Monitoring síťového provozu

RJ-45 v akci

NAJDETE NA CHIP DVD

DU meter	shareware	www.dumeter.com
BWMeter 2.4.2	shareware	www.desksoft.com
Connection Meter	shareware	www.conmet.cz
Net Activity Diagram 2.3	shareware	www.metaproducts.com
NetStat Live	freeware	www.analogx.com
Racoonworks SpeedTest	freeware	www.racoonworks.com
MyVitalAgent 8.0.1	freeware	www.lucent.com
Net.Medic	freeware	www.vitalsigns.com

Potřeba řešení lokálních úloh bez použití ústředního počítače vedla ke vzniku tzv. počítačových sítí, které umožňují uživatelům pracovat v síti i mimo ni. Rozvoj počítačových sítí umocnilo též prudké nasazení počítačů řady PC v komerční sféře, což se projevilo prudkým rozvojem sítí LAN v této oblasti (úřady, školy, závody, firmy). V tomto článku se budeme zabývat touto problematikou a představíme vám programy pro monitorování přenosů dat na síti a další utility.

Text: Zdeněk Janura,
zdenek_1@seznam.cz

Počítačové sítě LAN patří do rodiny datových sítí, které rozdělujeme podle územního rozložení do tří skupin:

1. WAN (wide area network) – veřejné datové sítě: jsou svým rozsahem neomezené, přičemž zabírají území států i kontinentů.
2. MAN (metropolitan area network) – městské datové sítě: zabírají území města, tedy řádově kilometry. Vznikají spojením vícerých vzdálených sítí LAN.
3. LAN (local area network) – lokální datové sítě: pokrývají území nepřesahující 1 až 2 km, tedy rozsah pracovišť, budov, závodů.

Sítě LAN mají mezi datovými sítěmi své specifické místo, což vyplývá z jejich rozlehlosti. Jsou typické tím, že přenosové médium je ve vlastnictví uživatele (uvnitř budov). K přenosu se využívají vysoké přenosové rychlosti, řádově MB až GB. Tyto sítě mají nízkou chybovost, což vyplývá z použití kvalitních kabelů a ze skutečnosti, že síť neprochází otevřeným prostorem s výrazným rušením.

Síť PC-LAN je de facto skupina počítačů PC, které jsou navzájem propojeny tak, aby byla možná jejich vzájemná komunikace. Svým uživatelů mohou sítě PC-LAN poskytovat následující služby: sdílení technických zařízení sítě, sdílení společných dat sítě, elektronickou poštu mezi uživateli sítě, monitorování jiných účastníků sítě, hlasovou a obrazovou komunikaci v síti.

Každá síť nemusí poskytovat všechny vyjmenované služby, jednotlivé sítě se zpravidla liší v množství a kvalitě poskytovaných služeb. Sítě poskytují svým uživatelům nejčastěji první dva druhy služeb: sdílení technických zařízení a sdílení společných dat jsou hlavní důvody, které vedou k nasazení sítí, a proto je většina výrobců na své síti zajišťuje. Kromě těchto služeb bývá obvykle nejvíc využívanou službou elektronická pošta, která umožňuje zasílat programy a textové soubory jednotlivým uživatelům sítě. Její realizace je u jednotlivých sítí odlišná, přičemž některé ze sítí ji nemají realizovanou vůbec.

Počítače zapojené do sítě PC-LAN mohou mít buď funkci serveru, nebo funkci pracovní stanice (workstation). Technickým vybavením se obyčejně neliší, vždy se však liší svým programovým vybavením.

Topologie sítí LAN

Všechny návrhy sítě vycházejí ze tří základních topologií, kterými jsou:

- sběrnicová topologie;
- hvězdicová topologie;
- prstencová topologie.

Další možností topologie sítě je neomezená topologie a varianty hlavních topologií.

Pokud jsou počítače zapojeny v řadě za sebou podél jediného kabelu (segmentu), nazývá se tato topologie sběrnicová. Jsou-li počítače zapojeny ke kabelovým segmentům, které vycházejí z jediného bodu neboli rozbočovače, nazývá se tato topologie hvězdicová. Jestliže jsou počítače zapojeny ke kabelu, který tvoří smyčku, nazývá se tato topologie prstencová.

