Kerio Network Monitor 2™

Uživatelský manuál

Kerio Technologies

Datum vydání: 10. dubna 2003

Aktuální verze produktu: *Kerio Network Monitor 2.1.0*. Změny vyhrazeny.

Obsah

Kapitola 1

Úvod

Kerio Network Monitor je malý, leč výkonný nástroj k online sledování síťového provozu. Nabízí celou řadu možností, jaké aktivity a události lze sledovat.

Grafický průběh zatížení linky Online průběh zatížení internetového připojení (příchozí i odchozí provoz) v časovém rozmezí 1 minuta až 1 rok. Zobrazovány jsou průměrné rychlosti za 3 sekundy (graf pro 1 minutu) až 3 dny (graf pro 1 rok). V grafu lze současně zobrazit celkový provoz i provoz za jednotlivé uživatele (počítače v síti). Tímto způsobem lze rychle zjistit, který počítač nejvíce zatěžuje internetové připojení.

Standardně je zobrazován provoz za všechny služby (např. WWW, FTP, Telnet atd.), kromě toho lze také zobrazovat pouze jednotlivé služby (předdefinované nebo vlastní — zadané protokolem a číslem portu) a sledovat tak jejich provoz odděleně. Provoz je zobrazován za jednotlivé IP adresy, které lze převést na jména počítačů (získaná z DNS nebo zadaná ručně).

Celkový objem dat za určité období Z naměřených dat můžete zjistit, kdo z vaší sítě nejintenzivněji využívá Internet. Lze vytvořit statistiku po dnech, týdnech nebo měsících (např. za poslední 2 měsíce po jednotlivých týdnech za všechny nebo jen vybrané počítače).

Zobrazení a záznam aktivních spojení Ve speciálním okně je možno sledovat (téměř) v reálném čase, jaká spojení mají jednotlivé stanice navázána. Historie těchto spojení se ukládá do záznamu (*Connection Log*).

Strom zachycených dat *Kerio Network Monitor* umí detailně zaznamenávat data určitých protokolů (např. SMTP, POP3, IMAP, HTTP atd.). Tato data se zobrazují ve tvaru přehledného stromu, kde jsou řazena buď podle stanic (IP adres) nebo podle protokolů. Volitelně je možno zaznamenávat i obsah posílaných e-mailů a navštívených WWW stránek (nejsou-li přenášeny šifrovanými protokoly).

Záznam navštívených WWW stránek Okno *HTTP Log* zaznamenává veškeré zachycené HTTP požadavky. Výběrem počítače ze seznamu se v záznamu barevně odliší požadavky generované právě touto stanicí.

Záznam o e-mailech Okno *Mail Log* zaznamenává informace o veškerých e-mailových zprávách, a to jak odesílaných protokolem SMTP, tak i stahovaných POP3 nebo IMAP

(pokud nebyly přenášeny šifrovaným spojením). Zaznamenávají se adresy odesílatele a příjemce a velikost posílané zprávy.

Záznam ICQ komunikace V okně *ICQ Log* se zobrazují informace o komunikaci protokoly *ICQ* a *ICQ2Go*. Zaznamenává se ICQ číslo a přezdívka (nickname) odesílatele a příjemce zprávy a vlastní obsah zprávy.

Vzdálený přístup *Kerio Network Monitor* má oddělenou sledovací službu (*Daemon*) a uživatelské rozhraní. Tyto dvě komponenty spolu komunikují pomocí TCP/IP. Z toho vyplývá, že veškeré sledování a konfiguraci je možno provádět nejen lokálně, ale i vzdáleně — z libovolného jiného počítače.

WWW přístup *Kerio Network Monitor* obsahuje zabudovaný WWW server, který umožňuje prohlížení a vyhodnocování dat pomocí běžného WWW prohlížeče. K dispozici je většina funkcí, které jsou obsaženy v uživatelském rozhraní (s výjimkou konfigurace programu).

Uživatelské účty Při připojování ke službě je vyžadováno uživatelské jméno a heslo. Ke *Kerio Network Monitoru* se tak může nezávisle připojovat více uživatelů s různou úrovní přístupových práv (prohlížení, konfigurace, správa uživatelských účtů...).

Export dat Data vytvořená *Kerio Network Monitorem* je možno dále zpracovávat: graf lze uložit jako obrázek, statistiku za určité období uložit do formátu CSV (lze zpracovat např. programem Microsoft Excel), záznamy zpracovávat externím analyzátorem (např. *Kerio Log Analyzer*).

Jak můžete Kerio Network Monitor *využít?*

- chcete mít přehled, jak jednotlivé počítače ve vaší firmě zatěžují linku do Internetu
- potřebujete podklady pro rozúčtování nákladů na internetové připojení na jednotlivé uživatele (počítače)
- požadujete kontrolu, jak vaši zaměstanci brouzdají po Internetu
- zajímá vás, jaké WWW stránky navštěvují, jaké soubory stahují, komu posílají e-maily...
- hledání a řešení problémů — *Kerio Network Monitor* Vám dává mnoho informací o historii komunikace ve vaší síti.

Kapitola 2

Rychlé nastavení

Tato kapitola uvádí stručný návod, jak rychle nastavit základní parametry programu *Kerio Network Monitor*, aby mohl být okamžitě používán. V případě nejasností v některém kroku si prostudujte kapitolu zabývající se příslušnou problematikou.

1. Vyberte vhodný počítač ve vaší síti a nainstalujte na něj obě komponenty programu *Kerio Network Monitor* (viz kapitoly 4 a 3.3).

2. Přihlašte se do prohlížecího programu (viz kapitola 5.1) a vyberte adaptéry, na nichž budou pakety sledovány (viz kapitola 5.3).

3. V menu *Action / Change password* nastavte heslo pro uživatele `Admin`.

4. Nepoužívají-li se v lokální síti privátní IP adresy, nastavte příslušné rozsahy IP adres v menu *Settings / Configuration*, záložka *IP addresses* (viz kapitola 6.1).

5. Je-li lokální síť připojena k Internetu pomocí proxy serveru, zkontrolujte a případně upravte nastavení pro proxy server v menu *Settings / Configuration*, záložka *IP addresses* (viz kapitola 6.1).

6. Běží-li v lokální síti či na internetové bráně poštovní server, rozhodněte, jakým způsobem má být měřen objem přenesené pošty, a proveďte příslušná nastavení v menu *Settings / Configuration*, záložka *IP addresses* (viz kapitoly 3.3 a 6.1).

Kapitola 3

Technické informace

3.1 Komponenty *Kerio Network Monitoru*

Kerio Network Monitor sestává ze dvou oddělených komponent:

Sledovací služba (*Daemon*) Výkonné jádro programu, které zachytává pakety a zaznamenává data do souborů na disku. Běží jako služba (ve Windows NT/2000/XP) nebo jako aplikace na pozadí (ve Windows 9x/Me).

Prohlížecí program Slouží k prohlížení a analýze shromážděných dat a konfiguraci služby. Komunikace mezi prohlížecím programem a *Daemonem* probíhá protokoly standardu TCP/IP — díky tomu je možno se připojit nejen lokálně (z téhož počítače), ale i z libovolného jiného počítače v lokální síti, resp. v Internetu. Detaily naleznete v kapitole 5.1.

3.2 Jak *Kerio Network Monitor* pracuje?

Sledování paketů

Kerio Network Monitor Daemon sleduje provoz na síti v tzv. promiskuitním režimu (tzn. dokáže přijímat i data, která nejsou adresována počítači, na němž běží). Zachytává veškeré pakety protokolu IP, z nichž získává požadované informace:

Objem přenesených dat V každém zachyceném IP paketu se provede kontrola zdrojové a cílové adresy. Jestliže jedna z těchto adres patří do lokální sítě a druhá do Internetu (jedná se tedy o přenos dat mezi lokální sítí a Internetem), změří se velikost datové části transportního protokolu (TCP nebo UDP) a tento údaj se zaznamená. Patří-li obě adresy do lokální sítě nebo obě do Internetu, objem dat se nezaznamenává.

Které IP adresy patří do lokální sítě a které do Internetu je dáno konfigurací programu — viz kapitola 6.1.

Poznámka: Různé nástroje pro monitorování sítě používají různí metody měření objemu přenesených dat (např. celé ethernetové rámce, objem dat v IP paketech včetně

hlaviček apod.). Údaje získané programem *Kerio Network Monitor* se proto mohou lišit od údajů získaných jinými nástroji (odchylka by však neměla přesáhnout cca 40% — jedná-li se např. o několikanásobný rozdíl, je třeba hledat chybu v síti či konfiguraci programu).

Sledování aktivních spojení Ve všech zachycených IP paketech jsou hledány TCP segmenty navazující a ukončující spojení (s příznaky *SYN* a *FIN*). *Kerio Network Monitor* tak má informaci o všech aktivních spojeních jednotlivých stanic v síti. Obdobným způsobem se zobrazuje komunikace protokolem UDP. Protože se však jedná o nespojovaný protokol, vyhodnocují se tzv. pseudospojení — spojení trvá, dokud interval výměny UDP datagramů mezi zdrojovou a cílovou stanicí nepřesáhne stanovený čas (standardně 180 sekund).

Sledování služeb Každý zachycený IP paket je zkontrolován, zda neobsahuje data některé z definovaných služeb (viz kapitola 6.2). Pokud ano, jsou tato data zaznamenána.

Jako příklad uveďme přenos pošty protokolem SMTP. Je-li zaznamenáno navázání TCP spojení s cílovým portem `25`, začnou se sledovat všechny pakety patřící do tohoto spojení a z nich pak může být zjištěna e-mailová adresa odesílatele a příjemce zprávy, případně zrekonstruován obsah celé zprávy.

Konfigurační soubor

Všechny konfigurační informace programu *Kerio Network Monitor* jsou uloženy v konfiguračním souboru `NetMon2.cfg`. Tento soubor je uložen v adresáři, kde je *Kerio Network Monitor* nainstalován (typicky `C:\Program Files\Kerio\Network Monitor`). Chcete-li zálohovat nastavení, stačí zkopírovat tento soubor.

Upozornění: Před jakoukoliv manipulací s konfiguračním souborem je třeba zastavit *Kerio Network Monitor Daemon* (viz kapitola 5.2)!

Ukládání dat

Naměřená data jsou ukládána do binárních souborů na disku. V datovém adresáři (standardně tentýž adresář, kde je *Kerio Network Monitor* instalován) jsou vytvořeny následující podadresáře:

- `high` — data s vysokým rozlišením (vzorkování po 3 sekundách)
- `low` — data s nízkým rozlišením (vzorkování po 1 hodině)

V těchto adresářích se vytvářejí další podadresáře dle IP adres jednotlivých počítačů v lokální síti a v nich pak soubory s naměřenými daty (data s vysokým rozlišením — jeden soubor denně, data s nízkým rozlišením — jeden soubor každých 28 dnů).

Dále se zde vytvářejí podadresáře:

- `browse` — informace o zachycených objektech sledovaných služeb (URL stránek, e-mailové adresy, FTP relace atd.)
- `captured` — zachycené objekty (např. zachycené WWW stránky, e-mailové zprávy apod.)
- `logs` — soubory se záznamy (viz kapitola 7.7)
- `debug` — data ukládaná při detailním sledování určité služby (viz kapitola 6.2)

Adresářová struktura pro ukládání dat je poměrně flexibilní, neboť umožňuje např.:

- sloučení dat s jinými daty (jedná-li se o dvě různá, navzájem se nepřekrývající období)
- vymazání záznamů pro určitý počítač (IP adresu)
- vymazání dat určité služby (např. WWW).

Před prováděním operací tohoto typu je třeba zastavit *Kerio Network Monitor Daemon* (viz kapitola 5.2).

Změna adresáře pro uložení dat

Potřebujete-li změnit adresář pro ukládání naměřených a zachycených dat a záznamových souborů (aby se např. data ukládala na jiný disk), je možné to provést úpravou příslušného parametru v konfiguračním souboru.

Nejprve je nutno zastavit službu *Network Monitor Daemon* (viz kapitola 5.2). Pak otevřete v libovolném editoru (např. *Notepad*) konfigurační soubor `NetMon2.cfg` (viz sekce *Konfigurační soubor*). Adresář pro data je uveden v parametru `main_dir`. Z technických důvodů musejí být při zápisu cesty zdvojována zpětná lomítka — cesta do zvoleného datového adresáře může tedy vypadat např. takto:

```
main_dir = "d:\\netmon_data"
```

Změnu datového adresáře je nejvhodnější provést ihned po instalaci programu *Kerio Network Monitor*, kdy ještě nejsou naměřena žádná data. Provádíte-li změnu až po určité době používání programu, je nutné do nového umístění zkopírovat (resp. přesunout) adresáře s naměřenými daty a záznamy, tj. `browse`, `captured`, `debug`, `high`, `logs`, `low` a `www`.

Upozornění: Podadresář `license` musí zůstat ve stejném adresáři jako programové soubory (tj. kam byl *Kerio Network Monitor* původně instalován)!

Po změně adresáře a případném zkopírování naměřených dat můžete opět spustit *Network Monitor Daemon*.

3.3 Technická omezení

Z principu, jakým *Kerio Network Monitor* pracuje, vyplývají některá drobná omezení. Ta je třeba mít na paměti zejména při výběru počítače, na který bude *Kerio Network Monitor* nainstalován.

Síťové prvky a topologie sítě

Obsahuje-li vaše síť switch (switching hub), myslete na to, že neposílá všechna data na všechny své porty! *Kerio Network Monitor* však potřebuje, aby se tato data vyskytovala v segmentu, do něhož je „jeho“ počítač připojen.

Možností řešení je několik:

- nainstalovat *Kerio Network Monitor* přímo na počítač, který je připojen k Internetu. Toto řešení je doporučeno vždy, pokud na internetové bráně běží operační systém typu Windows. (*Kerio Network Monitor* pak musí být nastaven pro sledování na „vnitřních“ síťových kartách — viz kapitola 6.1).
- některé typy switchů lze nakonfigurovat tak, aby na jeden (tzv. monitorovací) port posílal všechna data. K tomuto portu pak může být připojena stanice, na níž *Kerio Network Monitor Daemon* běží.
- připojit mezi switch a internetovou bránu malý hub (stačí 3 zásuvky — jedna na switch, druhá na bránu do Internetu a třetí k počítači, kde běží *Kerio Network Monitor Daemon*).

Je-li síť rozdělena směrovačem na více IP segmentů, musí být *Kerio Network Monitor Daemon* instalován na počítači v segmentu, kde je připojena internetová brána.

Má-li síť více segmentů, z nichž každý je připojen přímo k internetové bráně, musí být *Kerio Network Monitor* nainstalován přímo na tuto bránu. V opačném případě bude měřit data pouze v segmentu, do kterého je připojen.

Pošta

Přirozený požadavek správce sítě je sledovat také objem dat přenesených elektronickou poštou (e-mailem) přijatou lokálním poštovním serverem.

Nejčastějším případem je situace, kdy poštovní server běží na počítači, který je zároveň branou do Internetu. *Kerio Network Monitor* pak „vidí“ pouze lokální komunikaci klientů s poštovním serverem. Ve výchozím nastavení *Kerio Network Monitoru* jsou vytvořena pravidla, která považují tuto komunikaci za internetovou (aby se objem dat měřil). Je ale třeba mít na paměti, že se měří objem dat i v případě, kdy si uživatelé posílají poštu lokálně mezi sebou.

Běží-li poštovní server na jiném („vnitřním“) počítači, zaznamená *Kerio Network Monitor* e-mailovou komunikaci mimo lokální síť dvakrát: při komunikaci klienta s poštovním serverem a při komunikaci tohoto serveru se servery v Internetu. Pak je vhodné pozměnit předdefinovaná pravidla pro služby SMTP, POP3 a IMAP tak, aby platila pouze pro IP adresu poštovního serveru — např.:

```
<192.168.1.10> <255.255.255.255> TCP25 on Internet
```

a přidat pravidla, pro ignoraci jakékoliv jiné poštovní komunikace — např.:

```
<all addresses> <all addresses> TCP25 discard packet
```

Tato pravidla musejí být v seznamu pravidel níže než pravidla pro konkrétní poštovní server. Detaily naleznete v kapitole 6.1.

Proxy server

Podobně jako v případě poštovního serveru umístěného na počítači, jenž je branou do Internetu, nastává při sledování komunikace klientů s proxy serverem problém v případě, že jsou data brána z cache — i tato data budou vyhodnocena jako stažená z Internetu.

