITU.T). Jde o rozsáhlý a poměrně složitý standard, který kromě telefonie řeší například i videopřenosy, a zabývá se všemi aspekty, které s tím jsou spojeny. Samozřejmě pamatuje také na možnost propojení s klasickou veřejnou sítí, skrze příslušné brány (3).

Z pohledu uživatele jsou nejvýznamnější koncová zařízení, označovaná jako terminály. To mohou být buď specializovaná zařízení, uzpůsobená pro připojení k datové síti (tzv. IP telefony), nebo klasické (analogové) telefony, které s připojují k datové síti (IP síti) přes tzv. terminálové adaptéry). Nebo to mohou být běžné počítače, na kterých běží vhodné programy (tzv. SW telefony). Všechna tato koncová zařízení jsou sice značně inteligentní, ale přesto řadu funkcí nezvládnou samy (3).



Obrázek č. 5: Vedení hovoru v H.323

(Zdroj: 3)

Například v IP sítích jim mohou být přidělovány různé dynamické IP adresy, pod kterými jsou tyto terminály následně přístupné. Takže kdyby jim uživatel nějakého jiného terminálu chtěl volat, nevědělo by se, kam (na kterou IP adresu) směřovat slušné volání.
(3)

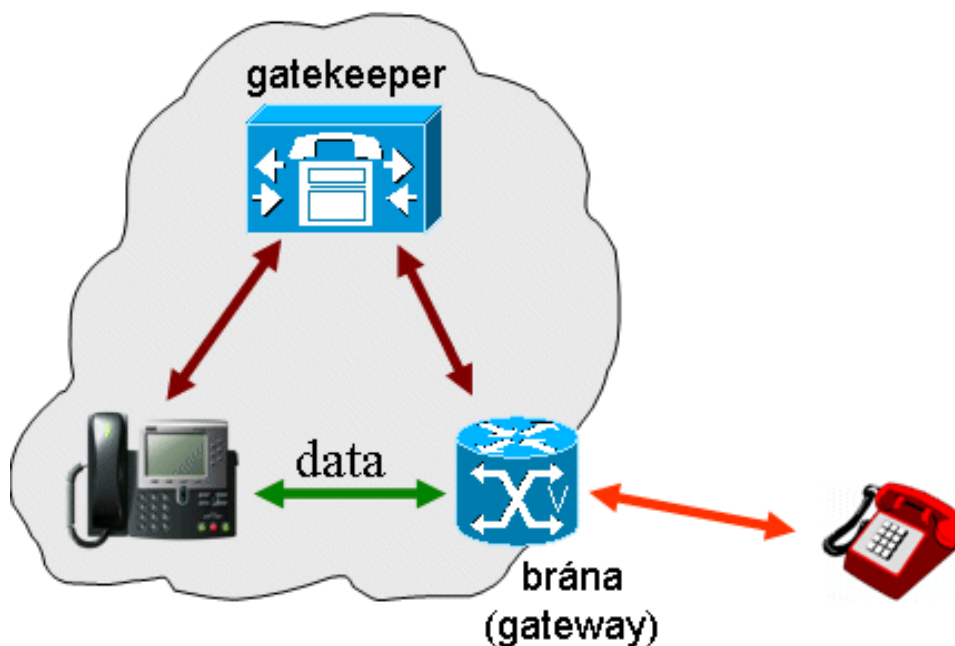
Proto pro určitou skupinu terminálů (tzv. zónu) vždy existuje jedno zařízení, v roli tzv. gatekeeperu (jakéhosi správce). Jeho funkce lze přirovnat i k funkcím telefonní ústředny - která "ví" o umístění jednotlivých terminálů, a zprostředkovává sestavování hovorů vedoucích jak od těchto terminálů, tak směřujících k nim (3).



Obrázek č. 6: Představa vedení hovoru v H.323
(Zdroj: 3)

Přesto je zde ale jeden zásadní rozdíl oproti klasické telefonní ústředně: přes ni totiž prochází i vlastní telefonní hovory. Zde, v prostředí IP telefonie, zajišťuje gatekeeper pouze "počáteční fáze" hovoru (vyhledání volaného, tzv. signalizaci a řízení hovoru), ale vlastní hovor již probíhá přímo, bez jeho účasti. Jinými slovy: průběžný přenos dat, představujících přenášený hlas v rámci hovoru, již neprochází přes gatekeeper, ale přímo mezi koncovými terminály (stylem "peer-to-peer").(3)

Standard H.323 samozřejmě pamatuje i na to, že se telefonní hovory mohou směřovat i mimo danou zónu. V takovém případě jednotlivé gatekeepery vzájemně spolupracují na sestavování hovorů. Pokud ale má hovor vést do úplně jiné telefonní sítě (například do klasické veřejné telefonní sítě, POTS, resp. PSTN), pak musí být k dispozici i vhodná hlasová brána (gateway), která zajišťuje potřebný přechod z/do jiného systému - a to jak pro potřeby vlastního hovoru ("hlasová data"), tak i pro potřeby jeho sestavení a řízení (řídící data). (3)



Obrázek č. 7: Architektura H.323
(Zdroj: 3)

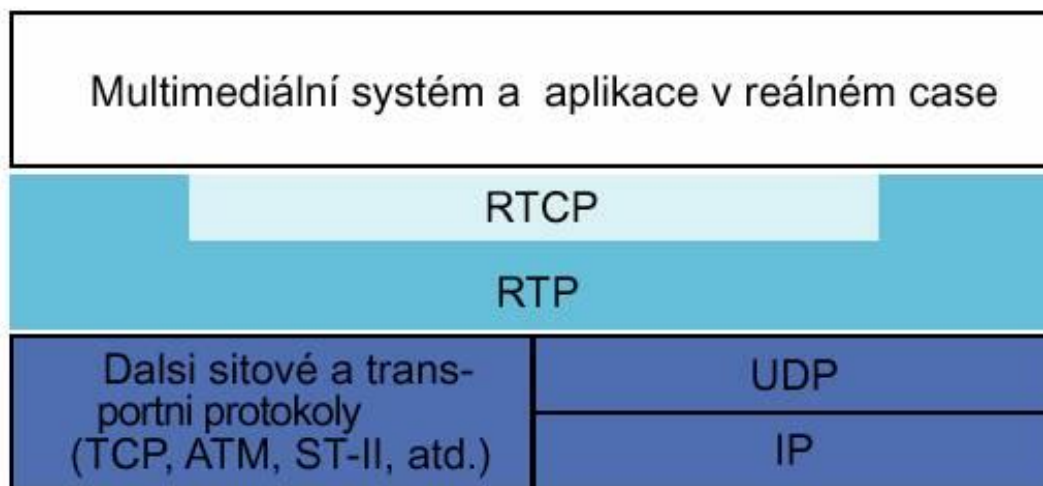
Do celkového obrázku o architektuře, kterou předpokládá standard H.323, nám schází ještě zmínka o zařízení MCU (Multipoint Control Unit). To má na starosti služby typu multicastu a broadcastu (kdy "na příjmu" je více zařízení současně). (3)

2.3.2 Vlastní přenos (RTP)

Přenos lze rozdělit na transport dat a kontrolní část. Transport dat je zde tvořen pomocí protokolu RTP (Real-Time Transport Protocol) – Protokol přenosu v reálném čase, tento protokol je definován ve standardu RFC 3550. Přenos takových dat v reálném čase vyžaduje výkonnou komunikační síť. To znamená, že musí splňovat vysoké nároky na přenosovou rychlost, zpoždění a kvalitu služeb. To je právě hlavní rozdíl mezi přenosem statických dat a přenosem dat v reálném čase. Proto protokoly užívané běžně pro přenos statických dat nevyhovují přenosům dat v reálném čase. Protokoly, které jsou vhodné pro spolehlivý přenos dat v síti s malou šířkou pásma jsou protokoly HTTP a FTP. Jsou založeny na protokolu TCP/IP. Zde platí, že pokud je paket ztracen či poškozen, dojde k jeho opětovnému vyslání. Z tohoto důvodu se pro přenos v reálném čase používají jiné protokoly než TCP. Jeden z nejčastěji používaných je protokol UDP (User Datagram Protocol). UDP je nespolehlivý protokol, který nezaručuje, aby každý vyslaný

paket byl doručen k cíli. Dokonce nezaručuje ani to, aby pakety dorazily ve správném pořadí. Internetovým standardem pro přenos dat v reálném čase je protokol RTP, který využívá zejména protokolu UDP (10).

RTP může být užíváno jak pro unicastové (pro každý cíl je vyslána ze zdroje jedna kopie) tak i pro multicastové (data jsou vyslána ze zdroje pouze jednou a je na síti, aby zajistila přenos dat do rozdílných míst) služby sítě. Multicasting je mnohem výhodnější pro přenos multimediálních dat, jakými jsou například data z videokonferenčních aplikací. RTP umožňuje před samotným zahájením přenosu identifikovat typ dat, která budou přenášena, určit pořadí paketů v jakém budou data zasílána a synchronizovat datové toky z rozdílných zdrojů. Pro datové pakety RTP není garantováno, že dorazí v pořadí, v jakém byly vysílány, ani není garantováno, že dorazí všechny. Je na adresátovi, aby rekonstruoval pořadí přijatých paketů a detekoval nepřijaté pakety pomocí informací v záhlaví paketů. Zatímco RTP neposkytuje žádný mechanismus k zajištění včasného doručení nebo k poskytnutí záruky jiné kvality služeb (QoS), jsou tyto mechanismy poskytovány kontrolním protokolem (RTCP), který umožňuje sledování kvality distribuce dat. RTCP také poskytuje kontrolní a identifikační mechanismus pro přenosy RTP (9).



Obrázek č. 8: Architektura RTP
(Zdroj: 9)

Vytvoření RTP spoje je vlastně asociace skupiny aplikací, komunikujících s RTP. Spoj je identifikován síťovou adresou a párem portů. Jeden port je určen pro přenos dat a

druhý port je určen pro RTCP data. Účastníkem je jeden stroj, hostitel nebo uživatel účastníci se spojení. Účastí ve spojení může být jednak pasivní příjem dat, vysílání dat nebo dokonce obojí, tj. příjem i vysílání. Každý rozdílný typ dat je přenášen jiným spojením. Například, pokud je při videokonferenci přenášen zvuk i obraz zároveň, je jeden spoj určen pro přenos audio dat a druhý spoj pro přenos video dat. To umožňuje účastníkovi výběr typu dat, který chce přijímat, např. pokud je někdo v místě s nízkou šířkou pásma, může zvolit pouze příjem audio dat z conference (9).

2.3.3 Kontrola přenosu (RTCP)

Kontrola přenosu dat je tvořena pomocí protokolu RTCP (Real Time Control Protocol). Protokol RTCP slouží pro přenos signalizace svázané s přenosem multimédií. Tento protokol také pracuje nad protokolem UDP. Signalizace je přenášena ve dvou typech paketů: pakety nesoucí informace o zdroji dat (Sender Report, SR) ve směru od zdroje k příjemci; pakety nesoucí informace o příjemci dat (Receiver Report, RR) ve směru od příjemce ke zdroji. Přenášeny jsou například informace o počtu zaslaných paketů (SR), ztrátovosti (RR), zpoždění (RR) atd. Dále tyto signalizační informace slouží k synchronizaci pomocí časových značek a identifikaci účastníků spojení (emailová adresa, uživatelské jméno atd.). Tato signalizace může být také poskytována dalším zájemcům za účelem vyhodnocování aktuálního stavu sítě (např. monitorovací aplikace) (11).

2.3.4 Kódování

Kvalita hovoru přes VoIP je úzce spojena s použitou metodou kódování. Meody kódování mají odlišnou hodnotu parametru MOS (Mean Opinion Score). MOS je stanoven subjektivní metodou hodnocení a může dosáhnout maximálně hodnoty 5. V tabulce 1. jsou uvedeny používané standardy kódování, názvy algoritmů, náročnosti na zpracování vyjádřené parametrem MIPS (počet miliónů instrukcí za sekundu), přenosové rychlosti kodeků a jejich kvalita ohodnocená parametrem MOS dle ACR (Absolute Category Rating) (12).