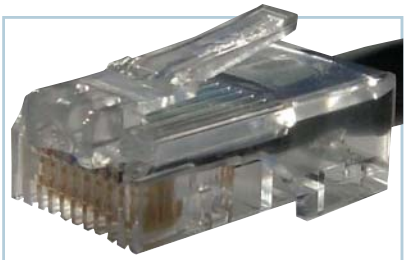
Zatímco tyto tři základní topologie jsou samy o sobě jednoduché, v praxi používané varianty často kombinují vlastnosti více topologií a mohou být složité.

TCP/IP

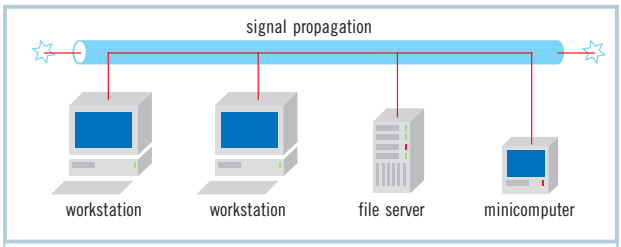
TCP/IP je zkratka slov Transmission Control Protocol/Internet Protocol. Tento protokol se používá po celé síti Internet, ale nejenom tam. Příkladem jeho dalšího použití mohou být platformy jako UNIX, Banyan VINES, Microsoft LAN Manager či →

VOLBA TOPOLOGIE

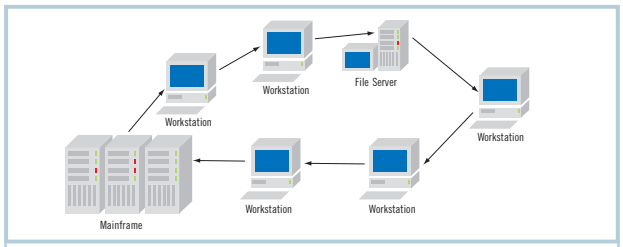
Topologie	Výhody	Nevýhody
Sběrnicová	Ekonomické využití kabelu. Média nejsou drahá a snadno se s nimi pracuje. Je jednoduchá a spolehlivá. Snadno se rozšiřuje.	Síť může při velkém provozu zpomalit. Problémy se obtížně izolují. Porušení kabelu může ovlivnit mnoho uživatelů.
Prstencová	Rovnocenný přístup pro všechny počítače. Vyvážený výkon i při velkém počtu uživatelů.	Selhání jednoho počítače může mít dopad na zbytek sítě. Problémy se obtížně izolují. Rekonfigurace sítě přeruší její provoz.
Hvězdicová	Snadná modifikace a přidávání nových počítačů. Centrální monitorování a správa. Selhání jednoho počítače neovlivní zbytek sítě.	Pokud selže centrální prvek, selže celá síť.



Konektor RJ-45 – nejpoužívanější konektor pro vytvoření sítě



Sběrnicová topologie



Prstencová topologie

Novell NetWare. Přestože se stal standardním souborem protokolů teprve v poslední době, je starý již více než dvacet let. V počátku byl použit pro spojení vládních počítačů (síť ARPANET – předchůdce dnešního internetu), nyní nachází největší využití právě v internetové síti, která se stala největší celosvětovou sítí. Jako TCP/IP standard se tento síťový protokol začal prosazovat v době, kdy byl implementován do systému UNIX a jemu podobných, zhruba někdy v 80. letech. Díky této podpoře a zároveň díky jeho vyplývající historické kompatibilitě vůči velkému množství hardwarových a softwarových systémů se dnes těší velkému rozšíření.

TCP – před každou výměnou dat mezi dvěma uzly musí být nejprve navázáno spojení a po přenosu musí být zase zrušeno. TCP protokol posílá data po jednotlivých bajtech, očekává tedy, že mu budou data předávána od jeho vyšší vrstvy v tzv. oketech. Ty pak kumuluje do vyrovnávacího bufferu, obvykle o velikosti 64 kb, a posílá je dále. Celý mechanismus sdružování jednotlivých bajtů do bloků je plně v režii protokolu TCP, který se přenosem větších celků snaží optimalizovat využití přenosových cest. Pro vyšší vrstvu je tento mechanismus neviditelný – vyšší vrstva pracuje s představou proudu jednotlivých bajtů. Pro některé aplikace však nemusí být přenos přes vyrovnávací buffer příliš vhodný. Proto zde existuje přímý odesílací mechanismus nazývaný push, kterým si lze odeslání dat vynutit, aniž by byl buffer plný.

