Uživatelská příručka

TINY Network Monitor 1.0

Obsah

Úvod

Tiny Network Monitor je malý, leč výkonný nástroj k online sledování využití a zatížení vašeho internetového připojení. Jeho dvě základní funkce jsou:

- grafické sledování aktuálního zatížení datovými přenosy z/do Internetu, a to v rámci celé sítě, vybraného počítače anebo skupiny počítačů
- zobrazení přehledné tabulky objemu přenesných dat pro jednotlivé uživatele za určité období (od 1 dne až do celkové doby, po kterou Tiny Network Monitor síť sleduje)

Kdy a k čemu můžete Tiny Network Monitor využít:

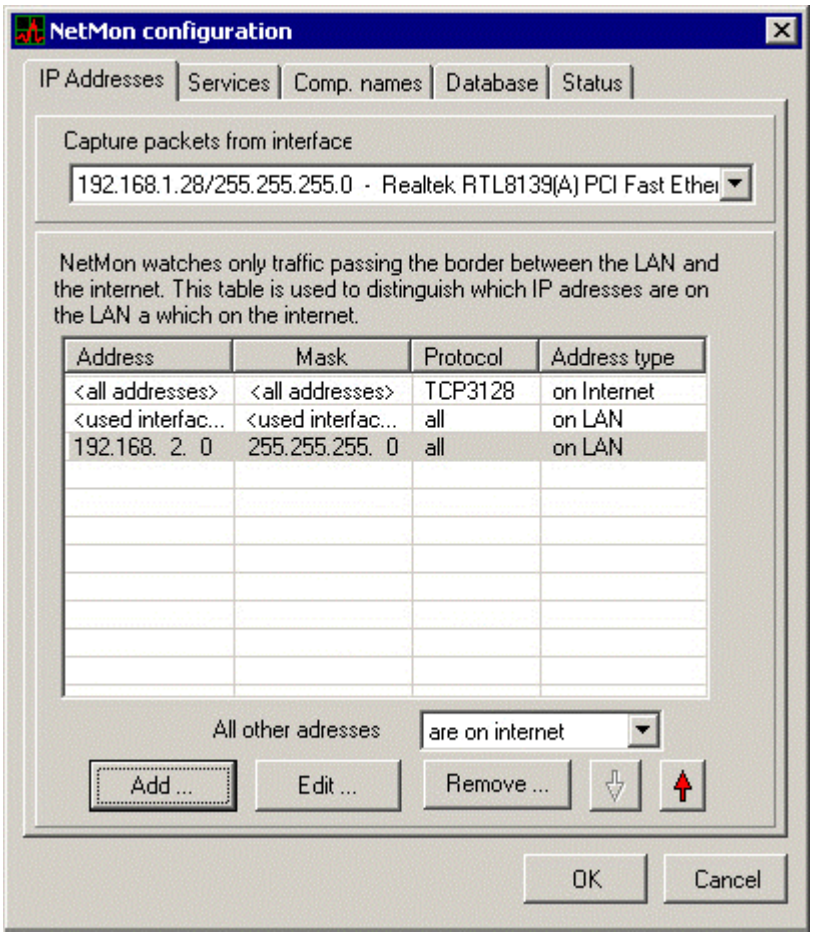
- chcete mít přehled, jak jednotlivé počítače ve vaší firmě zatěžují linku do Internetu
- požadujete kontrolu, kolik času tráví zaměstnanci brouzdáním po Internetu

Poznámka: Tiny Network Monitor nedokáže sledovat datové přenosy generované přímo počítačem, který je bránou do Internetu. Podrobnosti nalezenete v kapitole Technická omezení.

Instalace

Tiny Network Monitor může být nainstalován na libovolný počítač ve vaší lokální síti. Instalaci provedete jednoduše spuštěním distribučního programu (např. NM10EN.EXE) a zadáním složky (adresáře), kam má být nainstalován. Program spustíte z nabídky Start / Programy. Je-li vaše síť tvořena pouze jedním segmentem, není třeba žádné další nastavování.

V opačném případě zvolte v menu Actions / Setup, vyberte záložku IP Addresses, a zkontrolujte, zda jsou zde uvedeny všechny rozsahy IP adres odpovídající vaší síti. Pokud ne, přidejte tlačítkem **Add** požadované rozsahy IP adres s volbou **On LAN**.



