Old Man GURU Magazine

Wychodzi bardzo nieregularnie, kiedy wydaje mi się,
że mam coś ciekawego lub pożytecznego do napisania...

Numer 1/2009 **17 sierpień 2009 r.**

czterdzieści lat minęło...

od uruchomienia przez Kena Thompsona nowego systemu operacyjnego w Bell Labs na komputerze PDP-7. System ten nazwano **Unics**, od słów Uniplexed Information and Computing Service. Kiedy i w jaki sposób zmienił od nazwę na UNIX historia milczy...

Pierwsza dokumentacja systemu, sporządzona przez Kena Thompsona i Denisa Ritchie zatytułowana UNIX Programmer's Manual powstała w 1971 r. Niejako po drodze Ritchie opracował jeszcze język C...

Uniksy zaczęły między sobą rozmawiać już w 1976 roku, w którym Mike Lesk opracował UUCP, a od 1980 r. wprowadzono TCP/IP...

Dwa bardzo ważne wydarzenia nastąpiły w 1991 r. - Linus Thorvalds zaprezentował światu Linuksa, i SUN Microsystem wprowadził nową wersję swego systemu – SOLARIS.

Oszczędzę Państwu dalszych szczegółów – warto jednak wspomnieć, że w 1998 r. Thompson i Ritchie otrzymali od ówczesnego Prezydenta USA Clintona odznaczenie National Medal of Technology (Bill Gates też taki dostał!).

Wielu wieszczyło przy różnych okazjach śmierć Uniksa. Nie przewidzieli jednak, że UNIX dorobi się bardzo energicznego potomka, którym okazał się LINUX. Nie tylko przejęto (i udoskonalono) w nim rozwiązania opracowane dla Uniksa, ale co więcej – zachowano, a nawet rozwinięto ideę otwartości, która zawsze towarzyszyła Uniksowi, co znalazło wyraz w takich nazwach jak Open Software Foundation (złośliwi co prawda twierdzili, że OSF to skrót od Oppose Sun Forever), X/Open, Open Group itp. Stosunkowo mało osób zdaje sobie dziś sprawę, że nawet komercyjne Uniksy dopuszczały daleko idące modyfikacje systemu – oto wolne tłumaczenie licencji załączanej do plików jednego z popularnych Uniksów:

„Informacja zawarta w tym pliku przekazywana jest licencjobiorcy.
Licencjobiorca ma prawo do używania, modyfikowania oraz włączania tego kodu do innych produktów.
Informacja ta jest dostarczona na zasadzie „JAKA JEST” i nie jest objęta jakąkolwiek gwarancją”

Oczywiście licencja GPL rozszerzyła te uprawnienia o zezwolenie na kopiowanie, ale niektóre idee zawarte w „*stalmanowskich*” wolnościach były przestrzegane już ponad 20 lat temu!

Dziś mamy Open Source – dysponujemy więc nawet kodami źródłowymi jądra systemu – w komercyjnych Uniksach jądro się jedynie „linkowało”. Nikt jednak nie zabraniał jego modyfikacji i wprowadzania do jądra (i innych składników systemu) własnych modułów. Mogliśmy więc (podobnie jak dziś Linuksa) przystosować system do indywidualnych wymagań.

Unix podobnie jak dziś Linux wyraźnie rozgranicza rolę użytkownika i administratora systemu. Jest to zasadnicza różnica w porównaniu z systemami, które wyrosły wraz z komputerami osobistymi (PC) których użytkownik jest najczęściej także administratorem. Jest więc naturalne, że twórcy popularnych systemów dla komputerów osobistych dbają o ich zabezpieczenie przez błędami administratora.

W Linuksie (podobnie, jak w Uniksie) założono, że administrator jest fachowcem i dba o środowisko pracy użytkowników.

