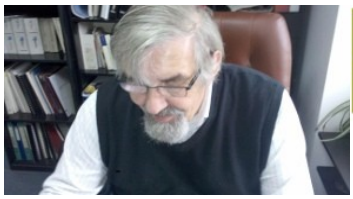


Old Man GURU Magazine

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

Numer 25/2011 23 styczeń 2011

No i mamy wysyp ataków sieciowych. Nie mam zamiaru dyskutować nad ich przyczynami, stroną etyczną oraz prawną. Myślę jednak, że warto się zastanowić nad tym, czy nasze sieci są należycie nadzorowane i czy ich administratorzy dysponują narzędziami, które monitorują przebieg ataku i czy gromadzone są dane, które mogą być w razie potrzeby użyte jako pomoc w jego analizie oraz w ewentualnym późniejszym śledztwie.

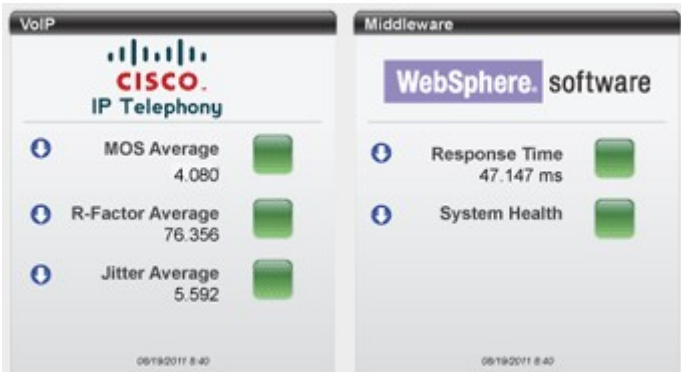
Nieodparcie nasuwa mi się porównanie z tak zwanymi „czarnymi skrzynkami", które jak dziś wszystkim wiadomo są wykorzystywane w lotnictwie, komunikacji morskiej itp. Zapisane w tych urządzeniach dane niejednokrotnie pozwoliły lub wręcz umożliwiły odtworzenie przyczyn i przebiegu zdarzenia, wypadku lub katastrofy.

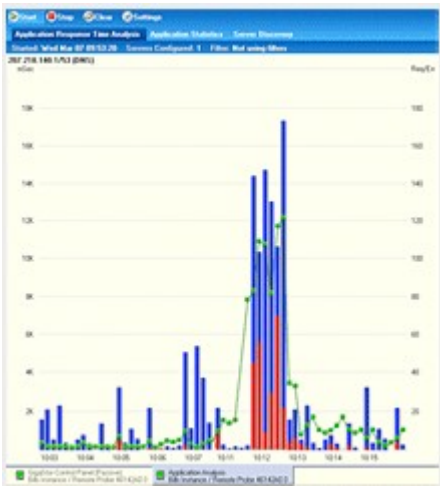
Chciałbym Państwu przedstawić urządzenia (a raczej rozwiązanie), które realizują podobną funkcję dla sieci komputerowych. Ich zadaniem jest zapis wszystkich bez wyjątku transmisji sieciowych w odpowiednich, przeznaczonych tylko do tego celu macierzach dyskowych o pojemności umożliwiającej przechowywanie zapisu nawet przez okres kilkunastu dni w celu ewentualnego przeprowadzenia szczegółowej ich analizy. Warto wiedzieć, że nowoczesne urządzania tego typu takie jak Network Instruments Gigastor umożliwiają nieprzerwany zapis transmisji sieciowych 10 Gigabit Ethernet z pełną prędkością Wire Speed przez okres ponad 40 godzin!