UDP – tento protokol vyšle data, aniž by navazoval jakékoliv spojení s nějakým uzlem. Na rozdíl od TCP posílá data v celém bloku. Očekává tedy od své bezprostředně vyšší vrstvy vždy celý blok dat, který se snaží přenést opět jako celek (v rámci jediného tzv. uživatelského datagramu), a na straně příjemce jej předává své bezprostředně vyšší vrstvě opět jako celek.

Při přenosu používá protokol TCP tzv. kladné potvrzování (positive acknowledgement), což znamená, že se potvrzují jen úspěšně přijatá data, naopak na „nepřijatá, chybná“ data se vůbec nereaguje. Chybně vyslaná data se posílají opětovně po určité době (po vypršení časového limitu – time out). Bylo by však značně neefektivní, kdyby protokol čekal na každé „dobré“ potvrzení. V praxi se přenos provádí tak, že se vyšle několik bloků dat ještě dříve, než je přijata informace o tom, že byla data úspěšně přijata tzv. kontinuální potvrzování (continuous acknowledgement).

SERVER

Jedná se o počítač, který poskytuje ostatním počítačům sítě svoje technické zařízení nebo svoje data. Slouží tedy potřebám sítě, z čehož plyne i jeho název: server – sluha.

Servery mohou být:

a) vyhrazené (dedicated) – slouží jen pro potřeby sítě, není je možné používat na jiné úlohy;
b) nevyhrazené (non dedicated) – vedle práce v síti je možné pracovat i na jiných aplikacích.

Podle poskytovaných služeb dělíme servery do několika skupin:

Diskové servery: poskytují uživatelům sítě část svého pevného disku, přidělují uživatelům sítě stopy a sektory pevného disku. Dnes se tyto druhy serverů používají zcela výjimečně.

Souborové servery: mají k dispozici také pevný disk, který je poskytován uživatelům sítě. Jedná se v podstatě o požadavky na otevírání, zavírání, zapisování a čtení souborů. U tohoto typu přístupu je možné kontrolovat práva uživatelů.

Tiskové servery: tyto servery poskytují síti kvalitní, obvykle laserovou tiskárnu. Udržují na serveru tzv. tiskovou řadu (Spool), do které se ukládají soubory uživatelů sítě určené pro tisk. Tyto soubory jsou postupně z „fronty“ posílány na tiskárnu. V praxi se obvykle vyskytuje kombinace souborového serveru s tiskovým.

Komunikační servery: obsahují obvykle přídavnou kartu pro přístup do jiné sítě (bridge).

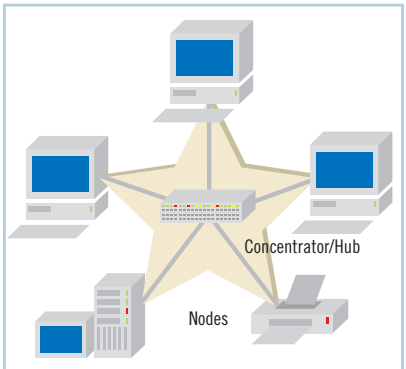
Databázové servery: poskytují síti rozsáhlou databanku. Manipulaci s ní zajišťuje speciální programovací jazyk SQL. Z toho plyne název SQL server.

Poštovní servery: Jedná se o servery, které jsou určeny výhradně k posílání, přijímání, ověřování a uchovávání e-mailů.

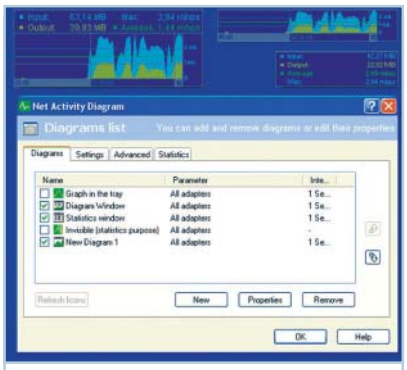
Workstation (pracovní stanice): počítač, který využívá služby sítě. Má k dispozici data a technická zařízení poskytovaná servery. Pracovní stanicí může být libovolný počítač.