Ponieważ z Uniksem zetknąłem się po raz pierwszy w 1978 r. na sławnym komputerze PDP-11 i udało mi się doczekać czasów, w których Linux pracuje na notebookach czuję się uprawniony do udzielania porad administratorom. Stąd pomysł wydawania „Old GURU Magazine” - chciałbym, aby stał się on polskim odpowiednikiem pisemka redagowanego w latach dziewięćdziesiątych ubiegłego wieku w USA przez Johna Esaka.

Jakie jest zadanie prawdziwego guru? Słowo „guru” w sanskrycie oznacza wskazującego drogę. I taki właśnie jest cel „Old GURU Magazine” - ułatwiać wybór odpowiedniej drogi administratorom. Czy podążyć wskazaną drogą musicie już Państwo sami zadecydować...

Troszkę o X Window

X Window jest traktowany przez fanów Linuksa nieco po macoszemu. Wynika to z mocno zakorzenionego przekonania, że środowisko „Windowsowe" jest niegodne zainteresowania prawdziwych „linuksiarzy" oraz niestety z braku głębszej wiedzy na temat tego środowiska, które jest najczęściej mylone z KDE lub Gnome.

Tymczasem X Window to nie środowisko graficzne – to jedynie podstawa do budowy tego środowiska czyli oprogramowanie obsługujące interfejs graficzny, klawiaturę, myszkę lub inne urządzenia wskazujące (np. nakładki dotykowe). Co jednak najważniejsze – X Window jest dostosowane do pracy sieciowej.

Co warto wiedzieć?

Każdemu programowi X Server odpowiada adres sieciowy w formacie
<adres_maszyny>:<nr_serwera>.<numer_ekranu>
Adres ten przechowywany jest w zmiennej systemowej DISPLAY – np.: 10.1.1.25:0 oznacza pierwszy serwer i (domyślnie) pierwszy ekran maszyny o adresie IP 10.1.1.25.

W większości standardowych dystrybucji Linuksa pierwszy X serwer (o numerze 0) jest uruchamiany na siódmej konsoli (Ctrl-Alt-F7). Konsole od 1 do 6 są rezerwowane dla środowiska znakowego – kojarzone są z nimi kopie getty (wpis w /etc/inittab). Konsole 8 do 12 są w standardowej instalacji niewykorzystywane. Możemy je wykorzystać np. jako terminale graficzne serwerów (a poprawniej hostów) systemów LINUX, UNIX lub MS Windows (usługi terminalowe):

Dla systemu LINUX/UNIX (z działającym demonem xdm) wystarczy wpisać w linii komend:

X :1 -ac tty8 vt08 -query 10.1.1.231

dla systemu MS Windows najpierw musimy uruchomić X Server w tle – np.:

X :2 tty9 vt09 &

potem podać wartość zmiennej DISPLAY:

export DISPLAY=:2

i uruchomić połączenie protokołem RDP:

rdesktop -f -kpl 10.1.1.221

Po wykonaniu podanych powyżej poleceń będziemy mieli dostępne:

Na konsoli 7 – środowisko graficzne lokalnego systemu LINUX (tak jak w domyślnej instalacji),
Na konsoli 8 – dostęp do środowiska graficznego firmowego serwera systemu LINUX/UNIX,
Na konsoli 9 – dostęp do firmowego serwera usług terminalowych MS Windows.

Wystarczy teraz tylko przygotować odpowiednie skrypty, podłączyć je np. pod ikonki w KDE i po przyjściu do pracy na naszym notebooku będziemy mogli korzystać z zasobów sieciowych firmy.

X zagnieżdżone w X – czyli Xnest

Jeśli w naszym systemie LINUX zainstalowaliśmy dodatkowe rozszerzenia Xorg, to będziemy mogli skorzystać z jeszcze jednej możliwości – uruchomienia X terminala jako okna na naszym pulpicie. Służy do tego program Xnest.