Nejpoužívanějším kodekem je jednoznačně pulzní kódová modulace PCM dle standardu ITU-T G.711. Druhým nejrozšířenějším kodekem je ITU-T G.729 s kódov

buzenou lineární predikcí CSACELP, který má obdobný MOS jako G.711, menší přenosovou rychlost a vyšší nároky na procesorový výkon. Kódování a dekodování je většinou zajišťováno na signálových procesorech DSP. Ačkoliv pohledem do tabulky se může zdát, že G.729 bude oproti G.711 osmkrát úspornější na pásmo v IP sítích, tak po vytvoření paketů a započtení jejich hlaviček si G.729 nárokuje v síti Ethernet zhruba 35 kbit/s a G.711 až 90 kbit/s (12).

Tabulka č. 2: Výkonnost kodeků používaných ve VoIP

(Zdroj: 12)

Standard	Algoritmus	MIPS	Přenosová rychlost (kbit/s)	MOS
G.711	PCM	0	64	4,1
G.726	ADPCM	1	32	3,85
G.728	LD-CELP	30	16	3,61
GSM 06.10	RPE-LTP	10	13	3,5
G.729	CS-ACELP	20	8	3,92
G.723.1	MP-MLQ	16	6,3	3,9
G.723.1	ACELP	20	5,3	3,65

U kodeku G.729 musíme počítat se zpožděním 10 ms pro každý rámec a dalších 5 ms tvoří dopředné zpoždění, a protože se většinou do jednoho RTP paketu vkládají dva rámce, tak musíme počítat se zpožděním 25 ms při kódování. Před dekodováním jsou přicházející pakety shromažďovány v mezipaměti, kde se vyrovnává proměnné zpoždění vznikající při přenosu IP sítí, toto zpoždění se označuje jako jitter, velikost mezipaměti je v násobcích časových velikostí přijímaných rámců. Zpoždění mezi odesílatelem a příjemcem a jeho vliv na kvalitu hovoru je popsán v doporučení ITU-T G.114, toto zpoždění by se mělo pohybovat do 150 ms, pokud překročí 300 ms, tak degradace kvality hovoru roste exponenciálně s narůstajícím zpožděním (12).

2.3.5 Možnosti realizace

Realizovat VoIP lze dvěma způsoby:

1. Vlastní server
2. SIP jako služba (Virtuální ústředna)

1. Vlastní server lze realizovat boxem, kde poběží pouze telefonní ústředna nebo softwarový systém na serveru, který může plnit více funkcí. Box zde může představovat Mini PC, kam se standardně instaluje operační systém Linux z důvodu nižší náročnosti na výkon. Na takovémto operačním systému pak běží telefonní ústředna. Softwarový systém, který běží na serveru zastávající více funkcí může být například Microsoft Hyper-V server. Kde Systém běží na virtuálním serveru.
2. SIP jako službu standardně nabízejí poskytovatele internetového připojení a telekomunikací. V takovém případě je systém umístěn na straně poskytovatele v cloudu. Pro toto řešení je třeba povolit na routeru určité porty, které umožní komunikovat se vzdáleným serverem.

2.3.5.1 Ústředna

Ústředna nám nabízí mnoho funkcí nastavení. Níže je jsou popsány a vysvětleny základní pojmy

- Skupiny telefonů
 - Tato funkce se používá například pro jednotlivá oddělení. Například pokud klient volá na podporu ICT oddělení, tak telefonní číslo je nastavenou pro celé toto oddělení a telefony začnou vyzvánět u všech členů tohoto oddělení.
- Rozhodování podle čísla volajícího/volaného
 - Ve větších firmách se může používat rozhodování podle čísla volajícího. Například pokud volající strana má předvolbu pro Slovensko (+421), hovor je automaticky přepojen na slovensky mluvící operátory. Tato funkce se standardně nastavuje jako pravidlo (Inbound rule) na ústředně. Při odchozích hovorech se pravidlo v anglickém znění nazývá Outbound rule.
- Interaktivní volba
 - Interaktivní volba umožňuje volající straně rozhodnout se během hovoru kam chce ubírat další kroky. Tato funkce je velmi často využívána u mobilních operátorů. Díky této funkci volající strana například sama zvolí

přesný problém, díky kterému je přepojena ke správnému oddělení a operátoři tak šetří náklady za personál, který by tuto službu musel vykonávat.

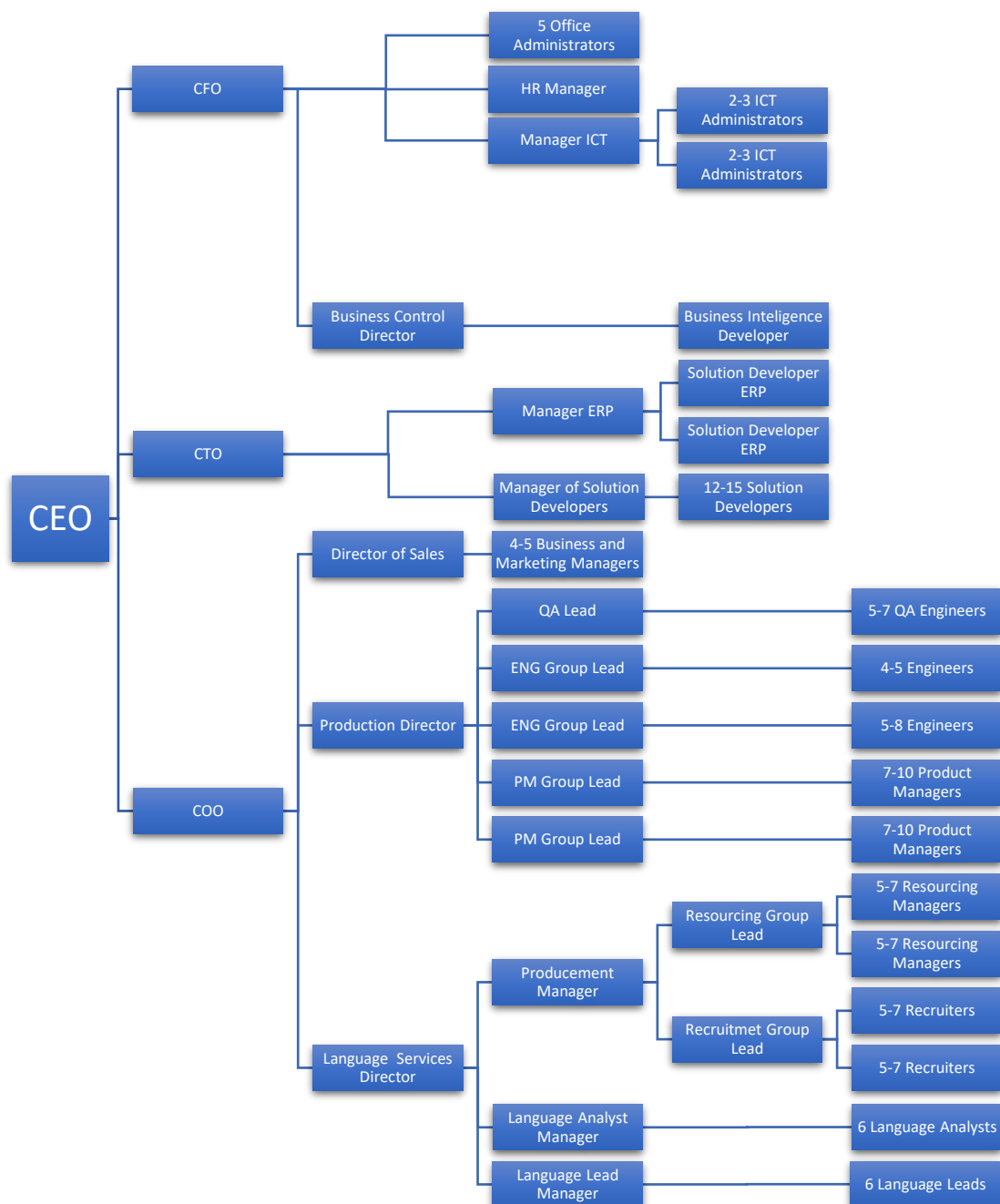
- Trunk
 - Trunkky jsou v podstatě telefonní linková vedení s přenosem přes IP prostřednictvím protokolu pro inicializaci relací. Pomocí tohoto standardního protokolu připojí poskytovatelé telekomunikačních služeb (VoIP) jeden či více kanálů k zákaznickově pobočkové ústředně. S tímto Trunkem jsou provázána telefonní čísla a mezinárodní přímé volby (DID). V mnoha případech lze do příslušného Trunku provést přenos čísel (13).

3 ANALÝZA SOUČASNÉHO STAVU

3.1 Firma

Jonckers Translation & Engineering s.r.o. je dceřiná společnost s mateřskou společností v Bruselu, která se specializuje na lokalizaci a překlady. Její brněnská pobočka, kde bude probíhat implementace VoIP má téměř 50 zaměstnanců. Po celém světě firma zaměstnává přes 300 zaměstnanců. Hlavním předmětem podnikání společnosti Jonckers je lokalizace produktů pro zákazníky zvučných jmen z oblasti IT. Náplní práce zaměstnanců většiny profesí je být v kontaktu se zákazníkem, dodavateli, případně s kolegy z různých poboček po celém světě. Z tohoto důvodu zaměstnanci využívají několik komunikačních kanálů, i pro případ, že by některý z nich přestal nečekaně fungovat. Dalším velmi důležitým důvodem, který zde telefony představují je uzavírání smluv s překladateli a s překladatelskými agenturami. Tento proces mají ve firmě na starosti recruiteři a jejich funkce ve firmě je velmi důležitá. Při vykonávání tohoto procesu jsou telefony nutností.

Vzhledem k tomu, že společnost se snaží udržet dobré vztahy se zákazníky, musí mnoho zaměstnanců cestovat do zahraničí na schůzky. Proto se stává, že zaměstnancům v kanceláři vyzvání telefony, ale nemá je kdo zvednout. Všichni tyto cestovatelé by uvítali možnost přesměrování hovorů na osobní mobilní telefony. Nezvedání telefonů a nemožnost se dovolat konkrétním osobám působí špatným dojmem.