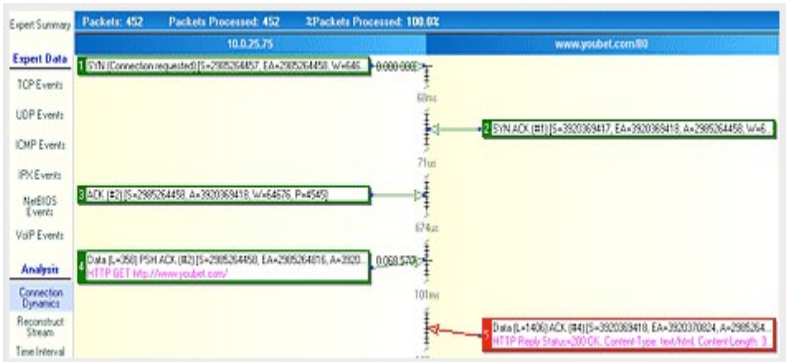
Oczywiście, sam zapis tak wielu danych (około 144 TB) nie jest zbyt wiele wart, jeśli nie dysponujemy odpowiednimi i bardzo wydajnymi narzędziami do jego analizy. Technika taka nosi nazwę RNA (Retrospective Network Analysis). Dzięki zapisowi dyskowemu transmisji sieciowych możemy z łatwością „cofnąć się w czasie" i sprawdzić, jakie połączenia sieciowe z naszym serwerem były realizowane np. przedwczoraj. Co więcej, informacje te możemy uzyskać w formie graficznej (np. w postaci wykresów i diagramów), co znacznie przyspiesza proces analizy i ułatwia wyciąganie właściwych wniosków.

Warto podkreślić, że urządzenia firmy Network Instruments współpracują znakomicie z rozwiązaniami innych producentów – takich jak np. CISCO, IBM, ORACLE czy Microsoft.

Dane do zapisu i analizy mogą być bezpośrednio pobierane z kabla sieciowego za pomocą specjalnych urządzeń nTAP pełniących rolę rozgałęźników (splitterów) również z możliwością buforowania. Unika się w ten sposób wpływu oprogramowania urządzeń sieciowych, systemów operacyjnych itp. i co może nawet ważniejsze zapisane dane są bardzo dobrze chronione i atakujący nie ma praktycznie żadnej możliwości usunięcia śladów swych działań.







Od skrótowej informacji do analizy czasowej - różne typu prezentacji danych

Analiza transmisji sieciowych wymaga dwóch podstawowych działań:

Po pierwsze – dane trzeba zapisać.

Jeśli zamierzamy później je analizować i wyciągać z tej analizy konkretne wnioski trzeba zapisać **wszystkie** transmisje sieciowe. A współczesne sieci komputerowe są szybkie oraz transmitują duże ilości danych. Jakich pojemności dysków będzie wymagał ich zapis?

Załóżmy, że nasza sieć jest oparta o Gigabit Ethernet i obciążona średnio w 30%. Pojemność dyskowa niezbędna do zachowania transmisji z 3 dni wyniesie wówczas około 8 TB. W praktyce taka pojemność jest niezbędna, aby można było odtworzyć, co działo się w naszej sieci podczas weekendu. Jeśli obciążenie sieci wzrośnie do 70% (cały czas mowa o sieci 1 Gbps i jednym połączeniu Full Duplex) to aby uzyskać zapis z trzech kolejnych dni będziemy już musieli skorzystać z pamięci o pojemności rzędu 24 TB.

Dla coraz popularniejszych sieci 10 Gbps będą oczywiście niezbędne większe pojemności pamięci – przy 30% obciążenie dla zapisu przez trzy dni będzie nam niezbędne 96 TB, zaś przy 70% obciążeniu średnim ponad 200 TB.

Sama pojemność dyskowa to oczywiście nie wszystko. Komputer (a raczej specjalizowane urządzenie typu „appliance", który ma służyć do zapisu i przechowywania transmisji sieciowych musi dysponować odpowiednią mocą (wiele procesorów lub rdzeni), pracować w trybie 64 bitowym i dysponować odpowiednią pamięcią RAM (minimum 12 GB na system oraz 24 GB dla oprogramowania i buforowania). Jednak i to może się okazać niewystarczające jeśli będziemy chcieli zapisywać transmisje z prędkością „Wire Speed" w trybie Full Duplex 10 Gbps to musimy zdać sobie sprawę, że konieczny będzie zapis na dyskach twardych z prędkością 20 Gigabit na sekundę – a nawet nieco więcej, ponieważ niezbędny będzie zapis dodatkowych informacji (znaczników). Wymagana prędkość zapisu sięga więc około 2/3 możliwości popularnej magistrali SATA II, jednak należy podkreślić, że mamy tu do czynienia z koniecznością ciągłego zapisu przez dłuższy czas przy zachowaniu pełnej prędkości. Aby zapewnić zapis w trybie Full Wire Speed prze okres na przykład kilku dni konieczne jest zastosowanie specjalizowanych macierzy dyskowych.