Należy pamiętać, że oknu Xnest powinniśmy przyporządkować unikalną wartość zmiennej DISPLAY – na przykład wydając komendę:

Xnest :3

Okno Xnest otrzyma w tym przypadku numer 3, zaś otwarte zostanie na konsoli, na którą wskazuje aktualna wartość zmiennej DISPLAY np. dla domyślnego pulpitu lokalnego będzie to :0.0 .

W oknie Xnest możemy uruchamiać dowolne programy – należy jedynie zadbać o podanie właściwej wartości zmiennej DISPLAY – np. xclock -display :3 spowoduje, że zegarek pojawi się w oknie otwartym przez Xnest.
Możemy także wykorzystać protokół XDMCP do uzyskania połączenia z maszyną LINUX/UNIX:

Xnest :3 -query 10.1.1.231

W oknie Xnest ukaże się winietka logowania maszyny 10.1.1.231 .

X Window w ABA-X3

Przyporządkowanie konsoli w terminalu ABA-X3 jest nieco inne w celu ułatwienia konfiguracji systemu:

Domyślny X Server (:0) jest uruchamiany na konsoli, której wartość jest przechowywana jako zmienna MAIN_CONSOLE w pliku /mnt/conf/pxes/pxes.conf . Jeśli tej zmiennej nadamy wartość „0” główny X server (a co za tym idzie i pulpit użytkownika) nie będzie uruchamiany.
Dopuszczalne wartości zmiennej MAIN_CONSOLE wynoszą od 0 do 9 (konsole 10, 11 i 12 są zarezerwowane do celów administracyjnych. Wartość zmiennej MAIN_CONSOLE można zmienić za pomocą konfiguratora graficznego, albo „z palca” edytując po prostu plik.

Pozostałe X Servery mogą być uruchamiane w miarę potrzeb – i przyporządkowywane dowolnej konsoli systemowej. Dzięki temu np. sekwencja Ctrl-Alt-F1 może uruchamiać dostęp do serwera MS Windows (usługi terminalowe), Ctrl-Alt-F2 – do określonego programu (np. Płatnika ZUS) zainstalowanego na tym samym lub innym serwerze, Ctrl-Alt-F3 – dostęp do maszyny LINUX, a Ctrl-Alt-F4 – przeglądarkę WWW (lokalną – lub zdalną w zależności od wyboru administratora).

Terminale ABA-X3 wyposażyliśmy także w Xnest, możliwość podłączania ekranów dotykowych oraz wiele innych ułatwień (X messaging itp.).
Nie bez znaczenia jest również intuicyjny interfejs administracyjny dostępny przez WWW oraz system automatycznej zdalnej konfiguracji.

O dalszych elementach środowiska graficznego opartego o X Window – programie zarządzania oknami (Window Manager) oraz obsługi pulpitu – w następnym numerze „GURU”.

Nieco o bezpieczeństwie – prawdziwym!

Gazety (Gazeta Wyborcza z 17 sierpnia 2009 r) znów doniosły o kradzieży notebooka:

Zaginął kolejny laptop z danymi w sprawie Olewnika

- przy okazji z prywatnego mieszkania skradziono także dyktafon z ważnymi zapisami. No cóż, dla kogoś ta sprawa jest widocznie bardzo niewygodna, jednak znów trzeba przypomnieć starą, dobrą zasadę bezpieczeństwa systemów komputerowych:

Nie istnieje oprogramowanie, które jest w stanie skutecznie zabezpieczyć sprzęt!

Jeśli nie zadbamy o skuteczne zabezpieczenie fizyczne sprzętu, na którym składowane są istotne dane to możemy mieć pretensje tylko do siebie. Komputerów w typowych pomieszczeniach biurowych nie można uznać za wystarczająco zabezpieczone. Przekonałem się o tym na własnej skórze, kiedy okradziono w tak zwany „długi weekend" prowadzony przeze mnie Ośrodek Szkoleniowy wynosząc komputery z 2 sal szkoleniowych. Z ochranianego budynku i mimo działającego systemu alarmowego!