Obrázek č. 9: Organizační struktura firmy
(Zdroj: Interní dokumenty společnosti Jonckers)

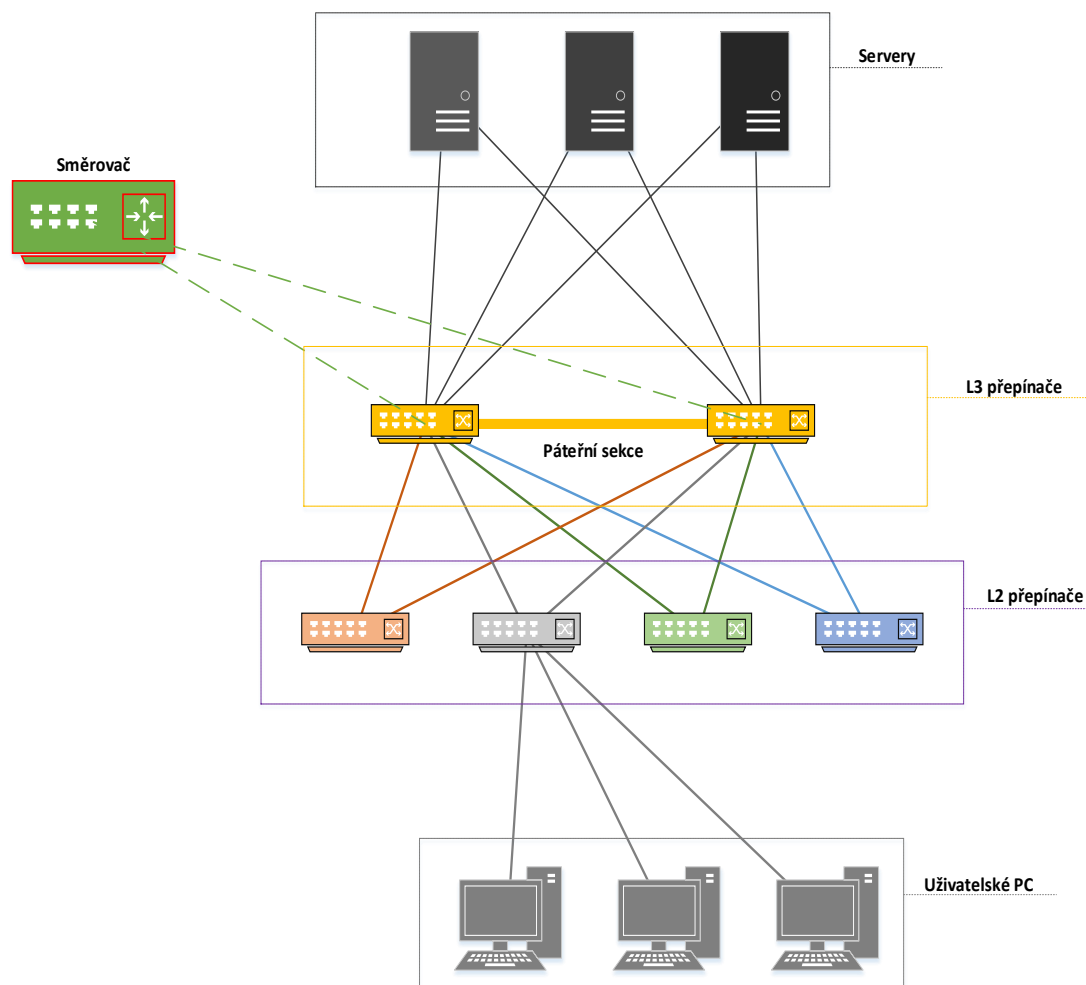
3.2 Počítačová síť

Tato kapitola se bude věnovat stavu kabeláže, aktivním prvkům a serverům, které se ve firmě používají.

3.2.1 Aktivní prvky

Společnost Jonckers používá výhradně síťové prvky od výrobce Cisco Meraki. Nákup prvků od tohoto výrobce umožňuje ovládání všech síťových prvků vzdáleně. Díky tomu mohou ICT administrátoři z celého světa měnit nastavení na všech síťových prvcích vzdáleně. Jediná výjimka mezi síťovými prvky jsou routery (řešení s firewallem). Neboť řešení od společnosti Cisco představovalo pro společnost Jonckers příliš vysoké náklady, a proto bylo zvoleno řešení od výrobce Peplink. V případě Cisco routerů nebyl největší problém jen pořizovací cena, ale i následné náklady spojené s prodloužením licencí. Navzdory této výjimce, síť není přehnaně fragmentovaná a její řízení tedy nepředstavuje velké problém.

Uživatelské stanice jsou napojeny na L2 switche Cisco Meraki MS220-48, kde každý switch má 48 portů. Tyto switche mohou pracovat s rychlostí až 1Gbps. Bohužel nepodporují PoE (Power of Ethernet) a proto zařízení, která vyžadují PoE (kamery, Access Pointy atd.) je nutno napájet z jiných zdrojů. L2 switche jsou dále zapojeny do L3 switchů Cisco Meraki MS250-24, Tyto L3 switche jsou umístěné na ve stejné serverovně ve dvou skříních. Propojení, neboli páteřní sekce, je zde tvořeno optickými kabelem mezi těmito přepínači. Díky těmto L3 switchům je síť rozdělena do několika VLAN (virtuálních sítí). L3 switche jsou dále zapojeny do routeru Peplink Balance 380, který také zajišťuje funkci firewallu. Toto zapojení je popsáno níže ve schématu.

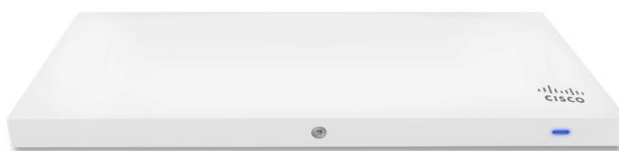


Obrázek č. 10: Schéma aktivních prvků počítačové sítě
(Zdroj: Vlastní zpracování)

Směrovač je dále připojen k internetu pomocí dvou přípojek. Primární připojení je tvořeno optickým připojením. Zde je rychlost download/upload garantována na 200 Mbit/s. SLA je v případě tohoto připojení stanoveno na 99,8 %. Druhá přípojka je realizována připojením na rádiový vysílač od společnosti Netbox. SLA je zde dohodnuto na 99,7 %. Tato kombinace byla zvolena z důvodu minimalizace výpadku připojení, neboť v případě výpadků téměř nikdo ze zaměstnanců nemůže efektivně pracovat.

Ve firemním prostředí lze rovněž zachytit bezdrátový signál pracující na 2,4 GHz a 5 GHz vycházející z access pointů. V kanceláři, kde analýza probíhá, můžeme nalézt 3 tyto prvky, které jsou rozmístěny takovým způsobem, aby v každé části kanceláři byl velmi silný signál. Přičemž se kanceláře rozprostírají na jednom patře budovy o užitkové ploše téměř 500 m². Při analyzování těchto prvků jsem došel k zajímavému zjištění

ohledně signálu. Silný signál, který vychází z těchto malých zařízení, není šířen žádnou externí anténou. Vzhled použitých access pointů je níže zobrazen na obrázku.



Obrázek č. 11: Používané access pointy
(Zdroj: Obchodní materiály společnosti Cisco Meraki)

3.2.2 Kabeláž

K této síti není možné dohledat žádná dokumentace. Síť v těchto kancelářských prostorách byla pravděpodobně vytvářena ve dvou fázích, neboť část prvků je jiného typu. Mezi tyto rozdílné prvky patří zásuvky, kabely a patch panely. Níže vypsane informace byly získány analýzou jednotlivých segmentů sítě.

3.2.2.1 Horizontální sekce

V kancelářích lze nalézt 192 síťových zásuvek. Síťových zásuvek je tedy dostatečné množství. Ovšem všechny tyto porty nejsou zapojeny do přepínačů (switchů). Tento fakt je dán nedostatkem přepínačů. Ovšem uživatelé nejsou schopni využívat ani zásuvky při současném stavu. Nákup nových přepínačů by tedy představoval zbytečné náklady.

3.2.2.2 Pracovní sekce

Rozvody mezi ústřednou a telefony jsou řešeny pomocí síťových kabelů Cat. 3 zakončených konektorem RJ11. Uživatelé po kabelech stále přejíždějí kolečkovými židlemi. Kabely jsou tedy ve špatném stavu. V mnoha případech kabely nemají ani vnější

izolaci. Spoj mezi počítači a síťovou zásuvkou je tvořen klasickými kabely Cat. 5 a Cat. 6 UTP zakončený koncovkou RJ45. V mnoha případech jsou kabely vedeny žlaby v podlaze. Zde je větší náchylnost proti poškození například při vylití vody do žlabu.

3.2.3 Serverová infrastruktura

Firma využívá mnoho serverů k mnoha účelům. Předně všichni uživatelé by si měli ukládat všechna důležitá data na server hned ze tří důvodů. Primární důvod ukládání je samozřejmě bezpečnost. Na serveru jsou disk uloženy v RAID poli, které mimo jiné využívá zrcadlení disků a pokud tedy jeden z disků přestane fungovat, data nejsou ztracena. Dalším důvodem je ochrana proti odcizení dat. Data na serveru jsou šifrována, tento server je uzavřen v monitorované místnosti, kam mají přístup pouze pověřené osoby. Celá budova, kde jsou kanceláře společnosti Jonckers umístěny, je navíc zabezpečena bezpečnostní agenturou 24 hodin denně. Posledním důvodem je dostupnost dat. Uživatelé se z domu připojují přes VPN (Virtual Private Network) a v práci si například nedopatřením vypnou počítač a nemají tedy přístup k datům uloženým na lokálním počítači. Server běží bez vypnutí i několik let, pokud nepočítáme chvilkové vypnutí z důvodu údržby.

V serverovně firmy Jonckers se nachází celkem 8 serverů. Výhradním dodavatelem serverových řešení je firma Dell. Tři servery fungují jako datová úložiště, jeden server funguje jako FTP server pro rychlejší přenos dat, další server funguje jako Hyper-V server v demilitarizované zóně (DMZ). Zde běží aplikace, které jsou viditelné „veřejně“ a využívají je externisté, kteří nemají přístup do vnitřní sítě. Poslední tři servery fungují jako Hyper-V servery ve vnitřní síti, kde je velké množství operačních systémů. Můžeme zde nalézt například docházkový systém, kamerový systém, terminálový server, server spravující Active Directory, VPN server a mnoho dalších. Toto řešení virtualizace OS má mimo jiné jednu hlavní výhodu oproti fyzickému řešení, kde na jednom počítači běží jeden operační systém. Virtuální OS lze velmi snadno přenést na jiný server. Pokud tedy nějaký z fyzických serverů přestane fungovat nebo je třeba ho dočasně použít pro jiné účely, lze jednoduše překopírovat virtuální disk (soubor s koncovkou .vhd) na jiný server nebo lze v Hyper-V Manageru vyexportovat OS na jiné zařízení.

Zapojení serverů do sítě je zde tvořeno jinak než u uživatelských počítačů. Vzhledem k tomu, že síť je rozdělena na virtuální síť (VLAN) pro uživatele a servery, jsou servery zapojeny přímo do L3 přepínačů. Na těchto přepínačích jsou pak jednotlivé porty nastaveny pro danou VLANu a podle konkrétních požadavků na server (například NIC Teaming). Více informací lze naléznout v logickém schématu sítě výše. Řešení bylo zvoleno z mnoha důvodů od bezpečnosti po snížení broadcastů v síti.

Všechny servery fungující jako datová úložiště jsou do sítě zapojeny specifitějším způsobem. Síťové zapojení do přepínačů zde není tvořeno pouze jedním fyzickým připojením, ale kombinací několika síťových kabelů, které logicky působí jako jeden. Díky tomu je dosaženo vyšších přenosových rychlostí. Zároveň je zajištěna vyšší garance dostupnosti v případě výpadků jednoho ze síťových kabelů, neboť server a switch poznají tuto změnu zapojení a přestanou daný port využívat.

3.2.4 Bezpečnost sítě

Společnost Jonckers používá velké množství bezpečnostních prvků, které mají za úkol chránit firemní síť a infrastrukturu. Mezi základní prvky patří samozřejmě router, který funguje rovněž jako firewall. Používaný router v analyzované společnosti je Peplink Balance 380.