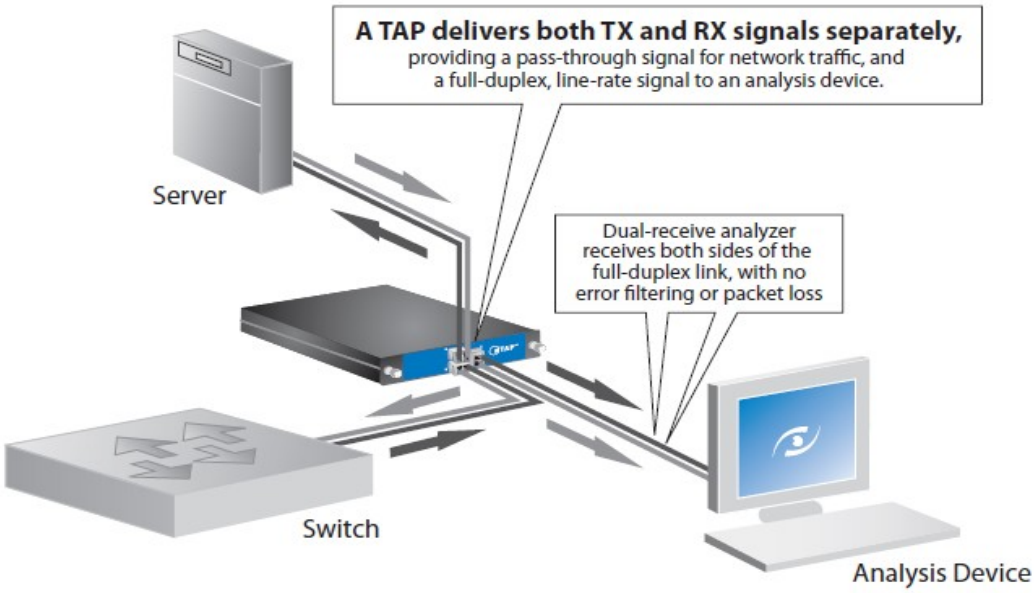
Drugim problemem w sieciach 10 Gbps jest zachowanie odpowiedniej rozdzielczości czasowej. Szeroko wykorzystywany do synchronizacji czasu protokół NTP zapewnia rozdzielczość rzędu 30 ms (maksymalnie 10 ms). Dla sieci potrzebna jest co najmniej dziesięć razy lepsza, a najlepiej aby osiągała wartości rzędu 100 ns. Najprościej wykorzystać w tym celu wzorzec czasu, który zapewnia system GPS. Można uzyskać w ten sposób rozdzielczość analizy czasowej rzędu 150 ns.

Sposób pobierania sygnału

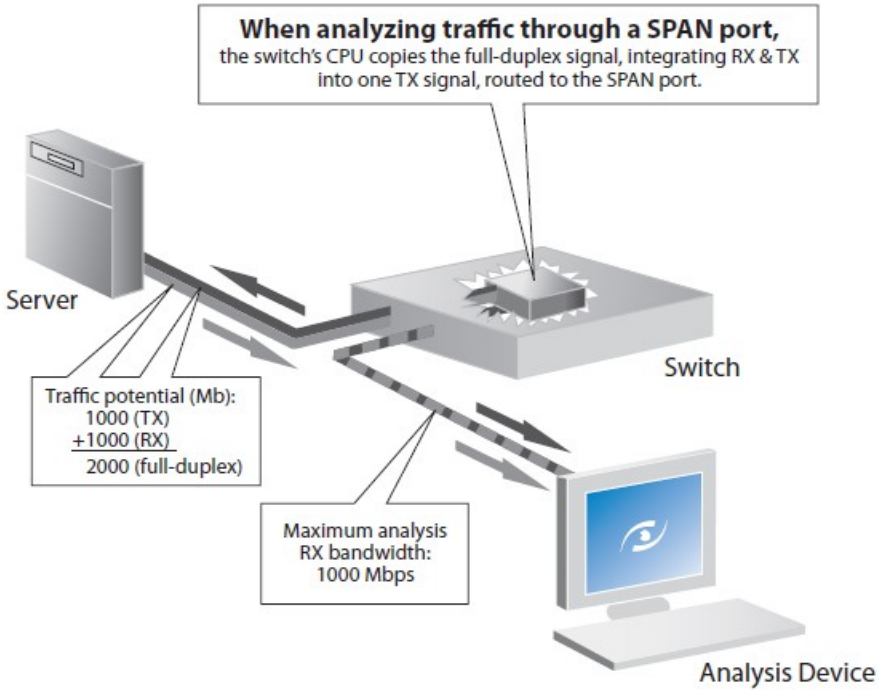
Zapis transmisji sieciowych w celu ich późniejszej kompleksowej analizy ma sens tylko wówczas, gdy możemy zapisać wszystkie dane. Najprostszą i pewną metodą jest bezpośrednie podłączenie się do kabla sieciowego – np. prowadzącego do serwera.