Pozornie kontrolowany dostęp do pomieszczeń biurowych nie wystarczy – w końcu kto będzie podejrzewał sprzątaczki – a w Polsce miał już miejsce przypadek kradzieży danych przez doktorantkę informatyki, która tylko w tym celu przyjęła stanowisko Pani Sprzątającej...

Fakt, że urządzenia zawierające dane stanowiące materiał dla Sejmowej Komisji Śledczej (sic!), a więc niewątpliwie zaliczające się do tak zwanych „danych wrażliwych" były przechowywane w prywatnym mieszkaniu asystentki posła najlepiej świadczy o poziomie ochrony danych elektronicznych w Polsce. Warto także podkreślić, że z mieszkania nie zginęły żadne inne rzeczy – ani sprzęt audiowizualny ani nawet pieniądze.

Czy przed konsekwencjami takich zdarzeń można się obronić? Oczywiście, że tak. Nie pomoże tu jednak nawet szyfrowanie danych na ich nośnikach – z twardym dyskiem notebooka włącznie ponieważ w wyniku kradzieży i tak będziemy pozbawieni dostępu do tych danych (o ile nie posiadamy aktualnej kopii awaryjnej – a z tym zwłaszcza w przypadku komputerów przenośnych bywa różnie) oraz będziemy musieli liczyć na to, że zastosowanych przez nas zabezpieczeń nie da się złamać, a z tym też bywa bardzo różnie. Na przykład wpisanie w „Google" frazy Excell forgotten password daje w wyniku ponad 17 mln odpowiedzi – w tym dostęp do gotowych programów typu „Excell password remover"!

Jedynym skutecznym rozwiązaniem jest silna ochrona fizyczna sprzętu, który jest w jakikolwiek sposób wykorzystywany do przechowywania i przetwarzania danych wrażliwych. A przecież prawie w każdej większej organizacji istnieje zazwyczaj dość dobrze zabezpieczona serwerownia. Standardem dla serwerowni są zabezpieczenia fizyczne (wzmocnione drzwi, dobre zamki, kraty antywłamaniowe), często spotyka się urządzenia do kontroli dostępu – a nawet zabezpieczenia przed ulotem elektromagnetycznym.

Serwerownia jest także wyposażona w system tworzenia kopii awaryjnych, istnieją związane z tym procedury i zasady bezpiecznego przechowywania tych kopii, programy typu „Disaster Recovery" itp. Taka profesjonalna serwerownia to właściwe miejsce do przechowywania danych. Przechowanie danych w serwerowni centralnej umożliwia również skuteczną kontrolę ich udostępniania.

Powstaje oczywiście pytanie, jak z tych danych w sposób bezpieczny korzystać. W wielu przypadkach można wykorzystać system terminalowy – wówczas całość przetwarzania danych będzie realizowana przez maszyny znajdujące się w serwerowni (a więc w bezpiecznym środowisku) – zaś transmitowane będą jedynie informacje przeznaczone do prezentacji (wyświetlenia) na ekranie terminala oraz sygnały z klawiatury i myszki. Sam terminal oczywiście nie będzie gromadził żadnych danych – zbędna więc staje się jego ochrona fizyczna (nawet jego kradzież pozostaje bez konsekwencji dla bezpieczeństwa danych).

W pewnych przypadkach konieczne jest jednak, aby użytkownik dysponował własnym komputerem do przetwarzania danych. Nic jednak nie stoi na przeszkodzie, aby taki komputer umieścić w odpowiednio zabezpieczonej serwerowni i podłączyć do niego tylko jedną końcówkę. Specjalny sprzęt do takich rozwiązań jest już dostępny – są to tak zwane Blade PC:

Kasety Blade PC umożliwiają instalację 10 jednostek PC we wspólnej obudowie przeznaczonej do montażu w typowej szafie 19”. Zapewniają więc bardzo duże „upakowanie” komputerów PC, ułatwiają rozwiązanie systemu chłodzenia, prowadzenie okablowania, stosowanie replikacji sprzętowej. Nie bez znaczenia jest również możliwość szybkiej wymiany uszkodzonej jednostki.