Tomuto problému lze zabránit pouze vypnutím cache, což však nemusí být vždy žádoucí.

Šifrované spojení

Jsou-li data přenášená určitým protokolem šifrována, *Kerio Network Monitor* nemůže tento protokol analyzovat. V takovém případě lze sledovat pouze objem přenesených dat.

Kapitola 4

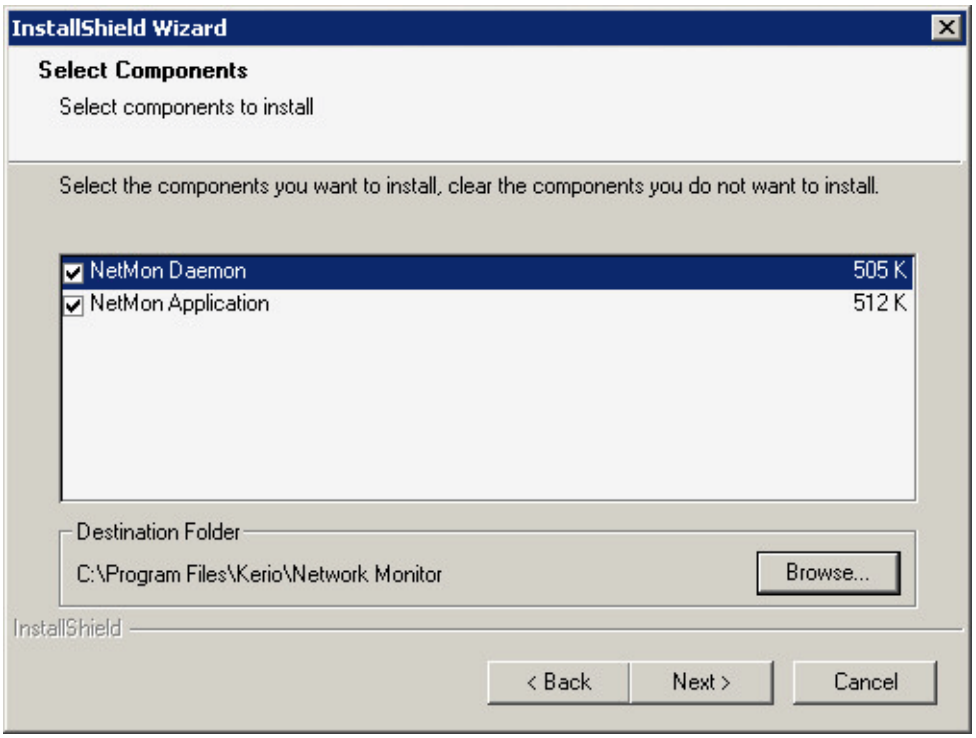
Instalace

Kerio Network Monitor může být nainstalován na libovolný počítač ve vaší lokální síti, na němž běží operační systém Windows 95 OSR2, 98, Me, NT 4.0, 2000 nebo XP. Starší verze než Windows 95 OSR2 již nejsou podporovány.

Instalaci provedete jednoduše spuštěním instalačního archivu — např.:

```
kerio-netmon-2.1.0-en-win.exe
```

Při instalaci je možno zvolit, které komponenty programu *Kerio Network Monitor* mají být instalovány:



NetMon Daemon Sledovací služba (*Daemon*). Musí být nainstalován na počítači, kde chcete komunikaci sledovat (typicky např. na internetové bráně).

Poznámka: Licenční podmínky povolují instalaci sledovací služby pouze na jeden počítač. Chcete-li provádět sledování sítě na více místech, je třeba zakoupit odpovídající počet licencí *Kerio Network Monitoru*.

NetMon Application Prohlížecí program. Může být nainstalován na libovolný počet počítačů, odkud se budete ke službě připojovat.

Poznámka: Na počítač, kde má být instalována sledovací služba (*Daemon*), doporučujeme nainstalovat také prohlížecí program (aby bylo možno se připojit lokálně v případě problémů se sítí; v operačních systémech Windows 9x/Me je to navíc jediný způsob, jak službu zastavit či spustit — viz kapitola 5.2).

Po instalaci se *Daemon* ihned spustí (není třeba restart počítače). Nyní je možno se přihlásit do prohlížecího programu (viz kapitola 5.1).

4.1 Upgrade a deinstalace

Chcete-li instalovat novější verzi *Kerio Network Monitoru* (upgrade) nebo program odinstalovat, je třeba ukončit prohlížecí program. Službu *Kerio Network Monitor Daemon* není nutné zastavovat, instalační program si ji zastaví sám.

Instalaci nové verze provedete spuštěním instalačního archivu (získaného např. z internetových stránek výrobce programu — `www.kerio.com`). Původní verzi není třeba odinstalovávat. Instalační program automaticky detekuje adresář předchozí verze, do něhož provede instalaci. Po úspěšném provedení upgrade se služba *Kerio Network Monitor Daemon* ihned spustí.

Deinstalaci programu *Kerio Network Monitor* provedete volbou *Přidat / ubrat programy* v *Ovládacích panelech*. Při deinstalaci se nesmažou adresáře a soubory, v nichž jsou uložena naměřená data. Ty musejí být smazány ručně (případně mohou být použity při další instalaci *Kerio Network Monitoru*, přeneseny na jiný počítač apod.).

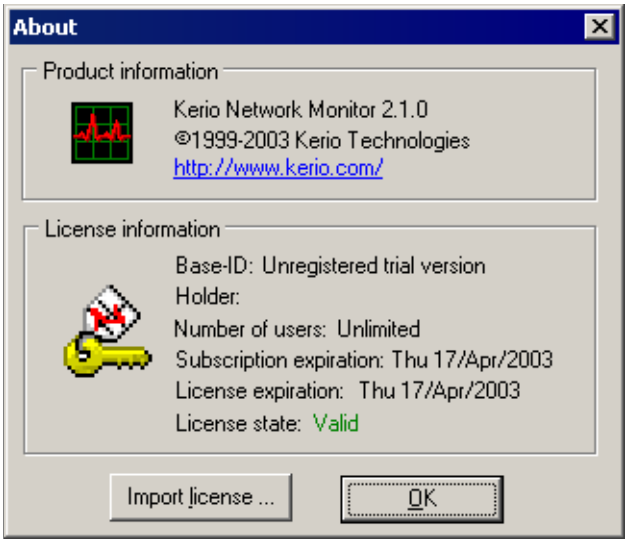
Poznámka: Zapomenete-li ukončit prohlížecí program nebo se instalačnímu programu nepodaří službu zastavit, instalační program si vyžádá restart počítače.

4.2 Import licenčního klíče

Kerio Network Monitor se po instalaci chová jako plně funkční demoverze s časovým omezením na 15 dnů ode dne instalace. Po uplynutí této doby přestane program měřit data.

Při zakoupení produktu obdržíte licenční klíč — soubor s digitálním certifikátem `license.key`. Jeho importem do programu *Kerio Network Monitor* se z demoverze stává plná verze a program může být dále používán po neomezenou dobu. Toto je možné provést i v případě, že 15-denní lhůta již vypršela a program je momentálně nefunkční. Po importu platného licenčního klíče začne opět fungovat v plném rozsahu.

Import licenčního klíče se provádí v menu *About / About*.



Stiskem tlačítka *Import license* se zobrazí dialog pro otevření souboru s licencí (`license.key`). Po jeho úspěšném načtení se v sekci *License information* zobrazí informace o aktuální licenci:

ID Identifikátor licence (slouží např. pro ověření pravosti licence)

Holder Držitel licence — osoba, nebo organizace, která produkt zakoupila

Number of users Počet uživatelů (t.j. IP adres počítačů v lokální síti, které mohou být sledovány). Je-li dosaženou tohoto počtu, další IP adresy se již neměří a při startu prohlížecího programu je zobrazeno upozornění, že byl překročen maximální počet uživatelů.

Subscription expiration Datum skončení nároku na bezplatný upgrade programu

License expiration Datum skončení platnosti licence (u demoverzí a časově omezených licencí)

License state Stav licence: platná (*Valid*) či neplatná (*Invalid*). Licence je neplatná, jestliže již nastalo datum její expirace nebo byl soubor s licencí poškozen apod.

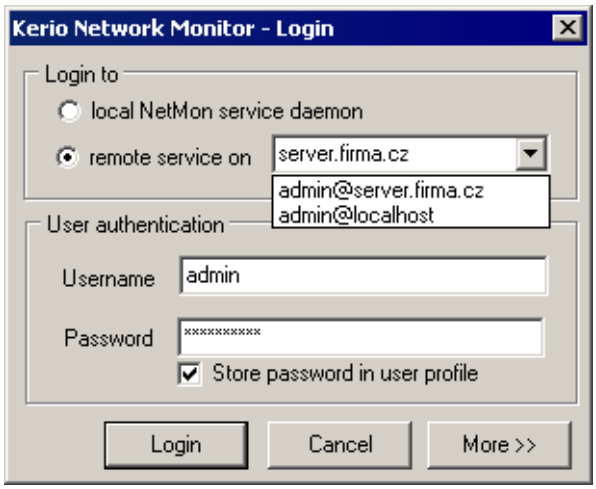
Poznámka: Je-li licence neplatná, *Kerio Network Monitor* neměří žádná data. Stále je však možno se přihlásit do prohlížecího programu a prohlížet starší data (naměřená v době, kdy licence platila), příp. provádět konfigurační úkony. Importováním platné licence (viz výše) se funkce programu obnoví v plném rozsahu.

Kapitola 5

Ovládání programu

5.1 Přihlášení do prohlížecího programu

Prohlížecí program spustíte volbou *Programy* → *Kerio* → *Network Monitor* v nabídce *Start*. Po jeho spuštění se nejprve zobrazí přihlašovací dialog.



V sekci *Login to* zvolte, kde služba *Kerio Network Monitor Daemon* běží:

local NetMon service Daemon Služba běží na tomtéž počítači, jako prohlížecí program.

remote service on Služba běží na jiném (vzdáleném) počítači.

V této položce je třeba zadat IP adresu nebo DNS jméno počítače, na kterém služba běží (dále jen „server“), případně vybrat některý ze serverů, ke kterému byl prohlížecí program již připojen. *Kerio Network Monitor* uchovává jména (resp. IP adresy) všech serverů, k nimž se podařilo úspěšně připojit, včetně příslušných uživatelských jmen. Neúspěšné pokusy o připojení si nezapamatovává. Hesla se z bezpečnostních důvodů neuchovávají.

Poznámka: Zadáním jména `localhost` nebo zpětnovazební adresy `127.0.0.1` dosáhnete stejného efektu jako volbou *local NetMon service Daemon* — připojení ke službě na lokálním počítači.

User authentication — zadejte své uživatelské jméno a heslo. Přihlašujete-li se do *Kerio Network Monitoru* poprvé (po instalaci), použijte předdefinovaný uživatelský účet `Admin` a heslo ponechte prázdné. Po zaškrtnutí volby *Store password in user profile* bude heslo uloženo do uživatelského profilu a nebude jej tedy třeba zadávat při příštím přihlášení znovu.

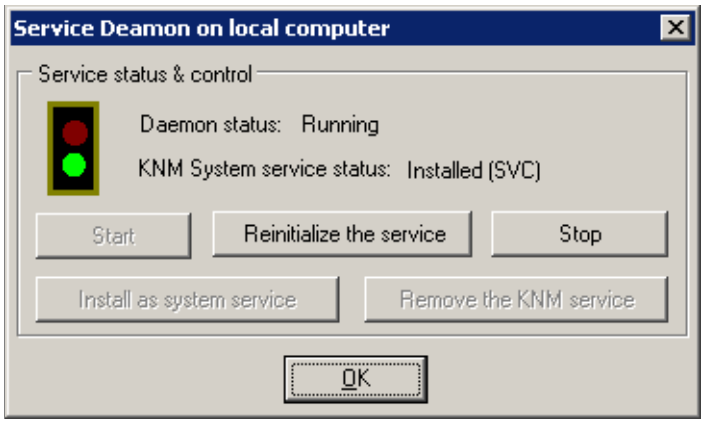
Tlačítkem *Login* provedete přihlášení. Tlačítko *Cancel* zruší přihlašovací dialog, čímž zároveň ukočí prohlížecí program. Tlačítko *More >>* rozšiřuje dialog o další volby. Po jeho stisku se změní na *Less <<* — tím lze rozšířené volby opět skrýt.

Store password in user profile Uživatelské jméno a heslo bude uloženo do uživatelského profilu ve Windows a nebude tak nutno jej zadávat při každém přihlašování. Doporučujeme používat tuto volbu pouze v případě, kdy nehrozí zneužití přístupových práv jinou osobou!

Don't restore windows settings Prohlížecí program nebude obnovovat rozložení jednotlivých oken. To může být užitečné např. při vzdáleném připojování přes pomalou linku, kdy se tak výrazně sníží objem přenášených dat, nebo v případě, že jeden uživatelský účet využívá více osob.

5.2 Ovládání služby

Po stisku tlačítka *More >>* v přihlašovacím dialogu se v pravém dolním rohu okna objeví ikona pro konfiguraci služby. Kliknutím na ni se zobrazí následující dialog:



Daemon status Zobrazuje stav služby — spuštěna (*Running*) nebo zastavena (*Stopped*).

KNM system service status Zobrazuje, zda je *Kerio Network Monitor Daemon* instalován jako systémová služba (*Installed (SVC)* — ve Windows NT/2000/XP), jako aplikace na pozadí (*Installed (APP)* — ve Windows 9x/Me) či není instalován jako služba (*Not installed (SVC)*).

Start Spuštění služby (je-li zastavena).

Reinitialize the service Opětovná inicializace služby (de facto zastavení a spuštění) — pouze pokud služba běží.

Stop Zastavení služby (je-li spuštěna).

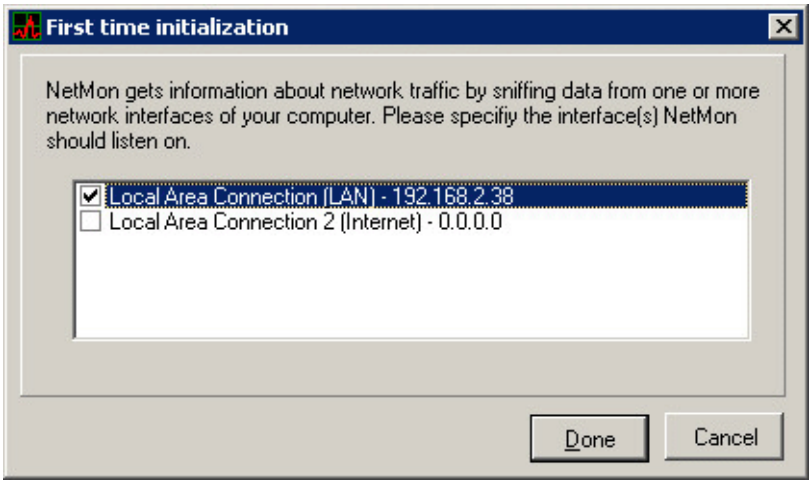
Install as system service Vytvoření služby *Kerio Network Monitor*, jestliže dosud neexistuje (ve Windows NT/2000/XP jako systémové služby, ve Windows 9x/Me jako aplikace na pozadí).

Remove the KNM service Odstranění systémové služby *Kerio Network Monitor*. Toto je samozřejmě možno provést pouze tehdy, pokud tato služba v systému existuje a je zastavena.

Poznámka: Je-li *Kerio Network Monitor Daemon* instalován jako služba v operačním systému Windows NT/2000/XP, je možno službu spouštět, zastavovat a restartovat také pomocí systémového ovládacího panelu *Služby*.

5.3 Počáteční konfigurace

Přihlásíte-li se do prohlížecího programu poprvé (po instalaci *Kerio Network Monitoru*), zobrazí se nejprve speciální dialog pro výběr rozhraní, na kterých budou pakety sledovány.



Zaškrtněte pole u všech adaptérů, na nichž chcete data sledovat. Zpravidla by to měly být všechny adaptéry vedoucí do lokální sítě. Sledovat pakety na adaptéru vedoucím do Internetu zpravidla nemá smysl — pokud se používá překlad adres (NAT), je zde vidět pouze adresa počítače, na němž *Kerio Network Monitor* běží.

