K vytvoření tohoto textu nebylo použito žádného softwarového produktu společnosti MicroSoft. Text byl vysázen v typografickém systému LaTeX 2_ε, vektorové obrázky byly vytvořeny pomocí balíku kancelářkých aplikací OpenOffice a na zpracování bitmapovych obrázků byl použit program GIMP. Veškeré programové vybavení bylo provozováno nad operačním systémem GNU/Linux.

Obsah

Seznam tabulek

Seznam obrázků

Část I
Úvod do problematiky

1 Úvod

Cílem práce je návrh protokolu pro přenos signalizačních zpráv pro řízení spojování telefonních hovorů v prostředí sítí pracujících nad protokoly rodiny TCP/IP. Podnětem pro tuto práci jsou problémy známé z doposud používaných protokolů realizujících spojovací procesy a přenos hovorových dat v sítích TCP/IP - VoIP, jejich omezení a některé nepříliš transparentní kroky, ke kterým došlo během jejich vývoje. Naproti tomu pak stojí zkušenosti z oblasti klasické telefonie a zde používaných signalizačních protokolů, které pracují již řadu let bez větších problémů. Metody používané v těchto signalizačních systémech byly proto značnou inspirací. Výsledkem práce je protokol určený pro přenos signalizačních zpráv pro řízení telefonních hovorů prostřednictvím sítě TCP/IP, který plně využívá všech výhod poskytovaných touto sítí a zároveň zohledňuje potřeby vycházející z postupného vývoje telefonních sítí, umožňuje zpětnou spolupráci spojovacích systémů a poskytuje nové možnosti při rozvoji moderních telekomunikačních služeb.

Popsaný návrh protokolu plně umožňuje přenos všech informací nutných pro řízení spojovacích procesů, tak jak jsou známé a používané signalizacemi v klasické telefonní síti. Protokol je navržen čistě jen pro přenos signalizace samotné, je nezávislý na transportním protokolu používaném pro přenos hovorových dat. Pro ty pak může být použité v podstatě libovolné médium včetně běžné TDM přenosové sítě či dokonce analogových okruhů. Návrh poskytuje nové metody přenosu telefonní signalizace mezi spojovacími systémy a nabízí možnost využití protokolu v heterogenních sítích a zjednodušit tak probíhající konvergenci v oblasti telekomunikačních sítí a následně realizaci nových služeb v prostředí těchto sítí.

Návrh klade důraz na transparentnost v místech, kde dochází k překladu zpráv ze signalizací používaných v klasické telefonii do zpráv přenášených v síti TCP/IP a zpět, tak aby při tomto procesu nedocházelo ke ztrátě jakýchkoliv informací a tím ke snížení výsledné jakosti poskytované služby.

Protokol je, s ohledem na dynamický vývoj v oblasti telekomunikací, navržen tak, aby ho bylo možné, v případě nutnosti, v budoucnu jednoduše rozšířit dle nově vzniklých požadavků.

2 Telefonní sítě

2.1 Prostředí sítí se spojováním okruhů

Tradiční telefonní sítě, pokrývající v současné době území celého světa, jsou založeny na principu sítí se spojováním okruhů (Circuit Switching Network). K přenosu jednotlivých telefonních hovorů, jak mezi telefonními ústřednami, tak mezi telefonní ústřednou a koncovým účastníkem je využíváno pevných okruhů s jasně definovanými vlastnostmi, které zaručují, předem stanovenou, jakost poskytované služby. S využitím těchto okruhů je pomocí spojovacích systémů, konkrétně pomocí spojovacích polí těchto systémů, sestaven okruh mezi účastníky realizující prostřednictvím telefonní sítě hovor. Takto vytvořené spojení je po dobu trvání telefonního hovoru pevné a okruhy pro něj použité jsou vyhrazeny právě jen pro toto spojení. Jakost služby, která je v těchto sítích poskytována, je přesně definovatelná na základě vlastností přenosových prostředků realizující jednotlivé okruhy v síti a spojovacích systémů, které vytvářejí telefonní spojení napříč celou sítí.

Současný model tradiční telefonní sítě je dán dlouhodobým historickým vývojem, jehož počátek zahájil již Alexander Graham Bell vynálezem telefonu v roce 1876. Z počátku jednoduchá zařízení realizující pouze spojení bod - bod se postupem času vyvinula v rozsáhlou mezinárodní síť s milióny koncových účastníků. Prostředky současných telefonních sítí jsou mezinárodně standardizované, v síti je používán jednotný způsob adresace koncových stanic a k řízení spojovacích procesů se využívá robustních signalizačních systémů, které umožňují realizovat stále nové moderní služby.

Procesy spojování v rámci spojovacích systémů, ale i celých telefonních sítí jsou řízeny pomocí signalizačních systémů. Telefonní signalizace slouží primárně k sestavení hovoru, dohled nad sestaveným spojením a ukončení hovoru a s ním související uvolnění spojovacích cest. Signalizace a její přenos je jedním z nejdůležitějších prvků celé telefonní sítě. Na správném přenosu informace pomocí signalizačního systémů závisí zda bude síť jako celek fungovat a plnit tak svůj účel.

Součástí vývoje telefonních sítí byl proto i vývoj jednotlivých signalizačních systémů. Vlastnosti a schopnosti signalizačních systémů postupně přibývaly a zlepšovaly se tak, jak postupně rostly schopnosti spojovacích systémů. Největšího vývoje dosáhly signalizační systémy při začlenění výpočetní techniky do spojovacích systémů. Během nástupu čtvrté generace spojovacích systémů došlo k vytvoření několika mezinárodních standardů signalizačních systémů pro různé úrovně telefonních sítí. Tyto signalizační systémy slouží nejen k řízení spojovacích procesů ale umožňují poskyto-

vání moderních doplňkových služeb.

Přenosová síť prošla podobně jako spojovací systémy postupným vývojem. Z počátku telefonie bylo k realizaci okruhu používáno jednotlivých symetrických párů tak, že každý okruh byl tvořen jedním párem. S postupným vývojem elektroniky docházelo v přenosových sítích k mohutným změnám. Nejprve bylo využití přenosových cest znásobeno nasazením systémů FDM (Frekvency Division Multiplex). Jednalo se o takzvané nosné systémy, kdy vícenásobné využití přenosových cest bylo řešeno pomocí analogových modulací. S nástupem digitální techniky došlo k zavádění systému TDM (Time Division Multiplex), kde je využití přenosových cest znásobeno s použitím metody řízení přístupu k médiu pomocí časových intervalů. Tato metoda přenosu je využívána dodnes.

2.2 Prostředí sítí se spojováním paketů

Ve snaze minimalizace nákladů na provoz, efektivnějšího využití přenosových tras a integrace technologií datových a telefonních sítí vznikají nové způsoby přenosu telefonních hovorů, než na které jsme zvyklí v tradiční telefonii. K přenosu v takto integrovaných sítích se nevyužívá spojování okruhů (Circuit Switching), jak bylo popsáno v předchozí sekci, ale metoda paketového přenosu dat (Packet Switching) do nedávné doby používaná výhradně v datových a počítačových sítích. Tento způsob hlasové komunikace s sebou přináší řadu výhod jako například kvalitnější využití přenosových tras, nebo snížení nákladů na použitou technologii, jak již bylo zmíněno, ale také některé nevýhody, které omezují jakost poskytované služby.

S nástupem technologií pro přenos samotného hovoru, či jiných multimediální dat v prostředí paketových sítí je nutné zajistit též bezproblémový přenos signalizace, která by umožnila řízení spojovacích procesů v novém prostředí.

Dalším důležitým bodem při návrhu protokolů pro realizaci telefonie v paketových sítích je umožnit, aby nově vznikající sítě plně spolupracovaly s existující telefonní sítí pracující na principech spojování okruhů.

2.3 Druhy přenosu

Podle typu hostitelské sítě se dnes využívá několik základních způsobů paketového přenosu hlasu. Jedná se o:

- **VoFR** - přenos hlasu po prostředcích sítě s přepojováním rámců Frame Relay (Voice Over Frame Relay)

- **VoATM** - přenos hlasu po prostředcích sítě s přepojováním buněk ATM (Voice Over ATM)
- **VoIP** - přenos hlasu po prostředcích počítačové sítě postavené na službách protokolů rodiny TCP/IP (Voice Over IP)

2.3.1 VoFR

VoFR využívá k přenosu hlasu prostředků sítě Frame Relay. Mezi výhody patří poměrně nízké navýšení množství přenášených dat způsobené služebními informacemi přenosového protokolu. Jako hlavní nevýhodu je nutné zmínit poměrně obtížné propojování sítí různých provozovatelů a problémy se spoluprací zařízení různých výrobců.

Technologie Frame Relay je v současné době již na ústupu, maximální rychlosti dosahované v síti nejsou pro současné potřeby postačující a náklady na provoz nepřiměřeně vysoké. Pro další vývoj telekomunikační techniky obecně není již síť na principu Frame Relay perspektivní, proto ani v oblasti přenosu telefonie neprobíhá již žádný další vývoj.

2.3.2 VoATM

VoATM je přenos hlasu po síti ATM. V síti ATM je minimální, respektive shodné jako u ostatních služeb v této síti, navýšení množství dat způsobené služebními informacemi přenosového protokolu, na rozdíl od VoFR a VoIP je však v síti ATM zajištěna jakost služby QoS (Quality Of Service) a to přímo návrhem základních principů sítě.

Telekomunikační sítě pracující na principech ATM jsou v dnešní době na ústupu. Důvodem poklesu zájmu o tuto technologii jsou v prvé řadě náklady na budování a provoz sítě. Dalším důležitým faktorem je problém při spolupráci zařízení různých výrobců, doporučení pro ATM jsou natolik komplexní a složitá, že při jejich implementaci docházelo k odlišnostem v konkrétních realizacích jejichž výsledkem je nekompatibilita některých zařízení.

Samotné sítě ATM se v dnešní době již dále nerozvíjejí, přesto však mnoho, často převratných, metod komunikace a řízení sítě je využíváno při návrhu nových protokolů. Příkladem může být MPLS, WiMAX, či jiné, zejména rádiové přístupové, systémy.

2.3.3 VoIP

VoIP využívá k přenosu hlasové informace služeb počítačové sítě založené na službách protokolů rodiny TCP/IP. Ze všech zmíněných možností paketového přenosu má tento způsob největší navýšení přenášených informací způsobené služebními informacemi IP protokolu. Je poměrně značný problém v zajištění jakosti služby QoS. Velkou výhodou je ovšem jednoduché propojování sítí různých provozovatelů a poměrně minimální problémy při spolupráci zařízení různých výrobců.

Sítě využívající protokoly rodiny TCP/IP jsou v dnešní době nejrozšířenější sítěmi pracující na principech spojování paketů. Vzhledem k jednoduchosti samotného návrhu mohlo a může docházet k rychlému rozšiřování těchto sítí a ke snadné a rychlé implementaci TCP/IP protokolu do nových zařízení. Příkladem rychlého vývoje v oblasti sítí s protokoly TCP/IP je vývoj sítě Internet podrobně popsaný v příloze A.

3 Prostředí sítí TCP/IP

Protokoly rodiny TCP/IP jsou protokoly pocházejícím z dob, kdy přenosové rychlosti byly ve srovnání se současností poměrně nízké a chybovost přenosu naopak vysoká. Systém protokolů byl navržen pro přenos dat pocházejících z počítačových systémů, proto při vývoji tohoto protokolu nebyly kladeny téměř žádné požadavky na zpoždění při přenosu, jitter a další veličiny ostře sledované v oblasti tradičních telefonních sítí. Při přenosu paketů sítí může docházet ke zpožděním, které jsou způsobeny možným přetížením sítě, ztrátou a následným opakováním paketů, odlišnou cestou paketů atd. Ze shodných či velice podobných příčin dochází ke vzniku značně většího rozptylu jitteru, než jaký bývá běžný v prostředí sítí se spojováním okruhů. Výše zmíněné vlastnosti nezpůsobují žádné problémy při běžné datové komunikaci. Při přenosu hovorových, či jiných multimediálních dat vyžadujících přenosy v reálném čase, mohou však znamenat degradaci vlastností přenosu nebo dokonce naprostou nepoužitelnost sítě pro tento druh komunikace.

Návrh modelu protokolů rodiny TCP/IP do jisté míry koresponduje s modelem RM-OSI [1], z čehož vyplývá vysoké množství služebních informací pocházejících z protokolů jednotlivých vrstev. Na druhou stranu vrstvová filosofie zaručuje shodnost implementace protokolů a umožňuje jejich jednoduchý, přehledný a přesný popis. Srovnání modelu protokolů rodiny TCP/IP a modelu RM-OSI je zobrazeno v tabulce 1. Výše popsaný způsob návrhu umožnil, v době vzniku protokolu, snadnou implementaci do operačního systému UNIX. Tento krok byl velmi důležitý ve vývoji jak samotných síťových protokolů, tak později ve vývoji celé sítě Internet. Jednoduchý, přehledný a snadno implementovatelný návrh znamenal následně značný úspěch a došlo k rychlému nárůstu počítačů a sítí využívající služeb protokolů rodiny TCP/IP. Podrobnější informace o postupné implementaci protokolů rodiny TCP/IP je možné najít v příloze A.

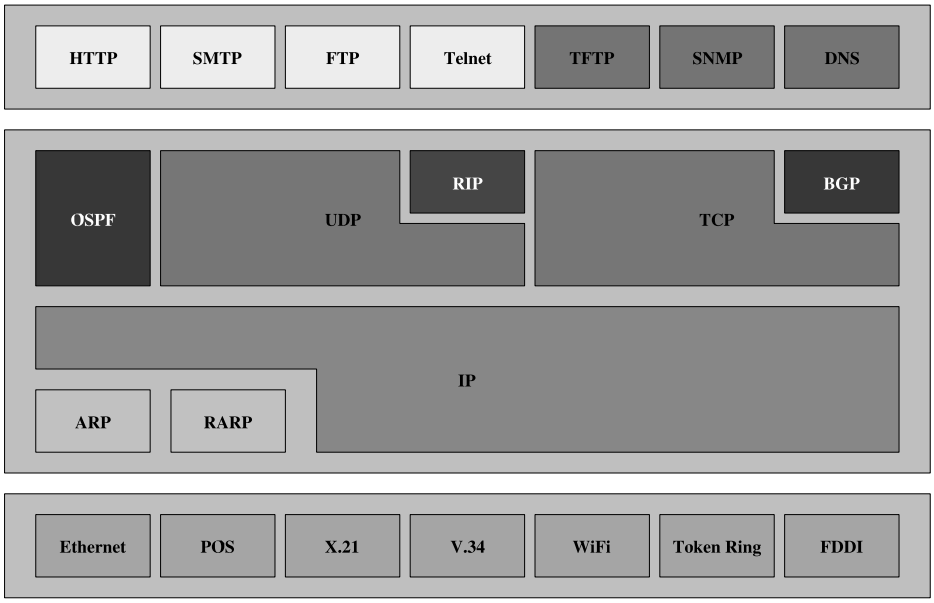
Jednotlivé protokoly z rodiny TCP/IP a jejich vzájemnou spolupráci ukazuje obrázek 1. V další části textu budou zjednodušeně popsány jednotlivé přenosové protokoly IP sítě, tj. IP, TCP a UDP s ohledem na využití IP sítě pro přenos hovorových dat a telefonní signalizace. Úplný a přehledný popis protokolů je uveden v [8].

V současné době jsou používané souběžně dvě verze IP protokolu. První z nich je verze 4, běžně označovaná IPv4, jde o původní návrh IP protokolu jehož základ

[1] Model protokolů rodiny TCP/IP byl navržen dříve než sedmi vrstvový otevřený model RM-OSI. Návrh RM-OSI byl modelem TCP/IP částečně inspirován a lze tudíž najít mezi oběma návrhy shodné znaky.

Referenční model OSI	TCP/IP
Aplikační vrstva	Aplikační vrstva
Prezentační vrstva	
Relační vrstva	
Transportní vrstva	Transportní vrstva
Síťová vrstva	Síťová vrstva
Spojová vrstva	Vrstva rozhraní sítě
Fyzická vrstva	

Tabulka 1: Porovnání architektury TCP/IP s modelem RM-OSI



Obrázek 1: Vzájemná závislost základních protokolů rodiny TCP/IP

byl dokončen na přelomu let 1979 a 1980. Protokol je používán téměř beze změn do dnes. Verze protokolu 4, ač s sebou nese značná omezení je stále nejpoužívanější verzí protokolu IP.

Druhou používanou verzí protokolu IP, která se pomalu začíná prosazovat do praxe je verze 6, označovaná IPv6. První doporučení s popisem 6 verze protokolu IP bylo vydáno v roce 1995 pod označením RFC1883. Verze 6 IP protokolu počítá se značným rozšířením adresního rozsahu, zjednodušuje záhlaví protokolu IP s ohledem na moderní technologie používané v současných telekomunikačních sítích, definuje metody pro zajištění jakosti služby - QoS atd. Celý návrh a následně implementace do praxe se však potýká se značnými problémy. Hlavními příčinami výše popsaných

problémů jsou:

- Protokol stále nemá, i po více jak deseti letech, ukončený vývoj. V návrhu stále dochází k poměrně zásadním změnám, které se často dotýkají samotných základů celého modelu.
- Popis protokolu je velice komplexní a pokrývá širokou oblast síťových funkcí, jeho implementace je proto značně náročná a do praxe a komerční sféry se prosazuje jen velmi pomalu a se značnými obtížemi. Implementace je nejen časově náročným procesem, ale vyžaduje i značné investice u kterých navíc není jasná jejich návratnost.

K nasazení protokolu IP ve verzi 6 došlo zatím v podstatě jen v oblasti výzkumných, experimentálních sítí a univerzitních sítí a jen velice málo v sítích komerčních poskytovatelů Internetu. V komerční oblasti nachází verze 6 uplatnění zvláště v oblasti Asie, kde je značný nedostatek volných IP adres a nasazení nové verze IP protokolu je východiskem z této situace. V sítích ostatní velkých poskytovatelů Internetu není nová verze protokolu podporovaná buď to vůbec, nebo jen jako okrajová bezvýznamná služba poskytovaná hlavně z prestižních důvodů, či jako doplnění celého portfolia služeb poskytovaných v oblasti IP.

3.1 Vrstva rozhraní sítě

Nejnižší vrstvou je v modelu protokolů TCP/IP vrstva rozhraní sítě (network interface). V modelu RM-OSI svými funkcemi v podstatě odpovídá prvním dvěma vrstvám, fyzické a spojové, jak je uvedeno v tabulce 1.

Protokoly rodiny TCP/IP jsou navrženy k zajištění komunikace mezi sítěmi v heterogenním prostředí. Protokoly zajišťují funkce síťové vrstvy a vrstev vyšších a nejsou nikterak vázány na přenosové médium případně na protokoly, které umožňují základní přenos informací po tomto médiu. Tato skutečnost je dalším z důležitých faktorů, proč došlo k tak masovému rozšíření sítí realizovaných prostřednictvím rodiny protokolů TCP/IP.

Protokoly rodiny TCP/IP je možné provozovat v podstatě na libovolném přenosovém prostředí od sériového spojení s protokolem V.24/V.28, přes telefonní modemy, sítě s protokolem X.21, Frame-Relay, Ethernet, Token-Ring až po současné moderní metody, jakými jsou například přenosové systémy SDH používané v páteřních sítích

WAN. Zde se využívá progresivního způsobu (IP over SONET/SDH), který minimalizuje množství přenášených řídících informací a maximálně využívá možností poskytnutých sítí SONET respektive SDH. Nebo na opačném konci celé síťové infrastruktury technologie WiFi či WiMAX pro realizaci bezdrátového připojení koncových klientských zařízení.

Současné technologie moderních směrovačů umožňují využít maximálně dostupných přenosových sítí SDH či WDM a je tak možné realizovat páteřní spoje WAN sítí s přenosovými rychlostmi 10 Gb/s. Podobně s pokrokem ve vývoji v technologiích lokálních sítí (LAN) je nyní k dispozici jak doporučení, tak konkrétní implementace pro spoje s přenosovou rychlostí 10 Gbit/s. Přenosové prostředky bezdrátových lokálních sítí nabízejí přenosové rychlosti v řádech desítek až stovek megabitů za sekundu.

3.2 Mezisíťová vrstva

Druhou vrstvou modelu TCP/IP je mezisíťová vrstva (internet layer). Svými vlastnostmi, poskytovanými službami i rozhraními přesně odpovídá třetí, síťové vrstvě modelu RM-OSI viz. 1.

3.2.1 IP

Základním protokolem, tvořícím pilíř sítě, je protokol IP (Internet Protocol). Jedná se o protokol síťové vrstvy, na které definuje datovou jednotku datagram. Jak již bylo v předchozí části popsáno v současné době se využívá souběžně dvou verzí IP protokolu a to IPv4 a IPv6. Vzhledem k zaměření práce a poměru s jakým je dnes obou verzí v praxi používáno se popis omezí pouze na značně rozšířenější verzi IPv4.

Jelikož samotný návrh využívá služeb protokolů vyšších vrstev, je popis pouze jedné z verzí IP protokolu pro uvedení do problematiky plně dostačující. Popsané obecné principy jsou, v konečném důsledku na samotný návrh, totožné.

IP protokol, jakožto protokol síťové vrstvy, pracuje s adresami koncových stanic a jednotlivých hostitelských sítí, které se pro upřesnění označůjí jako IP adresy. Na základě IP adres je prováděno směrováni v síti. IP adresy (zdrojová IP adresa a cílová IP adresa) jsou, mimo další údaje, součástí záhlaví IP datagramů. S využitím všech těchto informací, obsažených v záhlavích datagramů, které ukazuje tabulka 2, poskytuje síťová vrstva službu bez spojení. Každý datagram je samostatná jednotka a musí proto obsahovat všechny potřebné údaje pro jeho přesnou identifikaci. Formát záhlaví datagramu IP protokolu verze 4 včetně popisu je zobrazen v tabulce 2.

4	4	8	16	
Verze	Délka záhlaví	ToS - typ služby	Celková délka paketu	
Identifikace			Návěští	Číslo fragmentu
Životnost		Číslo protokolu	Zabezpečení záhlaví	
Zdrojová IP adresa				
Cílová IP adresa				
Volitelné možnosti				
Data (maximálně 65535 - délka záhlaví bytů)				

Tabulka 2: Formát IP datagramu

Služeb síťové vrstvy realizované IP protokolem využívají dva další protokoly reprezentující transportní vrstvu rodiny TCP/IP protokolů. Jde o protokoly TCP (Transmition Control Protocol) a UDP (User Datagram Protokol).

3.3 Transportní vrstva

Podobně jako v případě mezisíťové vrstvy i vrstva transportní koresponduje svými vlastnostmi a funkcemi s transportní vrstvou modelu RM-OSI. Funkce transportní vrstvy zajišťují v architektuře TCP/IP dva základní protokoly TCP (Transmition Control Protocol) a UDP (User Datagram Protocol).

3.3.1 TCP

Protokol TCP realizuje přenos se spojením, definuje jednotku paket a k přenosu sítí využívá služeb síťového protokolu IP. Poskytuje službu virtuálního okruhu pro spolehlivý přenos dat mezi koncovými účastníky. TCP realizuje funkce jako navázání a rušení relace, segmentace dat, číslování paketů, detekce, oprava chyb atd. Formát záhlaví je zobrazen v tabulce 3.

3.3.2 UDP

Protokol UDP podobně jako TCP využívá služeb síťového protokolu IP. Na transportní vrstvě definuje jednotku paket a poskytuje transportní službu bez spojení. Je určen pro aplikace, které nepotřebují zabezpečení v takovém rozsahu, jako nabízí protokol TCP. Pakety UDP se dále nefragmentují, proto platí jednoznačné mapování do datagramu IP. Protokol UDP jen doplňuje informace přenášené již v datagramu

16		**16**	
Zdrojový port		Cílový port	
Pořadové číslo			
Číslo potvrzení			
Délka záhlaví	Rezervováno	Funkce řízení	Šířka okna
Kontrolní součet		Označení urgentních dat	
Volitelné možnosti			
Data			

Tabulka 3: Formát paketu TCP

IP tak, aby mohl nabízet služby na vrstvě shodné s protokolem TCP. Záhlaví paketu UDP je uvedeno v tabulce 4.