V případě, že počítač, na němž Tiny Network Monitor běží, má více než jednu síťovou kartu, vyberte v nabídce **Capture packets from interface:** kartu, na níž má být provoz sledován. Jedná-li se o počítač poskytující rozhraní mezi vaší sítí a Internetem, je třeba vybrat kartu vedoucí do vnitřní sítě!

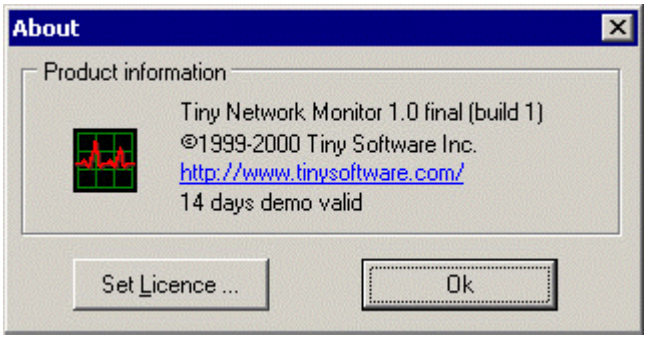
Jak Tiny Network Monitor pracuje?

Tiny Network Monitor (zkráceně NetMon) sestává ze dvou částí - prohlížecího programu (NetMon.exe) a tzv. daemona (NetMonD.exe), který se spouští při startu systému jako aplikace běžící na pozadí nebo jako služba ve Windows NT.

Daemon sleduje provoz na síti v tzv. promiskuitním režimu (tzn. dokáže přijímat i data, která nejsou adresována počítači, na němž běží) a počítá objem dat v jednotlivých paketech, o nichž na základě zdrojové a cílové IP adresy usoudí, že odcházejí do Internetu nebo naopak odtud přicházejí. Nasčítané výsledky ukládá do diskových souborů pro okamžité či pozdější zobrazení prohlížecím programem.

Zadání licenčních údajů

Po instalaci programu Tiny Network Monitor je třeba zadat licenční číslo, které jste obdrželi se zakoupeným produktem, jinak program funguje pouze po dobu 14 dní (jako demoverze). Licenční číslo lze zadat volbou **About** v hlavním menu a následným stiskem tlačítka **Set Licence**.

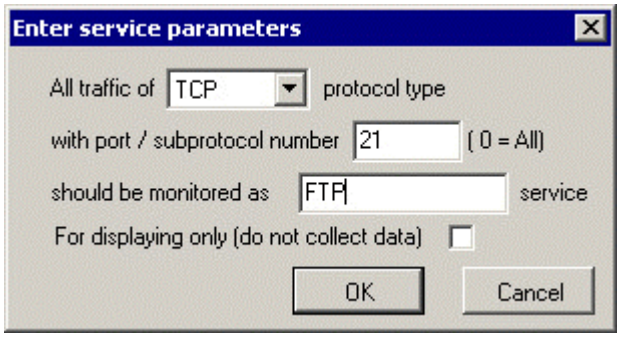


Konfigurace programu

Základní nastavení

Veškerá nastavení NetMonu se provádějí v okně NetMon Configuration, které otevřete volbou **Actions / Setup** v hlavním menu nebo stiskem kláves Ctrl+S.

Okno NetMon Configuration obsahuje následující záložky:

- **IP addresses** - dle této tabulky NetMon určuje, které IP adresy patří do lokální sítě a které do Internetu. Správné nastavení je důležité, aby NetMon rozpoznal, která data jsou přenášena z/do Internetu a mají být počítána, a která jsou v rámci lokální sítě a počítána být nemusejí.
- **Services** - zde můžete zadat služby, které se mají sledovat odděleně. Služba je určena typem protokolu a číslem portu. Speciální volba **For displaying only (do not collect data)** způsobí, že daemon přestane službu sledovat. Pak je možné pouze zobrazovat data, která byla pro tuto službu naměřena dříve, ale žádná další data již měřena nebudou.
- 

