UNIVERZITA PARDUBICE
ÚSTAV ELEKTROTECHNIKY A INFORMATIKY

SYSTÉM PRO SLEDOVÁNÍ DATOVÉHO A VOIP PROVOZU NA LOKÁLNÍCH SÍTÍCH

BAKALÁŘSKÁ PRÁCE

AUTOR PRÁCE: Martin Řehůřek
VEDOUCÍ PRÁCE: Ing. Martin Dobrovolný

2007

UNIVERSITY OF PARDUBICE
INSTITUTE OF ELECTRICAL ENGINEERING AND INFORMATICS

SYSTEM FOR MOMITORING OF DATA AND VOIP TRAFFIC ON LOCAL AREA NETWORKS

BACHELOR WORK

AUTHOR: Martin Řehůřek
SUPERVISOR: Ing. Martin Dobrovolný

2007

Univerzita
Pardubice
Ústav elektrotechniky
a informatiky

Vysokoškolský ústav: Ústav elektrotechniky a informatiky
Katedra/Ústav: Ústav elektrotechniky a informatiky
Akademický rok: 2006/2007

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Pro: Řehůřek Martin

Studijní program: Informační technologie

Studijní obor: Informační technologie

Název tématu: Systém pro sledování datového a VoIP provozu na lokálních sítích

Zásady pro zpracování:
Cílem práce je vytvořit systém pro sledování množství přenesených dat v lokální počítačové síti. Systém by měl být schopen rozlišit vybrané typy dat a zejména některé hlasové protokoly používané v technologiích VoIP.
Součástí práce bude:
1. popis stávajícího stavu a technologií používaných ve VoIP
2. popis a porovnání nejpoužívanějších VoIP protokolů
3. návrh řešení pro sledování provozu
4. návrh a realizace software typu klient / server pro monitoring provozu
5. praktická realizace na modelovém pracovišti
Klientské aplikace budou sledovat provoz a budou umožňovat nahlédnutí do aktuálního množství přenesených dat
Serverová aplikace bude schopná zpracovávat shromážděná data

Seznam odborné literatury:
Dostálek L., Kabelová A.: „***Velký průvodce protokoly TCP/IP a systémem DNS***“, Computer Press, Praha 2002
Kállay F., Peniak P.: „***Počítačové sítě***“, Grada 2003
Velte T.: „***Síťové technologie Cisco, Velký průvodce***“, Computers Press Brno 2003
Janeček J., Bílý M.: „***Lokální sítě***“, ČVUT Praha 2004
Cisco Systems: „***Cisco Networking Academy Program***“ 1-2. a 3-4. díl, Indianapolis, USA 2005

Rozsah: Rozsah 30-40 stran

Vedoucí práce: Dobrovolný Martin

Vedoucí katedry (ústavu): prof. Ing. Pavel Bezoušek, CSc.

Datum zadání práce: 31.11.2006

Termín odevzdání práce: 12.5.2007

Poděkování

Na tomto místě bych rád poděkoval Ing. Martinu Dobrovolnému za cenné rady a připomínky při zpracování bakalářské práce.

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně Univerzity Pardubice.

V Pardubicích dne 9. 5. 2007

(vlastnoruční podpis)

ABSTRAKT

Tato práce se zabývá problematikou sledování množství přenesených dat na počítačové síti s rozlišením datového a hlasového provozu. Pro tento účel bude navrhnut systém, který kromě sledování provozu bude tyto údaje shromažďovat v databázi a umožní grafický výstup v podobě grafu a dalších údajů, které pomohou určit jakým způsobem se projevuje nasazení VoIP technologií v prostředí lokální počítačové sítě.

Obsah

Seznam zkratek

Zkratka	Význam nebo vysvětlení
API	Application programming interface – rozhraní pro programování aplikací
b	Bit – základní jednotka informace (binární číslo)
B	Byte – jednotka informace složená z osmi bitů
BSD licence	Licence pro svobodný software – umožňuje volné šíření licencovaného obsahu
HTML	Hyper Text Markup Language – značkovací jazyk pro hypertext
HTTP	Hyper Text Transfer Protocol – protokol určený pro výměnu hypertextových dokumentů
IEEE 802.11	Standard pro lokální bezdrátové sítě (Wireless LAN, WLAN) vyvíjený 11. pracovní skupinou IEEE LAN/MAN
IP	Internet Protocol – protokol používaný v počítačových sítích
ITU	International Telecommunication Union – Mezinárodní telekomunikační unie
kb/s	Jednotka přenosové rychlosti (počet kilobitů vyslaných nebo přijatých za sekundu)
PBX	Private Branch Exchange – pobočková ústředna
PC	Personal Computer – osobní počítač
PCM	Pulse Code Modulation – způsob digitalizace hlasu
RTP	Real-time Transport Protocol – zajišťuje nepřerušovaný přenos hlasových paketů počítačovou sítí
TCP	Transmission Control Protocol – protokol transportní vrstvy
UDP	User Datagram Protocol – protokol pro přenos dat sítí bez kontroly doručení
WWW	World Wide Web – označení pro aplikace internetového protokolu HTTP

Úvod

Cílem této práce je sledovat data přenášená v prostředí počítačových sítí. Při sledování zohledňovat typ přenášených dat, a to především přenos lidského hlasu s určením podílu tohoto typu dat na celkovém objemu přenesených dat.

Přenos lidského hlasu (za účelem komunikace) prostřednictvím počítačové sítě se označuje jako *VoIP* (*Voice over Internet Protocol*). V dnešní době se *VoIP* stává perspektivním prvkem v oblasti telekomunikací. V současnosti *VoIP* technologie používá přibližně 22 procent [5] českých firem. S rozvojem vysokorychlostního připojení k Internetu toto číslo stále narůstá a je předpoklad, že kolem roku 2010 se zvýší podíl *VoIP* na ostatních hlasových přenosech na více než tři čtvrtiny (firemní zákazníci).

Počítačová síť při přenosu dat využívá principu přepojování IP paketů [1] a tím dokáže velmi efektivně hospodařit s dostupnou přenosovou kapacitou sítě. Avšak v oblasti přenosu hlasu na počítačových sítích skrývá tento způsob potenciální problémy. Tyto problémy vznikají zejména tím, že je *VoIP* technologie, oproti klasické telefonii, provozována na síti, která nebyla pro přenos hlasu (telefonii) vůbec koncipována. Jen díky moderním technologiím, které se neustále vyvíjejí a zlepšují, je přenos hlasu po datových IP sítích realizovatelný. Jde zejména o problém pravidelného doručování paketů. Tento problém řeší například zvýšení přenosové kapacity sítě nebo upřednostňování hlasových přenosů na uzlech sítě.

Tato situace je důvod, proč je zajímavé sledovat, jakým způsobem se podílí přenos hlasu na běžném provozu počítačové sítě. V této práci bude navržen a popsán systém, který umožní vyhodnotit podíl *VoIP* provozu na celkovém objemu přenesených dat a mimo jiné sledovat hodnoty maximálního datového přenosu. Takto získané údaje zodpoví především otázku, jakou mírou *VoIP* ovlivňuje vytížení počítačové sítě. Tyto údaje

mohou pomoci při analýze některých problémů s přenosem hlasu. Např. pokud správce sítě dostane informaci o špatné kvalitě hlasového spojení, může ověřit vytíženost sítě v daném čase. Na základě těchto údajů lze rozhodnout, zda mohlo dojít k problému pozdržení či zahození paketů z důvodu nízké propustnosti počítačové sítě.

Další uplatnění systému pro sledování síťového provozu lze najít u správců sítě, kteří chtějí sledovat množství přenesených dat jednotlivých uživatelů. Tímto lze například odhalit uživatele, kteří zatěžují počítačovou síť nadměrným přenosem dat.

1 Telekomunikační technologie v prostředí počítačových sítích

1.1 Pojmy používané při přenosu hlasu v počítačových sítích

***VoIP* (*Voice over Internet Protocol*)** – obecný název pro technologii umožňující přenášet lidský hlas po datových sítích používajících IP protokol.

Internetová telefonie – nasazení technologie *VoIP* ve veřejném Internetu, za účelem hlasové komunikace prostřednictvím Internetu.

IP telefonie – technologii *VoIP* je samozřejmě možné nasadit i mimo Internet, obecně všude tam kde lze provozovat protokol IP. Tedy například i v sítích privátních či poloprivátních. Pak se jedná o tzv. *IP telefonii*, která by měla být obecnějším pojmem než *telefonie internetová*, protože *internetová telefonie* je zvláštním případem *IP telefonie*, ale nikoli naopak.

1.2 Technologie přenosu hlasu

Telefonie je telekomunikační služba, jejíž hlavní funkcí je přenos lidské řeči mezi účastníky. Řeč je při telefonním hovoru pomocí záznamového zařízení (mikrofonu) převedena na elektrický signál, který je možno přenášet po telefonní síti (u *IP telefonie* je použita místo telefonní sítě síť datová), u příjemce je signál opět převeden na řeč. Princip telefonování prostřednictvím *VoIP* spočívá v možnosti uskutečnit telefonickou komunikaci pomocí zařízení připojeného k počítačové síti nebo Internetu. Toto zařízení může být počítač nebo IP telefon, který dokáže fungovat jako samostatný síťový prvek nezávisle na počítači.

Technologie *VoIP* používají různé architektury. Může být použito centralizované architektury, což je analogie ke klasickým veřejným telefonním sítím [2]. Jde o centralizované řízení sítě, kde koncová zařízení přijímají funkční pokyny z tohoto centrálního prvku. Tato

architektura je obecně založena na existenci řídícího zařízení[1], které plní zejména tyto funkce:

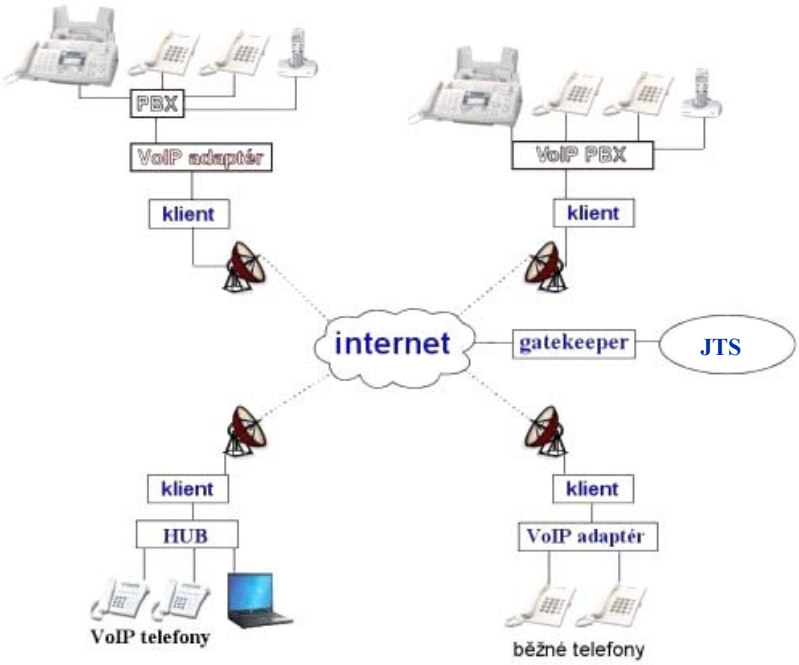
- připojení do veřejné telefonní sítě a převod hlasu/faxu na IP pakety.
- funkci řízení komunikací – udržování a správu konfigurace a směrování hovorů v rámci telefonní sítě.

Tato architektura je využívána především v prostředí lokálních sítí a v podstatě kopíruje architekturu sítí analogových.

Oproti tomu distribuovaná architektura více využívá filozofie IP sítí, kde jsou funkce ústředny (tedy sestavování hovorů, směrování a další) rozprostřeny do koncových bodů. Koncové body mohou být *VoIP* brány, IP telefony, media servery nebo jakékoliv zařízení schopné iniciovat a ukončit *VoIP* hovor. Této architektury se využívá hlavně v prostředí Internetu, kde je očekávána větší flexibilita. U této architektury závisí vlastnosti sítě především na koncových zařízeních. U distribuované architektury se jako koncová zařízení nejčastěji používají softwarové aplikace (*ICQ Phone*, *NetMeeting*).

Jako koncová zařízení lze pro *IP telefonii* použít i analogová zařízení jejich zapojením přes *VoIP* adaptér (viz Obrázek 1). Propojení sítě s technologií *VoIP* do jednotné telefonní sítě (*JTS*) je uskutečněno prostřednictvím zařízení[2] zajišťujícího konverzi mezi adresací v IP prostředí (IP adresy) a klasickým telefonním prostředím (telefonní číslo). Obrázek 1 představuje schématicky znázorněnou implementaci *VoIP*.

[1] Na obrázku číslo 1 označeno jako *VoIP PBX*
[2] Na obrázku číslo 1 označeno jako *gatekeeper*

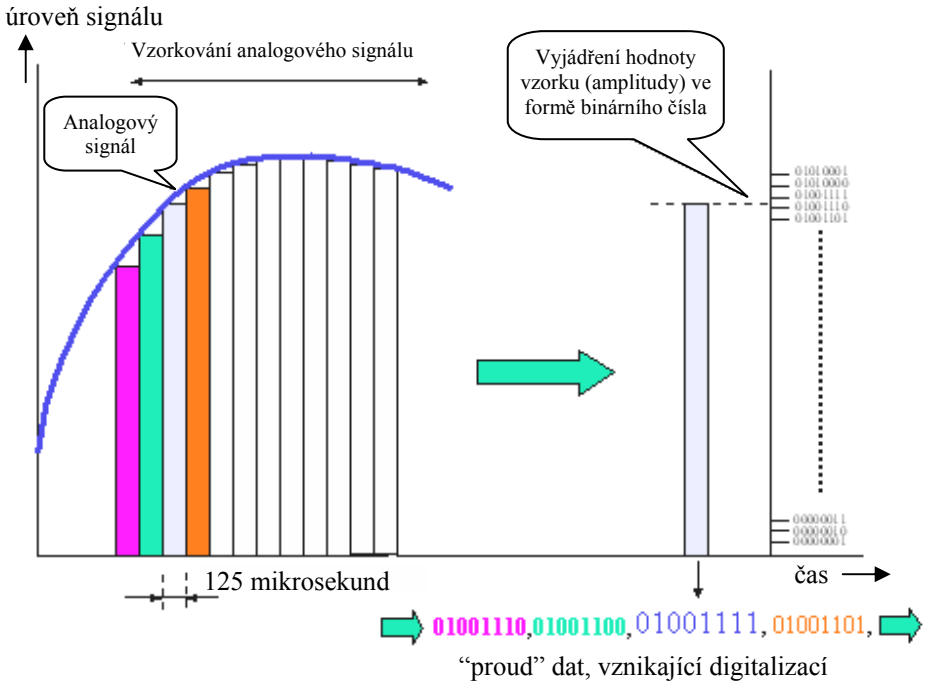


Obrázek 1: Ukázka použití VoIP technologií (6)

1.3 Digitalizace hlasu

Aby bylo možné přenášet lidský hlas po IP sítích, musí být převeden na data. Dodnes nejvíce používaná metoda digitalizace, nazvaná *PCM* (*Pulse Code Modulation*), byla poprvé použita v roce 1938 a standardizována pod označením *G.711* byla v roce 1960. Analogový signál (z mikrofonu) je vzorkován 8000 krát za vteřinu, přičemž každý vzorek může nabýt jedné z 256 hodnot amplitudy. 256 hodnot lze vyjádřit jako 2^8, tedy 8 bitů 8000 krát za sekundu znamená požadavek na 64000 bitů za sekundu – tedy 64 kb/s (proto má jeden ISDN B kanál kapacitu právě 64 kb/s [3]).

