Biuletyn WAT
Vol. LIX, Nr 4, 2010

Zastosowanie narzędzi i mechanizmów testowania w procesie diagnostyki realizacji usług sieci IPV4 i 6

DARIUSZ LASKOWSKI, MARIAN WRAŻEŃ

Wojskowa Akademia Techniczna, Wydział Elektroniki, Instytut Telekomunikacji,
00-908 Warszawa, ul. S. Kaliskiego 2

Streszczenie. Sieci komputerowe są złożonymi obiektami technicznymi zawierającymi komponenty charakteryzujące się wysokim poziomem zaawansowania technicznego. Komponenty te funkcjonują w środowisku licznych protokołów i interfejsów sieciowych z zasadniczym celem ukierunkowanym na dotrzymanie realizowalności zadeklarowanej palety usługowej. Osiągnięcie gwarancji dotrzymania zadeklarowanego poziomu jakości oferowanej usługi wiąże się z koniecznością prowadzenia ciągłego w czasie procesu diagnozowania wybranych własności sieci. Open source'owe narzędzia i mechanizmy testowania sieci IP zapewniają pozyskiwanie wiarygodnych informacji o stanie sieci, umożliwiając identyfikację zachodzących zjawisk adekwatnie do zmian przepustowości i opóźnienia.
Słowa kluczowe: sieć komputerowa, security, diagnostyka komputerowa, narzędzia diagnostyczne
Symbole UKD: 681.324.004.14

Wstęp

Sieci komputerowe (SK), będące komponentem sieci telekomunikacyjnych, stanowią szkielet powszechnie oferowanych usług telekomunikacyjnych. Wzrost mocy obliczeniowej procesorów implementowanych w stacjach sieciowych jest stymulatorem zwiększania zbioru różnego rodzaju punktów dostępowych do ogólnie dostępnych zasobów sieci rozległej. Tworzy to otwartość środowiska sieci na ewolucyjność w procesie realizacji usług telekomunikacyjnych. Usługi te wymagają wielodrożnego transportu pakietów danych w zdefiniowanych łańcuchach telekomunikacyjnych (multimedialne relacje *end-to-end*). Zgodnie z rekomendacją ITU-T Y.1241 [1] usługę w sieciach IP określono w postaci „…*Usługa dostarczana użytkownikowi końcowemu (lub elementowi sieci) przez warstwę usługową, która*

wykorzystuje właściwości transferu danych w sieci IP i związane z nimi funkcje sterujące i zarządzające dla dostarczenia użytkownikowi informacji określonych w kontrakcie na usługę (Service Level Agreement, SLA)…". Podstawowe usługi świadczone w sieciach IP to przeglądanie stron WWW, e-mail, transfer plików FTP/TFTP, grupy dyskusyjne, usługi multimedialne i wiele innych. Realizacja usług wiąże się z kontrolą miary jakości i wydajności.

Liczność i różnorodność środowisk realizacji usług powoduje, iż istnieją utrudnienia we wzajemnej integracji sieci ukierunkowanej na swobodny dostęp do medium i transport pakietów. Dostęp to przede wszystkim algorytmy dostępu dla łącza przewodowego CSMA/CD (ang. *Carrier Sense Multiple Access with Collision Detect*) i radiowego CA (ang. *Carrier Sense Multiple Access with Collision Avoidance*) charakteryzowane efektywnością optymalizacji liczby kolizji. Natomiast realizacja transportu wymusza wprowadzanie kolejnych wersji programów systemowych i aplikacyjnych. Są to złożone i powiązane relacjami zarządzania procesy wykorzystujące techniki i technologie sieciowe.

Zasadnicze kryteria efektywnej realizacji usług to wiarygodność i terminowość osiągane przez techniczne parametry sieciowe, tj. przepustowość, opóźnienia, sterowanie ruchem pakietów.

