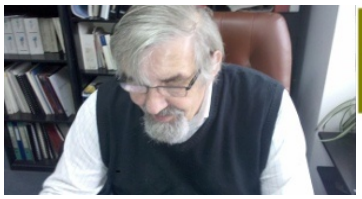
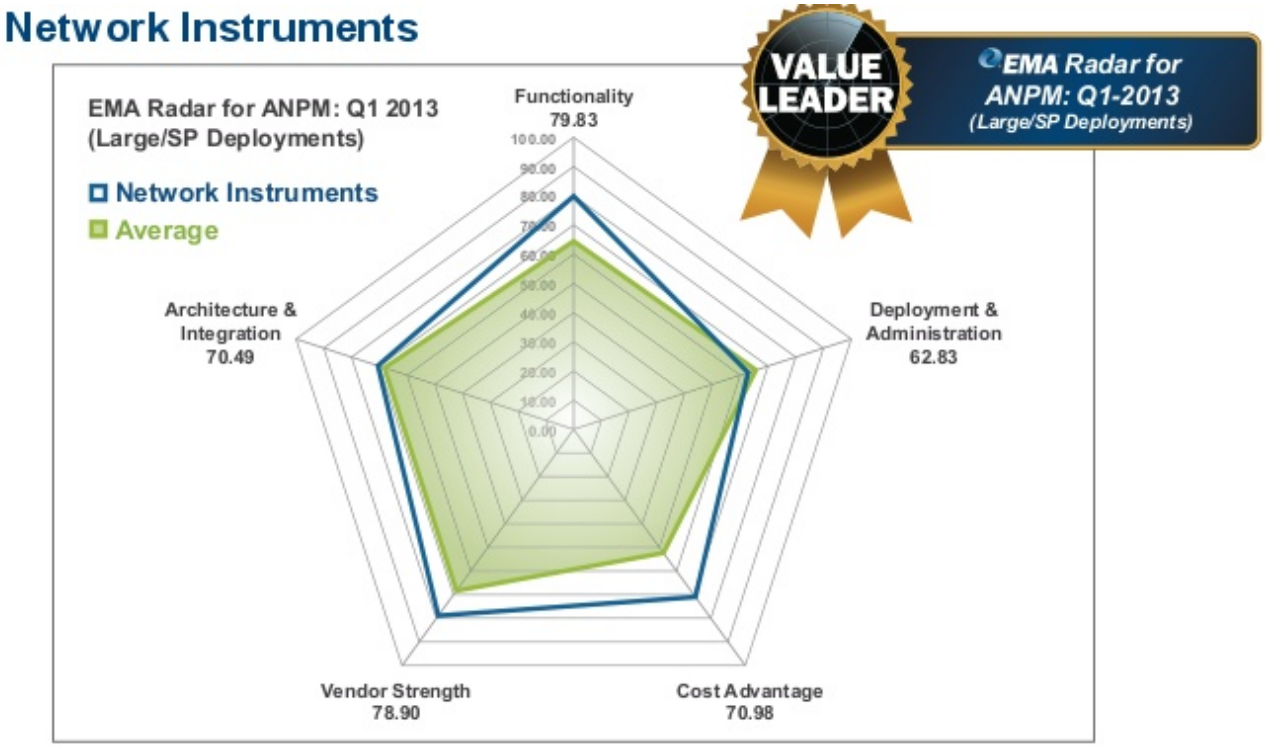


Old Man GURU Magazine

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

Numer 36/2013 3 czerwiec 2013

Network Instruments po raz kolejny pokonuje konkurencję!