PROGRAMY PRO SLEDOVÁNÍ PROVOZU NA SÍTI

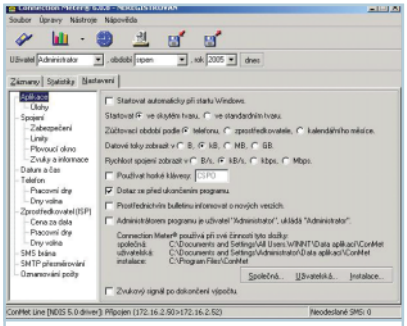
Připravili jsme pro vás také programy, které vám pomohou sledovat kvalitu připojení, jeho rychlost, množství dat směřujících ven nebo dovnitř. Programy tyto údaje přehledně zobrazí v grafech nebo tabulkách, abyste se v nich mohli lépe orientovat. Jedná se o malé programy, které by neměly zpomalit počítač – jen jejich ikonka bude indikovat, že vůbec existují a dělají to, co mají.



Hvězdicová topologie



Net Activity Diagram: **Ideální program pro dlouhodobější statistiky, díky jeho perfektním grafům.**



Connection Meter: **V tomto okně provádíte veškerá nastavení. Program toho nabízí opravdu hodně.**

BWMeter

BWMeter je výkonný nástroj pro monitorování a měření konektivity sítě. Umí rozlišit, odkud kam jaká data jdou. To mu dává možnost rozlišit lokální provoz a provoz v internetové síti. Jeho další výhodou je, že umožňuje omezit rychlost připojení, nebo dokonce přístup na vybrané stránky. Tento program umí vytvářet velmi pěkné a přehledné grafy z dat, která získá, a uživatel tak má přehled o tom, kolik dat mu do počítače přichází nebo kolik jich z počítače odchází. Grafy se dají nadefinovat – barvy, font, popis. Jejich konfigurace i definování jsou velmi lehké, čímž na nás program udělal dobrý dojem. Celkově jsou generovány dva grafy, jeden pro síť Internet a druhý pro lokální síť LAN.

Klíčové vlastnosti:

- grafické a numerické zobrazování přenosu dat;
- uživatelsky definované filtry pro měření;
- může monitorovat všechna síťová rozhraní a adaptéry;
- umí monitorovat a zobrazovat veškerý provoz na síti;
- vytváří denní, týdenní, měsíční a roční statistiky;
- při nadefinování jistých omezovacích filtrů spustí upozornění;
- jednoduchá instalace a konfigurace.

Connection Meter

Jedná se o velmi komplexní program pro sledování připojení v síti. Podporuje připojení pomocí modemu, CDMA, GPRS, ISDN, ADSL, Wi-Fi a kabelového modemu. Instalace tohoto programuje je jednoduchá a jedná se v zásadě o odklikání několika tlačítek. Po nainstalování a prvním spuštění se v systray objeví ikonka telefonu. Nyní jste požádáni o vybrání typu připojení a k němu i tarifu. Opět se jedná pouze o vybírání možností a není nutné nic psát. Pokud provedete všechny tyto kroky, zobrazí se vám ještě navíc malé obdélníkové okno se čtyřmi údaji: první uvádí dobu připojení, druhý sděluje, kolik peněz jste prosurfovali (odvíjí se od tarifu), a dále rychlost, jakou se stahuje obsah webové stránky, ftp anebo e-mailů. Čtvrtý údaj počítá odeslané SMS – tento program totiž dokáže odesílat i SMS zprávy na operátora, a proto dává možnost monitorovat i tento údaj. Toto plovoucí obdélníkové okno lze libovolně definovat a vybírat v něm, jaké údaje budou právě zobrazovány.

Connection Meter je šířen ve dvou verzích. Neregistrovanou je možné šířit a užívat bez omezení, obsahuje však reklamní proužek. Pokud chce uživatel rozšířit počet funkcí programu, má možnost registrace.

DU Meter

Jedná se o kvalitní nástroj, který nás nadchl již od začátku. Instalace je velmi jednoduchá, hned po ní dojde ke spuštění malého transparentního okénka, ve kterém je vidět aktuální rychlost downloadu a uploadu, a to jak v číselné, tak v grafické podobě.

Pojďme se teď podívat na možnosti nastavení programu. Jsou zde čtyři záložky: první z nich je obecná a poskytuje možnost nastavení vlastností okna, jako je transparence a minimalizace. Zobrazení si můžete vybrat grafické, numerické, nebo obojí dohromady. Pro rychlost připojení jsou pouze dvě možnosti, a to kb/s nebo kB/s. V záložce „graph options“ si můžete nadefinovat barvy, styly čar a maximální hodnoty na grafu.