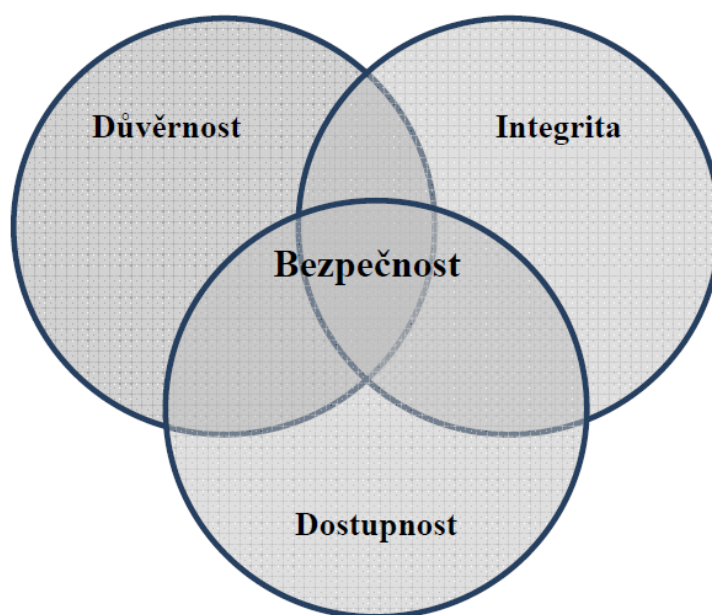


Obrázek č. 12: Peplink Balance 380

(Zdroj: obchodní materiály společnosti FrontierUS, distributora výrobků Peplink)

Toto zařízení funguje jako brána, která filtruje všechna nevyžádaná data. Pro tento účel používá router tabulku výjimek, kde lze nastavit jaké porty budou povoleny pro komunikaci. Případně jaké servery na těchto portech mohou komunikovat. Tyto routery jsou využívány ve všech kancelářích společnosti Jonckers. Díky plošnému použití těchto síťových prvků jsou tyto routery mezi sebou připojeny pomocí VPN. Díky tomu všichni

uživatelé mohou mapovat vzdálené síťové jednotky jako lokální. Použití VPN lze považovat za správné řešení z pohledu bezpečnosti. Nebýt tohoto propojení, uživatelé by si posílali data po veřejné síti bez jakéhokoliv šifrování a byla by zde větší pravděpodobnost bezpečnostního incidentu. Jedná se tedy o možnost příliš velké dostupnosti na úkor bezpečnosti. Tento vztah je zobrazen níže na obrázku.



Obrázek č. 13: Základní atributy informační bezpečnosti
(Zdroj: Studijní materiály Ing. Viktora Ondráka, Ph.D.)

Na router jsou dále zapojeny Cisco Meraki switche. K ovládací konzoli těchto prvků se lze připojit jednoduše přes webový portál bez nutnosti připojení v LAN. Toto lze chápat jako bezpečnostní hrozbu, neboť uživatel (zde ICT administrátor) může z jakéhokoliv zařízení pomocí pár kroků shodit celou síť. Navíc pokud se připojí k této webové konzoli z veřejné sítě, může být sledován provoz takového administrátora a záškodník se pak snadno dostane k nástroji, který může úplně vyřadit z provozu všechny sítě společnosti Jonckers.

Bezdrátová síť je zde rozdělena na dvě sítě. První síť je veřejná. Lze ji nalézt pod názvem „JTE-Visitors“ a je určena pro návštěvy, které by ovšem neměly mít přístup do vnitřní sítě. Druhá síť je skrytá a její SSID je „JTE-LAN“. Jedná se o síť určenou pro zaměstnance. Toto rozdělení bezdrátové sítě bylo zavedeno z důvodu bezpečnosti. Ovšem ve společnosti Jonckers stále platí nepsané pravidlo využívat bezdrátové sítě jen

minimálně, neboť bezpečnost bezdrátových sítí nelze zajistit tak dobře, jako v případě fyzického zapojení.

Síť společnosti Jonckers rovněž využívá rozdělení pomocí VLAN z důvodu zvýšení bezpečnosti a snížení broadcastové domény. Jako další silnou bezpečností stránku lze označit zabezpečení vstupu do firmy a následně do serverovny, kde jsou uložena všechna firemní data. Společnost Jonckers se nachází v areálu, který je střežen 24 hodin denně bezpečnostní agenturou. Vstup do prostor analyzované společnosti je možný pouze s návštěvnickou kartou. Vstupní dveře společně se serverovnou jsou monitorovány kamerovým systémem, který rovněž spadá pod správu ICT oddělení. Do serverovny má přístup pouze lokální administrátor a jednatel. Nikdo další do serverovny nesmí vstoupit bez povolení. Kombinace těchto faktorů zajišťuje vysokou bezpečnost proti fyzickému poškození všech zařízení v serverovně.

Společnost Jonckers se brání proti všem druhům počítačových virů, červů apod. pomocí antivirového řešení od společnosti Kaspersky. Tento antivirus má nainstalovanou konzoli na virtuálním serveru, ze které řídí všechny antivirové aplikace nainstalované na uživatelských počítačích. Uživatelé jsou dále chráněni pomocí VPN, v případě, že potřebují pracovat z domu. Díky VPN mají zabezpečený přístup do sítě, byť může být omezena rychlost připojení a přístup na některé webovské stránky, neboť se VPN řídí firemními pravidly a restrikcemi. Dalším zabezpečením pro uživatele představuje silné heslo, které musí splňovat požadavky minimálně osmi znaků, alespoň jedno malé a jedno velké písmeno, jedno číslo a jeden cizí znak. Toto heslo si uživatelé musí měnit každé tři měsíce. Toto zabezpečení může být kontraproduktivní, neboť po provedení analýzy v jedné z kanceláří bylo zjištěno, že část uživatelů si schovává své heslo napsané na papírek pod klávesnice.

Po dokončení analýzy považují za největší hrozbu špatnou komunikaci mezi ICT a HR (personálním) oddělením. Neboť HR oddělení píše tickety na Helpdesk ohledně zaměstnanců kančících ve firmě i s několika týdenním zpožděním. V takovém případě uživatel už nemá žádné vztahy se společností, ovšem stále má přístupy ve společnosti, protože ICT oddělení neví o jeho odchodu. Tuto bezpečnostní hrozbu lze označit klasifikačním stupněm č. 4 dle klasifikačního schématu aktiv. Hrozba plyne z možnosti,

že zhrzený uživatel může zneužít přístupů nebo firemních informací o strategii, utajených projektech, informace o klientech a poskytnout je konkurenční společnosti.

Tabulka č. 3: Klasifikační schéma aktiv

(Zdroj: studijní materiály Ing. Viktora Ondráka, Ph.D.)

Klasifikační stupeň	Klasifikační kritérium
1	Žádný dopad na organizaci
2	Zanedbatelný dopad na organizaci
3	Potíže či finanční ztráty
4	Vážné potíže či podstatné finanční ztráty
5	Existenční potíže organizace

3.3 Stav telefonie

Telefonie je využívána jen minimálně. Uživatelé se snaží využívat Skype for Business, který je součástí licence Microsoft O365, kterou má každý uživatel k dispozici. Tato aplikace poskytuje uživateli mnoho doplňujících služeb, např. sdílení obrazovky, posílání souborů, konferenční služby, záznam hovoru atd. Ne všichni zákazníci či partneři disponují tímto systémem nebo stabilní internetovou linkou a je třeba jim telefonovat na mobilní telefony.

3.3.1 PBX (telefonní ústředna)

Telefonní ústředna je uložena v serverovně. Jedná se o analogovou ústřednu, ke které se není možné vzdáleně připojit přes počítač (Remote Desktop Connection), což způsobuje horší podmínky pro administraci. Ústředna je napojena ven pomocí jedné analogové linky na poskytovatele UPC Česká republika, s.r.o. Měsíční náklady zde tvoří 1500 Kč. Vzhledem k tomu, že společnost UPC, která je poskytovatelem tohoto analogového připojení je rovněž primárním poskytovatelem internetového připojení (přes optický kabel), lze předpokládat menší zpoždění při využití trunku od tohoto poskytovatele.

3.3.2 Pevné telefony

Pevné telefony pozbyly funkce ve chvíli, kdy se zaměstnanci přesunuli k jinému stolu. Neboť u jiného stolu byl přednastavený telefon s jiným číslem. Vzhledem k tomu, že ve firmě delší dobu nebyla dostupná žádná ICT podpora, nastavení telefonů nebylo změněno pro dané uživatele a zaměstnanci přestali telefony využívat.

3.3.3 Číselný plán linek

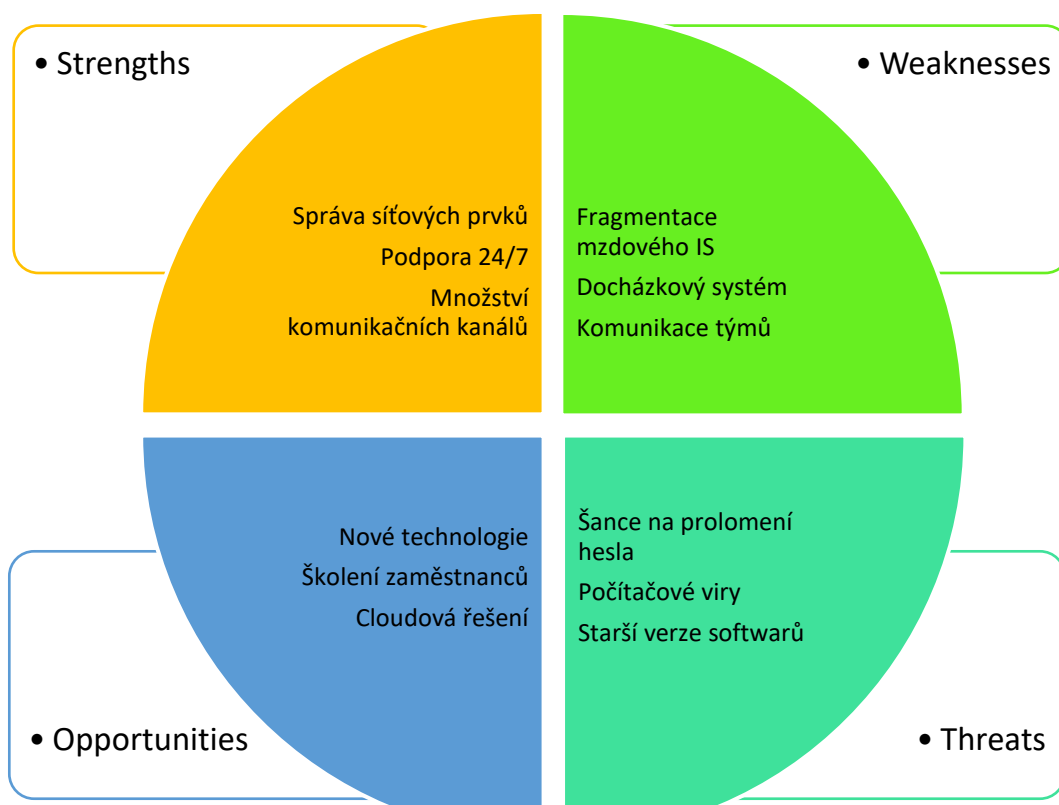
Každému zaměstnanci bylo při nástupu přiděleno telefonní číslo, které musí uvádět v podpisu emailu a na vizitkách. Všechna čísla tedy musí zůstat u zaměstnanců stejná i při jakýchkoliv změnách. Přidělování telefonních čísel probíhalo nahodile, tedy jasná struktura u číselného plánu linek není zavedena. Jako možný způsob přechodu na strukturovaný plán se jeví postupná obměna čísel díky fluktuaci zaměstnanců. Neboť ve společnosti, kde analýza probíhá, většina zaměstnanců nepracuje déle než 5 let.

3.4 Požadavky ze strany zadavatele

Zadavatelem implementace IP telefonie je management společnosti. Hlavními požadavky jsou nižší náklady, stejná kvalita přenosu hlasu jako u pevné linky, snazší administrace dostupná vzdáleně pro administrátory z různých poboček. Nižší náklady zde tvoří největší prioritu, neboť vedení firmy se snaží minimalizovat provozní náklady. Dalším požadavkem je větší množství současných hovorů.

3.5 SWOT analýza

SWOT analýza popsaná dále se zaměřuje na stav ICT ve společnosti. Analýza primárně zohledňuje stav bezpečnosti. Kromě primárního faktoru se zaměřuje na služby nabízené oddělením ICT, které zajišťuje podporu pro všechny systémy. Mezi tyto systémy patří docházkový systém, kamerový systém, antivirová ochrana a mnoho dalších.