Po stisku tlačítka *Done* se nastavení uloží a zobrazí se vlastní prohlížecí program. Tento dialog se při příštím přihlášení již nezobrazí. Provedená nastavení je samozřejmě možno v programu změnit.

Kapitola 6

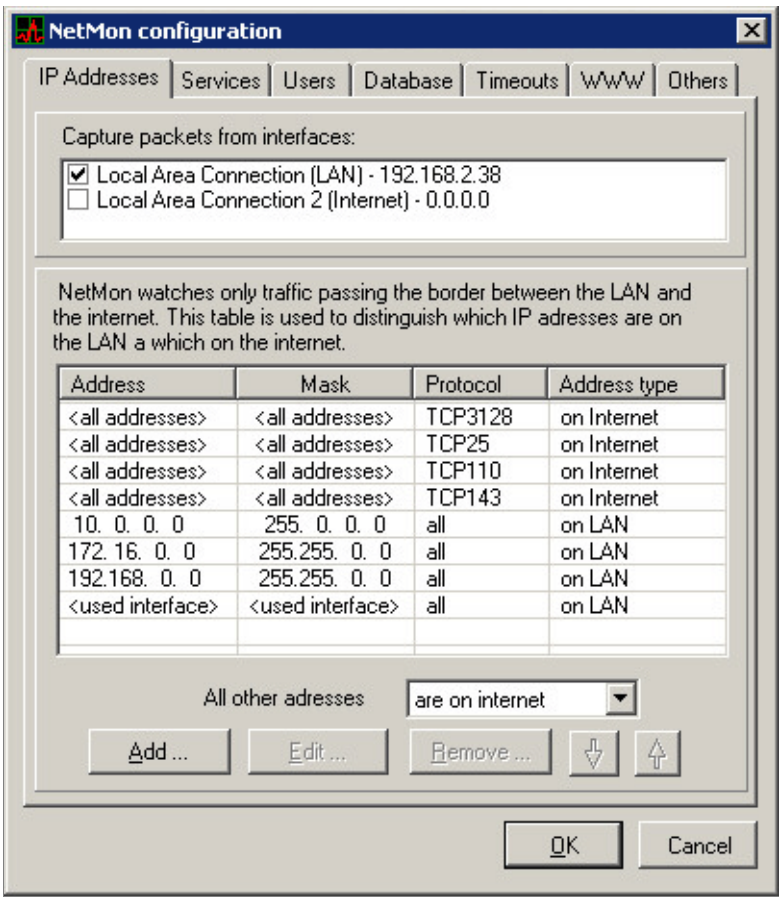
Konfigurace

Veškerá nastavení *Kerio Network Monitoru* se provádějí v okně *Configuration*, které se zobrazí z menu *Settings / Configuration*, případně stiskem klávesové zkratky *Ctrl+S*.

Poznámka: Všechna nastavení v dialogu *Configuration* mají okamžitý účinek (od stisku tlačítka *OK*). V žádném případě není třeba restartovat službu *Kerio Network Monitor Daemon*.

6.1 Rozsahy IP adres

Záložka *IP Addresses* umožňuje výběr rozhraní, na němž budou pakety zachytávány, a definici rozsahů IP adres, které mají být zaznamenávány.



Capture packets from interfaces Výběr rozhraní, na nichž budou pakety zachytávány. Zpravidla by to měly být všechny adaptéry vedoucí do lokální sítě. Sledovat pakety na adaptéru vedoucím do Internetu zpravidla nemá smysl — pokud se používá překlad adres (NAT), je zde vidět pouze adresa počítače, na němž *Kerio Network Monitor* běží.

Seznam skupin IP adres Zde jsou uvedeny jednotlivé definované skupiny IP adres a typ skupiny (*on LAN*, *on Internet* nebo *discard packet*). Detailní popis viz dále.

All other addresses Tato volba specifikuje skupinu, do níž mají být zařazeny IP adresy, které nevyhovují žádné z uvedených specifikací.

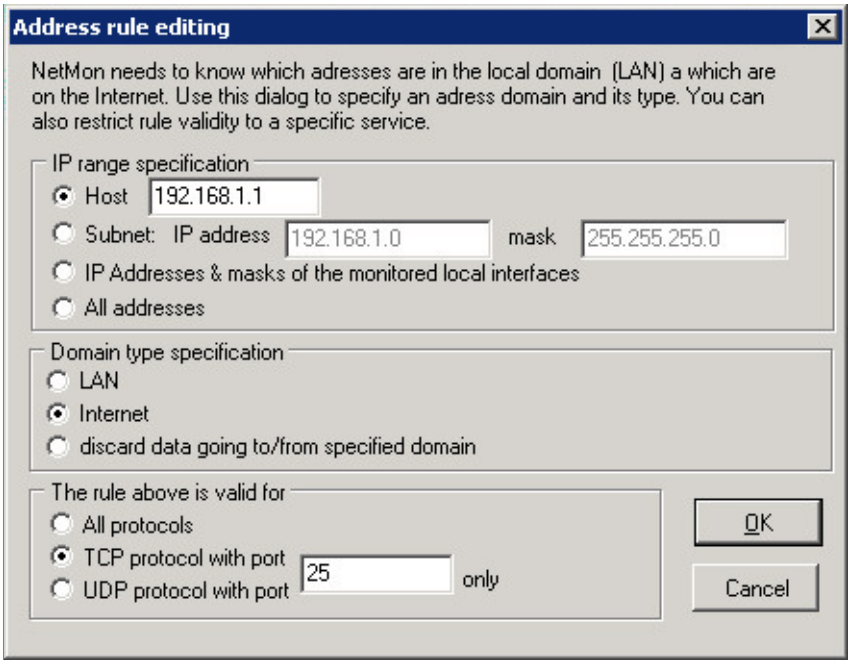
Typický příklad použití: specifikujeme adresy patřící do lokální sítě a touto volbou určíme, že „všechny ostatní adresy patří do Internetu“ (*are on Internet*).

Add, Edit, Remove Tato tlačítka slouží pro přidání nové skupiny adres, resp. pro úpravu či smazání vybrané skupiny.

Tlačítka se šipkami (nahoru / dolů) Seznam definic skupin IP adres je vždy procházen shora dolů. Definice tedy musejí být seřazeny (od nejspecifičtější k nejobecnější). Tlačítka se šipkami slouží k posunu vybrané definice v seznamu nahoru nebo dolů.

Definice skupiny IP adres

Po stisku tlačítka *Add* nebo *Edit* se zobrazí dialog pro definici skupiny IP adres.



IP range specification Typ skupiny. Je možno zvolit jeden z následujících typů:

- *Host* — IP adresa jednoho konkrétního počítače
- *Subnet: IP address / mask* — IP subsíť s příslušnou maskou
- *IP addresses & masks of the local interfaces* — do skupiny budou přidány IP adresy sítí, do nichž jsou připojeny adaptéry vybrané pro sledování paketů
- *All addresses* — všechny IP adresy

Domain type specification Typ (doména) skupiny IP adres. Tato volba určuje, jak budou zpracovávány pakety, jejichž zdrojová nebo cílová adresa patří do této skupiny. Skupinu adres lze zařadit do jedné z následujících domén:

- *LAN* — lokální síť. Specifickou vlastností této skupiny je, že všechny zachycené adresy z ní se zaznamenávají do seznamu počítačů (viz kapitola 7.1).
- *Internet* — adresy z této skupiny se měří, ale vytváří se z nich žádný seznam.
- *discard data* — patří-li zdrojová nebo cílová adresa paketu do této skupiny, nebude objem dat v tomto paketu měřen.

Poznámka: Objem dat v paketu bude změřen právě tehdy, jestliže jedna z adres v hlavičce paketu (zdrojová nebo cílová) patří do skupiny *LAN* a druhá do skupiny *Internet*. Detaily naleznete v kapitole 3.2.

The rule above is valid for Specifikace protokolu a portu, pro nějž má toto pravidlo platit. Takto je možno např. definovat, že budou měřena data pouze pro určitou službu.

- *All protocols* — pravidlo bude platit pro všechny protokoly (a tím i pro všechny služby)
- *TCP protocol with port* — pravidlo bude platit pouze pro protokol TCP a zadaný port. Protokol a port určuje konkrétní službu (např. SMTP, WWW apod.). Číslo portu 0 (nula) znamená všechny porty — tedy všechny služby využívající protokol TCP.
- *UDP protocol with port* — pravidlo bude platit pouze pro protokol UDP a zadaný port. Platí stejné úvahy jako v případě protokolu TCP.

Poznámka

Po instalaci *Kerio Network Monitoru* jsou v záložce *IP Addresses* předdefinovány určité skupiny adres. Jejich účelem je maximálně zjednodušit konfiguraci programu — tak, aby ve výchozím nastavení vyhověl co největšímu počtu standardních situací.

- Pravidla pro všechny adresy (*<all addresses>*) se specifikovanými protokoly a porty. Tato pravidla specifikují služby, které běží v lokální síti, ale měly by být monitorovány jako internetové (typicky proxy server a poštovní server).

  Je-li vaše síť připojena do Internetu pomocí proxy serveru, mělo by být pravidlo pro proxy server definováno (jinak nebudou žádná data naměřena, protože komunikace klientů s proxy serverem probíhá pouze v rámci lokální sítě). Výchozí pravidlo předpokládá standardní port `3128` (*TCP3128*). Běží-li proxy server ve vaší síti na jiném portu (např. `80` nebo `8080`), nastavte jej správně v tomto pravidle.

  Běží-li poštovní server na počítači, který je zároveň branou do Internetu, pak *Kerio Network Monitor* nemůže měřit objem odeslané a přijaté pošty, protože se jedná o komunikaci v rámci lokální sítě. Pro tento účel jsou předdefinována pravidla pro protokoly SMTP (*TCP25*), POP3 (*TCP110*) a IMAP (*TCP143*).

- Pravidla pro privátní rozsahy IP adres (`10.0.0.0`, `172.16.0.0` a `192.168.0.0`). Tyto adresy jsou vyhrazeny pro privátní sítě a nemohou se vyskytovat nikde v Internetu, proto *Kerio Network Monitor* automaticky předpokládá, že se jedná o lokální síť.

- Pravidlo pro adaptéry, na nichž jsou pakety zachytávány (*<used interfaces>*).

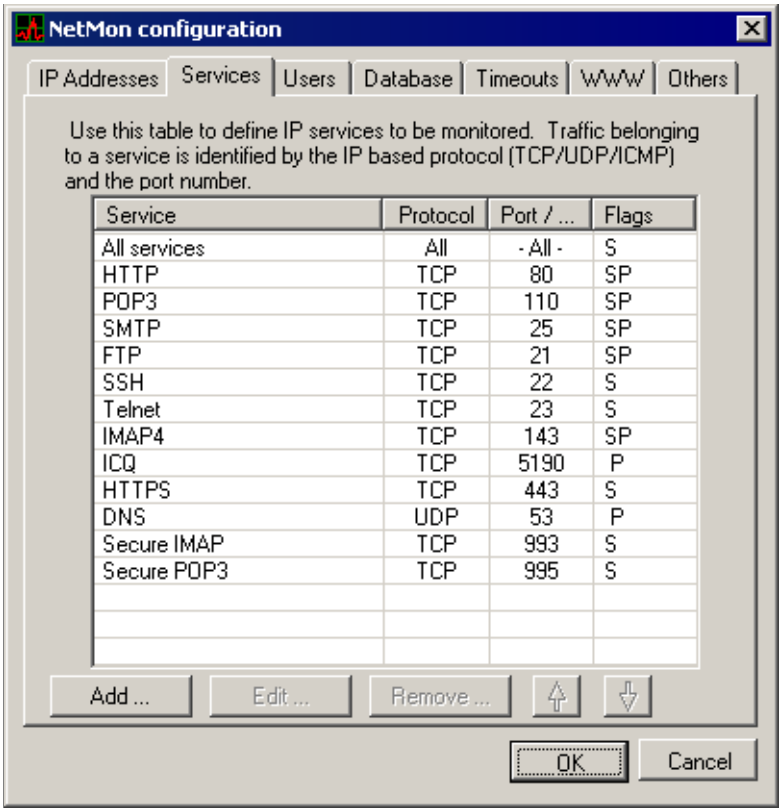
  Jak již bylo popsáno výše (viz též kapitola 5.3), pakety by měly být sledovány na rozhraních vedoucích do lokální sítě (aby *Kerio Network Monitor* rozpoznal IP adresy jednotlivých počítačů v ní). Proto se předpokládá, že adaptéry, které byly vybrány pro sledování paketů, jsou připojeny do lokální sítě (doména *LAN*).

  Není-li vaše lokální síť tvořena kaskádními segmenty (tj. více subsítěmi navzájem propojenými směrovači), pak již nemusíte definovat žádné další pravidlo pro IP adresy.

Všechna předdefinovaná pravidla je možno upravit či smazat, pokud nevyhovují konkrétní konfiguraci. Většinou to však není nutné — pokud jsou např. v lokální síti použity pouze IP adresy z rozsahu `192.168.0.0`, pravidla pro ostatní privátní rozsahy (`10.0.0.0` a `172.16.0.0`) jsou neúčinná, protože takové adresy *Kerio Network Monitor* nikdy nezachytí. Obdobná úvaha platí také pro pravidla pro poštovní a proxy server.

6.2 Sledované služby

Kerio Network Monitor umožňuje definovat síťové služby, které budou sledovány detailně. K tomuto účelu slouží v konfiguračním dialogu záložka *Services*.



Seznam služeb Okno zobrazuje seznam definovaných služeb (ve výchozím nastavení je již předdefinována většina standarsních služeb). Sloupce seznamu služeb mají následující význam:

- *Service* — název služby (zadaný při její definici)
- *Protocol* — protokol, který služba používá (TCP, UDP, ICMP, PPTP nebo libovolný — *All*)
- *Port / Subprotocol* — port, který služba využívá (pouze u protokolů TCP a UDP)
- *Flags* (příznaky) — indikace dalších parametrů, které byly pro službu nastaveny. Detaily viz dále.

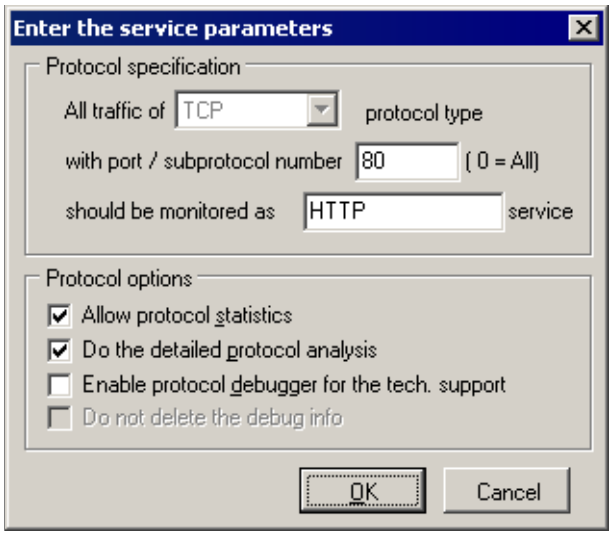
Tlačítka pod seznamem služeb umožňují definici nové služby (*Add*), změnu nastavení služby (*Edit*) nebo odstranění služby (*Remove*).

Tlačítka se šipkami (nahoru / dolů) slouží k uspořádání služeb v seznamu. Toto uspořádání má význam pouze pro lepší přehlednost; na funkci programu nemá žádný vliv.

Poznámka: S některými předdefinovanými službami (*HTTP*, *SMTP*, *POP3*, *IMAP4*, *FTP* a *DNS*) jsou spjaty další funkce programu *Kerio Network Monitor*, a proto je nelze odebrat.

Definice služby

Po stisku tlačítka *Add* nebo *Edit* se zobrazí dialog pro definici služby:



All traffic of ... protocol type Protokol, který daná služba využívá. Možnosti jsou: *TCP*, *UDP*, *ICMP* (protokol internetových řídicích zpráv), *PPTP* (protokol pro virtuální privátní sítě fy. Microsoft) a *All* (libovolný protokol — tj. veškerá IP komunikace).

with port / subprotocol number Číslo portu, který služba využívá (např. 25 = SMTP, 80 = WWW atd.). Hodnota 0 (nula) znamená všechny porty (tzn. veškerou komunikaci zvoleným protokolem).

Allow protocol statistics Oddělený záznam dat pro tuto službu. V grafu či reportu bude možno odděleně zobrazit objem dat přenesený pouze touto službou (detaily viz kapitoly 7.2, 7.6).