Obrázek 2 znázorňuje převod analogového signálu na digitální. Zde je každých 125 mikrosekund změřena úroveň analogového signálu hlasu a naměřená hodnota zaznamenána (max. hodnota 256). Výsledkem je proud dat s šířkou pásma 64 kb/s.



Obrázek 2: Ukázka digitalizace hlasu (7)

64 kb/s je poměrně hodně a protože je lidské ucho nedokonalé, lze používat ztrátové algoritmy, jimiž je při solidní kvalitě přenášeného hlasu dosahována požadovaná kapacita již kolem 6 kb/s.

Aby bylo možné uskutečnit hlasovou komunikaci v IP prostředí, je potřeba nejen navázat spojení a spojení opět ukončit, ale především přenést hlas mezi účastníky. Přenos vlastního telefonního hovoru, tzn. lidského hlasu, je tedy základním pilířem celé komunikace. Při tomto přenosu je nejprve analogový signál (zaznamenaný mikrofonem) převeden do digitální podoby a komprimován na výsledný datový tok. Dále následuje převod výstupních dat do paketů a jejich přenos sítí.

1.4 Nejpoužívanější kodeky

Přenést hlas počítačovou sítí je vcelku jednoduché, pokud nezáleží na kvalitě a rychlosti. Pro potřeby *VoIP* je však vhodné, aby byly splněny některé požadavky, mezi něž patří co nejmenší nutná šířka přenosového pásma a co nejmenší zpoždění při přenosu.

Velkou mírou obě kritéria ovlivňují použité kodeky. Kodek je zařízení umístěné v koncovém zařízení (IP telefon, *VoIP* brána a další), které

převádí analogový zvukový signál na digitální a ten dále komprimuje. Čím kvalitnější je komprese, tím déle trvá, a tím větší blok dat může potřebovat pro svoji funkci. Nejoptimálnější komprese by byla v případě, kdyby se celý hovor nejprve zaznamenal a teprve poté zkomprimoval. To však není vhodné pro hovory, kde by obě strany spolu chtěly aktivně komunikovat. Naopak nejrychlejší je převést hlas do jednoduché datové podoby a v reálném čase přenést sítí – tento přístup má však velké nároky na šířku pásma přenosu.

Tento problém je známý a proto byly vyvinuty různé kodeky. Navzájem se liší několika parametry – kvalitou komprese, nutným datovým tokem pro kvalitní přenos a velikostí jednotlivých paketů. Některé kodeky jsou volně k dispozici, některé jsou licenčně zpoplatněny. Tabulka 1 obsahuje přehled nejznámějších a nejpoužívanějších kodeků.

Tabulka 1: Přehled nejznámějších kodeků (4)

Kodek	Datový tok [kb/s]	Délka paketu [ms]	Komentář
G.711	64	10 - 20	Výborná kvalita, nejnižší zpoždění
G.726	16 - 40	20	Dobrý kompromis
G.729	8	20	Licencovaný, nejlepší kompromis
G.723@6.3	6.3	30	Licencovaný, nízká šířka pásma
GSM-EFR	12.2		Pro srovnání: mobilní telefony

U hodnoty datového toku je zároveň nutné počítat s tím, že maximální možný výsledný proud dat bude větší. Je to dáno skutečností, že každý paket obsahuje navíc IP a UDP hlavičky, což při počtu a velikosti odesílaných paketů hraje nezanedbatelnou roli.

Tabulka 2 zobrazuje přehled skutečně potřebných datových toků pro přenos sítí.

Tabulka 2: Skutečně potřebný datový tok kodeků (4)

Kodek	Datový tok [kb/s]	Skutečně potřebný datový tok [kb/s]
G.711	64	87.2
G.726	32	55.2
G.726	24	47.2
G.729	8	31.2
G.723.1	6.3	21.9

Všechny kodeky počítají s tím, že přenést ticho je zbytečným zatěžováním datové linky nulovou informací, proto se používá i detekce a potlačení ticha (*silence suppression*), při kterém se po síti nic neposílá.

Mezi nejčastěji používané a doporučované kodeky (hlavně pro přenosy na lokální síti) patří *G.711*, pokud není nutné použít co nejmenší šířku pásma.

2 Popis a porovnání nejpoužívanějších hlasových protokolů

2.1 Komunikační protokoly

Slouží k vlastnímu přenosu hlasu. Mezi komunikační protokoly *IP telefonie* patří protokoly *RTP* a *RTCP*.

RTP (*Real Time Protocol*) zajišťuje samotný přenos zvuku (případně videa) v reálném čase mezi koncovými body sítě. Přesněji zajišťuje doručení *paketů* ve správném pořadí pomocí časových razítek (*timestamp*), sekvenčních čísel apod. Při komunikaci přes IP se používá protokol UDP.

RTCP (*Real Time Control Protocol*) je analogie *RTP* pro řídící služby. Používá se k zasílání kontrolních paketů účastníkům hovoru. Hlavní funkcí je poskytovat zpětnou vazbu o kvalitě služby *RTP*.

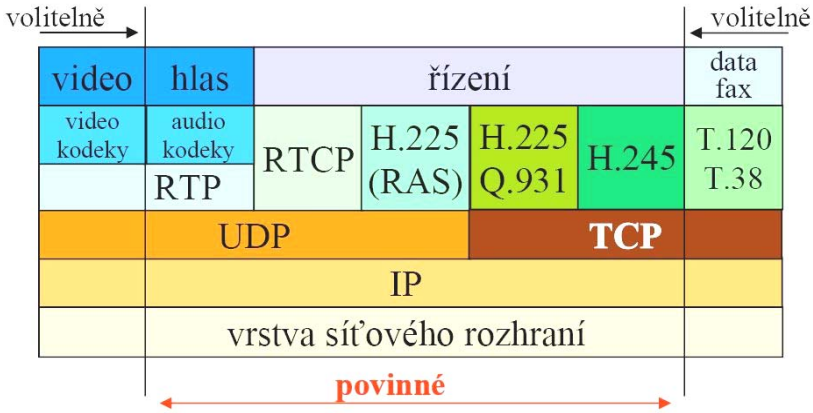
2.2 Signalizační protokoly

Signalizace se obecně v telefonii stará o spojování a rozpojování hovorů, dohodu komunikačních parametrů mezi účastníky a přenos služebních údajů, například identifikace volajícího směrem k volanému účastníku. U *IP telefonie* v současnosti existují dva hlavní protokoly pro signalizaci – *H.323* a *SIP*, dále pak existují např. *MGCP*, *Megaco*, *Skinny* a další. *H.323* a *SIP* protokoly se využívají v distribuované architektuře. *MGCP, Megaco* a *Skinny* se využívají v architektuře centralizované. Protokoly *H.323*, *SIP*, *MGCP* a *Megaco* používá např. IP ústředna *Asterisk*. *Skinny* protokol používají IP ústředny *Cisco CallManager* (nejnovější ústředny *Cisco CallManager v5.0* pracují i s protokolem *SIP*).

2.2.1 Protokoly standardu H.323

H.323 je sada standardů podporovaných organizací ITU-T a je dosud nejrozšířenější. Zahrnuje různé protokoly pro zajištění zvukové a obrazové komunikace v počítačové síti. Implementace jsou zpravidla stabilní a dobře pracující. Nevýhodou protokolů *H.323* je, že při rozšíření o nové možnosti vzniká nutnost vytvoření nové verze. Tyto protokoly jsou binární. V transportní vrstvě byl původně vyžadován protokol TCP, který je relativně obtížné implementovat v malých systémech, má-li například být *IP telefonie* přivedena až do telefonu. Od verze *H323v3* je možné použít i protokol UDP. Tabulka 3 znázorňuje architekturu protokolů standardu *H.323*.

Tabulka 3: Protokolová architektura dle ITU-T H.323 (8)



Význam jednotlivých signalizačních protokolů:

- H.225 – signalizace, tedy sestavování a rušení volání.
- H.225 RAS – registrace u správce (*gategeeper*).
- Q.931 – signalizace v sítích ISDN.
- H.245 – zjišťování vlastností jednotlivých terminálů.

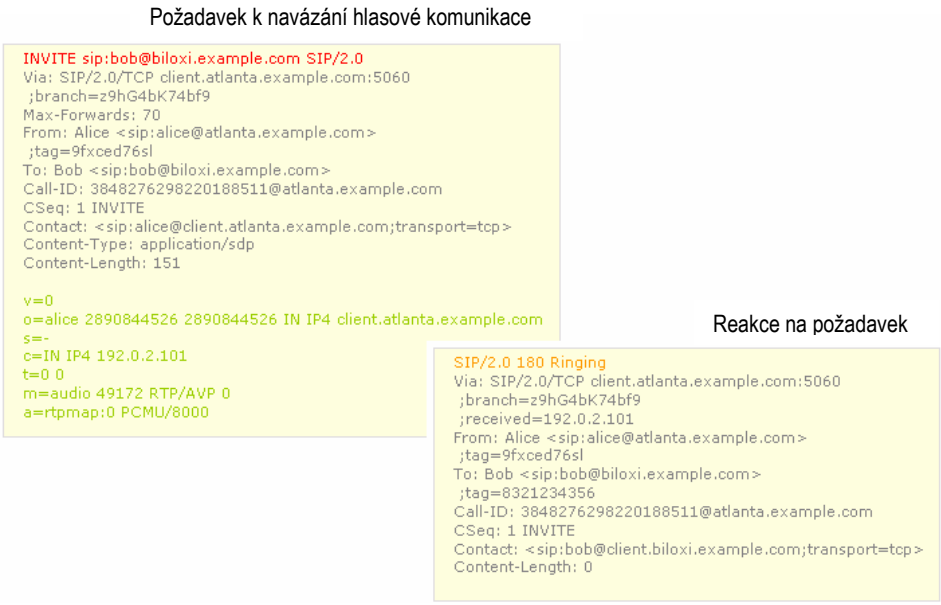
2.2.2 Protokol SIP

Protokol *SIP*, tedy *Session Initiation Protocol* (protokol pro inicializaci relací), vytvořený pracovní skupinou *MMUSIC* v rámci organizace *IETF* je založen na jiné koncepci. Je textový, svojí strukturou obdobný protokolu *HTTP*, používanému službou *WWW*, nebo protokolu *SMTP*,

používanému pro přenos elektronické pošty. U protokolu *SIP* se jednotlivé signalizační zprávy sestávají z posloupnosti textových hlaviček. Vzhledem k tomu, že je vytvořen na textové bázi, je otevřený a flexibilní. Stal se velice oblíbený a postupně nahrazuje protokoly standardu *H.323*. Protokol může být snadno rozšiřován přidáváním nových hlaviček, specifikovaných jako samostatné dokumenty *RFC* nebo *IETF* draft.

Protokol *SIP* nespecifikuje, jaký má být použit transportní protokol. Obvykle se proto používá protokol UDP, který lze snadno implementovat. Protokol *SIP* je určen pro spojování, rozpojování a správu spojení mezi dvěma nebo více účastníky. Není svázán s žádnými konkrétními protokoly pro vlastní přenos multimediálních dat. Uvnitř zprávy protokolu *SIP* pro navázání spojení je proto zapouzdřena zpráva jiného protokolu, který specifikuje použitá kódování pro multimediální data, jejich parametry a čísla portů, na kterých mají být data vysílána nebo přijímána. Obvykle se pro tento účel používá protokol *SDP* (*Session Description Protocol*), který je rovněž textový. Protokol *SIP* plní ještě jednu funkci – registraci uživatelů, která umožňuje používat pro identifikaci uživatelů logické adresy nezávislé na fyzickém umístění uživatele. Obrázek 3 zobrazuje ukázky zpráv protokolu *SIP* se zapouzdřenou zprávou protokolu *SDP*. Jde o zprávy sloužící k navázání spojení mezi volajícím účastníkem a volaným. Z těchto zpráv je možné vyčíst následující údaje:

- první řádek obsahuje název metody,
- *Via* položky ukazují cestu,
- položky *From* a *To* specifikují logickou adresu odesílatele a příjemce,
- *Call-ID* je jedinečný identifikátor během jednoho spojení,
- položka *Contact* obsahuje adresu pro přímou komunikaci,
- *Content-type* určuje typ obsahu,
- *Content-Length* určuje velikost obsahu.



Obrázek 3: Zprávy protokolu SIP (9)

3 Problematika hlasových přenosů v počítačových sítích

S rozvojem *VoIP* technologií, a především *IP telefonie*, zaniká potřeba tvorby samostatné telefonní sítě a samostatné počítačové sítě. Současným trendem je sjednocení obou těchto sítí. Pro počítačovou síť to znamená určité zvýšení zatížení novým druhem provozu. Dále je nutné si uvědomit, že počítačová síť svým charakterem přepínání paketů (u analogové telefonie použito přepínání okruhů) není pro hlasové přenosy v reálném čase vhodným prostředím. Hlas a data mají naprosto rozdílné požadavky na kvalitu přenosu (Tabulka 4).

Tabulka 4: Parametry ovlivňující kvalitu přenosu hlasu a dat (10)

Citlivost/tolerance	Hlas (v reálném čase)	Data
Zpoždění	citlivý	tolerantní
Změny zpoždění	citlivý	tolerantní
Šířka pásma	citlivý	citlivý
Ztráta dat	tolerantní	citlivý

K základnímu problému při přenosu hlasu po datové síti dochází v okamžiku, kdy součet souběžných požadavků na přenesení datových bloků překročí celkovou dostupnou přenosovou kapacitu sítě. V této situaci dojde k pozdržení nebo zahození paketů, což způsobí výpadky ve hlasové komunikaci, ozvěnu, zpoždění nebo dokonce přeruší hlasového spojení. Při přenosu dat toto zpoždění nezpůsobí vážnější problémy, pokud netrvá příliš dlouho. Avšak v hlasové komunikaci i krátké zpoždění působí znatelné problémy. Pokud při přenosu hlasu dojde ke zpoždění většímu než 50 ms, tak se to projeví tzv. echem, kdy hovořící bude slyšet sám sebe. Zpoždění větší než 250 až 300 ms způsobí, že si hovořící budou navzájem skákat do řeči. Rovněž proměnlivost zpoždění může způsobit, že bude hovor nesrozumitelný. Nedokonalost lidského ucha naopak nezaznamená jistou malou ztrátovost paketů.