Obrázek č. 14: SWOT analýza
(Zdroj: Vlastní zpracování)

3.6 Shrnutí analýzy

3.6.1 Negativní faktory

- K dispozici je jen jedna analogová linka, a proto není možno provozovat více souběžných hovorů.
- Zastaralá analogová ústředna neumožňuje seskupování příchozích hovorů do skupin, neposkytuje informace o volajícím na displeji telefonů uživatelů, není

možná správa integrovaného telefonního seznamu, přesun linky za zaměstnancem je velmi komplikovaný.

- Chybějící možnosti vyhodnocování proběhlých nebo probíhajících telefonátů neumožňuje společnosti efektivní analýzu potřeb telefonie.
- Připojení analogových telefonů je z pohledu fyzické infrastruktury nesystémové.

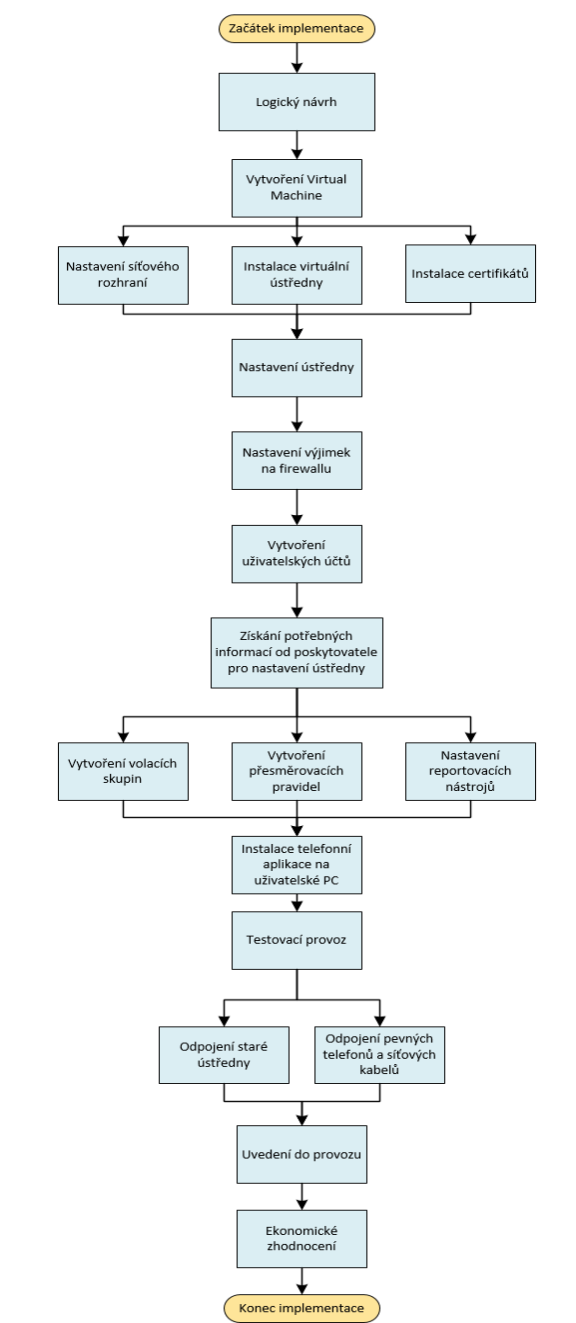
Všechny tyto faktory způsobily nízké využití současné telefonie ve společnosti a její nahrazení nesystémovým řešením kombinace mobilních telefonů a služby Skype for Business (součástí licencí Office365), které není možno jednotně vyhodnocovat.

3.6.2 Pozitivní faktory

- Dobře fungující virtualizace v oblasti serverů ve společnosti poskytuje široké možnosti hostovat na vlastní platformě virtuální řešení ústředny.
- Současný poskytovatel připojení se jeví jako bezproblémový.

4 VLASTNÍ NÁVRHY ŘEŠENÍ

Jednotlivé kroky a jejich návaznosti implementace VoIP systému jsou popsány ve vývojovém diagramu níže. Implementace zahrnuje i odstranění předešlého řešení, které bude nahrazeno novým systémem. Z původního systému se zachovávají pouze telefonní čísla, která budou později přidělena k SIP Trunku na straně poskytovatele.



Obrázek č. 15: Vývojový diagram implementace
(Zdroj: Vlastní zpracování)

4.1 Logický návrh

Logický návrh popsaný v této kapitole stanovuje základní parametry systému, který se dále bude implementovat.

4.1.1 Návrh požadavků na nový komunikační systém

Pro systém navrhuji stejný počet linek, jako dosavadní pevné linky, tedy 100 linek. Zároveň by měl systém umožnit až 16 současných hovorů. Od systému se očekává, že bude snadno ovladatelný a srozumitelný, celý v anglickém jazyce a měl by poskytovat podrobné statistiky telefonování v reálném čase, tj. umět odpovědět na otázky kdo, jak dlouho a za kolik peněz telefonoval. Mezi vlastnosti systému by rovněž mělo patřit vytváření volacích skupin, model provoleb v rámci interní struktury a směrování hovorů. Systém by měl komunikovat pomocí trunku. Jednou z dalších funkcí musí být snadná a rychlá obnova systému ze záloh.

Navrhuji koncové zařízení (klienta) řešit pomocí aplikace, která bude plně zastupovat funkce IP telefonu. Tento návrh plyne z doposud hojně využívané aplikace Skype for Business od poskytovatele Microsoft. Při využívání této aplikace uživatelé často používají headsety (sluchátka s mikrofonom), které lze využít i pro volání po IP síti. Tím bude dosaženo úspory velkých nákladů, které by jinak byly vynaloženy na nákup fyzických IP telefonů.

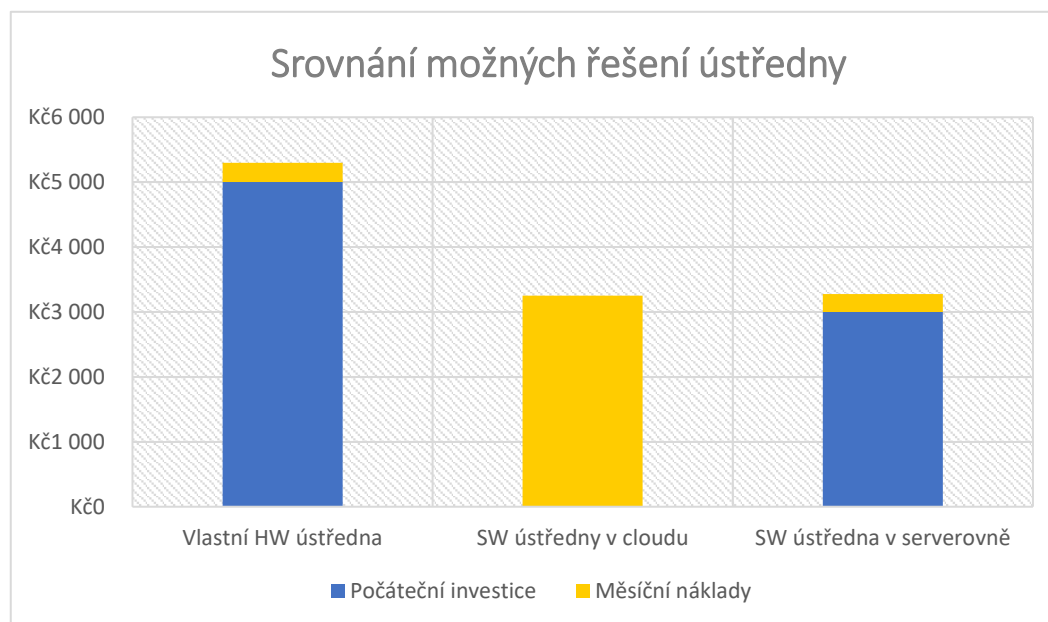
4.1.2 Návrh signalizace

Navrhuji, aby systém využíval SIP pro komunikaci, neboť oproti H.323 méně zatěžuje síť. Další výhodou SIP, kterou systém dovoluje využívat je posílání instantních zpráv neboli „chatování“, které v první fázi nebude implementováno.

4.1.3 Umístění a způsob realizace ústředny

Z důvodu vysoké ceny cloudového řešení, kterou si poskytovatel účtuje v rámci kompletního balíku služeb, doporučuji ústřednu umístit ve firmě a ušetřit tím značnou část finančních prostředků. Díky výkonným virtualizačním serverům, které má společnost Jonckers k dispozici, doporučuji řešit ústřednu pomocí softwaru běžícím ve

virtuálním prostředí. Toto řešení usnadňuje i možnost záloh, neboť se ústředna může snadno přemigrovat na jiný virtualizační server. Technicky je na toto interní řešení společnost Jonckers již připravena a nevyžaduje žádné další investice.



Graf č. 1: Srovnání možných řešení ústředny
(Zdroj: Vlastní zpracování)

V grafu výše vidíme srovnání počátečních investic a měsíčních nákladů. Měsíční náklady v sobě zahrnují i náklady na jednu hodinu práce kvalifikovaného administrátora, jehož hodinová sazba činí 250 Kč. Další položkou měsíčních nákladů pro provoz vlastní hardwarové ústředny nebo softwarové ústředny na serveru je spotřebované energie těmito systémy. Může se zdát, že spotřeba energie serveru je větší než řešení hardwarové ústředny, na serveru však běží téměř 30 virtuálních zařízení, a proto spotřebu energie (v provozu cca 300 W výkon) je nutno dělit počtem virtuálních počítačů. Stejným způsobem byla vypočtena i počáteční investice tohoto řešení. Přesněji, pořizovací cena serveru činila téměř 90 000 Kč, tudíž pořizovací cena řešení je $90\,000 \div 30 = 3\,000$ Kč. V případě softwarové ústředny v cloudu jsou zde náklady tvořeny z práce administrátora a ceny nájemného za cloud.

4.1.4 Výběr systému

Pro implementaci navrhuji systém 3CX, který splňuje všechny požadavky, které byly požadovány při zadání řešení. Tento systém navrhuji i díky tomu, že administrátoři

společnosti Jonckers nemají příliš velké zkušenosti s Linuxovým řešením, které nabízí konkurenční systém Asterisk. Kombinace pořizovací ceny (7 800+ Kč) a dalších nákladů na školení administrátorů (30 129 Kč/osoba) systému Asterisk vede k preferování systému 3CX. Pro společnost Jonckers je rovněž výhoda, že poskytovatel internetové přípojky je zároveň poskytovatelem tohoto systému. Díky tomu lze od poskytovatele očekávat minimální odezvu a již dobře známou technickou podporu.

4.1.5 Umístění ústředny

Ústřednu navrhuji umístit na jeden z virtuálních serverů v zemi, kde bude systém implementován (kvůli nízké odezvě), přičemž minimální požadavky na virtuální prostředí, kde ústředna poběží jsou následující: 2 048 MB operační paměti, jednojádrový procesor, 200 GB virtuální disk, síťové rozhraní pro připojení do lokální sítě. Jako operační prostředí navrhuji Windows Server 2008 nebo novější.

4.1.6 Číselný plán linek

Číselný plán linek se musí řídit podle předchozího řešení. Přesněji řečeno, uživatelé musí mít stejné číslo, jaké měli při starém řešení pomocí pevných linek. V případě pevných linek byl společnosti přidělen rozsah čísel 532 194 300 – 532 194 399.

4.1.7 Systém provoleb

Pro urgentní spojení s příslušným oddělením by měl být vytvořen systém provoleb pro ICT a Office Administration (recepční) oddělení. Jedná se o oddělení, od kterých může být požadována rychlá akce.