Je-li tato volba zapnuta, zobrazuje se ve sloupci *Flags* příznak *S*.

Do the detailed protocol analysis Provádět detailní analýzu této služby. Tato volba je dostupná pouze u standardních služeb, kde *Kerio Network Monitor* umí analýzu provést (*HTTP*, *SMTP*, *POP3*, *IMAP4*, *FTP* a *DNS*). Výsledky analýzy (tj. např. zachycené WWW stránky, e-mailové zprávy, přenášené soubory apod.) se zobrazují do okna

Scanned data, případně také do příslušného záznamu (*HTTP Log*, *Mail Log*, *ICQ Log*). Detaily naleznete v kapitolách 7.4 a 7.7.

Je-li tato volba zapnuta, zobrazuje se ve sloupci *Flags* příznak *P*.

Poznámka: K analýze protokolů se vztahují upřesňující volby v záložce *Others*. Jejich podrobný popis naleznete v kapitole 6.7.

Enable protocol debugger Detailní záznam dat této služby pro účely technické podpory. Tuto volbu lze využít při podezření, že *Kerio Network Monitor* nezaznamenává korektně data příslušné služby. Získaná data je možno předat technické podpoře *Kerio Technologies* k další analýze.

Je-li tato volba zapnuta, zobrazuje se ve sloupci *Flags* příznak *D*.

Do not delete the debug information Detailní data služby, zaznamenaná pro účely ladění (viz předchozí volba) jsou poměrně objemná a mohla by velice rychle zaplnit značnou část diskového prostotu. Proto jsou za normálních okolností mazána vždy při ukončení sledovaného spojení. Zapnutím této volby nebudou tato data automaticky mazána a zůstanou uchována až do ručního smazání.

6.3 Uživatelské účty

Při připojování ke službě *Kerio Network Monitor Daemon* prohlížecím programem je vyžadováno zadání uživatelského jména a hesla. Tím je zajištěno, aby přístup k datům a konfiguraci programu měli pouze oprávnění uživatelé a nemohlo dojít ke zneužití dat či jejich záměrnému zkreslení změnou konfigurace.

V *Kerio Network Monitoru* může být definován libovolný počet uživatelských účtů s různou úrovní přístupových práv. K tomuto účelu slouží v konfiguračním dialogu záložka *Users* (tuto záložku lze také otevřít pomocí menu *Settings / Users*).

Seznam uživatelů v této záložce obsahuje následující informace:

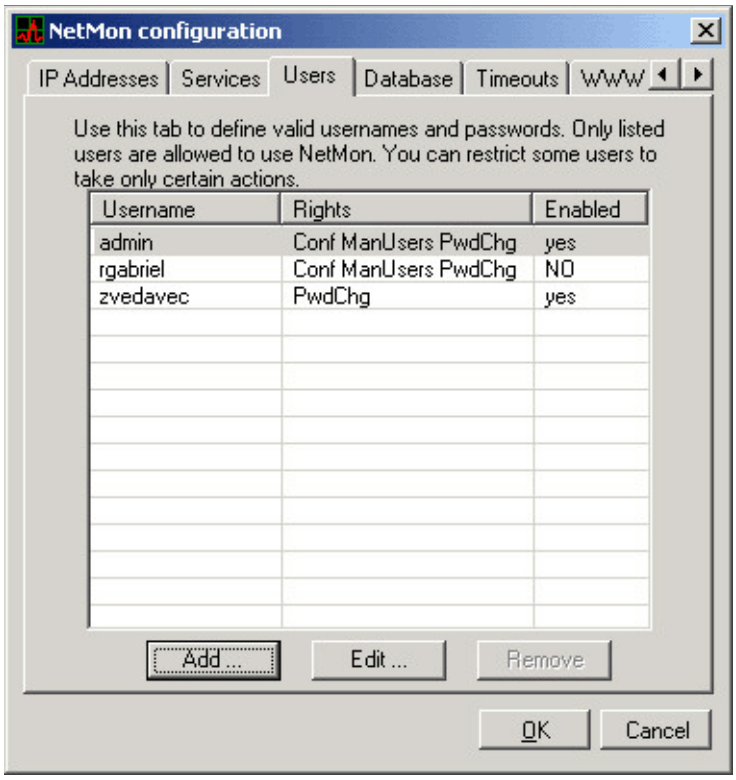
Username Uživatelské jméno (jímž se uživatel přihlašuje)

Rights Přístupová práva uživatele (detaily viz dále)

Enabled Stav účtu: povolen (*yes*) či blokován (*no*)

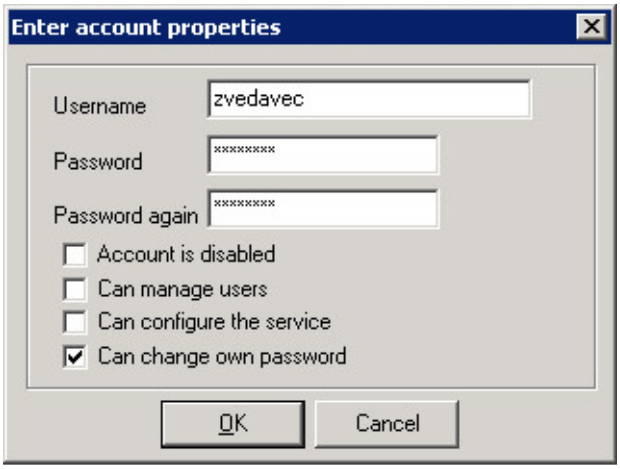
Tlačítka pod seznamem účtů umožňují definici nového uživatele (*Add*), změnu nastavení vybraného účtu (*Edit*) nebo odstranění účtu (*Remove*).

Poznámka: Předdefinovaný uživatelský účet Admin nelze odstranit ani mu měnit přístupová práva nebo jej zakázat.



Definice uživatele

Po stisku tlačítka *Add* nebo *Edit* se otevře dialog pro definici uživatelského účtu.



Username Uživatelské jméno. Nemělo by obsahovat mezery a interpunkční znaménka. Velká a malá písmena se nerozlišují.

Password Přístupové heslo uživatele. Může obsahovat libovolné tisknutelné znaky (včetně mezery); rozlišuje velká a malá písmena.

Password again Potvrzení hesla (pro kontrolu, že při jeho zadávání nedošlo k překlepu)

Upozornění: Z bezpečnostních důvodů se doporučuje nenechávat heslo prázdné! Rovněž heslo předdefinovaného uživatele `Admin` by mělo být po prvním přihlášení změněno.

Account is disabled Zapnutím této volby lze uživatelský účet dočasně deaktivovat („vypnout“).

Je-li tato volba zapnuta, zobrazuje se ve sloupci *Enabled* seznamu uživatelů *NO*, v opačném případě *yes*.

Can manage users Uživatel je oprávněn vytvářet, měnit a rušit uživatelské účty.

Tato volba zároveň aktivuje volbu *Can configure the service* a ve sloupci *Rights* seznamu uživatelů se zobrazuje jako *ManUsers* (resp. *Conf ManUsers*).

Can configure the service Uživatel může provádět konfiguraci služby *Kerio Network Monitor Daemon* (tzn. veškerá nastavení v dialogu *Configuration* s výjimkou záložky *Users*).

Toto právo se ve sloupci *Rights* seznamu uživatelů zobrazuje jako *Conf*.

Change own password Uživatel má právo změnit své vlastní heslo (v menu *Action / Change password*). Je-li zapnuta volba

Can manage users, nemá zapnutí či vypnutí této volby žádný účinek.

Toto právo se ve sloupci *Rights* seznamu uživatelů nezobrazuje.

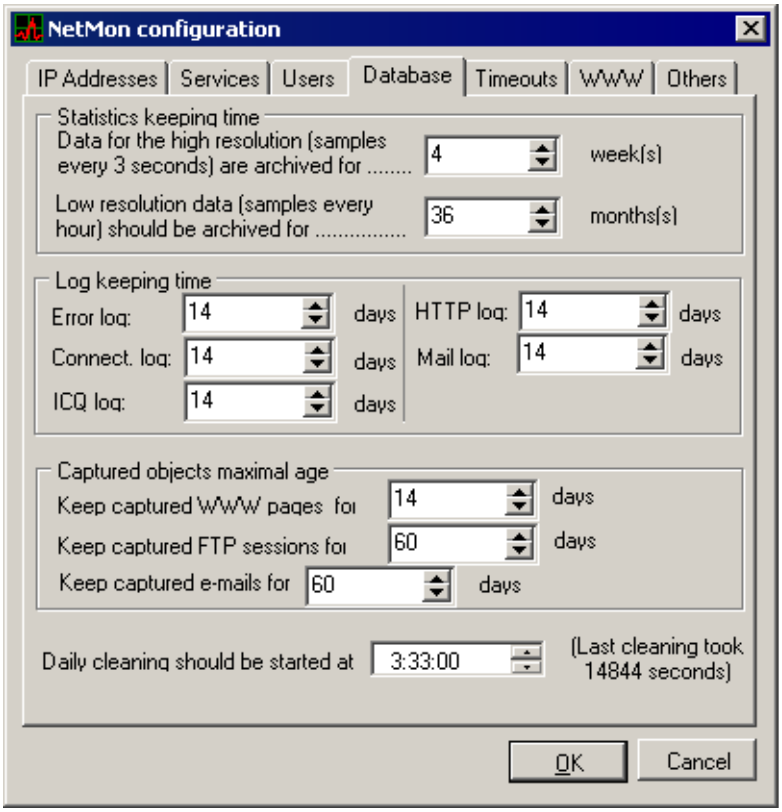
6.4 Volby pro ukládání dat

Záložka *Database* slouží k nastavení parametrů pro ukládání naměřených dat.

Statistics keeping time Maximální doba, po kterou budou udržovány statistiky — objem přenesených dat celkem a za jednotlivé definované služby. Optimální nastavení závisí jednak na požadavku, jak dlouho mají být naměřená data uchovávána, jednak na velikosti diskového prostoru a na intenzitě provozu (po dobu, kdy není zaznamenána žádná komunikace, se nic neukládá).

Dobu uchování dat určují dva parametry:

- *Data for the high resolution* — data s vysokým rozlišením (vzorkována po 3 sekundách). Doba uchování se udává v týdnech (*weeks*). Tyto údaje představují převážnou část všech uložených dat.
- *Low resolution data* — data s nízkým rozlišením (vzorkována po 1 hodině). Tato data zabírají na disku výrazně menší prostor než data s vysokým rozlišením, je-



jich přesnost je ale dostatečná při vyhodnocování delšího časového období (např. 1 týden a více).

Díky svému malému objemu mohou být data s nízkým rozlišením uchovávána po delší dobu — doba uložení se udává v měsících (*months*).

Log keeping time Doba uchování (resp. maximální stáří) záznamů v souborech *Error Log*, *Connection Log*, *HTTP Log*, *Mail Log* a *ICQ Log*. Udává se v počtu dnů (*days*).

Captured objects maximal age Doba uložení zachycených objektů (tj. informací, které se zobrazují v okně *Scanned data* — viz kapitola 7.4). Udává se v počtu dnů (*days*).

- *Keep captured WWW pages* — doba uložení zachycených WWW stránek. WWW stránky mohou obsahovat značné množství obrázků a dalších objektů, jedná se tedy o poměrně objemná data.
- *Keep captured FTP sessions* — doba uložení informací o připojení na FTP servery. Ukládají se pouze informace o relacích (server, uživatel, stažené či uložené soubory), nikoliv přenášené soubory. Objem uložených dat je proto velmi malý.
- *Keep captured e-mails* — doba uložení zachycených e-mailových zpráv. Zprávy se ukládají i s přílohami, mohou tedy představovat značný objem dat.

Daily cleaning should be started at Čas spuštění automatické údržby databáze (provádí se jednou denně). Hlavním úkolem při této akci je odstranění dat, jejichž stáří přesahuje stanovené hodnoty (viz volby popsané výše).

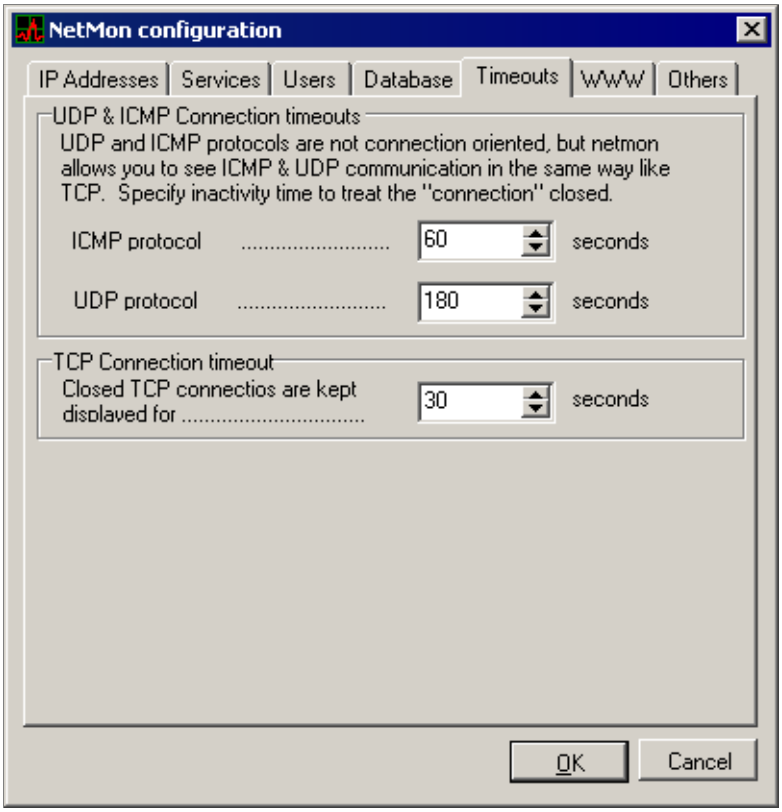
Tato údržba může trvat značnou dobu (v krajním případě až několik desítek minut — v závislosti na objemu uložených dat a rychlosti počítače). Po dobu údržby nelze zobrazovat právě zpracovávaný záznam (v příslušném okně se zobrazí hlášení o tom, že právě probíhá údržba). Proto by měla být údržba naplánována na dobu, kdy je provoz v síti minimální či nulový (např. v noci).

Poznámka: Je-li v nastavenou dobu počítač s *Kerio Network Monitorem* vypnut, údržba se pak provede ihned při nejbližším spuštění služby *Kerio Network Monitor Daemon*.

(Last cleaning took ... seconds) Zde se zobrazuje doba trvání poslední údržby databáze (v sekundách).

6.5 Parametry pro sledování protokolů

Záložka *Timeouts* slouží k nastavení časových parametrů pro sledování jednotlivých protokolů:



UDP & ICMP connection timeouts Protokoly UDP a ICMP jsou nespojované protokoly — komunikace probíhá výměnou jednotlivých zpráv (tzv. datagramů), mezi nimiž neexistuje (na úrovni síťové komunikace) žádná vazba. Typická komunikace je však tvořena jednou nebo několika sekvencemi požadavek — odpověď. Proto lze předpokládat, že pokud mezi dvěma počítači dochází k výměně UDP či ICMP v pravidelných (krátkých) intervalech, jedná se o jednu relaci (tzv. pseudospojení). Pokud se tento interval výrazně prodlouží, předpokládáme, že se již jedná o další relaci. Těchto principů se využívá při zobrazování UDP a ICMP pseudospojení v okně *Current connections* (viz kapitola 7.3).

K nastavení výše popsaných intervalů slouží volby *ICMP protocol* a *UDP protocol*.

TCP connection timeout Protocol TCP je spojovaný protokol (nejprve vytvoří spojení, kterým jsou pak přenášena vlastní data). V tomto případě je přesně známo, kdy spojení vzniklo a kdy bylo ukončeno. Jestliže se přenáší malý objem dat rychlou linkou, spojení může trvat jen velmi krátkou dobu (často méně než 1 sekundu). Aby bylo možno spojení sledovat v okně *Current connections* (viz kapitola 7.3), ponechává se zde zobrazeno určitou dobu po jeho skončení. Tuto dobu nastavuje volba *Closed TCP connections are kept displayed for*.

6.6 Parametry WWW rozhraní

Záložka WWW slouží k nastavení parametrů WWW rozhraní programu *Kerio Network Monitor*.