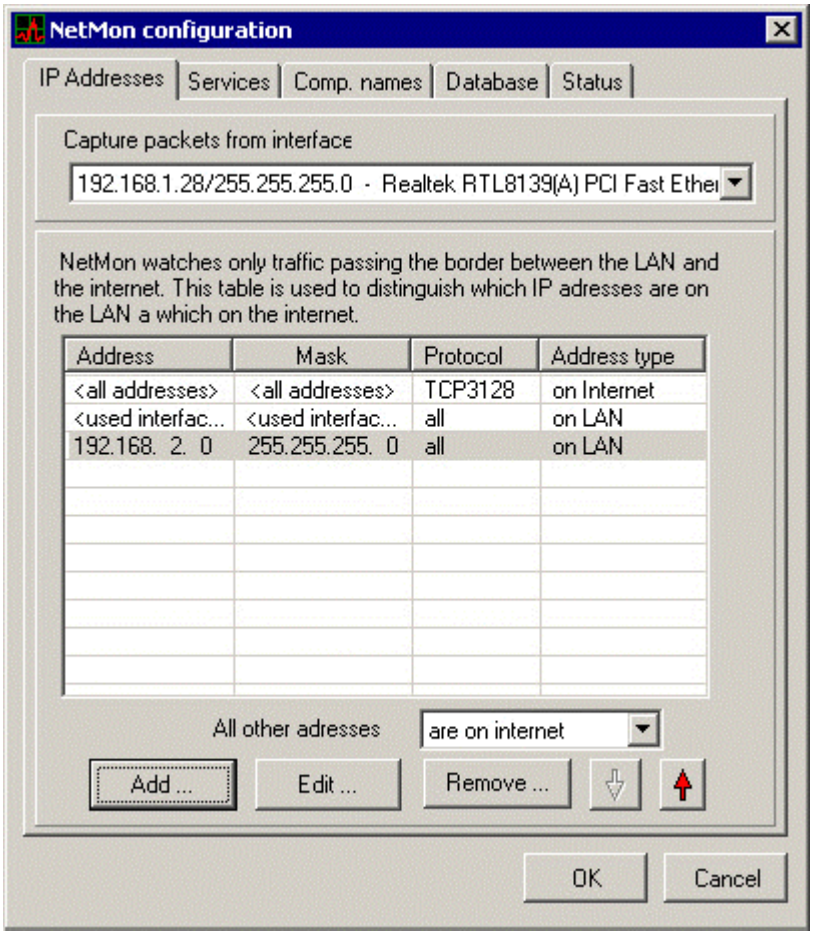
- **Comp. names** - tabulka určuje, jaká jména počítačů jsou přiřazena jednotlivým IP adresám. Jména lze zadat buď ručně (tlačítkem **Edit** po vybrání některé adresy), nebo automatickým dotazováním DNS vždy při nalezení nové adresy (volba **Automatically resolve names**) anebo jednorázovou komunikací s DNS (tlačítko **Resolve from DNS**). Mají-li se jména zjišťovat z DNS a pro určitou adresu není v DNS záznam, zobrazí se pak ve tvaru "no DNS - 192.168.1.1".
- **Database** - zde je možno zvolit adresář pro uložení datových souborů programu NetMon a maximální doby, po které mají být naměřená data uchovávána. Pole "**high resolution data**" udává dobu, po kterou budou uchována data s třísekundovými průměry a pole "**low resolution data**" dobu pro data s hodinovými průměry.

- **Status** - umožňuje zastavení a znovuspuštění daemona (nutné pro případný upgrade či odinstalování programu). Kromě toho je zde možno zvolit, zda ze ikona spuštěného programu NetMon bude zobrazovat na liště nebo v system tray.

IP addresses

Nejdůležitějším nastavením v okně Setup je záložka IP addresses. Zde je třeba správně nastavit, které IP adresy se nacházejí v lokální síti a které patří do Internetu (případně které jsou vyhrazeny a NetMon je nemá brát v úvahu).

Záložka IP addresses umožňuje provést následující nastavení:



Capture packets from interface - v případě, že má váš počítač více než jednu síťovou kartu, je zde třeba vybrat tu, na níž se mají pakety sledovat. Měla by to být ta, na níž se pakety vyslané lokálními počítači objeví - tedy např. na serveru tvořícím bránu do Internetu "vnitřní" karta, na routeru spojujícím dva lokální segmenty karta vedoucí do segmentu připojeného na Internet apod.