Biorąc pod uwagę rosnące oczekiwania użytkowników sieci, należy stwierdzić, że współczesne sieci telekomunikacyjne nie nadążają za wymaganiami w zakresie bezpieczeństwa i niezawodności oraz niskich kosztów usług. Technologie telekomunikacyjne w trybie asynchronicznym (ang. *Asynchronous Transfer Mode,* ATM) i sieci szerokopasmowe z integracją usług (ang. *Broadband Integrated Services Digital Network*, B-ISDN) stały się etapem ewolucji w kierunku sieci komputerowych z technologią transportu opartą na protokole IP (ang. *Internet Protocol*) wersji 4 i 6 z implementacją dynamicznego routingu oraz mechanizmami gwarantującymi bezpieczeństwo, takimi jak SSL (ang. *Secure Socket Layer*) i IPSec (ang. *Internet Protocol Security*), a także jakość usług QoS (ang. *Quality of Services*).

Obecnie oferowane na rynku telekomunikacyjnym usługi można pogrupować w niżej przedstawione zbiory usług:

- akustycznych (dźwięk, mowa, poczta głosowa, VoIP);
- przesyłania danych (współpraca stacji roboczej z odległym komputerem, transfer zbiorów między komputerami);
- wizualnych dla obrazów nieruchomych (tekst, zdjęcia, grafika, ViOIP) i ruchomych (*High Definition TV*, *Video On Demand*).

Powyższe usługi mogą być wiązane ze sobą, z uwzględnieniem wymagań jakościowych, celem realizacji usług multimedialnych. Zgodnie z zaleceniem (np. F.700) [2] pojęcie tzw. „multimediów" wyróżnia się w kontekście usługi i aplikacji oraz terminali i sieci. Zasadniczo usługi multimedialne to rodzaj usług, w których jednocześnie (z punktu widzenia użytkownika) przekazywane są co najmniej dwa rodzaje informacji (np. głos i obraz lub dane, sygnalizacja, itp.) w ustalonych

rygorach czasowych. Analogicznie do ww. rozumiane jest pojęcie aplikacji multimedialnej.

Szerokopasmowość sieci telekomunikacyjnych i wzrost zapotrzebowania użytkowników są nowym rodzajem i formą usług wymuszającą powszechność wprowadzania strumieniowych usług multimedialnych.

Uwzględniając powyższe, za celowe uważa się zapewnienie przez dostawcę (operatora) lub właściciela sieci zdatności funkcjonalnej zasadniczych komponentów SK. Ciągły nadzór nad stanem sieci umożliwia administratorowi zarządzanie usługami przez SLA. Jest to formalny kontrakt pomiędzy usługodawcą i użytkownikiem w zakresie jakości, dostępności i wydajności jakie zapewnić ma usługodawca. Monitoring sieci dostarcza danych dla optymalnego wykorzystania posiadanych zasobów, a systematyczny audyt pozwala zidentyfikować stan systemu i wskazać elementy do nowelizacji. Kolejne zastosowanie danych to baza *know-how* sieci w zakresie wydajności, ruchu, stanu bezpieczeństwa i niezawodności umożliwiająca wnioskowanie o efektywności realizacji usług multimedialnych przy optymalizacji posiadanych zasobów.