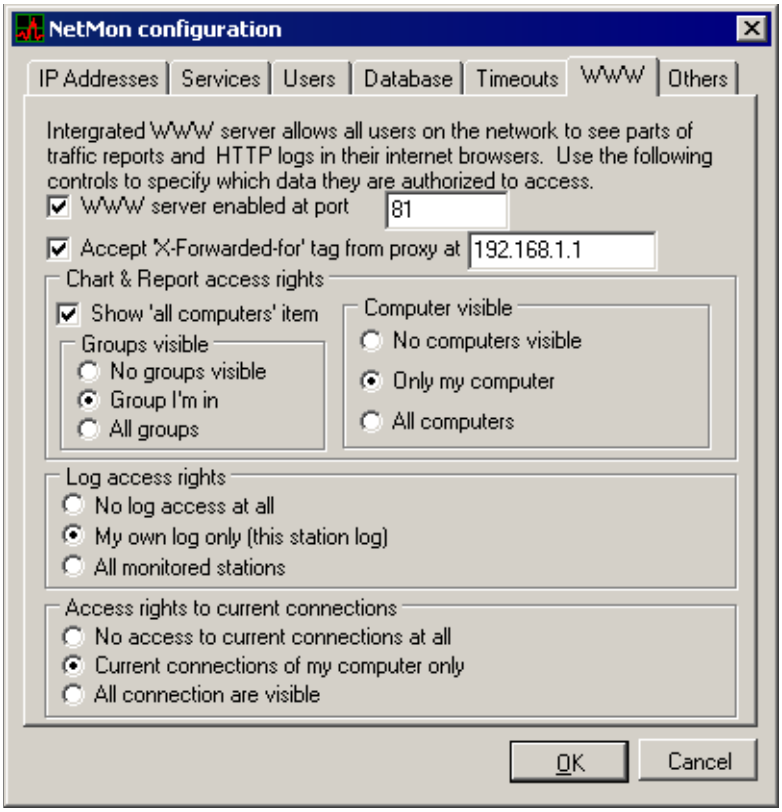
WWW server enabled at port Tato volba zapíná / vypíná vestavěný WWW server. Bude-li vypnuta, nebude WWW rozhraní k dispozici.

Dále se zde specifikuje port, na němž WWW server běží (standardně `81`). Jestliže na počítači, kde je *Kerio Network Monitor Daemon* instalován, neběží žádný jiný WWW server, je možno použít standardní port `80` — pak nebude nutno specifikovat port v prohlížeči při připojování k WWW rozhraní *Kerio Network Monitoru*.

Accept 'X-Forwarded-for' tag... Tato volba určuje, aby *Kerio Network Monitor* zjišťoval IP adresy klientských počítačů z položky `X-Forwarded-for` v HTTP požadadavku, který vestavěný WWW server přijal od proxy serveru.

Nastavte tuto volbu v případě, že lokální počítače používají pro přístup do Internetu proxy server. V takovéto konfiguraci totiž *Kerio Network Monitor* „vidí“ pouze požadavky proxy serveru. Z položky `X-Forwarded-for` (kterou doplňuje proxy server) je ale možno zjistit IP adresu klienta — skutečného původce HTTP požadavku.

Do příslušného pole zadejte IP adresu proxy serveru, z něhož má *Kerio Network Monitor* položku `X-Forwarded-for` akceptovat (nemůže být akceptována pro libovolný



proxy server, protože by této vlastnosti mohli klienti velmi snadno zneužít). Běží-li proxy server na tomtéž počítači jako *Kerio Network Monitor Daemon*, použijte zpětnovazební adresu `127.0.0.1`.

Výše popsaný problém lze řešit také nastavením WWW prohlížečů tak, aby nepoužívaly proxy server pro lokální adresy (tato nastavení si však zpravidla mohou uživatelé sami měnit).

Následující volby určují chování WWW rozhraní, jestliže jej otevře anonymní uživatel (tj. nepřihlásí se svým uživatelským jménem a heslem — viz kapitola 8.1).

Typické nastavení předpokládá, že každý uživatel si může zobrazit informace pouze o svém počítači (tom, z něhož se k WWW rozhraní připojuje). Má-li uživatel k programu *Kerio Network Monitor* přístupová práva (tj. má zde vytvořen uživatelský účet — viz kapitola 6.3), může se přihlásit a zobrazit si veškeré informace, které *Kerio Network Monitor* poskytuje.

Show 'All computers' item V seznamu počítačů se bude zobrazovat volba *All computers* (tj. zobrazení statistik za všechny počítače, které *Kerio Network Monitor* eviduje).

Groups visible Volba, které skupiny anonymní uživatel uvidí (*No groups visible* — žádné skupiny, *Groups I'm in* — pouze skupinu, do níž patří počítač, ze kterého se připojuje, nebo *All groups* — všechny skupiny).

Computers visible Volba, které počítače uživatel uvidí (*No computers* — žádné počítače, *Only my computer* — pouze počítač, ze kterého se připojuje, nebo *All computers* — všechny počítače).

Log access rights Přístupová práva k záznamům (*No logs access at all* — žádné záznamy, *My own logs only* — pouze záznamy pro počítač, ze kterého se připojuje, nebo *All monitored stations* — záznamy pro všechny registrované počítače).

Access rights to current connections Přístupová práva pro sledování aktivních spojení (*No access to current connections at all* — žádná spojení, *Current connections of my computer only* — pouze spojení pro počítač, ze kterého se připojuje, nebo *All connections are visible* — spojení pro všechny registrované počítače).

6.7 Upřesňující nastavení

Nastavení dalších voleb pro vzhled a chování programu *Kerio Network Monitor* lze provést v záložce *Others*.

Do NOT save mail message body *Kerio Network Monitor* nebude ukládat obsah zachycených e-mailových zpráv (pouze adresy odesílatele a příjemce).

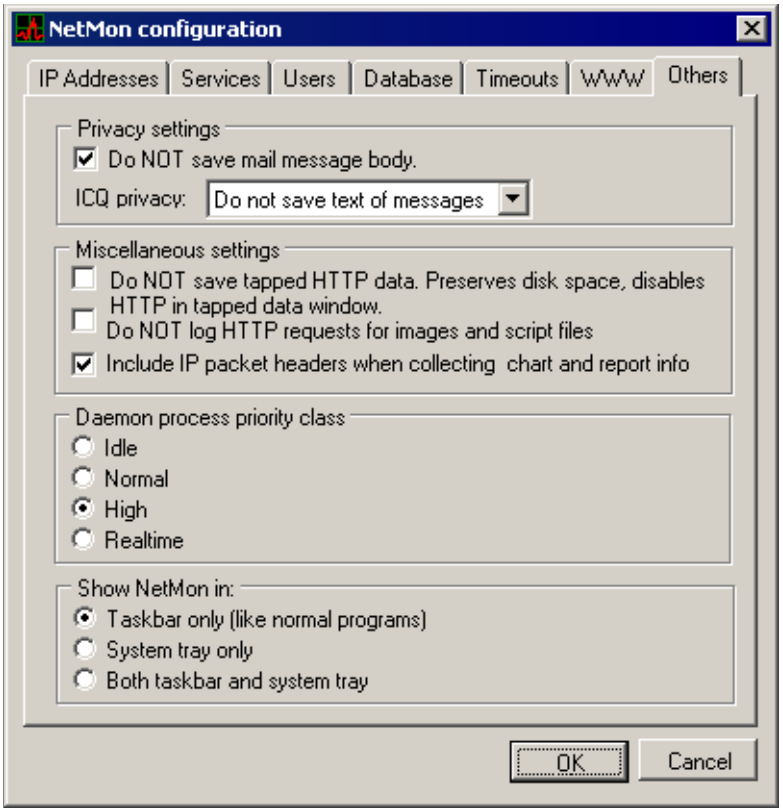
Poznámka: Sledovat a ukládat lze pouze zprávy, které nejsou přenášeny šifrovanými protokoly (v opačném případě je možno pouze měřit objem přenesených dat).

Upozornění: Je třeba mít na paměti, že sledování obsahu pošty je narušování soukromí uživatelů! Nebude-li tato volba zapnuta, měli by všichni uživatelé lokální sítě být informováni o tom, že jejich pošta je sledována!

ICQ privacy Volba, jakým způsobem má být sledována komunikace protokoly *ICQ* a *ICQ2Go*:

- *No privacy* (bez ochrany soukromí) — budou sledovány všechny dostupné informace (ICQ čísla, přezdívky, obsah zpráv)
- *Do not save text of messages* — *Kerio Network Monitor* nebude ukládat obsah jednotlivých zpráv (tzn. sledována budou pouze ICQ čísla a přezdívky uživatelů)
- *Disable ICQ analysator* — vypnutí analýzy protokolů *ICQ* a *ICQ2Go*.

  Poznámka: Stejného efektu lze dosáhnout vypnutím detailní analýzy protokolu v definici služby *ICQ* (podrobnosti viz kapitola 6.2). Sledování ICQ funguje tedy



pouze v případě, je-li zvoleno *No privacy* nebo *Do not save text of messages* a zároveň povolena detailní analýza protokolu v definici služby *ICQ*.

Do NOT save tapped HTTP data *Kerio Network Monitor* nebude ukládat obsah zachycených WWW stránek. Zapnutí této volby výrazně šetří místo na disku počítače, v okně *Tapped data* však nebude k dispozici volba HTTP (nebude možno prohlížet stránky navštívené jednotlivými uživateli).

Poznámka: Sledovat a ukládat lze pouze stránky, které nejsou přenášeny šifrovaným protokolem *HTTPS* (v opačném případě je možno pouze měřit objem přenesených dat).

Do NOT log HTTP requests for images... Při otevírání WWW stránky v prohlížeči musí být vyslán HTTP požadavek na každý objekt, který stránka obsahuje (obrázek, skript atd.). Do záznamu *HTTP Log* se standardně zaznamenávají všechny HTTP požadavky. Zapnutím této volby se budou zaznamenávat pouze požadavky na samotné

stránky — *HTTP Log* tak bude výrazně kratší a přehlednější. Ve většině případů je takovýto záznam HTTP požadavků plně postačující.

*Poznámka:*Záznam požadavků do okna / souboru *HTTP Log* lze provádět, pouze jedná-li se o komunikaci protokolem HTTP. V případě šifrovaného protokolu HTTPS se zaznamenává pouze objem přenesených dat.

Include IP packet headers... Zapnutí této volby způsobí, že budou do objemu přenesených dat započítávány celé IP pakety včetně hlaviček. Její použití závisí na tom, jaká data chcete získávat.

Poznámka: Chcete-li porovnávat údaje získané programem *Kerio Network Monitor* s údaji získanými jinými programy či údaji od poskytovatele internetového připojení, je třeba zjistit, jaká metodika měření se používá, a podle toho nastavit volbu *Include IP packet headers* v programu *Kerio Network Monitor*.

Daemon process priority class Nastavení priority procesu služby *Kerio Network Monitor*. Ve výchozím nastavení má vysokou prioritu (*high*). Toto nastavení doporučujeme měnit pouze v následujících případech:

- při podezření, že služba příliš zatěžuje systém — zkuste snížit prioritu procesu

  Poznámka: Jedná se pouze o dočasné řešení — v těchto případech doporučujeme použít výkonnější hardware.

- při častém výskytu hlášení o ztracených paketech v důsledku nedostatku systémových prostředků v záznamu *Error Log* (viz kapitola 7.7) — zkuste zvýšit prioritu procesu

Show NetMon in Volba, jak má být prohlížecí program *Kerio Network Monitor* zobrazován: *Taskbar only* (pouze na liště), *System tray only* (pouze jako ikonka v pravé části lišty) nebo *Both taskbar and system tray* (na obou místech).

Kapitola 7

Prohlížení a analýza naměřených dat

Kerio Network Monitor nabízí několik nástrojů pro zobrazení a analýzu naměřených dat. Tyto funkce lze zvolit z menu *View* nebo přímo ikonou na nástrojové liště (pořadí funkcí je v obou případech stejné):

Traffic chart Graf objemu přenesených dat. Umožňuje zobrazení objemu přenesených dat za vybrané období v několika grafických podobách. Odděleně je možno sledovat příchozí a odchozí data, jednotlivé počítače, skupiny apod.

Current connections Zobrazení aktuálních spojení z jednotlivých počítačů. Zobrazení v tomto okně se periodicky obnovuje.

Tapped data Zobrazení zachycených dat jednotlivých protokolů (WWW stránky, e-mailové zprávy, FTP relace atd.)

Status window Stav služby *Kerio Network Monitor Daemon* (přihlášený uživatel, statistika zachycených paketů, diskový prostor obsazený uloženými daty...)

Report Vytvoření přehledné tabulky objemu přenesených dat dle zadaných parametrů (časové období, druh provozu, úroveň podrobnosti...)

Connection log Zobrazení záznamu o spojeních z jednotlivých počítačů (historie okna *Current connections*)

HTTP log Záznam požadavků na WWW stránky z jednotlivých počítačů, příp. všech HTTP objektů (viz kapitola 6.7)

Mail log Záznam o zachycených e-mailových zprávách (e-mailová adresa odesílatele a příjemce, předmět a velikost zprávy)

ICQ log Záznam zachycených ICQ zpráv (ICQ čísla a přezdívky uživatelů a obsah zprávy)

Error log Záznam chyb a varovných hlášení. Správce *Kerio Network Monitoru* by měl tento zázname pravidelně sledovat a snažit se zjištěné chyby a problémy eliminovat.

KNM access log Záznam o přihlašování uživatelů do prohlížecího programu a přístupech ke stránkám WWW rozhraní. Každý řádek záznamu obsahuje datum, čas a informaci:

- o přihlášení uživatele (uživatelské jméno a DNS jméno nebo IP adresu počítače, ze kterého se přihlašuje)

  Poznámka: Zaznamenávají se i neúspěšné pokusy o přihlášení — ze záznamu lze např. zjistit, že se ke službě *Network Monitor Daemon* pokoušela přihlásit neoprávněná osoba.

- o požadavku na stránku WWW rozhraní (DNS jméno nebo IP adresa klientského počítače, jméno uživatele, HTTP metoda a adresa požadované stránky)

Všechny výše popsané funkce se chovají následujícím způsobem:

- Není-li příslušné okno dosud otevřeno, pak se po kliknutí na ikonu (či výběrem volby z menu) toto okno zobrazí.
- Je-li příslušné okno již otevřeno, pak se aktivuje a přesune do popředí.
- Zvolíte-li funkci při současném držení klávesy *Shift*, zobrazí se nové okno pro tuto funkci.

Tip: Třetím z popsaných způsobů je např. možno zobrazit pod sebou či vedle sebe grafy pro příchozí a odchozí provoz.

7.1 Seznam počítačů

Levý sloupec hlavního okna programu *Kerio Network Monitor* zobrazuje seznam jednotlivých počítačů v lokální síti. Tento seznam je vytvářen automaticky na základě údajů ze zachycených paketů. Počítač je do seznamu zařazen, jestliže jsou splněny tyto podmínky:

- IP adresa počítače patří do skupiny *LAN* (viz kapitola 6.1)
- *Kerio Network Monitor* již zachytil alespoň jeden paket, v jehož hlavičce byla tato IP adresa obsažena (jako zdrojová nebo cílová adresa) — tím se dozví, že v lokální síti existuje počítač s touto IP adresou.

Je-li to možné, je detekovaná IP adresa převedena na jméno počítače (reverzním DNS dotazem) a toto jméno zobrazeno, v opačném případě bude v seznamu počítačů zobrazena přímo detekovaná IP adresa.

Použití seznamu počítačů

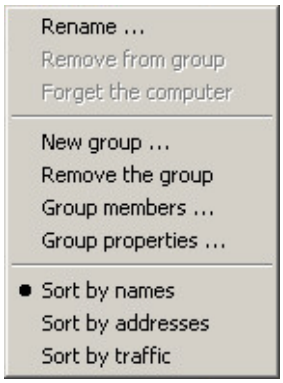
Seznam počítačů má význam pro zobrazení grafu (viz kapitola 7.2) a tabulky objemu přenesených dat (viz kapitola 7.6). Tyto funkce mohou zobrazovat údaje buď za všechny počítače v lokální síti (*All computers*) nebo pouze za vybraný počítač (resp. počítače). Počítače v seznamu je možno řadit do skupin (viz dále). Jeden počítač může být současně členem více skupin.