Aby se při přenosu hlasu v reálném čase minimalizovala proměnlivosti zpoždění, je použito zásobníku (*bufferu*). Hlasové pakety jsou u přijí-

macího zařízení umístěny do tohoto zásobníku a poté plynule doručovány. Uživatel je takto alespoň částečně ochráněn před problémy sítě. Rovněž existuje řada mechanismů, jak zajistit potřebnou prioritu pro hlasové pakety a minimalizovat tak zpoždění v síti. Na úrovni Ethernetu je to standard *802.1p*, na úrovni IP pak např. *TOS*, resp. *DiffServ*, *RSVP*, *MPLS* atd.

Zdrojem zpoždění může být samotná síť nebo např. doba potřebná ke kompresi. Pro případy, kdy je zdrojem zpoždění počítačová síť, je dobré mít informace o počtech přenesených dat na této síti. Z těchto informací lze vyvodit závěry, zda dochází k přetížení sítě a po jakou dobu, nebo lze zjistit, co je zdrojem přetížení. Analýzou údajů o počtu dat přenesených sítí lze tyto problémy odstranit např. lepším navržením sítě s rovnoměrnějším rozložením zátěže v čase.

Tím, že hlasové přenosy probíhají ve formě přenášení datových paketů sítí, je možné měřit jejich počet a velikost. Tímto měřením lze získat přehled o tom, jakým způsobem *IP telefonie* ovlivňuje vytížení počítačové sítě a naopak, jak datový provoz ovlivňuje provoz hlasový.

4 Návrh systému pro sledování provozu

Aby bylo možné měřit množství dat přenesených počítačovou sítí a zohlednit při tom jejich typ, je nutné získat k těmto datům přístup. Zpřístupnění a zpracování dat přenášených v rámci jedné počítačové stanice lze provést pomocí speciálního softwaru. Tento software je možné naprogramovat pomocí programovacího jazyka, který by obsahoval funkce umožňující přístup k síťovému adaptéru a datům, které přes něj prochází. Při programování lze také použít speciálních vývojových nástrojů resp. rozhraní.

Například operační systém Windows obsahuje knihovnu nazvanou *Internet Protocol Helper* (*IP Helper*). Tato knihovna umožňuje vyvíjet software pro získávání a modifikování síťového nastavení na lokálním počítači. Dále tato knihovna umožňuje poskytnout informace o počtu přenesených dat v prostředí počítačových sítí s TCP/IP protokolem, což je pro účely monitorování síťového provozu podstatné.

Výhodou této knihovny je, že je standardní součástí operačního systému Windows a není nutné ji zvlášť instalovat. Další výhoda spočívá v tom, že je možné kdykoliv zjistit celkový objem přenesených dat od okamžiku spuštění operačního systému.

Knihovna *IP Helper* ale neumožňuje přístup přímo k přenášeným datům, což je velkou překážkou při vyhodnocování typu přenášených dat. Z tohoto důvodu jsem jako nástroj pro monitorování síťového provozu zvolil knihovnu *WinPcap*, která tento požadavek splňuje. Knihovna *WinPcap* oproti knihovně *IP Helper* není standardní součástí operačního systému a je nutné ji doinstalovat.

4.1 Knihovna WinPcap

WinPcap je knihovna, která umožňuje přistupovat k síti a síťovým zařízením. Standardní *API* sice umožňuje pracovat s transportní i IP vrstvou modelu TCP/IP, ale neumožňuje jednoduše nahlédnout do přenášených dat. Tento problém řeší knihovna *WinPcap*.

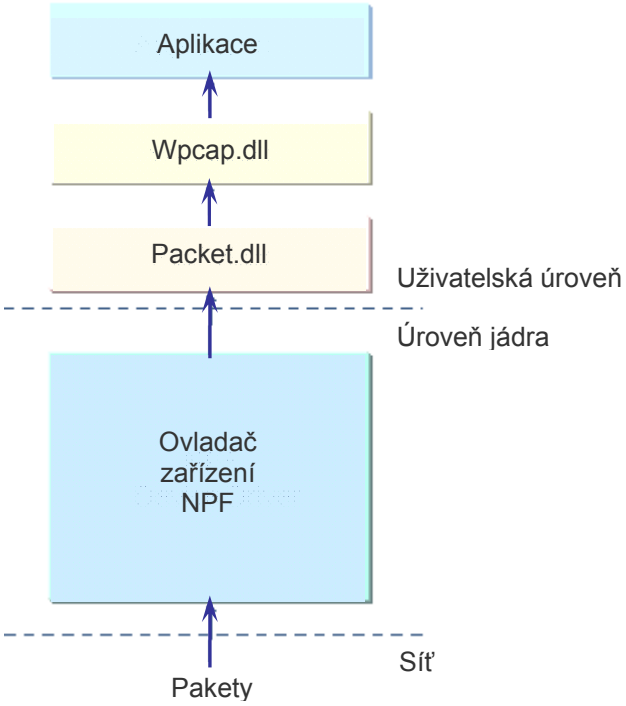
4.1.1 Základní informace o knihovně

WinPcap je *open-source* knihovna (je šířena pod *BSD open-source* licencí) určená pro operační systémy Windows. Lze ji použít také pod operačními systémy Linux, pro které je určena verze nazvaná *libpcap*.

Tato knihovna umožňuje programátorovi přistupovat přímo k datům získaných z IP vrstvy modelu TCP/IP. Dokáže získat kompletní obsah paketů přicházejících i odcházejících z daného zařízení. Má i soubor vlastních filtrovacích pravidel. Bohužel některé obzvláště paranoidní antivirové programy mohou označit *WinPcap* za vir či trojský kůň.

Knihovna *WinPcap* je vhodná především pro tvorbu aplikací, jako jsou síťové a protokolové analyzátory, síťové monitory, generátory provozu a *IDS* – obranné detekční systémy a bezpečnostní nástroje.

První částí knihovny *WinPcap* je ovladač *NPF* (*Netgroup packet filter*), který přímo komunikuje s ovladači síťových karet a získává od nich data. Dále jsou zde použity knihovny *packet.dll* a *wpcap.dll*, které tvoří *API* pro knihovnu – ovládají *NPF* a tvoří rozhraní mezi ním a uživatelskou aplikací (Obrázek 4).



Obrázek 4: Schéma komponent WinPcap (11)

WinPcap je nezávislá na *WinAPI* a pracuje paralelně se sokety Windows, ovšem využívá ve své implementaci i některé funkce z *Winsock*. Pomocí *raw soketů* lze také získat data procházející počítačovou sítí, avšak tyto data systém před zpřístupněním doupraví. Navíc je obtížné se v *raw soketech* společnosti Microsoft orientovat bez dostatečného nastudování dané problematiky. Naproti tomu knihovna *WinPcap* je velmi dobře zdokumentovaná a má jednodušší použití.

4.1.2 Použití knihovny WinPcap

Knihovna *WinPcap* se vyvíjí primárně pro sítě s protokolem TCP/IP. Existuje podpora i jiných sítí, ale není úplně stoprocentní.

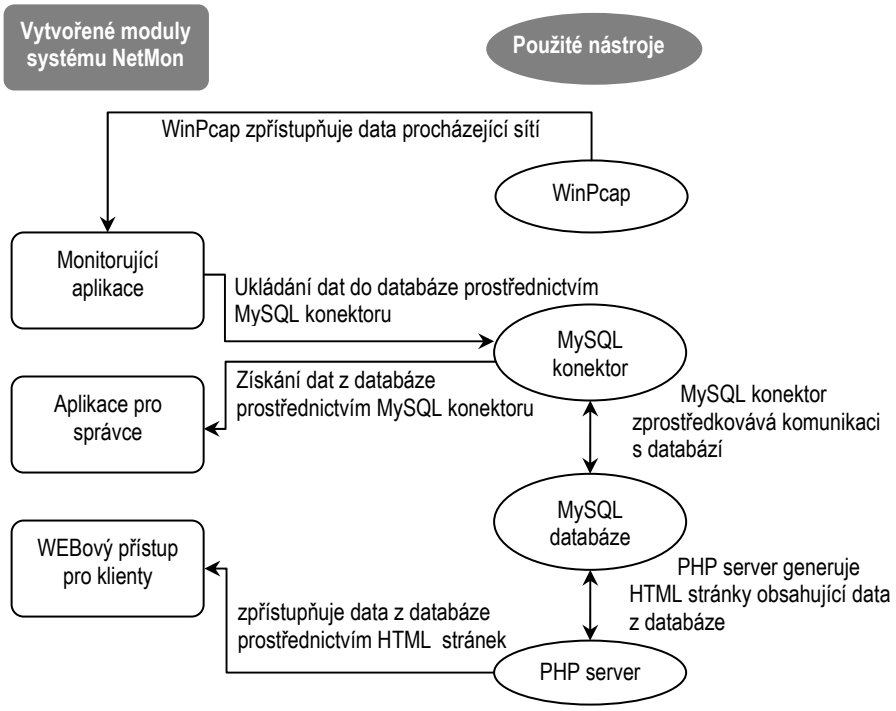
Samotná knihovna je napsána v jazyce *C* a jazyk *C* (popřípadě *C++*) se tímto nabízí i jako hlavní jazyk pro vývoj programů pro knihovnu *WinPcap*.

Aby bylo možné spustit program pracující s knihovnou *WinPcap*, je nutné knihovnu nejdříve nainstalovat. Instalační soubor této knihovny lze stáhnout na internetových stránkách výrobce [12].

Pro vývoj aplikací pracujících s *WinPcap* je třeba použít balíček *Developer´s pack* neboli balíček pro vývojáře – je nutný pro kompilaci programů a obsahuje všechny potřebné hlavičkové soubory a knihovny. Tento balíček lze také stáhnout na internetových stránkách výrobce [13]. Pro kompilaci programu bylo použito *Microsoft Visual Studio .NET 2003*, protože *WinPcap* oficiálně podporuje pouze *Microsoft Visual C++*. Balíček pro vývojáře obsahuje i dokumentaci popisující mimo jiné, jak program kompilovat a příklady zdrojových kódů.

5 Návrh a realizace software pro monitoring provozu

Systém pro sledování a vyhodnocování provozu na počítačové síti byl pojmenován *NetMon* a skládá se z několika modulů. Jednotlivé moduly obstarávají funkci monitorování provozu, shromažďování dat, vyhodnocování shromážděných dat a zpřístupnění výsledků statistik. Obrázek 5 znázorňuje komunikaci jednotlivých modulů a jejich činnost.



Obrázek 5: Popis jednotlivých modulů monitorovacího systému

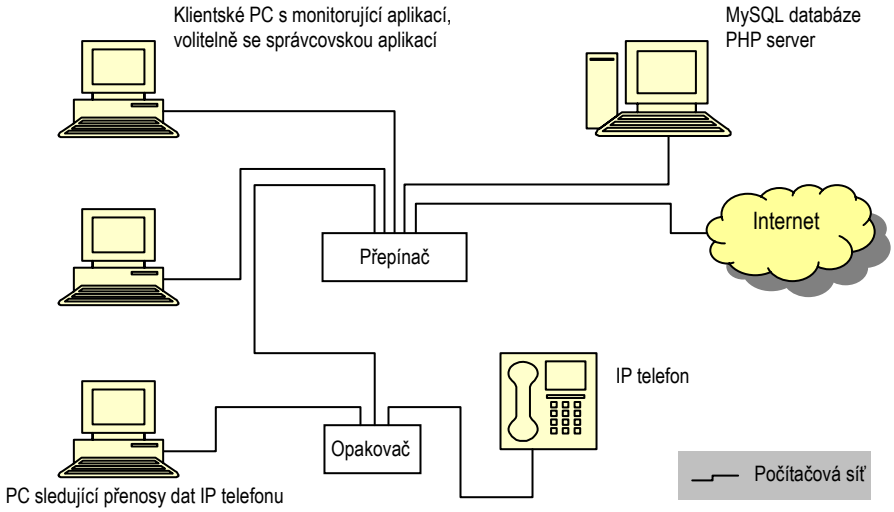
Sledování provozu na počítačové síti provádí monitorující aplikace, která musí být spuštěna na každém PC, jež má být sledován. Lze také sledovat další zařízení, která mají IP adresu. Informace o počtu a typu přenesených dat jsou ukládány do jednotné databáze.

Aplikaci pro správce je možné nainstalovat na jakýkoliv PC (s operačním systémem Windows) v síti, který má přístup k centrální databázi. Tato aplikace zpřístupňuje informace o přenesených datech a tyto údaje dále zpracovává.

Při sledování přenosu dat na PC je zaznamenáno jméno přihlášeného uživatele. Proto se jednotliví uživatelé mohou informovat o množství

přenesených dat, jež byla přenesena na jejich PC. Přístup k těmto informacím získají prostřednictvím WEBového rozhraní.

Obrázek 6 představuje příklad použití monitorovacího systému nasazeného na lokální síti.



Obrázek 6: Schéma systému pro sledování provozu na lokální síti

5.1 Monitorující aplikace

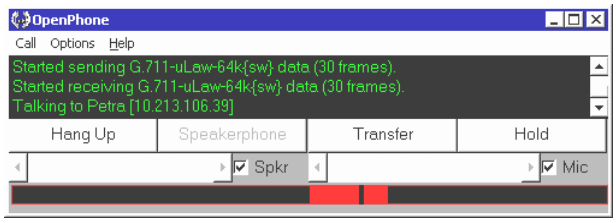
Na klientských počítačích bude spuštěna skrytá aplikace, která bude sledovat síťovou komunikaci daného počítače. U každého paketu aplikace vyhodnotí, zda odesílatel i příjemce pochází z lokální sítě a jde tedy o provoz na lokální síti, nebo jde o externí přenos dat. Vyhodnotí, zda jsou data přijímaná nebo odesílaná.

Tato aplikace je vytvořena v programovacím jazyce *C++* v prostředí *Microsoft Visual Studio 2003*. Sledovaná data síťové komunikace poskytuje aplikaci knihovna *WinPcap*, kterou je nutné do operačního systému doinstalovat.

Monitorující aplikace realizuje následující funkce. Počítá objem přenesených dat v rámci přenosu na jednotlivých definovaných portech. Dále rozlišuje, zda jde o *VoIP* provoz buď podle portu nebo dle detekce a rozboru několika vybraných *VoIP* protokolů. Například pokud bude mít uživatel nainstalovanou aplikaci *Skype* s nakonfigurovaným portem

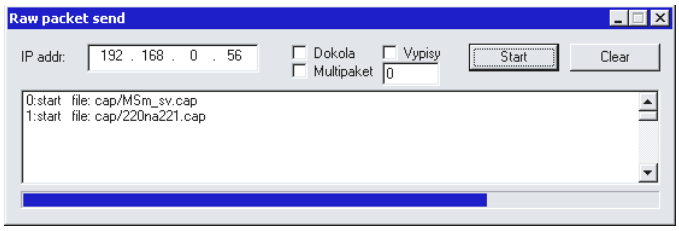
příchozího spojení číslo 64765, budou na základě příslušné konfigurace přenesená data na tomto portu sčítána samostatně a označena jako *VoIP*. Z *VoIP* protokolů dokáže aplikace rozpoznat a monitorovat hlasovou komunikaci s protokoly *H323*, *SIP* a *Skinny*.

