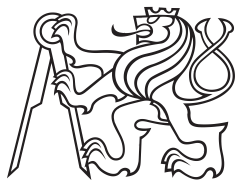


Diplomová práce



České  
vysoké  
učení technické  
v Praze

**F3**

Fakulta elektrotechnická  
Katedra telekomunikační techniky

## Platformy inteligentní sítě nové generace (NGIN)

**Bc. Martin Tóth**

Vedoucí: Ing. Pavel Troller, CSc.  
Obor: Elektronika a komunikace  
Studijní program: Komunikační sítě a internet  
Květen 2020



## I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Tóth** Jméno: **Martin** Osobní číslo: **434735**  
Fakulta/ústav: **Fakulta elektrotechnická**  
Zadávající katedra/ústav: **Katedra telekomunikační techniky**  
Studijní program: **Elektronika a komunikace**  
Specializace: **Komunikační sítě a internet**

## II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

**Platformy inteligentní sítě nové generace (NGIN)**

Název diplomové práce anglicky:

**New Generation Intelligent Network (NGIN) Platforms**

Pokyny pro vypracování:

Popište historický vývoj, základní vlastnosti, architekturu a využití NGIN platform. Stručně popište jednotlivé protokoly a jejich využití v rámci spolupráce se sítí. Věnujte se problematice výměny NGIN platformy z důvodu modernizace a implementace nových služeb. Popište současný stav řešení a porovnejte stávající a novou platformu z hlediska implementovaných služeb, dalších výhod a nevýhod a též případné cenové úspory plynoucí z výměny. V praktické části popište způsob konfigurace jednotlivých platform a funkci uživatelského portálu. Na závěr uveďte, jak probíhá měření a testování správného chodu platformy a zobrazení výsledků.

Seznam doporučené literatury:

- [1] ZUIDWEG, J.: Next Generation Intelligent Networks. Artech House 2002. ISBN 1-58053-263-2 / 978-1-58053-263-1.
- [2] BATES, Regis J.: Advanced Intelligent Networks. CRC Press 2016. ISBN 0-07139-159-2 / 978-0-07139-159-7.

Jméno a pracoviště vedoucí(ho) diplomové práce:

**Ing. Pavel Troller, CSc., katedra telekomunikační techniky FEL**

Jméno a pracoviště druhého(ho) vedoucí(ho) nebo konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: **08.01.2020**

Termín odevzdání diplomové práce: \_\_\_\_\_

Platnost zadání diplomové práce: **30.09.2021**

\_\_\_\_\_  
Ing. Pavel Troller, CSc.  
podpis vedoucí(ho) práce

\_\_\_\_\_  
podpis vedoucí(ho) ústavu/katedry

\_\_\_\_\_  
prof. Mgr. Petr Páta, Ph.D.  
podpis děkana(ky)

## III. PŘEVZETÍ ZADÁNÍ

Diplomant bere na vědomí, že je povinen vypracovat diplomovou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v diplomové práci.

\_\_\_\_\_  
Datum převzetí zadání

\_\_\_\_\_  
Podpis studenta



## Poděkování

Mé poděkování patří celé katedře telekomunikační techniky. Především mému vedoucímu Ing. Pavlovi Trollerovi, CSc. za cenné rady a dozor nad vypracováním diplomové práce. Dále bych chtěl poděkovat kolegům v práci za rady a předané know-how.

## Prohlášení

Prohlašuji, že jsem zadanou diplomovou práci zpracoval sám s přispěním vedoucího práce a používal jsem pouze literaturu v práci uvedenou. Dále prohlašuji, že nemám námitek proti půjčování nebo zveřejňování mé diplomové práce nebo její části se souhlasem katedry.

V Praze, 22. května 2020

## Abstrakt

Tato diplomová práce se zabývá výměnou platformy pro Chytrou síť. V teoretické části je popsán vývoj Chytré sítě a protokoly, které používá. Následují informace o původní a nové platformě. Jsou popsány rozdíly mezi nimi a proces výměny v síti. Další část se zabývá službami a prostředím pro jejich vytváření. V předposlední části je popsáno testování platformy a jsou zobrazeny výsledky měření. V závěru se věnujeme monitorování provozu a statistikám ze sítě.

**Klíčová slova:** Chytrá síť, protokoly, platformy, virtualizace, migrace, testování

**Vedoucí:** Ing. Pavel Troller, CSc.

## Abstract

This diploma thesis deals with the replacement of the platform for Intelligent network. The theoretical part describes the development of Intelligent network and the protocols which it uses. Information about original and new platforms follow thereafter. The differences between them and migration process are described. The next part deals with services and the environment for their creation. Testing of platform and results of measurement are illustrated in the penultimate section. Finally, I focus on traffic monitoring and statistics from the network.

**Keywords:** Intelligent network, protocols, platforms, virtualization, migration, testing

**Title translation:** New Generation Intelligent Network (NGIN) Platforms

## Obsah

<b>1 Úvod</b>	<b>1</b>	<b>5 Nová platforma</b>	<b>33</b>
<b>2 Chytrá síť</b>	<b>3</b>	5.1 Design platformy .....	34
2.1 CS-1 .....	4	5.2 Výhody oproti původní platformě	35
2.2 CS-2 .....	11	<b>6 Fáze implementace a migrace</b>	<b>37</b>
2.3 CS-3 .....	14	6.1 Fáze plánování .....	37
2.4 CS-4 .....	15	6.2 Fáze analýzy a návrhu .....	38
<b>3 Protokoly</b>	<b>17</b>	6.3 Implementační fáze .....	38
3.1 SS7 .....	17	6.4 Fáze testování .....	39
3.2 INAP .....	20	6.5 Migrace .....	39
3.3 CAP .....	21	<b>7 Služby běžící na platformě</b>	<b>41</b>
3.4 SIP .....	21	7.1 Služba překladu čísel .....	41
3.5 PINT, SPIRITS .....	24	7.2 Virtuální privátní síť .....	42
<b>4 Původní platforma</b>	<b>27</b>	7.3 Virtuální ústředna .....	43
4.1 Design sítě .....	28	<b>8 Prostředí vytváření služeb</b>	<b>45</b>
4.2 Hardware .....	29	8.1 Příklad A - logika služby pro odchozí hovory .....	47
		8.2 Příklad B - logika služby pro odchozí hovory .....	47

<b>9 Testování platformy</b>	<b>49</b>
9.1 Výkonnostní testy .....	52
9.2 Testy přetížení .....	55
9.3 Testy maximálního zatížení ....	56
<b>10 Monitorování</b>	<b>59</b>
10.1 EDR záznamy .....	61
<b>11 Závěr</b>	<b>65</b>
<b>Literatura</b>	<b>67</b>
<b>A Seznam zkratk</b>	<b>69</b>



## Obrázky

2.1 IN rovina služeb [2] .....	4	4.1 Přehled platformy [11] .....	27
2.2 Vztah mezi rovinou služeb a globální funkční rovinou [2] .....	5	4.2 Design sítě [11] .....	28
2.3 Struktura SIB [2] .....	6	4.3 HW prvky [12] .....	29
2.4 Distribuovaná funkční rovina [2] .	7	4.4 Prvky USAU HW [12] .....	30
2.5 Koncept polovičního hovoru [2] ..	9	5.1 Architektura platformy [13] ....	33
2.6 Fyzická rovina [2] .....	11	6.1 Fáze migrace [14] .....	37
2.7 Sloučení funkcí v přepínači [2] ..	11	7.1 VPN role [16] .....	43
2.8 High-level SIB [2] .....	13	8.1 Vybraný seznam modulů [18] ...	46
2.9 Nové propojení mezi FE v CS-2 [2] .....	14	8.2 Logika služby pro odchozí hovory koncových uživatelů [18] .....	47
2.10 Částečný pohled na DFP [2] ..	15	8.3 Strategie odchozího hovoru [18] .	48
3.1 Vrstvový model SS7 [4] .....	19	9.1 V model [19] .....	49
3.2 Role síťových prvků při vytváření spojení [9] .....	22	10.1 Využití CPU, paměti a disku ..	59
3.3 Základní tok volání [9] .....	24	10.2 Vybrané parametry databáze za posledních 6 hodin .....	60
3.4 PINT architektura [2] .....	25	10.3 Dostupnost sítí za posledních 30 dní .....	60
3.5 SPIRIT architektura [2] .....	25	10.4 Ukázka EDR záznamu .....	62

10.5 Celkový počet hovorů na platformě .....	62
10.6 Průměrné doby trvání .....	63
10.7 Délka hovorů .....	63
10.8 Ukončení hovoru .....	64
10.9 Ukončení hovoru .....	64

## Tabulky

2.1 Funkce definované v CS-1 [2] ....	5
5.1 Příklady servisních klíčů [13] ...	34
5.2 Přehled redundance serverů [13]	35
9.1 Naměřená data pro CAP hovory	52
9.2 Naměřená data pro SIP hovory .	52
9.3 Naměřená data pro CAP hovory	53
9.4 Naměřená data pro SIP hovory .	53
9.5 Naměřená data pro CAP hovory	53
9.6 Naměřená data pro SIP hovory .	54
9.7 Naměřená data pro CAP hovory	54
9.8 Naměřená data pro SIP hovory .	54
9.9 Výsledky maximálního SIP zatížení .....	56
9.10 Výsledky maximálního zatížení portálu .....	57
9.11 Výsledky maximálního zatížení portálu .....	57

10.1 Vybrané parametry EDR záznamů [13] .....	61
--	----



# Kapitola 1

## Úvod

První pokusy o přenos zvuků a lidské řeči jsou již ze 17. století z Anglie, kde byl sestrojen přístroj tvořený napnutým vláknem zakončený jemnou blánou [1]. Jednalo se o úspěch, ale vynález se používal pouze jako dětská hračka.

V 19. století se díky objevům v elektrotechnice otevírají nové možnosti pro telefony. V roce 1854 byl v časopisu vydán první článek o možnosti přenosu zvuku pomocí elektrických signálů. Odborná veřejnost však poznatky odmítá. Německý profesor fyziky Philips Reis sestavil první přístroj, který přinášel výsledky. Veřejnosti ho představil v roce 1861 a pojmenoval ho telefon (z řeckého téle = vzdálený a fóné = hlas). Další výzkum nebyl proveden, jelikož zkoušky neměly dobré výsledky. Označení telefon už zůstalo.

Již otec Alexandera Grahama Bella se zabýval metodami vyučování hluchoněmých. Bell navázal na jeho práci a začal stavět aparát zesilující lidský hlas, který umožní vnímat zvuk neslyšícím. Z aparátu se náhodou stal telefon. V roce 1875 předložil první popis zařízení sloužící k přenosu lidské řeči a o rok později požádal o patent. S následným vylepšením přišel Hughes, který do přístroje přidal mikrofon. Po jeho zavedení mohly začít pokusy s hovory na dálku. Jeden z iniciátorů a zakladatelů Světové poštovní unie Dr. Heinrich von Stephan o vynálezu informoval přítele Wenera von Siemense, který rychle pochopil převratný význam zařízení a již na konci roku 1877 vyráběl 700 přístrojů denně.

První telefonní síť v Čechách byla dlouhá 2,5 km a byla zavedena v dubnu 1881 z Ledvic do Duchcova. Udělení koncese v červenci 1881 Pražskému podnikatelství pro telefony bylo jednou z nejvýznamnějších událostí rozvoje

sítě. Ústředna s 11 účastníky zahájila provoz v roce 1882 s pracovní dobou od 8 do 12 hodin a od 14 do 18 hodin. Na starost ji měli dva úředníci, dva mechanici, pět manipulantek a sedm zřízenců.

Pražské podnikatelství pro telefony v roce 1884 ukončilo z finančních důvodů svoje působení na trhu. Síť převzaly anglické společnosti se sídlem ve Vídni. Investovaly do budování sítě a rozšiřování kapacit ústředen. Pro společnosti plynul z provozování velký zisk. Z toho důvodu vešel v platnost zákon z 29. prosince 1892 o zestátnění městských telefonních sítí a vykoupení koncesí. V dalších letech byla telefonní síť rozšiřována, budovala se nová meziměstská spojení, ústředny a docházelo k modernizaci sítě.

Telefonní síť sloužila pouze k uskutečňování hovorů. Příchod digitálních programovatelných přepínačů umožnil zavádění inteligentních služeb, jako je přesměrování hovorů, blokování hovorů, barevné linky, atd. [2] Do každého přepínače se ručně instalovaly služby. Při zavádění nové služby se musely přeprogramovat všechny přepínače v síti. Proces definování služby, její specifikace, testování a implementace trvala dva až čtyři roky. Neexistovala žádná správa služeb. I nejmenší oprava vyžadovala přeinstalování všech přepínačů. To bylo velice neefektivní a brzy se od toho opustilo. Společnost Telcordia přišla s konceptem pokročilých chytrých sítí (AIN - Advanced Intelligent Networks) pomocí protokolů sítě SS7. Umožňoval společnostem jednodušší zavádění a správu služeb s centralizací jejich řízení.

Mezinárodní telekomunikační unie (ITU - International Telecommunication Union) na základě úspěchu AIN zahájila na konci 80. let proces standardizace chytré sítě (IN - Intelligent Networks). Trval čtyři roky a v roce 1993 byl publikován první standard. Od té doby bylo provedeno mnoho vylepšení a rozšíření, avšak i dnešní standardy jsou do značné míry založeny na těch původních.



## Kapitola 2

### Chytrá síť

Cílem Chytré sítě (IN - Intelligent Networks) [2, 3] je integrace funkcí a výhod sítě nové generace. Umožňuje přenos různých druhů informací přes telefonní síť bez potřeby speciálních obvodů. Datový přenos, internetová komunikace a hlasové služby jsou konvergentní a poskytují novou sadu službu.

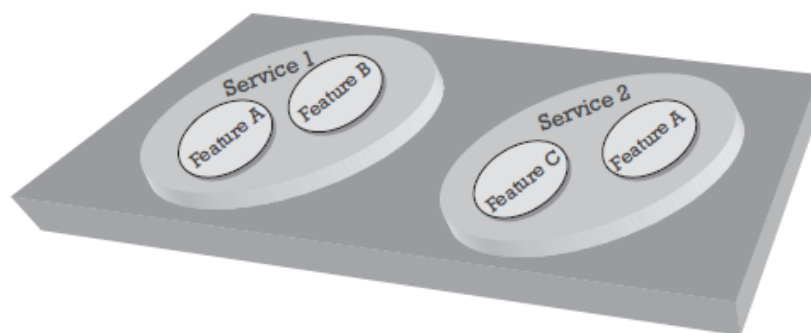
Dá se popsat několika způsoby. Jeden ze způsobů, jak se na IN dívat, je pohlížet na ni jako na doplněk ke stávající architektuře. Dá se říct, že to je sada dedikovaných počítačů, které vykonávají speciální ovládací funkce. Druhým způsobem můžeme IN považovat za softwarovou architekturu, která provozuje služby. Není to sada HW uzlů jako spíš softwarový framework.

Neustálé rozšiřování standardu v rychle se měnícím prostředí vedlo k rozhodnutí standardizovat v nepřetržitém procesu a v pravidelných intervalech ho zmrazovat. Specifikace intervalu se nazývají sady schopností (CS - Capability Sets) a definují sadu funkcí, ze kterých lze vytvářet služby. Jsou zpětně kompatibilní, nová CS přidává nové funkce, ale stávající zůstávají zachovány. Standardy kombinují různé zobrazení v koncepčním modelu chytré sítě (INCM - Intelligent Networks Conceptual Model). Porovnává různé fyzické a logické pohledy na architekturu. Jsou definovány čtyři různé roviny: rovina služeb, globální funkční rovina, distribuovaná funkční rovina a fyzická rovina. Nejsou to různé vrstvy protokolu, jak by se mohlo zdát, ale jde pouze o způsob pohledu na IN z různých úhlů.

## 2.1 CS-1

### 2.1.1 Rovina služeb

Rovina služeb (SP - Service Plane) je vrchní rovina INCM, která se na služby dívá z pohledu uživatele. Popisuje, z jakých funkcí se služba skládá, avšak neřeší, jak je naimplementována v síti. Na funkci lze koukat jako na opakovaně použitelný funkční blok. Koncept skládání služeb z jednotlivých funkcí je zobrazen na obrázku 2.1 a je zcela zásadní pro IN. Klíčovou filosofií IN je standardizování opakovaně použitelných funkcí, ne služeb. Provozovatel sítě může skládat služby i bez standardizovaných funkcí a jediným limitem je jeho představivost.



Obrázek 2.1: IN rovina služeb [2]

Hlavní funkce definované v CS-1 jsou popsány v tabulce 2.1. Je jich málo, jsou poměrně jednoduché a úzce odpovídají službám pobočkových ústředí a jejich doplňkovým službám. S rozvojem chytrých sítí se množství funkcí zvyšovalo, a tím rostly i možnosti nových služeb.