V „alerts and reports“ program dává možnost nadefinovat si upozornění pro nějaké významné události týkající se velikosti stahovaného souboru nebo množství již postahovaných dat. Poslední záložkou je „notification“, poskytující možnost přidat zvukové oznámení.

DU Meter také pomáhá chránit proti hrozbám na síti. Je tedy velmi schopným „bodyguardem“ proti některým nebezpečným aktivitám, které se dějí, když je uživatel on-line. Nelze totiž stoprocentně určit, jaká data jsou stahována a jaká nahrávána na váš počítač. Můžete pouze přibližně odhadnout, co se tak může odehrávat, když si pustíte webový prohlížeč nebo když se připojíte prostřednictvím ostatních programů. Co když se vám do PC dostala nějaká nechtěná aplikace, která si následně posílá, co chce a kam chce? Jedná se o každodenní případy mnoha uživatelů, které nejsou zrovna žádány. Tento program

NÁZEV PROGRAMU	BWMeter	NetStat Live	DU meter	Connection Meter	Net Activity Diagram
VÝROBCE	DeskSoft	AnalogX	Hagel Technologies	Epstudio	MetaProducts Corporation
INTERNET	*www.desksoft.com*	*www.analogx.com*	*www.dumeter.com*	*www.conmet.cz*	*www.metaproducts.com*
LICENCE	shareware	freeware	shareware	shareware	shareware
OMEZENÍ	30 dnů	–	30 dnů	neregistrovaná volná verze	30 dnů
CENA	30 USD	–	689 Kč	od 160 Kč	25 USD
VELIKOST INSTALACE	371,1 kB	257 kB	920,2 kB	1,5 MB	1,1 MB
OPERAČNÍ SYSTÉM	Windows 95/98/ME/NT/ 2000/XP/2003	Windows 98/ME/NT/ 2000/XP	Windows 95/98/ME/ NT/2000/XP	Windows 95/98/ ME/NT/2000/XP	Windows 95/98/ ME/NT/2000/XP
OVLÁDÁNÍ	■■■■■	■■■■■	■■■■□	■■■■■	■■■□□
INSTALACE	■■■■■	■■■■■	■■■■■	■■■■■	■■■■■
GRAFY, FUNKCE	■■■■□	■■■□□	■■■□□	■■■■□	■■■□□
PŘEHLEDNOST	■■■■■	■■■■■	■■■■□	■■■■□	■■■■■
CELKOVÝ DOJEM	■■■■■	■■■■■	■■■■□	■■■■□	■■■■□

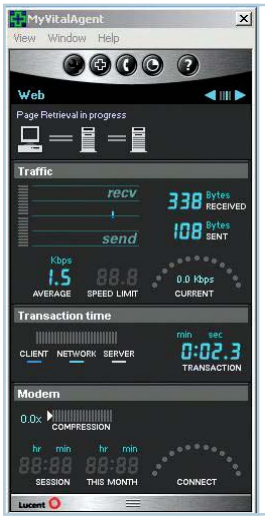
pomáhá sledovat, kdo (resp. co) a kde se pokouší přenášet různá data, a tím také omezovat takto vzniklé situace.

Net Activity Diagram

Net Activity Diagram (NAD) je program, který dokáže sledovat připojení k internetu a k počítačové síti. Program vytváří grafy a statistiky pro jednotlivá síťová připojení na jednom počítači.

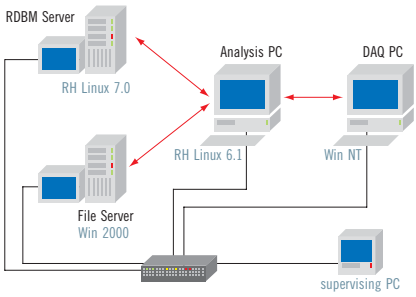
NAD vám umožní sledovat objemy síťových přenosů a veškerou aktivitu vašeho připojení. Program běží v systray menu a po kliknutí na ikonu zobrazí graf. Sleduje také veškeré přenosy, nejen prohlížení internetových stánek, ale i FTP či posílání e-mailů. Uživatelé Wi-Fi si jistě oblíbí „signal strength indicator" – indikátor síly signálu připojení.

Program nabízí čtyři záložky, ve kterých je možné nadefinovat si následující věci:
Diagrams – zde jsou předdefinované diagramy a grafy, je zde i možnost si nějaký přidat.
Settings – nabízí volbu jazyka, spuštění programu při startu, schování minimalizované ikony vedle hodin, potvrzení uzavření programu.