Możliwe jest także skorzystanie z możliwości oferowanych przez wirtualizację i udostępnianie użytkownikom maszyn wirtualnych zainstalowanych w serwerowni.

Najistotniejszą cechą powyższych rozwiązań (zdalne udostępnianie maszyn fizycznych lub wirtualnych) jest fakt, że dane nie opuszczają fizycznie zabezpieczonych pomieszczeń, a użytkownicy pracują na końcówkach, które z samej zasady swej budowy nie umożliwiają zapisu na nich żadnych danych (mogą nawet nie posiadać wewnętrznej pamięci Flash i ładować system operacyjny poprzez sieć od razu do pamięci RAM, której zawartość jest oczywiście tracona po wyłączeniu urządzenia). Transmisje sieciowe pomiędzy maszyną umieszczoną w serwerowni (data center) a terminalem można dość łatwo zabezpieczyć poprzez wprowadzenie certyfikatów (WPA_supplicant) zapewniających uwierzytelnienie terminala a nawet zaszyfrować.

Jeśli przesłanie danych na przenośny komputer (notebook) użytkownika jest uzasadnione oraz zgodne z przyjętą polityką bezpieczeństwa wynikającą z przeprowadzonej analizy ryzyka – to technicznie może to być zrealizowane bez żadnych problemów – a co ważniejsze taki fakt może być odnotowany, a co za tym idzie odpowiedzialność za poufność wydanych danych dokładnie zdefiniowana. Wiadomo również, jakie dane zostały wydane, komu i na czyje polecenie.

Uzyskanie dostępu do pomieszczeń biurowych, w których znajdują się końcówki nie stanowi większego ryzyka dla systemu – administrator może np. odłączyć w godzinach nocnych zasilanie urządzeń sieciowych (przełączników) zainstalowanych w serwerowni. Końcówki systemu będą w takim przypadku po prostu „martwe” i nie będzie możliwe uzyskanie dostępu do zasobów organizacji bez przełamania systemu fizycznych zabezpieczeń serwerowni.

Wdrożenie w takiej organizacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnego z normami rodziny ISO/IEC/PN 27000 jest proste, łatwe i przyjemne.

Na wielu spotkaniach poświęconych bezpieczeństwu systemów informatycznych podkreśla się rolę czynnika ludzkiego. Przypomina mi się wówczas jedno z Praw Myrphy'ego - „Jeśli jakaś część maszyny może być zamontowana odwrotnie, to zawsze znajdzie się ktoś, kto to zrobi”. Dlatego też inżynierowie starają się tak projektować maszyny, aby zminimalizować wpływ „czynnika ludzkiego” - zarówno przy ich montażu, jak i eksploatacji. Wiązki elektryczne współczesnego samochodu wykluczają możliwość ich błędnego połączenia – po prostu każda wtyczka pasuje tylko do właściwego dla niej gniazdka.

Warto wprowadzić podobną zasadę przy projektowaniu systemów komputerowych, zwłaszcza takich, od których wymagamy podwyższonego poziomu bezpieczeństwa – jednym słowem brać pod uwagę nieco zmodyfikowaną postać cytowanego Prawa Myrphy'ego - „Jeśli w systemie można zrobić coś, czego nie przewidział jego projektant, to zawsze znajdzie się ktoś, kto to zrobi”.

Co naprawdę w sieci piszczy?