Tabulka č. 4: Návrh směrování provoleb
(Zdroj: Vlastní zpracování)

Koncové dvojčíslí	Bude směrováno na:
00	Interactive Voice Response (neboli „plechová huba“)
01	Spojovatelka (recepční)
02	ICT Helpdesk

03-09	Prostor pro pozdější vytváření volacích skupin
10-99	Konkrétní linky – uživatelé

4.1.8 Návrh logiky směrování a volacích skupin

Ve společnosti musí být vytvořeny alespoň dvě základní volací skupiny pro oddělení ICT a Office Administration. Těmto volacím skupinám a všem ostatním uživatelům je nutno nastavit směrovací pravidlo, díky kterému se jim později bude moci dovolat. Pokud například nebude volání na linku přijato do 20 sekund, navrhuji přesměrovat hovor na volací skupinu (např. spojovatelka nebo volací skupina oddělení, do které uživatel linky spadá), pokud hovor nebude dále přijat do 60 sekund, bude přesměrován na hlasovou schránku původní linky. V případě specializovaných pracovních pozic může být vyžadováno individuální nastavení směrování. Například pro jednatele navrhuji nastavit směrování hovoru po 15 sekundách na jeho osobní mobilní telefon.

4.1.9 Hlasové schránky

Navrhuji nastavit všem uživatelům automatické ukládání hlasových vzkazů ve formátu MP3. V případě nového hlasového vzkazu bude uživatel informován emailem, který bude automaticky vygenerován po uložení vzkazu.

4.2 Vytvoření Virtual Machine

Společnost má několik serverů určených pro virtuální stroje. Tyto servery jsou rozmístěny po všech pobočkách společnosti Jonckers ve světě. Pro tento účel je nejvhodnější řešení využít server umístěný v kanceláři v Brně. Docílíme tím minimální odezvy při komunikaci s VM, neboť uživatelé budou alokováni ve stejné kanceláři a poskytovatel trunku je zde zároveň primárním poskytovatelem připojení k internetu. Vzhledem k tomu, že virtuální ústředna není náročná na výpočetní výkon, můžeme VM přidělit jeden virtuální procesor a alespoň 2 048 MB operační paměti. Operační paměť lze nastavit dynamickým přidělováním podle vytížení. V případě diskového úložiště je třeba vytvořit větší virtuální disk, neboť ústředna si bude nahrávat všechny hlasové

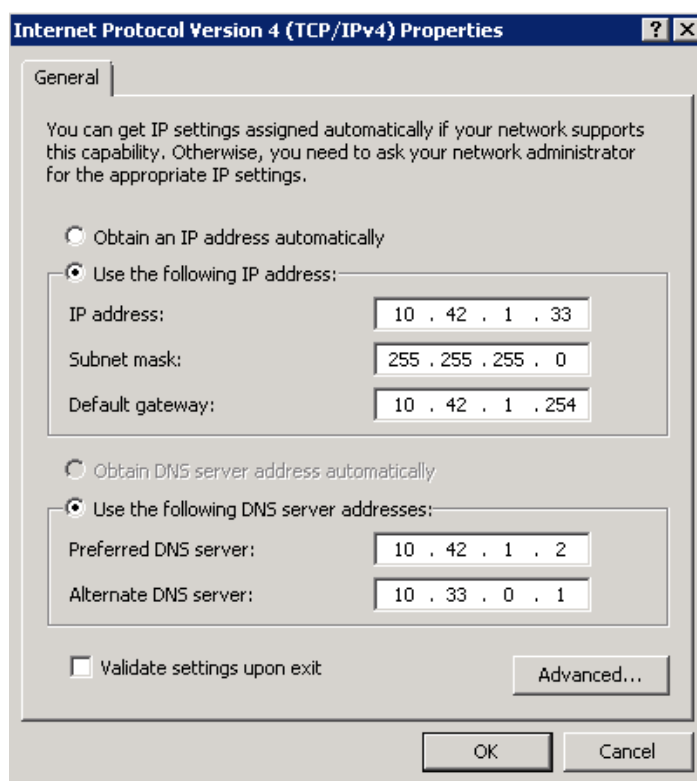
zprávy, záznamy o aktivitách apod. Podrobnější popis vytvoření VM je přiložen v příloze č. 2.

4.3 Instalace ústředny

Instalace ústředny je dále popsána ve třech částech. Aby s ústřednou šlo dále pracovat, je nutné nastavit každou z těchto tří částí.

4.3.1 Nastavení síťového rozhraní

Pro nastavení síťového rozhraní je nutné přidělit VM do správné VLAN. Pro tuto změnu je nejlepší vypnout VM. Po nastavení příslušné hodnoty změny uložíme a VM spustíme. Dalším krokem je nastavení statické IP adresy. Tento krok je nutný, aby všechna zařízení a aplikace, která později budou chtít komunikovat s ústřednou našla tuto ústřednou pod stejnou adresou.



Obrázek č. 16: Síťové nastavení ústředny
(Zdroj: Vlastní zpracování)

4.3.2 Instalace virtuální ústředny

Jak již bylo několikrát zmíněno, tato instalace bude probíhat v operační prostředí Windows Server. Pro instalaci ústředny je nutné si stáhnout instalační soubor na oficiálních stránkách 3CX a spustíme průvodce instalací. Instalace může vyžadovat doinstalaci některých dalších potřebných aplikací nutných pro běh ústředny.

4.3.3 Instalace certifikátů

Instalace certifikátů je nutná pro komunikaci SSL protokolu, který zajišťuje bezpečnou komunikaci s webovými servery pomocí protokolu HTTPS. Požadovaný certifikát lze doinstalovat v IIS Manageru. Lze ho vytvořit v sekci “Server Certificates”. Pro dokončení certifikace je nutný soubor s příponou .cer, který dostaneme od poskytovatele SSL certifikátů.

4.4 Nastavení ústředny

Nastavení ústředny lze provést v příkazovém řádku nebo ve webovském prohlížeči. Prvotní nastavení ústředny vyžaduje základní informace nutné pro její běh, mezi které patří například IP adresa, FQDN, určení portů pro komunikaci, vytvoření údajů pro administrátora, licenční údaje apod. Jako statickou IP adresu zvolíme 10.42.1.33, tedy stejnou adresu, jaká byla nastavena na VM. Na FQDN nastavíme název 3cx, tedy plný doménový název bude 3cx.jonckers.cz. Porty na kterých bude ústředna komunikovat jsou dále specifikovány v sekci „nastavení výjimek na firewallu“, neboť všechny porty, které bude ústředna využívat, musí být povoleny na firewallu. Přesnější popis nastavení ústředny je popsán v příloze č. 3.

4.5 Nastavení výjimek na firewallu

Aby mohla ústředna komunikovat s vnější sítí, je nutno nastavit výjimky na firewallu. Výjimky se tvoří pro porty, které byli již definovány při nastavení ústředny. Je tedy nutné nastavit výjimky na portech 5060 (UDP i TCP), 443 (TCP), 9000-9500 (UDP), 5090 (UDP i TCP). Příklad nastavení jedné z výjimek je zobrazen v obrázku níže.

Inbound Service	
Enable	☒ Yes ☐ No
Service Name	3CX_SIP
IP Protocol	TCP ← :: Protocol Selection Tool :: →
Port	Single Port Service Port: 5060
Inbound IP Address(es) (Require at least one IP address)	Connection / IP Address(es) ☒ UPC ☒ (Interface IP) ☐ NETBOX ☐ WAN 3 ☐ Mobile Internet ☐ PepVPN
Included Server(s) (Require at least one IP address)	Server ☒ 3CX (10.42.1.33) Weight 10

Obrázek č. 17: Nastavení výjimky na firewallu
(Zdroj: Vlastní zpracování)

4.6 Vytvoření uživatelských účtů

Tato část návrhu implementace zabere jistý čas a není moc velký prostor pro automatizaci procesu vytváření uživatelských účtů. Pro každého uživatele je tedy nutno přidělit číslo a zadat základní informace. Mezi základní informace patří jméno, příjmení a email. V základním nastavení vypneme hlasovou schránku, neboť zprávy, které jsou podány přes hlasovou schránku mohou být podány i přes mail, který je ve firmě preferován. Po vytvoření uživatelských účtu by měli uživatelé obdržet uvítací email, kde si stáhnou aplikaci pro volání.

4.7 Získání potřebných informací od poskytovatele pro nastavení ústředny

Ze strany poskytovatele musíme získat dva základní prvky. Tím prvním je licence pro virtuální ústřednu, ve které je zahrnuta i podpora poskytovatele v případě poruchy. Druhým prvkem je SIP trunk, po kterém bude probíhat všechna komunikace. Poskytovatel by nám měl o SIP trunku zaslat následující informace: IP adresu, Outbound Proxy, SIP User ID a heslo. Získané informace následně nastavíme na ústředně.

4.8 Vytvoření směrovacích pravidel a reportovacích nástrojů

Tato část práce se bude věnovat návrhu vytvoření volacích skupin, směrovacích pravidel a reportovacích nástrojů.

4.8.1 Vytvoření volacích skupin

Volací skupiny je nutno použít u oddělení, kde může být vyžadována rychlá reakce. Mezi tyto oddělení můžeme zařadit například recepcce nebo Helpdesk. Volací skupina by měla sloužit k tomu, že volající nemusí volat konkrétní osobě, ale celému oddělení. Zamezíme tím potřeby znát každého člena všech oddělení ve společnosti. Stačí pouze vytvořit seznam čísel volacích skupin na které se mohou uživatelé (převážně interní) odkázat. Další výhodou těchto skupin je možnost automatického forwardingu od uživatele na skupinu. Přesněji řečeno, pokud uživatel nepřijme hovor do určitého časového intervalu (který lze snad nastavit v konzoli), hovor může být přesměrován na volací skupinu a zvýšíme tím pravděpodobnost přijmutí hovoru.

4.8.2 Vytvoření směrovacích pravidel

Příchozí směrovací pravidla (Inbound rules) jsou klíčová pro uživatele. Aby se uživatel mohl spojit s příchozím hovorem, musí ústředna nasměrovat příchozí hovor na správného uživatele. Tyto pravidla se vytvářejí ve dvou krocích. Prvním je vytvoření DID (Direct Inward Dialing) na příslušném trunku, kde je nutno specifikovat všechna čísla uživatelů. Druhým krokem je již vytváření příchozích směrovacích pravidel. Zde v nastavení vybereme i pro příslušného uživatele dané DID.

4.8.3 Vytvoření reportovacích nástrojů

Pro evidenci provedených telefonátů a sledování nákladů za hovory je žádoucí nastavit nástroje, které nás budou automaticky informovat o aktuálním stavu. Virtuální ústředna 3CX umožňuje zasílání takovýchto reportů na email. Jako nejvhodnější řešení se jeví zasílání týdenních reportů, aby byl správce ústředny schopen rychle reagovat na

velké výdaje některých uživatelů. V takovýchto reportech můžeme přesně sledovat čas a datum všech příchozích a odchozích hovorů a jaký obnos každý hovor stál. Tyto reporty by tedy měli obdržet kromě správců ústředny i zaměstnanci z účetního oddělení, aby bylo možno kontrolovat částky uvedené v těchto reportech a částky uvedené ve fakturách vystavených poskytovatelem.