16	**16**
Zdrojový port	Cílový port
Délka	Kontrolní součet
Data	

Tabulka 4: Formát paketu UDP

3.4 Aplikační vrstva

Nejvyšší vrstva architektury TCP/IP je vrstva aplikační. Aplikační vrstva architektury TCP/IP plní funkce tří nejvyšších vrstev modelu RM-OSI, tj. vrstvy relační, prezentační a aplikační.

Na obrázku 1 je naznačena vazba některých protokolů aplikační vrstvy na protokoly vrstvy transportní. Na jaký protokol transportní vrstvy má konkrétní protokol aplikační vrstvy vazbu je dáno jeho návrhem.

Některé protokoly aplikační vrstvy jsou přímo svázané s konkrétním transportním protokolem, příkladem mohou být protokoly pro přenos elektronické pošty (SMTP), webových stránek (HTTP) či protokol pro přenos souborů (FTP).

Další skupina obsahuje protokoly, které využívají pro přenos informací obou protokolů transportní vrstvy. To který protokol je použit je dáno funkcí, ke které je použit. Příkladem takového protokolu může být protokol pro komunikaci se servery doménových jmen (DNS). Komunikuje-li běžný klient se serverem DNS k přenosu informace je použit protokol UDP, v případě, kdy komunikace, sloužící k synchroni-

zaci informací, probíhá přímo mezi jednotlivými DNS servery, je k přenosu využito protokolu TCP.

Poslední skupinu tvoří protokoly, které mohou mít vazbu na libovolný z protokolů transportní vrstvy. To, který protokol bude v konkrétním případě použit je závislé na implementaci. Příkladem může být protokol pro řízení relací (SIP), který bude podrobněji popsán v jedné z dalších kapitol.

4 Signalizace v tradičních telefonních sítích

V době vzniku telefonní sítě, kdy veškeré telefonní hovory byly spojovány manuálně, byla signalizace mezi účastníkem a spojovatelkou omezena pouze na uzavření smyčky a vyzvánění. Signalizace tak, jak ji známe v dnešní době, se začala vyvíjet v roce 1890, kdy Almon B. Strowger sestrojil první automatický spojovací systém.

4.1 Základní principy

Signalizační systémy používané v tradiční telefonii se rozdělují do základních skupin podle toho, zda je signalizační spoj přímo asociován se spojem pro přenos hovorového signálu, či je využit společný signalizační spoj, který nemá přímou vazbu na spoj určený k přenosu hovorových dat.

- **Channel Associated Signaling (CAS)** - signalizace přidružená k hovorovému kanálu
- **Common Channel Signaling (CCS)** - sdružená signalizace využívající nezávislé přenosové cesty

Vzhledem k návaznostem v budoucích kapitolách budou následně popsány signalizační systémy z druhé skupiny, tedy CCS.

4.2 CCS

(Common Chanel Signaling)

Signalizace v sítích ISDN jsou založeny na sdružené signalizaci CCS (Common Chanel Signaling) poprvé použité v roce 1976. Systém CCS je založen na existenci signalizační sítě oddělené od hovorových cest. Principy používané v signalizační síti jsou zcela shodné s principy datových sítí s přepojováním paketů, však terminologie je odlišná. Tabulka 5 uvádí používané termíny v datových a signalizačních sítích.

Signalizační síť přenáší signalizační zprávy, které slouží k sestavení spojení, dohledu nad existující relací a k ukončení spojení. Signalizace používané v sítích ISDN můžeme rozdělit na signalizace síťové a signalizace přístupové.

Koncept	Datové sítě	Signalizační sítě
Uzel sítě	Node (Uzel)	Signal Transfer Point (Signální přenosový bod)
Spoj	Data Link (Datový spoj)	Signal Data Link (Signalizační spoj)
Datová jednotka	Packet	Signal Unit (Signální jednotka)
Koncový účastník	DTE - Data Terminal Equipment (Koncový terminál)	Signal Point (Koncový signální bod)

Tabulka 5: Termíny používané v popisu signalizační sítě

4.3 Síťová Signalizace

(Interexchange Signaling)

Síťové signalizace slouží k sestavování spojení mezi jednotlivými ústřednami v síti. Pomocí síťové signalizace jsou sítí dále přenášeny informace o koncových účastnících, požadavky na kvalitu nosné služby, informace o službě a požadavky na její změnu během přenosu atd. Jako klasický příklad síťové signalizace je možno jmenovat signalizační systém č.7 (SS7).

4.4 Přístupová Signalizace

(Subscriber Signaling)

Přístupová signalizace, jak název napovídá, slouží pro přístup koncových účastníků k síti (respektive k sítím). Přístupové signalizační systémy ISDN jsou schopny sestavit spojení nejen v telefonní, ale i v datové síti. Stejně tak je možné sestavovat spojení jak po síti se spojováním okruhů (circuit switched network), tak v síti se spojováním paketů (packet switched network). V dnešní době je klasickým případem moderní digitální přístupové signalizace DSS1 (Digital Subscriber System No.1) podrobně popsaná v doporučení ITU-T Q.931.

4.5 Signalizace ve veřejných sítích

V současné době je telefonní síť je složena z mnoha různých zařízení všech generací, dále je k veřejné telefonní síti připojeno množství privátních telefonních sítí.

Aby byla zaručena funkčnost takto složitého systému je nutné přesně specifikovat vlastnosti jednotlivých signalizačních systémů používaných v síti. Ve veřejné síti je standardizace zaručena mezinárodní společností ITU.T (dříve CCITT) již velice dlouhou dobu. V dnešní době je jedinou mezinárodně standardizovanou síťovou signalizací ISDN pro použití ve veřejné telefonní síti signalizační systém SS7. Obdobně existuje doporučení přístupové signalizace. Signalizace doporučená pro přístup k síti ISDN je DSS1 (Digital Subscriber System No.1).

4.6 Signalizace v pobočkových sítích

Zavádění digitálních signalizačních systémů do prostředí privátních telefonních sítí šlo cestou odlišnou. Společnosti zabývající se vývojem a výrobou pobočkových telefonních systémů začaly vyvíjet každý svůj vlastní digitální signalizační systém. Většina těchto signalizačních systému vycházela z veřejné telefonní sítě známého signalizačního systému SS7. Takto vznikající digitální signalizační systémy byly navzájem neslučitelné a nebyla možná spolupráce pobočkových telefonních ústředen různých výrobců v jedné privátní síti. Pochopitelně paralelně se vznikem mnoha síťových signalizačních systémů vznikala řada přístupových signalizačních systémů sloužících pro připojení digitálních telefonních přístrojů a datových měničů. Z této doby pochází například signalizační systém Cornet firmy Siemens, který sloužil jak pro propojení ústředen HiCom v rámci jedné sítě, tak jako přístupová signalizace.

Prvním pokusem ujednotit onu nepřehlednou situaci byl signalizační systém DPNSS (Digital Private Network System Signaling). Paralelně s tímto systémem byl vyvinut i systém přístupové signalizace k veřejné telefonní síti DAS (Digital Access Signaling). Dalším krokem byl vznik mezinárodně standardizované síťové signalizace pro použití v privátní síti Q-Sig, který postupně již téměř vytlačil navzájem neslučitelné signalizace různých výrobců.

4.7 Současný stav signalizačních sítí

Trend vývoje signalizačních sítí směřuje k zavedení jednotného signalizačního systému jak do sítí veřejných, tak do sítí privátních. Ve veřejných sítích jsou postupně vytlačovány signalizace používané systémy nižších generací (dochází k likvidaci těchto systémů a jejich nahrazování moderními spojovacími systémy čtvrté generace) a zavádí se systém sdružené ISDN signalizace SS7. Paralelně s tímto vývojem dochází k zavádění přístupového signalizačního systému DSS1 pro připojení privátních sítí a

koncových účastníků. I v privátních sítích dochází k postupnému vytlačování starších druhů signalizací a zavadí se jednotný systém Q-Sig. Vývoj směřuje k používání pouze výše zmíněných tří signalizačních systémů.

4.8 SS7

(Signaling System No.7)

Jedná se o robustní, mezinárodně standardizovaný, signalizační systém určený především pro použití ve veřejné telefonní síti. SS7 umožňuje nasazení technologie IN - Inteligentní síť (Inteligent Network) do telefonních sítí, spolupráci mobilních telefonních sítí jak mezi sebou, tak se sítí pevnou a další moderní služby až po širokopásmové sítě B-ISDN.

Ačkoliv byl signalizační systém SS7 primárně určen pro veřejné sítě, někteří výrobci implementovali jeho služby do svých pobočkových telefonních ústředen. Příkladem může být pobočková telefonní ústředna HiCom firmy Siemens či některé pobočkové systémy firmy Alcatel. Signalizace č.7 je také součástí operačního systému pro použití ve veřejné síti k pobočkové telefonní ústředně MD110 Ericsson. Nutno však podotknout, že se jedná o čínskou mutaci SS7, která je s původním doporučením zcela neslučitelná.

Přesná specifikace je uvedena v radě doporučení ITU.T Q.700.

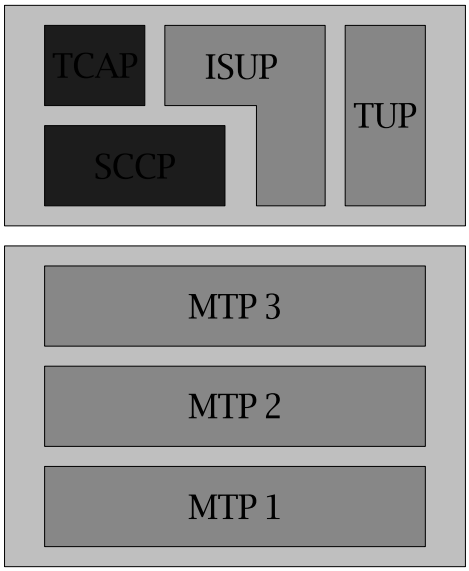
Obrázek 2 uvádí jednotlivé vrstvy SS7 a jejich vzájemnou spolupráci. Přesnější specifikace jednotlivých bloků bude uvedena v dalším textu.

4.8.1 Fyzická vrstva

Fyzická vrstva je v případě signalizačního systému SS7 označována jako MTP1 (Message Transfer Part Level 1). K přenosu signalizace č.7 se využívá přenosových kanálů v multiplexu I. řádu. Může být využito libovolného kanálového intervalu (mimo nultého, neboť ten nese synchronizační informace). Pro přenos signalizace v jednom směru může být využito libovolné množství signalizačních kanálů podle vytížení signalizační sítě v daném směru.

4.8.2 Spojová vrstva

Spojová vrstva nese dle doporučení označení MTP2 (Message Transfer Part Level 2). Druhá, spojová vrstva zaručuje synchronizaci signálních bodů, korekci a detekci



Obrázek 2: Referenční model signalizačního systému číslo 7

chyb při přenosu, tvorbu testovacích a výplňových bloků. Komunikace ve druhé vrstvě probíhá jen na signalizační cestě mezi sousedními signálními body.

Na úrovni druhé vrstvy se přenášejí tři typy signálních jednotek (Signal Units).

MSU (Message Signal Unit) Signální jednotka určená pro přenos signalizační zprávy

LSSU (Link Status Signal Unit) Tato signální jednotka slouží k sestavení signalizačního spojení při uvádění do provozu

FISU (Fill-In Signal Unit) Signální jednotka FISU slouží k vyplňování signalizační cesty v době, kdy není vysílána žádná signalizační zpráva

4.8.3 Síťová vrstva

Třetí, síťová vrstva (MTP3 - Message Transfer Part Level 3) tvoří rozhraní mezi uživatelskými vrstvami SS7 a nižšími přenosovými vrstvami. Zahrnuje procedury pro směrování v síti, doplňuje signalizační zprávy z vyšších vrstev o údaje umožnující toto směrování atd.

4.8.4 Služby vyšších vrstev

Na úrovní vyšších vrstev dochází k sestavování signalizačních zpráv pro vytváření, rušení a dohledu nad relacemi. Bloky SCCP (Signaling Connection Control Part) a

TCAP (Transaction Capabilities Application Part) slouží k zavedení služeb inteligentní sítě, jejich popis není součástí toho textu. Bloky TUP (Telephone User Part) a ISUP (ISDN User Part) jsou uživatelské vrstvy zahrnující procedury pro řízení spojení.

TUP je schopen sestavovat pouze telefonní relace a je historicky starší než ISUP. ISUP je schopný vytvářet všechny druhy spojení a dále nabízí všechny služby spadající do oblasti ISDN.

4.9 DSS1

(Digital Subscriber Signaling System No.1)

Signalizační systém DSS1 je v dnešní době jediným používaným signalizačním systémem mezi koncovým účastníkem ISDN a telefonní ústřednou, ke které je účastník připojen. Signalizační systém DSS1 vznikl na půdě organizace ITU-T, paralelně se síťovým signalizačním systémem č.7. DSS1 umožňuje účastníkovi využít veškerých služeb, které nabízí sítě typu ISDN.

4.9.1 Fyzická vrstva

Na úrovni první, fyzické vrstvy, se k přenosu signalizace využívá speciálních signalizačních D kanálů. Přenosové rychlosti pro D kanály se rozdělují podle druhu přístupu k ISDN síti.

- **Basic Rate Access (BRI)** - D kanál pro BRI (Basic Rate Access) má přenosovou rychlost 16 kb/s. Tento kanál je možné využít mimo přenos signalizačních zpráv také pro přenos uživatelských dat. Kanál je využit pro přenos uživatelských dat pouze pokud není nutné přenášet žádné signalizační zprávy. Přenos dat může být kdykoliv přerušen přenosem signalizační zprávy, neboť přenos signalizace má vyšší prioritu než přenos uživatelských dat. Možná rychlost pro přenos dat je 2400 b/s.

- **Primary Rate Access (PRI)** - Při spojení se sítí prostřednictvím přípojky PRI (Primary Rate Access) je přenosová rychlost D kanálu 64 kb/s. Přípojka PRI je realizována PCM multiplexem I. řádu. K přenosu D kanálu v tomto multiplexu se využívá výhradně 16. kanálový interval. I v tomto případě je možné D kanálem přenášet uživatelská data. Podle poslední revize doporučení ITU.T je tento přenos možný rychlostí až 9600 b/s.

4.9.2 Spojová vrstva

Na úrovni druhé, spojové vrstvy je pro přenos signalizace DSS1 doporučením předepsáno použití linkového protokolu LAP-D. LAP-D je bitově orientovaný linkový protokol, který vznikl dílčími úpravami ověřeného linkového protokolu HDLC pocházejícího z paketových sítí. Protokol je podrobně popsán v doporučení ITU.T X.25.

4.9.3 Přenos signalizačních zpráv řízení volání

Signalizační systém DSS1 je přístupový signalizační systém pro spojení typu bod - bod. Není proto nutné na úrovni třetí vrstvy přenášet údaje potřebné pro směrování v síti. Nad spojovou vrstvou je přenášena již přímo signalizační zpráva. Formát signalizační zprávy dle doporučení ITU.T Q.931 je uveden v tabulce 6.

Octets/Bits	8	7	6	5	4	3	2	1
a	Protocol discriminator							
	0	0	0	0	1	0	0	0
b	Call reference length							
	0	0	0	0	0	0	0	1
c	F	Call reference value						
d	Message type							
1	IE Identifier							
2	IE Length							
3	IE Contents (value)							
.								
.	Other IEs							
n								

Tabulka 6: Formát signalizační zprávy DSS1

Oktety v tabulce označené písmeny a - d představují hlavičku signalizační zprávy a oktety označené čísly 1 - n informační pole signalizační zprávy.

4.10 Q-Sig

Signalizační systém Q-Sig je jediným mezinárodně standardizovaným signalizačním systémem určeným pro použití v privátních sítích. Systém je jakousi obdobou signalizačního systému SS7 pro použití v privátních sítí. Z pohledu návrhu protokolu však signalizační systém Q vychází z osvědčeného a dobře fungujícího modelu signalizace DSS1.

Signalizační systém Q-Sig je podrobně popsán v doporučeních ETS 300 012, ETS ETS 300 125 a ETS 300 170 - ETS 300 173.

4.10.1 Fyzická vrstva

K přenosu signalizace Q se využívá 16. kanálu v multiplexu I. řádu, podobně jako v případě signalizace DSS1.

4.10.2 Spojová vrstva

Na úrovni druhé, spojové vrstvy je pro přenos signalizace Q doporučením předepsáno použití linkového protokolu LAP-D. Protokol spojové vrstvy byl převzat z doporučení ITU-T pro signalizaci DSS1

4.10.3 Přenos signalizačních zpráv řízení volání

Na úrovně třetí vrstvy definuje doporučení tři subvrstvy:

- **Q-SIG Basic Call (QSIG BC)** - protokol pro řízení běžných ISDN volání. Na rozdíl od protokolu DSS1 je však Q-SIG symetrickým protokolem, to znamená, že obě strany spoje disponují totožnými funkcemi.
- **Q-SIG Generic Functional Procedures (QSIG GF)** - subvrstva poskytuje standardizované mechanismy pro řízení doplňkových služeb v privátních sítích. Subvrstva poskytuje jak služby spojově orientované, tak bez spojení
- **Q-SIG Supplementary Services (QSIG SS)** - subvrstva definuje některé specifické funkce v referenčním bodě Q.

Část II
Současný stav problematiky

5 Signalizace v sítích TCP/IP

5.1 Protokol H.323

H.323 je doporučení definující protokol pro přenos hovorových signálů IP sítí vzniklé na půdě ITU-T. Jedná se o komplexní protokol, který poskytuje všechny služby nutné pro přenos jak signalizace, tak samotného hovorového signálu. Tento protokol se stal prvním mezinárodně standardizovaným protokolem pro přenos hovorových signálů po IP sítích. Protokol H.323 je binárně orientovaným protokolem. Na diagnostiku spojení je proto nutné použití speciálních a to jak softwarových, tak hardwarových prostředků.

5.1.1 Popis protokolu

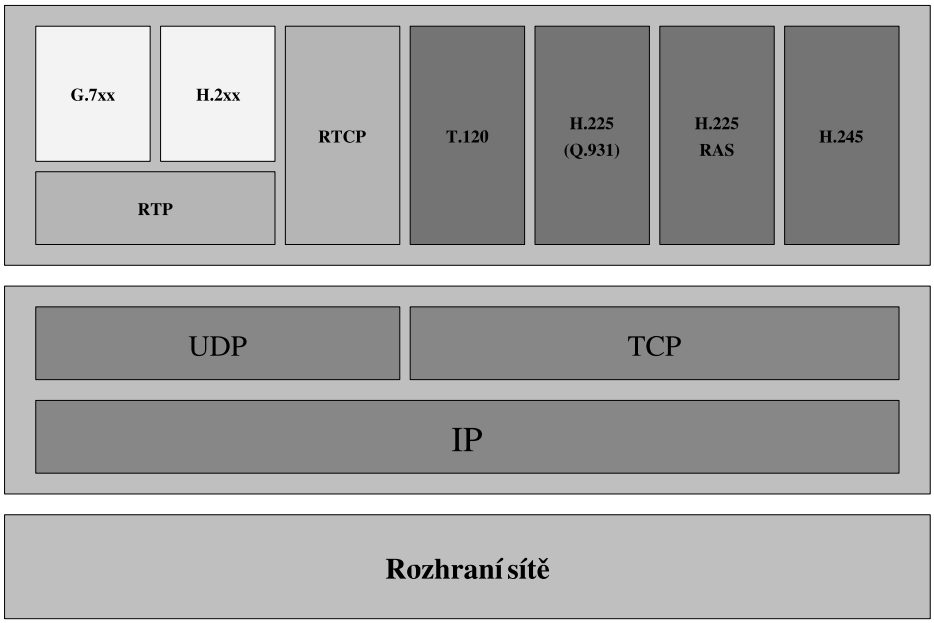
Protokol H.323 využívá pro přenos signalizačních informací služeb protokolu TCP. To zajišťuje spolehlivý přenos mezi jednotlivými účastníky spojení[2]. Návaznost jednotlivých protokolů z doporučení H.323 na protokoly rodiny TCP/IP znázorňuje obrázek 3. Typické využití jednotlivých portů protokolů TCP a UDP je uvedeno v tabulce 7

Vlivem nedostatků IP sítě, popsaných v kapitole 3, však může využití služeb protokolu TCP s sebou přinést i problémy, které se projeví velkým zpožděním relací protokolu H.323.

Port	Protokol	Popis	H.323 Klient	H.323 MCU	H.323 Gatekeeper
1503	TCP	T.120	*	-	-
1718	TCP	Gatekeeper Discovery	*	*	*
1719	TCP	Gatekeeper RAS	*	*	*
1720	TCP	H.323 - sestavení hovoru	*	*	-
1731	TCP	řízení spojení	*	*	-
1024 - 65535	TCP	H.245 (parametry hovorového kanálu)	*	*	-
1024 - 65535	UDP	RTP (video stream data)	*	*	-
1024 - 65535	UDP	RTP (audio stream data)	*	*	-
1024 - 65535	UDP	RTCP (řídící informace)	*	*	-

Tabulka 7: Porty využívané protokoly z doporučení H.323

[2]Účastníky spojení jsou zde myšleny dva koncové body spojení H.323, to nemusí nutně znamenat totožnost s koncovými účastníky telefonní relace.



Obrázek 3: Návaznosti protokolů dle doporučení H.323

Na vlastnostech protokolu se výrazně projevila skutečnost, že tvůrci protokolu měli velice blízko k technologiím telefonních sítí a poněkud opomněli výhodné vlastnosti a zvyklosti ze sítí počítačových. Protokol definuje v síti několik center a na jejich existenci a funkčnosti je závislá funkčnost celého systému. Tento přístup vnáší do celého systému potenciální nebezpečí selhání celku z důvodu poruchy pouze jedné z jeho částí. Odborníci z prostředí počítačových sítí se snaží maximálně odprostit od tohoto modelu a celý systém decentralizovat a tím zvýšit jeho odolnost proti proti možným poruchám. Na druhou stranu existence těchto center přináší řadu výhod, které umožňují například možnost adresace z využitím telefonních čísel[3], sběr dat nutných pro tarifikaci provozu, definovat centrálně brány pro určité směry atd.

Logická topologie sítě pro přenos hlasových dat s využitím protokolu H.323 je definovaná pomocí několika základních pojmů:

- **Entita** - Každá komponenta H.323, včetně terminálů, bran (Gateway), řadičů spojení (Gatekeeper), řadičů konferencí (Multipoint Controller) a dalších jednotek nutných pro zajištění spojení.
- **Koncový bod (Endpoint)** - Jedná se o koncové terminály, brány (Gateway) a řadiče konferencí (Multipoint Controller). Každý koncový bod sítě H.323 může

[3]V telefonní síti zcela běžný způsob identifikace koncového účastníka využívaný již téměř sto let.

sestavovat a rušit spojení, případně být volán. Každé hovorové spojení v síti H.323 začíná a končí vždy koncovým bodem.

- **Brána (Gateway)** - Bránou se rozumí rozhraní mezi sítí H.323 a jinými sítěmi. Brána je koncovým bodem H.323 sítě a zajišťuje v reálném čase dvoucestnou komunikaci mezi koncovými body z jedné H.323 domény a koncovými body jiných H.323 domén či jiných sítí.

- **Řadič spojení**[4] **(Gatekeeper)** - Řadič spojení je H.323 entita zajišťující překlad adres a řízení přístupu pro všechny H.323 koncové body tj. terminály, brány a ostatní příslušenství. Řadič spojení může pomocí signalizace dohlížet nad všemi službami, které síť nabízí koncovým účastníkům, včetně řízení a dohledu samotných spojení a sběr tarifních informací.

- **Řadič konference (Multipoint Controller)** - Řadič konference (zkráceně označovaný MC, či MCU) je stanicí, která řídí v reálném čase konferenci více uživatelů.

Přesná a úplná definice jednotlivých pojmů je součást doporučení ITU-T H.323.

Celý systém je možno provozovat ve dvou možných režimech:

1. **Sestavení spojení se provede přímo s koncovým účastníkem, nebo s bránou.** V tomto případě musí koncový bod, který spojení sestavuje znát ne jen telefonní číslo volaného účastníka, ale i IP adresu cíle. V případě, že hovor má být směrován mimo IP síť musí volající sám rozhodnout o použití určité brány, přes kterou bude hovorové spojení sestaveno. Tento způsob je použitelný pouze pro malé sítě u kterých není potřebný celkový dohled a tarifní údaje.