Służą do tego urządzenia nTAP (network Testing Access Point). Nie wpływają one na transmisję danych, lecz dzięki rozgałęzieniu sygnału trafiają one również na dodatkowe porty, które są podłączone do urządzenia zapisującego transmisję (analizatora). Konieczne są oczywiście dwa porty, ponieważ monitorujemy transmisje w trybie Full Duplex.

Na kolejnej stronie zamieściłem rysunek ilustrujący taki sposób pobierania sygnału (za zezwoleniem firmy Network Instruments). Proszę zwrócić uwagę na kierunek przesyłania danych określany przez strzałki.

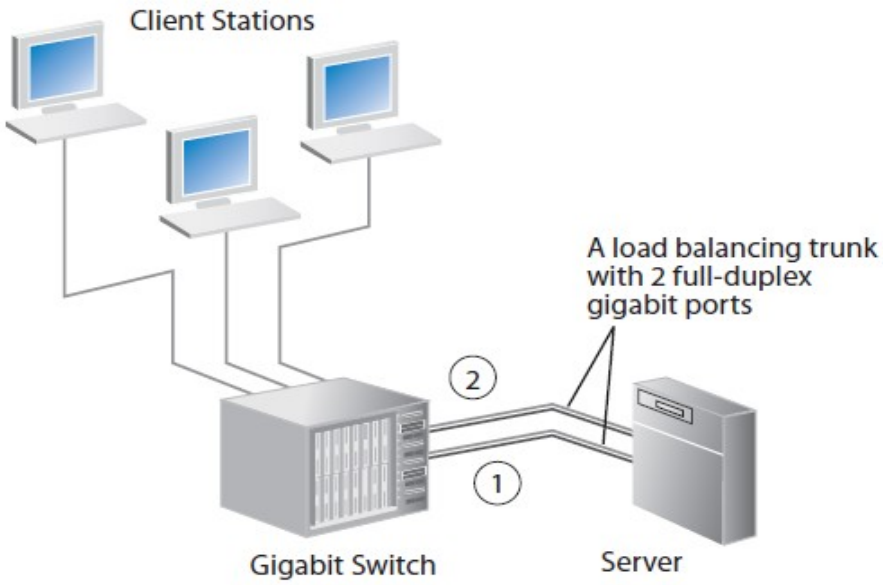


W wielu prostych instalacjach do jako źródło sygnału wykorzystywany jest tak zwany „port mirroring". W urządzeniach firmy CISCO stosowana jest nazwa SPAN (Switched Port Analyzer), inni producenci często stosują własne nazwy. Metodę tą ilustruje kolejny rysunek (również z materiałów firmy Network System):



Warto zwrócić uwagę, że w przypadku wykorzystywania portu SPAN dane do analizatora są transmitowane za pomocą jednego połączenia, zaś transmisje sieciowe są realizowane w trybie Full Duplex (Rx i Tx mogą transmitować równocześnie). Wynika stąd, że połączenie do analizatora ma przepustowość 1 Gbps (dla sieci Gigabit Ethernet). Wydajność połączenia do analizatora nie pozwala więc na przesłanie wszystkich danych. Spowoduje to utratę części zapisywanych informacji w chwilach maksymalnego obciążenia sieci, a tym samym uniemożliwi przeprowadzenie poprawnej i kompletnej analizy.