Typy IP adres - zde je možno definovat IP adresy nebo rozsahy adres a určit, zda patří do lokální sítě nebo do Internetu. Příklad nastavení na obrázku:

- 1. řádka - libovolná adresa je považována za patřící do Internetu, jestliže je jedná o protokol TCP a port 3128. Toto nastavení má za následek, že i komunikace přes proxy server (jehož adresa je samozřejmě lokální) bude vyhodnocována jako přístup do Internetu (ovšem i v případě, že budou data ve skutečnosti stahována z cache proxy serveru - viz kap. Technická omezení).
- 2. řádka - adresy ze subsítě, do níž je připojena vybraná síťová karta, budou považovány za lokální
- 3. řádka - do lokální sítě má být rovněž zahrnut segment 192.168.2.0 (tj. další subsíť, oddělená routerem)

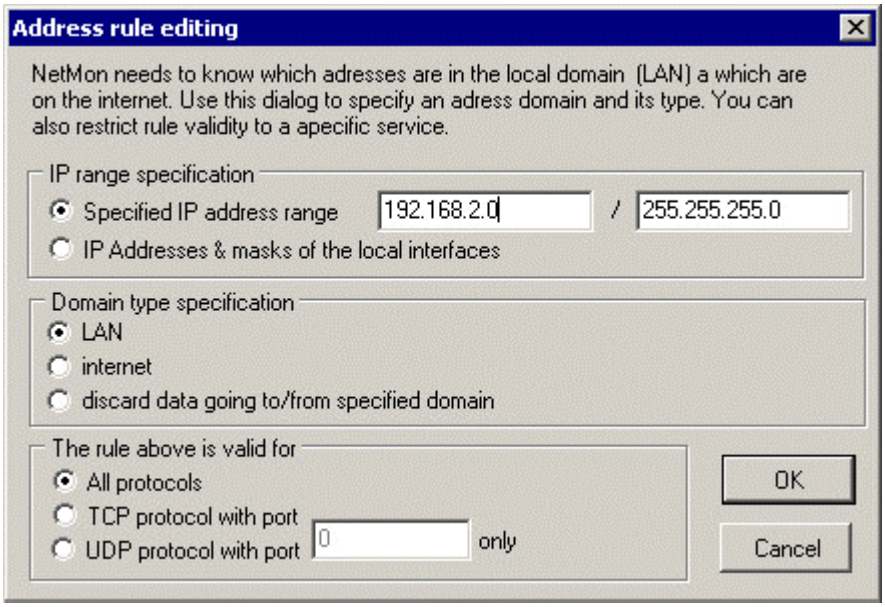
První dvě z uvedených nastavení jsou přidávána automaticky, lze je však rovněž pozměnit či odstranit.

Volba **All other addresses říká**, jakým způsobem mají být zpracovány IP adresy, které nejsou v seznamu uvedeny. Standardní nastavení je **are on Internet** - "vše, co není nastaveno jako lokální, patří do Internetu", jsou zde však umožněny i volby **on LAN** (patří do lokální sítě) a **should be discarded** (tyto adresy nebudou brány v úvahu).

Tlačítka ve spodní části okna umožňují přidat, změnit nebo vymazat záznam v tabulce, tlačítka se šipkami pak měnit pořadí těchto pravidel (zpracování probíhá shora dolů, a pravidla by tedy měla být seřazena od nejspecifičtějších k nejobecnějším).

Definice rozsahu IP adres

Nový rozsah IP adres lze přidat tlačítkem **Add**.



- **IP range specification** - definice rozsahu IP adres, pro nějž má být nastavano pravidlo (lze buď zadat, anebo zvolit lokální subsíť karty, na níž se sledování paketů provádí).
- **Domain type specification** - určení, kam bude definovaný rozsah náležet. Možnosti jsou lokální síť (**LAN**), **Internet** anebo adresu neuvažovat (**discard**).
- **The rule is valid for** - lze vybrat službu, na niž se má pravidlo vztahovat. **All protocols** znamená všechny služby (protokoly vyšších úrovní) nad IP. Protokol TCP či UDP s příslušným portem pak určují jednotlivé služby (např. TCP port 80 = WWW).

```
Poznámka: Je třeba mít na paměti, že NetMon
  zaznamenává právě ty pakety, jejichž zdrojová
  adresa patří do rozsahu "on LAN" a cílová do
  "Internet" nebo naopak!  Jsou-li obě adresy ze
  stejných rozsahů, nejsou přenesená data
  sledována.
```

Technická omezení

Switchované sítě

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

Možností řešení je několik:

- nainstalovat NetMon přímo na počítač, který je připojen k Internetu (NetMon pak musí být nastaven pro sledování na **vnitřní** síťové kartě - viz kap. Instalace).
- překonfigurovat switch tak, aby posílal na dotyčný port všechna data
- připojit mezi switch a internetovou bránu malý hub (stačí 3 zásuvky - jedna na switch, druhá na bránu do Internetu a třetí k počítači s NetMonem).