2. **Sestavení spojení provádí každý účastník sítě pomocí gatekeeperu.** V tomto případě postačuje k realizaci spojení znalost cílového telefonního čísla a IP adresa gatekeeperu. Volající účastník osloví gatekeeper, předá mu telefonní číslo, se kterým chce sestavit hovorové spojení. Gatekeeper disponuje údaji, podle kterých zjistí IP adresu kam má být volaní směrováno, případně určí vhodnou (většinou podle finančních nákladů) bránu, přes kterou bude hovor dále směrován mimo IP síť. Gatekeeper také vyhodnotí, zda má účastník na dané spojení kategorii a zaznamená údaje nutné pro zpoplatnění služby.

[4] Termín *„řadič spojení"* je převzat z [11], autorovi se zdál býti výstižnější než například *„strážce brány"*

5.1.2 Adresace

K adresaci účastníků v síti H.323 se používá běžných telefonních čísel, jako v tradiční telefonní síti dle doporučení ITU-T E.164. Přepočet na IP adresy provádí, pro menší sítě, sám koncový účastník (přesněji jeho koncové zařízení), nebo gatekeeper v případě složitějších sítí.

5.1.3 Spolupráce s tradiční telefonní sítí

Spolupráce s tradiční telefonní sítí není v případě H.323, z pohledu doporučení, téměř žádný problém. Při dodržení doporučení E.164 pro mezinárodní číslovací plán ISDN je možné dosáhnout stavu, kdy koncoví účastníci nepoznají rozdíl mezi spojením v síti H.323 a v klasické telefonní síti[5].

5.2 Protokol SIP

(Session Initiation Protocol)

Alternativním protokolem k výše popsanému H.323 je protokol SIP a návazné protokoly navržené odborníky z IETF. Protokol SIP jako takový je určen pouze k přenosu signalizace, všechny ostatní funkce nutné pro realizaci služeb VoIP obstarávají další podpůrné protokoly jako SDP, RTP, RTCP a další.

5.2.1 Popis protokolu

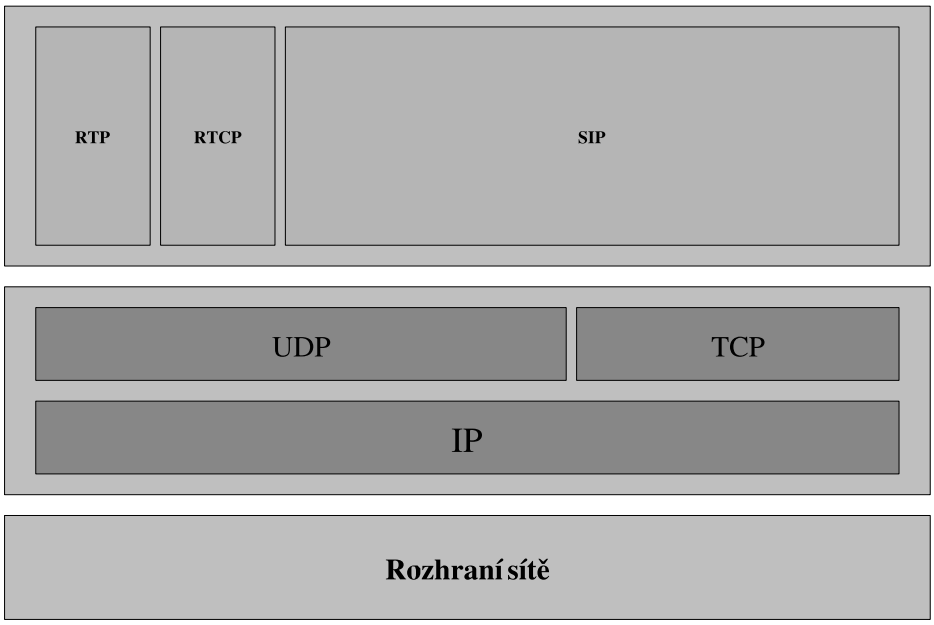
Přístup k řešení problému tj. k přenosu hovorových signálů IP sítí je diametrálně odlišný od přístupu který je použit u protokolu H.323. Zatímco ITU-T vyřešilo problém jedním protokolem poskytující veškeré potřebné služby pro realizaci přenosu hovorového signálu, IETF zvolilo cestu, běžnou z prostředí sítě Internet, kterou je vytvoření řady protokolů realizující pouze konkrétní část služeb nutných pro přenos hovorových dat, jako například signalizaci, či přenos multimediálních informací. To umožňuje v případě potřeby výměnu pouze jednoho elementárního protokolu a tím snadnou úpravu celého systému.

Protokol SIP vychází z osvědčených a praxí ověřených protokolů jako HTTP (Hyper Text Transfer Protocol), či SMTP (Simle Mail Transfer Protocol), jedná se proto

[5]Myšleno tím rozdíl v průběhu sestavování spojení. V průběhu sestaveného spojení bude vždy patrný rozdíl v kvalitě přenášeného signálu.

o protokol realizující spojení klient - server. Protokol je znakově orientovaný. To umožňuje použití (v IP síti) běžných technických prostředků pro diagnostiku přenosu, jako například softwarový nástroj tcpdump, známý z prostředí operačního systému Unix, k monitorování druhu a obsahu přenášených paketů. Není proto nutný nákup speciálního programového vybavení, případně zařízení pro diagnostiku provozu.

V případe protokolu H.323 je přenos signalizace realizován výhradně prostřednictvím protokolu TCP. V návrhu protokolu SIP není přímá vazba na některý z protokolů transportní vrstvy modelu TCP/IP. V doporučení je preferován protokol UDP, většina konkrétních implementací také právě protokol UDP využívá, přesto je možné využít k přenosu též protokol TCP. Návaznost protokolu SIP a dalších souvisejících protokolů je patrná z obrázku 4. Na komunikaci pomocí protokolu SIP byl vyhrazen port 5060.



Obrázek 4: Návaznosti protokolu SIP na model TCP/IP

Na rozdíl od protokolu H.323 je použita strategie maximální decentralizace řízení, protokol nedefinuje žádná centrální místa v síti, komunikace probíhá výlučně mezi koncovými body. Tento přístup podstatně zvyšuje odolnost celého systému vystavěného na službách protokolu SIP jak proti výpadkům některých jeho částí, tak proti výpadkům IP sítě. Na druhou stranu je velký problém se sběrem údajů nutných pro zpoplatňování hovorů. Není téměř možné využít systém zpoplatňování telekomunikačních služeb známý z prostředí tradičních telefonních sítí. Zpoplatňování telefonních hovorů je nutné převádět na platby za množství přenesených dat do okolních sítí, či

paušální poplatky.

Tuto nevýhodu je možné potlačit realizací funkcí tzv. softswitche. Jedná se o centrální místo v síti, které se ke koncovým účastníkům chová obdobně jako běžný spojovací sytém známý z tradiční telefonie. Všechna realizovaná spojení jsou v tomto případě směrována přes toto centrální zařízení. Takto navržený model telefonní sítě však do značné míry popírá původní záměr se kterým protokol vznikal.

V doporučení IETF pro protokol SIP jsou definovány čtyři základní prvky sítě:

- **Uživatelský agent (User Agent)** - Uživatelská aplikace, umožňující koncovým účastníkům sítě obousměrnou komunikaci pomocí protokolu SIP. User Agent (UA) je dále rozdělen na dvě části:
  - **UA Client** - klientská část uživatelského agenta sloužící k sestavování a řízení odchozích relací
  - **UA Server** - serverová část uživatelského agenta sloužící k přijetí a řízení příchozích relací
- **SIP Proxy Server** - provádí funkce jako: hledání účastníka v koncové síti, směrování hovorů (spolupráce s Firewallem či NATem), zprostředkování styku s jinou sítí.
- **SIP Redirect Server** - směruje volání jiným serverům v síti.
- **SIP Registrar** - slouží k registraci koncových uživatelů (obdoba HLR u GSM)

Přesná definice pojmů je součástí patřičných doporučení RFC od IETF.

Při sestavování spojení se vždy využívá doménové jméno stroje v síti IP. V prvním kroku se provede hledání IP adresy koncového účastníka případně SIP serveru pomocí DNS (Domain Name Service). Dalším kroku se sestaví spojení s koncovým účastníkem, případně se využije služeb nějakého SIP serveru, není-li možné sestavit spojení přímo (například když je účastník umístěný za Firewallem či NATem, nebo je mobilní). Směruje-li se spojení mimo síť SIP protokolu, musí volající účastník sám rozhodnout, kterou bránu pro spojení použije a znát její doménovou, případně IP adresu. Tento problém je však již v současné době řesitelný pomocí proxy serveru a jeho vhodné konfigurace.

5.2.2 Adresace

K adresaci koncových účastníků v síti se využívá formátu zápisu shodného pro zápis e-mailových adres. Směrování v IP síti se pak provádí na základě IP adresy, která se určí využitím služby DNS.

5.2.3 Spolupráce s tradiční telefonní sítí

Spolupráce sítě, která využívá služeb protokolu SIP s běžnou telefonní síti je velice obtížné. Při odchozím spojení z IP sítě směrem k tradiční telefonní je možné využití odchozí brány[6]. Určení volaného se provede zápisem SIP adresy ve tvaru například: +420224531111@sipgw.praha.supertel.cz. Přesný formát, ve kterém bude uváděno před „zavináčem" není standardizován a je čistě v rukou provozovatele sítě. Telefonní číslo v uvedeném příkladu by proto mohlo být také ve tvaru 24351111, nebo 224351111 či 022435111 atd.

Spojení v opačném směru tj. ze sítě telefonní do sítě IP s protokolem SIP není možné jednoduše realizovat. Tuto velkou nevýhodu, která je způsobená použitým způsobem adresace, je možné částečně odstranit zavedením přepočtů na některém SIP proxy severu.

5.2.4 SIP INFO

Metoda SIP INFO rozšiřuje protokol SIP o možnost přenosu dalších doplňkových informací vztažených k sestavené relaci. Tato metoda není určena k řízení spojení sestavených pomocí základní signalizace SIP, neslouží ani k přenosu informací, které by vedly ke změně stavu již sestavené relace. Jedná se o rozšíření komunikačních vlastností systému postaveném na protokolu SIP a tím o zlepšení nabízených služeb. Přesný popis tohoto rozšíření protokolu SIP je uveden v [20].

Metodu SIP INFO je možné použít k přenosu informací mezi koncovými body prostřednictvím signalizační cesty. Toho lze s úspěchem využít například k přenosu DTMF znaků vysílaných během sestaveného spojení, či k přímému přenosu signalizace mezi dvěma bránami na hranicích se sítěmi tradiční telefonie. K přenosu těchto doplňkových informací se využívá těla zprávy v protokolu SIP, kam jsou informace pomocí speciálních MIME kontejnerů mapovány. Přesný způsob mapování je popsán v příslušných RFC doporučeních.

[6] Známe-li adresu brány pro oblast, kam se chceme dovolat. V opačném případě se nám volání sestavit nezdaří.

Značnou výhodou tohoto řešení je implementace poměrně mocného komunikačního nástroje při současném zachování jednoduchosti protokolu. Na druhou stranu telefonní signalizace z prostředí tradiční telefinie jsou mapovány ve své původní, tedy binární, podobě. To částečně popírá jednu ze základních vlastností protokolu SIP a to jeho textovou orientaci.

5.3 MGCP

(MediaGateway Control Protocol)

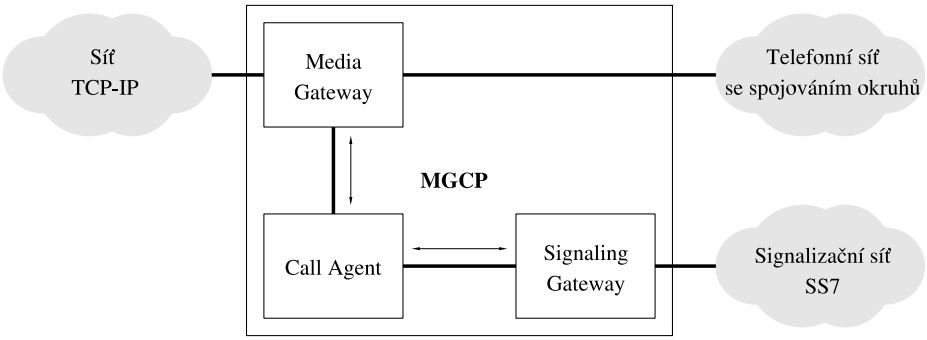
Na rozdíl od H.323 a SIP, kde jsou koncové uzly relativně samostatné a řídícími centy komunikují prostřednictvím krátkých ucelených zpráv, je v modelu MGCP situace naprosto odlišná. Protokol MGCP, jak již jeho název napovídá řídí sestavení spojení pomocí sledu kroků, kdy řídící systém postupně předává koncovému bodu povely, jak se má v dané chvíli zachovat. Návrh protokolu, podobně jako v případě SIPu, pochází z od IETF a je podrobně popsán v RFC2705.

5.3.1 Popis protokolu

V případě protokolu MGCP se nejedná o signalizační protokol jako v případě protokolu H.323 nebo SIP. Návrh protokolu MGCP počítá s jeho nasazením na komunikačních cestách mezi řídícím systémem a bránou, respektive bránami na rozhraní sítí. Samotná komunikace, která mezi řídícím systémem a bránou probíhá se skládá z příkazů, posílaných řídícím systémem, které přímo řídí chování brány a informací kterými brána informuje centrální řídící systém o změnách svého stavu.

Doporučení IETF pro protokol MGCP rozděluje bránu - gateway, tedy rozhraní mezi sítěmi různého typu, na tři funkční bloky:

- **Media Gateway (MG)** - Slouží ke konverzi samotných multimediálních dat mezi jednotlivými sítěmi
- **Signalling Gateway (SG)** - Slouží ke konverzi telefonní signalizace mezi jednotlivými sítěmi
- **Call Agent** - Řídící blok celé brány, komunikuje jak s MG, tak s SG. Ke komunikaci je použito právě MGPC protokolu.



Obrázek 5: Blokové schéma gatewaye

Blokové schema architektury brány je uvedeno na obrázku 5. Přesná definice pojmů je součástí patřičných doporučení RFC od IETF.

Na rozdíl od H.323 nebo SIP, je MGCP (Media Gateway Control Protocol) přísně hierarchický. Komunikace mezi call agentem a jednotlivými bránami probíhá metodou Master/Slave. Řídící komunikace mezi call agentem a bránou je proto během sestavování spojení výrazně intenzivnější, to umožňuje lépe centralizovat příslušné funkce, jako například správu číslovacího plánu, autentizaci, autorizaci a sběr tarifních informací. V případě bran do ISDN je obvyklá implementace tím způsobem, že signalizační kanál ISDN je přímo ke call agentu, který se stará i o signalizaci s vnějšími telefonními sítěmi a bráně pouze přes MGCP říká, na kterých kanálech ISDN linky má zpracovávat hovory.

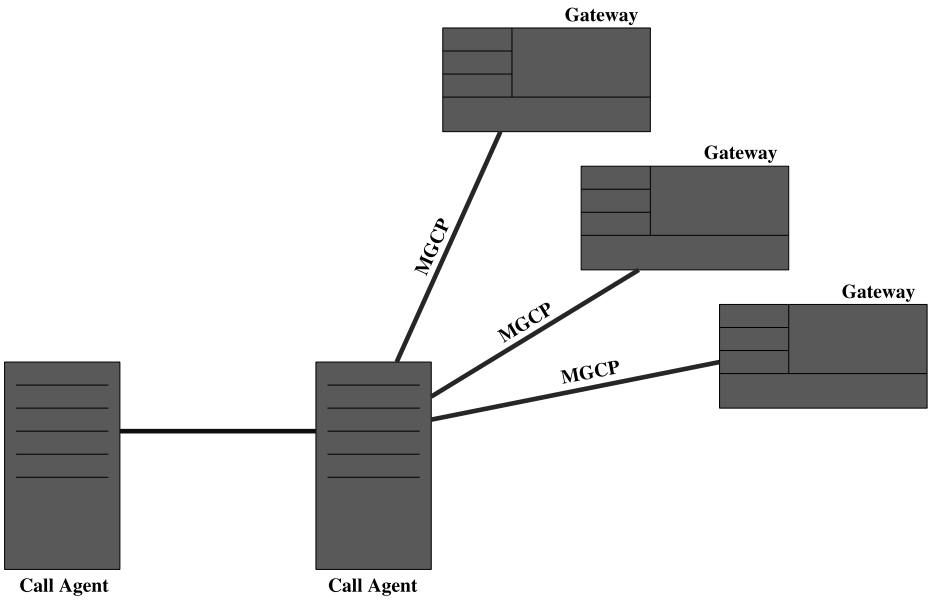
MGCP v běžných implementacích využívá na úrovni transportní vrstvy k přenosu informací napříč sítí TCP/IP protokol UDP. Na komunikaci prostřednictvím MGCP protokolu byl alokován port 2427.

MGCP naopak nedefinuje žádná pravidla na komunikaci mezi jednotlivými Call Agenty, případně call agenty a jinými řídícími bloky sítě. Tato komunikace pak často probíhá za použití jednoho z výše uvedených protokolů, tedy H.323, nebo SIP. Typické nasazení MGCP protokolu v síti naznačuje obrázek 6.

Protokol MGCP je vhodný pro velké sítě s jednotnou správou a umožňuje robustní řešení VoIP komunikace.

5.3.2 Spolupráce s tradiční telefonní sítí

Jelikož protokol MGCP je přímo navržen pro řízení bran mezi různými sítěmi a popis brány mezi tradiční telefonní sítí na bázi spojování okruhů je přímo součástí doporučení, není ve spolupráci s tradiční telefonní sítí téměř žádný problém. Existují



Obrázek 6: Návaznosti protokolu MGCP na model TCP/IP

také jasné definice pro napojení na signalizační systémy ISDN, konkrétně SS7.

5.4 IAX

(Inter Asterisk eXchange)

Protokol IAX byl původně navržen pro interní komunikaci v pobočkovém spojovacím systému Asterisk vyvíjeném na bázi Open Source společností Digium. Jeno název vnikl proto přímo z názvu projektu, Inter-Asterisk eXchange. Protokol IAX není standardizován žádným standardizačním orgánem. V současné době se pracuje na přípravě RFC dokumentu.

5.4.1 Popis protokolu

IAX je obecně velmi robustní a plnohodnotný protokol, zároveň je však jednoduchý. Jde o protokol typu peer-to-peer, koncové body udržují stavy asociované s protokolovými operacemi. IAX lze použít jako transportní protokol prakticky pro všechny typy přenášených dat. U hlasového přenosu protokol nerozeznává používané kodeky. IAX design byl vytvořen na základě zkušeností s mnoha dnešními řídícími a přenosovými standardy včetně Session Initiation Protocol (SIP), Media Gateway Control Protocol (MGCP) pro řízení a Real-time Transfer Protocol (RTP) pro streamování

média přenosu.

Hlavním rozdílem proti v předchozím textu uvedeným protokolům je multiplexování signalizace a vícenásobných multimediálních toků do jediného UDP toku mezi dvěma koncovými body. Uvedeným způsobem se dosahuje hned několika výhod proti protokolům používajících tradičních metod. Jelikož je samotný datový tok nesoucí hovorová data přenášen totožnou cestou jako signalizační informace, odpadají veškeré problémy s firewally a překladem adres známé z protokolů H.323 a SIP. Druhou výhodu, kterou návrh protokolu přináší, je značná úspora v množství přenášených dat a tím větší množství možných hovorů při zachování kapacity sítě.

Celý návrh má však i své zápory. Prvním z nich je binární orientace protokolu, případné hledání problémů v komunikaci se tak značně komplikuje a je nutné využít speciálních softwarových prostředků k dekódování přenášených informací. Druhým problémem je právě společný komunikační kanál jak pro signalizaci, tak pro přenos multimediálních informací. Implementace takto navrženého protokolu je poněkud komplikovanější a může s sebou nésti úskalí v podobě problémů při uvádění konkrétní implementace do provozu a hledání možných programátorských chyb. Podobně může dojít i ke komplikacím v hledání problémů a trasování spojení v produkční síti.

5.4.2 Spolupráce s tradiční telefonní sítí

Projekt Asterisk od svého počátku počítá s přímou spoluprací s tradiční telefonní sítí. Protokol IAX byl navržen jako součást projektu Asterisk a tudíž jeho návaznost na telefonní síť, používající k adresaci běžný ISDN číslovací plán dle doporučení ITU-T, je v návrhu zohledněna. Z pohledu signalizace je portfolio zpráv v podobném rozsahu jako v případě protokolu SIP.

6 Srovnání popsaných protokolů pro VoIP

6.1 Srovnání protokolů

Při srovnání popsaných protokolů nutno konstatovat, že nelze jednoznačně prohlásit, který protokol je ten vhodný[7].

Protokol H.323 má nesporné výhody, které umožňují jednoduchou spolupráci s tradiční telefonní sítí, nabízí služby nutné pro zpoplatňování provozu a v současné době je již běžně implementován v síťových prvcích (například od firmy Cisco). Na druhou stranu se jedná o protokol, který se bude jen těžko dále vyvíjet, neboť je velice komplexní a úpravy by zcela určitě způsobovaly zpětnou nekompatibilitu. Další nevýhodou je jeho binární orientace, která s sebou přináší řadu problémů při monitorování a měření provozu.

Protokol SIP je jednoduchý, flexibilní a snadno implementovatelný protokol. Další jeho vývoj není problém, lze proto v brzké době očekávat řadu dalších vylepšení. Jeho implementace se začíná pomalu objevovat v nových verzích operačních systému pro síťové prvky (například je již součástí nových IOSů k zařízení firmy Cisco). Nutno však ukázat na dvě hlavní nevýhody:

1. Problematická spolupráce s tradiční telefonní sítí. Některé služby nelze dokonce obousměrně realizovat. Chceme-li potlačit tyto problémy, dochází k degradaci vlastností protokolu.

2. Problémy se sběrem tarifních informací, běžný model zpoplatňování služeb nelze na síť s protokolem SIP nasadit a je nutné hledat další metody, jak vhodně zajistit ocenění nabízených služeb.

Vážnou nevýhodou obou protokolů je poměrně složitá spolupráce s hraničními prvky privátních sítí, jako je FireWall a NAT. Jelikož je IP adresa jednotlivých konců spojení součástí obsahu paketu a ne jen jeho záhlaví, není možné uskutečnit spojení přes výše uvedené prvky bez jejich úpravy, či bez pomocného proxy serveru. To může být značnou překážkou při nasazování uvedených protokolů do běžného provozu, kdy z důvodu nedostatku IP adres využívá většina podnikových sítí privátních rozsahů. Tento problém vyřeší nasazení protokolu IPV6[8].

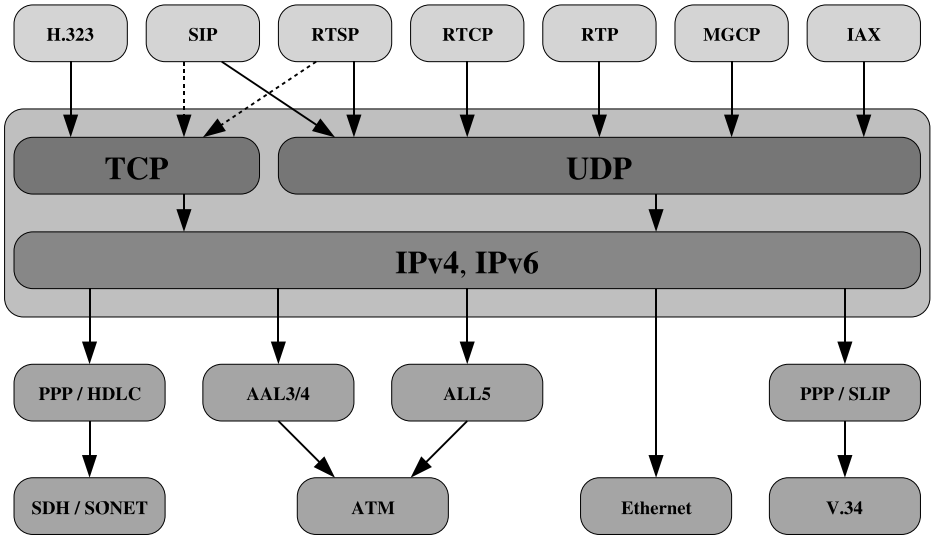
[7] Toto je názor autora, který vyplývá ze studia vlastností obou protokolů a praktických zkušeností se skutečným provozem.