Trudno sobie wręcz wyobrazić współczesny system komputerowy bez połączeń sieciowych. I to coraz szybszych i efektywniejszych. Gigabit Ethernet, który propagowaliśmy na naszych Konferencjach w połowie lat 90 ubiegłego wieku (jak to brzmi...) jako nowość dziś jest w codziennym użyciu – serwery, a coraz częściej i komputery klasy desktop są standardowo wyposażone w karty gigabitowe, zaś coraz większą popularność uzyskuje sieć Ethernet o prędkości 10Gbps. Fibre Channel też nie jest już egzotycznym rozwiązaniem w sieciach SAN, zaś OC12 w sieciach rozległych także nie należy do rzadkości.

Zestaw protokołów również uległ poważnym zmianom. Wiele z nich po prostu zanikło (choćby bardzo popularny niegdyś IPX/SPX), pojawiły się nowe – na przykład RDP, ICA, VoIP. W powszechnym użyciu znajdują się dziś także protokoły specjalizowane – choćby medyczny DICOM.

Rosnąca rola transmisji sieciowych, ogromny wzrost ich prędkości a tym samym objętości przesyłanych danych spowodowały, że analiza pracy sieci komputerowej w sporej organizacji stała się poważnym wyzwaniem. A sprawność sieci komputerowej to warunek efektywnego obiegu informacji w nowoczesnym przedsiębiorstwie. Administratorzy odpowiedzialni za pracę sieci powinni więc mieć do dyspozycji odpowiednie narzędzia, które umożliwią błyskawiczną diagnozę poprawności jej pracy (Network Vital Signs), określenie przyczyn ewentualnych problemów np. czy sygnalizowane przez użytkowników opóźnienia w pracy systemu mają swą przyczynę w sieci czy też w dużym obciążeniu serwerów, sprawdzenie jak zachowa się infrastruktura sieciowa jeśli obciążymy ją dodatkowym ruchem, przyczynami przerw w połączeniach VoIP itp. Co ważne – profesjonalny analizator sieciowy powinien umożliwiać dokonywanie analizy „historycznej" - np. co było przyczyną zakłóceń, które wystąpiły około godziny 9:15 rano, a także pozwalać na analizę pracy łączy agregowanych (np. połączenia 2x1000BaseLX z lokacją zapasową).

Większość nawet bardzo wyrafinowanych wymagań administratorów w zakresie analizy sieci spełnia dystrybuowany przez firmę ABA Network Instruments OBSERVER (to już jego 13 wersja!). Warto zwłaszcza polecić gotowe do pracy wielokrotnie nagradzane analizatory typu „portable" (na obrazku):

Są one dostarczane w kilku odmianach:
Gigabit (do 8 monitorowanych połączeń równocześnie),
10 Gigabit o powiększonej do 16 GB pamięci RAM,
Fibre Channel Gen2,
WAN (T1/E1, DS3/T3/E3, OC3x/OC12c),
oraz mogą być wyposażone w szybkie podsystemy dyskowe wykorzystywane do przechowywania danych „historycznych" o pojemności 4TB. Maksymalnie z dodatkową kasetą z dyskami GigaStor obsługuje do 288TB pamięci dyskowej!

Możliwości samego analizatora można łatwo sprawdzić pobierając wersję demo ze strony producenta – www.networkinstruments.com

Ale nawet najlepszy analizator wymaga podłączenia do sieci. Ponieważ znakomita większość współczesnych sieci wykorzystuje przełączniki najprostszą metodą jest wykorzystanie portu przełącznika SPAN (Switch Port Analyser – mirroring port). Niestety, to rozwiązanie, choć najprostsze ma sporo wad ze względu na wykorzystywanie wewnętrznej struktury przełącznika – np. przełącznik eliminuje błędne ramki Ethernet – a więc niemożliwe jest wykrycie tego typu błędów generowanych przez uszkodzone stacje, które mogą w znacznym stopniu zakłócać pracę sieci. Niemożliwe jest również analizowanie ruchu na łączach agregowanych (zwielokratnianych), które są coraz częściej stosowane.