Počítač (resp. skupinu počítačů) je možno vybrat kliknutím myší na jeho název. Více počítačů (a / nebo skupin) lze vybrat při současném držení klávesy *Shift*. Kruhové pole vedle názvu počítače (či skupiny) zobrazuje, zda byl vybrán či nikoliv.

Vybraným počítačům bude automaticky přidělena barva (dostatečně kontrastní vůči pozadí grafu a ostatním, již použitým barvám). Touto barvou se budou v grafu odděleně zobrazovat hodnoty pro vybranou množinu počítačů.

Údržba seznamu počítačů

Po kliknutí pravým tlačítkem v seznamu počítačů, resp. přímo na vybraném počítači nebo skupině, se zobrazí menu s funkcemi pro seznam počítačů.



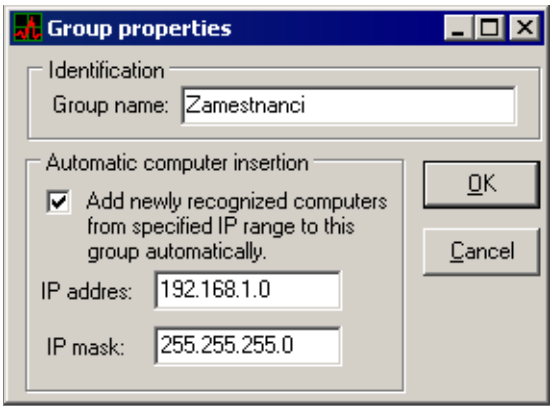
Rename Přejmenování vybrané skupiny nebo počítače. Tato funkce má význam zejména u počítačů — automaticky detekované jméno nemusí být vždy dostatečně popisné nebo není známo vůbec (v seznamu se zobrazuje IP adresa).

Remove from group Vyjmutí vybraného počítače ze skupiny, do níž náleží.

Forget the computer Odstranění vybraného počítače se seznamu. Tato funkce může být užitečná např. při trvalém odpojení počítače ze sítě či změně IP adresy.

Poznámka: Bude-li kdykoliv později zachycen paket s příslušnou IP adresou, počítač bude opět automaticky přidán.

New group Vytvoření nové skupiny. Dialog pro vytvoření či změnu skupiny obsahuje následující parametry:



- *Group name* — název skupiny. Měl by být dostatečně popisný (tzn. vyjadřovat obecně typ počítačů, které budou do této skupiny přidávány).
- *Add newly recognized computers* — po zapnutí této volby budou všechny nově detekované počítače (IP adresy) ze zadané subsítě automaticky přidají do této skupiny. Zadejte požadovanou subsíť s příslušnou maskou.

  Poznámka: Tato volba může být zapnuta u více skupin současně, a to i pro tutéž subsíť.

Remove the group Odstranění vybrané skupiny ze seznamu. Tato volba neodstraňuje počítače, které skupina obsahuje, pouze zruší jejich členství v této skupině.

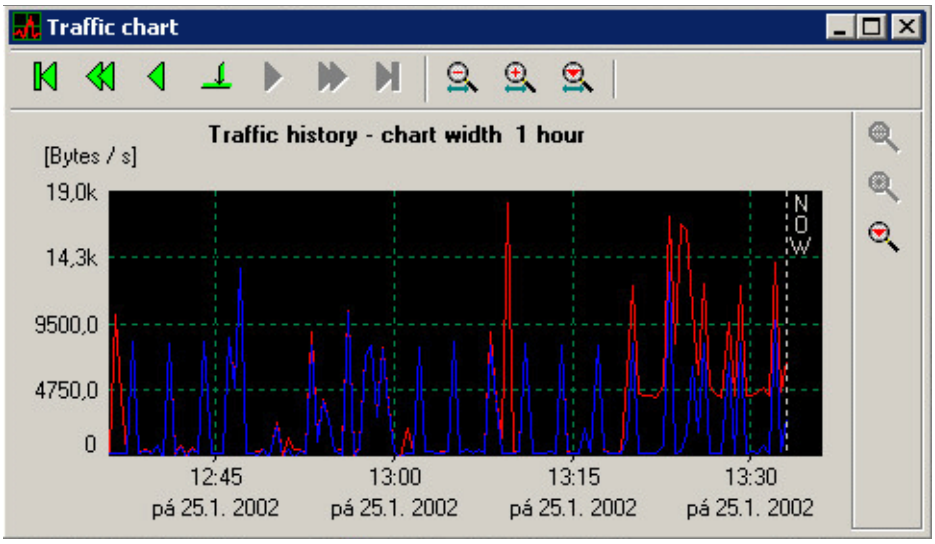
Group members Jednoduchý dialog pro přidávání či odebírání počítačů z/do vybrané skupiny.

Group properties Dialog pro změnu parametrů vybrané skupiny (shodný s dialogem pro vytvoření nové skupiny — viz výše).

Řazení počítačů v seznamu Poslední tři volby v menu určují, jak bude seznam počítačů řazen: dle jmen (*Sort by names*), dle IP adres (*Sort by addresses*) nebo sestupně dle objemu přenesených dat (*Sort by traffic*).

7.2 Graf objemu přenesených dat

Volba *Traffic chart* zobrazuje graf přenesených dat. Na vodorovné ose grafu je čas, na svislé pak zatížení linky (v bytech za sekundu).



Šipková tlačítka nad grafem slouží k posunu po vodorovné ose (v pořadí zleva doprava):

- Skok na začátek grafu (tj. celého období, za které byla data měřena)
- Dlouhý skok vzad
- Krátký skok vzad
- Skok na zadanou pozici (datum a čas)
- Krátký skok vpřed
- Dlouhý skok vpřed
- Skok na konec grafu (tj. aktuální čas)

  Poznámka: Délka krátkého a dlouhého skoku závisí na nastaveném měřítku grafu.

Tlačítka s lupou nad grafem nastavují měřítko vodorovné osy — tj. časový úsek, který bude v grafu zobrazen. Rozsah zobrazeného úseku může být v rozmezí 1 minuta až 1 rok.

Tlačítka s lupou vpravo vedle grafu nastavují měřítko svislé osy. Navíc je zde k dispozici volba *Auto*, která automaticky přizpůsobuje měřítko této osy největší naměřené hodnotě v daném zobrazení (tato volba je zapnuta ve výchozím nastavení). Tím je trvale zajištěna dobrá přehlednost grafu.

Stiskem pravého tlačítka myši na ploše grafu se zobrazí menu s dalšími volbami:

Save chart as picture Uložení grafu jako obrázku ve formátu JPEG nebo BMP.

Zoom in, Zoom out Zvětšení / zmenšení měřítka vodorovné osy (časového úseku). Tyto volby mají stejný účinek jako tlačítka „lupa +“ a „lupa -“ nad grafem.

Režim zobrazení Uživatel má možnost přepínat mezi následujícími režimy zobrazení:

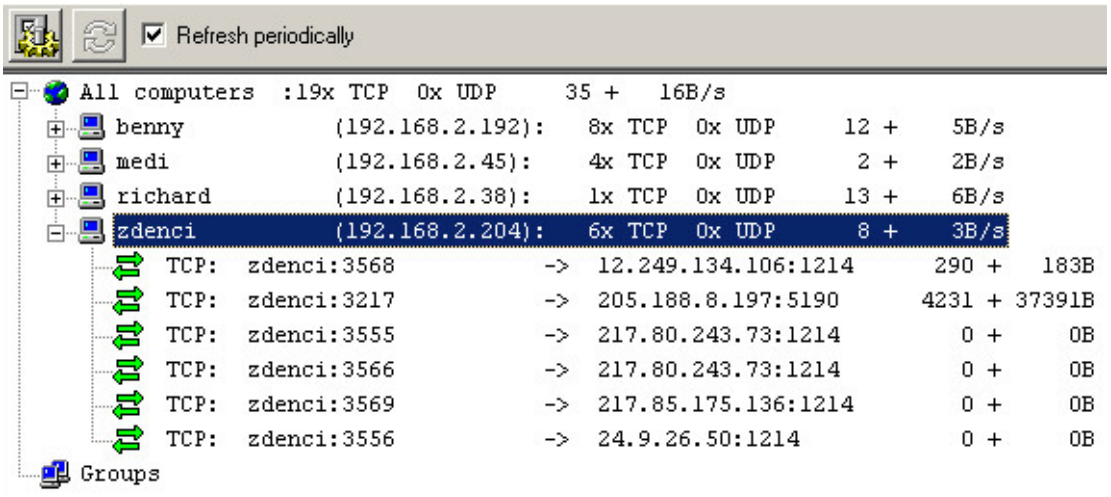
- *Sum of incoming and outgoing traffic* — v grafu bude zobrazována jedna křivka představující součet objemu odchozích a příchozích dat (výchozí nastavení)
- *Incoming traffic* — graf bude zobrazovat pouze objem příchozích (stažených) dat
- *Outgoing traffic* — graf bude zobrazovat pouze objem odchozích (odeslaných) dat
- *Both directions at once* — v grafu budou odděleně zobrazeny dvě křivky — jedna pro příchozí a druhá pro odchozí provoz

Typ grafu Graf může být zobrazován v jedná z následujících podob:

- *Draw lines* — křivka (výchozí nastavení)
- *Draw bars* — sloupcový graf
- *Draw polygons* — plošný graf (vyplněná plocha pod křivkou)

7.3 Zobrazení aktivních spojení

Volba *Current connections* zobrazuje okno aktivních spojení. Toto okno obsahuje informace o aktuálních TCP spojeních, příp. UDP a ICMP pseudospojeních z jednotlivých stanic v lokální síti.



Zobrazení v okně *Current connections* má tvar stromu se dvěma základními položkami:

- *All computers* — pod touto položkou se zobrazují všechny počítače, které má *Kerio Network Monitor* ve své databázi (viz kapitola 7.1).
- *Groups* — zde se zobrazují jednotlivé skupiny (definované v seznamu počítačů).

V okně *Current connections* se zobrazují pouze ty počítače (resp. skupiny), které mají aktuálně otevřeno alespoň jedno spojení (neaktivní počítače se nezobrazují).

Pod každou skupinou se dále zobrazují jednotlivé počítače v ní obsažené, a pod každým počítačem jednotlivá spojení tohoto počítače. Záznam pro konkrétní spojení má následující podobu:

```
TCP: zdenci:3568 -> 12.249.134.106:1214 290 + 183B 13 + 23B/s 3 /
2s Active *unknown*
```

- `TCP:` — komunikační protokol (TCP, UDP nebo ICMP)
- `zdenci:3568` — jméno (příp. IP adresa) počítače v lokální síti (typicky klienta) a číslo portu
- `12.249.134.106:1214` — jméno či IP adresa počítače v Internetu (typicky serveru) a cílový port
- `290 + 183B` — objem odeslaných a přijatých dat (v bytech)
- `13 + 23B/s` — rychlost přenosu odchozích (odeslaných) a příchozích (přijatých) dat (v bytech za sekundu)
- `2 + 3s` — doba posledního přenosu dat a celková doba otevření spojení (v sekundách)
- `Active` — stav spojení (`Syncing` — navazuje se, `Active` — aktivní / otevřené, `Closing by initiator` — ukončováno klientem, `Closing by responder` — ukončováno serverem, `Closed` — ukončeno, `!!! ERROR !!!` — ukončeno z důvodu chyby).

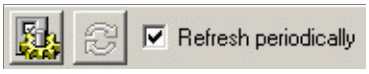
  Uzavřená spojení zůstávají v okně *Current connections* zobrazena po dobu nastavenou v konfiguraci programu (viz kapitola 6.5).

  Chyba nastává v případě, že se ztratí některý paket ze spojení a spojení se rozsynchronizuje (následně zaniká a případně je navázáno nové).
- `*unknown*` — název služby (je-li v *Kerio Network Monitoru* definována — např. `SMTP`, `HTTP`, `FTP` atd.) nebo `*unknown*` (neznámá služba)

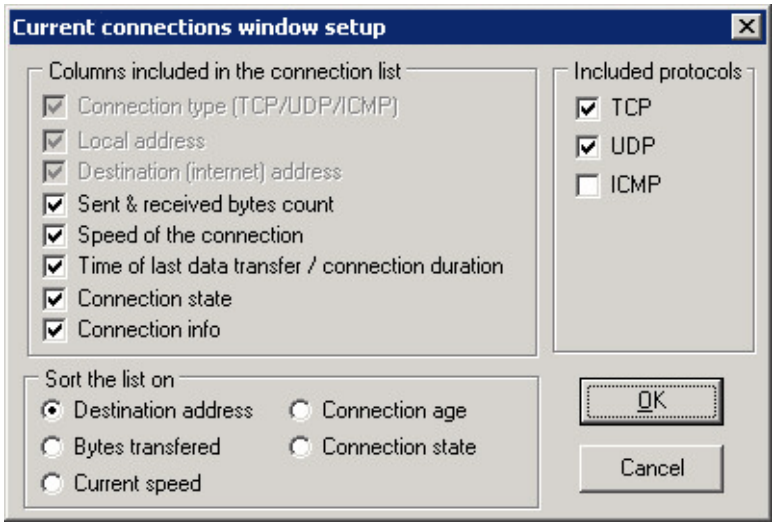
Poznámka: Jména počítačů v Internetu zjišťuje *Kerio Network Monitor* analýzou protokolu DNS. To je možné provést pouze v případě, že byl před zahájením spojení vyslán DNS dotaz. Má-li klient tyto informace ve své lokální DNS cache, DNS dotaz se nevysílá a *Kerio Network Monitor* „vidí“ pouze IP adresu cílového serveru.

Funkce okna aktivních spojení

Nástrojový pruh okna *Current connections* obsahuje následující funkce a volby (v pořadí zleva doprava):



Select columns & setup sorting Toto tlačítko otevírá dialog pro nastavení parametrů okna *Current connections*.



Columns included in the connection list V této sekci je možno vybrat sloupce (informace), které budou v okně *Current connections* zobrazovány.

- *Connection type* — typ spojení (TCP spojení nebo UDP či ICMP pseudospojení)
- *Local address* — jméno nebo IP adresa lokálního (zdrojového) počítače a zdrojový port
- *Destination* — jméno nebo IP adresa vzdáleného (cílového) počítače a cílový port

Výše uvedené tři funkce zobrazují základní informace o spojení a nelze je proto vypnout (skrýt).

- *Sent & received bytes count* — počet odeslaných a přijatých bytů
- *Speed of the connection* — rychlost přenosu dat (v příchozím a odchozím směru)
- *Time of last data transfer / connection duration* — doba trvání posledního přenosu dat a celková doba otevření spojení
- *Connection state* — stav spojení (aktivní, ukončené atd.)
- *Connection info* — informace o službě (je-li v programu definována)

Included protocols Volba protokolů, které mají být v okně aktivních spojení sledovány. Výchozí nastavení zahrnuje protokoly TCP a UDP.

Sort the list on Volba položky, podle které má být výpis v okně řazen (*Destination address* — cílová IP adresa, *Bytes transferred* — objem přenesených dat, *Current speed* — rychlost spojení, *Connection age* — doba trvání spojení, *Connection state* — stav spojení).

Refresh now Obnovení (aktualizace) informací v okně *Current connections*.

Refresh periodically Zapnutím této volby se budou informace v okně *Current connections* automaticky obnovovat v pravidelných intervalech (každou 1 sekundu).

7.4 Strom zachycených dat

Volba *Scanned data* otevírá okno, v němž je možno prohlížet zachycená data jednotlivých služeb (WWW stránky, e-mailové zprávy, FTP relace atd.).

Strom dat (v levé části okna) obsahuje dvě základní větve:

- *By client* — data řazená dle IP adres klientů (tj. počítačů v lokální síti)
- *By protocol* — data řazená dle jednotlivých protokolů (služeb)

Obě tyto větve obsahují zcela identická data — liší se jen způsobem jejich řazení.

Rozbalením vybrané větve stromu a kliknutím na konkrétní objekt (např. WWW stránku na daném serveru) se tento objekt zobrazí v pravé části okna.

Poznámka: Obsah e-mailových zpráv se zobrazuje pouze tehdy, není-li to v konfiguraci programu zakázáno (viz kapitola 6.7).

Poznámka 2: V případě WWW stránek ukládá *Kerio Network Monitor* příslušné URL a obsah stránky (HTML kód bez obrázků, aplikací atd.). Zobrazení stránky se provádí tak, že je otevřen tento kód a příslušné objekty se stahují přímo ze serveru (tedy stejně jako při přístupu prohlížečem).