Funkčnost monitorování přenosu hlasu prostřednictvím *VoIP* protokolu standardu *H323* byla na monitorující aplikaci vyvíjena a testována pomocí aplikace *OpenPhone* (Obrázek 7). Aplikace *OpenPhone* je software umožňující hlasovou komunikaci mezi počítači. Tato aplikace byla vytvořena v rámci projektu *OpenH323Project* [13].



Obrázek 7: Aplikace OpenPhone s grafickým rozhraním

Sledování hlasové komunikace s *VoIP* protokoly *SIP* a *Skinny* bylo na monitorující aplikaci vyvíjeno a testováno pomocí programového simulátoru *Winsraw* vytvořeného ve společnosti Retia, a.s. (Obrázek 8).



Obrázek 8: Simulátor síťového provozu Winsraw

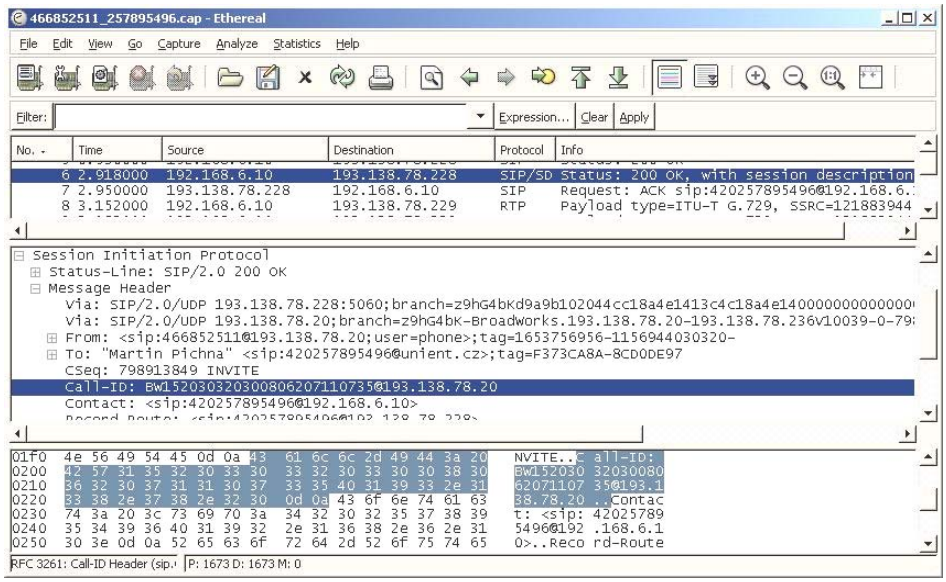
Tento simulátor do sítě vysílá komunikaci, která byla předem zaznamenána a uložena do souboru. Záznam síťové komunikace do souboru, pro tento simulátor, lze provézt pomocí programu *Ethereal* nebo *Network Monitor*. Síťový provoz pro testování byl zaznamenán na *VoIP* komunikaci v prostředí IP ústředny *Cisco CallManager* verze 5.0. Tato IP ústředna primárně pracuje se signalizačním protokolem *Skinny*, verze 5.0 však nově podporuje i protokol *SIP*.

Signalizační protokol standardu *H323* komunikuje na portu číslo 1720. Protokol *SIP* používá port číslo 5060 a protokol *Skinny* port číslo 2000.

U všech těchto protokolů je při navazování hlasového spojení vyslána signalizační zpráva nesoucí mimo jiné informaci s označením čísla portu, na kterém bude hlasový přenos probíhat. Dále tato zpráva obsahuje identifikační číslo přenosu, které umožňuje dalším signalizačním zprávám jednoznačně určit ke kterému přenosu patří. Pro monitorující aplikaci je klíčové znát číslo portu uskutečněného spojení. Data přenášená na tomto portu monitorující aplikace vyhodnocuje jako *VoIP* a přiděluje označení použité služby (*H323*, *SIP*, *Skinny*). Tuto komunikaci sleduje až do ukončení hlasového přenosu.

Při ukončování hlasové komunikace je mezi účastníky vyslána zpráva obsahující identifikační číslo přenosu, který je ukončován. Na základě této zprávy je ukončeno sledování portu, na kterém probíhal hlasový přenos.

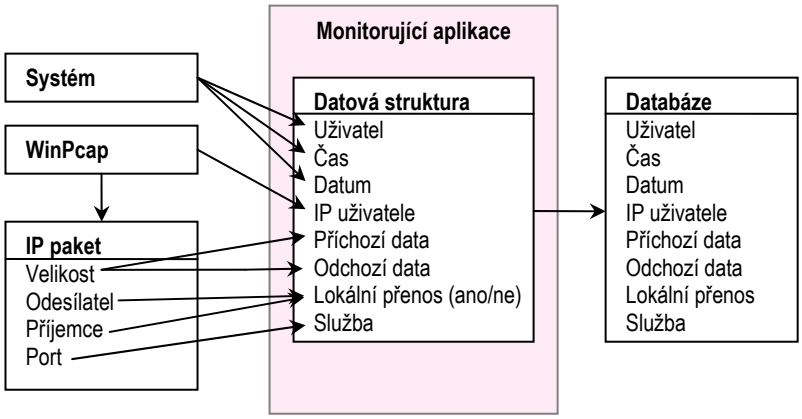
Pro rozbor *VoIP* protokolů, kontrolu funkce monitorující aplikace a pořizování záznamů síťové komunikace byl použit síťový analyzátor *Ethereal* (Obrázek 9). *Ethereal* ve verzi pro Windows používá při komunikaci se síťovým adaptérem knihovnu *WinPcap*. Instalační soubor programu *Ethereal* lze stáhnou na internetových stránkách výrobce [14].



Obrázek 9: Síťový analyzátor Ethereal

Načítané počty přenesených dat jsou ukládány do centrální databáze v intervalu pět minut s informací o jméně přihlášeného uživatele, IP

adrese počítače (na kterém přenos probíhal), datem a časem, druhem dat a označením, zda jde o lokální nebo externí přenos. V případě, že nebude možné navázat spojení s databází, uloží se data do souboru a odešlou až v okamžiku úspěšného spojení. Obrázek 10 zobrazuje zjednodušené schéma funkce monitorující aplikace, kde je na základě zpracování IP paketu procházejícího sítí plněna datová struktura, jejíž data jsou ukládána do databáze.



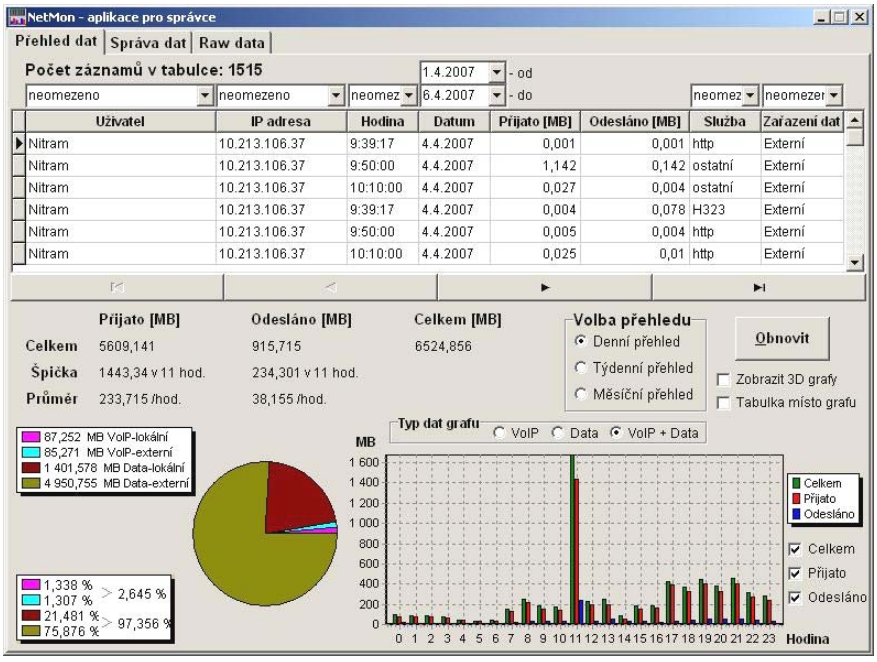
Obrázek 10: Schéma monitorující aplikace

Podle konfigurace je také možné zadat sledování jiných (vzdálených) PC, resp. jiných zařízení zapojených do počítačové sítě majících IP adresu. Toho lze využít pro sledování provozu u zařízení, jako jsou např. IP telefony nebo PC, na které není možné nainstalovat monitorující aplikaci (např. z důvodu nepodporovaného operačního systému). Sledování vzdálených zařízení je možné jen v případě, že bude tato komunikace přístupná pro PC s monitorující aplikací. To je nejčastěji realizováno zrcadlením komunikace pomocí opakovače (Obrázek 6) nebo SPAN portu[3] přepínače. Důvod, proč nejsou takto monitorována všechny klientské PC v lokální síti, je nutnost rekonfigurace počítačové sítě pro zřízení zrcadlení provozu na jeden vyhrazený PC s monitorující aplikací. Na tomto PC by navíc vznikalo velké zatížení jak síťového rozhraní, tak monitorující aplikace. Dále by tímto způsobem došlo ke ztrátě informací o přihlášených uživatelích.

[3] Port přepínače, na který je zrcadlen provoz sledovaného zařízení

5.2 Aplikace pro správce

Další částí monitorovacího systému je grafická aplikace pro správce. Tato aplikace je vytvořena v prostředí *C++ Builder* od společnosti Borland. Tato aplikace komunikuje s centrální databází a zobrazuje statistiku shromážděných dat. Spravuje seznam uživatelů a přiřazuje názvy ke sledovaným portům resp. službám. Obrázek 11 znázorňuje hlavní stránku programu.

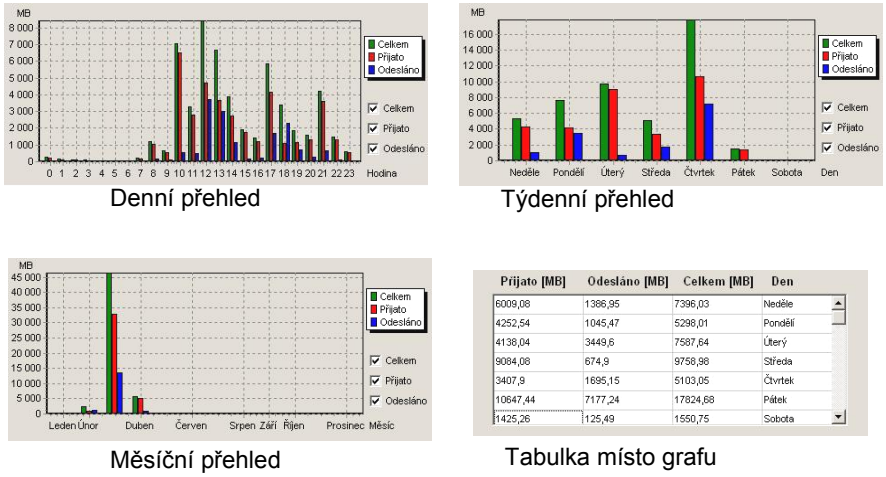


Obrázek 11: Aplikace pro správce s grafickým výstupem

Výstup této aplikace poskytuje přehled o objemu přenesených dat. V základní tabulce lze tento přehled zobrazit bez omezení, tzn. tak jak byly údaje načteny monitorovací aplikací. Také lze tento přehled filtrovat dle jednotlivých parametrů, tedy jednotlivých uživatelů, IP adres klientských PC, času záznamu, data, jednotlivých služeb nebo lokální/externí přenos. Pro zpřehlednění je možné údaje seřadit dle velikosti kliknutím na hlavičce příslušného sloupce tabulky.

Program poskytuje statistické údaje o celkovém počtu přenesených dat ve zvoleném časovém úseku. Dále zjišťuje, kdy bylo přeneseno nejvíce dat za zvolenou časovou jednotku a také průměrný počet dat přenesených za tuto časovou jednotku. Časovou jednotku lze volit ve skupině přepínačů nazvané *Volba přehledu*. Pomocí přepínačů ve skupině *Volba přehledu*

lze zobrazit přehled přenesených dat v průběhu jednotlivých hodin dne přepnutím na volbu *Denní přehled*. Obdobně lze zvolit *Týdenní přehled* a *Měsíční přehled*. Změnou této časové jednotky je kromě statistických údajů ovlivněno také zobrazení průběhu přenesených dat v čase ve formě sloupcového grafu, volitelně ve formě tabulky. Tyto varianty grafického zobrazení průběhu přenesených dat jsou zobrazeny na následujícím obrázku (Obrázek 12).



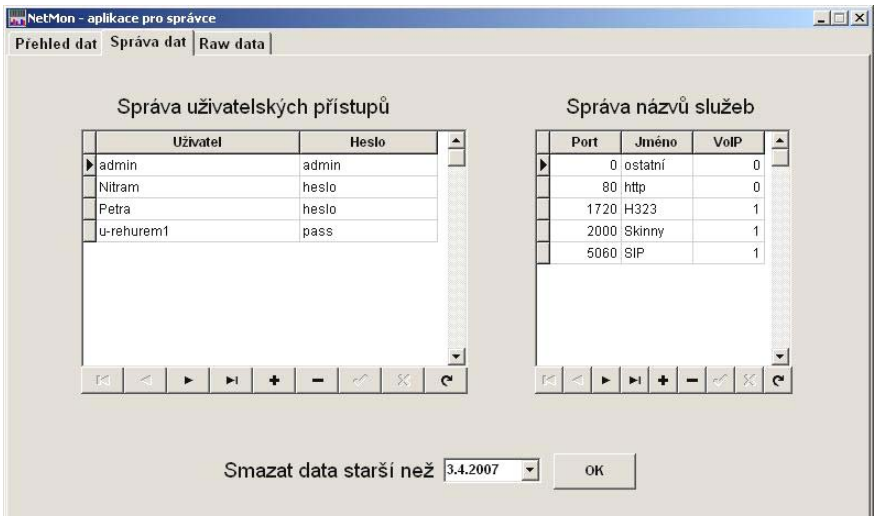
Obrázek 12: Přehled průběhu přenesených dat

Průběh přenesených dat ve sloupcovém grafu lze volitelně zobrazit jako průběh přijímaných dat, odesílaných dat anebo kumulovaně. Průběh přenesených dat lze dále zobrazit bez omezení typu dat, nebo lze zobrazení omezit na data typu *VoIP*, či ostatní datový přenos.

Výsečový graf této aplikace zobrazuje čtyři kategorie přenesených dat. Jsou to data přenesená v rámci lokální počítačové sítě a data přenesená v rámci komunikace s vnější sítí – internetem. Stejné rozdělení platí pro další kategorii, tedy *VoIP* provoz (*VoIP* lokální a externí). Na tomto grafu lze vyčíst procentuální zastoupení *VoIP* v celkovém provozu.