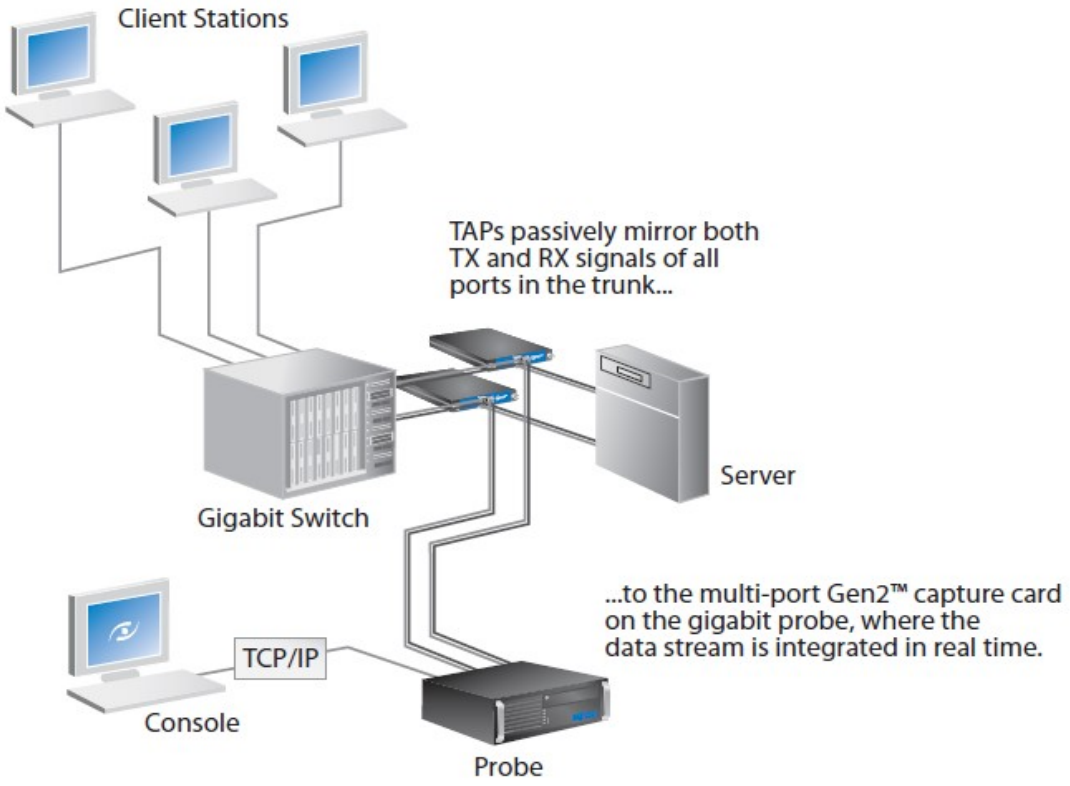
Kolejnym wyzwaniem dla jest analiza łączy zwielokratnianych, które są często stosowane do podłączania serwerów.



In client/server conversations, a packet going in either direction could travel on either port of the trunk.

Analizator musi w takim przypadku nie tylko mieć możliwość zapisania całego ruchu, lecz również odpowiednie zestawienie informacji pochodzących z obu połączeń. Rozwiązania tego typu są dość popularne, ponieważ można je realizować wykorzystując standardowy sprzęt dla sieci gigabit ethernet. Połączenia zbiorcze z serwerem pozwala na obsługę szerszego pasma transmisji.

Należy jednak wziąć pod uwagę, że w nowoczesnych rozwiązaniach o tym, które łącze zostanie w danej chwili wykorzystane decyduje aktualne obciążenie – a więc pakiety odpowiadające określonej sesji mogą być przesyłane przez dowolne łącze, a zadaniem analizatora jest ich odpowiednie uszeregowanie.



Analiza transmisji realizowanych przez serwer jest w takim przypadku możliwa jedynie za pomocą rozgałęźników nTAP. W przypadku, który ilustruje rysunek konieczne będzie użycie dwóch takich urządzeń oraz próbnika wyposażonego w dwa porty. Umożliwi to zintegrowanie wszystkich strumieni danych oraz przeprowadzenie pełnej ich analizy. Oczywiście w przypadku większej liczby łączy zwielokrotnionych będziemy potrzebować odpowiedniej liczby nTAPs oraz próbnika z większą ilością portów.