Funkce okna zachycených dat

Nástrojový pruh okna *Scanned data* obsahuje následující funkce a volby (v pořadí zleva doprava):

Stop current transfer Zastavení přenosu otevírané WWW stránky (jako v prohlížeči)

Refresh tree Obnovení informací ve stromu (od okamžiku otevření okna *Scanned data* mohla být zachycena nová data).

Tuto funkci lze rovněž vyvolat stiskem klávesy *F5*.

Max age Maximální stáří dat, která mají být ve stromu zobrazena (v rozsahu 5 minut až jeden týden, příp. neomezené stáří — **unlimited**). Volba maximálního stáří dat výrazně ovlivňuje velikost a přehlednost stromu.

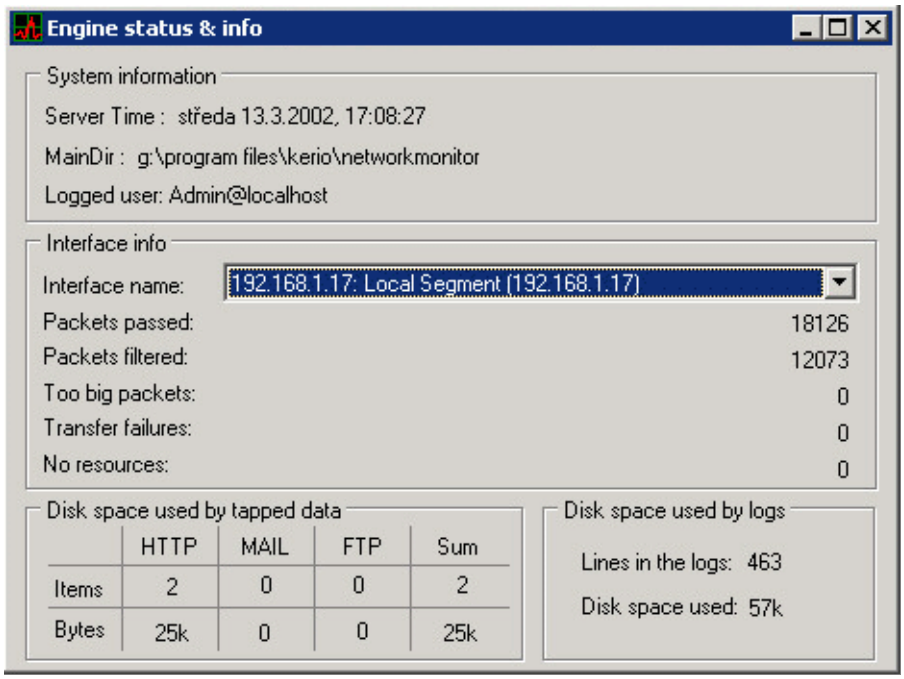
Show formatted Zobrazení WWW stránky či e-mailové zprávy formátovaně

Show as plain text Zobrazení WWW stránky či e-mailové zprávy v textové podobě (zdrojový text)

Open as document Otevření stránky či zprávy jako dokumentu (ve výchozím WWW prohlížeči nebo e-mailovém klientu)

7.5 Stavové informace

Okno *Status window* zobrazuje informace o systému, na němž *Kerio Network Monitor Daemon* běží, o jednotlivých síťových rozhraní a diskovém prostoru obsazeném databází naměřených dat.



System information Systémové informace (aktuální čas serveru, instalační adresář a aktuálně přihlášený uživatel). Přihlášený uživatel se zobrauje ve tvaru `jméno@server`, kde `server` je DNS jméno nebo IP adresa počítače, na němž běží služba *Kerio Network Monitor Daemon* (k níž je uživatel připojen).

Interface info Statistické informace o jednotlivých rozhraních, na nichž *Kerio Network Monitor* zachytává pakety. Všechny tyto informace jsou počítány od startu služby *Kerio Network Monitor Daemon*. Restartem služby se tyto statistiky nulují.

- *Interface name* — výběr rozhraní, pro něž mají být statistiky zobrazeny. V této nabídce jsou všechna rozhraní, která byla vybrána pro sledování paketů při konfiguraci programu (viz kapitola 6.1).
- *Packets passed* — celkový počet paketů, které byly předány *Daemonu* ke zpracování (jejich zdrojová a cílová adresa patří do různých skupin)
- *Packets filtered* — počet paketů, které byly filtrovány (zahozeny) — jejich zdrojová a cílová adresa patří do stejné skupiny, nebo některá z těchto adres patří do skupiny *Discard packet* (viz kapitola 6.1)
- *Too big packets* — počet paketů, které nemohly být zpracovány, protože jejich velikost přesahovala maximální velikost vyrovnávací paměti nízkoúrovňového ovladače *Kerio Network Monitoru*. Zvýšený počet těchto paketů může indikovat systémovou chybu nebo pokus o útok.
- *Transfer failures* — počet paketů, které se nepodařilo zkopírovat z interní vyrovnávací paměti síťového adaptéru. Tato chyba by za normálních okolností neměla nastávat (může indikovat problém s adaptérem nebo jeho ovladačem).
- *No resources* — počet paketů, které nemohly být zpracovány z důvodu nedostatku systémových prostředků.

  Dosahuje-li tato hodnota řádu tisíců a vyšších, měl by být *Kerio Network Monitor* instalován na výkonnější počítač, případně na počítač, u něhož nepracuje žádný uživatel.

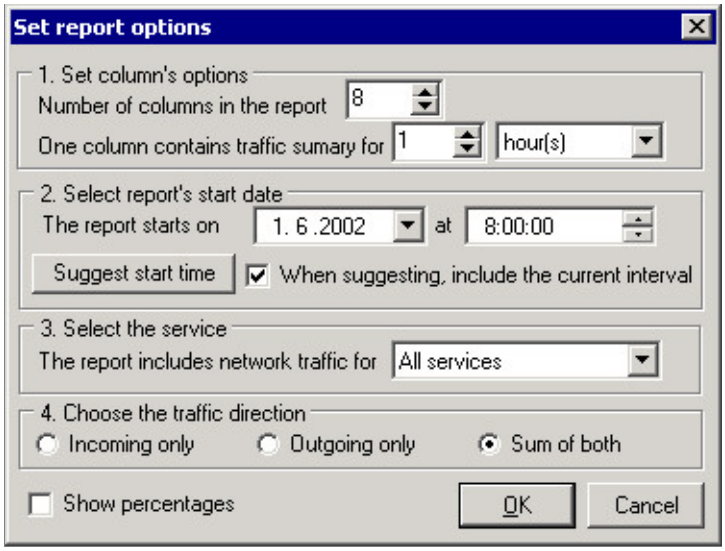
Disk space used by scanned data Velikost diskového prostoru zabraného zachycenými daty jednotlivých služeb. Zobrazuje se počet objektů (*Items*) a bytů (*Bytes*). Sloupec *Sum* obsahuje celkový prostor (součet všech služeb).

Poznámka: Uvedené údaje nezahrnují místo obsazené databází objemu přenesených dat (tj. podadresáře `high` a *low*).

Disk space used by logs Celkový diskový prostor obsazený soubory záznamů a celkový počet řádek v těchto souborech.

7.6 Tabulka objemu přenesených dat

Funkce *Report* zobrazuje oknou s tabulku objemu přenesených dat dle zadaných parametrů. Není-li okno otevřeno, zobrazí se nejprve dialog pro nastavení těchto parametrů:



Set column's option Základní údaje o rozsahu tabulky:

- *Number of columns* — počet sloupců tabulky
- *One column contains traffic sumary* — časové období, které má být obsaženo v jednom sloupci

Kombinace těchto dvou parametrů určuje celkový rozsah tabulky.

Příklad: Chceme zobrazit objem přenesených dat za týden po jednotlivých dnech. Do položky *Number of columns* zadáme hodnotu *7* (týden má obvykle 7 dní) a v položce *One column contains traffic sumary* nastavíme *1 day(s)* (1 den).

Select report's start date Nastavení počátečního data a času (od kdy mají být data vyhodnocována). Od tohoto data se vyhodnotí období nastavené v předchozí sekci. Tlačítko *Suggest start date* nastaví počáteční čas tak, aby nastavené období končilo aktuálním časem.

Příklad: Nastavíme-li rozsah tabulky dle předchozího příkladu, tlačítko *Suggest start date* nastaví datum a čas před sedmi dny (tzn. výsledná tabulka bude zobrazovat posledních 7 dní).

Volba *When suggesting, include the current interval* určuje, zda má doporučený počáteční čas zahrnovat i aktuální interval (který dosud není ukončen).

Příklad: Dnes je sobota 1. 6. 2002, 12:00 hodin. Uvažujme nastavení intervalu v předchozím příkladě (tj. údaje za jeden týden po jednotlivých dnech). Tlačítko *Suggest start time* nastaví jako datum minulou sobotu (tj. 25. 5. 2002). Tabulka tedy bude obsahovat údaje za období sobota 25. 5. 2002 — pátek 31. 5. 2002. Zaškrtneme-li

volbu *When suggesting, include the current interval*, bude doporučené datum neděle 26. 5. 2002 a tabulka bude obsahovat údaje za období neděle 26. 5. 2002 — sobota 1. 6. 2002. Poslední sloupec tabulky bude tedy obsahovat údaje za část dnešního dne, která již uplynula (tj. 0:00 — 12:00 hodin). Je zřejmé, že necháme-li vytvořit tabulku se stejnými parametry např. v 18:00 hodin, údaje v posledním sloupci se budou lišit.

Select the service Volba služby, jejíž data budou v tabulce zobrazena. Je možno vybrat konkrétní službu (např. *HTTP*, *SMTP*, *FTP* apod.) nebo všechny služby (*All services*).

Choose the traffic direction Volba směru dat, která mají být zaznamenána: *Incoming only* (pouze příchozí data), *Outgoing only* (pouze odchozí data) nebo *Sum of both* (součet odchozích a příchozích dat).

Show percentages Zobrazit procenta namísto objemu přenesených dat u jednotlivých počítačů. Bude-li tato volba zapnuta, pak se v tabulce zobrazí pouze celkový objem přenesených dat za příslušná období (řádka *All computers*) a u jednotlivých počítačů bude zobrazen jejich procentuální podíl na tomto objemu.

Po stisku tlačítka *OK* se vytvoří a zobrazí tabulka dle zadaných parametrů.

Funkce pro tabulku objemu dat

Nástojový pruh okna *Accounting report* nabízí následující funkce (v pořadí zleva doprava):

Change report parameters Změna parametrů tabulky. Tato volba zobrazí dialog pro nastavení tabulky (viz výše) a poté je vytvořena a zobrazena nová tabulka.

Print the report Tisk tabulky. Tato volba otevře standardní systémový dialog pro tisk, kde je možno zvolit tiskárnu atd.

Save the report Uložení tabulky ve formě HTML stránky nebo formátu *CSV* (Comma Separated Values — čísla oddělená čárkami). Formát *CSV* je poměrně rozšířený a může být zpracován řadou programů (např. Microsoft Excel).

Sort the table Seřazení tabulky podle vybraného sloupce. Tato volba může být použita opakovaně — není třeba tabulku znovu vytvářet.

Transfer the table to MS Excel Je-li na počítači, kde je spuštěn prohlížecí program, instalována aplikace *Microsoft Excel*, pak lze stiskem tohoto tlačítka tabulku přímo přenést do této aplikace. *Microsoft Excel* nabízí široké možnosti dalšího zpracování naměřených dat.

7.7 Okna záznamů

Okna všech záznamů (*Connection Log*, *HTTP Log*, *Mail Log* a *Error Log*) mají nástrojovou lištu s těmito funkcemi (v pořadí zleva doprava):

Copy selection to clipboard Zkopírování vybraného textu do schránky (v okně lze myší označit libovolnou část textu). Tuto funkci lze také vyvolat standardní klávesovou zkratkou *Ctrl+C*.

Save log to file Uložení záznamu do textového souboru v textovém formátu (`*.txt`) nebo formátu *LOG* (`*.log`). Tuto funkci lze také vyvolat klávesovou zkratkou *Ctrl+W*.

Obecně lze říci, že formát *LOG* je vhodnější pro automatické zpracování, zatímco textový formát je lépe čitelný pro uživatele. V případě záznamu HTTP Log znamená formát *LOG* standardní (unixový) log, a textový formát zachovává podobu, v jaké je záznam vidět na obrazovce. U všech ostatních záznamů se ve formátu *LOG* uvádějí výhradně IP adresy, v textovém formátu jsou nahrazeny jmény počítačů (jsou-li známa).

Show only lines passing the rule Filtrování záznamu. Umožňuje zobrazení pouze řádek obsahujících zadaný řetězec. Takto je možno zobrazit např. část záznamu vztahující se k určitému datu.

Čtení a analýza záznamů

Každá řádka záznamu obsahuje informace o jedné události (např. o e-mailové zprávě, HTTP požadavku, chybovém hlášení atd.).

Záznamové zoubory mohou být dále zpracovávány externími analytickými nástroji (např. programem *Kerio Log Analyzer* — viz `www.kerio.com`).

Connection Log

```
TCP: richard:1524 -> 205.107.97.6:80 171 + 2927By,
```

```
2s -HTTP:205.107.97.6
```

- `Fri 8/Mar/2002 10:18:31` — datum a čas vzniku (zahájení) spojení
- `TCP:` — použitý komunikační protokol transportní úrovně (*TCP/UDP*)
- `richard:1524` — jméno či IP adresa klienta (počítače, který spojení zahájil) a zdrojový port
- `205.107.97.6:80` — jméno či IP adresa cílového počítače (serveru) a cílový port
- `171 + 2927By` — objem vyslaných (`171`) a přijatých (`2927`) dat v bytech (`By`)
- `2s` — doba trvání spojení (v sekundách)
- `-HTTP:205.107.97.6` — popis služby (jedná-li se o službu, která je v *Kerio Network Monitoru* definována). Tento zápis znamená „služba HTTP na severu s IP adresou 205.107.97.6“. Jestliže *Kerio Network Monitor* danou službu nezná, zobrazí se hlášení `-unknown service`.

Poznámka: Jména počítačů v Internetu zjišťuje *Kerio Network Monitor* analýzou protokolu DNS. To je možné provést pouze v případě, že byl před zahájením spojení vyslán DNS dotaz. Má-li klient tyto informace ve své lokální DNS cache, DNS dotaz se nevysílá a *Kerio Network Monitor* „vidí“ pouze IP adresu cílového serveru.

HTTP Log

```
richard - Fri 8/Mar/2002 11:57:46
GET http://www.kerio.com/resources/home.gif
HTTP/1.1 200 1221
```

- `richard` — jméno (příp. IP adresa) klienta (tj. počítače, který HTTP požadavek vyslal)
- `Fri 8/Mar/2002 11:57:46` — datum a čas požadavku
- `GET` — metoda protokolu HTTP (*GET/POST*)
- `http://www.kerio.com/resources/home.gif` — kompletní URL požadovaného objektu
- `HTTP/1.1` — verze protokolu HTTP (v současné době `1.0` nebo `1.1`)

- 200 — návratový kód protokolu HTTP (viz dokument *RFC2068* — www.ietf.org/rfc)
- 1221 — velikost objektu (v bytech)

Mail Log

```
richard - Fri 8/Mar/2002 14:26:01 SMTP From:"Richard Gabriel"
<richard@kerio.com>, to:<info@zaluzi.cz>, subj:Objednavka, 43
lines, 1366 bytes
```

- richard — jméno (příp. IP adresa) klienta (tj. počítače, který se připojoval k poštovnímu serveru)
- Fri 8/Mar/2002 14:26:01 — datum a čas přenosu zprávy
- SMTP — použitý poštovní protokol (*SMTP*, *POP3* nebo *IMAP*)
- From: ... — e-mailová adresa odesílatele zprávy (příp. i jeho osobní jméno, bylo-li uvedeno)
- to: ... — e-mailová adresa příjemce zprávy (příp. i jeho osobní jméno, bylo-li uvedeno)
- subj: ... — předmět zprávy
- 43 lines — počet řádek v těle zprávy
- 1366 bytes — celková velikost zprávy (v bytech)

Error Log

```
Fri 8/Mar/2002 14:59:59 Warn - 192.168.2.38:
 5 packets lost - lack of resources (61-56)
Fri 8/Mar/2002 15:02:11 Warn - (192.168.2.40 -> 201.7.55.112)
 Connection has died
Fri 8/Mar/2002 15:17:22 Err: 206 - Error creating file
'c:\Program Files\Kerio\Network Monitor\logs\mail.idx'
```

- Fri 8/Mar/2002 14:26:01 — datum a čas, kdy byla chyba zaznamenána
- Warn — typ hlášení (Warn — varovné hlášení nebo Err: xxx — chybové hlášení včetně kódu chyby)

Varovná hlášení znamenají chyby, které nemají závažný charakter. Správce *Kerio Network Monitoru* by však neměl ani tato hlášení ignorovat a měl by se snažit veškeré chyby neprodleně odstranit.