Rozwiązaniem tego problemu są proste i stosunkowo niedrogie urządzenia -nTAP (network Test Access Point). Są one włączane bezpośrednio do kabla sieciowego - dostępne są różne wersje nTAP zarówno dla kabli miedzianych, jak i światłowodowych 62,5um, 50 um, 9um, długości fali (okna) itp. Urządzenia nTAP nie tylko udostępniają analizatorowi cały ruch sieciowy (łącznie z zakłóceniami, błędami itp.) w trybie Full Duplex, lecz również pozwalają na równoczesne podłączenie do analizatora 2 lub 4 łączy agregowanych. Analizator może wówczas śledzić ruch na wszystkich parach połączeń równocześnie – i np. skojarzyć poprawnie pakiety SYN z odpowiadającymi im pakietami ACK nawet wówczas gdy są one przesyłane różnymi drogami fizycznymi.

Porównanie wyników analizy sieci z wykorzystaniem SPAN oraz nTAP pozwala na dokładne określenie wpływu samego przełącznika na pracę sieci (np. wykrycie blokowania, określenie ruchu wewnątrz przełącznika itp.).

Warto zwrócić uwagę, że podczas analizy sieci spotykamy się z dwoma problemami. Pierwszym jest zapewnienie efektywnej rejestracji (z prędkością Wire Speed) całego ruchu sieciowego oraz jego zapamiętanie w celu dalszej analizy. Aby je spełnić konieczne jest zaangażowanie sprzętu o odpowiedniej wydajności oraz interfejsów sieciowych zbudowanych specjalnie pod kątem analizy transmisji. Oczywiście musimy dysponować także szybkim i pojemnym podsystemem dyskowym.
Z tego właśnie powodu celowe jest rozważenie zakupu kompletnego, gotowego do pracy analizatora typu „portable" w miejsce zakupu samego oprogramowania analizującego i zainstalowania go na własnym sprzęcie (PC z systemem MS WINDOWS XP Pro). Analizator typu „portable" jest odpowiednio konfigurowany fabrycznie i oczywiście objęty pełną gwarancją producenta jako całość.

Drugim problemem jest analiza zebranych danych. Tu największą rolę pełni oprogramowanie. Należy zdać sobie sprawę, że przy ruchu „gigabitowym" ilość danych zebranych nawet w stosunkowo krótkim czasie może być bardzo znaczna. Oprogramowanie powinno więc pozwalać na szybkie wyszukanie interesujących nas informacji w dużym (lub bardzo dużym) zbiorze danych, znalezienie interesujących korelacji i zaprezentowanie wyników w sposób przyjazny dla administratora. Tą rolę pełni z równym powodzeniem sam OBSERVER – niezależnie od tego czy jest on zainstalowany na zwykłym komputerze czy też na maszynie specjalizowanej.
Funkcje udostępniane administratorowi będą w obu przypadkach identyczne – zmianie ulegnie jedynie prędkość odpowiedzi oprogramowania.

Analizatory typu „portable" są flagowymi produktami firmy Network Instruments. Warto się z nimi zapoznać, aby ocenić w pełni możliwości nowoczesnych analizatorów sieciowych. Niestety, cena tych urządzeń jest adekwatna do ich jakości i funkcjonalności. W wielu przypadkach tak znaczna wydajność nie jest konieczna i funkcję analizatora spełni dobrze silny notebook z zainstalowanym OBSERVEREM. Niestety, będziemy ograniczeni również tylko do analizy sieci Ethernet.

Firma Network Instruments to swego rodzaju ewenement w skali światowej – istnieje 15 lat (współpracujemy z nią od początku jej istnienia), dostarczyła już około 50000 licencji na oprogramowanie OBSERVER – i co najważniejsze nie oferuje praktycznie (oprócz Link Analyst) żadnego innego produktu! Skala jej działalności także w Europie (aż 3 biura regionalne!) oraz bogata lista referencyjna najlepiej świadczą o jakości i uznaniu dla OBSERVERA.