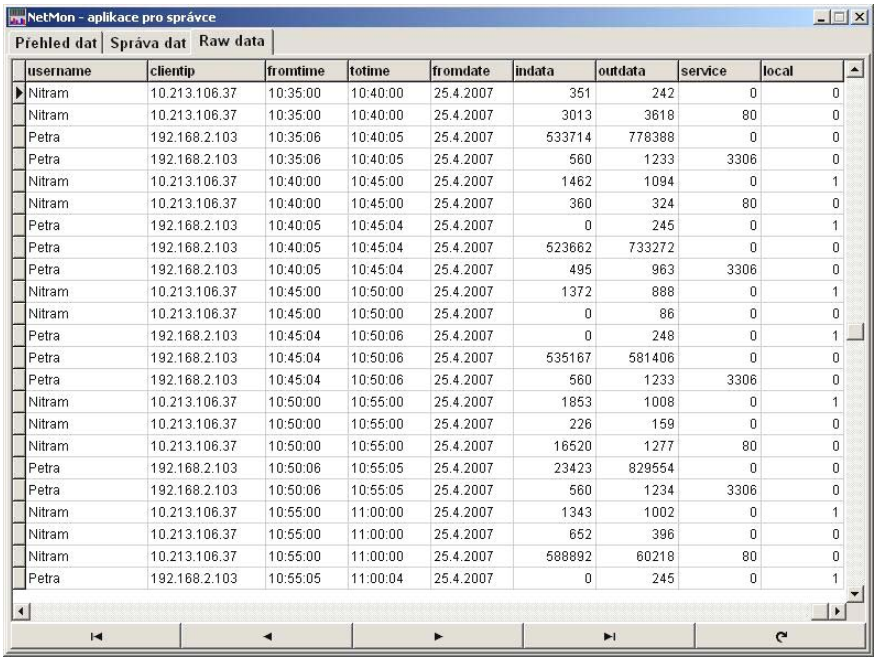
Na záložce *Správa dat* lze přidávat, odebírat a nastavovat hesla uživatelských účtů, které slouží k přihlášení u WEBového přístupu. Dále je možné přiřadit název jednotlivým sledovaným portům, resp. službám. Bude-li monitorující aplikací sledován nějaký port, budou na stránce *Přehled dat* záznamy o datech přenesených na tomto portu zobrazeny pouze, pokud tomuto portu bude přidělen název. Toho lze využít

k odfiltrování záznamů s určitým typem dat. V tabulce *Správa názvů služeb* lze dále definovat, zda se provoz určité služby vyhodnotí jako *VoIP*. Na stránce programu *Správa dat* je dále možné smazat staré a nepotřebné údaje z databáze.



Obrázek 13: Správa dat aplikace pro správce

Na záložce *Raw data* jsou zobrazena nezpracovaná data tak, jak byla přijata monitorující aplikací (Obrázek 14). Toto zobrazení slouží především pro kontrolu a sledování funkcí monitorující aplikace.



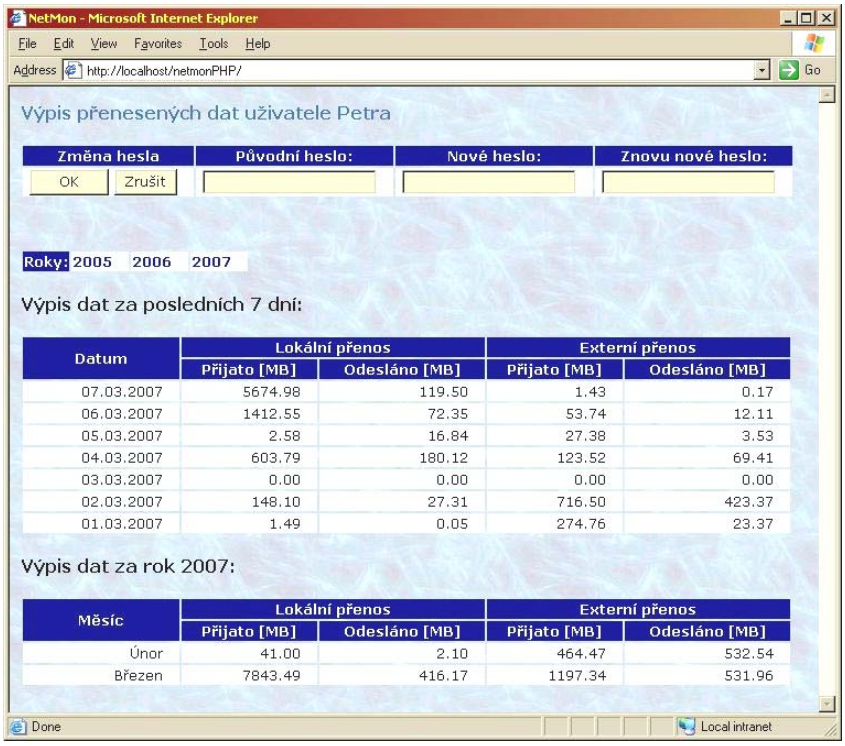
Obrázek 14: Nezpracovaná data z databáze

Umožňuje zobrazení shromážděných dat bez použití filtrů a poskytuje některé další parametry, které nejsou, z důvodu zjednodušení, zobrazeny

v základní tabulce, jako např. sloupec *rowid*. Sloupec *rowid* je identifikační číslo záznamu v databázi a s každým záznamem se navyšuje. Tímto lze zjistit, zda byly některé záznamy odmazány, nebo zapsány dodatečně. Dodatečný zápis do databáze vzniká například z důvodu ztráty spojení monitorující aplikace s databází.

5.3 WEBový přístup pro klienty

Po zadání příslušné adresy v internetovém prohlížeči mají jednotliví uživatelé možnost zobrazení údajů o počtu přenesených dat za posledních 7 dní a jednotlivé měsíce v roce. Před načtením stránky je nutné zadat uživatelské jméno a heslo příslušného uživatele. Pro tento účel musí být nakonfigurovaný WEBový server. Tyto stránky pro uživatelský přístup jsou vytvořeny v jazyce *PHP*. Po zadání uživatelského jména a hesla jsou z databáze vyčteny údaje patřící pouze tomuto uživateli a na jejich základě je vygenerována *HTML* stránka (Obrázek 15).

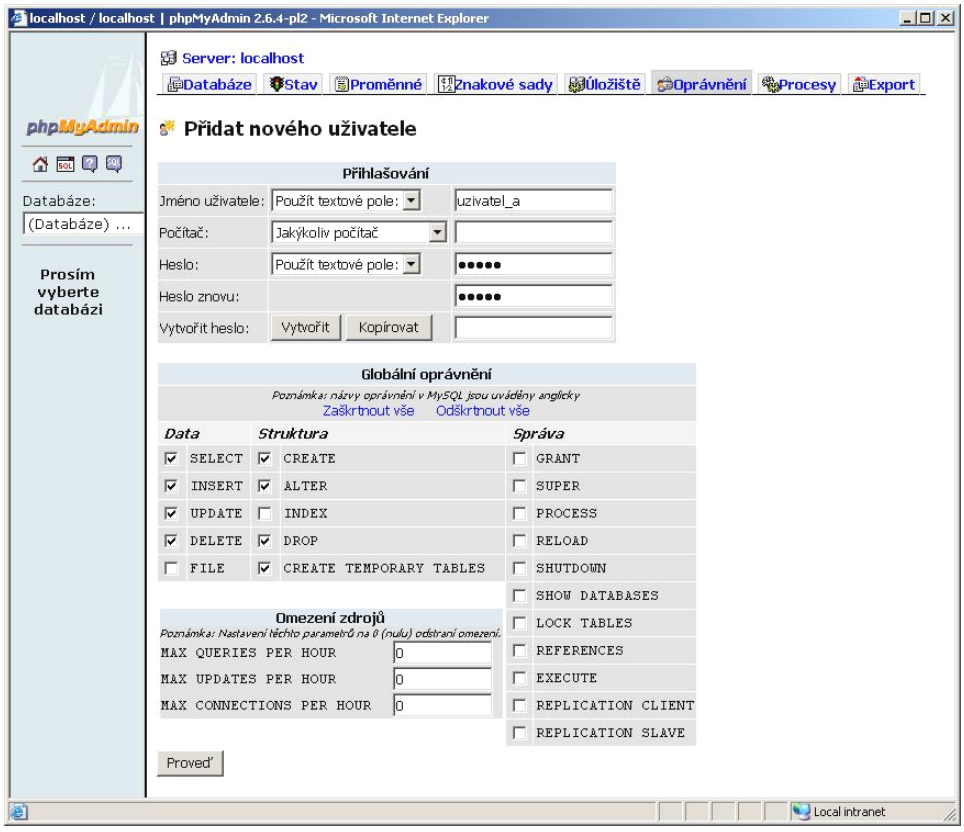


Obrázek 15: WEBový přístup pro klienty

Na stránce WEBového přístupu je dále možné změnit heslo přihlášeného uživatele.

5.4 Databáze

Informace o počtu přenesených dat, seznam uživatelských účtů a pojmenování sledovaných služeb jsou uloženy v *MySQL* databázi. Aplikace pro monitorování provozu a aplikace pro správce komunikuje s databází pomocí *MySQL ODBC* konektoru. *MySQL ODBC* konektor proto musí být nainstalovaný a nakonfigurovaný na každém počítači, na kterém by měla být provozována monitorující aplikace nebo aplikace pro správce. Pro správu databáze, nahlížení na data, či vytvoření uživatelského přístupu k databázi je vhodné použít WEBového správce *phpMyAdmin*. Obrázek 16 zobrazuje příklad vytvoření uživatelského přístupu k databázi v administraci *phpMyAdmin*.



Obrázek 16: Vytvoření přístupu k databázi

WEBovou administraci *phpMyAdmin* je možné stáhnout na internetových stránkách výrobce [15]. Aby administrace *phpMyAdmin* mohla fungovat, musí být umístěna v pracovní složce WEBového serveru podporujícího jazyk *PHP*.

5.5 Instalace

Pro účely instalace monitorovací aplikace a aplikace pro správce byl vytvořen instalační průvodce (instalátor). Tento instalátor byl vytvořen v programu *Inno Setup Compiler*, což je program s licencí freeware, který umožňuje tvorbu instalačních průvodců tvořených jedním exe souborem.

V průběhu instalace monitorovací aplikace a aplikace pro správce je nutné zadat adresu *MySQL* serveru a přihlašovací údaje k databázi, které slouží k vytvoření datového zdroje *MySQL* konektoru. Dále je možné při instalaci zvolit, zda se nainstaluje monitorovací aplikace současně s aplikací pro správce, nebo je možné zvolit instalaci pouze jedné z nich.

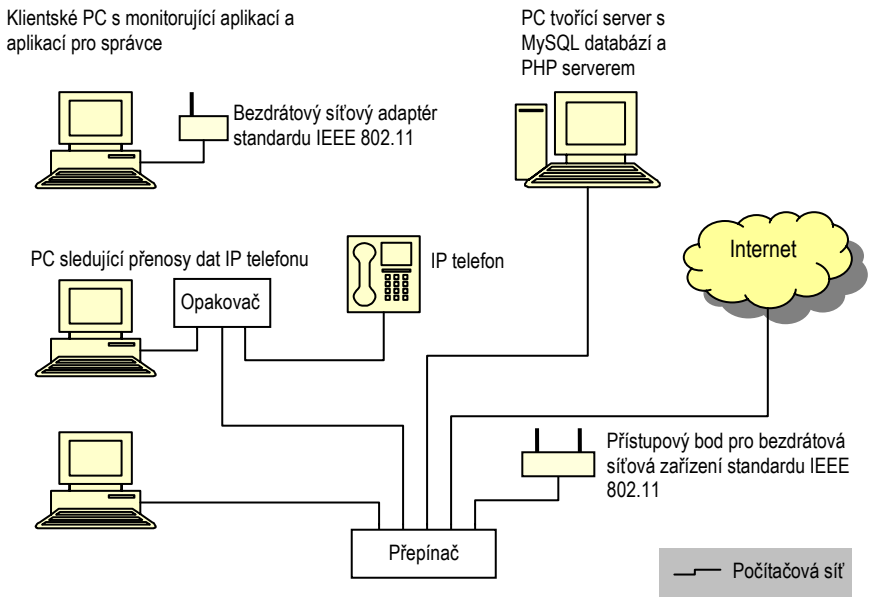
V průběhu instalace je v registrech Windows kontrolována přítomnost *MySQL ODBC* konektoru, který je podmínkou funkčnosti komunikace obou aplikací s *MySQL* databází a v případě, že není nalezen, spustí se jeho instalace.

Při instalaci monitorovací aplikace je v registrech Windows kontrolována přítomnost knihovny *WinPcap*, která je podmínkou funkčnosti monitorování síťového provozu a v případě, že není nalezena, spustí se její instalace.

Při instalaci aplikace pro správce je v registrech Windows kontrolována přítomnost *Borland Database Engine*, což je komponenta nezbytná pro databázové funkce této aplikace a v případě, že není nalezena, spustí se její instalace. Další podrobnosti o instalaci a konfiguraci systému pro sledování síťového provozu *MetMon* jsou uvedeny v příloze A.

6 Realizace modelového pracoviště

Celý monitorovací systém byl nasazen na modelovém pracovišti složeném z několika počítačů. Na jednom z počítačů byl nainstalován databázový server *MySQL 5.0* a vytvořena databáze pro ukládání dat zasílaných z monitorující aplikace. Dále byl na tomto počítači nainstalován WEBový server *Apache 2.0* a podpora jazyka *PHP*. WEBový server s podporou jazyka *PHP* byl využíván pro klientský přístup k databázi a pro administraci databáze *phpMyAdmin*. Na všech použitých počítačích byla nainstalována monitorující aplikace a aplikace pro správce. Obrázek 17 zobrazuje schéma modelového pracoviště.



Obrázek 17: Modelové pracoviště

Toto modelové pracoviště bylo po několik dní vytvořeno v rámci počítačové učebny, kde probíhal běžný provoz (výuka). V tomto prostředí byly použity síťové komponenty s přenosovou rychlostí 100 Mb/s. Bezdrátové síťové prvky standardu IEEE 802.11, použité v rámci modelového pracoviště, podporovaly přenosy dat do rychlosti 22 Mb/s. Monitorovací systém v prostředí modelového pracoviště pracoval bezúdržbově. Pomocí aplikace pro správce bylo možné sledovat výsledky naměřených hodnot. Aplikace pro správce umožňuje sledovat:

- průběh přeneseného množství dat v čase a zjištění přenosové špičky,
- data přenesená u jednotlivých uživatelů,
- úroveň přenesených dat v určitém okamžiku,
- množství přenesených dat v časové ose u sledované služby,
- podíl lokálního přenosu a externího přenosu dat,
- poměr *VoIP* a datového přenosu,
- podílu přijatých a odeslaných dat.