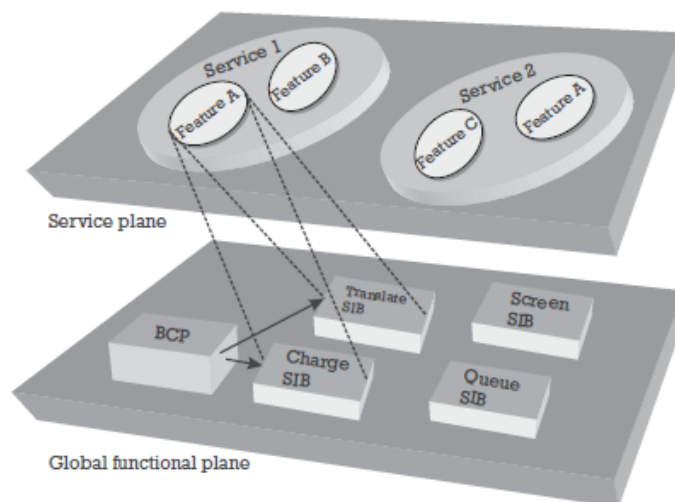
### 2.1.2 Globální funkční rovina

Globální funkční rovina (GFP - Global Functional Plane) se dívá na služby z pohledu poskytovatele služeb. Popisuje, jaké softwarové komponenty musí poskytovatel nasadit, aby mohl sestavovat služby. Komponenty se nazývají SIB (System Information Block) a z nich se následně sestavují celé struktury. Funkce definovaná v rovině služeb je implementována jedním nebo více SIB v GFP. Vztah je zobrazen na obrázku 2.2.



Skupina funkcí	Funkce
Číslování	Zkrácená volba, jedno číslo, osobní číslo, plán soukromého číslování
Směrování	Přesměrování hovorů, směrování v závislosti na čase, směrování závislé na původu, distribuce hovorů
Nabíjení	Prémiová sazba, reverzní rozdělení
Přístup	Ověřování, autorizační kód, přístup mimo síť
Omezení	Omezovač hovorů, uzavřená skupina uživatelů, ukončení testování volání
Přizpůsobení	Správa profilu zákazníka, oznámení nahrané zákazníkem, přizpůsobené vyzvánění
Uživatelská interakce	Původní výzva uživatele, výzva cílového uživatele, obsluha, konzultační volání
Další funkce	Čekání hovoru, automatické zpětné volání, přidržení hovoru s ohlášením, řazení do fronty, přepojení hovoru, hromadné volání, konference

**Tabulka 2.1:** Funkce definované v CS-1 [2]

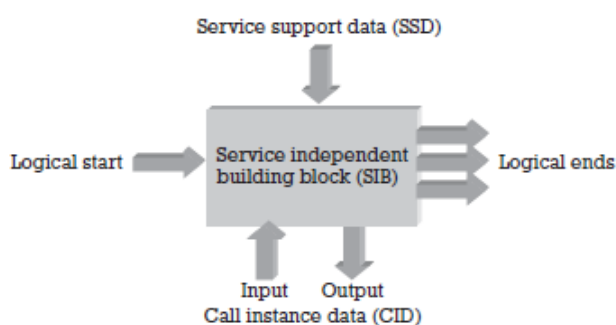


**Obrázek 2.2:** Vztah mezi rovinou služeb a globální funkční rovinou [2]

## ■ SIB

SIB jsou softwarové komponenty, ze kterých se skládají služební skripty. Má jeden logický počáteční bod a vícero logických zakončení. Komponenta se do řídicího toku připojuje logickým začátkem a koncem. Více logických zakončení umožňuje použít SIB jako rozhodovací bod. V CS-1 jich je popsáno celkem 14 a jejich funkcionalita je základní. Každý má přesně popsán logický začátek, konec, SSD a CID.

Působí na instanci dat volání (CID - Call-instance Data), které je závislé na volaných datech, včetně adresy původce, volaného čísla a cílové směrovací adresy. Může potřebovat data ze služeb (SSD - Service Support Data), která jsou nezávislá na volání. Příkladem SSD je seznam pro detekci hovorů (black list), tabulka pro přesměrování hovorů nebo schéma zapojení. Struktura SIB včetně parametrů je znázorněna na obrázku 2.3.



Obrázek 2.3: Struktura SIB [2]

## ■ Základní proces volání

Mezi SIB je i jeden z nejdůležitějších stavebních bloků reprezentujících volání. Nazývá se základní proces volání (BCP - Basic Call Process) a popisuje fáze nastavení telefonního hovoru od jednoho uživatele k druhému. V každé fázi je možné přerušit proces nastavení hovoru a začít provádět servisní program. Přerušování může být zpracováno pouze v bodech zahájení (POI - Point of Initiation).

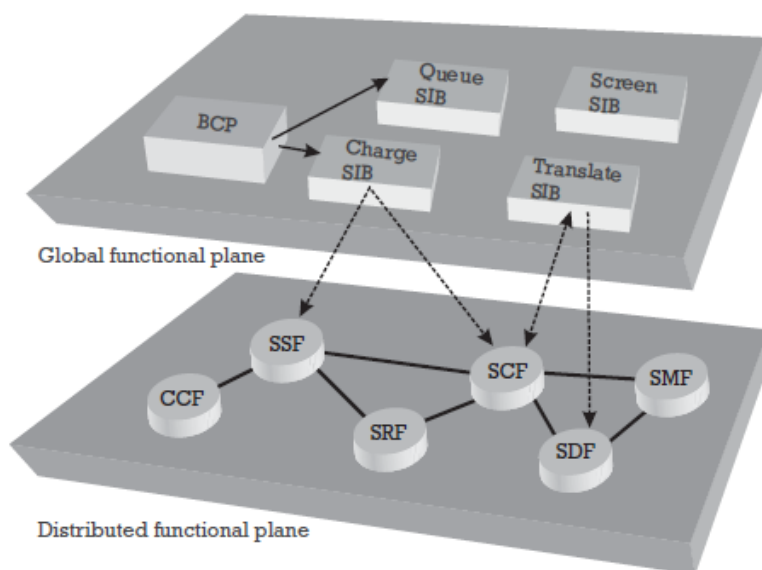
Při spuštění BCP předá CID prvnímu spuštěnému SIBu. Libovolná komponenta tvořící službu může podle požadavků měnit CID, například při přesměrování hovorů změni cílovou adresu. Po dokončení zpracování služby

se poslední SIB vrátí zpět do BCP. Může se vrátit na libovolné místo, nemusí se vracet na místo, kde byl vyvolán. Bod, kde byl prvek předán zpět do BCP, se nazývá bod návratu (POR - Point of Return) a lze v něm přikázat, jak má BCP zacházet s voláním.

GFP pomáhá identifikovat komponenty, které skládají služby. Pohled na síť je zjednodušený a neříká nám, jak v reálné síti implementovat služby. Ve skutečnosti však nespravujeme síť jako jeden stroj s jediným BCP pro každé volání. Síť má složitou strukturu vrstev a skládá se z mnoha specializovaných prvků. Začneme-li přemýšlet o hovorech mezi dvěma různými operátory, celá struktura se ještě více zkomplikuje.

### 2.1.3 Distribuovaná funkční rovina

Distribuovaná funkční rovina (DFP - Distributed Functional Plane) poskytuje realističtější pohled na síť, avšak reflektuje distribuci funkcí. Rozlišuje různé funkční entity (FE), které tvoří telefonní síť. Funkční entity jsou distribuované síťové funkce, které spouští BCP a další SIB. Na jeden SIB může být mapováno více funkčních entit. Z toho důvodu popisuje datový tok mezi funkčními entitami a definuje, které informace se musí mezi nimi vyměnit při implementaci SIBu.



Obrázek 2.4: Distribuovaná funkční rovina [2]

Nejvýznamnější funkční entity v CS-1:

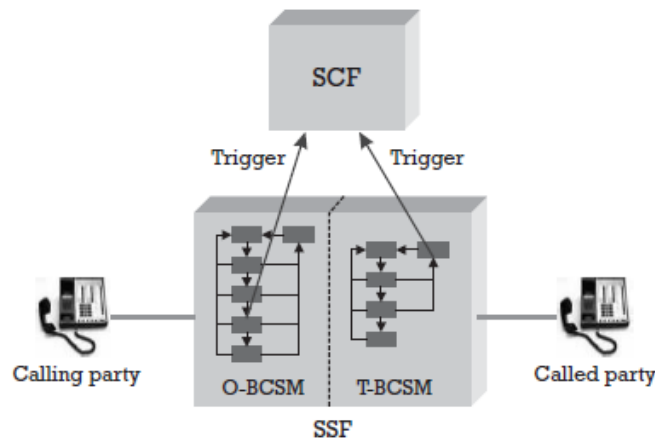
- Call control function (CCF) - udržuje stav hovoru, např. vyzvánění nebo obsazení linky.
- Service switching function (SSF) - ovládá spojení během hovoru, obvykle hlasové obvody.
- Service control function (SCF) - programy, které řídí služby. Nazývají se servisní logika.
- Service data function (SDF) - databáze, které uchovávají data pro podporu služeb, např. zůstatek předplacené karty, tabulka překladů čísel.
- Service management function (SMF) - funkce pro správu, např. pro instalaci nových služeb, přidávání nebo odebrání předplatitelů, aktualizace dat služeb.
- Special resource function (SRF) - speciální funkce v síti, které mohou být potřeba k realizaci služby, např. přehrávání oznámení, hrající tóny, konferenční hovory.

Hlavní důvod rozdělení CCF a SSF spočívá v rozlišování mezi hovorem a spojením. Kvůli tomuto konceptu můžeme hovor rozšířit na konference, multimediální komunikace nebo na internetové spojení. Servisní logika může přidávat nebo odebírat spojení v rámci jediného hovoru.

### ■ Poloviční hovor

Nejdůležitější upřesnění základního procesu volání je zohlednění distribuované povahy hovoru. Hovor se nepovažuje za jeden abstraktní proces, ale zpracování hovoru se rozlišuje mezi volající a volanou stranou.

Základní proces volání je rozdělen do dvou částí nazývaných původní model základního stavu volání (O-BCSM) a ukončovací model základního stavu volání (T-BCSM). O-BCSM popisuje postup při zahájení hovoru, kdežto T-BCSM postup přijetí jednoho hovoru. Oba modely mohou spustit služby v SCF, viz. obrázek 2.5. Důvod rozdělení je prostý. Existují služby, které se zabývají pouze odchozími hovory (např. zkrácená volba) a služby zabývající se příchozími hovory (např. blokování hovorů). Kromě toho volající a volaná strana nemusí být připojena ke stejnému přepínači nebo připojena na stejnou síť.



Obrázek 2.5: Koncept polovičního hovoru [2]

### ■ Detekční body

O-BCSM a T-BCSM lze chápat jako podrobnější variantu BCP. Zobrazují se jako stavové diagramy a popisují stavy zpracování hovorů a přechody mezi nimi, kde stavy jsou body v hovoru a přechody jsou způsobeny událostmi, jako např. vyvěšení telefonu, vytočení čísla, zavěšení telefonu. Ke každé události může být přiřazen bod detekce, který může být považován za implementaci POI a SSF v nich může pozastavit zpracování hovoru a předat kontrolu do SCF.

V závislosti na službě mohou detekční body odkazovat na různé postupy. Žádají o to dvěma způsoby:

1. Spouštěcí detekční body (TDP) - jsou nastaveny staticky v době nasazení služby, nebo když se uživatel přihlásí ke službě (např. služba bezplatný telefon).
2. Body detekce událostí (EDP) - nastavují se dynamicky během hovoru podle logiky služeb (např. automatické zpětné volání na obsazeno).

Existují dva druhy akcí při objevení detekčního bodu:

1. Oznámení - BCSM odešle informace do SCF a bez čekání na odpověď dál zpracovává hovor
2. Žádost - BCSM pozastaví zpracování hovoru a předá informace do SCF. Čeká na odpověď. Po jejím přijetí pokračuje ve zpracování hovoru, pravděpodobně s novými parametry.

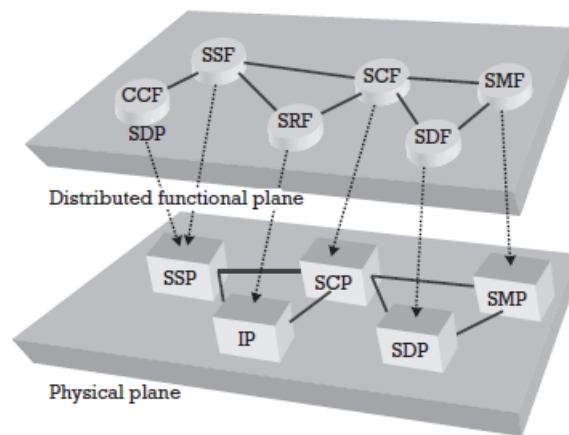
Například přesměrování hovorů lze spustit pouze jako žádost, protože se čeká na přeložení čísla. Naopak televizní služba může vyžadovat pouze zaslání informací do SCF bez přerušení hovoru.

#### ■ 2.1.4 Fyzická rovina

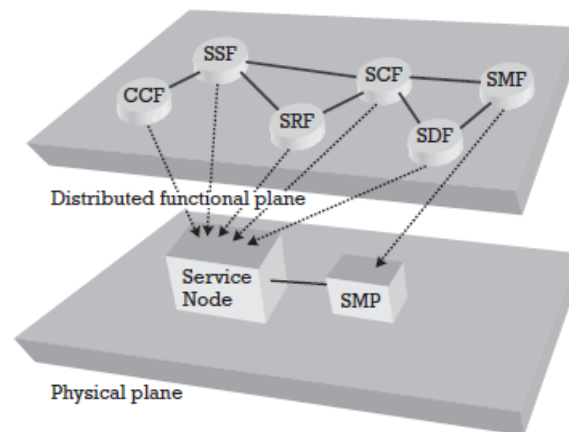
Fyzická rovina (PP - Physical Plane) zobrazuje funkce chytré sítě na fyzických uzlech. Nejjednodušší mapování přiděluje pro každou funkci samostatný uzel:

- Service switching point (SSP) - obsahuje přepínač, ale obvykle také SCF a SSF
- Service control point (SCP) - obsahuje SCF
- Service data point (SDP) - obsahuje databáze, které tvoří SDF
- Service management point (SMP) - vlastní SMF
- Intelligent peripheral (IP) - implementuje SRF

Obrázek 2.6 zobrazuje přímé mapování funkcí na uzly, z něhož vyplývá, že implementace systému IN vyžaduje minimálně čtyři nebo pět strojů. V menších sítích, při malém počtu služeb nebo jejich předplatitelů, lze počet strojů snížit sdružením funkcí na fyzickém uzlu. Nejméně HW lze využít při konfiguraci, kdy sloučíme SSP, SCP, SDP a IP do jednoho uzlu. Označuje se jako servisní uzel a mnoho výrobců kombinuje tyto funkce se samotným přepínačem, viz. obrázek 2.7, avšak obtížněji se u něj garantuje vysoká propustnost.



Obrázek 2.6: Fyzická rovina [2]



Obrázek 2.7: Sloučení funkcí v přepínači [2]

## 2.2 CS-2

IN byly navrženy pro pevné hlasové telefonní sítě vlastněné jedním operátorem. Standard CS-1 byl silný a jednoduchý, ale již v době nasazování byl zastaralý, neboť svět prošel razantními změnami. Proběhla deregulace telekomunikačního trhu a otevření konkurence. Aby se podpořila hospodářská soutěž, regulační orgány začaly vyžadovat přenositelnost čísel. Druhá polovina 90. let byla érou mobilního telefonu a internetu. To přispělo k explozi složitosti v síti. CS-2 si dala za cíl odstranění omezení CS-1 a zároveň s ní zůstat plně kompatibilní. Nové rozšíření lze shrnout takto:

1. umožňuje komunikovat mezi vícero SCF a vícero SDF. Logika a data služeb mohou být distribuovaná a řízená přes hranice operátora.

2. Dokáže zpracovávat hovory mezi více jak dvěma stranami. Jedna instance logiky služeb v SCF může řídit více BCSM najednou.
3. Nový základní proces nesouvisející s voláním (BUCP), který umožňuje interakci uživatele mimo hovor.
4. Podpora signalizačního spojení, které nesouvisí s hovorem nebo s telefonní sítí, např. SMS v GSM.
5. Zobecňuje koncept vytváření služeb. Upřesňuje SIB, který se stává skutečným modelem komponenty.
6. Předdefinovává pokyny pro správu služeb.
7. Přidává pokyny k řešení konfliktů mezi nekompatibilními službami.

### 2.2.1 Rovina služeb

Rovina služeb zavádí nové funkce, které mohou poskytovat více možností než služby založené na přepínačích. Udává minimální sadu služeb a funkcí, které lze implementovat nebo které bychom měli být schopni naimplementovat.

Služby jsou zpětně kompatibilní se službami z CS-1 a přidává další funkce pro internetworking, call-party handling (CPH), interakce uživatelů mimo kanál, správu a tvorbu služeb.

### 2.2.2 Globální funkční rovina

Důležitou změnou je přidání BCUP, zvláštního SIBu, který popisuje proces interakce uživatele nesouvisející s hovorem. Příkladem použití tohoto procesu je registrace uživatele do sítě nebo terminálu. BCUP obstarává také ověřovací a registrační postupy mimo kontext hovoru.