Pošta

Přirozený požadavek správce sítě je sledovat také objem dat přenesených elektronickou poštou (e-mailem) přijatou lokálním mailserverem. Problém však nastává v případě, že mailserver běží na počítači, který je zároveň branou do Internetu pro lokální síť - v takovém případě se totiž příslušné pakety do lokální sítě nedostanou a NetMon je tedy nezaznamená.

Možnosti, jak tuto situaci řešit, jsou následující:

- Nastavit NetMon tak, aby sledoval i komunikaci uživatelů s mailserverem (data by se tedy sledovala až v okamžiku, kdy si je koncový uživatel z mailserveru stáhne). To lze provést obdobně jako nastavení pro proxy server (viz kap. Konfigurace programu - IP addresses) - všechny adresy, protokol TCP, port 110 (POP3), budou prohlášeny "on Internet". Pak bude NetMon sledovat i přenesenou poštu, ovšem včetně lokální pošty, kterou si uživatelé ve vaší síti posílají mezi sebou.
- Umístit mailserver na jiný ("vnitřní") počítač. Pak není třeba NetMon nijak nastavovat - komunikace mailserveru s dalšími mailservery v Internetu bude sledována správně a komunikace lokálních uživatelů s mailserverem sledována nebude.

Proxy server

Podobně jako v případě mailserveru umístěného na počítači, jež je branou do Internetu, nastává při sledování komunikace klientů s proxy serverem problém v případě, že jsou data brána z cache - i v tomto případě budou vyhodnocena jako stažená z Internetu.

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

Ovládání prohlížecího programu

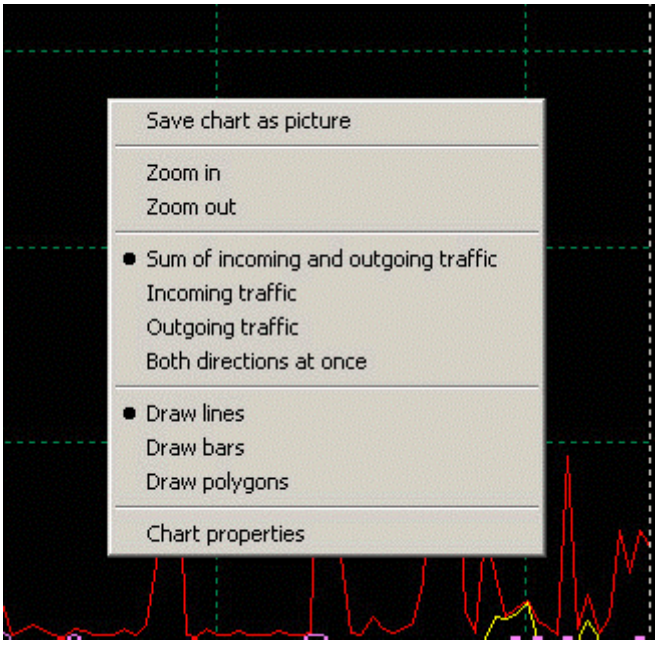
Prohlížecí program spustíte pomocí menu Start / Programy / Tiny Network Monitor. Hlavní okno obsahuje dvě záložky: **Traffic history chart** a **Accounting report**.

Traffic history chart

Traffic history chart je online analyzátor, zobrazující aktuální průběh zatížení linky. Na vodorovné ose je čas, jehož měřítko lze volit v rozmezí 1 minuta až 1 rok, a na svislé ose přenosová rychlost (v B/s). Při pohybu kurzoru po grafu v pravé části stavové řádky (na dolním okraji okna) zobrazují údaje odpovídající aktuální poloze (tedy čas a přenosová rychlost).