Call Reports

Schedule Report Cancel

Call Reports

Type

Call Reports

Name

Report pro správce Vojtěch Sommer

Report format

Adobe Acrobat (.pdf)

E-mail address

vojtech.sommer@jonckers.com

Frequency

Weekly

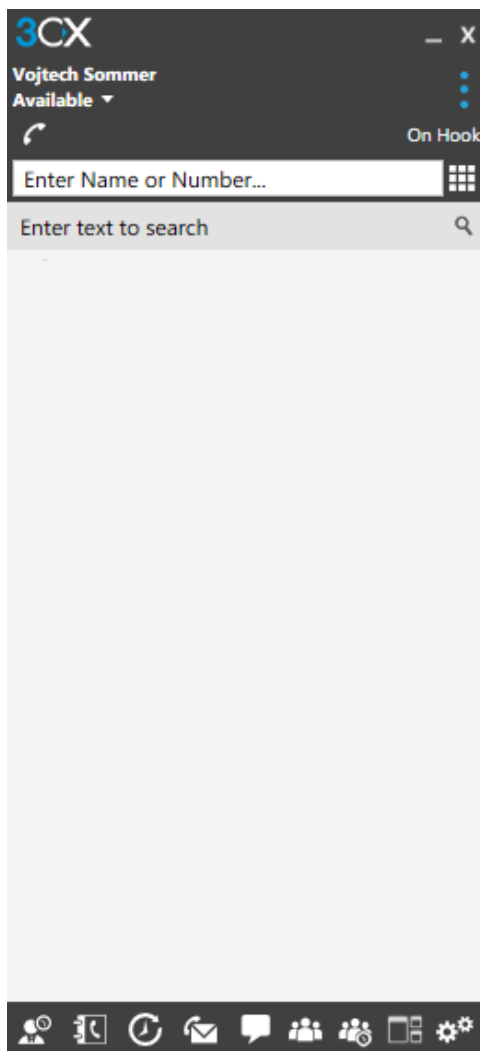
Sunday

Obrázek č. 18: Vytvoření reportovacích nástrojů
(Zdroj: Vlastní zpracování)

4.9 Instalace telefonní aplikace na uživatelská zařízení

Instalace aplikací na uživatelská zařízení je velmi snadná a lze ji popsat ve dvou krocích. Instalace by tedy neměla být problém i pro uživatele, kteří nemají velké zkušenosti s informačními technologiemi. Prvním krokem je instalace aplikace 3CX, kterou lze nainstalovat za pomoci emailu, který dostal každý uživatel, který byl zaregistrován ve virtuální ústředně. V tomto emailu si uživatel pouze vybere operační systém, který používá, otevře příslušný hypertextový odkaz a spustí se instalace. Druhým

krokem je pouze otevření konfiguračního souboru, který je přiložen v emailu. Pro uživatele je to jediné, co musí pro nastavení udělat. Následně by měla být aplikace funkční. To poznáme tak, že v pravém horní rohu je status „On Hook“.



Obrázek č. 19: 3CX Aplikace
(Zdroj: Vlastní zpracování)

4.10 Testovací provoz

V rámci testovacího provozu je nutno otestovat všechny funkcionality systému. Je tedy nutné vyzkoušet volání všemi způsoby případně i do jiných zemí. V základním nastavení mají uživatelé zakázáno volat mimo naši síť. Je tedy vhodné připojit se k jiné síti a ozkoušet, zda je hovor zamítnut. Tento zákaz je nastaven z důvodu bezpečnosti, aby uživatele nemohl nikdo „odposlouchávat“ když bude připojen v neznámé síti. Další

důležitá část testování je zkouška kvality hovoru. Zda je druhá strana dobře slyšet, zda uživatel volající z 3CX je dobře slyšet, zda mikrofony používané do teď pro Skype jsou vyhovující i pro 3CX aplikaci apod.

Během testování byla objevena chyba, která vznikala na straně poskytovatele. Zjistilo se, že hovor se automaticky po 58 minutách ukončí. Po komunikaci s poskytovatelem bylo zjištěno, že je to limit pro délku jednoho hovoru nastavený na straně poskytovatele. Chyba byla následně opravena.

4.11 Odstranění pevných linek a PBX

4.11.1 Pevné linky a kabeláž

Před samotnou implementací nové hlasové služby je nutné odstranit původní řešení. Prvním krokem je odpojení pevných telefonů. Tuto činnost je vhodné vykonávat v době, kdy je v kanceláři minimum lidí, neboť kromě odpojení telefonů je rovněž nutno odpojit všechny síťové kabely spojené s pevnými linkami. Kabeláž je nutno odpojit jak v serverovně mezi ústřednou a patch panelem, tak mezi koncovým zařízením a zásuvkou.

4.11.2 Telefonní ústředna

Kromě pevných linek a kabeláže je nutné odpojit i telefonní ústřednu. Tato ústředna by měla mít pouze dva zbývající kabely, které je nutné odpojit. Napájecí kabel a přívodní síťový kabel ze switchu poskytovatele. Ve chvíli, kdy je ústředna vypnutá, můžeme požádat poskytovatele o přidělení dosud používaných čísel (532 194 3xx) k SIP Trunku, který později nastavíme ve virtuální ústředně.

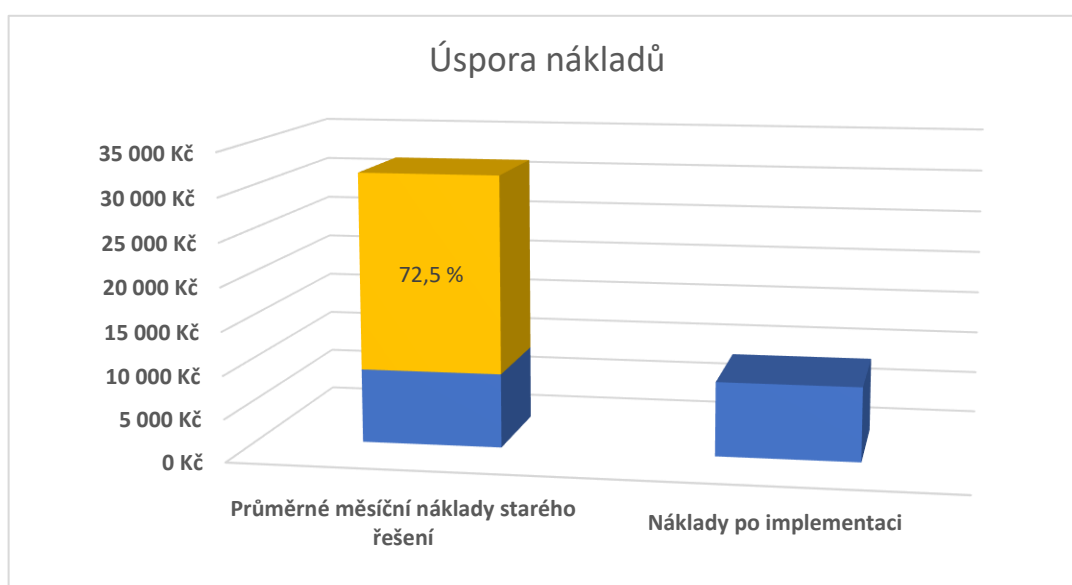
4.12 Uvedení do provozu

Uvedení do provozu můžeme provést ve chvíli, kdy v 3CX ústředně máme vše nastavené. Tím docílíme minimální ztráty konektivity. Tuto část společně s odstraněním pevných linek a PBX je dobré provádět o víkendu. Tedy v době, kdy je v kanceláři minimální fluktuace zaměstnanců. Po odstranění pevných linek a ústředny pro pevné

linky je nutno kontaktovat poskytovatele a požádat ho o přidělení rozsahu čísel na SIP Trunk. V tu chvíli se stává ústředna funkční.

4.13 Ekonomické zhodnocení

Na základě informací zjištěným v průběhu vybírání systému, bylo zvoleno řešení, které pro společnost Jonckers představuje malou počáteční investici a jen minimální měsíční náklady. V měsíčních nákladech představuje největší podíl hodina práce kvalifikovaného administrátora a jen minoritní podíl zde představují náklady spojené se spotřebou energie. Toto řešení se jeví jako ekonomicky nejvýhodnější.



Graf č. 2: Znázornění úspor nákladů
(Zdroj: Vlastní zpracování)

Měsíční náklady původního řešení pomocí pevných linek dosahovaly průměrné hodnoty 31 608 Kč. Takové náklady by firma musela vynaložit každý měsíc, pokud by nezaimplementovala řešení pomocí VoIP. Tyto náklady tedy již společnost Jonckers po zavedení systému 3CX nehradí. Od března roku 2018, od kdy je systém plně funkční, bylo možné sledovat pomocí reportovacích nástrojů náklady za měsíce březen a duben. Vypočtením průměrných nákladů za tyto dva měsíce se dostáváme k průměrným měsíčním nákladům nového řešení 8 691 Kč. Tyto náklady jsou zobrazeny v grafu č. 2, jehož účelem je porovnat rozdíl nákladů před a po implementaci. Náklady za telefonování se díky implementaci nového řešení snížili o více než 70%.

Tak velké snížení nákladů za telefonování lze přikládat nízkým cenám hovorů do celého světa při využití VoIP řešení. Společnost Jonckers spolupracuje s dodavateli ve více jak 100 zemích světa, se kterými je nutné udržovat pravidelný telefonický kontakt. Tento fakt měl nemalý podíl na vysokých nákladech původního řešení. Úspory po implementaci VoIP byly společností Jonckers očekávány.

4.13.1 Návratnost investice

Velmi důležitým parametrem každé investice je její návratnost. V této práci se jedná o ukazatel, který nám sděluje, za jakou dobu se společnosti Jonckers vrátí investovaný kapitál na provedenou implementaci ve formě úspor, které společnost získala po zavedení nového systému. Ukazatel návratnosti investice ROI (Return Of Investment) je vypočten podle následujícího vzorce.

$$ROI = \frac{\text{úspory}}{\text{investice}} * 100\%$$

Úspory zde představuje rozdíl průměrných měsíčních nákladů před a po implementaci. Vzhledem k tomu, že úspory jsou počítány z měsíčních nákladů, bude i výsledek ukazovat průměrnou procentuální návratnost za jeden měsíc.

Investice se zde skládá ze tří částí. První částí jsou náklady vynaložené na řešení ústředny, které byly vyhodnoceny na hodnotu 3 000 Kč. Přesnější informace o způsobu výpočtu byly popsány v kapitole 4.1.3. Druhou částí investice je realizace ústředny. Ústředna byla realizována administrátorem, který byl odměňován za tuto činnost mimo náplň své práce. Hodinová odměna činila 250 Kč, přičemž administrátor strávil na realizaci 40 hodin práce. Tedy tato činnost představuje náklad ve výši 10 000 Kč. K této částce je nutno připočítat zdravotní pojištění (9 % ze mzdy) a sociální pojištění (25 % ze mzdy), které společnost Jonckers musí za zaměstnance odvádět státu. Po připočtení těchto pojištění získáváme superhrubou mzdu, která činí 13 400 Kč. Poslední částí investice představuje nákup licence pro 3CX ústřednu. Ta se stanovuje podle limitu možných současně prováděných hovorů. V tomto případě společnost zvolila licenci, která umožňuje až 16 současných hovorů. Cena takovéto licence je 6 000 Kč. Celková vstupní investice tedy činila 22 400 Kč. Průměrné měsíční úspory činí 22 917 Kč. Po dosažení

těchto hodnot do vzorce dostáváme návratnost investice 102,31 %. Tedy po přepočtení na dny se nám investice vrátí na úsporách po 29 dnech.

Doba návratnosti investice je nezvykle krátká. Dle poskytnutých informací od jednatele společnosti Jonckers již byl vyvinut tlak na implementaci nového řešení telefonování v minulosti. Ovšem sehnat specialistu v oboru IT na současném trhu práce je nesnadné i pro velké korporátní společnosti, natož pak pro středně velkou společnost.

Společnost Jonckers je plátcem daně z přidané hodnoty, tudíž veškeré výdaje se rozumí v částkách bez DPH.

ZÁVĚR

Internet se v dnešní době stává nedílnou součástí každodenního života nás všech. Díky možnostem, které internet poskytuje, se usnadňuje práce, komunikace, nakupování, cestování a mnoho dalších činností. V internetu vidím velký potenciál, jako je například Internet of Things, který je nutno rozvíjet obezřetně kvůli bezpečnosti v počítačových sítích.

Systém propojených počítačových sítí chápu jako multifunkční nástroj, který lze přirovnat ke švýcarskému noži. Tento druh nože rovněž obsahuje mnoho funkcionalit, které jsem neměl možnost použít. Jednou z těchto funkcí internetu je VoIP, neboli přenos hlasu po IP síti. Díky tomuto nástroji můžeme telefonovat z jakéhokoliv místa, kde je dostupné připojení k internetu.