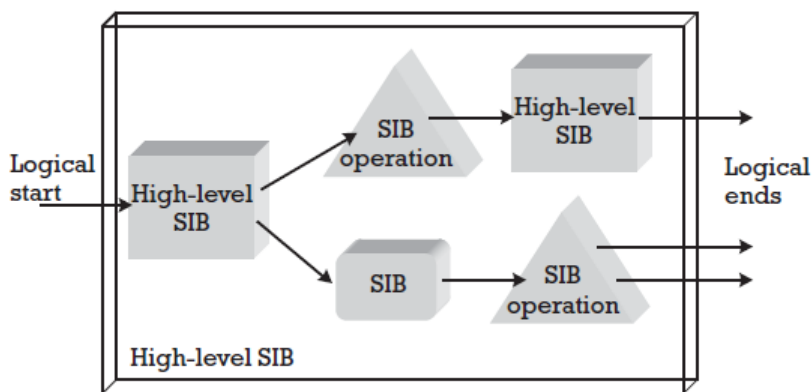
Rozšiřuje BCP o nové POI a POR, čímž poskytuje více kontrolních bodů v hovoru. Představuje POI pro midcall přerušení pomocí hook flash nebo stiskem speciálního R tlačítka na telefonu. Nové POR jsou spojeny s individuálním zpracováním připojení mezi volajícími.

Proces služby nemusí být tvořen jediným SIB, ale může zahrnovat více procesů. Během provádění logiky programu služby může vytvářet nové procesy,



ty běží paralelně a mohou si mezi sebou posílat zprávy. Některé SIB jsou předdefinované a zároveň jsou přidány nové. Uživatelská interakce SIB je rozšířena tak, že zpracovává interakce uživatelů mimo kanál a interakce nesouvisející s hovorem uživatele. Kromě BCUP je nové i CPH, které má na starosti připojení a odpojení stran v rámci hovoru, řízení procesů při vytváření a odstraňování paralelních služeb i komunikaci mezi nimi.

SIB je dodefinován o rekurzivní model vytváření služeb, kdy operace SIBu představuje nejjednodušší operaci, která nejde rozdělit. High-level SIB je pak složka složená ze SIB, operací SIB nebo jiných HLSIB. Kvůli zpětné kompatibilitě byly zachovány i SIBy z CS-1.



Obrázek 2.8: High-level SIB [2]

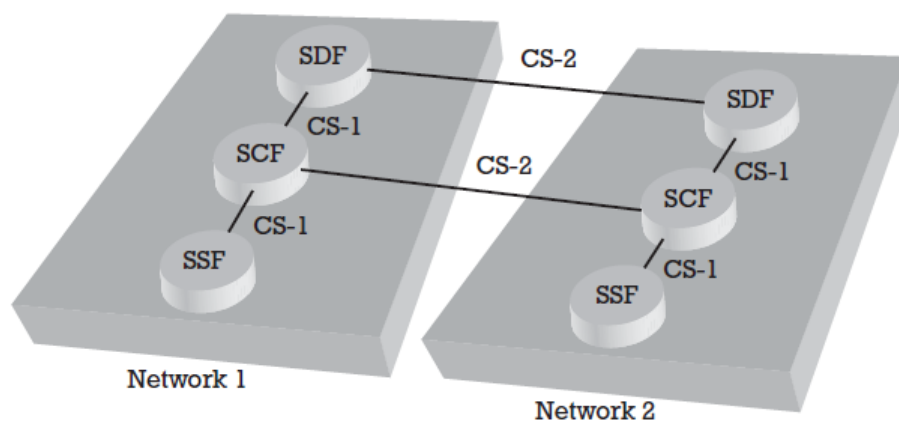
### 2.2.3 Distribuovaná funkční rovina

Přidává nové FE, stávající rozšiřuje o nové funkcionality a představuje tři funkce pro mobilní síť. Rádiový přístup není hlavním cílem CS-2, proto tyto FE a jejich datové toky mají pouze informativní status.

Uvedení nových datových toků mezi existujícími FE umožňuje SCF komunikovat přímo s ostatními a distribuovat řízení služeb. Data mohou být distribuována i přes SDF. Obrázek 2.9 ukazuje tato tvrzení. Možnost distribuce řízení služeb a dat je užitečná v případech, kdy služba musí být poskytována napříč poskytovateli.

Definuje nové BCUSM, které reprezentuje interakci uživatele mimo kontext hovoru. Má jednoduchou strukturu. Stavby a přechody reprezentují aktivaci a odpojení signalizačního kanálu a příjem uživatelských dat ve formě komponent. Všechno se děje mimo kontext hovoru. Další novou důležitou funkcí

je CPH, která umožňuje individuální vytvoření a uvolnění jednotlivé části hovoru, to znamená, že hovor a připojení nejsou stejné, konfigurace připojení se může během hovoru měnit. Nezbytné pro řízení služeb jako je konference nebo jednodušší služba call waiting.



Obrázek 2.9: Nové propojení mezi FE v CS-2 [2]

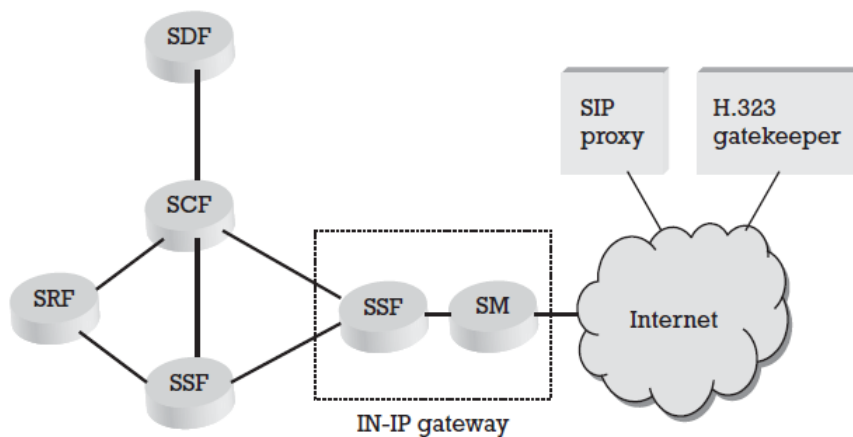
## 2.3 CS-3

Když začala standardizace, výrobci a operátoři se stále potýkali s konsolidací CS-2, která představovala novou úroveň složitosti, nejasnosti a problémů s interpretací normy. Ve výsledku je CS-3 považována za aktualizovanou verzi CS-2. Nepředstavuje nový koncept INCM, ale pouze vylepšuje možnosti spolupráce s mobilní sítí, širokopásmovou a úzkopásmovou ISDN a Internetem. Nejdůležitější částí standardu je predefinování INAP protokolu.

## 2.4 CS-4

Internet, mobilní sítě a deregulace měnily telekomunikační scénu dramatickým způsobem. Objektové programování se stalo standardem v IT. Zavádí proto důležité inovace a přizpůsobuje se komunikaci nové éry: hlas, video, multimédia, datová komunikace. Zahrnuje mobilní stanice a začíná využívat paketový přenos místo přepojování okruhů. Poskytuje objektově orientovaný model pro služby a komponenty služeb, který je v souladu s průmyslovými standardy.

Dominantní částí standardu je revize INAP protokolu. Jediná vylepšená část INCM je DFP. Nejdůležitější novou funkcí je podpora komunikace přes internet. Představuje správce relací (SM), nový FE pro zpracování hlasových a multimediálních relací na internetu při použití protokolu H.323 nebo SIP. Z pohledu internetu SM vypadá jako H.323 gatekeeper nebo SIP proxy. Z pohledu sítě jako speciální typ telefonní ústředny, která může spouštět služby přes SSF.



Obrázek 2.10: Částečný pohled na DFP [2]



## Kapitola 3

### Protokoly

#### 3.1 SS7

SS7 je signalizační síť. Obsahuje sadu protokolů a využívá se v telekomunikacích. Poskytuje spolehlivá signalizační spojení nezávislá na přenosovém médiu. Protokoly mají vysokou míru flexibility pro podporu nových funkcí. Byla představena v roce 1975 firmou AT&T a dodnes je nejmodernější. Je klíčovým aktivátorem veřejné telefonní sítě (PSTN), digitální sítě integrovaných služeb (ISDN), inteligentních sítí (IN) a veřejných pozemních mobilních sítí (PLMN) [4].

Jedná se pravděpodobně o nejdůležitější prvek z pohledu kvality služby, jelikož poruchy na SS7 mají téměř vždy dopad na QoS (Quality of Service). Špatně nastavené uzly mohou účastníkům omezit služby, jelikož ztráta jednoho signalizačního spojení by teoreticky mohla snížit kapacitu sítě o tisíce hovorů. Proto je síť extrémně spolehlivá a odolná. Zařízení musí mít dostupnost 99,999%, kterou dosahují třemi hlavními způsoby: obsahují protokol pro spolehlivé doručování zpráv, samoopravné kódy a robustní fyzickou síť. Pracují s 20 až 40% zatížením a mají plnou redundanci síťových prvků. Jedná se tak o jednu z nejrobustnějších a nejspolehlivějších existujících sítí.

### ■ 3.1.1 Architektura

Sít se dělí na dvě nezávislé úrovně: národní a mezinárodní. Uzly v síti se nazývají signalizační body (SP - Signaling Points) a jsou adresovány 14 bitovým číslem zvaným bodový kód (PC - Point Code). Na národní úrovni je PC unikátní pouze v rámci sítě jednoho operátora. Na mezinárodní úrovni jsou PC jedinečné v rámci celé sítě. SP jsou propojeny signalizačními linkami. Obvyklá šířka pásma je 64kbps. K zajištění větší šířky pásma a/nebo pro redundanci lze mezi dvěma SP použít až 16 linků. Z důvodu správy a sdílení jsou linky mezi SP logicky seskupeny a nazývají se linkset. Trasy jsou předurčené cesty mezi zdrojem a cílem a zajišťují se staticky v každém SP. Neexistují žádné mechanismy na dynamické zjišťování tras [4, 5].

V síti rozlišujeme 2 typy uzlů, kdy každý má rozdílnou funkcionalitu. **SP** – zdroj/cíl zprávy. Vytváří nebo přijímá zprávy, ale nestará se o směrování. Pokud přijme zprávu s PC, který se s jeho adresou neshoduje, tak ji zahodí. **STP** – stará se o přenos signalizačních zpráv mezi uzly sítě. Tedy zprávy přijme na jednom spoji a přepoše je na jiný.

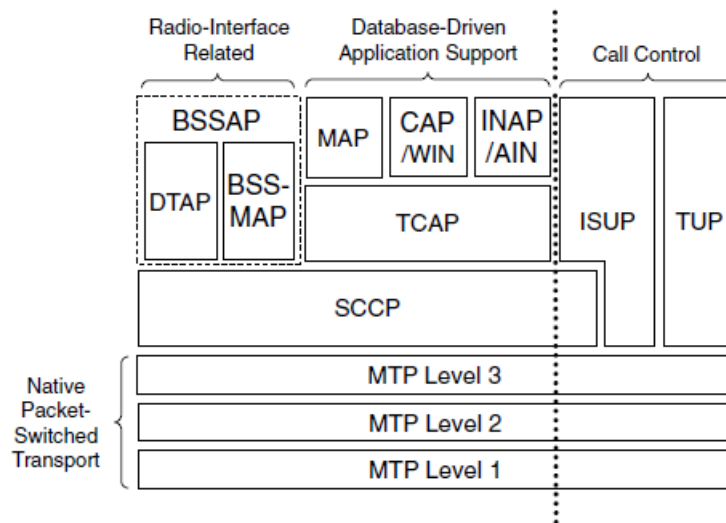
### ■ 3.1.2 Přehled protokolu SS7

SS7 se používá různě dle typu služby. Jiné použití má v celulárních sítích nebo v inteligentních sítích, zda se používá přes IP, nebo zda využívá jinou síť. Proto se zavedl pojem tradiční SS7, která má přehledně definovaný vrstvý model a obsahuje používané protokoly od 80. let až do současnosti.

### ■ MTP (Message Transfer Part)

Zahrnuje funkce pro přenos informací z jednoho uzlu do druhého. Přenáší signalizační zprávu ve správném pořadí bez ztráty nebo duplikace informace. Poskytuje spolehlivý přenos a doručení signalizačních zpráv.

MTP 1 odpovídá fyzické vrstvě referenčního OSI modelu. Signalizační datový okruh se realizuje dvěma analogovými nebo digitálními přenosovými kanály v opačných směrech (full duplex) s minimální rychlostí 4,8 kbit/s. Za standardní přenosovou rychlost je považováno 64 kbit/s. Využívá se jeden timeslot na lince E1. Při vysoké zátěži může použít i celou linku E1 (2 Mbit/s).



**Obrázek 3.1:** Vrstvový model SS7 [4]

MTP 2 je shodná spojové vrstvě OSI modelu. Zajišťuje spolehlivý přenos signalizačních zpráv, které zapouzdřuje do SS7 paketů s proměnnou délkou. Tyto pakety se nazývají signální jednotky (SU - Signal Unit). Monitoruje chyby linek a provádí korekci chyb opakovaným přenosem a řízením toku dat.

Síťová vrstva MTP 3 vykonává dvě funkce. Příchozí zprávy doručuje do uživatelské části a odchozí směřuje k jejich příjemci. Každá zpráva obsahuje PC zdrojového a cílového uzlu, podle kterých se provoz směřuje. Druhou činností je monitorování linksetů a routesetů a poskytování statusu uzlům. V případě poruchy přesměruje přenos a provede nápravná opatření [4, 5].

## ■ TUP a ISUP

Telephone User Part (TUP) a ISDN User Part (ISUP) [4] jsou protokoly poskytující signalizaci při spojování okruhů. Nastavují, udržují a ukončují hovory. TUP podporuje pouze analogové volání, a proto byl nahrazen ISUP protokolem, který podporuje analogové i digitální volání a má větší flexibilitu a řadu dalších funkcí, jako např. službu automatického zpětného volání, identifikaci telefonní linky. Používají se k provádění signalizace meziswitchového volání.

## ■ SCCP

Protokol SCCP obsahuje mechanismy pro přenos dat přes síť SS7, poskytuje flexibilnější způsoby směrování a funkce pro správu aplikací. Používá se ke komunikaci s databázemi. Další využití nachází při připojování rádiových komponent v buňkových sítích, např. přenáší dotazy a odpovědi mezi registrem lokace návštěvníka (VLR) a domovským lokačním registrem (HLR). Primárním důvodem přenosu je aktualizace HLR, aby předplatitel mohl přijímat příchozí hovory.

Směrování globálního názvu (GT - Global Title) je označení pro rozšířené směrování. Zamezuje uzlům mít velké směrovací tabulky, které by bylo obtížné zajistit a následně udržovat. GT je číslo adresáře, které slouží jako alias pro fyzickou síťovou adresu. Je složeno z PC a čísla subsystému. Centralizované STP se používají k převodu GT adresy na fyzickou adresu [4].

## ■ TCAP

Protokol umožňující subsystémům komunikovat navzájem přes SS7 síť pomocí dohodnutých datových prvků, tzv. komponent. Na komponenty lze nahlížet jako na instrukce odesílané mezi aplikacemi. Zajišťuje správu transakcí, což umožňuje spojit více zpráv [4].

## ■ 3.2 INAP

Intelligent Network Application Protocol (INAP) je signální protokol pracující nad TCAP. Zprávy obsahují informace vyměňované mezi funkčními bloky, zejména mezi SSP, inteligentními periferiemi a centralizovanou síťovou databází. Nestará se o bezchybný přenos zpráv, opravy chyb nebo sledování stavu dialogu. O to všechno se starají protokoly SS7. Neposílají se samostatné zprávy, ale zprávy následované určitým řádem, tzv. dialogem, který je definován v distribuované funkční rovině [6].

Pomocí INAP se definuje např. služba jednoho čísla, služba osobního přístupu, služba nerušit a virtuální privátní síť.



## 3.3 CAP

CAMEL Application Part (CAP) [7] je signalizační protokol pracující nad TCAP. Používá se k připojení mobilní sítě do IN a poskytuje pokročilé telekomunikační služby, jako např. Call screening, VPN, přesměrování hovorů. Pravděpodobně nejdůležitější charakteristikou je aspekt mobility. Poskytovatel může účastníkům nabízet služby jak v domácí síti, tak i při roamingu v jiných sítích.

Jeho potřeba rostla s vývojem GSM, protože předtím byla IN používána hlavně pro pevné sítě, jako PSTN a ISDN. S potřebou pokročilejších služeb, než které byly definovány v GSM, začali operátoři používat stávající standardy, které měly spoustu nedostatků pro mobilní síť, např. nebyl definován roaming. Za účelem vyřešení problémů byl ETSI specifikován nový řídicí protokol CAMEL a aplikační protokol CAP, který implementuje prakticky stejné postupy jako INAP.