- `192.168.2.38` — IP adresa počítače, kde byla chyba zaznamenána. Zde mohou být rovněž uvedeny adresy zdroje a cíle spojení, v němž byla chyba zaznamenána
- `5 packets lost - lack of resources (61-56)` — podrobný popis chyby (v tomto případě: ztráta paketů z důvodu nedostatku systémových zdrojů)

Poznámka: Chybových zpráv a varovných hlášení, které se mohou v záznamu *Error Log* objevit, existuje velmi značné množství a jejich popis je nad rámec tohoto manuálu. Nedokážete-li nějakou chybu odstranit svépomocí, kontaktujte prosím oddělení technické podpory *Kerio Technologies* — viz `www.kerio.com`.

Kapitola 8

WWW rozhraní

Kerio Netwok Monitor nabízí přístup k naměřeným datům pomocí jednoduchého WWW rozhraní. Toto rozhraní umí zobrazit graf zatížení linky, aktivní spojení a záznamy a vytvořit tabulku objemu přenesených dat dle zadaných parametrů.

WWW rozhraní funguje ve dvou režimech: anonymně nebo s přihlášením.

- V anonymním režimu může uživatel prohlížet pouze údaje pro počítač, z něhož se připojuje (případně sumární údaje pro celou síť, je-li to povoleno). Předpokládá se, že uživatel se k tomuto rozhraní bude připojovat ze „svého“ počítače, a uvidí tedy údaje právě o tomto počítači
- Přihlášený uživatel může prohlížet veškeré údaje, které má *Kerio Netwok Monitor* k dispozici (tj. o všech počítačích v lokální síti).

8.1 Připojení k WWW rozhraní

Pro připojení k WWW rozhraní *Kerio Netwok Monitoru* je třeba do prohlížeče zadat DNS jméno počítače, na němž běží *Kerio Netwok Monitor Daemon* (případně jeho IP adresu, pokud není v DNS zanesen) a specifikovat port, na němž WWW rozhraní běží (standardně *81*). Konkrétní URL tedy bude vypadat např.:

```
http://server.firma.cz:81
```

nebo

```
http://192.168.1.1:81
```

Pokud na počítači, kde je instalován *Kerio Netwok Monitor Daemon*, neběží žádný jiný WWW server, je možno spustit WWW rozhraní na standarním portu *80* (viz kapitola 6.6) — pak nebude nutno v URL port specifikovat:

```
http://server.firma.cz
```

nebo

```
http://192.168.1.1
```

Přihlášení uživatele

Ve WWW rozhraní *Kerio Netwok Monitoru* není přihlášení uživatele explicitně vyžadováno. Ihned po připojení se rozhraní nachází v tzv. anonymním režimu (viz výše).

Chcete-li zobrazovat údaje o všech počítačích v lokální síti, přihlašte se v sekci *login*. Po úspěšném přihlášení budou dostupné informace o všech počítačích, v opačném případě zůstane WWW rozhraní i nadále v anonymním režimu.

8.2 Stránka *main*

Tato sekce zobrazuje informace o systému, na němž *Kerio Network Monitor Daemon* běží (systémový čas, údaje o licenci, obsazený diskový prostor...).

Informace na této stránce (s výjimkou několika detailů) odpovídají oknu *Engine status & info* — viz kapitola 7.5.

8.3 Stránka *chart*

Stránka *chart* zobrazuje graf objemu přenesených dat (jako okno *Traffic chart* — viz kapitola 7.6).

Pro nastavení parametrů grafu slouží volby v levé části stránky:

Select red / blue / green serie Graf na této WWW stránce umí zobrazit maximálně 3 křivky (červenou, modrou a zelenou). Pro každou křivku je možno zvolit typ informace, kterou má zobrazovat. Možnosti jsou následující:

- *All computers* — celkový objem přenesených dat za všechny počítače
- Název počítače nebo skupiny — objem přenesených dat pro vybraný počítač nebo skupinu
- *<none>* — křivka nebude v grafu zobrazena. Tato volba je dostupná pouze u druhé a třetí (tj. zelené a modré) křivky.

Select chart width Volba časového úseku, který má být v grafu zobrazen (1 minuta až 1 rok).

Show Zobrazení grafu dle zvolených parametrů.

Na grafem je zobrazena řada tlačítek pro pohyb po vodorovné ose grafu. Prostřední tlačítko *Refresh* slouží k obnovení grafu (z technických důvodů se graf na WWW stránce automaticky neobnovuje).

8.4 Stránka *report*

Tato stránka odpovídá oknu *Accounting report*. Po jejím otevření se nejprve zobrazí volby pro nastavení parametrů tabulky:

Select format Výběr formátu tabulky (HTML stránka nebo soubor ve formátu *CSV*)

Specify report parameters Nastavení parametrů tabulky (viz kapitola 7.6).

Show the report Zobrazení tabulky objemu přenesených dat dle zadaných parametrů.

8.5 Stránka *connections*

Tato stránka zobrazuje aktivní spojení jednotlivých počítačů — ekvivalent okna *Current connections*. Zobrazení nelze konfigurovat.

Detaily o zobrazení aktivních spojení naleznete v kapitole 7.3.

8.6 Stránka *logs*

Tato stránka umožňuje zobrazení zvolených informací ze záznamů *HTTP Log*, *Mail Log* a *Connection Log* (záznam *Error Log* lze zobrazovat pouze v prohlížecím programu).

Select log Výběr záznamu (*HTTP Log*, *Mail Log* nebo *Connection Log*).

Specify log options Stanovení parametrů pro řádky záznamu, které mají být zobrazeny:

- *Show last ... days* — zobrazit pouze záznamy za posledních ... dnů. Tato volba výrazně ovlivňuje délku zobrazené stránky, proto doporučujeme zvolit jen období, které vás skutečně zajímá.
- *at most ... lines* — maximální počet zobrazených řádek
- *Show only lines containing ...* — zobrazit pouze řádky obsahující zadaný řetězec (pro zobrazení všech řádek ponechte toto pole prázdné)
- *Resolve IP addresses of local computers* — bude-li tato volba zapnuta, budou se lokální počítače zobrazovat DNS jménem (pokud existuje), v opačném případě se budou zobrazovat jejich IP adresy.

  Poznámka: Vzdálené počítače (tj. ty, které nepatří do lokální sítě) se zobrazují vždy pouze IP adresami.

Show the log Zobrazení řádek vybraného záznamu dle zadaných parametrů

8.7 Integrace WWW rozhraní do firemního webu

WWW rozhraní *Kerio Network Monitoru* umožňuje přístup k jednotlivým stránkám či jejich částem pomocí speciálních URL. Takto můžete do vašeho vlastního webu integrovat např. grafy zatížení linky, tabulky objemů přenesených dat, výpis aktivních spojení apod.

Obecný formát URL

URL stránek WWW rozhraní má obecně tento formát:

```
http://netmon:81/adresar/stranka
 ?parametr1=hodnota&parametr2=hodnota...
```

kde:

- `netmon` — DNS jméno nebo IP adresa počítače, na němž *Kerio Network Monitor* běží

  Poznámka: Při integraci do jiného webu je třeba brát v úvahu, zda se ke stránkám bude přistupovat z interní sítě, z Internetu či z obou stran. Nejvhodnější je uvést jméno serveru, pro něž existuje odpovídající záznam v interním i veřejném DNS.

- `81` — port, na němž běží WWW rozhraní *Kerio Network Monitoru* (viz kapitola 6.6)

- `adresar` — adresář virtuálního WWW serveru, kde je příslušná stránka uložena

- `stranka` — název stránky (viz dále)

- `parametr=hodnota` — název parametru a příslušná hodnota (viz dále). Parametry jsou nepovinné — nebude-li některý parametr uveden, bude do něj dosazena výchozí hodnota. Neznámý (neexistující) parametr bude ignorován. Některé stránky žádné parametry nevyžadují.

Poznámka: V názvech stránek a parametrů by měla být dodržena malá a velká písmena. Na pořadí parametrů nezáleží.

Veškeré operace budou prováděny s právy nepřihlášeného uživatele.

Zobrazení aktivních spojení

Stránku aktivních spojení (*Current connections*) zobrazíme pomocí URL:

```
http://netmon:81/conn.html
```

Tato stránka nemá žádné nastavitelné parametry.

Graf objemu přenesených dat

K zobrazení stránky s grafem objemu přenesených dat slouží následující URL:

```
http://netmon:81/chart/form.html
 ?resolution=1&IP1=1.2.3.4&IP2=5.6.7.8&IP3=10.11.12.13&service=1
```

kde:

- `resolution` — výběr časového úseku dle následující tabulky:

Hodnota	0	1	2	3	4
Význam	1 minuta	5 minut	15 minut	1 hodina	6 hodin

Hodnota	5	6	7	8
Význam	1 den	1 týden	1 měsíc	1 rok

- `IP1, IP2, IP3` — IP adresy, pro něž bude v grafu zobrazován objem přenesených dat (červeně, zeleně a modře — v tomto pořadí). Místo IP adresy konkrétního počítače lze také uvést adresu `0.0.0.0` (součet objemu dat za všechny počítače) nebo `127.0.0.1` (zpětnovazební adresa; bude nahrazena IP adresou počítače, z něhož byla stránka otevřena)
- `service` — výběr sledované služby:

Hodnota	0	1	2	3	4	5	6	7
Význam	Všechny služby	HTTP	POP3	SMTP	FTP	Telnet	IMAP4	SSH

Pro zobrazení samotného grafu (obrázku) použijte následující URL:

```
http://netmon:81/chart/image.png
```

Všechny výše popsané parametry zůstávají v platnosti.

Příklad:

```
http://netmon:81/chart/image.png
 ?resolution=3&IP1=0.0.0.0&IP2=127.0.0.1&service=1
```

zobrazí samotný graf pro období 1 hodina, červeně bude znázorněn objem přenesených dat za všechny počítače a zeleně pro počítač, z něhož stránky prohlížíme.

Tabulka objemu přenesených dat

Následující URL zobrazí tabulku objemu přenesených dat (*Report*) podle zadaných parametrů:

```
http://netmon:81/report/output.html
 ?interval=2&back=7&columnscount=7&columnswidth=1
 &sort=3&direction=3&service=0
```

kde:

- `interval` — základ šířky sloupce, násobí se parametrem `columnwidth`. Možné hodnoty jsou:

Hodnota	0	1	2	3	4	5
Význam	minuty	hodiny	dny	týdny	měsíce	roky

- `back` — počet časových období, o která se má *Network Monitor* „posunout zpět“ (nastavení začátku tabulky). Hodnota `0` znamená aktuální období.
- `columnscount` — počet sloupců v tabulce
- `columnswidth` — šířka sloupce. Součin tohoto parametru s parametrem `interval` udává časové období obsažené v jednom sloupci.
- `sort` — hodnota, podle které bude tabulka seřazena:

Hodnota	1	2	3
Význam	IP adresa	jméno počítače	objem přenesených dat

- `direction` — směr dat, který má být v tabulce zobrazen:

Hodnota	1	2	3
Význam	příchozí (download)	odchozí (upload)	součet dat v obou směrech

- `service` — služba, pro niž má být objem dat zobrazen (viz výše — sekce *Graf objemu přenesených dat*)

Správné nastavení parametrů tabulky nejlépe vysvětlí příklad.

```
http://netmon:81/report/output.html
 ?interval=2&back=1&columnscount=7&columnswidth=1
 &sort=3&direction=3&service=0
```

- `interval=2` — základní jednotkou šířky sloupce bude den
- `columnswidth=1` — šířka sloupce (časové období) bude 1 den

- `columnscount=7` — počet sloupců tabulky bude 7, celá tabulka tedy bude pokrývat časové období 7 dní (1 týden)
- `back=1` — časový posun o jedno období (tj. 1 týden) zpět. V důsledku to znamená, že tabulka bude zahrnovat období „-2 týdny až -1 týden“.
- `direction=3` — tabulka bude obsahovat součet příchozích i odchozích dat
- `service=0` — zobrazen bude celkový objem přenesených dat (pro všechny služby)

Záznamy

Pro zobrazení záznamů slouží URL:

```
http://netmon:81/log/output.html
 ?log=2&age=7&maxlines=1000&filter=text
```

kde:

- `log` — číslo záznamového souboru dle následující tabulky:

Hodnota	2	3	4
Význam	HTTP Log	Connection Log	Mail Log

- `age` — maximální stáří záznamu (v dnech)
- `maxlines` — maximální počet řádek ve výstupu (vyhovuje-li ostatním podmínkám více řádek, zobrazí se pouze nejnovější záznamy)
- `filter` — hledaný text. Ve výstupu budou zobrazeny pouze řádky záznamu obsahující tento text.

Kapitola 9

Slovníček pojmů

E-mailová adresa Určuje příjemce a odesílatele zprávy při komunikaci elektronickou poštou.

HTTP Protokol pro přenos WWW stránek. Standardně používá protokol *TCP*, port *80*.

HTTPS Zabezpečená verze protokolu HTTP. Pro zabezpečení se používá šifrovací protokol SSL.

HTTPS standardně používá protokol *TCP*, port *443*.

IMAP Protokol umožňující klientům pracovat se svými e-mailovými zprávami na serveru, bez nutnosti stahování na lokální počítač.

IMAP standardně používá protokol *TCP*, port *143*.

Paket Datová jednotka síťové úrovně (tj. nezávislá na přenosovém médiu). V TCP/IP pracuje na paketové úrovni protokol IP.

POP3 Post Office Protocol je protokol, který umožňuje uživatelům stahovat e-mailové zprávy ze serveru na svůj lokální disk.

POP3 standardně používá protokol *TCP*, port *110*.

Port 16-bitové číslo (`1–65535`) používané protokoly TCP a UDP pro identifikaci aplikací (služeb) na daném počítači. Na jednom počítači (jedné IP adrese) může běžet více aplikací současně (např. WWW server, poštovní klient, WWW klient — prohlížeč, FTP klient atd.). Každá aplikace je však jednoznačně určena číslem portu. Porty `1–65535` jsou vyhrazené a používají je standardní, příp. systémové služby (např. `80` = WWW). Porty nad `1024` (včetně) mohou být volně použity libovolnou aplikací (typicky klientem jako zdrojový port nebo nestandardní aplikací serverového typu).

Protokol Specifikace formátu přenášených dat a způsobu zacházení s nimi. Aby mohly dva počítače spolu komunikovat, musejí používat stejné protokoly.

Většina síťových protokolů je standardizována, aby mohly být použity pro komunikaci mezi zařízeními různých výrobců. Jako příklad uveďme sadu protokolů používaných v síti Internet, která je označována souhrnným názvem TCP/IP.

Proxy server Starší metoda sdílení internetového připojení. Klient v lokální síti nekomunikuje s cílovým serverem v Internetu přímo, ale předá svůj požadavek proxy serveru, který jej vyřídí a předá mu odpověď.

SMTP Základní protokol, který se používá pro odesílání pošty v Internetu. Odesílatel a příjemce zprávy je určen e-mailovou adresou.

SMTP standardně používá protokol *TCP*, port *25*.

Služba V síťové terminologii označení pro aplikaci, která může být využívána síťově. V TCP/IP je služba dána transportním protokolem a portem (např. služba HTTP používá protokol *TCP*, port *80*.

SSL Protokol pro zabezpečení a šifrování TCP spojení. Původně vznikl a byl používán pro zabezpečení přenosu WWW stránek protokolem HTTP (tento protokol je označován jako HTTPS), dnes je podporován téměř všemi standardními internetovými službami — SMTP, POP3, IMAP, LDAP atd.

Na začátku komunikace se nejprve asymetrickou šifrou provede výměna šifrovacího klíče, který je pak použit pro (symetrické) šifrování vlastních dat.

TLS Transport Layer Security. Nástupce SSL, de facto SSL verze 4.

Kapitola 10

Rejstřík