[8] Stále avizované nasazení protokolu IPV6 však není otázkou blízké budoucnosti, jak by se mohlo na první pohled zdát.

Problémy s Firewallem a NATem jsou plně potlačeny v návrhu protokolu IAX, který ke komunikaci používá jeden společný kanál pro přenos veškerých informací mezi dvěma koncovými body. Velkou nevýhodou tohoto protokolu je, že doposud neexistuje platný standard a tudíž je velice obtížné protlačit tento protokol ve větší míře do praxe. Dalším problémem, který pravděpodobně způsobuje též zpomalení procesu přijímání doporučení, je binární orientace protokolu.

Dalším popisovaným protokolem je MGCP. Protokol je určený pro komunikaci mezi bránami a společným řídícím centrem. Velkou výhodou protokolu, je že umožňuje bezproblémovou návaznost na ISDN signalizační systémy a tím velice dobrou spolupráci s tradičními telefonními sítěmi. Z pohledu provozovaní sítě je jistou nevýhodou nutnost jednotné správy všech zařízení, komunikujících prostřednictvím MGCP protokolu.

Srovnání jednotlivých protokolů z pohledu návaznosti na model TCP/IP je patrné z obrázku 7.



Obrázek 7: Návaznosti jednotlivých VoIP protokolů na TCP/IP model

Tabulka 8 uvádí přehledné srovnání protokolů z pohledu jejich návrhu, funkce a spolupráce s okolními sítěmi.

	H.323	**SIP**	**MGCP**	**IAX**
Transportní protokol	TCP	UDP/TCP	UDP	UDP
Peer-to-peer	ANO	ANO	NE	ANO
Problém s Firewallem	ANO	NE	NE	NE
Problém s NATem	ANO	ANO	ANO	NE
Samostatný komunikační kanál pro signalizaci	ANO	ANO	ANO	NE
Samostatné doporučení pro signalizační protokol	NE	ANO	ANO	NE
Přímá kompatibilita s ISDN signalizací	ANO	NE	ANO	NE
Textově orientovaný protokol	NE	ANO	ANO	NE

Tabulka 8: Srovnání protokolů pro VoIP

Část III

Cíle disertační práce

7 Výchozí požadavky pro návrh protokolu

Na základě skutečností popsaných v předchozích kapitolách vznikly první základní požadavky kladené na návrh nového protokolu. Během práce na návrhu protokolu došlo ještě k jejich upřesnění a vyvstaly též další problémy jejichž řešení bylo nutné v celkové koncepci návrhu vzít v úvahu.

Počáteční podmínky a vstupní požadavky ze kterých celý návrh vychází lze shrnout a popsat v několika blocích, které jsou jako součást této kapitoly uvedeny v následujícím textu.

7.1 Nezávislý protokol pro signalizaci

Cílem práce je položit základy pro návrh signalizačního protokolu, nezávislého na přenosové cestě použité pro přenos samotných multimediálních informací. Nejde jen o vytvoření protokolu k řízení spojení uvnitř TCP/IP prostřednictvím nezávislého spojení, záměrem práce je položit základy signalizačního protokolu, který pro potřeby přenosu zpráv bude využívat síť TCP/IP, avšak dokáže řídit spojovací procesy na libovolném médiu. To znamená, že samotný přenos multimediálních informací nebude vázán jen na síť TCP/IP, ale bude možno využit v podstatě libovolné prostředí včetně dosavadních telefonních sítí na principu spojování okruhů.

7.2 Úplnost signalizace

Jednou ze základních podmínek je schopnost signalizačního protokolu postihnout všechny stavy, které mohou nastat během spojovacího procesu. Je nutné, aby obdobně jako v signalizačních systémech známých z tradiční telefonie, byly spojovací systémy či brány, instalované na rozhraní různých sítí pracující s různými signalizačními systémy, schopny informovat protistranu o jakékoliv skutečnosti, ke které dojde během celého spojovacího procesu. Jen tak lze zajistit korektní fungování celé telefonní sítě a správné informování účastníků o stavech sestavovaného spojení pomocí sady tónů nebo hlásek.

7.3 Návaznost na současné signalizační systémy

Aby bylo možné nový protokol zaintegrovat a plně využívat v současných telefonních sítích je nutné se podrobně zaměřit na schopnosti nového protokolu spolupracovat s dosavadními signalizačními systémy. V první řadě je nutné, aby nový signalizační systém plně spolupracoval se signalizacemi používanými v současné době v tradičních telefonních sítích, konkrétně tedy hlavně ISUP, DSS1 (Q.931) a Q-sig. Je tedy nutné navrhnout systém jednotlivých signalizačních zpráv a jejich parametrů, tak aby umožnil přenos všech informací přenášených doposud používanými protokoly pro přenos telefonní signalizace. Mimo to je nutné systém doplnit o další zprávy a jejich parametry, tak aby pokryl i nové požadavky vycházející z vlastností hostitelské sítě a potřeb nově se rozvíjejících služeb poskytovaných telefonní sítí.

7.4 Síťová signalizace

V tradiční telefonii je možné používané signalizační protokoly rozdělit, mimo jiné, na dvě základní skupiny, jak bylo popsáno v kapitole 4. První z nich je skupina síťových signalizací,které realizují spolupráci jednotlivých spojovacích systémů uvnitř páteřních sítí a do druhé skupiny je možné zařadit signalizační systémy používané pro přenos řídících a dohledových informací mezi koncovým účastníkem, či skupinou účastníků a páteřní sítí.

- **Síťová signalizace** Ať již se jedná městské sítě, transitní sítě globálních operátorů, či jen pobočkové sítě provozované některými velkými společnosti pro vlastní potřebu je nutné, aby použitý signalizační systém splňoval požadavky vycházející ze samotného účelu nasazení toho systému jako systému síťové signalizace.

  Jelikož se jedná o komunikaci mezi rovnocennými prvky sítě je požadováno, aby použitý protokol byl symetrický a umožnil tak oběma stranám využít shodný rozsah prostředků. Konkrétně je tedy možné, aby libovolná strana mohla zahájit komunikaci o sestavení telefonního spojení, disponovala shodnými prostředky pro jeho dohled a přenos doplňujících informací během sestaveného spojení a na závěr mohla využít shodných metod k ukončení realizovaného spojení. Přitom samotná komunikace mezi jednotlivými stranami bude z principu totožná bez ohledu na to, která ze stran komunikaci započala.

  Dalším důležitým požadavkem na síťovou signalizaci je schopnost umožnit oběma

komunikujícím stranám včas rozpoznat problémy s daným signalizačním spojem a poskytnout možnost využití záložního spoje, pokud tento existuje.

V případě síťové signalizace je vždy předem znám partner pro komunikaci, jeho identifikace, vlastnosti a možnosti, kterými disponuje a podobně. V běžné telefonní síti je spojovací systém, či brána spojující sítě využívající k přenosu odlišných transportních metod, spojen s omezeným množstvím sousedů. Je tedy možné bez nejmenších problémů uvést všechny sousedy, tedy partnery pro komunikaci prostřednictvím signalizačního systému, v konfiguraci spojovacího systému či brány. Tento postup je zcela běžný v případe tradiční telefonní sítě pracující se signalizačním systémem číslo 7.

- **Přístupová signalizace** V případě přístupových signalizací je situace odlišná. Ke spojovacímu systému bývá obvykle připojeno velké množství koncových účastníků, jejich vlastnosti a možnosti často nejsou jasně dopředu známé a tudíž je není možné jednotlivě a jasně popsat jako součást konfigurace systému. Je proto nutné zjištění stavu zajistit pomocí funkcí signalizačních protokolů.

  Z důvodů popsaných v minulém odstavci není většinou možné zajistit průběžný dohled všech signalizačních spojení ke všem koncovým účastníkům. To v praxi znamená, že případný problém je detekován až při pokusu o komunikaci na daném spoji. V jonečném důsledku to obvykle znamená, že k odhalení závady na signalizačním spoji dojde až při pokusu o sestavení spojení.

  Přístupové signalizační systémy přenášejí odlišné informace od koncového účastníka k síti a od sítě ke koncovému účastníku. Jejich vlastnosti bývají proto často nesymetrické, kopírující požadavky na obsah přenášených informací.

Při rozboru vlastností, v současné době využívaných protokolů pro realizaci VoIP, bylo zjištěno, že z pohledu signalizace, se svými vlastnostmi blíží k signalizaci v přístupových sítích. Tento stav je dán převážně historickým vývojem protokolů pro realizaci VoIP, kdy primární důraz byl kladen na metody umožňující spojení mezi libovolnými body v síti, tedy systémy spojení každý s každým *peer-to-peer*. Realizace takzvaných IP trunků je sice možná, v praxi se tohoto způsobu spojení hojně využívá, avšak protokoly nejsou prioritně navrhované pro toto použití.

Jelikož se práce primárně orientuje na návrh protokolu pro přenos signalizace v páteřních sítích je nutné uplatnit výše popsané skutečnosti v návrhu.

7.5 Spolehlivost signalizačního spoje

Signalizační systém je základním pilířem každé telefonní sítě, proto je nezbytně nutné při jeho návrhu implementovat metody, které umožní dohled a řízení signalizačního spoje. Signalizační systém musí být schopný včas detekovat problémy na signalizačním spoji a o nich informovat proces řízení spojování hovorů, tak aby nedošlo ke ztrátě hovorů, či k chybnému spojování.

Dále je nutné zajistit jasnou a jednoznačnou identifikaci obou komunikujících stran, tak aby nebylo možné podvrhnout neplatnou signalizační zprávu do sestaveného spoje. Tento mechanismus je nutný nejen z důvodu obrany před případným útokem na signalizační spoj, ale hraje významnou roli též jako obrana pro možným chybám v síti.

7.6 Textově orientovaný protokol

Velká většina aplikačních protokolů, používaných v prostředí sítí TCP/IP, jsou textově orientované. Klasickým příkladem mohou být dlouhodobě používané, osvědčené a ustálené protokoly, jakými jsou například http, smtp a podobné. V současné době jsou pro realizaci VoIP používané jak textově orientované protokoly, tak bitově orientované protokoly, jak bylo popsáno v kapitole 5. Jak binárně orientované tak textově protokoly, mají své klady a zápory, jak již bylo popsáno, pro návrh čistě signalizačního protokolu je však výhodnější využít textově orientovaného protokolu a to minimálně z následujících důvodů:

- v případě potřeby je jednodušší implementace nových funkcí do stávajícího návrhu
- snadnější implementace
- během implementace je možné snáze odhalit případné chyby
- jednodušší odhalování problémů během uvádění systémů do provozu

Jistou nevýhodou použití textově orientovaného protokolu je větší množství přenášených dat, které nenesou žádnou konkrétní informaci a slouží pouze k formátování jednotlivých informačních polí. Vzhledem k celkovému množství přenášených informací, intenzitě komunikace a prostředí, pro které je protokol navrhován, nezpůsobuje tato nevýhoda významější překážku.

7.7 Implementace

Již během samotného návrhu protokolu je nutné brát v úvahu způsoby implementace, problémy, které během ní mohou nastat dále také způsoby testování, jejich náročnost a úspěšnost v odhalení možných chyb atd. Vhodný koncept protokolu může výrazně urychlit implementaci a následné testování a tak snížit celkové náklady nutné na uvedení nového protokolu do praxe. Z těchto důvodů bylo při návrhu protokolu použito osvědčeného značkovacího jazyka XML a jeho metody určené ke kontrole jím neseného obsahu. Během implementace a následné kontroly bude možné využít těchto mechanismů nejen ke kontrole syntaxe zpráv, ale také jejich obsahu.

7.8 Konvergence

Velice důležitým aspektem při návrhu protokolu, který má libovolné návaznosti na poskytování hlasových služeb je probíhající konvergence v oblasti telekomunikačních sítí. Doposud není k dispozici signalizační protokol, který by umožnil jednotné řízení spojovacích procesů v prostředí heterogenních telekomunikačních sítí.

7.9 Shrnutí

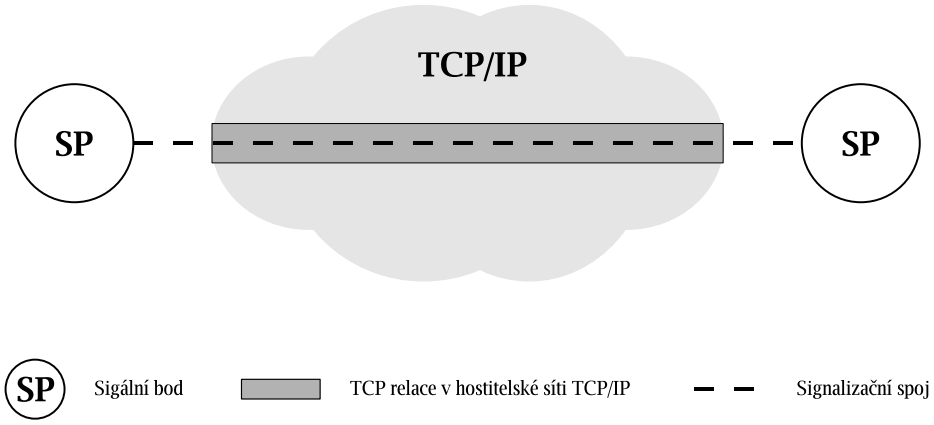
- Signalizační protokol, bez přímých vazeb na transportní mechanismy pro přenos samotných telefonních hovorů, či jiných multimediálních dat
- Protokol navržený primárně jako síťový pro nasazení v páteřních sítí poskytovatelů hlasových služeb
- Využití semipermanentního okruhu v IP síti pro přenos signalizace
- Průběžná kontrola kontinuity vystaveného semipermanentního okruhu
- Možnost využití signalizačního spoje pro řízení spojovacích procesů na libovolném médiu
- Spolupráce se signalizacemi pro tradiční telefonii
- Jednoznačné mapování běžně používaných ISDN signalizací na rozhraní sítí
- Textově orientovaný protokol
- Snadná implementace a její následná kontrola

Část IV
Výsledky

8 Koncept

Základní koncepce návrhu signalizačního protokolu vychází z osvědčených principů používaných v sítích tradiční telefonie. Jak bude popsáno dále podobné mechanismy však nejsou nikterak neobvyklé ani v sítích se spojování paketů, postavených na protokolech rodiny TCP/IP.

Základní koncept a jednotlivé entity používané v následujícím popisu návrhu protokolu jsou patrné z obrázku 8.



Obrázek 8: Základní model signalizačního spoje

8.1 Signální bod

Signálním bodem v daném konceptu je zařízení, komunikující s okolním pomocí protokolů rodiny TCP/IP, na aplikační úrovni pak disponující funkcemi popisovaného protokolu. Signální bod může, ale nezbytně nemusí být schopen pracovat též s okruhy, či spojeními pro přenos samotných hovorových, či jiných multimediálních dat, neboť vzniklá signalizační síť tvoří samostatnou rovinu podobně jak je tomu i v případě digitálních signalizačních systémů v tradiční telefonii (SS6 a SS7). Jelikož je protokol navrhovaný s ohledem na spolupráci s se sítěmi tradiční telefonie, jsou i vlastnosti a chování signálního bodu blízké signálnímu bodu, tak jak je definován v konceptu signalizačního systému SS7.

8.2 Signalizační spoj

Základní myšlenkou, která od samého počátku staví navrhovaný protokol do odlišné pozice oproti používaným signalizačním protokolům pro VoIP, je vytvoření semipermanentního komunikačního okruhu v síti TCP/IP mezi předem známými koncovými body. Každá ze stran má, jako součást své konfigurace, kompletní informace o protistraně, se kterou má navázat komunikaci. Okruh se tedy ustanoví na základě konfigurace obou stran, nikoliv pouze na základě požadavku o sestavení hovoru. Tento okruh je poté používán k výměně signalizačních zpráv mezi oběma koncovými body. Přenášené signalizační zprávy slouží k řízení směrovacích procesů, které jsou mezi dotčenými body sítě realizovány. Popsaný okruh tedy není svázán s konkrétním hovorovým kanálem, ale slouží k přenosu veškerých signalizačních informací mezi oběma stranami.

Koncept ideově vychází z vlastností protokolu BGP (Border Gateway Protocol). Protokol BGP slouží k přenosu směrovacích informací mezi autonomními systémy. Jeho podrobný popis je k dispozici v doporučeních IETF [13], [14] a [20]

Takto navržená koncepce umožní zadefinování obdobných funkcí pro řízení a kontrolu signalizačního spoje jako na vrstvě MTP2 signalizačního systému SS7.

Spojení je po celou dobu komunikace průběžně monitorováno, obě strany tedy mají úplnou informaci o tom, zda je signalizační spoj plně provozuschopný, či nikoliv. Dojde-li k zjištění libovolného problému během komunikace, signalizační spoj je automaticky vyřazen z provozu a dojde k pokusu o opětovné sestavení spojení. O tomto stavu je informován systém řízení spojovacích procesů, přestává využívat tento spoj pro přenos signalizačních zpráv, tak aby nedošlo ke ztrátě volání. Po úspěšném obnovení provozu je předána patřičná informace řízení spojovacích procesů a spoj začne být opět využíván ke komunikaci.

8.3 Signalizační výměna

Samotná komunikace mezi koncovými body probíhá za pomocí signalizačních zpráv. Celé portfolio navržených signalizačních zpráv a jejich parametrů je podrobně popsáno v kapitole 9 a 10. Návrh počítá s čistě textovým vyjádřením jednotlivých signalizačních zpráv vytvořených pomocí značkovacího jazyka XML. Každou zprávu bude tedy možné popsat pomocí XML schématu a tím jasně definovat její formát a parametry.

Výše popsaný způsob návrhu vyjádření signalizačních zpráv umožní jejich exaktní

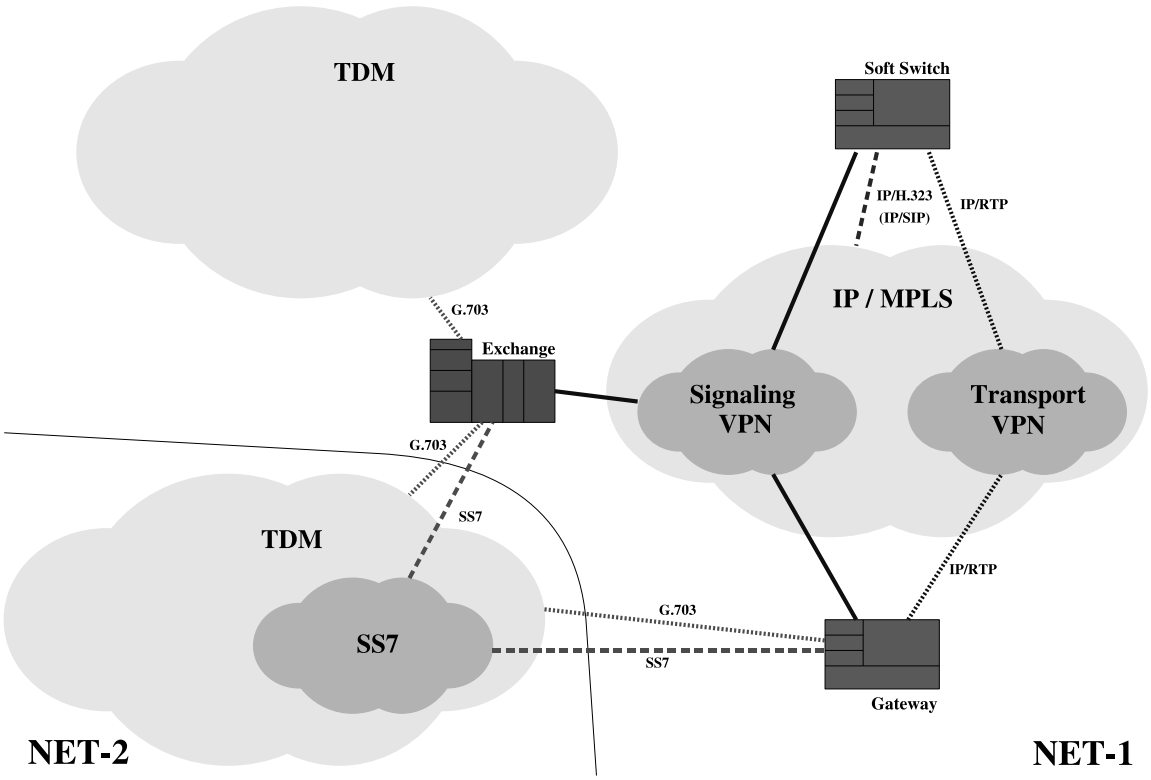
popis a následně usnadní možnou implementaci protokolu a jeho kontrolu při provozu v síti.

8.4 Signalizační síť

Protokol je navržen tak, aby bylo možné s jeho pomocí realizovat vytvoření jednotné signalizační sítě, která překryje doposud existující telefonní sítě a sjednotí je v síť s jedním signalizačním systémem, která umožní bezproblémové provozovaní běžných ISDN služeb napříč heterogenní přenosovou sítí.

Návrh počítá též s obdobím, kdy bude nutné provozovat souběžně existující signalizační systémy, jedná se hlavně o systém SS7 v prostředí veřejných telefonních sítí a dále Q-sig v prostředí privátních pobočkových systémů. Jednotlivé zprávy navrhovaného signalizačního protokolu a jejich parametry byly koncipovány tak, aby bylo možné zajistit jednoznačné mapovaní existujících ISDN signalizačních systémů.

Příklad možné realizace telefonní sítě využívající heterogenních přenosových prostředků avšak jednotné signalizace pro řízení spojovacích procesů v této síti uvádí obrázek 9



Obrázek 9: Příklad nasazení protokolu v heterogenní síti

Příklad uvádí spojení sítí TDM a TCP/IP v jednu telefonní síť s jednotným signalizačním systémem. V prostředí TCP/IP jsou pomocí technologie MPLS (Multi Protocol Label Switching) vytvořeny dvě L3 MPLS VPN (Virtual Private Network) sítě. První z nich slouží pro realizaci spojení nesoucí samotné multimediální informace, jde tedy v podstatě o samotnou transportní síť. Druhá VPN slouží k realizaci signalizační sítě, která zastřešuje heterogenní transportní síť.

Využití MPLS umožní jasně definovat potřebné parametry v síti TCP/IP a tím zajistit potřebnou jakost služby pro přenosy probíhající v části sítě pracující nad TCP/IP protokolem. Další výhodu, kterou lze v této konfiguraci s úspěchem využít je úplné oddělení signalizační sítě a přenosové sítě. Takto navržená struktura sítě umožní realizaci přehlednější topologické struktury a poskytne lepší možnosti při nastavovaní QoS v prostředí sítě TCP/IP.

8.5 Konfigurace signálního bodu

Následují příklad konfigurace signálního bodu naznačuje možnosti, které systém může nabídnout. Popsaná konfigurace využívá strukturu danou pomocí XML formuláře. Využití XML pro formátování konfiguračního souboru není nutné, na druhou stranu XML je využito k formátovaní samotných signalizačních zpráv a není žádný důvod nevyužít XML též k formátování konfigurace signálního bodu. Možné použití XML pro tvorbu konfigurace umožní jednoduchou kontrolu jak syntaxe, tak z větší části i obsahu konfiguračního souboru a to ještě před jeho aplikací v samotném systému.

Z příkladu uvedeného v tabulce 9 je patrné, že je možné konfiguraci signálního bodu rozdělit do dvou částí. V první části je konfigurace vztahující se k lokálnímu signálnímu bodu, jeho identifikace, jak v globální síti, tak i v síti operátora a dále výchozí parametry chování signálních spojů. V druhé části konfigurace jsou informace vztahující se k jednotlivým protistranám, se kterými bude navázáno signalizační spojení. V konfiguraci je IP adresa protistrany, její identifikace a parametry ovlivňující jedno konkrétní spojení s danou protistranou.

8.5.1 Význam jednotlivých polí v konfiguraci

- **local** - sekce obsahující lokální konfiguraci signálního bodu a výchozí parametry platné globálně pro konfiguraci spojení se všemi sousedními signálními body signalizační sítě.