Z výstupních údajů aplikace pro správce bylo možné vyvodit několik závěrů o síťovém provozu na modelovém pracovišti. Bohužel nebylo možné v těchto podmínkách navodit běžné používání technologií *VoIP*. Pomocí pokusů se však bylo možné zjistit, kolik je přeneseno dat při použití jednotlivých typů *VoIP* zařízení, která byla dostupná. Např. byl změřen počet dat přenesených za jednu minutu u oboustranné hlasové komunikace s využitím standardu *H.323* a kodekem *G.711*. Tento přenos byl uskutečněn prostřednictvím aplikace *OpenPhone* a v tomto časovém úseku bylo přenášeno průměrně 138,5 kb/s dat. Dále bylo zjištěno, že během doby vyučování jednoho předmětu (devadesát minut), jeden uživatel přenesl průměrně 90 MB dat, což odpovídá průměrnému přenosu 136,5 kb/s.

Z tohoto měření lze určit, že použití technologií *VoIP* v lokální síti s přenosovou rychlostí 100 Mb/s, resp. 22 Mb/s by nemělo způsobovat znatelné zatížení lokální počítačové sítě. Také *VoIP* komunikace na takovéto síti by neměla být negativně ovlivněna ostatním provozem. Určité snížení kvality hlasových *VoIP* služeb však docházelo u zařízení, které bylo do lokální sítě připojeno pomocí bezdrátového síťového adaptéru. U tohoto zařízení se vyskytovaly výpadky v komunikaci z důvodu velké ztrátovosti paketů způsobené nedostatečnou úrovní signálu. Z tohoto důvodu není použití bezdrátových síťových prvků pro *VoIP* technologie příliš vhodné.

V prostředích, kde není možné garantovat požadovanou kvalitu přenosu dat, jako jsou bezdrátové sítě nebo Internet, je vhodné použít *VoIP* zařízení, které pro přenos hlasu používá minimální šířku přenosového pásma. Např. u oboustranné hlasové komunikace s aplikací *OpenPhone*, u níž byl zvolen hlasový kodek *G.729*, byl naměřen průměrný přenos dat 37,3 kb/s. S tímto kodekem byl naměřen téměř čtyřikrát menší datový tok než u kodeku *G.711*. S použitím kodeku *G.729* se sice mírně snížila poslechová kvalita přenášeného hlasu (oproti kodeku *G.711*), ale také se snížilo riziko pozdržení či zahození paketů přenášených sítí díky snížení požadavku na šířku pásma.

Závěr

Systém pro sledování síťové komunikace vytvořený v rámci této práce splnil očekávání a splňuje všechny body zadání. Díky jednoduché instalaci a snadnému použití je tento systém dobrým nástrojem pro sledování provozu na počítačové síti. Uplatnění tohoto systému lze najít především u správců sítě, kteří chtějí sledovat množství přenesených dat jednotlivých uživatelů nebo služeb. Tímto lze například odhalit uživatele nebo druh činnosti, která zatěžuje počítačovou síť nadměrným přenosem dat. Naopak je také možné tímto systémem odhadnout rezervy počítačové sítě před instalováním nového systému (např. *IP telefonie*).

Příliš velké zatížení počítačové sítě může mít nepříznivý vliv na kvalitu služeb této sítě. Pomocí systému pro sledování provozu lze odhalit, zda k takovýmto přetížením dochází, resp. hrozí jejich vznik vysledováním přenosových špiček. Pokud jsou na počítačové síti odhaleny okamžiky s nadměrným zatížením, lze pomocí aplikace pro správce analyzovat zdroj nebo zdroje zatížení a navrhnout příslušná opatření.

Seznam obrázků

Seznam tabulek

Seznam použité literatury

[1] Kállay, F.; Peniak, P.,*Počítačové sítě a jejich aplikace*, 2. vydání. Praha: GRADA Publishing, 2003. 356 s. ISBN 80-2470-545-1

[2] Svoboda, J. a kol. *Telekomunikační technika - díl 1.* Praha: Nakladatelství Hüthing&Beneš, 1999. 136s.

[3] Dostálek, L.; Kebelová, A. *Velký průvodce protokoly TCP/IP a systémy DNS*. Praha: Computer Press, 2000. 426 s. ISBN 80-7226-323-4

[4] Lorenc, Václav. *Dovolali jste se na číslo 10.0.1.12* . Zpravodaj ÚVT MU. ISSN 1212-0901, 2004, roč. XIV, č. 4, s. 5-9.

[5] Vyleťal, Martin. *Cenové srovnání VoIP* [online]. [cit. 2007-03-05]. Dostupný z WWW: <http://www.lupa.cz/clanky/cenove-srovnani-voip/>

[6] *Praktické informace pro telefonování - IP Telefonie - VoIP Telefonie* [online]. [cit. 2007-04-13]. Dostupný z WWW: <http://www.netspojeni.estranky.cz/clanky/vseobecne-informace/ip-telefonie---voip-telefonie>

[7] Peterka, Jiří. *Způsob digitalizace - PCM nebo něco lepšího?* [online]. [cit. 2006-12-16]. Dostupný z WWW: <http://www.earchiv.cz/a912s200/a912s214.php3>

[8] Peterka, Jiří. *Rodina protokolů TCP/IP verze 2.3 Část 11: VOIP, IP telefonie* [online]. [cit. 2007-2-14]. Dostupný z WWW: <http://www.earchiv.cz/l215/gifs/P11_23.pdf>

[9] Vozňák, Miroslav. *SIP – protokoly, mechanizmy, komunikace* [online]. [cit. 2007-03-23]. Dostupný z WWW: <http://www.cesnet.cz/doc/seminare/20061103/sip-voznak.pdf>

[10] Lasek, Petr. *Technologie TDMoIP* [online]. [cit. 2007-04-10]. Dostupný z WWW: <http://www.stech.cz/articles.asp?ida=170&idk=190>

[12] *WinPcap internals* [online]. [cit. 2007-03-13]. Dostupný z WWW: <http://www.winpcap.org/docs/docs31/html/group__internals.html>

[13] *WinPcap: The Windows Packet Capture Library* [online]. [cit. 2006-12-12]. Dostupný z WWW: < http://www.winpcap.org/install/default.htm >

[14] *OpenH323 Project* [online]. [cit. 2006-12-12]. Dostupný z WWW: < http://www.openh323.org/ >

[15] *EtherealDownload* [online]. [cit. 2007-4-4]. Dostupný z WWW: < http://www.ethereal.com/download.html >

[16] *The phpMyAdmin Project* [online]. [cit. 2007-3-13]. Dostupný z WWW: < http://www.phpmyadmin.net/home_page/index.php >

Příloha A

Uživatelský manuál aplikace NetMon

Požadavky serverové části

- MySQL databáze verze 5.0 pro uchovávání dat
- Apache 2.0 + PHP 5.0.5 pro HTML přístup

Požadavky klientské části

- Knihovna WinPcap 4.0
- MySQL konektor ODBC 3.51 Driver

Celý systém pro sledování a vyhodnocování provozu na počítačové síti se skládá z několika modulů. Jednotlivé moduly obstarávají funkci monitorování provozu, shromažďování dat, vyhodnocování dat a zpřístupnění výsledků statistik.

Moduly aplikace NetMon

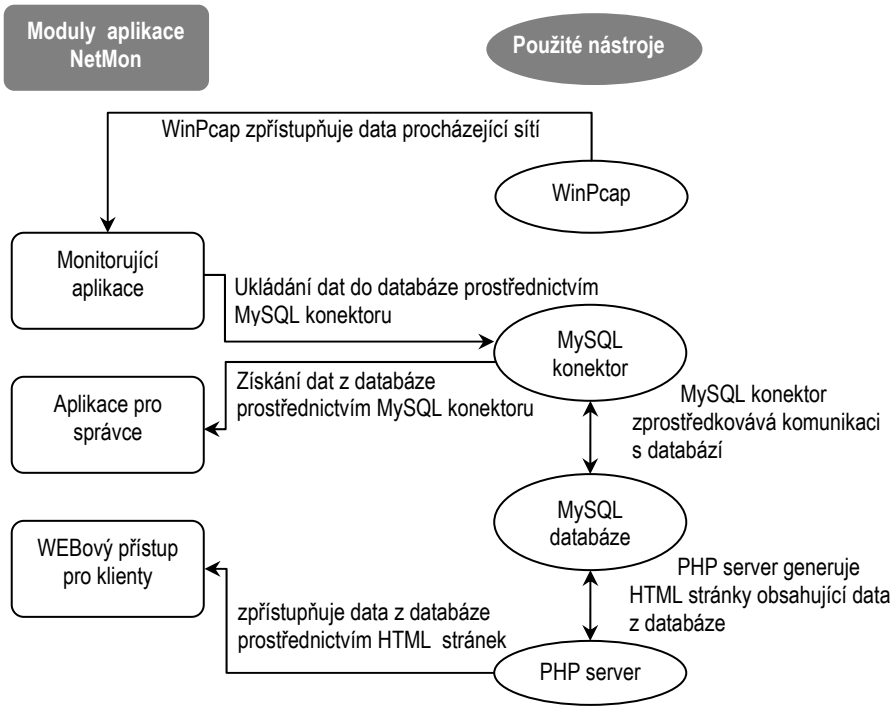
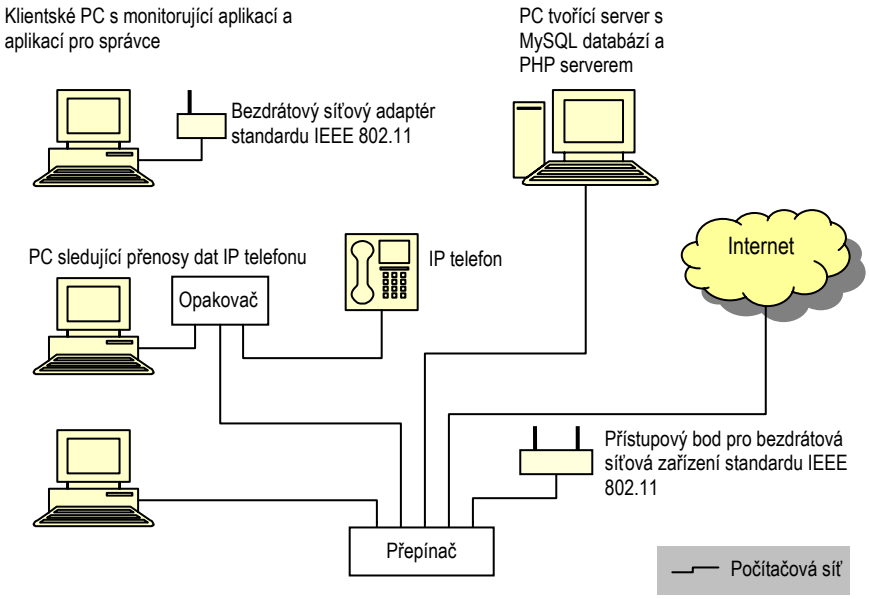


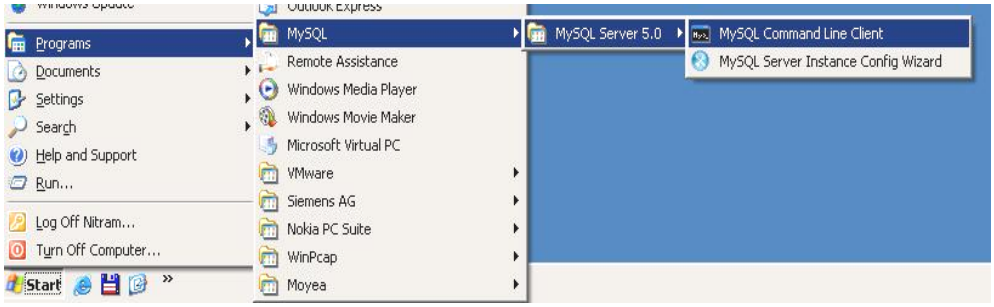
Schéma použití aplikace NetMon



Instalace serverové části

Vytvoření databáze

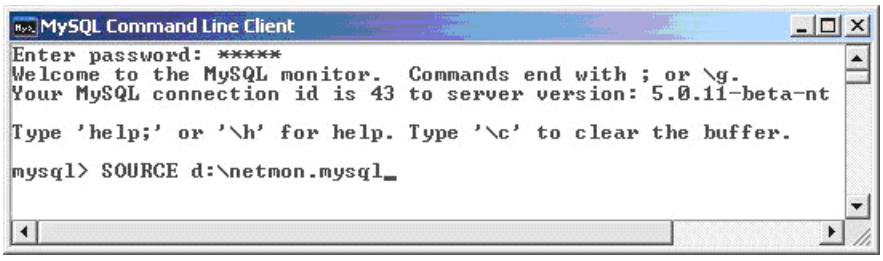
Nabídka: *Start > Programy > MySQL > MySQL Server 5.0 > MySQL Command Line Client*



V příkazovém řádku konzole MySQL serveru zadejte heslo pro přístup k databázi.

Po úspěšném přihlášení zadejte příkaz `SOURCE cesta\netmon.mysql;` pro spuštění skriptu, který vytvoří databázi a databázovou strukturu. Zde `cesta` znamená cestu k souboru `netmon.mysql`, který obsahuje skript pro vytvoření databáze a její struktury.

Soubor se skriptem pro vytvoření databáze `netmon.mysql` je umístěn na instalačním CD v adresáři *NetMon – instalace/MySQL*.



Vytvoření HTML přístupu

Pro vytvoření WEBového přístupu pro uživatele je nutné překopírovat soubory *index.php*, *config.php*, *styly.css* a *pozadi.gif* do pracovní složky nebo podsložky PHP serveru.

PHP skripty pro vytvoření WEBového přístupu jsou umístěny na instalačním CD v adresáři
NetMon – instalace/netmonPHP.

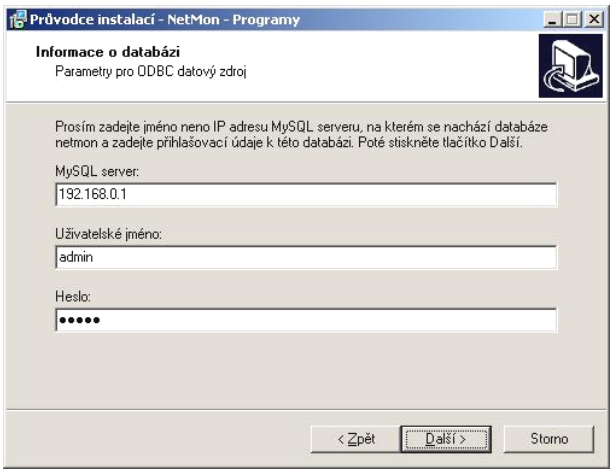
Soubor *config.php* obsahuje text:

```
<?
$spojeni = mysql_connect("localhost", "login", "password");
mysql_select_db("netmon", $spojeni);
?>
```

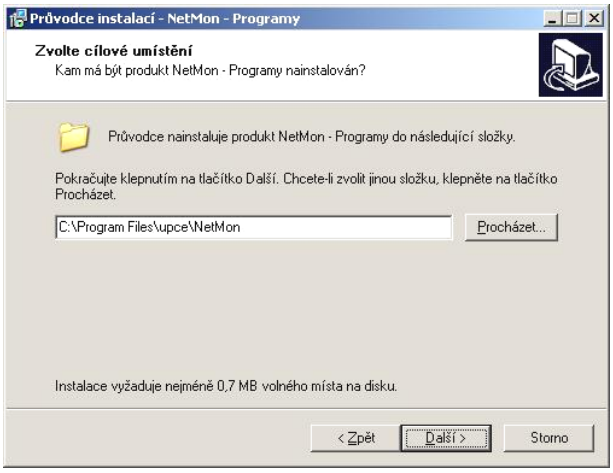
Nahraďte řetězec `login` přihlašovacím jménem uživatele databáze a řetězec `password` heslem tohoto uživatele. Pokud, je PHP server umístěn na jiném PC než MySQL, zadejte místo řetězce `localhost` název MySQL serveru.