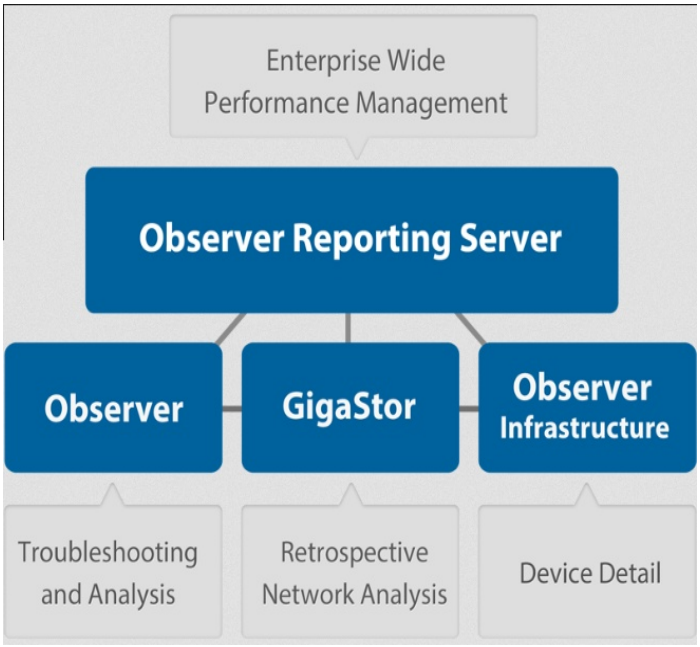


Firma analityczna EMA - http://www.enterprisemanagement.com przeprowadziła szczegółową ocenę rozwiązań Applicationaware Network Performance Management (ANPM). Pod uwagę wzięto produkty 24 czołowych dostawców. Szczegółowa analiza wykazała, że zarówno pod względem funkcjonalności, jak i ceny rozwiązanie naszego wieloletniego Partnera - firmy Network Systems góruje nad rozwiązaniami konkurencji.

W rezultacie otrzymało ono tytuł „Value Lider" wyprzedzając rozwiązania CA Technologies, EMC, Fluke, HP, NetScout i innych producentów podobnych rozwiązań.

Pełny raport z analizy EMA można pobrać ze strony Network Instruments (www.networkinstruments.com). Warto podkreślić, że jeśli wziąć pod uwagę stosunek funkcjonalności do ceny rozwiązania to jego przewaga na tle konkurencji jeszcze wzrośnie.

Pomimo, że samo wyróżnienie dla NI przyznane zostało w klasie „Large/SP Deployments” to w raporcie podkreślono skalowalność oraz elastyczność rozwiązania, dzięki czemu można go z powodzeniem stosować zarówno w stosunkowo niewielkich instalacjach (zawierających kilkadziesiąt do kilkuset stacji sieciowych) jak i w wielkich sieciach korporacyjnych, a nawet telekomunikacyjnych. Zwracają także uwagę urządzenia przenośne typu „portable”, które są przeznaczone głównie dla integratorów systemów oraz firm serwisujących złożone sieci IT.



Dla niewielkich sieci:

Dla takich sieci przeznaczone są przede wszystkich rozwiązania programowe (software only solutions) dla systemów rodziny Windows. Aby w pełni wykorzystać właściwości oprogramowania NI Observer konieczne jest stosowanie wydajnego komputera wyposażonego w czterordzeniowy procesor klasy Pentium oraz 8 GB RAM (minimalne wymagania to dwurdzeniowy procesor i 2 GB RAM).

Oprogramowanie NI Observer można wykorzystywać w razie potrzeby, a więc nie wymaga ono dedykowanego komputera. Warto jednak wyposażyć go w specjalną kartę sieciową, która nie będzie dokonywać żadnych operacji (np. zatrzymywania błędnych ramek Ethernet). Jedynie takie karty umożliwiają wykrycie źródła tego typu błędów – praca karty w trybie nasłuchiwania (*promiscuous mode)* nie zapewnia wykrywania takich błędów, ponieważ w typowych kartach oprogramowanie wewnętrzne odrzuca błędne ramki, a więc nie docierają one do programu analizatora.