## 3.4 SIP

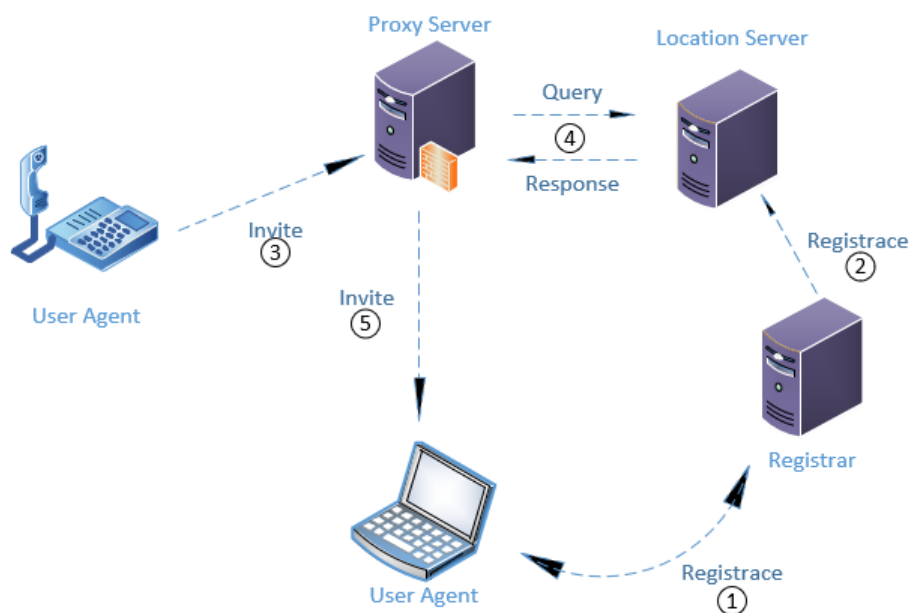
SIP (Session Initiation Protocol) [8] je nejběžnější protokol používaný ve VoIP technologii. Nachází se v aplikační vrstvě a pracuje ve spojení s dalšími protokoly. Řídí relace multimediální komunikace přes internet.

Jedná se o signalizační protokol používaný k vytvoření, upravení a ukončení multimediální relace přes internetový protokol. Jako relace se zde označuje jednoduché volání mezi dvěma koncovými body, což může být telefon, notebook, atd. Model systému je klient-server. Byl navržen velmi jednoduše s omezenou sadou příkazů. Je textový, takže kdokoliv dokáže přečíst SIP zprávu předávanou mezi koncovými body. Vychází z HTTP ze kterého převzal URI (Uniform Resource Identifier) a ze SMTP převzal schéma kódování a styl hlavičky. Využívá protokol SDP (Session Description Protocol), který popisuje relaci a protokol RTP (Real Time Transport Protocol) k doručování hlasu a videa přes IP síť. Kromě relace dvou stran (Unicast) umí založit i multiparty (Multicast). Další využití nachází v přenosu souborů, zasílání zpráv, videokonferencích a online hrách. [9]

### ■ 3.4.1 Síťové prvky

Síť je tvořena prvky, kde každý prvek je identifikován SIP URI, který slouží jako adresa. Prvky se dělí následovně:

- User Agent
- Proxy Server
- Registrar Server
- Redirect Server
- Location Server



**Obrázek 3.2:** Role síťových prvků při vytváření spojení [9]

#### ■ User Agent

Jedná se o koncový bod a jeden z nejdůležitějších prvků v síti. Může zahájit, upravit nebo ukončit relaci. Jedná se o nejinteligentnější zařízení SIP sítě. Může to být mobilní telefon, notebook nebo pevný telefon.

Logicky se dělí na dvě části, dle modelu server-klient:

- User Agent Client (UAC): prvek který posílá žádosti a přijímá odpovědi.
- User Agent Server (UAS): prvek který posílá odpovědi a přijímá žádosti.

### ■ Proxy Server

Síťový prvek, který přijímá požadavek od User Agenta a předává ho jinému uživateli. V zásadě se podobá routeru. Obsahuje inteligenci k porozumění požadavku a pomocí URI ho směřuje dále v síti. Je umístěn mezi dvěma User Agenty, avšak mezi zdrojem a cílem může být maximálně 70 proxy serverů [10].

Existují tři typy proxy serverů:

- Stateless Proxy Server: jednoduché směrování přijatých zpráv. Neukládá si žádné informace o hovorech nebo transakcích.
- Stateful Proxy Server: sleduje každou přijatou žádost a odpověď. V případě potřeby ji použije v budoucnu. Například může znovu poslat žádost, není-li z druhé strany včasná odezva.
- B2BUA (Back-to-back user agent): ústředna, která se stará o veškerou signalizaci. Nepřeposílá zprávy, ale zpracovává je – sama si zakládá hovory s volající a volanou stranou (jeví se jako terminační bod hovoru). Je univerzálnější a chytřejší, ale pomalejší.

### ■ Registrar Server

Přijímá registrační žádosti od user agentů. Autentizuje je, ukládá jejich URI a umístění do databáze, což pomáhá dalším serverům ve stejné doméně.

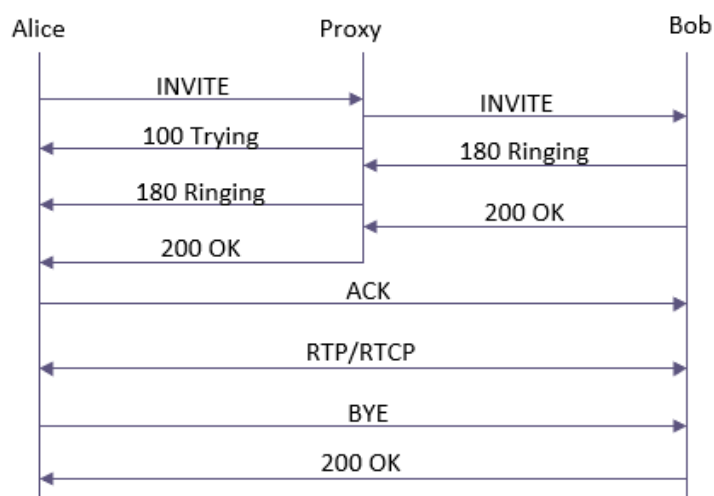
### ■ Redirect Server

Přijímá žádosti a vyhledává koncového příjemce požadavku v databázi vytvořené registrátorem.

## ■ Location Server

Poskytuje informace o umístění proxy a redirect serveru. Současně pouze tyto servery ho můžou kontaktovat.

### ■ 3.4.2 Základní tok volání



Obrázek 3.3: Základní tok volání [9]

## ■ 3.5 PINT, SPIRITS

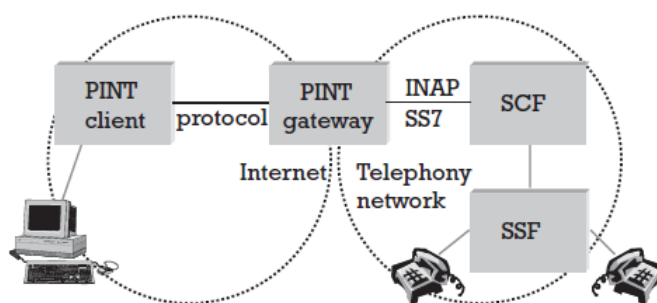
PINT (Public Switched Telephony Network Internet Internetworking) je protokol standardizovaný k interakci chytré sítě a Internetu [2]. Použit se dá např. na webové stránce, na které je umístěno vytáčení tlačítka. Přijímaná strana pomocí přihlášení nebo cookies dostane veškeré informace o volajícím.

PINT specifikuje internetový protokol, nikoli služby a obsahuje několik referenčních scénářů:

1. Click-to-dial, scénář požadující nastavení telefonního hovoru přes Internet.

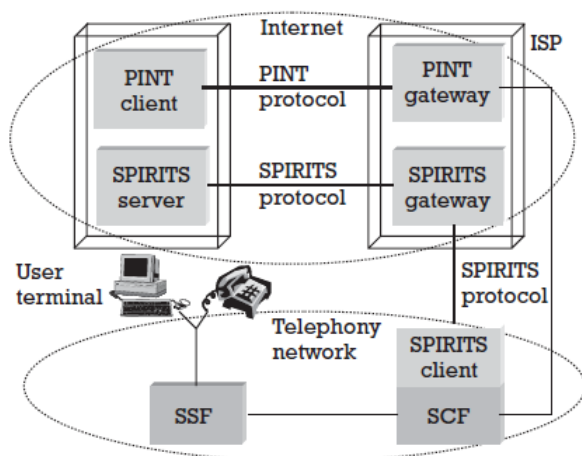
2. Click-to-fax, scénář k odeslání faxu přes Internet. Obsah faxu může být napsán na stránce nebo přiložen v souboru.
3. Click-to-fax-back, totožné s předchozím scénářem rozšířený o zpětné zaslání faxu žadateli o službu
4. Voice-access-to-content, požaduje přístup k hlasovému obsahu na internetu. Hlasový server čte informace uživateli.

Architektura je jednoduchá a skládá se pouze ze dvou prvků. PINT klient je software hlasové služby a PINT brána, která dotazy převádí na SS7 požadavky pro telefonní síť.



Obrázek 3.4: PINT architektura [2]

SPIRIT (Services in the PSTN/IN Requesting Internet Services) protokol slouží k obrácenému scénáři oproti PINTu. [2] Tedy žádost jde z chytré sítě do internetu. Příchozí hovor se volané straně zobrazí jako zpráva na počítači a v závislosti, co chce s hovorem udělat, ho může odmítnout, přeměrovat nebo přijmout. Uživatel musí mít na počítači nainstalovaného PINT klienta a SPIRIT server, obvykle malá aplikace poskytovaná operátorem.



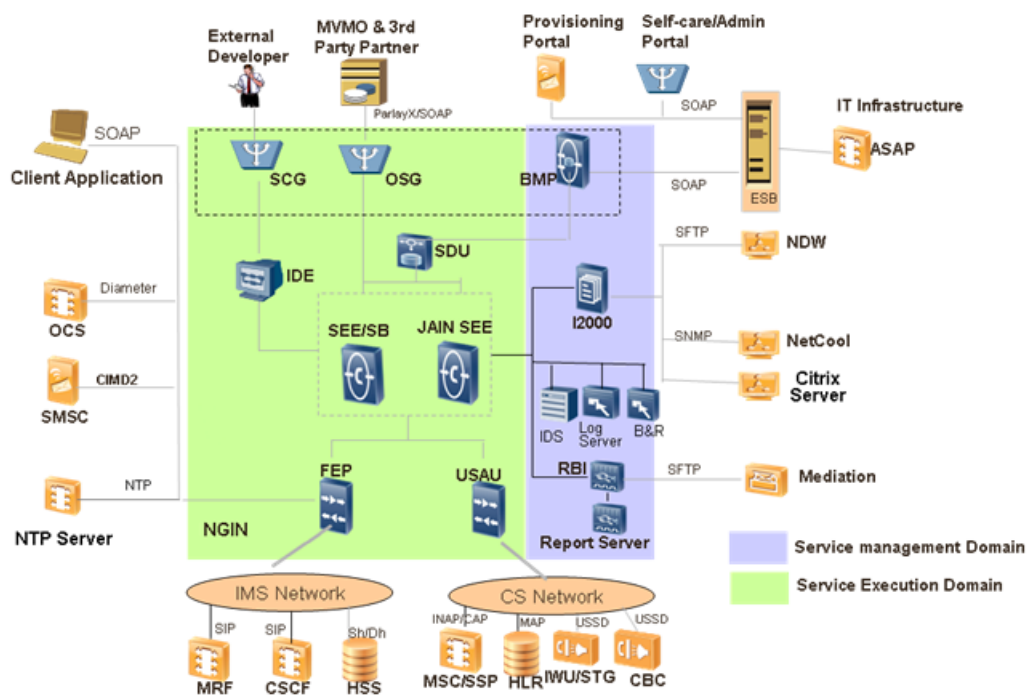
Obrázek 3.5: SPIRIT architektura [2]



# Kapitola 4

## Původní platforma

Platforma poskytuje konvergentní řešení pro poskytování služeb s přidanou hodnotou. Podporuje PSTN, GSM, 3G a IMS sítě.

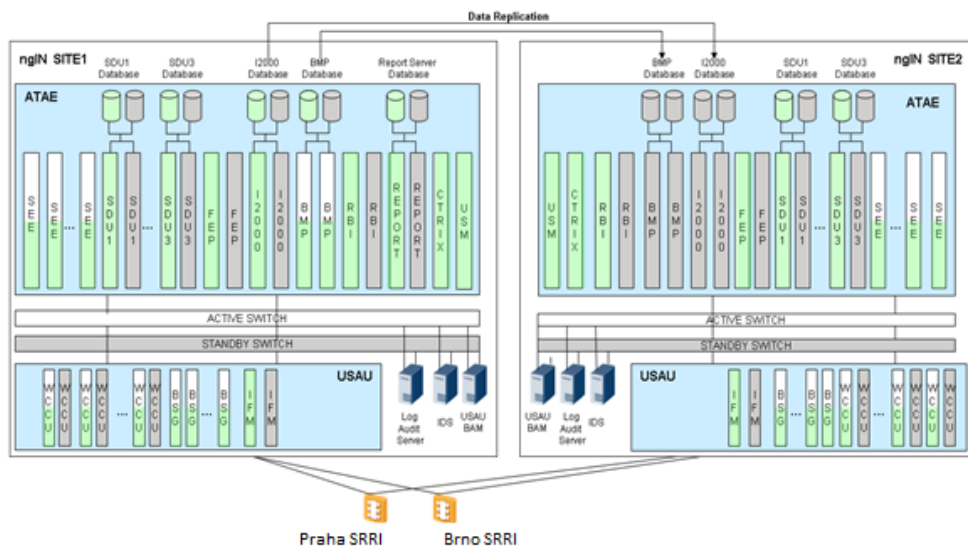


Obrázek 4.1: Přehled platformy [11]

Dle funkčnosti je rozdělena do čtyř logických domén. Front-end doména představuje přístupový bod pro jádro sítě a externí funkční entity. Obsahuje Front End Processor (FEP) a Uniform Signaling Access Unit (USAU). FEP

je přístupový bod IP protokolu. Má na starosti správu komunikace s vnějšími entity. Distribuuje přijaté zprávy do SEE/Service Brokeru a posílá data do externích systémů. USAU je přístupový bod SS7 sítě. Podporuje protokoly SS7 a SIGTRAN. Back-end doména tvoří jádro platformy. Skládá se ze SEE (Service Execution Environment), ve kterém se nasazují a běží služby. Service Broker je primární rozhraní ze sítě. Zpracovává příchozí požadavky, lokalizuje aplikaci, provádí převod protokolu, koordinuje procesy a doručuje požadavky do SEE. Poslední částí je SDU (Service Data Unit), centrální úložiště pro uživatelská data. Expoziční doména vystavuje funkcionality uživatelům, vývojářům nebo třetím stranám. Přes SCG/OCG se přistupuje k funkcím vytváření služeb a BMP (Business Management Point) vystavuje rozhraní pro podporu samoobsluhy. Poslední management doména slouží ke správě služeb, zařízení, předplatného a předplatitelů. I2000 poskytuje GUI pro správu prvků. Zodpovídá za topologii, směrování, software, konfiguraci, atd. RBI shromažďuje EDR ze SEE a přeposílá je do mediačního systému. Reportovací server analyzuje EDR záznamy. IDS detekuje škodlivou aktivitu na platformě jako je útok odmítnutí služby nebo skenování portů. Monitoruje síťový provoz a brání jakémukoli pokusu o proniknutí do systému [11].

## 4.1 Design sítě



Obrázek 4.2: Design sítě [11]

Na obrázku 4.2 jsou zobrazeny dva servery označené jako SITE 1 a SITE 2. Každý je umístěn v jiné lokaci a jsou redundantní. Mechanismus používaný ke geografické redundanci je režim sdílení zátěže, kdy se provoz rozděluje mezi servery rovnoměrně. Na tomto základě sdílejí všechny služby stejný zdroj.

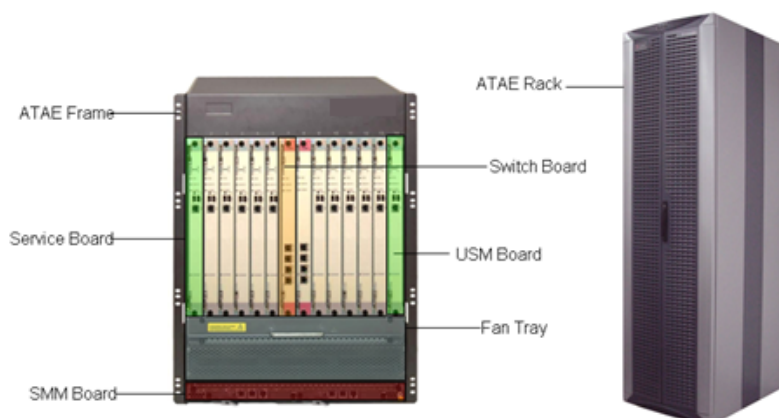


Zdroj HW lze dynamicky distribuovat mezi všechny služby, což zajišťuje jeho optimální využití. Každý site má svůj vlastní USAU a FEP, které jsou sdíleným přístupovým bodem pro SEE. Lokální SEE pracují v režimu sdílení zátěže a USAU distribuují hovory do SEE v round-robin režimu. Také mají BMP a I2000, které pracují v aktivním pohotovostním režimu. Současně je aktivní pouze jeden BMP a jeden I2000, které spravují všechny prvky na obou sitech. V případě, že BMP na jednom site vypadne, aktivuje se BMP na druhém a začne přijímat a zpracovávat požadavky z dohledových systémů. Shodně funguje také I2000.

## 4.2 Hardware

### 4.2.1 ATAE

Rozšířené telekomunikační aplikační prostředí (ATAE) je platforma pro zpracování třídy nosiče, která je navržena tak, aby splňovala požadavky na aplikaci služeb tříd operátora.