- **neighbour** - sekce obsahující konfiguraci spojení s jedním konkrétním sousedním bodem sítě.
- **description** - pole slouží pouze k informativním účelům a umožní snazší orientaci v konfiguračním souboru. Pole může být použito jak v sekci local, tak v sekci neighbour. V obou sekcích má totožný význam.
- **system name** - identifikační údaj definující jméno signálního bodu. V sekci local slouží k definici jména signálního bodu. V sekcích neighbour slouží k zadání jména sousedního signálního bodu. Parametr je povinný ve všech sekcích. Během komunikace slouží ke kontrole komunikace na signálním spoji.
- **network name** - identifikační údaj definující příslušnost signálního bodu ke konkrétní síti. Pole může být součástí obou sekcí. V sekci local definuje příslušnost lokálního signálního bodu k síti, v sekcích neighbour pak definuje síť vzdáleného signálního bodu. Parametr není povinný v případě, že sousední signální bod je součástí stejné sítě, v ostatních případech se jedná o parametr povinný. Při komunikaci se tento parametr používá ke kontrole konfigurace a správné komunikace mezi sousedními signálními body sítě.
- **ip** - v sekci local definuje toto pole IP adresu, ke které bude proces obsluhy lokálního signálního bodu asociován. V sekcích neighbour se jedna o IP adresu sousedního systému, se kterým bude sestaven signalizační spoj. Pole IP je povinné v všech sekcích.
- **hold timer** - nastavuje výchozí hodnotu pro čítač vyčkávání. V sekci local se jedná o globální hodnotu platnou pro všechny sekce neighbor. V sekcích neighbour toto pole ovlivní chování jen jednoho konkrétního spojení. Popis použití čítače vyčkávání je součástí kapitoly 13.
- **keepalive timer** - nastavuje výchozí hodnotu pro čítač kontroly spoje. V sekci local se jedná o globální hodnotu platnou pro všechny sekce neighbour. V sekcích neighbour toto pole ovlivní chování jen jednoho konkrétního spojení. Popis použití čítače kontroly je součástí kapitoly 13.
- **type** - pole type je platné pouze pro sekce neighbour a definuje, zda spojení bude sestaveno uvnitř sítě jednoho poskytovatele, či půjde o spojení propojující sítě dvou různých poskytovatelů. Nastavení ovlivní typ a množství informací přenášených v záhlavích jednotlivých zpráv.

- **win** - hodnota pole ovlivňuje přímo chováni TCP protokolu, konkrétně umožní nastavení maximální velikosti okna pro potvrzení doručení.
- **ttl** - hodnota pole ovlivňuje chování IP protokolu. Nastavuje maximální počet uzlů IP sítě, kterými může datagram projít.
- **version** - pole version nese informaci podle jakého XML schématu budou signalizační zprávy formátovaný při jejich odesílání a naopak jaké schéma bude použito pro kontrolu přijímaných zpráv. V sekci global je hodnota braná jako výchozí hodnota pro chování všech sestavovaných spojení požití pole version v sekci neighbour ovlivní jen spoj s jedním daným sousedním signálním bodem.

Využití jednotlivých parametrů při komunikaci na signalizačním spoji a jejich vliv na chování spoje bude podrobně popsán v příslušných částech příštích kapitol.

```
<signal_point>
  <local>
    <ip>10.1.0.1</ip>
    <description>SP_INT_1</description>
    <system_name>SYS_ID_1</system_name>
    <network_name>NET_ID_1</network_name>
    <win>65535</win>
    <hold_timer>500</hold_timer>
    <keepalive_timer>100</keepalive_timer>
    <version>ver2.0</version>
  </local>
  <neighbour>
    <ip>10.1.0.2</ip>
    <description>SP_INT_2</description>
    <ttl>1</ttl>
    <version>ver2.0-c</version>
    <type>internal</type>
    <system_name>SYS_ID_2</system_name>
  </neighbour>
  <neighbour>
    <ip>10.2.0.1</ip>
    <description>SP_EXT_1</description>
    <ttl>4</ttl>
    <win>32768</win>
    <hold_timer>100</hold_timer>
    <keepalive_timer>20</keepalive_timer>
    <type>external</type>
    <system_name>SYS_ID_1</system_name>
    <network_name>NET_ID_2</network_name>
  </neighbour>
</signal_point>
```

Tabulka 9: Příklad možné konfigurace signálního bodu

9 Signalizační zprávy

Přehledný seznam zpráv použitých v návrhu protokolu je shrnut v tabulce 10. V prvním sloupci je název zprávy, tak jak je použit v návrhu protokolu. Ve druhém sloupci je zařazení zprávy do konkrétní funkční skupiny. Třetí sloupec obsahuje stručný popis zprávy, její obsah a využití v signalizačním procesu. Následuje typ zprávy, který určuje zda je zpráva globálního či lokálního charakteru, to jest, zda informace jsou přenášeny napříč celou sítí a jsou postupně využity všemi body sítě, či zda jde čistě o výměnu informací mezi sousedními body sítě. V posledním poli je směr přenosu dané zprávy, braný z pohledu sestavování telefonního spojení v síti.

Zprávy jsou rozděleny do tří základních skupin:

- **Signalizační spoj** - V této skupině jsou obsaženy veškeré signalizační zprávy určené k řízení samotného signalizačního spoje. Zprávy zajišťují inicializaci spoje, kontrolu vlastností spoje, obnovení spojení v případě detekce problému a přenos řídících informací mezi oběma stranami.

- **Spojovací proces** - Sekce označená spojovací proces obsahuje zprávy určené k řízení spojovacího procesu v telefonní síti. Zprávy zde uvedené slouží k sestavení telefonního hovoru v síti, k dohledu na tímto sestaveným spojením a v poslední fázi k jeho korektnímu ukončení a uvolnění použitých spojovacích vedení a to jak v podobě fyzických spojů, tak sestavených virtuálních okruhů v síti TCP/IP.

- **Globální informace** - V sekci, v tabulce označené globální informace, jsou zprávy určené pro přenos informací používaných, či alespoň použitelných, v celé síti. Konkrétně jde o přenos informací sloužících jako parametry využitelné během procesu směrování telefonních hovorů uvnitř celé telefonní sítě.

9.1 Zprávy řízení signalizačního spoje

Zprávy popsané v této sekci slouží k řízení a dohledu samotného signalizačního spoje. Nastavují jeho provozní parametry během procesu sestavování signalizačního spojení, zajišťují integritu signalizačního spoje napříč TCP/IP sítí a umožňují restart signalizačního spoje v případě detekce problému.

Zpráva	Skupina	Funkce	Typ zprávy	Směr přenosu
ALERT	spojovací proces	volaný účastník vyzváněn	globální	zpětný
CALLPR	spojovací proces	spojovací proces zahájen	lokální	zpětný
CONACK	spojovací proces	potvrzení zprávy CONN	lokální	dopředný
CONN	spojovací proces	přihlášení vzdáleného účastníka	globální	zpětný
INFO	spojovací proces	doplňující směrovací informace	globální	dopředný
LINKCACK	signalizační spoj	potvrzení přijetí zprávy LINKCHCK	lokální	oba směry
LINKCHCK	signalizační spoj	výplňová jednotka pro kontrolu spoje	lokální	oba směry
LINKIACK	signalizační spoj	potvrzení přijetí zprávy LINKINIT	lokální	oba směry
LINKINIT	signalizační spoj	inicializace signalizačního spoje	lokální	oba směry
LINKRACK	signalizační spoj	potvrzení přijetí zprávy LINKRST	lokální	oba směry
LINKRST	signalizační spoj	žádost o restart signalizačního spoje	lokální	oba směry
LINKSACK	signalizační spoj	potvrzení přijetí zprávy LINKSTAT	lokální	oba směry
LINKSTAT	signalizační spoj	žádost o zaslaní informací o stavu signalizačního spoje	lokální	oba směry
NUMACK	globální informace	potvrzení přijetí a zpracování zpráv NUMADD a NUMDEL	lokální	oba směry
NUMADD	globální informace	přidání telefonního čísla do procesu směrování	lokální	oba směry
NUMDEL	globální informace	odebrání telefonního čísla ze směrovacího procesu	lokální	oba směry
NUMRST	globální informace	žádost o zaslaní kompletního seznamu směrovaných čísel	lokální	oba směry
REL	spojovací proces	závěr účastníka, ukončení spojení	globální	oba směry
RELC	spojovací proces	potvrzení ukončení spojení a uvolnění vedení	lokální	oba směry
RESET	spojovací proces	žádost o reset hovoru	globální	oba směry
RESUME	spojovací proces	žádost o obnovení suspendovaného hovoru	globální	oba směry
RSTACK	spojovací proces	potvrzení přijetí zprávy RESET	globální	oba směry
SETACK	spojovací proces	potvrzení přijetí zprávy SETUP	lokální	zpětný
SETUP	spojovací proces	zahájení procesu sestavování hovoru	globální	dopředný
STAT	spojovací proces	žádost o zaslaní informace o stavu hovoru	globální	oba směry
STATACK	spojovací proces	potvrzení přijetí zprávy STACK	lokální	oba směry
SUSPEND	spojovací proces	žádost o suspendování hovoru	globální	oba směry

Tabulka 10: Signalizační zprávy

9.1.1 LINKINIT

Zpráva LINKINIT je odesílaná vždy jako první zpráva po sestavení spojení v síti TCP/IP. Slouží k nastavení základních parametrů signalizačního spoje na obou jeho stranách a zahájení komunikace.

Podobně jako v ostatních případech v této sekci je zpráva LINKINIT lokální a slouží čistě jen pro komunikaci dvou sousedních signálních bodů prostřednictvím sítě TCP/IP.

9.1.2 LINKIACK

Zpráva LINKIACK je potvrzením přijetí zprávy LINKINIT a informuje o provedení všech potřebných kroků k zahájení komunikace na daném signalizačním spoji.

9.1.3 LINKSTAT

Zpráva LINKSTAT je signálním bodem odeslaná ve dvou možných případech. V prvním případě je LINKSTAT požadavkem na odeslání informací o stavu signalizačního spoje a vzdáleného signalizačního bodu. V případě druhém zpráva informuje vzdálenou stranu o změně stavu signalizačního spoje.

9.1.4 LINKSACK

Zpráva LINKSACK je odpovědí na zprávu LINKSTAT a nese požadované informace o stavu signalizačního spoje.

9.1.5 LINKCHCK

Zpráva slouží k zajištění kontroly integrity spoje, je vysílaná v případě, když koncový systém nemá žádná data, které by bylo možné přes spoj přenést. Jedná se o obdobu zprávy FISU v signalizačním systému SS7.

9.1.6 LINKCACK

LINKCACK je potvrzením korektního přijetí zprávy LINKCHCK.

9.1.7 LINKRST

Zpráva LINKRST je žádostí o provedení restartu signalizačního spoje. Zpráva je vysílaná v případě detekovaní chyby na signalizačním spoji. Zpráva inicializuje proceduru znovusestavení celého spojení.

9.1.8 LINKRACK

Potvrzení přijetí zprávy LINKRST a zahájení procesu restartu signalizačního spoje.

9.2 Zprávy pro přenos globálních informací

Následující sekce popisuje zprávy určené k přenosu globální informace uvnitř signalizační sítě. Součástí této práce není návrh, či popis jednotlivých algoritmů využívajících tyto údaje. Současně není ani seznam zpráv zde uvedených konečný či jakkoliv závazný. Zprávy obsažené v tomto bloku je možné použít k řízení směrovaní v telefonní síti, k přenosu informace použitelné v platformě inteligentní sítě a podobně.

Navrhovaný komunikační protokol je otevřený a je tedy možné v budoucnu dodefinovat další signalizační zprávy dle potřeb a vývoje telefonní sítě a její signalizace. Naskýtá se například možnost přenášet zprávy obsahující informace o zatížení jednotlivých trunků v telefonní síti a na základě těchto údajů dynamicky měnit směrování v síti, tak aby nedocházelo k přetěžování jednotlivých spojů a případné ztrátě telefonních hovorů.

9.2.1 NUMADD

Zpráva nese informaci o možné dosažitelnosti konkrétního telefonního čísla či série čísel. Součástí zprávy je podobně jako v případě směrovacího protokolu BGP informace o tom, jaká brána má k sobě účastníka, čí účastníky připojené a jaká je nejkratší cesta k účastníkovi s tímto telefonním číslem.

9.2.2 NUMDEL

Zpráva nese informaci o zrušení směrování daného telefonního čísla či celé série z dané brány, či přes tuto bránu.

9.2.3 NUMRST

Požadavek na zaslání aktuálního seznamu dostupných telefonních čísel, či sérií.

9.2.4 NUMACK

Zpráva je generovaná jako potvrzení o přijetí a zpracování nové směrovací informace odeslané pomocí zpráv NUMADD, nebo NUMDEL.

9.3 Zprávy pro řízení spojovacího procesu

V této sekci je popis jednotlivých správ používaných během procesu sestavování a rušení telefonního spojení. Zprávy jsou navrženy tak, aby pomocí jejich parametrů bylo možné přenášet celé portfolio informací známých z tradiční telefonních sítích a jejich signalizací, jako například DSS1 dle doporučení Q.931, ISUP ve veřejných telefonních sítích, či Q-sig v pobočkových sítích.

9.3.1 SETUP

Zpráva SETUP je první zprávou odesílanou při zahájení procesu sestavení spojení. Zpráva je vysílaná ze stany volajícího směrem ke straně volaného. Obsahuje všechny údaje nutné k započetí spojovacího procesu, jako například číslo volaného či jeho část, identifikaci sestavovaného volání, identifikaci přenosového okruhu a podobně.

Ve většině, v současnosti provozovaných, telefonních sítích je telefonní číslo volaného přenášené vcelku jako jedna informace en-bloc. Příkladem může být signalizace v mezinárodní ISDN síti s použitím SS7 s ISUP. V tomto případě nese zpráva SETUP kompletní informaci nutnou k vytvoření spojení. Z důvodů zajištění zpětné

kompatibility je počítáno s možností přenosu telefonního čísla volaného také metodou overlap, kdy telefonní číslo volaného je signalizační sítí přenášeno po částech. V tomto případě zpráva SETUP ponese první známou část telefonního čísla, zbylé části telefonního čísla budou přeneseny za použití signalizační zprávy INFO.

Zpráva SETUP je zprávou globální a obsahuje informace přenášené napříč telefonní sítí.

9.3.2 SETACK

Zpráva SETACK je potvrzením příjetí zprávy SETUP. Je vysílaná ve směru od volající strany k volané. Může obsahovat též informaci o tom, že přijatá informace je dostatečná pro započetí spojovacího procesu. Je-li tato informace ve zprávě SETACK přenesena, není již vyžadován přenos doplňujících informací pomocí zpráv INFO. V opačném případě je očekáván přenos upřesňujících informací, tak aby bylo možné zahájit proces spojování. Obdržení kompletních směrovacích údajů je pak potvrzeno zprávou CALLPR.

Zpráva SETACK je zprávou lokální a slouží ke komunikaci dvou sousedních bodů signalizační sítě

9.3.3 INFO

Zpráva INFO slouží k přenosu doplňujících směrovacích informací o sestavovaném spojení během již započatého směrovacího procesu, případně během již sestaveného spojení. Zpráva může nést část telefonního čísla volaného účastníka v případě, že je telefonní číslo přenášené metodou overlap, dále nese informace o změně čísla volaného, či volajícího během již sestaveného telefonního hovoru, informace o aplikované tarifikaci atd.

Zpráva INFO je globální zprávou nesoucí informace využívané napříč telefonní sítí.

9.3.4 CALLPR

Zpráva CALLPR informuje o zahájení spojovacího procesu. Jde o zprávu zpětnou, je tedy přenášena signalizační sítí ze strany volaného směrem k volajícímu. Tato zpráva je též informací, že doposud přijatá informace ve zprávách SETUP a případně INFO je dostatečná k započetí procesu sestavování spojení. V případě, že byla směrovací

informace ve zprávě SETUP kompletní a bylo potvrzeno její přijetí zprávou SETACK, není zasílání zprávy CALLPR vyžadováno.

Jde o lokální zprávu sloužící k přenosu informace mezi sousedními body v signalizační síti.

9.3.5 ALERT

Zpráva je přenášena ze strany volaného směrem ke straně volajícího. Zpráva informuje o dokončení spojovacího procesu a vyzvánění volaného účastníka.

ALERT je globální zpráva přenášející údaje napříč telefonní sítí.

9.3.6 CONN

Zpráva je vyslána ve směru od volaného k volajícímu a informuje o přihlášení volaného účastníka.

Zpráva CONN je globální zprávou.

9.3.7 CONACK

Zpráva je vysílaná jako potvrzení přijetí zprávy CONN.

CONACK je lokální zpráva sloužící ke komunikaci dvou sousedních bodu signalizační sítě.

9.3.8 REL

Zprávu REL může odeslat libovolná ze stran jako požadavek na okamžité ukončení spojení a s ním související uvolnění vedení využitých pro sestavený telefonní hovor. Zpráva nese podobně jako zpráva DISC v Q.931 či REL v ISUP informaci o důvodu ukončení spojení, informaci o původci zprávy atd. Zpráva REL je též odesílána v případě že se během spojovacího procesu nepodařilo sestavit telefonní spojení. I v tomto případě je příčina onoho nezdaru přenášena v těle zprávy.

Jedná se o globální zprávu přenášenou napříč telefonní sítí.

9.3.9 RELC

Zpráva RELC je potvrzením zprávy REL a informuje o dokončení procesu ukončení spojení a uvolnění použitých vedení, či zrušení virtuálních okruhů v síti TCP/IP.

Zpráva RELC je zprávou lokálního charakteru a slouží ke komunikaci dvou sousedních bodů sítě.

9.3.10 RESET

Žádost o resetování sestaveného spojení.

Zpráva RESET je lokálního charakteru.

9.3.11 RSTACK

Potvrzení provedeného resetu spojení.

Zpráva RSTACK je lokálního charakteru.

9.3.12 SUSPEND

Žádost o suspendování sestaveného spojení, hovor je suspendován ale spojení zůstává sestaveno.

Zpráva SUSPEND má globální charakter, informační obsah je přenášen napříč telefonní sítí.

9.3.13 RESUME

Žádost o obnovení suspendovaného spojení.

Zpráva RESUME má globální charakter, informační obsah je přenášen napříč telefonní sítí.

9.3.14 STAT

Žádost o zaslání doplňující informace o stavu konkrétního telefonního spojení.

9.3.15 STATACK

Zpráva STATACK je odpovědí na zprávu STAT, která ve svém těle obsahu obsahuje vyžádané informace o hovorovém spojení.

10 Parametry signalizačních zpráv

Obsahem této kapitoly je popis jednotlivých parametrů přenášených v záhlaví a těle signalizačních zpráv.

Parametry je možné rozdělit do dvou základních skupin podle toho, zda jsou součástí všech signalizačních zpráv popsaných v kapitole 9 a nesou tedy základní obecné informace o identifikaci, operátora, systému a podobně, či jde o konkrétní informaci vztaženou například ke konkrétnímu telefonnímu hovoru, stavu signalizačního spoje atd. První skupina parametrů, tedy parametry přenášené jako součást všech signalizačních zpráv [9] jsou obsaženy v záhlaví zprávy, druhá skupina parametrů je součástí těla zprávy.

10.1 Parametry záhlaví zprávy

Jak bylo naznačeno v předchozím odstavci záhlaví zpráv nese informace o identifikaci zprávy signálního bodu ze kterého byla zpráva odeslána a signálního bodu kam je zpráva směrovaná.

Informace přenášené v záhlaví zprávy mají významný vliv během procesu navazování spojení, kdy jsou kontrolovány informace přenesené v záhlaví zprávy LINKINIT s informacemi obsaženými v konfiguraci signálního bodu. Nedojde-li během tohoto procesu ke shodě, je proces ustanovení signalizačního spoje přerušen a obě strany jsou informovány o chybné konfiguraci signálních bodů. Postup ustanovení signalizačního spoje je podrobně popsán v kapitole 13.

Během komunikace jsou průběžně kontrolovány identifikační údaje přenášené v záhlavích zpráv a dojde-li k neshodám v přenesených a konfigurovaných hodnot, řízení signalizačního spoje přejde do stavu restartu spoje s cílem odhalit případnou chybu komunikace. Proces je opět podrobně popsán v kapitole 13.

Záhlaví každé zprávy obsahuje tři základní identifikační údaje. Identifikaci zprávy, identifikaci původce zprávy a identifikaci cíle, do kterého je zpráva odesílána. Tyto udaje jsou obsažené v parametrech msg_id, msg_ack, src a dst.

- **msg_id** - Parametr msg_id, je jednoduchým nestrukturovaným parametrem a slouží k identifikaci. Hodnota parametru je generována systémem, kde zpráva vznikla, je jedinečná a jednoznačně identifikuje danou zprávu. Mimo identifikaci

[9] ne všechny signalizační zprávy musí nezbytně nutně obsahovat veškeré identifikační informace, podrobný popis formátu záhlaví zpráv je popsán v kapitole 11

signalizační zprávy má parametr další důležitou roli v systému řízení a kontroly signalizačního spoje, kterou je kontrola integrity a signalizačního spoje a dle použitého algoritmu i samotné signalizační zprávy.

Algoritmus generování čísla zprávy může být od jednoduché inkrementace až po využití hashovacích funkcí a klíčů. Důležitým požadavkem na algoritmus použitý ke generování identifikace zprávy je poskytnou cílovému systému nástroj na detekci chyby vzniklé výpadky, opakováním, či "podstrčením" falešné zprávy. Aby bylo toto možné je nutné zajistit, aby cílový systém byl schopen spočítat předpokládanou hodnotu tohoto parametru ke každé přijímané zprávě a tu následně porovnat se skutečnou hodnotou přijatou v záhlaví zprávy. Bude-li během tohoto procesu detekována neshoda v přijaté a vypočítané hodnotě, dojde k zastavení provozu signalizačního spoje a systém řízení signalizačního spoje přejde do stavu restartu spoje s cílem detekce vzniklého problému a jeho odstranění. Proces řízení signalizačního spoje je podrobně popsán v kapitole 13.

Počáteční hodnoty čítačů zpráv, či výměna klíčů pro generování kontrolních součtů jsou přenášeny během procesu sestavování spojení v těle zpráv LININIT, případně LINKIACK.

- **msg_ack** - jednoduchý nestrukturovaný parametr, který je povinný ve všech zprávách, které slouží jako odpověď na přijatou zprávu, případně jako potvrzení přijetí konkrétní zprávy. Hodnotou parametru je číslo zprávy, na kterou odesílaná zpráva navazuje.

- **src** - Parametr src je strukturovaným parametrem, jeho obsahem jsou údaje nutné k identifikaci zdrojového systém v rámci sítě, kde je provozován. Struktura parametru bude odlišná pro případ, kdy půjde o spoj uvnitř sítě jednoho provozovatele a pro spoj, který bude sloužit k propojení sítí dvou poskytovatelů.

  Bude-li spoj provozován uvnitř sítě jednoho poskytovatele, je dostatečnou identifikací jméno zdrojového systému. Pro přenos jména systému slouží subparametr **sys**. V případě, že spoj bude provozován na rozhraní sítí dvou poskytovatelů bude parametr src doplněn o další subparametr nesoucí identifikaci sítě provozovatele. Subparametrem sloužícím k identifikaci sítě provozovatele je subparametr s názvem **net**.

- **dst** - Parametr dst je podobně, jako parametr src, strukturovaným parametrem, který obsahuje identifikační údaje cílového systému.

Další struktura parametru dst je v podstatě totožná s parametrem src, není proto nutné tuto strukturu popisovat.

Přesný popis formátu záhlaví zprávy je součástí kapitoly 11.

10.2 Parametry těla zprávy

Shodně s rozdělením signalizačních zpráv do tří skupin podle jejich funkce v rámci celé sítě jsou i jednotlivé parametry zpráv rozděleny do totožných skupin přidružených ke konkrétní skupině zpráv. Popis parametrů přenášených v signalizačních zprávách, v jednotlivých skupinách je součástí následujících tří podkapitol.

10.2.1 Parametry zpráv pro řízení signalizačního spoje

Přehled všech parametrů, které jsou součástí celé skupiny zpráv pro řízení signalizačního spoje je uveden v tabulce 11. Tabulka ukazuje též vazbu parametrů na jednotlivé zprávy. Písmeno M značí, že parametr je povinným parametrem dané zprávy. Písmeno O znamená, že se jedná o volitelný parametr.

V dalším textu je pak podrobný popis jednotlivých parametrů a jejich vliv na chování signalizačního spoje.