Jeśli sieć ma być monitorowana w wielu punktach można zastosować software probe (oprogramowanie dla systemu MS Windows do zainstalowania we własnym zakresie) lub hardware probe (gotowe do pracy „network appliances” wraz z systemem operacyjnym). Wszystkie próbniki niezależnie od rodzaju mogą być obsługiwane z jednego stanowiska – OBSERVER Console.

Duże instalacje:

Rozwiązanie Network Instruments OBSERVER może być bardzo łatwo rozbudowywane i zdobyło zasłużoną popularność w dużych sieciach, co potwierdza przyznany tytuł Lidera – wśród klientów firmy NI znajdują się między innymi BT, Deutsche Telecom, France Telecom, Deutsche Bank, ING, HSBC, Ford, US Navy, CISCO i wielu innych. Listę wybranych referencji można zobaczyć pod adresem:
https://www.networkinstruments.com/about/customers/list.php

Dla takich instalacji przeznaczone są przede wszystkim specjalizowane urządzenia (network appliances) o nazwie Gigastor wyposażone w specjalne karty sieciowe (Gen2) oraz pamięci dyskowe umożliwiające zapis wszystkich transmisji sieciowych w trybie Full Duplex z prędkością WireSpeed aż do 40 Gbps. Ich pojemność dyskowa może wynosić od 2 TB aż do 5 PB (Gigastor Expandable).

Najważniejsze korzyści, które uzyskują użytkownicy tego typu urządzeń są następujące:

Retrospective Analysis:

Zapis wszystkich transmisji sieciowych umożliwia sprawdzenie, dlaczego w określonym czasie nastąpiły zakłócenia w pracy sieci. W praktyce bardzo często mamy do czynienia z przypadkami, że użytkownicy kontaktują się z „Help Deskiem" skarżąc się np. na wolną pracę sieci. Takie zakłócenia mają bardzo często charakter przejściowy i nim „sprawa" dotrze do administratora sieci okazuje się, że wszystko już jest w porządku. I użytkownik otrzymuje „standardową" odpowiedź „u nas wszystko działa dobrze".

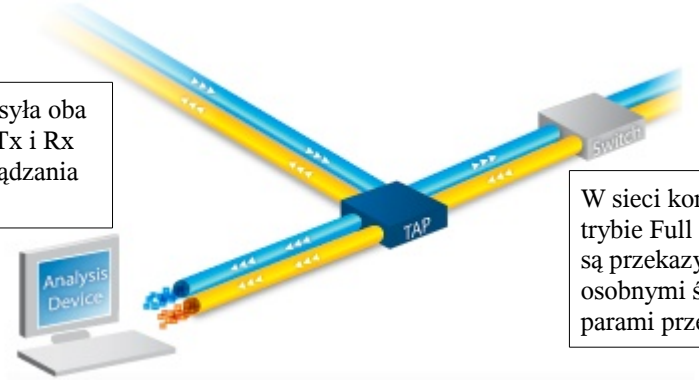
Dysponując zapisem transmisji administrator może odtworzyć transmisje, które były realizowane w czasie, gdy wystąpiły zakłócenia i wykorzystując możliwości systemu eksperckiego sprawdzić, co było powodem tych zakłóceń. Dzięki takiej możliwości administrator nie jest zdany jedynie na własną intuicję – a to pozwala uniknąć wielu zbędnych lub nie trafionych inwestycji.

Network forescenics:

Problem pełnej kontroli nad transmisjami sieciowymi i możliwość ich odtworzenia ma zasadnicze znaczenie dla informatyki śledczej. Zapis transmisji sieciowych oraz efektywny system ich filtrowania, które zapewniają rozwiązania firmy Network Systems pozwala na dokładne odtworzenie przebiegu ataku sieciowego – a tym samym metod, które wykorzystał atakujący oraz ułatwia dotarcie do źródła (źródeł) ataku.