Instalace klientské části

Monitorovací aplikaci a aplikaci pro správce je možné nainstalovat pomocí instalačního průvodce (`NetMon - Programy.exe`), kterého lze nalézt na instalačním CD v adresáři *NetMon - instalace.* V průběhu instalace je nutné zadat adresu MySQL serveru a přihlašovací údaje k databázi, které slouží k vytvoření datového zdroje – MySQL konektoru.

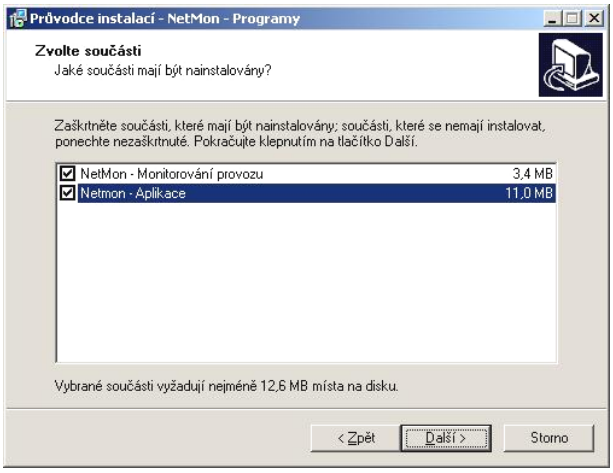


Následuje výběr cílové cesty instalace

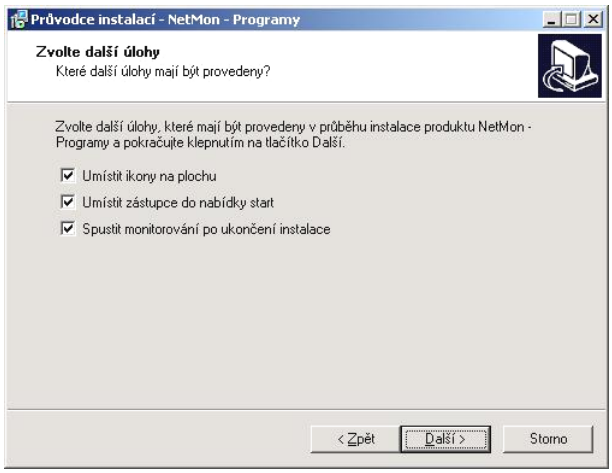


Dále je možné při instalaci vybrat, zda se nainstaluje pouze monitorovací aplikace nebo aplikace pro správce a nebo obě aplikace současně.

Poznámka: monitorující aplikace je spouštěna automaticky po přihlášení uživatele.

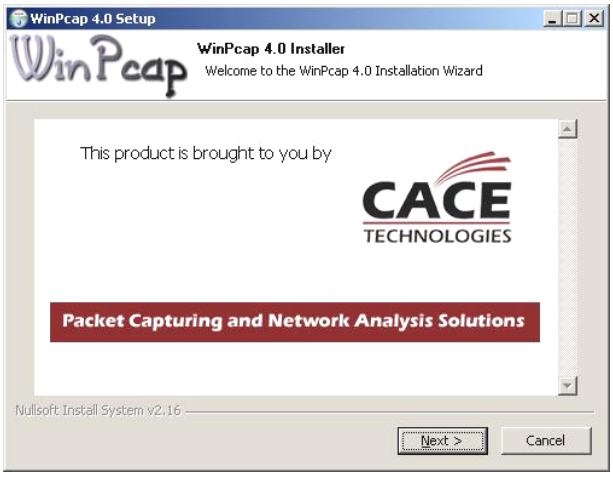


Následují volby, zda se umístí zástupce aplikace na ploše nebo v nabídce Start a zda se má po dokončení instalace spustit monitorující aplikace.



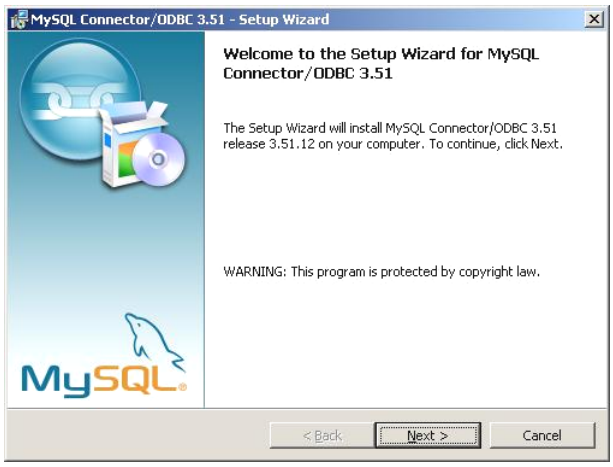
Při instalaci aplikace pro správce, je v registrech Windows kontrolována přítomnost Borland Database Engine, což je komponenta nezbytná pro databázové funkce této aplikace a v případě, že není nalezena, spustí se její instalace.

Při instalaci monitorovací aplikace je v registrech Windows kontrolována přítomnost knihovny WinPcap, která je podmínkou funkčnosti monitorování síťového provozu a pokud není nalezena, spustí se její instalace.



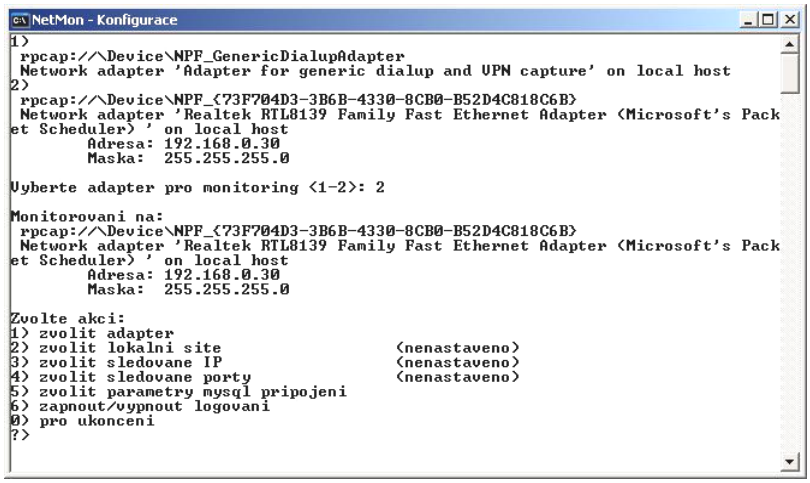
V průběhu instalace je v registrech Windows kontrolována přítomnost MySQL konektoru, který je podmínkou funkčnosti komunikace obou aplikací s MySQL databází a v případě, že není nalezen, spustí se jeho instalace.

Poznámka: komunikace MySQL konektoru s databází je někdy blokována firewallem. Aby k těmto problémům nedocházelo, je nutné příslušně nakonfigurovat firewall počítače.



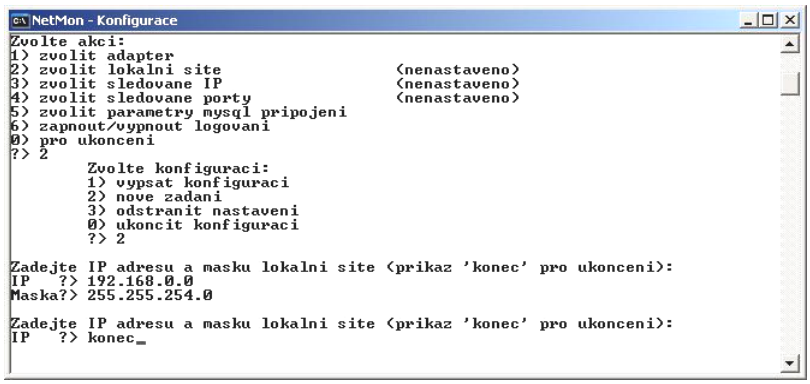
Pokud byla vybrána instalace monitorovací aplikace, následuje spuštění jejího konfiguračního programu. Prvním a povinným bodem konfigurace je výběr síťového adaptéru, který bude monitorován.

Výběr se provede vepsáním příslušného čísla adaptéru uvedeného u jeho názvu a stiskem klávesy Enter.



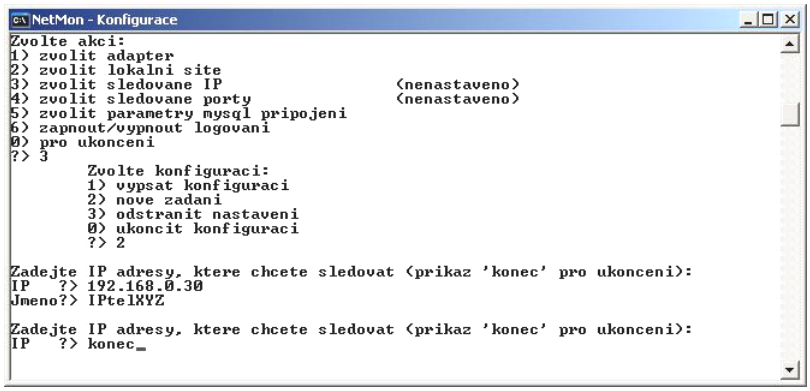
Druhý nepovinný bod konfigurace je zvolení seznamu lokálních sítí - IP adresy a masky sítí, u kterých se bude komunikace vyhodnocovat jako lokální. Tato konfigurace se zvolí zadáním číslem 2 v hlavním menu a stiskem klávesy Enter. Zadávání nových údajů se zvolí číslem 2 a potvrdí klávesou Enter. Následuje dotazování na IP adresu sítě a masku sítě. Zadávání se ukončí vepsáním příkazu „konec“ a potvrzením klávesou Enter. Další volby této konfigurace jsou zadáním:

1 – výpis stávající konfigurace na obrazovku,
3 – úplné odstranění konfigurace lokálních sítí,
0 – ukončení konfigurace lokálních sítí.



Třetí nepovinný bod konfigurace slouží k nastavení promiskuitního sledování více zařízení, kde hodnota Jméno je v administrátorské aplikaci zobrazena ve sloupci Uživatel. Tato konfigurace se zvolí zadáním čísla 3 v hlavním menu a stiskem klávesy Enter. Zadávání nových údajů se zvolí číslem 2 a potvrdí klávesou Enter. Následuje dotazování na IP adresu sledovaného zařízení a název zařízení. Zadávání se ukončí vepsáním příkazu „konec“ a potvrzením klávesou Enter. Další volby této konfigurace jsou zadáním:

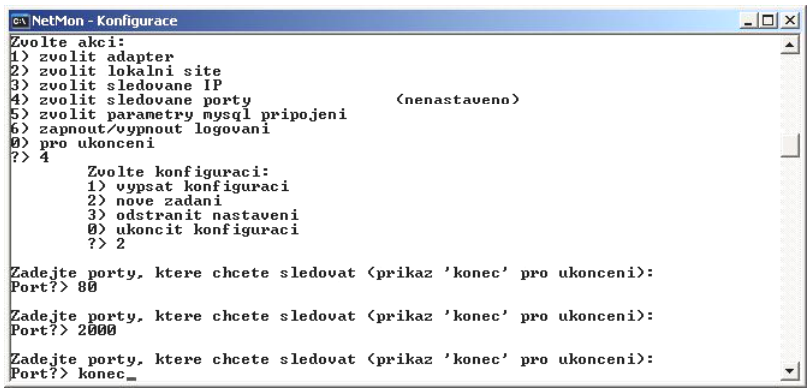
1 – výpis stávající konfigurace na obrazovku,
3 – úplné odstranění konfigurace sledovaných zařízení,
0 – ukončení konfigurace.



Čtvrtý nepovinný bod konfigurace je nastavení portů, které se mají sledovat. Tato konfigurace se zvolí zadáním číslem 4 v hlavním menu a stiskem klávesy Enter. Zadávání nových údajů se zvolí číslem 2 a potvrdí klávesou Enter. Následuje dotazování na čísla sledovaných portů. Zadávání se ukončí vepsáním příkazu „konec“ a potvrzením klávesou Enter. Další volby této konfigurace jsou zadáním:

1 – výpis stávající konfigurace na obrazovku,
3 – úplné odstranění konfigurace sledovaných portů,
0 – ukončení konfigurace sledovaných portů.

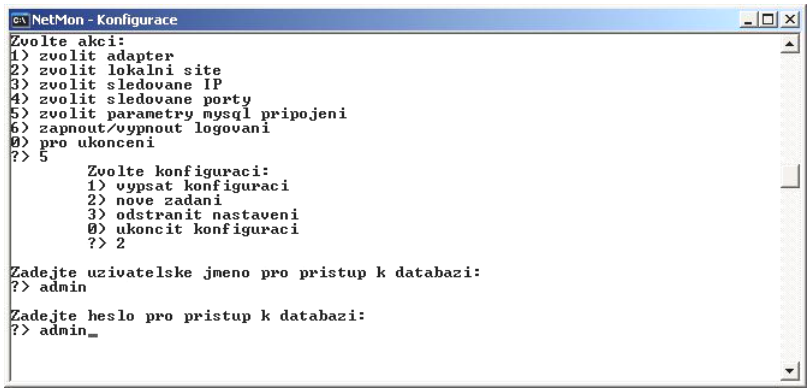
Příklad některých portů: 80 – http, 1720 – H323, 2000 – Skinny, 5060 – SIP.



Pátým bodem konfigurace je nastavení parametrů přihlášení k databázi. Tato konfigurace je provedena automaticky při instalaci a není třeba ji měnit.

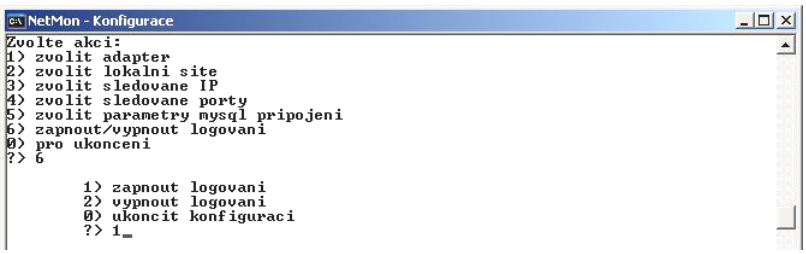
Tato konfigurace se zvolí zadáním čísla 5 v hlavním menu a stiskem klávesy Enter. Následuje dotaz na zadání uživatelského jména pro přístup k databázi a hesla pro přístup k databázi. Další volby této konfigurace jsou zadáním:

1 – výpis stávající konfigurace na obrazovku,
3 – úplné odstranění konfigurace (budou použity přednastavené hodnoty admin / admin),
0 – ukončení konfigurace.