- **counter** - jednoduchý nestrukturovaný parametr nesoucí informaci o počátečním stavu čítače zpráv. Tato hodnota je přenášena protistraně ve zprávě LINKINIT při procesu sestavování signalizačního spoje.
- **key** - jednoduchý nestrukturovaný parametr, který slouží k přenosu bezpečnostního klíče. Klíč může být využit algoritmem pro generování čísla zprávy.
- **stat** - strukturovaný parametr obsahující informace o stavu signalizačního spoje. Parametr obsahuje dvě pole. Prvním z nich, **code**, je povinným subparametrem parametru stat a obsahuje kód stavu, ve kterém se spoj nachází, respektive kód události, která způsobila změnu stavu signalizačního spoje. Výčet jednotlivých kódů s jejich popisy je součástí níže uvedené tabulky.

Hodnota	Popis
0	signalizační spoj pracuje bez problémů
1	požadavek na ukončení provozu signalizačního spoje
2	informace o ukončení provozu signalizačního spoje
3	nastala neznámá chyba
4	došlo k porušení integrity spoje, bylo přijato neplatné číslo zprávy
5	přijatá zpráva má neplatnou, nebo poškozenou strukturu
6	během doby vymezené čítačem vyčkávání nedošlo k přijetí žádné zprávy (Hold Timer expired)
7	verze protokolu nesouhlasí
8	nesouhlasí konfigurační údaj typ spojení (type)
9	nesouhlasí identifikace zdrojového systému (system-name v sekci neighbour lokální konfigurace)
10	nesouhlasí identifikace zdrojové sítě (network-name v sekci neighbour lokální konfigurace)
11	nesouhlasí identifikace cílového systému (system-name v sekci neighbour vzdálené konfigurace)
12	nesouhlasí identifikace cílové sítě (system-name v sekci neighbour vzdálené konfigurace)

Druhým, volitelným, subparametrem je **note**, který může obsahovat doplňující údaje v textové podobě, které mohou sloužit protistraně při hledání příčiny případných problémů.

- **ver** - nestrukturovaný parametr obsahující řetězec identifikující verzi protokolu a patřičnou DTD šablonu, nebo XML schéma, které danou verzi protokolu definuje.

		Zpráva							
		LINKCACH	LINKCHCK	LINKINCK	LINKINIT	LINKINCK	LINKRSTT	LINKSACK	LINKSTAT
Parametr	Popis								
counter	počáteční hodnota čítače zpráv			O	M				
key	klíč, který bude použit pro následující komunikaci			O	O				
stat	informace o stavu spoje					O	O	O	O
ver	verze protokolu používaná ke komunikaci			M	M			O	O

Tabulka 11: Parametry signalizačních zpráv pro řízení signalizačního spoje

10.2.2 Parametry zpráv pro přenos globálních informací

Obsahem této kapitoly je popis parametrů druhé skupiny signalizačních zpráv. Vazbu mezi jednotlivými zprávami a jejich parametry je opět uveden v tabulce 12, která obsahuje informace v sumarizované formě.

- **num** - jednoduchý nestrukturovaný parametr, který obsahuje řetězec, popisující telefonní číslo, či sérii, která má být přidána, respektive odebrána ze směrovací tabulky protistrany. Z důvodu větší flexibility je pro popis použito regulárního výrazu. K sestavení regulárního výrazu je mimo číslic použito též speciálních znaků. Seznam použitých speciálních znaků a jejich význam je obsahem tabulky:

Výraz	Význam
.	libovolná jedna číslice
$[x-y]$	interval číslic v rozsahu x-y
$[xyz]$	výčet číslic v rozsahu x, y, z
?	libovolný řetězec číslic
!	negace následujícího výrazu

Parametr je povinným parametrem zpráv NUMADD a NUMDEL. Každá zpráva musí obsahovat minimálně jeden parametr num, maximální množství však není omezeno.

- **rej** - podobně jako v předchozím případě je parametr rej jednoduchým parametrem. Dojde-li k odmítnutí některého z telefonních čísel, či sérií, je toto číslo respektive série obsahem právě tohoto parametru. Parametr rej je volitelným parametrem zprávy NUMACK.

- **type** - jednoduchý nestrukturovaný parametr obsahující informaci o způsobu, jakým dojde k výměně údajů ve směrovací tabulce po obdržení nového seznamu telefonních čísel respektive sérií. Jsou možné tři postupy , které mohou být pro aktualizaci tabulky směrovacích informací použity. Jejich seznam a odpovídající hodnotu parametru obsahuje následující tabulka.

Hodnota	Význam
0	vyprázdnění tabulky a následné postupným načítaní nových informací
1	postupná výměna kolizních záznamů za nové
2	sumarizace přijatých údajů a jejich následná jednorázová výměna

		Zpráva			
Parametr	Popis	NUMACK	NUMADD	NUMDEL	NUMRST
num	řetězec definující telefonní číslo, či sérii, která má být přidána resp. vyňata ze směrovacích tabulek		M	M	
rej	řetězec definující telefonní číslo, či sérii, která nebyla přijata protistranou	O			
type	Definuje způsob, jakým dojde k výměně směrovacích informací				M

Tabulka 12: Parametry signalizačních zpráv pro přenos globálních informací

10.2.3 Parametry zpráv pro řízení spojovacích procesů

Následující text popisuje jednotlivé parametry zpráv v sekci řízení spojovacích procesů. Tabulky 13 a 14 jsou pak sumarizací informací popsaných v textu. Tabulky opět ukazují vazbu mezi jednotlivými zprávami a jejich parametry.

- **bck_inf** - strukturovaný parametr obsahující informace a požadavky na síť spojené se stranou volaného. Parametr je povinným parametrem zprávy ALERT a volitelným parametrem CALLPR a CONN.

- **call_id** - tento parametr je povinnou součástí všech zpráv pro řízení spojovacích procesu. Jde o jednoduchý nestrukturovaný parametr, jehož hodnota jednoznačně identifikuje konkrétní hovorové spojení v celé síti. Hodnota parametru je složena ze tří částí oddělených znakem "–". První část je identifikátor sítě, druhou část tvoří identifikátor systému, kde hovor vznikl. Poslední část je číslo telefonního spojení generované systémem, kde spojení vzniklo.

- **category** - jednoduchý parametr obsahující kategorii volajícího. Parametr je povinnou součástí zprávy SETUP a volitelným parametrem zprávy STATACK. Parametr může nabývat hodnot 0 -15. Prvních osm hodnot je totožných s hodnotou kategorie v signalizaci SS7/ISUP, druhá polovina je určena pro možné rozšíření poskytovaných služeb. Konkrétní kategorii vyjádřená hodnotou parametru je na oboustranné dohodě provozovatelů jednotlivých systémů.

- **cause** - strukturovaný parametr, jehož obsah určuje zdroj a příčinu, proč bylo dané spojení ukončeno, případně z jakého důvodu se nepodařilo jeho sestavení. Parametr cause je povinným parametrem zprávy REL a volitelným parametrem zpráv CALLPR a CONN.

  První subparametr **location** určuje, kde zpráva vznikla. Druhý parametr **clc** obsahuje hodnotu indikující důvod, proč došlo k ukončení spojení, respektive důvod, proč se spojení nepodařilo sestavit. Hodnota subparametru je přejata z doporučení Q.931 a odpovídá hodnotám informačního elementu IE.6.

- **cir_id** - povinný parametr zprávy SETUP nesoucí informaci o spojovací cestě. jedná se o strukturovaný parametr, jeho struktura je závislá na tom, pomocí jaké transportní sítě bude realizované spojení.

  První část parametru tvoří informace o typu média, který je použitý pro vytvoření spojovací cesty. Tato informace je přenášena jako hodnota subparametru **type**. Seznam hodnot, které může subparametr nabývat je, včetně jejich popisu, součástí následující tabulky.

Hodnota	Význam
WIR	okruh realizovaný pomocí měděného páru
TDM	okruh realizovaný v síti na principu TDM
IP	okruh realizovaný v paketové sítí pracující nad protokoly rodiny TCP/IP

Druhou částí parametru je identifikace okruhu v síti. Identifikace je odlišná podle typu zvoleného média.

- **WIR** - identifikace okruhu, který je realizován pomocí měděného páru je řešena pomocí dvou subparametrů. První identifikuje skupinu vedení (**trunk**) a druhý (**pair**) identifikuje konkrétní pár uvnitř skupiny.
- **TDM** - pro identifikaci okruhu v síti TDM je použitý totožný způsob, který využívá signalizační systém SS7. Okruh je identifikován pomocí parametru CIC, jehož formát je shodný s formátem dle doporučení ITU-T pro patřičnou část signalizace SS7.
- **IP** - je-li okruh sestaven v prostředí sítě TCP/IP, je okruh identifikován zdrojovou IP adresou, cílovou IP adresou a dvěma porty protokolu UDP. Jelikož okruh v síti TCP/IP je realizován pomocí protokolu RTP, je nutné alokovat UDP port nejen pro samotný přenos multimediálních informací, ale také pro řídící informace přenášené protokolem RTCP. Tato skutečnost se dle doporučení RFC pro tyto protokoly řeší pomocí alokovaní sousedící dvojice portů, pro identifikaci obou portů pak stačí pouze číslo portu pro RTP. Protokol RTCP využije číslo portu o zvýšené o jedničku. Z tohoto důvodu je nutné, aby port identifikující RTP/RTCP spojení byl vždy sudý.

  Subparametry nesoucí výše popsané informace jsou:

  loc_ip, **loc_port**, **rem_ip** a **rem_port**.

- **cont_chck** - jednoduchý nestrukturovaný parametr informující o úspěchu, či neúspěchu provedeného testu kontinuity hovorové cesty. Parametr je volitelnou součástí zprávy INFO.

Hodnota	Význam
err	test kontinuity skončil chybou
ok	test kontinuity byl úspěšný

- **dst_num** - nestrukturovaný parametr obsahující telefonní číslo, případně část telefonního čísla volaného. Je-li během spojovacího procesu použita metoda přenosu telefonního čísla volaného *en-bloc* nese parametr celé telefonní číslo volaného ve formátu E.164. V případě, že je telefonní číslo přenášeno sítí po částech, tedy jde o metodu *overlap*, je hodnotou parametru patřičná část telefonního čísla volaného. Parametr dst_num je volitelným parametrem zpráv SETUP a INFO.

- **dtmf** - nestruktorovaný parametr sloužící k přenosu znaků volených během sestaveného spojení jednou ze stran pomocí DTMF. Parametr je volitelnou součástí zprávy INFO.

- **event** - jednoduchý parametr popisující událost, která nastala během sestavování spojení. Parametr je povinnou součástí zprávy CALLPR. Volitelně pak může být tento parametr součástí zprávy SETACK. K dispozici je následující výčet hodnot popisující možné události:

Hodnota	Význam
alert	volaný účastník vyzváněn
progres	probíhá spojovací proces
info	k dispozici jsou doplňující informace přenášené v přenosovém kanále
busy-fwd	došlo k přesměrování z důvodu obsazení
noans-fwd	došlo k přesměrování z důvodu nepřihlášení volaného
uncon-fwd	došlo k nepodmíněnému přesměrování hovoru

- **fwd_inf** - strukturovaný parametr obsahující informace a požadavky na síť spojené s volající stranou. Parametr je povinnou součástí zprávy SETUP. Obsahuje informace nesoucí požadavky na druh a kvalitu spojení.

- **new_num** - Došlo-li během hovoru k přesměrování může být informace o novém telefonním čísle poslaná při jeho ukončení poslaná systému, který hovor započal. Parametr je volitelným parametrem zprávy REL. Formát parametru je totožný s parametrem src_num.

- **orig_num** - jednoduchý nestrukturovaný parametr. Jde-li o přesměrovaný hovor, je hodnotou parametru původní telefonní číslo volaného. Parametr orig_num je volitelným parametrem zprávy SETUP

- **originator** - nestrukturovaný parametr nesoucí informaci o původci akce suspendování, či obnovení spojení. Parametr je povinným parametrem zpráv SUSPEND a RESUME.

Hodnota	Význam
usr	původce akce je účastník
net	původce akce je je spojovací systém

- **rdr_inf** - jednoduchý nestrukturovaný parametr informující o příčině přesměrování hovoru. Parametr je volitelnou součástí zpráv SETUP a REL.

- **rdr_num** - parametr který v případě přesměrování hovoru nese informaci o telefonním čísle účastníka, který proces přesměrování inicioval. Parametr rdr_num je volitelným parametrem zprávy SETUP. Formát parametru je totožný s parametrem src_num.

- **req** - jednoduchý nestrukturovaný parametr, který je povinnou součástí zprávy STAT. Hodnotou parametru je identifikace informací požadovaných od protistrany.

Hodnota	Význam
src-num	číslo volajícího
category	kategorie volajícího

- **src_num** - strukturovaný parametr, jehož hodnota je telefonní číslo volajícího ve formátu dle doporučení E.164 a doplňující informace o volajícím účastníkovi. Hlavní částí parametru je subparametr **num** nesoucí samotné telefonní číslo volajícího. Dalšími subparametry jsou **si** a **ri**. První z nich obsahuje informaci o tom, kdo volajícího identifikoval. Hodnota druhého z nich pak určuje, zda je, či není povoleno zobrazení telefonního čísla volajícího volanému. Parametr je povinným parametrem zprávy SETUP.

- **tone** - strukturovaný parametr nesoucí specifikaci tónu, který bude účastníkovi posílán a jakým způsobem bude generován. Parametr je volitelným parametrem zpráv ALLERT, CALLPR a REL. V případě, že parametr nebude součástí zprávy, spojovací systém použije standardního postupu a tón bude vybrán z interní sady tónů spojovacího systému, či brány na základě informací přenesených pomocí běžné signalizace o stavu spojení.

  - **type** - subparametr type určuje, zda bude vysílán některý ze standardních tónů, či bude tón generován protistranou a následně přenášen v hovorovém kanále, případně zda bude generován speciální tón na základě přesné definice uvedené v subparametru **gensq**. Možné hodnoty subparametru **type** jsou uvedeny v následující tabulce.

Hodnota	Význam
busy	žádost o zaslání obsazovacího tónu
cong	žádost o zaslaní informace o přetížení sítě - rychlý obsazovací tón
dial-pub	žádost o zaslání standardního oznamovacího tónu pro veřejné telefonní sítě
dial-pri	žádost o zaslání standardního oznamovacího tónu pro privátní telefonní sítě
sit	informace, že během pokusu o spojení došlo k neočekávané chybě
unav	informace o volbě neexistujícího telefonního čísla
wait	žádost o vyslání tónu s požadavkem o vyčkávání účastníka
inband	tón bude přenášen uvnitř hovorového pásma
generator	tón bude vygenerován na základě informací v parametru gensq

  - **gensq** - subparametr nese popis dle kterého bude generován účastníkovi libovolný tón. Tón bude generován na základě popisu zadaného pomocí textového řetězce sestaveného podle následujících pravidel:

znak = frekvence1[+frekvence2]*[modulace]/[delka|C]
skupina = znak[-R|-znak]
tón = skupina[,skupina]

Frekvence1 a frekkvence2 jsou jsou frekvence jednotlivých složek tónu v hertzích. Modulace udává modulační frekvenci použitou při generování tónu, opět je zadávána v hertzích. Délka udává dobu trvání definovaného znaku tónu v milisekundách. Znak C, použitý namísto délky znamená trvalý tón.

Pomocí jednotlivých znaků je možné složit tónovou skupinu. Je-li posledním znakem skupiny R bude takto definovaná skupina periodicky opakována.

Výsledný tón je pak zadán pomocí kombinace skupin. Tento způsob zápisu umožní definici v podstatě libovolného tónu.

- **transport** - nepovinný parametr, který slouží k mapování informací z pole Access Transport v případě návaznosti na SS7/ISUP, případně informačních elementů IE.4 (called party subaddress), IE.5 (calling party subaddress), IE.8 (high layer compatibility), IE.10 (low layer compatibility) a IE.11 (progress indicator) v případě spolupráce s Q.931. Jde o strukturovaný parametr obsahující pole: **src_addr**, **dst_addr**, **hlc**, **llc**, **progress**. Do těchto polí jsou přímo mapovány výše popsané informace ze signalizací SS7/ISUP, případně Q.931

- **usr2usr** - jednoduchý nestrukturovaný parametr umožňující přímou komunikaci mezi koncovými účastníky. Podobně jako v případě SS7/ISUP není formát parametru blíže specifikován a je ponechán čistě na domluvě provozovatelů sítí.

		Zpráva							
Parametr	**Popis**	**ALERT**	**CALLPR**	**CONACK**	**CONN**	**INFO**	**REL**	**RELC**	**RESET**
bck_inf	doplňující informace odesílané dopředně	M	O		O				
call_id	identifikace hovorového spojení	M	M	M	M	M	M	M	M
category	kategorie volaného účastníka								
cause	příčina rozpadu resp. ukončení spojení		O		O		O		
cir_id	identifikace použitého okruhu						M		
cont_chck	výsledek testu kontinuity hovorové trasy					O			
dst_num	telefonní číslo volaného				O				
dtmf	přenos volby DTMF během hovoru					O			
event	popis události, která nastala během spojování					O			
fwd_inf	doplňující informace odesílané zpětně								
new_num	telefonní číslo volaného po přesměrování						O		
orig_num	původní číslo volaného před přesměrováním								
originator	původce akce suspendování, resp. obnovení hovoru								
rdr_inf	informace o přesměrování hovoru						O		
rdr_num	telefonní číslo iniciátora přesměrování								
req	požadavek doplňujících informací								
src_num	telefonní číslo volaného								
tone	specifikace tónu	O	O				O		
transport	transport informací ze signalizace Q.931								
usr2usr	signalizace mezi koncovými účastníky	O	O		O	O	O		

Tabulka 13: Parametry signalizačních zpráv pro řízení spojovacích procesů - část I.

		Zpráva						
Parametr	**Popis**	**RESUME**	**RSTACK**	**SETACK**	**SETUP**	**STAT**	**STATACK**	**SUSPEND**
bck_inf	doplňující informace odesílané dopředně							
call_id	identifikace hovorového spojení	M	M	M	M	M	M	M
category	kategorie volaného účastníka				M		O	
cause	příčina rozpadu resp. ukončení spojení							
cir_id	identifikace použitého okruhu				M			
cont_chck	výsledek testu kontinuity hovorové trasy							
dst_num	telefonní číslo volaného				O			
dtmf	přenos volby DTMF během hovoru							
event	popis události, která nastala během spojování			O				
fwd_inf	doplňující informace odesílané zpětně			M				
new_num	telefonní číslo volaného po přesměrování							
orig_num	původní číslo volaného před přesměrováním			O				
originator	původce akce suspendování, resp. obnovení hovoru	M						M
rdr_inf	informace o přesměrování hovoru			O				
rdr_num	telefonní číslo iniciátora přesměrování			O				
req	požadavek doplňujících informací				M			
src_num	telefonní číslo volaného			M			O	
tone	specifikace tónu							
transport	transport informací ze signalizace Q.931			M				
usr2usr	signalizace mezi koncovými účastníky			O				

Tabulka 14: Parametry signalizačních zpráv pro řízení spojovacích procesů - část II.

11 Formát signalizačních zpráv

K formátování jednotlivých zpráv je použit značkovací jazyk XML. Standard XML se v posledních letech stává velice často používaným prostředkem pro návrh různých protokolů určených k synchronizaci informací mezi databázovými systémy, řízení průmyslových aplikací, propojení informačních systémů v jeden spolupracující celek a podobně.

Důvodů pro využití XML při návrhu protokolu je několik:

- **Textově orientovaný protokol** - jedním ze základních požadavků pro návrh protokolu je jeho textová orientace. V počátku návrhu byly dvě možné cesty, první z nich bylo využití nějakého, již existujícího způsobu formátování a druhou cestou byla možnost navrhnout způsob nový. Vybrána byla první cesta. Standard XML je přímo určen pro formátování informací přenášených, či uchovávaných v textové podobě a je proto onou nejlepší volbou pro formátování signalizačních zpráv. Výsledkem je přehledná forma textového zápisu dobře čitelná člověku a snadno zpracovatelné obslužným programovým vybavením.

- **Jednoznačnost definice zpráv** - Standard XML je navržen tak, že při správném použití v podstatě vylučuje výskyt nejednoznačností v informací, které jsou jeho pomocí formátovány pro přenos či zpracování.

- **Snadná rozšiřitelnost protokolu** - důležitým cílem při návrhu je otevřenost protokolu a snadná implementace nových funkcí a to jak v průběžném vývoji, ale též možnost doplnit strukturu o informace ze strany provozovatele. Formát jednotlivých zpráv zapsaných v jazyce XML je možné popsat pomocí DTD šablon, či XML schématu a tak definovat v podstatě libovolné rozšíření protokolu.

- **Možnost kontroly formátu zpráv** - Standard XML nabízí několik silných nástrojů na kontrolu struktury dokumentu formátovaného pomocí XML. Funkce realizující tuto kontrolu jsou dostupné v knihovnách pro řadu programovacích jazyků.

- **Možnost kontroly obsahu zpráv** - Pomocí XML schématu lze kontrolovat nejen strukturu dokumentu, v tomto případě XML zprávy, ale částečně též jeho obsah. Existují metody, které umožní kontrolu typů jednotlivých polí.

- **Snadná implementace** - Vzhledem k dynamickému vývoji v tomto odvětví je nutné mít možnost rychlé implementace protokolu do nových systémů, pří-

padně pružně reagovat na změny v protokolu a průběžně nové funkce implementovat do již existujícího programového vybavení systémů. Jelikož XML je značně rozšířeným mezinárodním standardem, jsou potřebné funkce, sloužící k práci s dokumenty formátovanými pomocí XML součástí speciálních knihoven pro většinu programovacích jazyků. Rychlost a kvalitu implementace značně ovlivní též vlastnosti popsané v minulých dvou bodech.

11.1 Formát zprávy

Každá zpráva navrhovaného protokolu obsahuje dva základní bloky informací. Prvním blokem je záhlaví zprávy, které obsahuje základní údaje o identifikaci zdrojového a cílového systému a identifikaci zprávy samotné. Existence záhlaví je povinná v každé signalizační zprávě. Druhým blokem je samotné tělo zprávy nesoucí konkrétní informace využitelné vzdáleným systémem pro řízení signalizačního spoje, řízení spojování, případně řízení směrování v síti. Tělo zprávy není povinnou součástí každé zprávy, není-li požadován přenos konkrétních informací (například jde-li o potvrzení přijetí zprávy bez nutnosti dalšího upřesnění), může být tělo zprávy vypuštěno. Základní struktura zprávy - její rozdělení do jednotlivých bloků je patrné z obecného zápisu, který ukazuje tabulka 15.

```
<ZPRAVA>
  <head>
  </head>
  <body>
  </body>
</ZPRAVA>
```

Tabulka 15: Obecný formát zprávy

Značka <ZPRAVA> bude v konkrétním případě nést označení zprávy dle výčtu zpráv uvedených v kapitole 9.

11.2 Formát záhlaví zprávy

Formát záhlaví zprávy je odlišný pro případ, kdy půjde o komunikaci uvnitř sítě jednoho provozovatele a pro případ, kdy půjde o komunikaci na rozhraní sítí dvou

provozovatelů. Důvodem rozdílů v záhlavích jsou odlišné požadavky na množství a obsah informací nezbytných pro přesnou identifikaci komunikujících systémů, jednotlivých hovorů, či použitých přenosových prostředků.

V případě komunikace uvnitř sítě jednoho provozovatele není nutné přenášet informace spojené se sítí provozovatele, neb tyto informace jsou shodné na všech systémech v síti a jsou součástí konfigurací jednotlivých síťových bodů signalizační sítě operátora. Naproti tomu mohou existovat parametry, které není nutné, případně které není ani žádoucí přenášet mezi sítěmi jednotlivých operátorů. Může se jednat například o prioritizaci určitých zpráv vázaných na konkrétní služby, či volání, globální informace sloužící k řízení spojování uvnitř sítě provozovatele s cílem maximálního využití sítě, nebo doplňkové informace umožňující přesnější monitorování provozu v síti.

Formát záhlaví zpráv přenášených mezi spojovacími systémy v síti jednoho provozovatele je uveden v tabulce 16.

```
<head>
  <msg_id>CISLO_ZPRAVY</msg_id>
  <msg_ack>CISLO_ZPRAVY</msg_ack>
  <src>
      <sys>JMENO_ZDROJOVEHO_SYSTEMU</sys>
  </src>
  <dst>
      <sys>JMENO_CILOVEHO_SYSTEMU</sys>
  </dst>
</head>
```

Tabulka 16: Záhlaví zprávy v případě interní komunikace

Formát záhlaví zpráv přenášených mezi spojovacími systémy pracující v sítích různých provozovatelů je uveden v tabulce 17.