Szczególne znaczenie ma zapewnienie autentyczności i obiektywności takiego zapisu oraz zabezpieczenie go przed celowym wyłączeniem lub zniekształceniem przez atakującego. Urządzenia firmy Network Instruments mogą być podłączane do sieci za pomocą pasywnych rozgałęźników - nTAP (dostępnych w wersjach dla instalacji miedzianych lub światłowodowych). Zasadą ich pracy jest przekazywanie do urządzenia zapisującego wszystkich transmisji Tx oraz Rx realizowanych w trybie Full Duplex dwoma osobnymi kanałami.

Rozgałęźnik (TAP) przesyła oba transmitowane sygnały Tx i Rx dwoma kanałami do urządzania analizującego.



W sieci komputerowej pracującej w trybie Full Duplex sygnały Tx i Rx są przekazywane w obu kierunkach osobnymi światłowodami lub parami przewodów miedzianych.

Urządzenie analizujące jedynie odbiera transmisje sieciowe, a nie nadaje żadnych informacji. Tym samym nie sygnalizuje swojej obecności w sieci. W przypadku włączenia urządzenia analizującego wprost do portu przełącznika (SPAN – Switch Port ANalyzer) występuje kilka niekorzystnych zjawisk:

- w przypadku korzystania z jednego portu SPAN i pełnym wykorzystywaniu pasma Full Duplex część pakietów (w granicznym przypadku aż połowa) nie dociera do analizatora (pasmo jednego kanału nie jest wystarczające do przekazania obu transmisji Tx i Rx w przypadku znacznego obciążenia sieci),
- Skuteczny atak na przełącznik (switch) umożliwia wyłączenie zapisu transmisji sieciowych – wystarczy wyłączenie portu SPAN,
- Konieczne jest zwrócenie uwagi na priorytet obsługi portu SPAN przez przełącznik,
- Do analizatora nie docierają pakiety odrzucane przez przełącznik co uniemożliwia detekcję błędów występujących z najniższych warstwach modelu ISO/OSI.
-

Efekty te nie występują w przypadku zastosowania rozgałęźników nTAP.

Unified Communications:

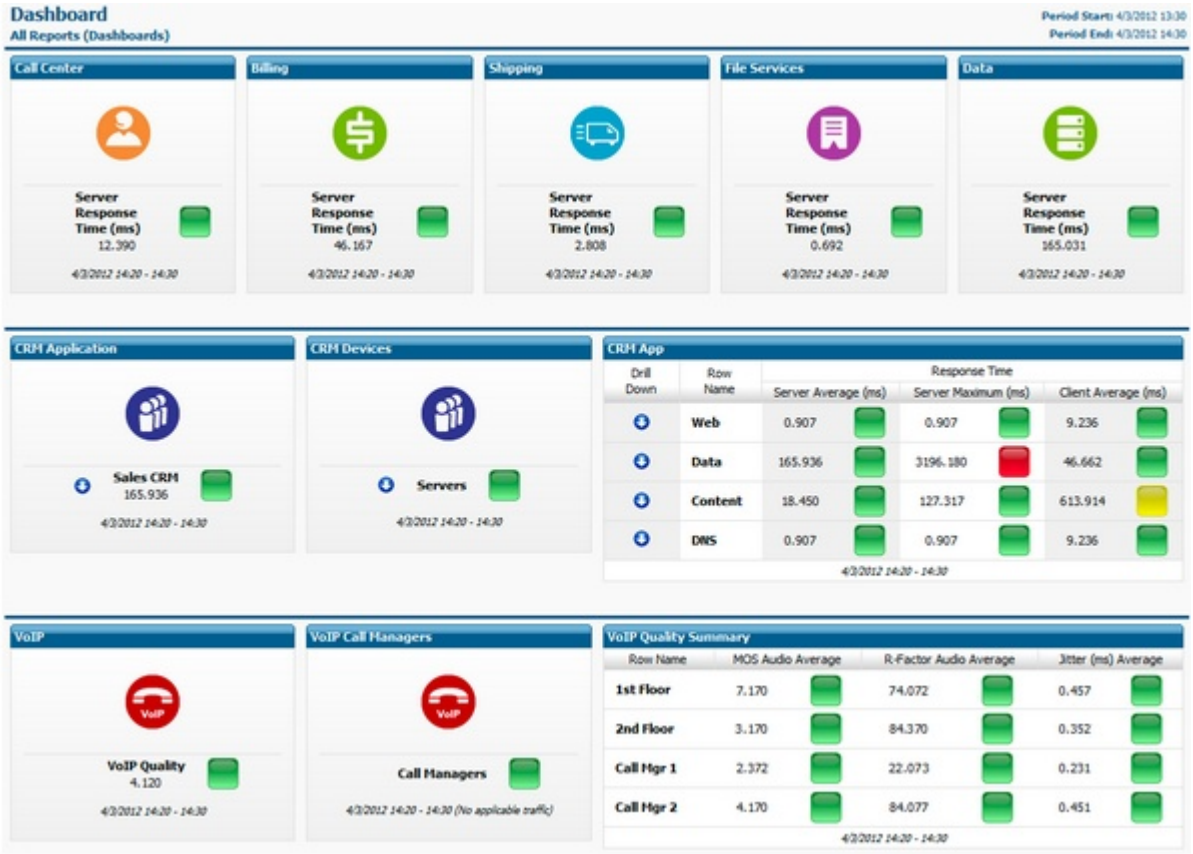
Współczesna sieć komputerowa to nie tylko klasyczna transmisja danych – to zestaw szeregu innych usług - VoIP, telekonferencje, IPTV itp. Poprawna praca, a przede wszystkim płynna praca tych usług wymaga monitorowania zaawansowanych parametrów sieci takich jak „round trip delay", „jitter". Ze względu na to, że wiele firm stosuje własne rozwiązania konieczna jest implementacja różnych „standardów" - Cisco, Avaya, Nortel, Microsoft (np. Lynx)...
Sieć wykorzystują również protokoły specjalizowane – na przykład finansowy (FIX – www.fixprotocol.org), medyczny (DICOM www.medicalimaging.org).

Możliwość separacji ruchu podczas analizy oraz określenia specyficznych parametrów, które wpływają na jakość transmisji (również dźwięku i obrazu), wpływu wprowadzenia nowych usług – w tym także jednolitej komunikacji (Unified Communications) na tradycyjne transmisje sieciowe to zasadnicze zadania stawiane systemowi nadzorowi pracy sieci, które spełniają rozwiązania firmy Network Systems.

Monitorowanie pracy aplikacji i praca w chmurach:

Truizmem jest stwierdzenie, że odbiorców usług realizowanych w chmurach – niezależnie - publicznych oraz prywatnych interesuje dostępność zasobów i wydajność udostępnianych aplikacji. Usługodawcy udostępniający chmury wykorzystują często bardzo złożone środowiska rozproszone i zwirtualizowane, co stawia wysokie wymagania systemom do analizy ich pracy.

Dzięki technice „Distributed Network Analysis" użytkownicy rozwiązań Network Instruments mogą bez problemów uzyskiwać aktualne oraz historyczne informacje o wydajności aplikacji oraz serwerów. Dane zbierane przez dowolne próbniki mogą być przekazane do specjalnego urządzenia o nazwie NI Observer Reporting Server. Administrator systemu uzyska w ten sposób zbiorcze informacje o aktualnym stanie sieci, historii jej pracy, obciążeniu maszyn (fizycznych i wirtualnych), wydajności programów użytkowych, dostępności zasobów, jakości połączeń audio i video itp.



Ważną cechą rozwiązania Network Instruments jest jego elastyczność oraz praktycznie nieograniczone możliwości rozbudowy – system nadzoru pracy sieci oraz wydajności aplikacji może więc rosnąć wraz z siecią i potrzebami.

Wszystkich zainteresowanych rozwiązaniem Network Instruments zapraszam do bezpośredniego kontaktu.