Vpravo od grafu je umístěn seznam počítačů v lokální síti, vytvářený dle IP adres v monitorovaných paketech (tzn. že každý počítač se v tomto seznamu objeví teprve poté, co přenese nějaká data z/do Intenetu). Počítače jsou reprezentovány buď IP adresami, anebo jmény zjištěnými z DNS - dle vašeho aktuálního nastavení (viz kap. Konfigurace programu). Vyberete-li některý z počítačů v tomto seznamu, zobrazí se jinou barvou křivka přenosu pro tento konkrétní počítač. Přidržením klávesy Ctrl při výběru lze označit i více počítačů současně (skupinu).

Stiskem pravého tlačítka na grafu lze zvolit další možnosti:



- **Save chart as picture** - umožňuje uložit aktuální podobu grafu do souboru ve formátu JPEG nebo BMP
- **Zoom in, Zoom out** - změna měřítka časové osy (lze provést i pomocí ikon nad grafem)
- Volba zobrazení přenosů ve směru ven, dovnitř či v obou směrech: **Sum of incoming and outgoing traffic** zobrazí součet zatížení v obou směrech, **Incoming** a **Outgoing traffic** ve směru z a do Internetu a **Both directions at once** zobrazí dvě křivky - pro každý směr jednu
- **Draw lines, bars, polygons** - volba, jak má být graf vykreslován: čárový, sloupcový nebo plošný

Pravým tlačítkem na seznamu počítačů lze zvolit některou z následujících funkcí:

- **Select all, Deselect all** - výběr nebo zrušení výběru všech počítačů v seznamu
- **Sort by...** - volba řazení seznamu počítačů dle jména, IP adresy či objemu přenesených dat
- **Resolve names from DNS** - provede jednorázové převedení zjištěných IP adres na jména dle DNS (pokud v něm příslušné záznamy existují). Volba má samozřejmě význam pouze v případě, že není zapnuto automatické dotazování DNS (Action / Setup / záložka Comp. names, volba Automatically resolve names)

Výběrové pole **Display only this service** umožňuje zvolit monitorování buď všech IP přenosů, nebo jen vybrané služby (viz kap. Konfigurace programu).

Tlačítka s lupou nad, popř. vedle grafu slouží ke změně měřítek jednotlivých os, tlačítka se šipkami pak posun po vodorovné ose (v čase) po menších či větších úsecích, příp. na začátek a na konec. Prostřední z těchto tlačítek (se šipkou dolů) umožňuje zvolit libovolné datum a čas.

Accounting report

Tato záložka slouží k vyhodnocení celkového objemu dat přeneseného jednotlivými počítači za určitou dobu. Nejprve je třeba nastavit požadované parametry této tabulky. Pro větší názornost jsou jednotlivá pole očíslována v pořadí jednotlivých kroků, které je nutno provést.

Nastavení parametrů tabulky bude vysvětleno na jednoduchém příkladu: chceme, aby obsahovala objem dat přenesený jednotlivými počítači každý den za posledních 7 dní.

1 **Set column's options** - zde se nastavují parametry sloupců tabulky: **One column contains traffic summary for...** - jaké období má být obsaženo v každém sloupci. V našem případě zvolíme **1 day(s)**. **Number of columns in the report** - kolik takových sloupců má tabulka obsahovat. Zvolíme **7** (pro 7 dní).

2 **Select report's start date** - zde lze nastavit datum "začátku" (tj. prvního sloupce). V našem případě požaduje posledních 7 dní - bylo by tedy na místě odečíst od dnešního data 7 dní a toto datum zvolit. Mnohem jednodušší je však v tomto případě použít tlačítko **Suggest start date**, které nastaví počáteční datum automaticky na základě nastavených parametrů sloupců.

3 **Choose which traffic to include** - zda má tabulka obsahovat objem přenesených dat celkem (**incoming + outgoing**), ve směru z Internetu (**incoming**) anebo do Internetu (**outgoing**).

4 **Make the report** - vytvoření tabulky na základě nastavených parametrů. Jednotlivá tlačítka umožňují zobrazit tabulku na obrazovce (**Display**), vytisknout na tiskárně (**Print...**) anebo uložit do souboru v podobě HTML stránky (**Save as...**).

Co s problémy?

Firma Tiny Software Inc. poskytuje na produkt Tiny Network Monitor bezplatnou e-mailovou podporu. Své dotazy, zjištěné nedostatky a náměty na vylepšení do příštích verzí můžete posílat na adresu **monitor@tinysoftware.com**.