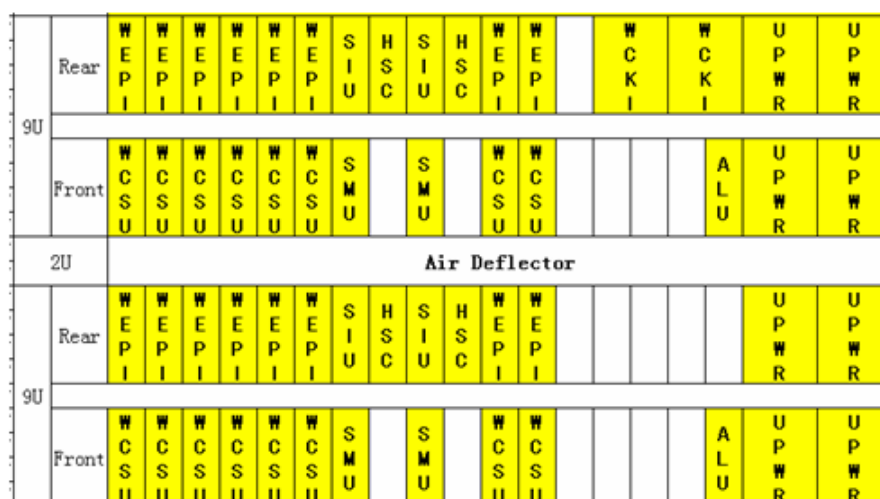
Obrázek 4.3: HW prvky [12]

ATAE stojan slouží k uchycení ATAE rámců. Maximálně pojme 2 rámy. Má děrované přední dveře, pevnou zadní stranu a perforovanou horní stranu s aktivní ventilátorovou jednotkou. ATAE rám zajišťuje komponentám napájení, propojení, odvod tepla a funkce správy. Maximálně pojme 12 slotů pro service boardy, 2 sloty pro switch boardy a 2 sloty pro SMM. Service board je deska, na které je nainstalovaná platforma a služby NGIN. Specifikace desky jsou: 2x CPU Xeon Due, 16GB RAM, 2x 148GB SAS pevné disky, 1 sériový port a 6 GE portů. Switch board se stará o síťové směrování, má 24 GE portů

a 16 optických portů. SMM board monitoruje zařízení, napájení a integruje alarmy do I2000. USM board centralizovaně řídí ATAE komponenty. Podporuje grafická rozhraní pro monitorování a správu ATAE rámu, síťového systému, úložného systému, operačního systému a servisních desek [12].

#### 4.2.2 USAU HW

USAU hardware je rozdělen do tří vrstev: stojan, rám, deska. Má přední a zadní typ desky. Mezi přední desky patří poplachová deska (ALU), přepínací deska (SMU) a deska WCSU. Mezi zadní desky SIU, HSC, BFI a EPI. Z obou stran jde zapojit napájecí deska (UPWR).



Obrázek 4.4: Prvky USAU HW [12]

ALU (Alarm Unit) monitoruje stavy všech desek včetně napájecího modulu a posílá hlášení o chybových informacích. EPI slouží jako zadní deska pro WCSU. Poskytuje fyzická rozhraní pro SS7 signalizaci. HSC (Hot-Swap and Control Unit) ovládá hot-swap desky a přepínání ethernetové sběrnice v rámu. SIU (System Interface Unit) je vázaná na SMU. Poskytuje ethernetové rozhraní a sériové porty. SMU (System Management Unit) je hlavní řídicí deska servisních rámců. UPWR (Universal Power Board) zajišťuje rámcům napájení. WCSU (Widely Calling Control Unit and Signaling Process Unit) zpracovává zprávy MTP2, MTP3 a aplikační vrstvy přes SS7. Následně je přenáší prostřednictvím TCP/IP do SEE [12].

### ■ 4.2.3 Škálovatelnost

Výměna hardwaru v případě selhání nebo aktualizace desky nemá vliv na existující data, protože ta jsou uložena v nezávislém souborovém systému a databázi. Upgrade firmware probíhá uzel po uzlu, nejprve se aktualizuje pohotovostní uzel, poté se přepne provoz a následuje aktualizace aktivního uzlu.

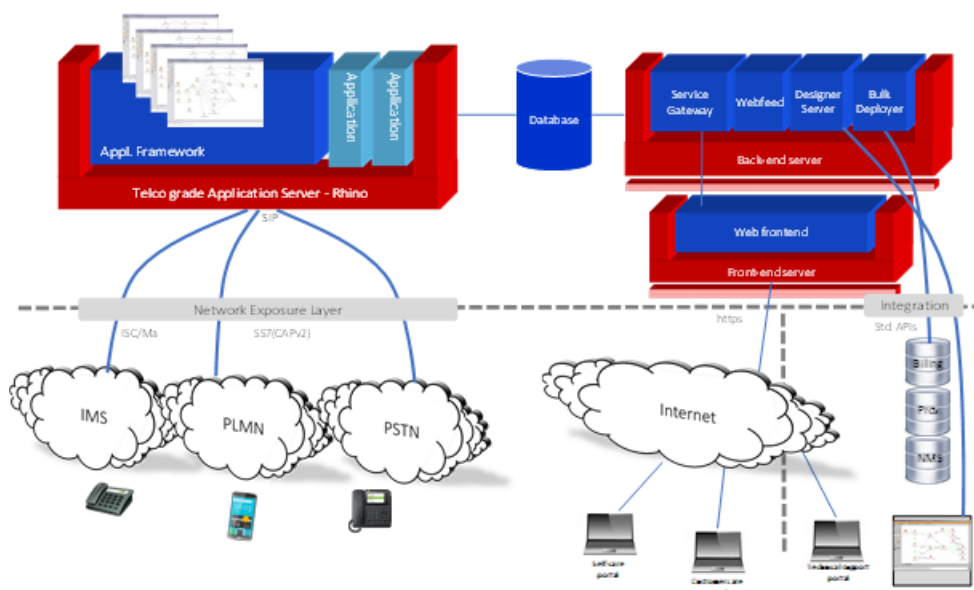
Rozšíření systému umožňuje zvládat rostoucí zatížení systému nebo zavádět nové služby. Je možné rozšiřovat dvěma směry. V horizontálním přidáváme další desky do rámu. V případě plného rámu přidáme další rám a nebo celou skříň. Vertikálně zvyšujeme výkon a kapacitu desek přidáním pamětí a dalších procesorů, popřípadě nahradíme stávající výkonnějším.



## Kapitola 5

### Nová platforma

Architektura je rozdělena na dvě části. Levá telekomunikační strana realizuje funkce zpracování hovorů v reálném čase a pravá internetová strana poskytuje různá uživatelská rozhraní a integraci do externích systémů. Uprostřed je databáze poskytující údaje o zákaznících a relacích.



**Obrázek 5.1:** Architektura platformy [13]

Každá strana je postavena na horizontálním vrstevném modelu, kde vrstvy jsou na sobě nezávislé. Vrstva síťové expozice umožňuje aplikacím přístup k základním síťovým prostředkům a základním sítím přístup k funkcím platformy. Nabízí abstrakci různých síťových technologií a mechanismů. Aplikací

server poskytuje prostředí k provádění servisních aplikací a zjednodušuje jejich integraci a nasazení. Jedna z aplikací se používá pro vyřizování hovorů. Přes vrstvu síťové expozice přicházejí na komponentu hovory, ta si načte data z relační databáze a provede danou službu. Servisní aplikace implementuje základní funkční logiku síťovým prvkům a různým typům uživatelů, např. koncovému uživateli, správci nebo poskytovateli služeb [13].

Používá SIP jako základní protokol pro veškerý přenos v reálném čase. Ostatní protokoly, jejich operace a významné parametry, jsou převedeny do SIP zpráv. K určení, jaká servisní strategie se má vyvolat, se používají primární parametry SS7 servisní klíč a detekční bod, viz. tabulka 5.1. V případě protokolu CAP se extrahují ze zprávy InitialDP a přidávají se jako proprietární SIP záhlaví.

servisní klíč	typ hovoru	protokol	popis
505	příchozí	CAP	Příchozí VPN hovor
500	odchozí	CAP	Odchozí VPN hovor
525	příchozí	SIP	Příchozí VPN hovor
700	odchozí	SIP	Odchozí NTS hovor

**Tabulka 5.1:** Příklady servisních klíčů [13]

## 5.1 Design platformy

Z bezpečnostních důvodů je signalizační doména oddělena od internetové domény firewallem. Komponenty provádějící hovory nejsou závislé na ostatních částech provádějících směrování, nastavení nebo statistiky.

Systém je nadimenzován tak, aby každý modul pracoval s maximálně 50% zatížením. Všechny nasazené moduly jsou redundantní a fungují v režimu sdílení zátěže. Chyby se automaticky detekují na systémovém modulu, komponentě nebo serveru a provoz je následně přesměrován na funkční část. Systém je postaven na technologii VMware. Jeho celková kapacita může být lineárně navýšena přidáním dalšího hardwaru nebo softwaru, tj. nasazením nových virtuálních strojů.

Signalizační brány pracují v režimu active - active. Může být nakonfigurována jako jeden logický bod s jedním point kódem nebo jako množina nezávislých bodů každý s vlastním point kódem. Operátorovi to umožňuje konfigurovat sdílení zátěže nebo kritéria při selhání.

Aplikační servery pracují v režimu active - active a jsou postaveny na operačním systému Linux nebo Sun. Síťová redundance je ovládána z OS.

Databáze pracují v režimu active - standby. Platforma automaticky přepne na standby databázi, když se na aktivní objeví chyba nebo je nedostupná.

Webové servery pracují v režimu active - active. Sdílení zátěže je požadováno pro distribuované načítání webových aplikací.

Celková architektura umožňuje plnou redundanci sítí. Množina všech funkčních komponent je z důvodů bezpečnosti, výpadků, 99,999% dostupnosti služby geograficky redundantní. Pracuje v režimu active - active. Konfigurace nemá single-point-of-failure a umožňuje výpadek celého jednoho situ, kdy druhý převezme veškerý provoz.

Typ serveru	Testovací prostředí	Předprodukční prostředí	Produkční prostředí
Aplikační server	2	2	5
Signalizační server	2	2	3
Databáze	3	3	3
Webové servery	1	2	2

Tabulka 5.2: Přehled redundance serverů [13]

## 5.2 Výhody oproti původní platformě

Největší rozdíl je virtualizace, která přináší mnoho výhod, jakými jsou nezávislost na hardwaru dodavatele, snazší a levnější rozšiřování, jednodušší zavádění nových služeb a lepší využití výpočetních zdrojů.

Dalšími výhodami jsou: nativně SIPová technologie podporující všechny hlasové přístupové technologie a prostředí (CAP, SIP-ISC interface, atd.). To umožnilo ze sítě vyřadit staré INAP ústředny a tím ušetřit za provoz. Většina operátorů uvažuje i o vypnutí starých 2G a 3G sítí s CAP protokolem. Služby jsou fixně-mobilní, jsou nezávislé na koncovém zařízení a sítích.

Požizovací náklady se pohybují v desítkách milionů korun, ale oproti původní platformě byly 10x menší. Také provozní náklady jsou díky virtualizaci nižší. Vize do budoucna je přemigrovat všechny hardwarové platformy do jedné softwarové a co nejvíce snížit provozní náklady společnosti.

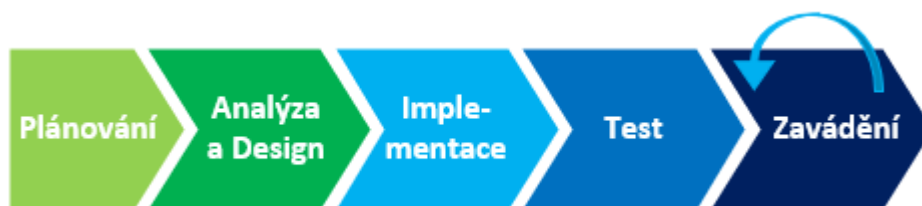




## Kapitola 6

### Fáze implementace a migrace

Postup migrace je rozdělen do několika fází, viz. obrázek 6.1. Probíhá za provozu a z důvodu snížení rizik je lepší fázi zavádění dělat po dílčích částech, což je znázorněno smyčkou.



Obrázek 6.1: Fáze migrace [14]

#### 6.1 Fáze plánování

Podrobné plánování následujících fází migrace založené na analýze požadavků a dat. V analýze se řeší integrace platformy s cílovými portály OSS/BSS a telekomunikačním prostředím. U dat se zaměřuje na parametry, které mají být převedeny (např. volitelný nebo povinný parametr) a zvažuje se jejich důležitost pro služby na nové platformě [14].

Probíhá zde úzká spolupráce mezi zúčastněnými stranami, aby se dosáhlo společného objasnění technických požadavků a postupů. Podrobně se popisuje

organizace projektu, milníky, kritéria, atd. Výstupem je High Level Design (HLD) dokument, s kterým se pracuje v následujících fázích.

## 6.2 Fáze analýzy a návrhu

Zaměření se na detailní návrh, závěrečné analýzy a upřesnění požadavků. Klade se důraz na analýzu migračních dat, integraci s cílovými portály OSS/BSS a telekomunikačním prostředím. Důkladně jsou rozpracovány integrační nástroje a návrh bezpečnostního řešení.

Podrobně jsou vyjasněny tyto body. U migrovaných dat je sladění datový model služeb na staré a nové platformě, definován proces pro export dat (API, rozhraní, výkon, atd.), vytvořen koncept nouzového scénáře, objasněný dopad na původní systém a služby na něm běžící. Je hotový průzkum sítě a potenciální dopady na externí systémy (správa alarmů, účtovací systém). Známe integrační proces migračních nástrojů a zabezpečení. Důsledky pro stávající platformu jsou zhodnoceny, jsou porovnány různé strategie (Big-drop vs. postupné kroky) a jsou známy a zhodnoceny rizika [14].

Po této fázi je dokončen Low Level Design (LLD), který obsahuje specifikace návrhu migrace včetně pracovních skupin a zdrojů.

## 6.3 Implementační fáze

Cílem je implementovat potřebné nástroje, ověřit jednotlivé kroky a otestovat moduly. Dokončují se pravidla pro transformaci dat mezi službami a zákaznickými informacemi starých a nových platform. V závislosti na implementační strategii se posuzují potenciální dopady na externí systémy a portály [14].

Zahrnuje témata jako např. konečná definice postupu integrace a migrace, pravidla transformace služeb a zákaznických dat, zohledňuje přetížení během migrace a dopady na systémy inteligentní sítě, detailní plánování sítě, atd.

## 6.4 Fáze testování

Po úspěšném testování modulů se provádí testy v laboratoři výrobce. Provedeny budou mimo jiné tyto činnosti a testy: test kompletní procedury s anonymními daty, optimalizace procedury na základě výsledku a test nouzového postupu. Zkoušky poskytnou první výsledky prováděného postupu a migračních nástrojů.

Následují integrační a end-to-end testy v testovací síti operátora. Kompletní procedura se testuje na reálných datech a optimalizuje se postup na základě výsledků.

Specifikuje se explicitní migrační pilot. Pilotní fáze začíná s omezeným počtem účastníků služeb ještě před hromadným zaváděním. Umožňuje to ověřit nové provozní procesy, individuální procesy a procedury, reakci řešení v reálném prostředí a zatížení [14].

Na konci této fáze se vydává migrační procedura a tím je všechno připraveno na zavádění do sítě.

## 6.5 Migrace

Reálné zavádění do produkční sítě se provádí během dohodnutého servisního okna (např. v noci, o víkendu). V tomto období jsou zákazníkovi zakázány jakékoliv modifikace dat (tzv. zmrazení), čímž se zajistí, že nedojde ke ztrátě dat. Samotná služba však zůstává plně funkční [14].

Kompletní migrace začíná exportováním dat ze staré platformy a změnou formátu pomocí transformačních pravidel. Upravená data se nahrají na novou platformu. Připraví se směrování a řídicí systémy (HLR, OSS, BSS). Následuje přepnutí provozu a synchronizace systémů. Regresivním testováním se ověří funkcionality migrovaných služeb a rozhodne se o úspěchu, nebo neúspěchu.



## Kapitola 7

### Služby běžící na platformě

V síti je provozováno několik platforem. V první fázi se migrovala pouze platforma popsaná výše a proces byl rozdělen do dvou částí. Nejprve se na konci roku 2019 převáděla služba virtuální privátní síť a po jejím úspěšném dokončení následovala na začátku roku 2020 služba překladu čísel. Druhá fáze je naplánovaná na rok 2021, kdy se bude rušit platforma provozující službu virtuální ústředna. Do budoucna se předpokládá integrace dalších služeb z ostatních platforem.

#### 7.1 Služba překladu čísel

Služba překladu čísel (NTS - Number Translation Service) [15] překládá pomocí dynamického překladu vytáčené číslo na telefonní číslo, které je skryto před volající stranou. Klíčovou funkcí služby je individuální plán směrování plně řízený ze samoobslužného portálu předplatitelem služby. Směřuje se podle kritérií jako je například oblast původu, datum a čas, atd. Služba založená na platformě je pro pevné a mobilní sítě konvergentní a podporuje typy IFS, PRM, UAN a zelená linka.

Mezinárodní bezplatná služba (IFS - International Freephone Service) - umožňuje uživateli volat bezplatně vytočením národního čísla 800, univerzálního adresáře 00800 nebo národního specifického bezplatného přístupového čísla ze zahraničí, která jsou nakonec přeložena a směrována na cílová čísla. Poplatek za volání se účtuje předplatiteli služby.