Pole **msg_id** nese číslo zprávy. Číslo zprávy je generováno systémem, kde zpráva vznikla, je jedinečné a jednoznačně identifikuje danou zprávu. Možné algoritmy generování čísla zprávy a jeho využití je součástí kapitoly 10

Pole **msg_ack** je součástí pouze takových zpráv, které jsou odpovědí, případně potvrzením jiné zprávy.

Pole **src** respektive **dst** nesou identifikaci zdrojového respektive cílového systému. V případě, že se jedná o komunikaci uvnitř sítě jednoho provozovatele postačí jako

```
<head>
  <msg_id>CISLO_ZPRAVY</msg_id>
  <msg_ack>CISLO_ZPRAVY</msg_ack>
  <src>
      <sys>JMENO_ZDROJOVEHO_SYSTEMU</sys>
      <net>JMENO_ZDROJOVE_SITE</net>
  </src>
  <dst>
      <sys>JMENO_CILOVEHO_SYSTEMU</sys>
      <net>JMENO_CILOVE_SITE</net>
  </dst>
</head>
```

Tabulka 17: Záhlaví zprávy v případě externí komunikace

identifikace jméno systému. Jde-li o signalizační spoj propojující systémy, které jsou součástí sítí různých poskytovatelů je nutné identifikaci rozšířit o informaci nesoucí jméno sítě, které je systém součástí.

Jak již bylo popsáno v úvodu této kapitoly, uvedený formát zprávy je pouze výchozím, základním kamenem formátu záhlaví a může být snadno rozšířen o další informace, bude-li si to situace vyžadovat.

11.3 Formát těla zprávy

Jednotlivé parametry zpráv popsané v kapitole 10 jsou přenášeny v těle zprávy ve dvou možných formátech. První možností je je vyjádření parametru pomocí jednoduchého pole, obecný formát takového parametru je uveden v tabulce 18. Takový formát je vhodný pro parametry nesoucí jednoduchou nestrukturovanou informaci, například telefonní číslo volaného. Druhým možným formátem použitelným pro formátování parametru pole je strukturovaný parametr, jehož obecný formát je znázorněn v tabulce 19. Tento formát parametru je vhodný pro případ, kdy není možné obsah parametru vyjádřit jednou hodnotou, ale je zapotřebí uvnitř jednoho parametru přenést více různých informací. Tato možnost formátování parametru těla zprávy je vhodná pro parametry zpráv pro řízení spojovacích procesů, kde zajistí formátování a přenos potřebných informací tak, aby bylo možné jednoznačné mapování informací ze zpráv signalizačních systémů ISUP, Q.931 a Q-sig.

Opět i v tomto případě platí, že portfolio použitých parametrů může být snadno doplněno o další samostatná pole, případně celé strukturované bloky, bude-li to budoucí vývoj na poli telekomunikací vyžadovat.

```
<JMENO_PARAMETRU>HODNOTA_PARAMETRU</JMENO_PARAMETRU>
```

Tabulka 18: Obecný formát nestrukturovaného parametru zprávy

```
<JMENO_PARAMETRU>
  <INFORMACE-1>HODNOTA</<INFORMACE-1>
  <INFORMACE-2>HODNOTA</<INFORMACE-2>
  <INFORMACE-3>HODNOTA</<INFORMACE-3>
  ...
</JMENO_PARAMETRU>
```

Tabulka 19: Obecný formát strukturovaného parametru zprávy

12 Signalizační transakce

Tato kapitola popisuje signalizační výměny při sestavování a rušení spojení v síti. První část kapitoly popisuje signalizační transakce navrhovaného protokolu pro oba způsoby přenosu telefonního čísla volaného, tedy jak metodu *en-bloc*, tak i druhou v dnešní době již méně používanou metodu *overlap*. V druhé části jsou pak popsány signalizační transakce v návaznosti na signalizační systém DSS1 (Q.931) a SS.7/ISUP. V závěru kapitoly je pro úplnost uvedena i možnost napojení na analogové signalizační systémy U a E-M.

12.1 Signalizační transakce při řízení spojovaní hovoru

12.1.1 Metoda en-bloc

Obrázek 10 ukazuje jak probíhá signalizační výměna mezi dvěma body sítě, použije-li se k přenosu telefonního čísla volaného účastníka metoda *en-bloc*. V praxi to znamená, že telefonní číslo se přenáší sítí jako celek. O přenos se postará zpráva SETUP. Po jejím přijetí má vzdálená strana dostatečné množství informací na to, aby započala spojovací proces.

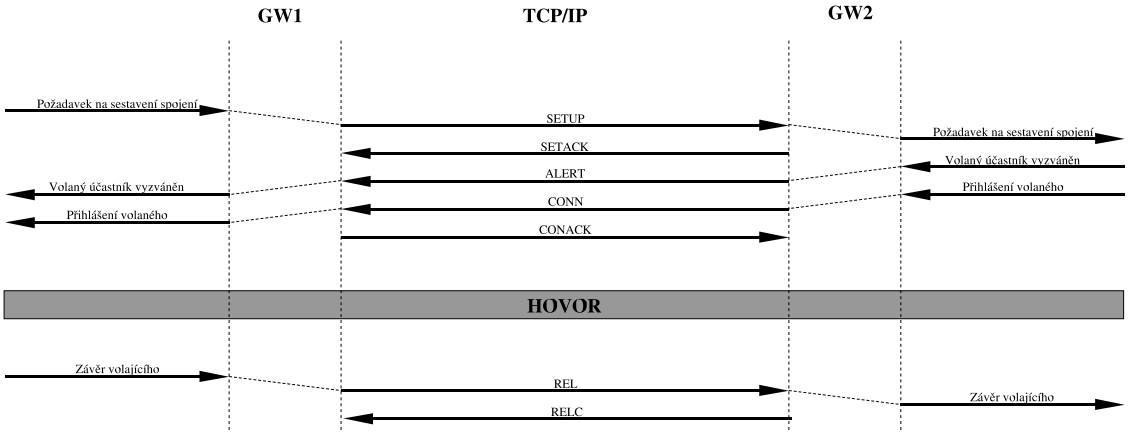
Informace o to, že směrovací informace je opravdu kompletní a spojovací proces byl zahájen, je přenesena směrem do výchozího spojovacího systému zprávou SETACK, která v tomto případě neslouží jen k informaci o úspěšném přijetí zprávy SETUP, ale zároveň potvrzuje úplnost přenesených informací.

Dojde-li k úspěšnému spojení spojovacích systémů volajících stran a následně k nazkoušení volaného, je spojovací systém na straně volajícího o tomto stavu informován zprávou ALERT. Ve stejném okamžiku začne být též vyzváněn volaný účastník.

Po přihlášení volaného účastníka dojde k vygenerování zprávy CONN, která o tomto stavu informuje stranu volajícího. Pro zajištění správné funkce celého systému je zpráva CONN, jako jedna z nejdůležitější zpráv signalizační výměny, potvrzena zprávou CONACK.

Po ukončení zmíněnéného procesu je hovorová trasa spojena od volajícího k volanému a může začít probíhat samotný hovor.

Dojde-li k závěru na jedné ze stran, způsobí tato akce vygenerování zprávy REL, která o závěru informuje protistranu. V těle zprávy jsou všechny potřebné informace nutné ke správné tarifikaci hovoru. Po přijetí zprávy REL začne spojovací systém proces ukončení spojení a dojde též k uvolnění veškerých vedení a spojovacích cest,



Obrázek 10: Výměna signalizačních zpráv při přenosu telefonního čísla volaného metodou *en-bloc*

které byly pro spojení využity.

Potvrzením úspěšného dokončení celého procesu a uvolnění spojovacích cest je vygenerování zprávy RELC.

12.1.2 Metoda overlap

Signalizační výměnu, která proběhne mezi spojovacími systémy v případě využití metody *overlap* k přenosu telefonního čísla popisuje diagram uvedený na obrázku 11.

Obdobně jako v předchozím případě, celý proces začíná zprávou SETUP. V případě použití metody *overlap* však není telefonní číslo volaného účastníka obsaženo v zprávě SETUP. Zpráva SETUP může, ale nemusí, nést pouze jeho část.

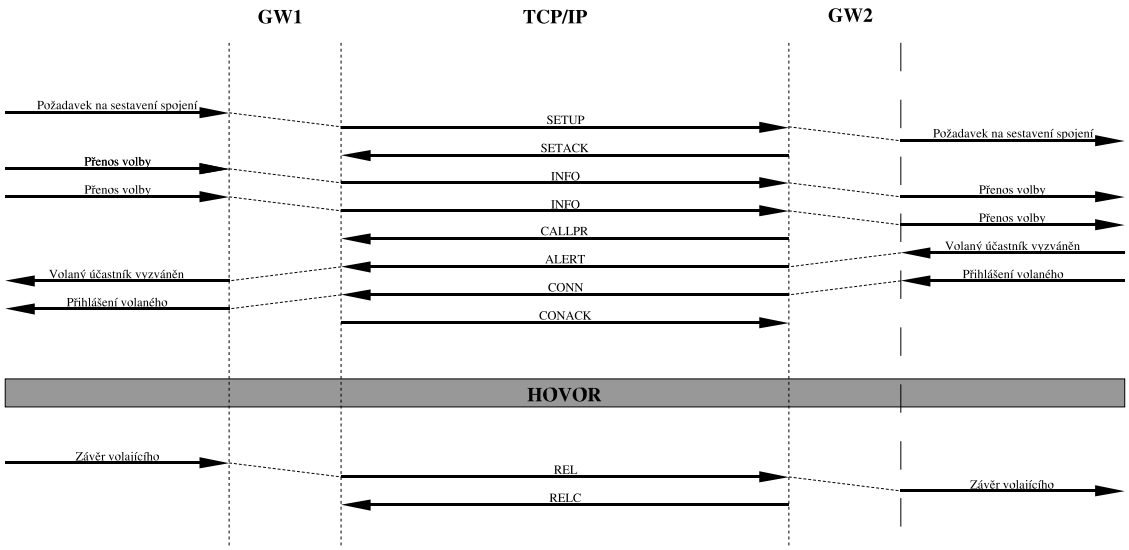
Obdrží-li vzdálený systém zprávu SETUP, která neobsahuje dostatečné množství informací nutných pro započetí spojovacího procesu, odešle zpět směrem k volající straně prázdnou zprávu SETACK. Tím potvrdí úspěšné přijetí zprávy SETUP a zároveň požádá o zaslaní dalších informací nutných pro spojovací proces.

Další, doplňující informace jsou pak přenášeny v jedné nebo více zprávách INFO až do chvíle, kdy vzdálený systém rozhodne, že množství přijatých informací je dostatečné a o tomto stavu informuje stranu volajícího.

Informaci o tom, že přijatá informace je dostatečná a proces spojování byl zahájen obdrží systém volaného ve zprávě CALLPR.

Od tohoto bodu je následující sled kroků již shodný s předchozím případem.

Podobně proces ukončení spojení se nikterak neliší od případu, kdy je k přenosu



Obrázek 11: Výměna signalizačních zpráv při přenosu telefonního čísla volaného metodou *overlap*

telefonního čísla použito metody *en-bloc* a není proto nutné tento proces znovu popisovat.

12.2 Návaznost na jiné signalizační systémy

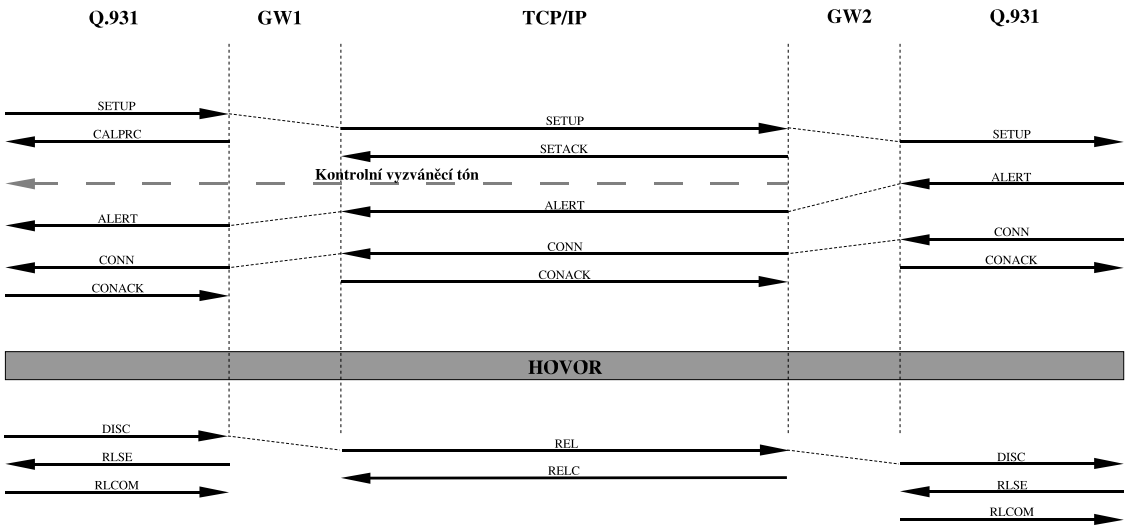
12.2.1 Návaznost na signalizace ISDN

V této kapitole jsou popsány signalizační výměny pro případ, že bude protokol navázán na již existující ISDN signalizační systémy jako DSS1 (Q.931) a SS.7/ISUP.

Jednotlivé zprávy a jejich parametry byly navrženy tak, aby bylo možné jednoznačně namapovat informační pole zpráv z ISDN signalizací do parametrů zpráv navrhovaného protokolu, tak aby nedocházelo k nejednoznačným stavům, či ke ztrátám potřebných informací na rozhraní sítí s různými signalizačními systémy. Popsané signalizační transakce jednoznačně popisují sestavení, či rušení základní hlasové služby napříč sítí používající různé signalizační systémy.

12.2.2 DSS1

Napojení na signalizační systém DSS1 ukazuje obrázek 12. Z obrázku je patrná jasná návaznost signalizačních zpráv na zprávy navrhovaného signalizačního protokolu. Uvedený diagram signalizační výměny popisuje případ, kdy je pro přenos telefonního čísla volajícího využita metoda en-bloc.



Obrázek 12: Signalizační výměna v návaznosti na DSS1 (Q.931)

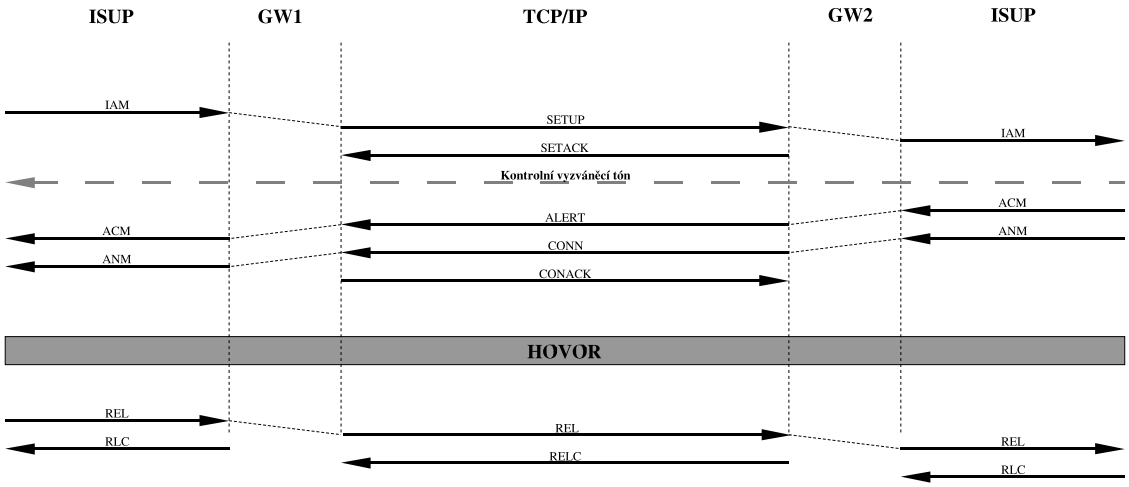
Pro případ použití metody overlap bude situace velice podobná a je možné ji snadno odvodit z obrázků 12 a 11. Zprávy INFO signalizačního systému DSS1 budou v tomto případě navazovat na zprávy INFO navrhovaného signalizačního systému a budou, jak již bylo popsáno, sloužit k postupnému přenosu telefonního čísla volaného.

12.2.3 ISUP

Propojení navrhovaného protokolu se signalizačním systémem SS.7/ISUP je popsáno diagramem uvedeným na obrázku 13. Obdobně jako v případě popisu spolupráce se signalizačním systémem DSS1 je i v tomto případě uveden diagram signalizační výměny pouze pro případ přenosu telefonního čísla metodou en-bloc. Tato metoda přenosu směrovací informace je v současných sítích výrazně častější, než metoda overlap. I zde platí, že signalizační výměna pro metodu overlap lze snadno odvodit z kombinací diagramů na obrázcích 13 a 11. Nositelem doplňkových směrovacích informací je v signalizačním systému SS.7/ISUP zpráva SAM. Tato zpráva bude proto iniciátorem odeslání zprávy INFO navrhovaného signalizačního protokolu.

12.2.4 Návaznost na analogové signalizace

Jelikož je protokol navrhovaný s cílem vytvořit universální síťový signalizační protokol použitelný nejen pro páteřní sítě poskytovatelů služeb, ale též pro rozsáhlé podnikové sítě, kde se stále poměrně hojně využívá různých systémů, které disponují analogovými přenašeči, je nutné umožnit též mapování těchto signalizací do navrhovaného



Obrázek 13: Signalizační výměna v návaznosti na ISUP

řešení.

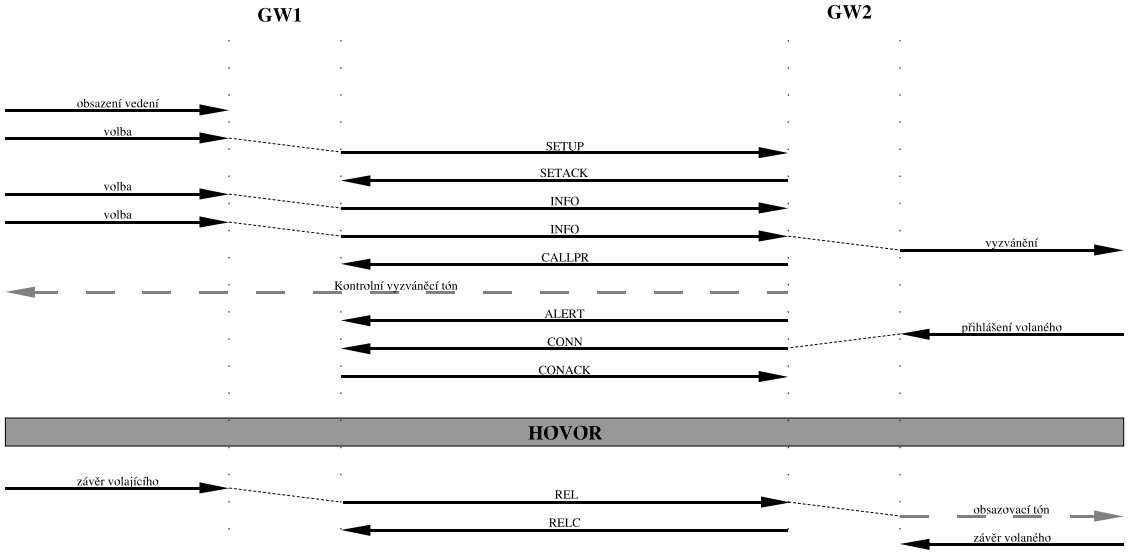
12.2.5 U

Signalizace typu U, čili smyčková signalizace je nejstarším signalizačním systémem používaným v tradiční telefonii. Signalizace je přesto stále "živou", neboť je využívána na analogových účastnických přípojkách a to jak ve veřejných telefonních sítích, tak na úrovni privátních podnikových systémů. Diagram uvedený na obrázku 14 popisuje mapování jednotlivých stavů, které mohou nastat na vedení se signalizaci U do zpráv navrhovaného signalizačního systému.

12.2.6 E-M

Signalizace E-M je jednou z nejčastěji používaných analogových signalizací v oblasti privátních telefonních sítí. Často je využívána na příčkách mezi pobočkovými systémy pracujícími v jedné lokalitě, k propojení pobočkových spojovacích systémů s branami, které propojují sítě různého typu, jako například VoIP brány na napojeni tradiční technologie na sítě využívající k přenosu hlasu IP protokolu, či mobilní brány, které slouží k propojení pobočkových telefonních sítí se sítěmi mobilních operátorů a podobně. Důvodem hojného využívání signalizace E-M je její jednoduchost a zároveň schopnost postihnout všechny důležité stavy, které mohou na příčkovém vedení nastat.

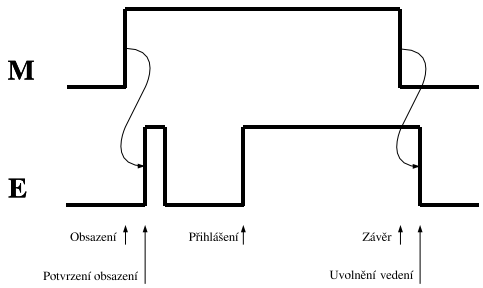
Vyjádření jednotlivých stavů spoje pomocí signalizace E-M popisují obrázky 15 a



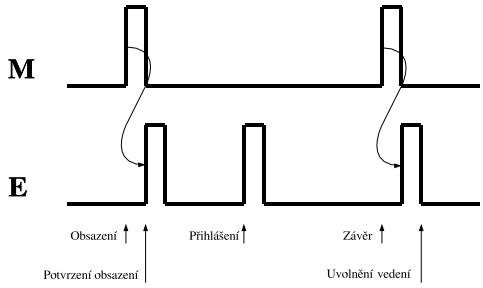
Obrázek 14: Signalizační výměna v návaznosti na signalizaci U

16. Trvalá varianta E-M signalizace je obsahem obrázku 15 a impulsní variantu uvádí obrázek 16.

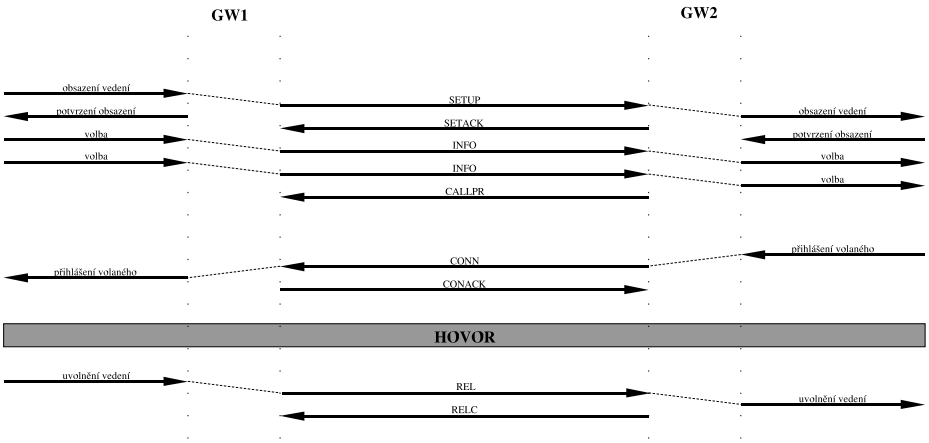
Návaznost E-M signalizace na navrhovaný protokol ukazuje diagram na obrázku 17.