MyVitalAgent: S tímto programem máte veškerý přehled o aktivitách na síti.

Advanced – nabízí možnost posouvání grafů doleva nebo doprava, automatické nebo ruční zobrazování hodnot v B, kB, MB, GB a s tím související vzhled přenosové rychlosti v B nebo b. V dalším nastavení si zvolíme možnost, jak často se má programový čítač grafu nulovat.



Zapojení různých OS do sítě LAN

Statistic – poskytuje výběr ze dvou zobrazovacích modů, možnost zvolení cesty, kam se mají statistické údaje ukládat, možnosti zobrazení diagramu aktivit, zobrazení, co kam odchází z jakého portu, množství dat a mnoho dalších údajů.

NetStat Live

Prográmek pro sledování rychlosti připojení na první pohled nadchne jednoduchostí a zároveň praktičností. Přehledně a odděleně zobrazuje příchozí a odcházející provoz na síti, jeho aktuální, průměrnou i maximální rychlost. Grafické znázornění rychlostí je jednoduché a i méně zkušený uživatel okamžitě pozná, o co se jedná. Jedinou nevýhodou je absence dalších grafů a statistik, ale možná i díky tomu je program tak uživatelsky příjemný a nezatěžuje zbytečnostmi.

Racoonworks SpeedTest

Chcete si ověřit, jak rychlé připojení k internetu máte? Pomocí programu SpeedTest to můžete zjistit dokonce pro konkrétní lokace na internetu. Stačí zadat jmennou nebo číselnou URL adresu a spustit test. Výsledek se zobrazuje také graficky a je tak jednoduše možné porovnat různé výsledky. Racoonworks SpeedTest umožňuje spustit i serverovou komponentu, která zajišťuje přesnější měření rychlosti připojení pomocí zasílání souboru na váš počítač.

MyVitalAgent 8.0.1

Tento software podporuje připojení typu DSL, kabelové, vytáčené a modemové při přístupu na internet. Uživatel vidí všechny aktivity, které se dějí na síti, a má o nich přehled, program zobrazuje celkový počet přenesených dat (a to jak ven, tak dovnitř), jejich rychlost (momentální i průměrnou). Grafické rozvržení je vkusné a uživatel se v něm neztratí, když potřebuje získat informace o svém připojení. V menu je možné nadefinovat, co se má a nemá zobrazovat. Jediné, co programu snad chybí, aby uživatel mohl být maximálně spokojen, je grafická podoba připojení, tj. absence statistických grafů. Pokud ovšem uživateli stačí číselné hodnoty bez někdy až složitých nebo nic neříkajících grafů, je tento program zajisté dobrou volbou.

Net.Medic

Net.Medic je program spolupracující s webovým prohlížečem. Diagnostikuje a monitoruje připojení pro internet i intranet. Net.Medic identifikuje způsob připojení (modem, LAN atd.) a vše diagnostikuje, ve zlomku sekundy rozpozná problémy a opraví je, případně alespoň doporučí postup na jejich opravu. Dále přehledně počítá statistiky, zobrazované ve formě grafů, z nichž je pak lehké zjistit, kdy je server, ke kterému se připojujete, nejvíce zatížen, kdy máte jak rychlý přístup k internetu, jaká je četnost chyb atd. Zároveň též obsahuje velké množství grafů a různých statistik, které dají větší přehled o stavu připojení, jeho kvalitě a zatížení. Celkové grafické uspořádání je vyhovující a přehledné a nenutí uživatele hledat důležité věci, ale okamžitě je zobrazuje. K tomuto programu bychom snad měli jen dodat, že i náročný uživatel by mohl být spokojen se všemi funkcemi a grafy, které tento software nabízí.

NET.MEDIC	RACOONWORKS SPEEDTEST	MYVITALAGENT 8.0.1
Vitalsigns	Alan Fletcher	Lucent Technologies
www.vitalsigns.com	*www.racoonworks.com*	*www.lucent.com*
freeware	freeware	freeware
–	–	–
–	–	–
1 MB	1,1 MB	1,42 MB
Windows 95/98/ME/NT/2000/XP	Windows 98/ME/NT/2000/XP	Windows 95/98/ME/NT/ 2000/XP
■■■■□	■■■■□	■■■□□
■■■■■	■■■■■	■■■■■
■■■■■	■■■□□	■■■□□
■■■■□	■■■■□	■■□□□
■■■■□	■■■□□	■■■□□