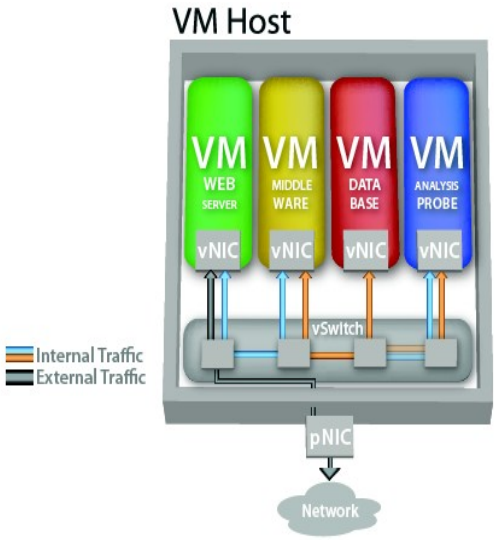
Wirtualizacja i analiza sieci:

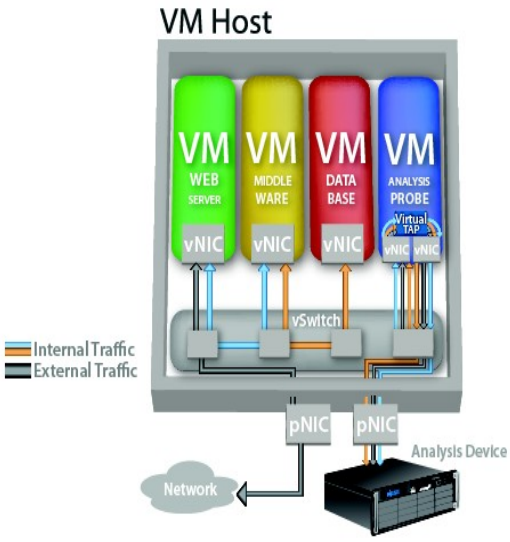
Wirtualizacja serwerów stała się bardzo popularna. W rezultacie często mamy do czynienia z sytuacją, że na jednym komputerze pracuje wiele serwerów. Oczywiście komunikują się one między sobą oraz z siecią zewnętrzną. Bardzo częstym rozwiązaniem jest wykorzystywanie w tym celu mostu (bridge):

```
szef:~ # brctl show
bridge name    bridge id      STP enabled    interfaces
pan0      8000.1cc1de9c3c10   no             eth0
                                              vnet0
                                              vnet1
```

W powyższym przykładzie dwie maszyny wirtualne (interfejsy vnet0 oraz vnet1) korzystają w z mostu pan0 (przykład dotyczy systemu SuSE Enterprise Linux). Zgodnie z zasadą działania bridge separuje segmenty sieciowe w 2 warstwie modelu ISO/OSI – tak więc ruch pomiędzy maszynami vnet0 i vnet1 będzie realizowany wewnątrz systemu gospodarza. Rozwiązanie takie jest oczywiście korzystne ze względu na brak obciążania interfejsu fizycznego transmisjami pomiędzy maszynami wirtualnymi (np. serwerem WWW i serwerem bazy danych) utrudnia jednak analizę tego ruchu. W tym przypadku będzie nas oczywiście przede wszystkim czasy odpowiedzi maszyn wirtualnych i ogólna sprawność zwirtualizowanego rozwiązania.

Jeśli chcemy monitorować ruch pomiędzy maszynami wirtualnymi konieczne będzie utworzenie kolejnej maszyny wirtualnej, która będzie pełniła rolę „Network Probe”:





Dostęp do maszyny, na której pracuje analizator możemy realizować za pomocą standardowego połączenia sieciowego lub dodatkowego interfejsu sieciowego (patrz powyższe schematy). Umożliwia to analizę ruchu pomiędzy serwerami oraz nadzór nad działaniem całego zwirtualizowanego systemu Serwer WWW – MiddleWare – Baza danych. Zapis tego ruchu jest kluczowy w przypadku potrzeby udokumentowania ataku na nasz system (np. nieautoryzowanego dostępu do bazy danych).

Czy sieciowa „czarna skrzynka” jest potrzebna?

Dowodzi to popularność takich rozwiązań na Świecie. Znajomość ruchu sieciowego, który był realizowany w dowolnym czasie w przeszłości to nie tylko „informatyka śledcza”. Dysponując takimi informacjami możemy również sprawdzić, czy nasz system nie jest okresowo przeciążany oraz czy czasy dostępu do danych lub wydajność „streamingu” (wraz z IPTV), VoIP itp.