Univerzální přístupové číslo (UAN - Universal Access Number) - umožňuje uživateli volat pomocí vytočení čísla univerzálního adresáře, které je přeloženo a směrováno na cílové číslo.

Prémiová služba (PRM - Premium Rate Service) - umožňuje uživateli vytvořit konfigurovatelný hovor a zajistit sdílení výnosů s poskytovatelem obsahu.

Zelená linka - služba umožňuje uživateli volat bezplatně vytočením čísla adresáře, které je přeloženo a směrováno na číslo předplatitele služby. Ten také platí poplatky za volání.

V nedávné době bylo na platformě zprovozněno volání na linku Městské policie 156. Využívá identifikaci původu volání k překladu čísla na nejbližší policejní stanici. Služba je provozována pro volání na linku z fixních i mobilních sítích všech operátorů - O2, T-Mobile a Vodafone.

## 7.2 Virtuální privátní síť

Virtuální privátní síť (VPN - Virtual Private Network) [16] označuje virtuální komunikační prostředí v rámci společnosti. Umožňuje organizaci použít stávající veřejnou telekomunikační infrastrukturu, veřejnou pozemní mobilní síť (PLMN) a veřejnou telefonní síť (PSTN), jako soukromou síť. Členům nabízí rozšířené funkce jako vytáčení krátkých čísel, pokročilé směrování hovorů dle různých kritérií, omezování hovorů, black/white list, atd. Společnost má lepší kontrolu nad náklady díky schopnosti omezení příchozích nebo odchozích volání. Stejná funkce poskytuje zabezpečení, protože může blokovat různá čísla.

### 7.2.1 VPN úrovně a role

Poskytovatel služeb nastavuje konfiguraci na úrovni služby, zatímco správce VPN skupiny nastavuje konfiguraci na úrovni VPN skupiny, PNP skupiny a člena VPN. V mobilní síti je vztah jedna ku jedné mezi VPN členem a PNP, u fixní síti naopak žádný vztah není. Jeden předplatitel může mít předplatné do více VPN skupin. Jedno předplatné může mít buď fixní PNP, nebo mobilní PNP, ale nesmí mít oboje.



Obrázek 7.1: VPN role [16]

## 7.3 Virtuální ústředna

Služba Virtuální ústředna je hostovaná privátní pobočková ústředna, která zákazníkovi umožňuje využívat funkce ústředny bez nutnosti kupovat vlastní [17]. Zákazník může konfigurovat vlastní strukturu včetně různých skupin, oddělení a spravovat všechny doplňkové služby. Služba podporuje mnoho koncových zařízení: pevné SIP telefony, SIP PC klienty, POTS, ISDN2, ISDN 30 s GW, VoLTE telefony, 2G a 3G telefony, PBX.

Zákazník spravuje ústřednu pomocí webových aplikací. Administrační aplikace umožňuje konfigurovat a spravovat entity a jejich služby. V CallManageru si koncový uživatel nastavuje hovory pomocí funkcí, jako například přidržení hovoru, konference, atd. Poslední aplikací je AttendantConsole, která umožňuje sledovat stav a probíhající volání k uživatelům.

Plánuje se integrace a rozšíření s již funkční VPN. Členům virtuální ústředny umožníme funkce PBX, naopak VPN členové zůstanou nezměněni. Zákazníkům tím umožníme mít v jedné skupině centrexové, fixní i mobilní členy.





## Kapitola 8





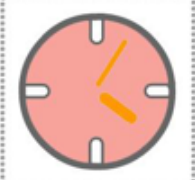


### Prostředí vytváření služeb

Součástí platformy je nástroj pro návrh a řízení služeb na platformě. Jedná se o program s grafickým rozhraním napsaný v Javě. Umí navrhovat služby, uložit nebo načíst design ze souboru, zobrazovat služby v různých formátech (JPEG, HTML, XML) a nasadit služby na platformu.

Při implementaci nové služby nebo při modifikaci stávající se postupuje podle třech základních kroků. Nejprve se v grafickém rozhraní nadefinuje servisní logika služby. Následuje nasazení služby na platformu. Aplikace obsahuje funkci na okamžité nasazení, která službu nainstaluje. Posledním krokem je testování, které může probíhat jak na reálném, tak na simulovaném provozu. V případě, kdy testy nedopadnou dle očekávání, se vracíme zpět ke kroku jedna, službu upravíme a znovu nahrajeme. Cyklicky postupujeme do doby, než dosáhneme správného výsledku.

Služby jsou modelovány jako orientované grafy, které jsou označovány jako servisní strategie. Skládají se z modulů propojených hranami. Každý modul odpovídá konkrétnímu prováděcímu kroku, zatímco hrany potenciální prováděcí sekvenci. Provedení služby je zahájeno z vyhrazeného startovacího modulu a sekvenčně se pak provádí ostatní moduly. Výsledek z aktuálního modulu určí, přes kterou hranu se bude postupovat dále. Strategie definuje všechny možné prováděcí cesty služby.

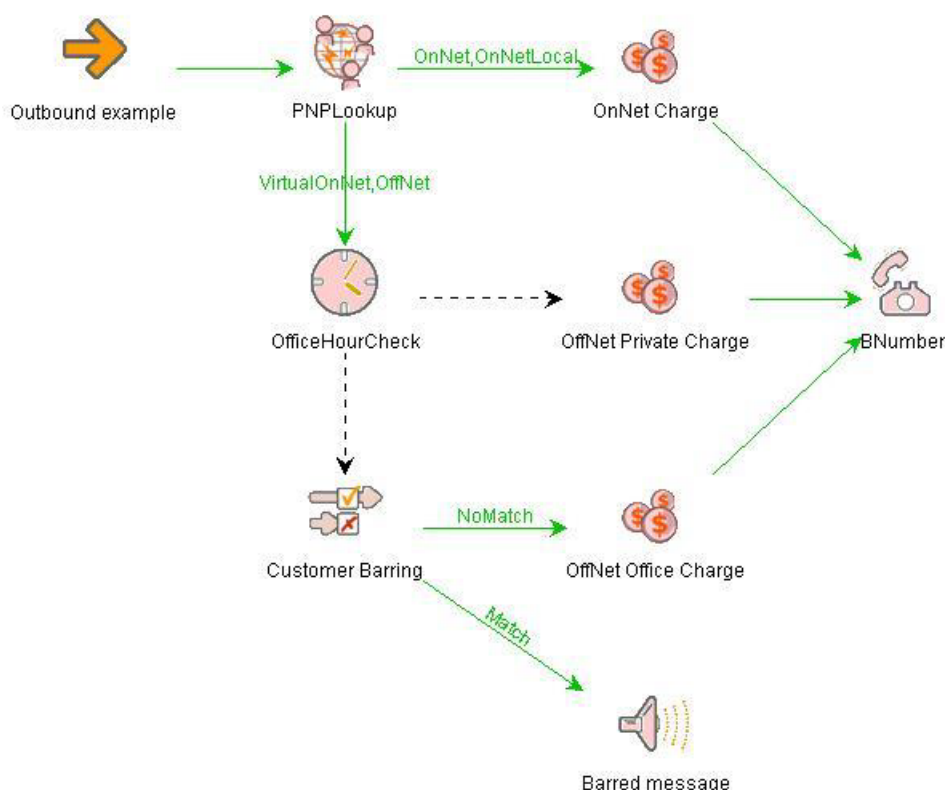
V programu jsou předefinovány moduly a funkce, které se dělí do dvou skupin. Základní skupina obsahuje funkce pro řízení hovoru. Druhou skupinou jsou webové funkce, které slouží pro spolupráci s internetem. Poslední možností je doprogramování libovolné funkce nebo modulu [18].

	<p style="text-align: center;"><b>Private Number Module</b></p> <p>Analyzuje detaily volání (volající a volané číslo) a detekuje aktuální konfiguraci. Při použití krátkého čísla se ještě přeloží.</p>
	<p style="text-align: center;"><b>Charging Module</b></p> <p>Přidává do cesty volání speciální účtovací událost. Používá se pouze tehdy, když se v odlišných cestách hovor účtuje odlišně.</p>
	<p style="text-align: center;"><b>Conference Module</b></p> <p>Na základě vstupu uživatele nastavuje konferenci.</p>
	<p style="text-align: center;"><b>Hunt Group Module</b></p> <p>Pomocí hunting listů přesměrovává hovory. Může být nadefinováno několik seznamů, které se spravují z webového rozhraní.</p>
	<p style="text-align: center;"><b>Time Module</b></p> <p>Směrování příchozích hovorů je závislé na čase a/nebo dni v týdnu.</p>
	<p style="text-align: center;"><b>Barring module</b></p> <p>Slouží k blokování odchozích hovorů. Používá k tomu black/white listy, které se definují z webového rozhraní.</p>
	<p style="text-align: center;"><b>Announcement module</b></p> <p>Přepojení hovoru k IVR nebo mediálnímu serveru. Přehraje hlasovou zprávu volajícímu a volitelně může hovor ukončit.</p>

Obrázek 8.1: Vybraný seznam modulů [18]

## 8.1 Příklad A - logika služby pro odchozí hovory

Na obrázku 8.2 je zobrazen příklad logiky služby pro odchozí volání koncových uživatelů, který se provádí, když uživatel uskuteční hovor. Účtování je odlišně stanoveno na základě povahy hovoru (v síti, mimo síť) a denní době. U mimo síťových se dále kontroluje denní doba a v úředních hodinách se ještě navíc kontroluje, zda je odchozí hovor povolen, či nikoliv.

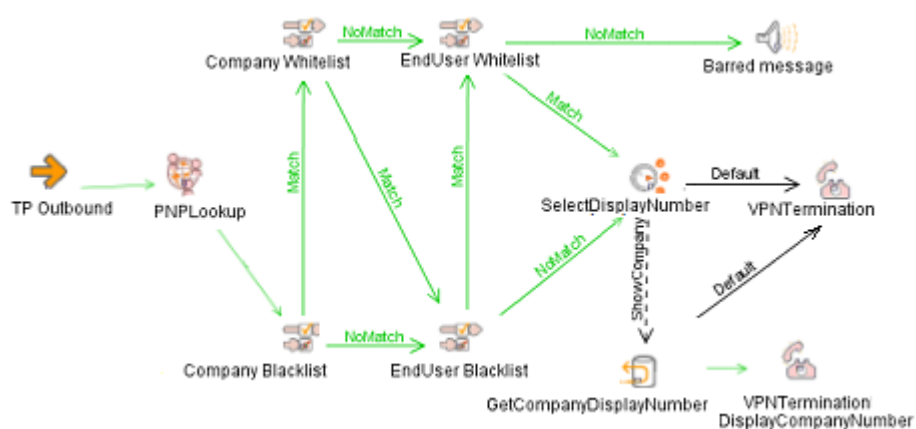


Obrázek 8.2: Logika služby pro odchozí hovory koncových uživatelů [18]

## 8.2 Příklad B - logika služby pro odchozí hovory

Druhý příklad uvedený na obrázku 8.3 zobrazuje strategii odchozího volání pro koncové uživatele. Začíná PNP modulem. Rozšíří se krátká čísla a nastaví správné účtování u hovorů uvnitř nebo mimo síť. Nejprve se zkontrolují firemní black/white listy a následně individuální uživatelské listy. Není-li hovor blokován, uživatel na voliči rozhodne, jaké číslo se zobrazí volané straně

(CLI). Tento model umožňuje výběr mezi vlastním číslem volajícího nebo hlavním firemním číslem. Nakonec dojde k uskutečnění hovoru.

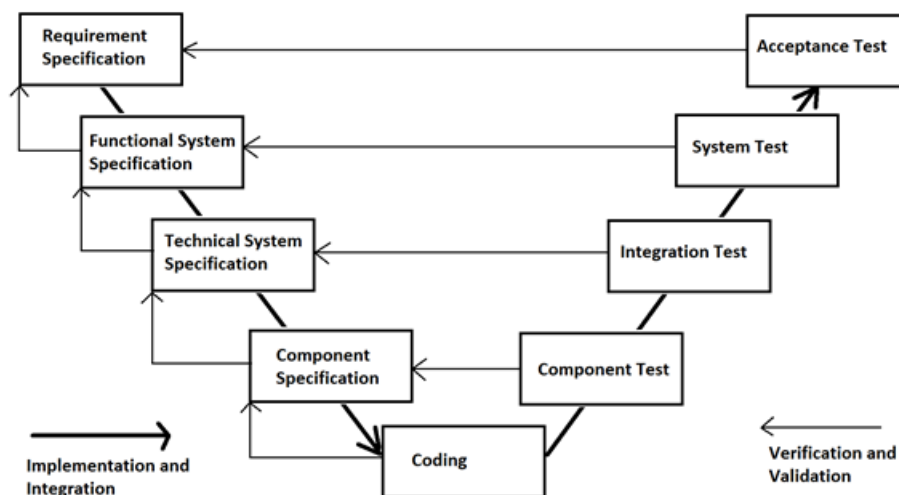


Obrázek 8.3: Strategie odchozího hovoru [18]

## Kapitola 9

### Testování platformy

Pro každou provedenou specifikaci je naplánována odpovídající testovací aktivita, která ověří její funkčnost. K tomuto účelu se používá V-model, který na levé straně ilustruje hierarchii specifikací až po kódování služby a pravá strana ukazuje testovací úrovně a jim odpovídající referenční specifikaci.



Obrázek 9.1: V model [19]

Z modelu vyplývá, že se provádějí čtyři různé úrovně akceptačního testování za účelem ověřit specifikaci a její kvalitu. FAT testy slouží k testování komponent. Provádí je dodavatel a kontroluje požadavky systému. SAT testy odpovídají integračnímu a systémovému testu. Provádí se operátorem v testovací síti a zkoumá, jestli systém jako celek splňuje stanovené požadavky a zda funguje integrace se stávajícími externími systémy. Dále zajišťuje end-to-end

test ověřující funkční chování. Provádí se zkoušky provozního chování jako je výkon, robustnost a redundance, aby se ověřila připravenost platformy. Posledními akceptačními testy jsou UAT. Provádí je operátor za účelem ověření, zda dodávka splňuje podepsanou smlouvu [19].

K testování se používají různé nástroje a aplikace, které si nyní popíšeme.

### ■ Protractor

Protractor je end-to-end testovací framework pro Angular a AngularJS aplikace. Provádí aplikační testy aplikace v prohlížeči a interaguje s ní jako skutečný uživatel. Používá se pro testování portálu [19].

### ■ Scenario Simulator

Scenario Simulator slouží ke generování CAPv2 a SIP hovorů. Pro implementaci testovacích případů používá deklarativní model. Testovací případy jsou definovány jako scénáře, které popisují simulaci od začátku do konce. Nástroj je nakonfigurován v předprodukčním a produkčním prostředí a umožňuje automatické spuštění FAT testů. Lze s ním také generovat zátěž pro testování výkonu [19].

### ■ Airdroid

Airdroid umožňuje generovat hovory pocházející z ČR [19]. 10 GSM zařízení z aplikace bude připojeno do sítě a budou generovat odchozí 2G, 3G a 4G volání.

### ■ SIP software telefon

Lze použít libovolný softwarový telefon umožňující generování SIP hovorů. Bude použito 10 testovacích telefonních čísel.

## ■ MasterClaw

Nástroj používaný k monitorování signalizace (SIP, CAP, Diameter, atd.). Poskytuje detailní tok volání, analyzuje a reportuje data [20].

## ■ Aplikační manažer

Nástroj sloužící k monitorování hardwaru, softwaru a generování alarmů. Alarmy jsou prioritně rozděleny do 5 kategorií. Kritická chyba ovlivňuje služby. Není možné akceptování a další testování je zastaveno. Majoritní chyba neumožňuje zpracování relace, účtování nebo signalizace, avšak test pokračuje. Střední chyba neprovede proces jak je definován, ale nemá žádný vliv na signalizační provoz. Např. chybné některé funkce z GUI, ale z command line jsou plně funkční. Minoritní chyba nemá vliv na provoz, ale v budoucnu bude opravena. Jedná se např. o designové chyby v uživatelském prostředí. Poslední kategorie je vylepšení, kdy se nejedná o chybu, ale o návrh na zlepšení kvality [19].

## 9.1 Výkonnostní testy

### 9.1.1 Základní zatížení na obou sitech

Test spočíval ve spuštění základního zatížení na obou sitech. Trval 12 hodin a bylo provedeno 11 milionu CAP volání, 4 miliony SIP hovorů a základní zatížení portálu a dohledu. Během testů nedošlo k žádným chybám ani zmeškaným hovorům, viz. tabulky níže.

CAP				
Site	Server	Počet hovorů	Celkem hovorů	Ztraceno hovorů
1	2	50 cps	2 219 342	0
1	3	50 cps	2 217 214	0
2	1	50 cps	2 212 510	0
2	2	50 cps	2 211 376	0
2	3	50 cps	2 211 713	0

Tabulka 9.1: Naměřená data pro CAP hovory

SIP				
Site	Server	Počet hovorů	Celkem hovorů	Ztraceno hovorů
1	1	10 cps	439 606	0
1	2	10 cps	439 600	0
1	3	10 cps	439 610	0
1	4	10 cps	439 599	0
1	5	10 cps	439 638	0
2	1	10 cps	439 845	0
2	2	10 cps	439 861	0
2	3	10 cps	439 914	0
2	4	10 cps	439 937	0
2	5	10 cps	439 961	0

Tabulka 9.2: Naměřená data pro SIP hovory



### 9.1.2 Základní zatížení na jednom situ

Test spočíval ve spuštění základního zatížení na jednom situ. Trval 12 hodin a bylo provedeno 14 milionu CAP volání, 4,7 milionů SIP hovorů a základní zatížení portálu a dohledu. Bylo zaregistrováno pouze 21 ztracených CAP volání. Na ostatních rozhraních nebyly zmeškány žádné zprávy, hovory nebo zaznamenány jiné chyby.