Obrázek 15: Trvalá E-M signalizace



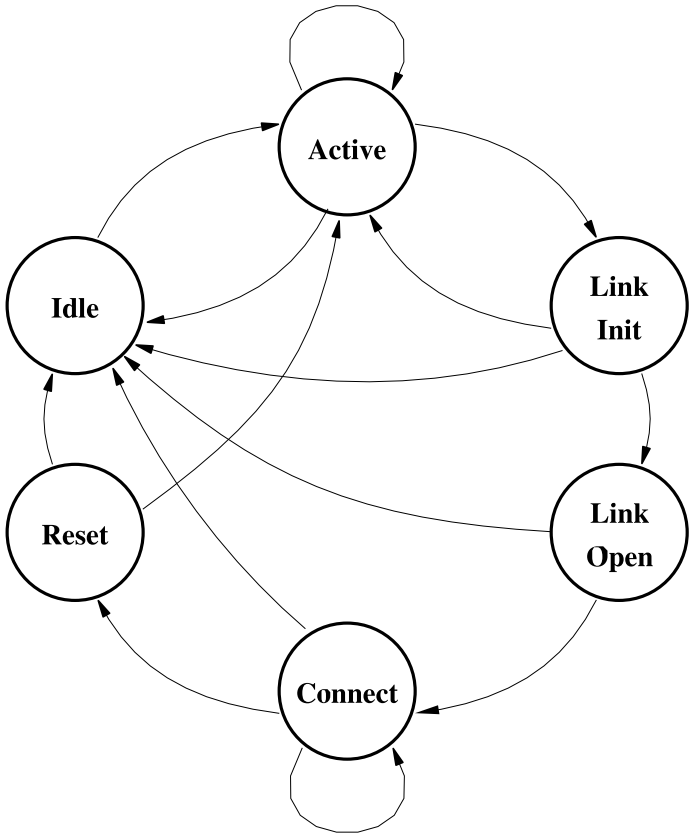
Obrázek 16: Impulsní E-M signalizace



Obrázek 17: Signalizační výměna v návaznosti na signalizaci E-M

13 Řízení signalizačního spoje

Tato kapitola popisuje proces ustanovení signalizačního spoje a jeho následné chování při výskytu událostí mající přímý vliv na jeho funkce. Stavový diagram popisující chovaní stavového automatu s konečným počtem stavů *Finite State Machine - FSM*, kterým je možné chování signalizačního spoje modelovat je uveden na obrázku 18. Podrobný popis jednotlivých stavů a událostí, jejichž důsledkem je změna stavu bude obsahem dalšího textu. Souhrn všech stavů uvádí tabulka 20, souhrn všech událostí je uveden v tabulce 21 a tabulka 22 je kompletní přechodovou tabulkou popisující chovaní stavového automatu.



Obrázek 18: Stavy signálního bodu

13.1 Idle

Stav Idle je výchozím stavem do kterého se systém řízení signálního spoje dostane ihned po jeho startu. V tomto stavu nejsou alokovány žádné systémové zdroje, nedo-

Číslo stavu	Stav
1	Idle
2	Active
3	Link Init
4	Link Open
5	Connect
6	Reset

Tabulka 20: Tabulka stavů

chází k vysílaní žádných zpráv a recipročně nejsou ani žádné zprávy přijímány. Není sestaveno žádné TCP spojení se sousední stanicí a není možné ho navázat, neboť na vstupním port není připraven žádný proces, který by tento pokus o spojení obsloužil. Stav Idle slouží k inicializaci systému a alokovaní potřebných zdrojů. Ihned po ukončení základních inicializačních kroků dojde ke změně stavu do stavu Active.

13.2 Active

V tomto stavu se signální bod pokouší sestavit TCP relaci s protistranou, dle jeho lokální konfigurace. Při neúspěchu zůstává systém nadále ve stavu Active. Po uplynutí doby, která je určená čítačem pro vyčkávání (Hold Timer) se pokusí opětovně o spojení.

V případě že se úspěšně podaří sestavit TCP relaci dojde k odeslání první inicializační zprávy LINKINIT k protistanici a dojde k překlopení do stavu Link Init.

Obdrží-li systém řízení signálního spoje požadavek o ukončení sestavování spojení od nadřazeného procesu, dojde k překlopení zpět do stavu Idle a následně k uvolnění veškerých používaných systémových zdrojů.

13.3 Link Init

Ve stavu Link Init systém čeká na zprávu LINKINIT od své sousední stanice. Nedojde-li k přijetí zprávy během doby, která je určená čítačem vyčkávání, dojde k přechodu systému do stavu Active a k opětovnému vyslání zprávy LINKINIT směrem k protistanici.

V případě příjetí zprávy LINKINIT během stanoveného intervalu dojde k otestování informací ze záhlaví zprávy a porovnání s konfigurací signálního bodu. Došlo-li během přenosu k chybě a nelze vyhodnotit správnost informací ze záhlaví zprávy,

Číslo události	Událost
1	Inicializace protokolu
2	Otevření TCP relace
3	Uzavření TCP relace
4	Chyba při sestavování TCP spojení
5	Přijetí zprávy LINKINIT
6	Přijetí zprávy LINKIACK
7	Přijetí zprávy LINKCHCK
8	Přijetí zprávy LINKCACK
9	Přijetí zprávy LINKRST
10	Přijetí zprávy LINKRACK
11	Přijetí zprávy LINKSTAT
12	Přijetí zprávy LINKSACK
13	Přijetí zprávy pro řízení spojovacích procesů
14	Přijetí zprávy pro přenos globálních informací
15	Vypršení časovače pro vyčkávání (Hold Timer)
16	Vypršení časovače pro kontrolu spojení (Keepalive Timer)
17	Ukončení protokolu

Tabulka 21: Tabulka událostí

systém přejde do stavu Active a celý proces se zopakuje. V případě správného přijetí zprávy, která však obsahuje chybné informace, dojde k odeslaní zprávy LINKSTAT, která protistranu informuje o chybném nastavení a systém se vrátí do stavu Idle.

Jsou-li přijaté informace v souladu s konfigurací a došlo-li k úspěšnému nastavení všech počátečních hodnot pro komunikaci, dojde k odeslaní zprávy LINKIACK a systém přejde do stavu Link Open.

Dojde-li k přijetí požadavku na ukončení komunikace na signálním spoji, je protistraně odeslána zpráva LINKSTAT s informací o této skutečnosti a systém přejde do stavu Idle.

13.4 Link Open

Ve stavu Link Open systém vyčkává, po dobu určenou časovačem vyčkávání, přijetí zprávy LINKIACK od své protistanice. Jakmile dojde k přijetí této zprávy je signalizační spoj ustanoven a dochází ke změně stavu do stavu Connect. V opačném případě, to jest když zpráva nebude doručena během daného intervalu, dojde k odeslání zprávy LINKSTAT a následně k přechodu do stavu Idle.

13.5 Connect

Stav Connect je stavem, kde se systém nachází ve svém funkčním stavu. V tomto stavu jsou přenášeny zprávy řízení spojovacích procesů a zprávy nesoucí globální informace.

Není-li k dispozici žádná zpráva ve vstupní vyrovnávací paměti je po uplynutí doby dané čítačem pro kontrolu spojení (Keepalive timer) odeslána zpráva LINKCHCK, která slouží jako výplňková zpráva a je určena pouze pro udržování kontroly na funkci signálního spoje.

Dojde-li k chybě při přenosu zpráv na signalizačním spoji, systém odešle zprávu LINKRST své protistraně, jako informaci o nesrovnalostech při přenosu a požadavek na novou inicializaci spoje. Současně je informován o tomto stavu nadřazený systém, aby přestal signalizační spoj používat k přenosu jiných zpráv, než zpráv určených k řízení spoje. Po těchto úkonech dojde k přechodu do stavu Reset.

Chyba může být detekována třemi možnými způsoby. Prvním z nich je pravidelná komunikace na signalizačním spoji. Nedojde-li během doby určené čítačem čekání doručena žádná zpráva, je tento stav označen jako chyba signalizačního spoje. Druhý způsob poskytuje pole msg-id, které umožní detekci chyby v případě přijetí jiné, než očekávané informace. Posledním způsobem je detekce informace (ať již v záhlaví zprávy, či v samotném těle zprávy), které syntakticky, či sémanticky neodpovídá XML schématu dané verze protokolu.

Dojde-li k přijetí požadavku na ukončení komunikace na signálním spoji, je protistraně odeslána zpráva LINKSTAT s informací o této skutečnosti a systém přejde do stavu Idle.

13.6 Reset

Stav reset slouží k určení závažnosti problému, který na signalizačním spoji nastal během komunikace. Systém v tomto stavu čeká na přijetí zprávy potvrzující požadavek o restartování signalizačního spoje. Dojde-li k přijetí této zprávy během doby určené časovačem čekání, systém přejde do stavu Active a dojde k inicializaci signálního spoje. V opačném případě dojde k přechodu do stavu Idle a k uvolnění veškerých alokovaných systémových zdrojů a celý proces se ocitne na samém počátku.

Stav Událost	**Akce**	**Odeslaní zprávy**	**Následující stav**
Idle			
1	Inicializace systémových zdrojů	-	Active
Active			
2	Inicializace systémových zdrojů	LINKINIT	Link Init
4		-	Active
17	Uvolnění systémových zdrojů	LINKSTAT	Idle
Link Init			
3		-	Idle
5	Přijatá zpráva je bez chyb	LINKIACK	Link Open
	Přijatá zpráva nebyla korektně přijata	-	Active
	Přijatá zpráva obsahuje chybné identifikační udaje	LINKSTAT	Idle
15		LINKSTAT	Active
17	Uvolnění systémových zdrojů	LINKSTAT	Idle
Link Open			
3		-	Idle
6	Dokončení inicializace spoje	-	Connect
15	Uzavření TCP relace	-	Idle
17	Uvolnění systémových zdrojů	LINKSTAT	Idle
Connect			
3		-	Idle
7	Nastavení hodnoty čítače pro kontrolu spoje	LINKCACK	Connect
9	Nastavení hodnoty čítače pro kontrolu spoje	LINKRACK	Connect
11	Nastavení hodnoty čítače pro kontrolu spoje	LINKSACK	Connect
13	Nastavení hodnoty čítače pro kontrolu spoje	*	Connect
14	Nastavení hodnoty čítače pro kontrolu spoje	*	Connect
15	Informování procesu řízení spojování	LINKRST	Reset
16	Nastavení hodnoty čítače pro kontrolu spoje	LINKCHCK	Connect
17	Uvolnění systémových zdrojů	LINKSTAT	Idle
Reset			
3		-	Idle
10	Informovaní procesu řízení spojování	-	Active
15	Uzavřeni TCP relace	LINKSTAT	Idle
17	Uvolnění systémových zdrojů	LINKSTAT	Idle

Tabulka 22: Stavová tabulka

Část V
Závěr

14 Závěr

Práce obsahuje základ nového protokolu pro přenos signalizačních informací v telefonních sítích. Popsaný protokol využívá odlišného pohledu na současnou problematiku a nabízí nové možnosti. Dojde-li k dopracování popsaného protokolu a následné implementaci, může výrazně zjednodušit probíhající konvergenci v oblasti telekomunikačních sítí, zlepšit subjektivní kvalitu poskytovaných služeb a umožnit též zavádění nových moderních doplňkových služeb.

Metody použité při návrhu protokolu výrazně zjednoduší budoucí implementaci a tudíž ovlivní i ekonomický aspekt závádění nového protokolu do reálného provozu.

Navržený koncept protokolu zajišťuje jeho otevřenost a v budoucnu snadnou rozšiřitelnost o další zprávy, parametry, či metody komunikace. Návrh dává značnou volnost provozovatelům sítí, kterým je dána možnost doplní protokolu o nové funkce pro použití uvnitř vlastní sítě.

Literatura

[1] John G. van Bosee: Signaling in telecommunication networks, John Wiley and Sons, Inc. 1997

[2] Mark A. Miller, P.E.: Voice Over IP Technologies, Hungry Minds, New York 2002

[3] Uyless Black: Voice Over IP, Prentice Hall PTR, New Jersey 1999

[4] Elliotte Rusty Harold and Scoot Means: XML v kostce, Computer Press, Praha 2002

[5] Jiří Kuthan, GMD Fokus: SIP Telephony, CVUT/CS, Praha, 2000

[6] Teorie a praxe IP telefonie, Kongresové centrum Hotelu Olšanka Praha, 2004

[7] xmlprague - conference on XML, ITI, Praha, 2005

[8] Rita Pužmanová, Pavel Šmrha: Propojování sítí s TCP/IP, Koop, České Budějovice, 1999

[9] Pavel Šmrha, Vladimír Rudolf: Internetworging pomocí TCP/IP, Koop, České Budějovice, 1995

[10] Libor Dostálek: Velký průvodce protokoly TCP/IP, Computer Press, Praha 2001

[11] Martin Tomek: Diplomová práce - Internet protokol telefonie, K332, Fel - ČVUT, Praha, 2000

[12] Vladimír Vrabec, Aleš Čapek: Internet CZ - Průvodce českého uživatele, Grada, Praha 1995

[13] RFC1105

[14] RFC1771

[15] RFC1889

[16] RFC2474

[17] RFC2543

[18] RFC2705

[19] RFC2976

[20] RFC4271

[21] http://www.openh323.org

[22] http://www.linuxtelephony.org

[23] http://www.computerhistory.org/

[24] Robert H'obbes' Zakon, http://www.zakon.org/robert/internet/timeline/

[25] www.ietf.org

[26] www.iana.org

A Vývoj sítě Internet

První krok

Naprosté počátky vzniku Internetu se datují do roku 1957, kdy je v reakci na vypuštění první umělé družice Země, Sputniku, ve Spojených Státech Amerických založena agentura na podporu vědeckého výzkumu ARPA *(Advanced Research Projects Agency)*. Skutečný počátek dějin Internetu však můžeme hledat až v roce 1969, kdy byl spuštěn experimentální provoz sítě ARPANET. V té době ARPANET propojil čtyři uzly, jednalo se o University of California Los Angeles, Stanford Research Institute, University of California Santa Barbara a University of Utah. Síť APRANET se tedy stala prvním dílkem obrovské skládačky, která se od roku 1969 začala budovat, nejprve na území USA a následně na celém světě.

Nekomerční provoz

V následujícím období, které trvalo až do roku 1992 se síť vyvíjí výhradně na akademické a nekomerční půdě. Důležitým mezníkem vývoje Internetu se stává rok 1973, kdy ARPANET poprvé překračuje hranice USA a dokonce i světadílu. Tohoto roku je k ARPANETu připojena londýnská universita - University College of London. Od tohoto roku se začíná též intenzivně pracovat na návrhu nových protokolů a na jejich následné implementaci do prostředí sítě ARPANET. Jedná se o protokoly rodiny TCP/IP, které tvoří pilíř sítě Internet až do dnes. Rychlost růstu sítě v tomto období je vidět v tabulce 23. V roce 1992 dochází k velmi důležité události, která navždy změnila Internet ovlivnila jeho další vývoj. Od roku 1992 je možné využít síť Internet i ke komerčním účelům.

Nástup Internetových technologií do komerční sféry

V této době si začíná do té doby čistě akademické prostředí Internetu zvykat na komerční podmínky. Také komerční svět hledá možnosti, které Internet nabízí a pokouší se je efektivně využít. Oba světy k sobě postupně hledají cestu. Pro komerční svět je velice důležitou událostí napsání prvního grafického prohlížeče webových stránek Mozaic v roce 1993. Nyní tedy již nic nebránilo masovému rozšíření Internetu, při kterém se středem zájmu stala právě možnost grafických presentací prostřednictvím webových stránek. V období mezi rokem 1992 a 1994 se zvýšilo množství připojených počítačů z 727 tisíc, na konci ledna 1992, až na téměř 2,5 milionu na konci roku 1993.

Datum	Počet počítačů
12/69	4
06/70	9
10/70	11
12/70	13
04/71	23
10/72	31
01/73	35
06/74	62
03/77	111
12/79	188
08/81	213
05/82	235
08/83	562
10/84	1.024
10/85	1.961
02/86	2.308
11/86	5.089
12/87	28.174
07/88	33.000
10/88	56.000
01/89	80.000
07/89	130.000
10/89	159.000
10/90	313.000
01/91	376.000
07/91	535.000
10/91	617.000
01/92	727.000

Tabulka 23: Počet připojených počítačů do roku 1992

Masový rozvoj

K masovému rozvoji Internetu začíná docházet roku 1994. V této době, kdy již jsou k dispozici nástroje, které umožňují výrobu a prohlížení grafických webových stránek se Internet nejen začíná plnit množstvím reklamních a propagačních materiálů, ale stává se i místem, kde se začínají nabízet služby a realizovat obchody. Nejprve Internet využívají pouze velké společnosti, neboť ceny připojení jsou poměrně vysoké. Později se vlivem rozvoje nových technologií podařilo ceny snížit na tolik, že se k Internetu začínají připojovat i malé a střední podniky. V poslední fázi došlo k takovému snížení nákladů na připojení a současně se Internet stal zdrojem nespočetného množství informací, že se k němu začaly připojovat i domácnosti. Rychlost rozvoje sítě je

patrná z tabulky 24. Z tohoto období stojí za zmínku dva roky. Prvním je rok 1995, teprve tohoto roku jsou k dispozici první nástroje pro tvorbu interaktivních webových stránek. Druhým rokem je rok 1999 v tomto roce jsou v USA v Indianě poprvé nabídnuty služby přímého bankovnictví prostřednictvím sítě Internet.

Datum	**Počet počítačů**
01/95	5.846.000
07/95	8.200.000
01/96	14.352.000
07/96	16.729.000
01/97	21.819.000
07/97	26.053.000
01/98	29.670.000
07/98	36.739.000
01/99	43.230.000
07/99	56.218.000
01/00	72.398.092
07/00	93.047.785
01/01	109.574.429
07/01	125.888.197
01/02	147.344.723
07/02	162.128.493

Tabulka 24: Počet připojených počítačů od roku 1994

Současnost

V současné době je růst Internetu zpomalený recesí, která postihla celou oblast telekomunikací. Investice provozovatelů páteřních sítí jsou snížené na minimum, dochází ke snižování stavu zaměstnanců a dokonce i ke krachům velkých společností, které tvořily svými sítěmi až doposud jádro Internetu. Pro představu o rozsahu problémů stačí zmínit krach společnosti Worldcom, která vlastnila jednu z největších sítí světa, krach společnosti KPNQwest a následný zánik největší evropské sítě EBONE, či obrovské finanční potíže společnosti Genuity, která stála u zrodu Internetu a její síť propojuje většinu vládních institucí v USA. I přes uvedené problémy Internet stále roste, posilují se kapacity spojů tvořící páteřní sítě a možná více, než kdy před tím upevňuje své pozice na místě největšího globálního informačního systému na světě.

1957 Vypuštěna první umělá družice Země, Sputnik. V reakci na tuto událost zřizuje vláda Spojených Států Amerických agenturu na podporu vědeckého výzkumu - ARPA *(Advanced Research Projects Agency)*

1961 Vznik první teorie popisující technologii sítě se spojováním paketů

1962 Vznik projektu počítačové sítě při agentuře DARPA *(Defense Advanced Research Project Agency)*

1966 První plán na vybudování sítě ARPANET

1969 ARPANET - experimentální síť s přepojováním paketů (4 uzly: University of California Los Angeles, Stanford Research Institute, University of California Santa Barbara a University of Utah)

1969 Páteřní síť má rychlost pouze 50 kb/s

1971 ARPANET se rozrostl na 15 uzlů a 23 počítačů

1972 ARPANET demo cca 20 směrovačů a 35 počítačů (použit nový protokol NCP - *Network Control Protocol*)

1972 Zahájení provozu elektronické pošty

1973 První mezinárodní spoj v ARPANETu, přes NORSAR je připojena londýnská universita (University College of London)

1973 Vznik architektury Ethernet (do dnes nejpoužívanější) pro použití v lokálních sítích

1973 - 1979 Vývoj protokolů rodiny TCP/IP a jejich postupná implementace do prostředí ARPANETu

1974 BBN spouští projekt Telenet - první komerční služba založená na spojování paketů - komerční verse ARPANETu

1976 Vydaní první knihy o ARPANETu

1977 Začíná vývoj základní architektury protokolů TCP/IP. (Stadford University, Bolt Beranek and Newman, University College London)

1979 Dokončení základů protokolů TCP/IP

1980 Zahájení experimentálního provozu TCP/IP v prostředí sítě ARPANET

1980 Na universitě v Berkeley (University of California at Berkeley) pracují na implementaci TCP/IP do akademické distribuce systému UNIX - BSD *(Berkeley System Distribution)*

1980 Připojeno celkem 250 000 síťových uživatelů (ne počítačů)

1983 Protokoly rodiny TCP/IP se stávají jedinými komunikačními protokoly sítě ARPANET

1983 Rozdělení ARPANETu na dvě sítě MILNET *(Military Network)* a ARPANET

1983 SUN Microsystems přenáší TCP/IP do komerční sféry

1983 Vznik sítě EARN *(European Academic and Research Network)*

1984 Zahájení provozu systému DNS (Domain Names System)

1985 Zahájení programu NSFNET - propojení 6 superpočítačových center; NSF *(National Science Foundation)*

1985 - 1995 NSF sponzoroval rozvoj sítě hodnotou 200 milionů dolarů. Vznik hlavní páteřní sítě severoamerického Internetu; NSFNET umožnil připojování lokálních sítí k Internetu na národní a regionální úrovni. Internet se stal otevřený pro akademickou sféru.

1986 První komerční výrobce směrovačů na světě

1987 Zahájení provozu sítě UUNET; první komerční ISP *(Internet Service Provider)* s vlastní páteřní sítí

1989 Formuje se agentura RIPE *(Reseaux IP Europeens)*; koordinátor výstavby IP sítě na evropském kontinentě

1990 Počet připojených počítačů překračuje 100.000

1990 Konec ARPANETu

1991 Vznik hypertextu a systému WWW *(World Wide Web)*

1991 Vznik sítě EBONE; patřila mezi největší páteřní sítě světa, v Evropě figurovala na prvním místě

1991 Koncem roku probíhají první testy s připojením ČVUT

1992 13. února byla formálně ČSFR připojena k síti Internet; první propojení vedlo z Lince na OVC ČVUT *(Oblastní Výpočetní Centrum)*; vzniká projekt akademické sítě FESNET *(Federal Educational and Scientific Network)*

1992 Přeměna hlavního správního orgánu Internetu IAB *(Internet Activities Board)* na *(Internet Architecture Board)*, veškerá odpovědnost za doporučení přebírají IETF *(Internet Engineering Task Force)* a IESG *(Internet Engineering Steering Group)*

1992 Internet se začíná komercializovat; do tohoto roku bylo nutné při připojení k Internetu (tj. k sítím ARPANET, BITNET, EARN) podepsat prohlášení, že nebude používán ke komerčním účelům

1992 V listopadu byly propojeny dva hlavní uzly akademické sítě v ČSFR; Praha a Brno

1992 - 1993 Internet propojuje 727.000 počítačů (únor 92); přes 1 milion počítačů (říjen 92); 1.5 milionu počítačů (květen 93)

1993 Po rozpadu ČSFR se síť FESNET rozpadá na CESNET *(Czech Educational nd Scientific Network)* a SANET *(Slovak Academic Network)*

1993 Vznik prvního grafického prohlížeče WWW - Mozaic

1993 K síti se připojilo OSN

1993 K síti CESNET je připojeno 9 měst

1994 Masová komercializace Internetu

1995 Federální výbor FNC *(Federal Networking Council)* schválil rezoluci definující Internet jako globální informační systém

1995 IETF vydává doporučení RFC1883 definující Internet Protokol verze 6 (IPv6)

1995 Vznik jazyka pro tvorbu interaktivních webových stránek - JAVA

1995 Vznik aplikace Real Audio

1998 ICANN *(Internet Corporation for Assigned Names and Numbers)* přebírá od IANA *(Internet Assigned Numbers Authority)* a NSI *(National Security Institute)* odpovědnost za registraci doménových jmen a přidělování IP adres => poslední zásah vlády USA do rozvoje Internetu

1999 První Internetová banka - Bank of Indiana

2002 Dochází ke sloučení společností KPNQwest a GTS, po sloučení páteřních sítí vzniká nové uskupení, které v Evropě provozuje 25 000 kilometrů dlouhou síť s přípojnými body v 60 evropských velkoměstech a 14 metropolitních sítí.

2002 LINX umožňuje svým členům připojit se pomocí 10 gigabitového Ethernetu

2002 Po ekonomickém kolabsu společnosti KPNQwest se v Belgii 1. července 2002 začíná odpojovat páteřní síť EBONE

2002 27. listopadu dochází ke sloučení sítí Genuity a LEVEL3

2004 4. března NIX přesahuje hranici 3 Gb/s

2004 11. listopadu NIX přesahuje hranici 4 Gb/s

2005 7. prosinec NIX přesahuje hranici 10 Gb/s

2006 21. listopad NIX přesahuje hranici 20 Gb/s

2006 koncem roku dosahují toky ve velkých peeringových centrech Evropy 100 - 200 Gb/s