VoIP mě zaujalo natolik, že jsem se tomuto tématu rozhodl věnovat ve své bakalářské práci. Díky společnosti JONCKERS TRANSLATION & ENGINEERING s.r.o., která se mnou sdílela zájem o tuto novou technologii, mi bylo umožněno implementovat VoIP systém ve firemním prostředí a odstranit tak zastaralé řešení pevných linek a zkomplikovaného řešení zastaralé hardwarové ústředny.

Výsledkem této kooperace je oboustranná spokojenost. Ze strany společnosti Jonckers bylo docíleno velkého snížení nákladů za telekomunikace. Tento výsledek si společnost cení nejvíce. Sekundárními výhodami na straně společnosti je snazší administrace telekomunikační sítě, větší flexibilita telefonního systému a možnost snadného rozšíření do dalších zemí, ve kterých společnost Jonckers má své zastoupení. Z mé osobní strany si cením zkušeností a znalostí, které jsem během implementace získal. Za největší osobní úspěch však považuji zavedení nové síťové technologie, která lidem opravdu pomáhá.

SEZNAM POUŽITÝCH ZDROJŮ

- (1) BITTO, Ondřej. *Základy VoIP* (online). (cit. 2017-03-06). Dostupné z: <http://www.lupa.cz/clanky/jak-se-vola-pres-internet-zaklady-voip/>
- (2) WALLACE, Kevin. *Cisco VoIP: autorizovaný výukový průvodce*. Brno: Computer Press, 2009, 527 s. ISBN 978-80-251-2228-0.
- (3) PETERKA, Jiří. *VoIP, IP telefonie*. Praha, 2006. Publikace. Katedra softwarového inženýrství, Matematicko-fyzikální fakulta, Univerzita Karlova, Praha.
- (4) VOZŇÁK, Miroslav. *Signalizace SIP*. Hotel Olšanka, 2006. VŠB – TUO, FEI, Katedra elektroniky a telekomunikační techniky.
- (5) SIP. *CESNET* (online). 1122 (cit. 2017-03-05). Dostupné z: <https://sip.cesnet.cz/cs/protokoly/sip>
- (6) JAIN SCHIGG, John. *SIP. Communications Convergence* (online). San Francisco: UBM, 2002, 10(5), 20 (cit. 2017-03-07). ISSN 15342840. Dostupné z: http://search.proquest.com.ezproxy.lib.vutbr.cz/docview/222636884?rfr_id=info%3Axi%2Fsid%3Aprim
- (7) ZOURZOUVILLYS, T. a E. RESCORLA. *An Introduction to Standards-Based VoIP: SIP, RTP, and Friends*. Internet Computing, IEEE (online). USA: IEEE, 1003, 14(2), 5 (cit. 2017-03-07). DOI: 10.1109/MIC.2010.31. ISSN 10897801. Dostupné z: <http://ieeexplore.ieee.org.ezproxy.lib.vutbr.cz/document/5427399?reload=true>
- (8) YORK, Dan. *SIP Trunking and PSTN Interconnection - CHAPTER 5. Seven Deadliest Unified Communications Attacks*. 2nd edition. 30 Corporate Drive, Suite 400, Burlington, MA 01803, USA: Elsevier, 2010, s. 93-116. DOI: 10.1016/B978-1-59749-547-9.00005-3. ISBN 9781597495479.
- (9) HUJKA, Petr. *Real - Time Transport Protocol a aplikační rozhraní RTP Java Media Framework* (online). Ústav telekomunikací, FEKT VUT Brno, 2003, , 6 (cit. 2017-11-10). Dostupné z: <http://www.elektrorevue.cz/clanky/03018/index.html>

- (10) C. Perkins, "*RTP: Audio and Video for the Internet*" Addison Wesley Professional; July 2003
- (11) KOMOSNÝ, Dan. *Nové směry vývoje protokolu RTP/RTCP pro rozsáhlé konference v Internetu* (online). Ústav telekomunikací, FEKT VUT Brno, 2004, , 10 (cit. 2017-11-10). Dostupné z: <http://www.elektrorevue.cz/clanky/04052/index.html>
- (12) VOZŇÁK, M. a D. ZUKAL. *Kvalita hovoru v prostředí VoIP* (online). Praha, 2005, 9 (cit. 2017-11-11). Dostupné z: <http://archiv.cesnet.cz/doc/techzpravy/2005/voip/kvalitahovoru.pdf>
- (13) *Přechod z veřejné telefonní sítě na SIP trunk: vysvětlení SIP trunking* (online). , 2 (cit. 2017-11-12). Dostupné z: <https://www.3cx.cz/voip-sip-webrtc/sip-trunking/>
- (14) RADA, Milan. *Metody signalizace v telekomunikačních sítích* (online). , 11 (cit. 2017-12-03). Dostupné z: <http://www.itpoint.cz/archiv/2004/clanky/?i=metody-signalizace-v-telekomunikacnich-sitich-4918>
- (15) JOHNSTON, Alan B. *SIP: understanding the session initiation protocol*. 3rd ed. Boston: Artech House, 2009, xxix, 395 s. : il. ISBN 978-1-60783-995-8
- (16) PEREA, Rogelio Martínez. *Internet multimedia communication using SIP: a modern approach including java practice*. Amsterdam: Elsevier ; Morgan Kaufmann, 2008, xxiii, 576 s. : il. ISBN 978-0-12-374300-8

SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

VoIP Voice over Internet Protocol

SIP Session Initiation Protocol

IP Internet Protocol

RFC Request For Comments

ROI Return Of Investment

VM Virtual Machine

VPN Virtual Private Network

SEZNAM GRAFŮ

Graf č. 1: Srovnání možných řešení ústředny	45
Graf č. 2: Znázornění úspor nákladů	55

SEZNAM OBRÁZKŮ

Obrázek č. 1: Pojmy a prvky architektury služby SIP	16
Obrázek č. 2: Registrace	17
Obrázek č. 3: Navázání spojení	18
Obrázek č. 4: Komunikace se SIP serverem	19
Obrázek č. 5: Vedení hovoru v H.323	22
Obrázek č. 6: Představa vedení hovoru v H.323	23
Obrázek č. 7: Architektura H.323	24
Obrázek č. 8: Architektura RTP	25
Obrázek č. 9: Organizační struktura firmy	31
Obrázek č. 10: Schéma aktivních prvků počítačové sítě	33
Obrázek č. 11: Používané access pointy	34
Obrázek č. 12: Peplink Balance 380	36
Obrázek č. 13: Základní atributy informační bezpečnosti	37
Obrázek č. 14: SWOT analýza	41
Obrázek č. 15: Vývojový diagram implementace	43
Obrázek č. 16: Síťové nastavení ústředny	48
Obrázek č. 17: Nastavení výjimky na firewallu	50
Obrázek č. 18: Vytvoření reportovacích nástrojů	52
Obrázek č. 19: 3CX Aplikace	53

SEZNAM TABULEK

Tabulka č. 1: Chybová hlášení protokolu SIP	19
Tabulka č. 2: Výkonnost kodeků používaných ve VoIP	27
Tabulka č. 3: Klasifikační schéma aktiv	39
Tabulka č. 4: Návrh směrování provoleb.....	46

SEZNAM PŘÍLOH

Příloha 1: Vytvoření Virtual Machine

Příloha 2: Nastavení ústředny

Příloha 3: Srovnání možných řešení ústředny

Příloha 1: Vytvoření Virtual Machine

Vytvoření virtuálního počítače bude probíhat v prostředí Windows Server 2016. Základní součástí tohoto operačního systému je Hyper-V manager. Tento nástroj doinstalujeme v Server Manageru. V levém horním rohu zvolíme „Add Roles and Features“ a přes průvodce instalací doinstalujeme Hyper-V na fyzickém serveru. Po instalaci tohoto nástroje otevřeme průvodce pro vytvoření nové Virtual Machine (dále jen VM), kde si rovněž projdeme průvodcem nastavení. Jako název VM zvolíme CZ-3CX. Průvodce se nás následně zeptá, kterou generaci VM chceme. Zde musíme zvolit Generaci 1. Tuto generaci je nutno zvolit, neboť společnost má stále mnoho virtualizačních serverů běžících na operační systému Windows Server 2008, kde by novější generace nemusela fungovat. Dalším bodem je přidělení operační paměti. V našem případě přidělíme 2048 MB RAM staticky. Následně vybereme síťovou jednotku, přes kterou má VM komunikovat. Dále se je nutno nastavit virtuální disk. Protože vytváříme úplně nový systém, vytvoříme i nový virtuální disk o velikosti 180 GB. Větší velikost disku si můžeme odůvodnit jako žádoucí prostor v případě většího množství nahrávek, které se můžou vytvořit v naší ústředně. Posledním krokem je vybrání instalačního souboru pro operační systém. Soubor má koncovku .iso. V našem případě se jedná o Windows Server 2008 R2 Standard. Soubor vyhledáme pomocí průzkumníku Windows Explorer. Následně dokončíme průvodce nastavením, jehož výsledkem by měla být Virtual Machine. Tuto VM zapneme a spustíme instalaci operačního systému. Po dokončení instalace a prvního spuštění OS je nutné povolit účet lokálního administrátora a zvolit heslo. Následně se v rámci testování přihlásíme na účet lokálního administrátora a vymažeme všechny nežádoucí a nepotřebné účty.

Příloha 2: Nastavení ústředny

Po dokončení instalace virtuální ústředny budeme dotázáni v příkazovém řádku, zda chceme provést nastavení ústředny ve webovském prohlížeči nebo v příkazovém řádku. Pro větší pohodlí jsem zvolil nastavení v prohlížeči. Tedy i následný popis dále bude popisován z tohoto prostředí.

Hned v úvodním bodu je uživatel vyzván k zadání licenčního klíče. Licenční klíč lze získat zdarma po dobu jednoho roku. To je velmi dobrá vlastnost systému, neboť umožňuje dostatek času pro testovací účely. Po zadání licenčního klíče následuje definování uživatele a hesla. Následně zadáme IP adresu, kterou jsme nadefinovali výše a nastavíme ji jako statickou. Dále zadáme FQDN, díky kterému budeme moci přistupovat k administrátorské konzoli přes webový prohlížeč. FQDN zvolíme 3cx, tedy plné jméno pro počítač bude následně 3cx.jonckers.cz. Dalším bodem nastavení je nastavení portů, na kterých bude ústředna komunikovat. Doporučená čísla portů jsou již předepsána v textovém poli. Vzhledem k tomu, že doporučené porty nejsou v našem firemním prostředí využívány pro jiné účely, lze ponech defaultní nastavení ústředny. Je dobré si poznamenat čísla těchto portů, neboť později budou nutná pro nastavení výjimek na firewallu. Jedním z posledních bodů průvodcem nastavení ústředny se táže na síťový adaptér, který chceme využít pro komunikaci. Po zvolení adaptéru dojde ke konfiguraci ústředny, po které následuje několik základních otázek nutných pro běh systému. Tyto otázky obsahují email pro zasílání informační zpráv (aktualizace, útoky na ústřednu, diagnostické zprávy, zprávy o disfunkci ústředny), stát a časovou zónu ve které bude ústředna operovat, operátorskou klapku, která je využívána jako defaultní klapka pro příchozí hovory, státy a světadíly kde je volání z ústředny povoleno, jazyk systému a název společnosti. Následně proběhne konfigurace ústředny jejíž výsledkem je dokončení nastavení a otevření přihlašovací stránky do ústředny.

Příloha 3: Srovnání možných řešení ústředny

Řešení	Počáteční investice	Měsíční náklady
Vlastní HW ústředna	5 000 Kč	300 Kč
SW ústředny v cloudu	0 Kč	3 250 Kč
SW ústředna na serveru	3 000 Kč	275 Kč