CAP				
Site	Server	Počet hovorů	Celkem hovorů	Ztraceno hovorů
1	2	150 cps	7 017 772	6
1	3	150 cps	7 005 577	15

Tabulka 9.3: Naměřená data pro CAP hovory

SIP				
Site	Server	Počet hovorů	Celkem hovorů	Ztraceno hovorů
1	1	20 cps	939 253	0
1	2	20 cps	938 960	0
1	3	20 cps	938 845	0
1	4	20 cps	938 697	0
1	5	20 cps	938 540	0

Tabulka 9.4: Naměřená data pro SIP hovory

### 9.1.3 Špičkové zatížení na obou sitech

Test spočíval v provedení špičkového zatížení na obou sitech. Trval 3,5 hodiny a bylo provedeno 7,6 milionu CAP volání, 1,2 milionu SIP hovorů a špičkové zatížení portálu a dohledu. Bylo zaregistrováno 15 ztracených CAP volání. Na ostatních rozhraních nebyly zmeškány žádné zprávy, hovory nebo zaznamenány jiné chyby.

CAP				
Site	Server	Počet hovorů	Celkem hovorů	Ztraceno hovorů
1	2	50 cps	1 533 265	5
1	3	50 cps	1 528 499	5
2	1	50 cps	1 526 692	5
2	2	50 cps	1 520 576	0
2	3	50 cps	1 515 838	0

Tabulka 9.5: Naměřená data pro CAP hovory

SIP				
Site	Server	Počet hovorů	Celkem hovorů	Ztraceno hovorů
1	1	20 cps	254 926	0
1	2	20 cps	254 727	0
1	3	20 cps	254 624	0
1	4	20 cps	254 486	0
1	5	20 cps	254 358	0
2	1	20 cps	247 546	0
2	2	20 cps	247 281	0
2	3	20 cps	246 978	0
2	4	20 cps	246 673	0
2	5	20 cps	246 228	0

**Tabulka 9.6:** Naměřená data pro SIP hovory

#### 9.1.4 Špičkové zatížení na jednom situ

Test spočíval v provedení špičkového zatížení na jednom situ. Trval 3 hodiny a bylo provedeno 6,3 milionu CAP volání, 1,2 milionu SIP hovorů a špičkové zatížení portálu a dohledu. Bylo zaregistrováno 107 ztracených CAP volání. Na ostatních rozhraních nebyly zmeškány žádné zprávy, hovory nebo zaznamenány jiné chyby.

CAP				
Site	Server	Počet hovorů	Celkem hovorů	Ztraceno hovorů
2	1	168 cps	2 118 822	73
2	2	168 cps	2 076 696	15
2	3	168 cps	2 079 467	17

**Tabulka 9.7:** Naměřená data pro CAP hovory

SIP				
Site	Server	Počet hovorů	Celkem hovorů	Ztraceno hovorů
1	1	20 cps	247 275	0
1	2	20 cps	247 203	0
1	3	20 cps	247 369	0
1	4	20 cps	247 380	0
1	5	20 cps	247 723	0

**Tabulka 9.8:** Naměřená data pro SIP hovory

## ■ 9.2 Testy přetížení

### ■ CAP

Kapacita DSI serveru je 32 spojů s propustností 64kbit/s. Při 60% využití se počítá s přibližně 350 CAP hovory. Když je dosaženo maxima, komponenta DSI blokuje provoz z STP a to začne směřovat provoz na jiný DSI server. CAP simulátor se při generování zátěže okolo 200 CAP hovorů stával nestabilním. Kvůli tomu jsme nedosáhli na přetížení vůči DSI serveru a test nemohl být proveden.

### ■ SIP

V operačním systému je možné nastavit limit počtu událostí za sekundu. Během testu byl nastaven na 10 000 událostí/sec. odpovídající zhruba 240 cap hovorů. Očekávaný průběh byl následující: u IMS se předpokládalo, že obdrží 500 hovorů a následně zastaví odesílání provozu. DSI bude blokovat server a STP přesměruje na určitou dobu provoz na jiný server. Výsledkem testu bylo, že přetížení fungovalo správně. Avšak simulátory nebyly schopny zvládnout chyby hovorů jdoucí přes přetížení.

### ■ Portál

Provádí se přidáním omezovače, který se používá jako proxy. V tomto testu se nakonfiguroval na kapacitu 500 událostí za sekundu pro každou IP adresu a veškerý přenos přicházel z jedné IP adresy. Výsledkem bylo úspěšné zpracování všech 500 událostí/s, kdy normální provoz se odhaduje na 2 události/s.

### ■ Dohled

Neexistuje žádný mechanismus na zajišťování přetížení na dohledu, protože maximální zatížení je mnohem vyšší než odhadovaný provoz, takže nemá smysl používat ochranu proti přetížení.

## 9.3 Testy maximálního zatížení

### CAP

Test spočívá ve spuštění základní zátěže a zvyšování CAP provozu, dokud se nedosáhne maximálního zatížení. Opět zde nastal problém se simulátorem, který se při generování velkého zatížení stává nestabilním. Se zátěží do 900 CAP byla odezva menší než 40 ms.

### SIP

Test spočívá ve spuštění základní CAP a SIP zátěže a zvyšování SIP provozu, až do jeho maximálního zatížení. Simulátor se stal nestabilním při generování 2000 požadavků. Z toho důvodu jsou zde zobrazeny tyto výsledky.

Generátor		CAP výsledky		SIP výsledky	
CAP	SIP	Neúspěšné volání	Odezva	Neúspěšné volání	Odezva
285	1000	0	<40 ms	0	<20 ms
285	1200	0	<40 ms	0	<20 ms
285	1500	0	<40 ms	0	<20 ms
285	2000	5	selhání	2000	selhání

**Tabulka 9.9:** Výsledky maximálního SIP zatížení

Test byl proveden pouze na jednom serveru, kde jsem dosáhl 600 požadavků bez chyby s odezvou menší než 20 ms.

### Portál

Během testu bylo zvýšeno zatížení portálu na 1000 požadavků za sekundu. Systém to neovlivnilo a jelikož provoz byl 500x vyšší než je očekávaný, zatížení se dále nezvyšovalo.

Generátor			Portál	
CAP	SIP	Rq/s	Neúspěšné volání	Odezva
150	15	1000	0	avg 149 ms

**Tabulka 9.10:** Výsledky maximálního zatížení portálu

## ■ Dohled

Během testu se zvyšovalo zatížení na dohledovém systému. Systém nevykazoval žádné problémy nebo zpomalení, odezva byla menší než 1 ms pro více než 7700 rq/s, což je mnohonásobně víc, než předpokládaná zátěž 2rq/s. Jelikož zatížení bylo 3850x větší, nepokračovali jsme v testu dále.

Generátor			Dohled	
CAP	SIP	Rq/s	Neúspěšné volání	Odezva
285	15	7700	0	<1 ms

**Tabulka 9.11:** Výsledky maximálního zatížení portálu

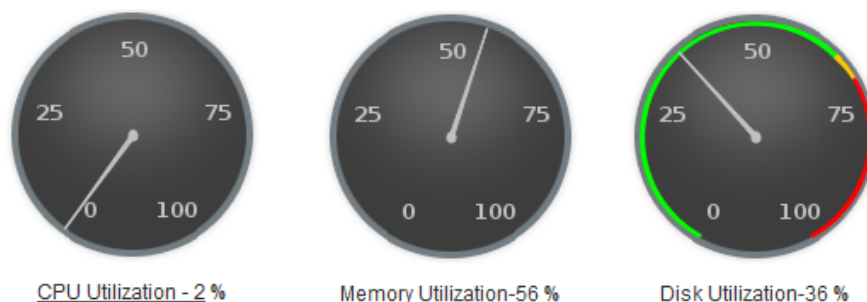


## Kapitola 10

### Monitorování

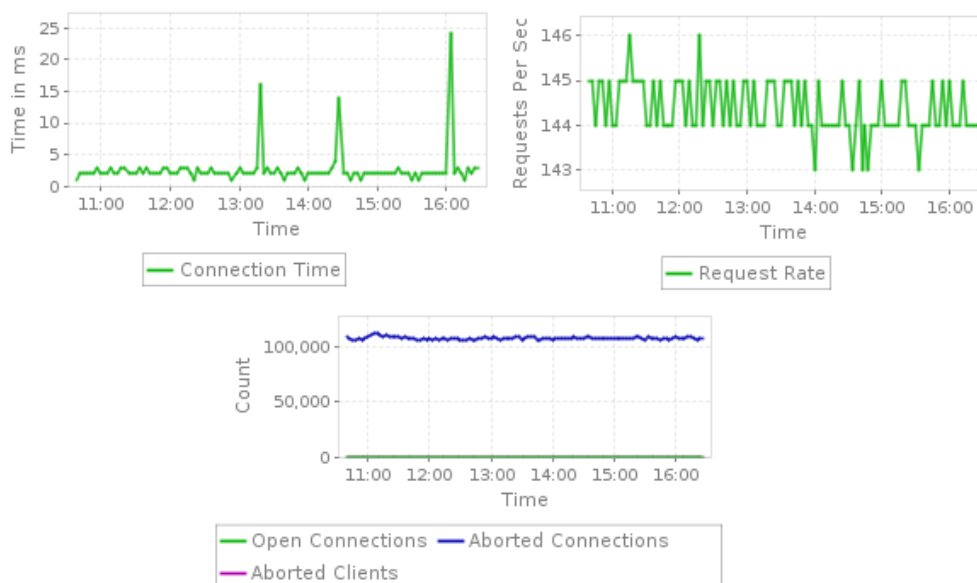
K monitorování a generování alarmů se používá Aplikační manažer. Jedná se o webovou aplikaci, která umožňuje kontrolovat platformu z různých pohledů, např. operační systém, databáze, webové servery a aplikační servery.

U operačního systému sledujeme všechny jeho aspekty. Mezi nejzákladnější parametry patří využití CPU, paměti a disku, viz. obrázek 10.1, ale také jsou kontrolovány služby a procesy na něm spuštěné. Při překročení prahových hodnot jsou generovány varovné nebo kritické poplachy. Když se stav vrátí na normální úroveň, odešle se mazací událost.



**Obrázek 10.1:** Využití CPU, paměti a disku

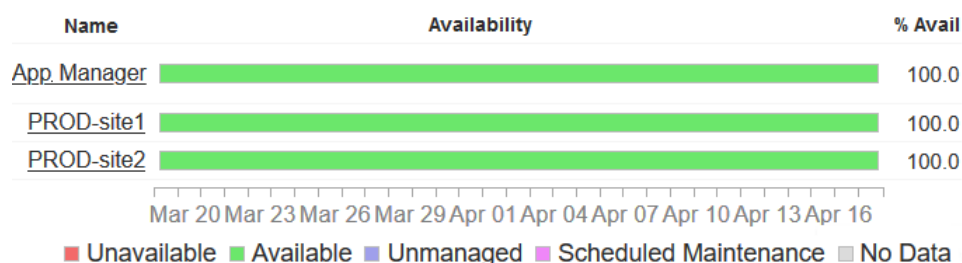
U databáze sledujeme parametry, jako např. doba připojení, počet žádostí za sekundu, statistika připojení, viz. obrázek 10.2. Na aplikačních serverech se v aplikaci zpracovávají hovory. Sledované parametry jsou využití paměti, doba odezvy, stav aplikace, počet požadavků za sekundu, počet relací, atd. I zde jsou nastaveny prahové hodnoty ke generování alarmů.



**Obrázek 10.2:** Vybrané parametry databáze za posledních 6 hodin

Dále se používají monitorovací skripty, které kontrolují protokoly a zjišťují chyby a další události na platformě. Kromě kontroly můžou poskytovat KPI statistiky. Zaznamenávají se KPI jako CAP hovory, BHCA, počet probíhajících konverzací, celkový počet konverzací, atd.

Pro lepší orientaci jsou vytvořeny dashboardy s vybranými parametry. Stav daného systému je barevně označen, aby na první pohled bylo zřejmé, v jakém stavu se nachází. Na obrázku 10.3 můžeme vidět, že za posledních 30 dní byly oba sity 100% času dostupné a nebyly na nich zaznamenány žádné chyby.



**Obrázek 10.3:** Dostupnost sítí za posledních 30 dní



## 10.1 EDR záznamy

Záznam podrobnosti událostí (EDR - Event Data/Detail Record) [21] je datový záznam generovaný telekomunikačním zařízením (ústředna, IN platforma, atd.), který dokumentuje podrobnosti o telefonním hovoru nebo jiné transakci (např. textová zpráva) procházející přes zařízení. Během telefonního hovoru se vygeneruje jeden nebo více záznamů. Tato data se předávají do účtovacího systému a na jejich základě se vystavuje měsíční vyúčtování [22].

Každá instance aplikačního serveru průběžně zapisuje nové EDR záznamy do databáze. V té je nastavena úloha pro periodické ukládání dat z databáze do dočasného souboru. Data v databázi zůstávají uchována po určitou dobu. Když je dočasný soubor uzavřen pro zápis, tak je přejmenován a připraven k dalšímu zpracování.

Pokud dojde k nedostatku místa na disku nebudou záznamy mazány, přesunuty ani zkomprimovány. Pokus o zápis do souboru selže a dočasné soubory nebudou exportovány. Položky však budou zůstávat v databázi. Později, až se uvolní místo, bude proces již úspěšně zopakován. Nesmí se stát, že by se kvůli kapacitě disků záznamy ztratily.

### 10.1.1 Parametry EDR

Záznam může mít různý počet parametrů. Vždy musí obsahovat povinné (P) položky, v některých situacích má i položky volitelné (V). Parametry jsou dvojího typu: numerické obsahují pouze sekvenci čísel nebo alfanumerické, které se skládají ze znaků a čísel.

Název	Typ	Volitelný	Obsah
session_id	N	P	Unikátní identifikace hovoru.
sequence_no	N	P	Pořadové číslo týkající se stejného hovoru. První záznam má číslo 0.
a_number	A	P	Číslo volající strany.
b_number	A	P	Číslo volané strany.
c_number	A	V	Na jaké číslo byl hovor přeměřován.
term_code	N	V	Způsob ukončení hovoru.
connect_time	N	P	Doba trvání hovoru.

**Tabulka 10.1:** Vybrané parametry EDR záznamů [13]

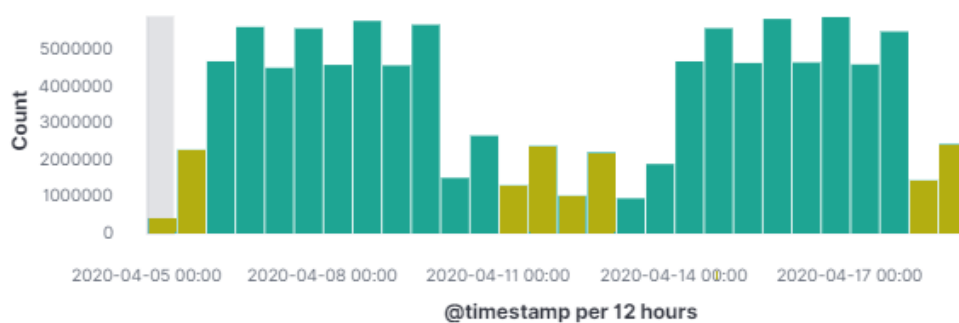
EDR záznam je zobrazen na obrázku 10.4, avšak z bezpečnostních a právních důvodů jsou provozní údaje upraveny. Z jeho parametrů lze vyčíst informace jako jsou číslo volaného a volajícího, msc adresu, datum, čas a délku hovoru, způsob ukončení, atd.

```
b_number: volané číslo   paging_time: 0   @timestamp: Apr 18, 2020 @
18:59:55.000   served_user: volající číslo   @version: 1   tags: inasprod,
edrhistory, beats_input_codec_plain_applied   overhead_time: 0
sequence_no: 0   a_clir: 0   edr_type: 0   msc_address: msc číslo
session_id: 1918128155   cid: 400   sub_service_id: 6
```

Obrázek 10.4: Ukázka EDR záznamu

## 10.1.2 Statistiky

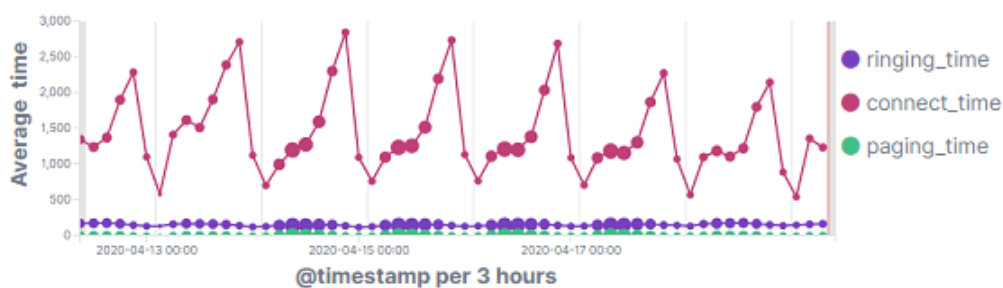
Na základě těchto záznamů můžeme v síti sledovat různé statistiky. V grafu 10.5 je znázorněn celkový počet hovorů, které byly za dva týdny (od 5.4.2020 do 18.4.2020) obslouženy platformou. Lze z něj vypočítat typické periodicky se opakující chování uživatelů. Jelikož se jedná o služby používané především firemními zákazníky, je počet volání v pracovní dny větší než o víkendy nebo ve svátek.