Šestým bodem konfigurace lze zapnout nebo vypnout logování akcí monitorovací aplikace do souboru *netmon.log* umístěného ve složce *log* v místě, kam byla aplikace nainstalována. Po restartu aplikace se předchozí *netmon.log* soubor přejmenuje na *netmon.bak* a vznikne nový soubor *netmon.log*.

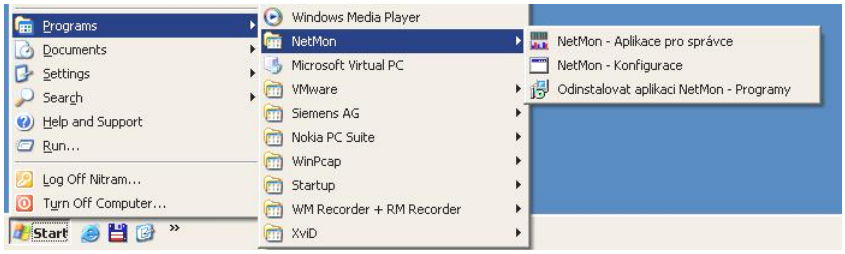
Tato konfigurace se zvolí zadáním číslem 6 v hlavním menu a stiskem klávesy Enter. Zadáním čísla 1 se logování zapne, zadáním čísla 2 se logování vypne. Další volby této konfigurace jsou: 0 – ukončení konfigurace.



Změny konfigurace se projeví po restartu monitorující aplikace.

Obsluha aplikací – klientská část

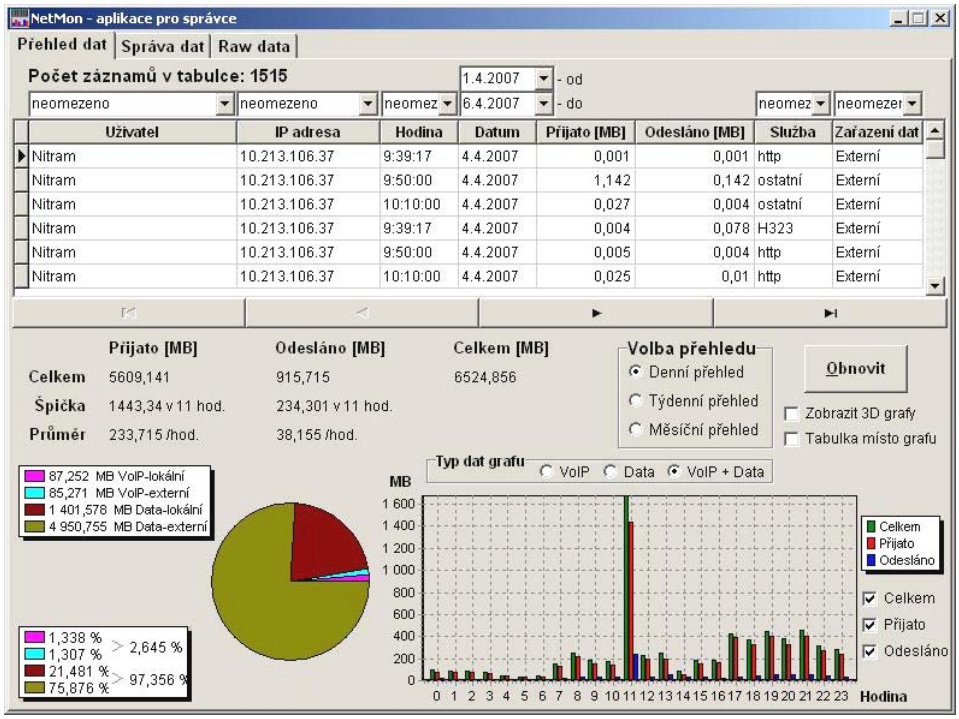
Zástupci aplikace jsou dle voleb instalace na ploše nebo v nabídce *Start* > *Programy* > *NetMon*. V nabídce Start jsou nainstalováni zástupci pro odinstalaci, konfiguraci monitorovací aplikace a zástupce administrátorské aplikace.



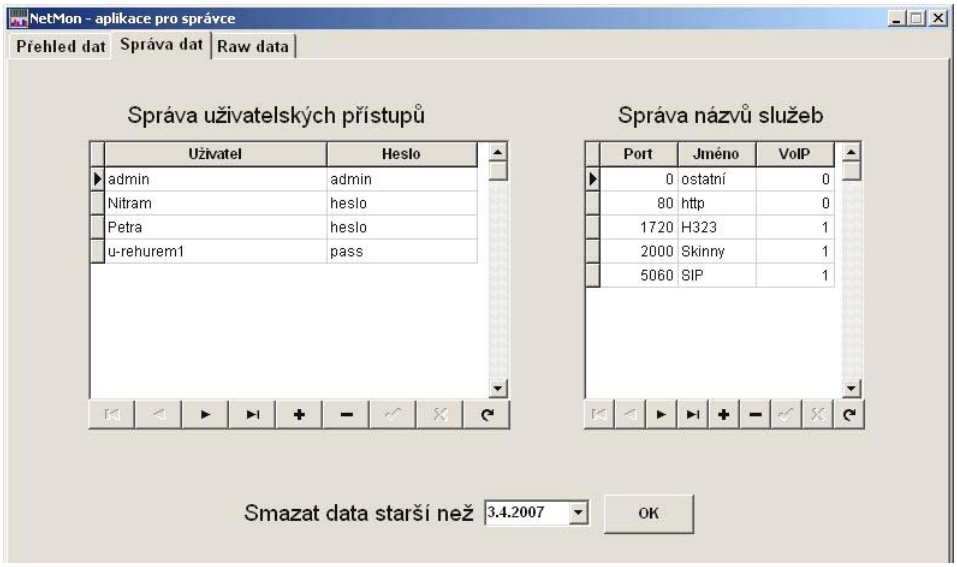
Administrátorská aplikace

Po spuštění zástupce *NetMon – Aplikace pro správce* se spustí administrátorská aplikace. Pro přístup k databázi je nutné zadat přihlašovací údaje k databázi.

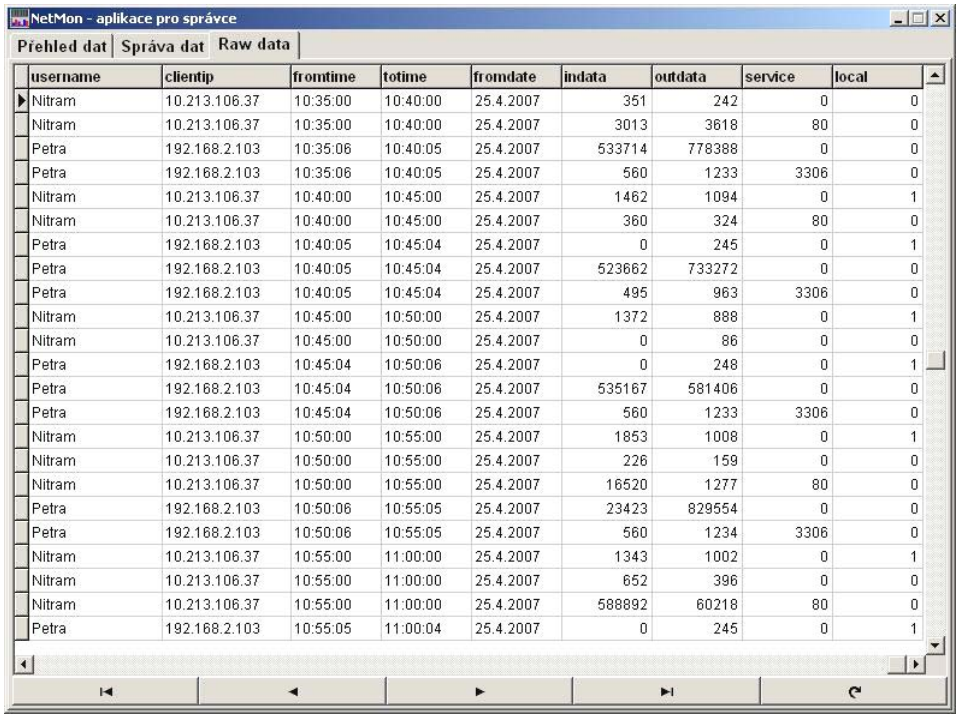
Na záložce **Přehled dat** tato aplikace zobrazuje statistiku shromážděných dat. Data lze zobrazovat v grafickém přehledu za jednotku času – 24 hodin, dny v týdnu, měsíce roku dle nastavení přepínače *Volba přehledu*. Data lze filtrovat dle jednotlivých klientských PC, jednotlivých uživatelů, jednotlivých služeb nebo lokální/externí přenos s určením podílu VoIP provozu.



Na záložce **Správa dat** lze spravovat (přidávat, odebírat a nastavovat hesla) uživatelských účtů, které slouží k přihlášení u WEBového přístupu. Dále je zde možné odstranit data z databáze od zvoleného data.



Záložka **Raw data** obsahuje tabulku „surových“ nezpracovaných dat tak, jak byla přijata monitorující aplikací.

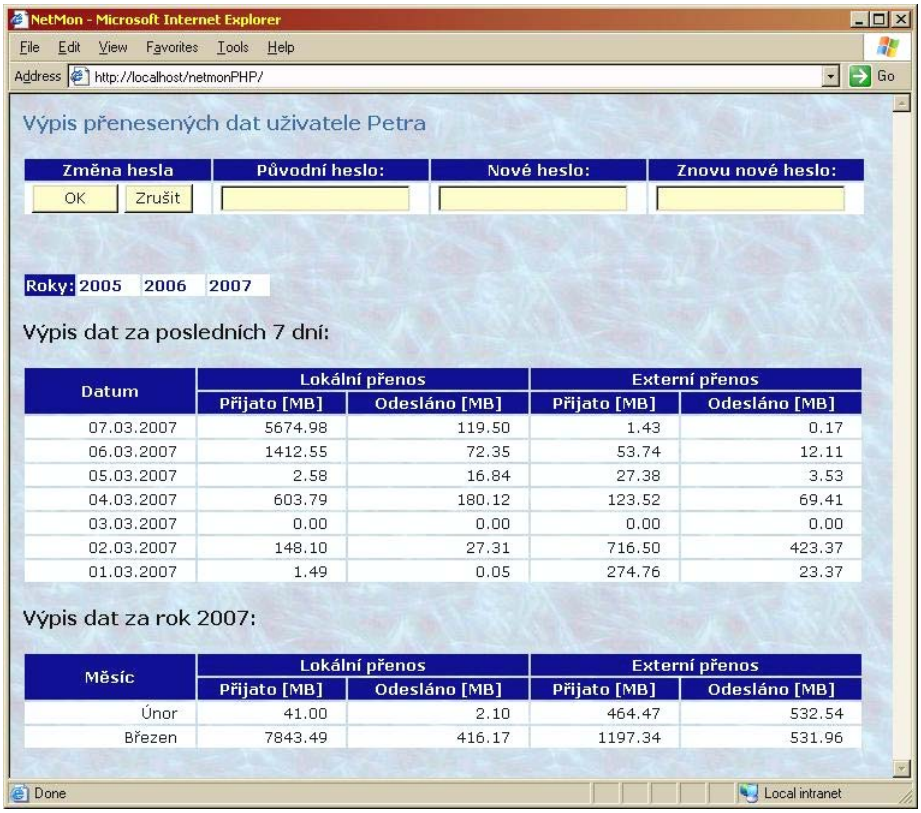


username	clientip	fromtime	totime	fromdate	indata	outdata	service	local
Nitram	10.213.106.37	10:35:00	10:40:00	25.4.2007	351	242	0	0
Nitram	10.213.106.37	10:35:00	10:40:00	25.4.2007	3013	3618	80	0
Petra	192.168.2.103	10:35:06	10:40:05	25.4.2007	533714	778388	0	0
Petra	192.168.2.103	10:35:06	10:40:05	25.4.2007	560	1233	3306	0
Nitram	10.213.106.37	10:40:00	10:45:00	25.4.2007	1462	1094	0	1
Nitram	10.213.106.37	10:40:00	10:45:00	25.4.2007	360	324	80	0
Petra	192.168.2.103	10:40:05	10:45:04	25.4.2007	0	245	0	1
Petra	192.168.2.103	10:40:05	10:45:04	25.4.2007	523662	733272	0	0
Petra	192.168.2.103	10:40:05	10:45:04	25.4.2007	495	963	3306	0
Nitram	10.213.106.37	10:45:00	10:50:00	25.4.2007	1372	888	0	1
Nitram	10.213.106.37	10:45:00	10:50:00	25.4.2007	0	86	0	0
Petra	192.168.2.103	10:45:04	10:50:06	25.4.2007	0	248	0	1
Petra	192.168.2.103	10:45:04	10:50:06	25.4.2007	535167	581406	0	0
Petra	192.168.2.103	10:45:04	10:50:06	25.4.2007	560	1233	3306	0
Nitram	10.213.106.37	10:50:00	10:55:00	25.4.2007	1853	1008	0	1
Nitram	10.213.106.37	10:50:00	10:55:00	25.4.2007	226	159	0	0
Nitram	10.213.106.37	10:50:00	10:55:00	25.4.2007	16520	1277	80	0
Petra	192.168.2.103	10:50:06	10:55:05	25.4.2007	23423	829554	0	0
Petra	192.168.2.103	10:50:06	10:55:05	25.4.2007	560	1234	3306	0
Nitram	10.213.106.37	10:55:00	11:00:00	25.4.2007	1343	1002	0	1
Nitram	10.213.106.37	10:55:00	11:00:00	25.4.2007	652	396	0	0
Nitram	10.213.106.37	10:55:00	11:00:00	25.4.2007	588892	60218	80	0
Petra	192.168.2.103	10:55:05	11:00:04	25.4.2007	0	245	0	1

Obsluha aplikací – serverová část

WEBový přístup pro klienty

Po zadání příslušné adresy, v internetovém prohlížeči, mají jednotliví uživatelé možnost zobrazení údajů o počtu přenesených dat za posledních 7 dní a jednotlivé měsíce v roce.



ÚDAJE PRO KNIHOVNICKOU DATABÁZI

Název práce	SYSTÉM PRO SLEDOVÁNÍ DATOVÉHO A VOIP PROVOZU NA LOKÁLNÍCH SÍTÍCH
Autor práce	Martin Řehůřek
Obor	Informační technologie
Rok obhajoby	2007
Vedoucí práce	Ing. Martin Dobrovolný
Anotace	Tato práce se zabývá problematikou sledování množství přenesených dat na počítačové síti s rozlišením datového a hlasového provozu. Je zde navržen a popsán systém, který kromě sledování provozu bude tyto údaje shromažďovat v databázi a umožní grafický výstup v podobě grafu a dalších údajů.
Klíčová slova	VoIP, IP telefonie, monitoring