Obrázek 10.5: Celkový počet hovorů na platformě

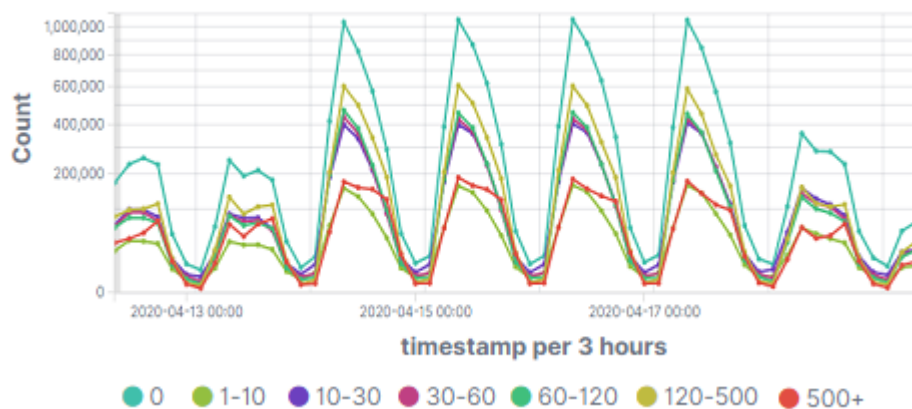
## VPN

Na níže uvedených statistikách je zobrazen celý průběh hovoru VPN členů. Na obrázku 10.6 můžeme vidět, že průměrná doba navázání spojení (paging\_time) je menší než 100 ms, vyzvánění (ringing\_time) trvá v průměru 150 s a délka hovoru (connect\_time) v průměru 1600 s.



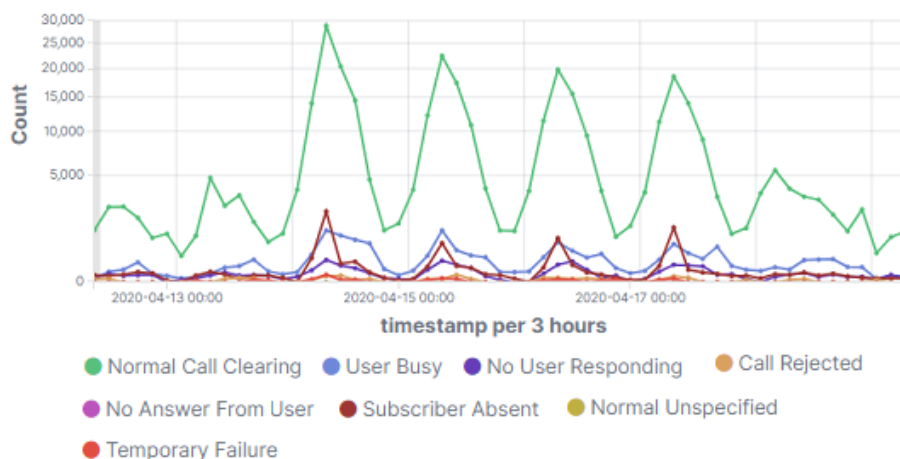
Obrázek 10.6: Průměrné doby trvání

Na následujícím obrázku 10.7 je zobrazen počet hovorů a jim odpovídající délka. Nejvíce hovorů je kratších než 1 minutu. Naopak nejméně hovorů je delších než 500 minut. Platí zde nepřímá úměra, tedy že čím jsou hovory delší, tím menší je jejich počet.



Obrázek 10.7: Délka hovorů

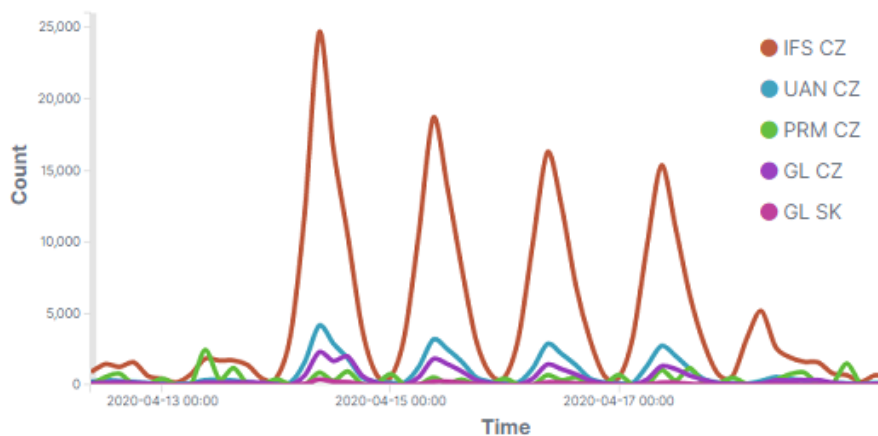
Na posledním obrázku 10.8 je zobrazeno, jak jsou hovory ukončovány. Přes 75% hovorů je ukončeno normálně, tedy volající nebo volaná strana ukončí spojení. Ve zbývajících 25% se hovor ukončí z jiných důvodů, např. uživatel je obsazený nebo neodpovídá, je špatně zadané volané číslo nebo z důvodu nějaké dočasné chyby.



Obrázek 10.8: Ukončení hovoru

## ■ NTS

U služby překladu čísel pozorujeme u hovorů podobné hodnoty a grafy jako u VPN. Zajímavější je počet hovorů pro jednotlivé typy NTS. Na obrázku 10.9 lze vidět, že nejvíce používaným typem je IFS. Na opačném konci se nachází PRM typ. Tato statistika je však velmi ovlivněna počtem zákazníků, kteří používají dané služby.



Obrázek 10.9: Ukončení hovoru

# Kapitola 11

## Závěr

Cílem této práce bylo popsat proces výměny platformy pro Chytrou síť z důvodu modernizace sítě. Dalším cílem bylo porovnat architekturu obou platforem a zhodnotit jejich výhody, nevýhody a finanční náklady pro operátora. V neposlední řadě se zaměřit na používané protokoly, způsob testování systému a implementaci služeb.

V teoretické části byl popsán vývoj Chytré sítě. Bylo uvedeno, že standardizace probíhala v nepřetržitém procesu a v pravidelných intervalech byla zmrazena. Specifikace se nazývají sada schopností a celkem jsou definovány čtyři sady. Každá zachovává původní funkce a přidává další nové. Tyto specifikace jsou mezi sebou zpětně kompatibilní a jsou popsány ze čtyř pohledů: rovina služeb, globální funkční rovina, distribuovaná funkční rovina a fyzická rovina.

Po výměně platformy se v rámci komunikace se sítí používají pouze dva protokoly. Fixní členové komunikují pomocí protokolu SIP a mobilní členové protokolem CAP, který je součástí rodiny protokolů SS7. Staré INAP ústředny byly vypnuty a odebrány ze sítě.

Původní platforma byla do sítě implementována v roce 2010. Jednalo se o hardwarovou platformu a byla plně redundantní se sity v Praze a v Brně. Skládala se z USAU a ATAE hardwaru. Její provoz, údržba a rozšiřování bylo finančně nevýhodné, a proto byla v roce 2019 nahrazena novou, která je celá virtualizovaná a postavená na technologii VMware. To přineslo výhody jako jsou nezávislost na hardwaru, levnější a rychlejší rozšiřování, snazší zavádění nových služeb a maximální využití výpočetních zdrojů.

Proces migrace byl rozdělen do dílčích fází. Začínalo se plánováním, analýzou a designem. Vznikl podrobný popis služeb a následoval jejich vývoj a implementace do systému. Následně byly provedeny čtyři různé úrovně akceptačního testování. Na základě výsledků z testů byla provedena optimalizace systému. Po úspěšném otestování se během servisního okna migrovala data na nový systém a překonfigurovalo směrování dat v síti.

Na platformě jsou v současné době provozovány dvě služby. Virtuální privátní síť byla spuštěna na konci roku 2019 a umožňuje používat stávající veřejnou telekomunikační infrastrukturu jako soukromou síť. Služba překladač čísel byla spuštěna v prvním kvartálu roku 2020. Mezi nejdůležitější zákazníky patří Městská policie, kdy linku 156 je provozována pro všechny operátory v ČR. Do budoucna se předpokládá integrace dalších služeb. V roce 2021 by to měla být služba Virtuální ústředna.

Při výkonnostním testování platformy bylo simulováno základní a špičkové zatížení na jednom nebo obou sitech. Testy proběhly úspěšně dle očekávání. Ke ztrátě hovorů došlo pouze u CAP protokolu, ostatní systémy pracovaly bezchybně. Testy přetížení byly provedeny pouze u portálu, kde bylo dosaženo úspěšného zpracování 500 událostí/s. CAP a SIP simulátory nebyly schopny testy provést a stávaly se nestabilní. Stejný problém s nestabilitou nastal i u testů maximálního zatížení. U CAP protokolu bylo dosaženo zátěže 900 požadavků a u SIP 1500 požadavků. Následovaly problémy se simulátory a ukončení testu. Na portálu bylo zatížení 500x větší než bylo očekáváno, u dohledového systému dokonce 3850x větší. Z toho důvodu nebylo dále postupováno v testování systému, jelikož se taková situace v reálném prostředí neočekává.

Monitorování platformy probíhá nepřetržitě za pomoci nástroje Aplikační manažer. Jsou sledovány parametry aplikačních serverů, signalizačních serverů, databází, atd. Vybrané parametry jsou zobrazeny v grafech. Pro každý hovor obslužený platformou jsou generovány EDR záznamy. Z jejich parametrů je možné určit různé statistiky. Např. byl vybrán celkový počet hovorů, který zobrazuje typické periodické chování zákazníků, kdy větší počet volání je v pracovní dny, viz obr. 10.5. Ostatní statistiky jsou zobrazeny výše v práci.



## Literatura

1. TOMÁŠKOVÁ, Helena. *Historický vývoj poštovníctví a řízení pošt a telegrafů v Praze po roce 1918 do roku 1935*. Pardubice, 2010. Diplomová práce. Univerzita Pardubice, Filozofická fakulta, Katedra historických věd.
2. ZUIDWEG, Johan. *Next generation intelligent networks*. Boston: Artech House, 2002. ISBN: 1-58053-263-2 / 978-1-58053-263-1.
3. BATES, Regis J. *Advanced Intelligent Networks*. CRC Press, 2016. ISBN: 0-07139-159-2 / 978-0-07139-159-7.
4. DRYBURGH, Lee; HEWETT, Jeff. *Signaling System No. 7 (SS7/C7): protocol, architecture, and services*. Indianapolis: Cisco Press, 2005. ISBN: 1-58705-040-4.
5. TROLLER, Pavel. *Signalizační systém SS7 [přednáška]*. Praha: ČVUT v Praze, 2010.
6. *Intelligent Network Application Part (INAP)* [<http://www.telecomspace.com/ss7-in.html>]. [Online; 25. 4. 2020].
7. NOLDUS, Rogier. *Camel: Intelligent Networks for the GSM, GPRS and UMTS Network*. Chichester: John Wiley, 2006. ISBN: 978-0-470-01694-7.
8. JOHNSTON, Alan B. *SIP: Understanding the Session Initiation Protocol*. 2. vyd. Artech House Telecommunications Library, 2004. ISBN: 1-58053-655-7.
9. TUTORIALS POINT. *Session Initiation Protocol - Introduction* [[https://www.tutorialspoint.com/session\\_initiation\\_protocol/session\\_initiation\\_protocol\\_quick\\_guide.htm](https://www.tutorialspoint.com/session_initiation_protocol/session_initiation_protocol_quick_guide.htm)]. [Online; 25. 4. 2020].

10. TROLLER, Pavel. *Signalizační protokoly SIP/SDP, H.323, IAX2, MGCP a SCCP. Přenosový protokol RTP/RTCP [přednáška]*. Praha: ČVUT v Praze, 1.5.2019.
11. NOVOTNÁ, Hana. *02 - NGIN Solution FRS*. Praha, 2010.
12. NOVOTNÁ, Hana. *03 - NGIN Platform FRS*. Praha, 2010.
13. LEBEDA, Roman. *NGIN - High Level Design (HLD)*. Praha, 2019.
14. LEBEDA, Roman. *NGIN - Migration document*. Praha, 2019.
15. NOVOTNÁ, Hana. *01 - NGIN Number Translation Service (NTS) FRS*. Praha, 2010.
16. NOVOTNÁ, Hana. *01 - NGIN Virtual Private Network (VPN) FRS*. Praha, 2010.
17. NOVOTNÁ, Hana. *INAS IP Centrex Solution Description*. Praha, 2020.
18. LEBEDA, Roman. *NGIN - Platform Solution Description*. Praha, 2019.
19. LEBEDA, Roman. *NGIN - Test Approach Document*. Praha, 2019.
20. ANRITSU. *MasterClaw Monitoring* [<https://www.anritsu.com/en-gb/service-assurance/masterclaw-monitoring>]. [Online; 25. 4. 2020].
21. CONTRIBUTORS, Wikipedia. *Telecommunications rating — Wikipedia, The Free Encyclopedia* [[https://en.wikipedia.org/w/index.php?title=Telecommunications\\_rating&oldid=861029808](https://en.wikipedia.org/w/index.php?title=Telecommunications_rating&oldid=861029808)]. 2018. [Online; 25. 4. 2020].
22. REA, Roger. *Real-time Big Data Analytics for Telecommunications* [<https://www.ibmdatahub.com/blog/real-time-big-data-analytics-telecommunications>]. 2013. [Online; 25. 4. 2020].





## Příloha A

### Seznam zkratk

AIN	Advanced Intelligent Networks
ALU	Alarm Unit
API	Application Programming Interface
ATAE	Advanced Telecommunications Application Environment
B2BUA	Back-to-back user agent
BCP	Basic Call Process
BCSM	Basic-Call-State Model
BCUSM	Basic-Call-Unrelated-State Model
BMP	Business Management Point
BSS	Business Support Systems
BUCP	Basic Call-Unrelated Process
CAP	CAMEL Application Part
CCF	Call Control Function
CID	Call-instance Data
CPH	Call-Party Handling
CS	Capability Sets
DFP	Distributed Functional Plane
EDP	Event Detection Points
EDR	Event Data/Detail Record
ETSI	European Telecommunications Standards Institute
FAT	Factory Acceptance Test
FE	Functional Entity
FEP	Front End Processor
GFP	Global Functional Plane
GSM	Global System for Mobile
GT	Global Title
HLD	High Level Design
HLR	Home Location Register

HLSIB	High-level SIB
HSC	Hot-Swap and Control Unit
IFS	International Freephone Service
IMS	IP Multimedia Subsystem
IN	Intelligent Networks
IN	Intelligent Networks
INAP	Intelligent Network Application Protocol
INCM	Intelligent Networks Conceptual Model
IP	Intelligent Peripheral
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
ITU	International Telecommunication Union
LLD	Low Level Design
MTP	Message Transfer Part
NGIN	Next Generation Intelligent Network
NTS	Number Translation Service
O-BCSM	Originating Basic-Call-State Model
OSS	Operations Support Systems
PBX	Private branch exchange
PC	Point Code
PINT	Public Switched Telephony Network Internet Internetworking
PLMN	Public Land Mobile Network
POI	Point of Initiation
POR	Point of Return
POTS	Plain Ordinary Telephone Service
PP	Physical Plane
PRM	Premium Rate Service
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RTP	Real Time Transport Protocol
SAT	System Acceptance Test
SCCP	Signalling Connection Control Part
SCF	Service Control Function
SCP	Service Control Point
SDF	Service Data Function
SDP	Service Data Point
SDP	Session Description Protocol
SDU	Service Data Unit
SEE	Service Execution Environment
SIB	System Information Block
SIP	Session Initiation Protocol
SIU	System Interface Unit
SM	Session Manager
SMF	Service Management Function
SMP	Service Management Point
SMTTP	Simple Mail Transfer Protocol

SMU	System Management Unit
SP	Service Plane
SP	Signaling Points
SPIRIT	Services in the PSTN/IN Requesting Internet Services
SRF	Special Resource Function
SSD	Service Support Data
SSF	Service Switching Function
SSP	Service Switching Point
STP	Signal Transfer Point
T-BCSM	terminating Basic-Call-State Model
TCAP	Transaction Capabilities Application Part
TDP	Trigger Detection Points
TUP	Telephone User Part
UAC	User Agent Client
UAN	Universal Access Number
UAS	User Agent Server
UAT	User Acceptance Test
UPWR	Universal Power Board
URI	Uniform Resource Identifier
USAU	Uniform Signaling Access Unit
VLR	Visitor Location Register
VPN	Virtual Private Network
WCSU	Widely Calling Control Unit and Signaling Process Unit