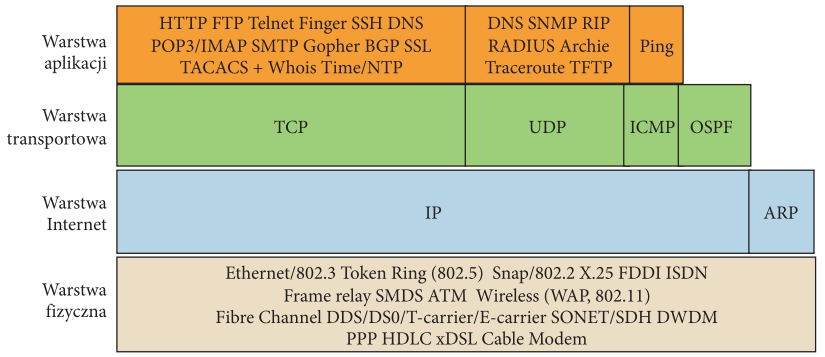
1. Usługi sieci TCP/IP

Z analizy dostępnej literatury, publikacji zamieszczanych na stronach WWW wynika, że współczesny użytkownik poszukuje szerokiej palety usług spełniających jego zapotrzebowania w zakresie wymiany tekstu, obrazu i danych. Producenci sprzętu i oprogramowania podążają za ciągłym rozwojem wymagań i udoskonalają urządzenia końcowe i komunikacyjne z uwzględnieniem możliwości technologicznych i postępu naukowego.

Internet z implementacją IPv4 jest dziś najpowszechniej wykorzystywaną siecią, a stos protokołów TCP/IP, opracowany w Stanach Zjednoczonych na początku lat 70. ubiegłego wieku, jest łatwo implementowany (rys. 1). Zasadniczym elementem modelu jest protokół IPv4 wykorzystujący 32-bitowy adres hosta i sieci rozróżniany maską. Przydzielanie adresu, odbywające się w sposób dynamiczny (ang. *Dynamic Host Configuration Protocol*, DHCP) lub statyczny, i logowanie (identyfikator, hasło) stanowią dwa zasadnicze wymogi procesu dostępu do sieci.

Sieci telekomunikacyjne ciągle ulegają zmianom w kierunku optymalizacji rozwiązań sieciowych, oferujących mobilność abonentom w środowisku sieciowym IP. Za celowe uważa się przebudowę założeń dotyczących systemowo-aplikacyjnej platformy i zaprojektowanie nowych urządzeń szkieletowych i dostępowych. Sugeruje się, aby kolejne platformy telekomunikacyjne integrowały wiele środowisk, tworząc spójną sieć obsługującą abonentów stacjonarnych i mobilnych. Praktyczna realizacja wymaga implementacji rozwiązań dostosowanych do wymagań rynku i opłacalności produkcji oraz wdrożeń dla informacji użytkowej, sterowania

w transporcie (transmisji, komutacji, konwersji) i dostępie (dostępem, usługą, komunikacją, transportem).



Rys. 1. Uogólniony model czterowarstwowej struktury

Poprawność funkcjonalną osiąga się przez stosowanie zestawu akceptowanych standardów (norm, wytycznych, zaleceń) pozwalających na współpracę urządzeń oferowanych przez różnych producentów. Szkielet standardów wywodzi się z sieci telefonicznej (ITU-T H.323) [3] i Internetu (*Session Initiation Protocol*, SIP-RFC 3261) [4]. Narzędzia w postaci H.323 i SIP umożliwiają oferowanie usług multimedialnych w zakresie przekazywania różnych form danych i ich przekazu (np. tekst, dźwięk, grafika, animacja, wideo) celem dostarczania odbiorcom informacji lub rozrywki.

Można zatem przyjąć, że usługi multimedialne umożliwiają łączne przetwarzanie i przesyłanie informacji wiążących ze sobą dźwięk, obraz, tekst i grafikę przez realizację różnych aplikacji, tj.:

— transferu zbiorów danych — to najczęściej realizacja usług multimedialnych w klasycznych sieciach. Prostota realizacji sieci wynika z mniejszych wymagań jakościowych w stosunku do innych usług;
— przesyłania danych multimedialnych do wielu punktów jednocześnie, np. w lokalnej telewizji kablowej lub innych systemach rozgłaszania.

Rosnące zapotrzebowanie na szerokopasmwe usługi transmisji danych wymaga ograniczenia w stosowaniu skrętek miedzianych kategorii 5e i 6 na korzyść kabli światłowodowych ze względu na ich większą przepustowość i postępujący spadek cen urządzeń techniki światłowodowej. W praktycznych realizacjach występują także rozwiązania hybrydowe: światłowód (szkielet) — skrętka (dostęp) — łącza satelitarne (transport) na niskich orbitach (ang. *Low Earth Orbit*, LEO). Szczególnie ciekawym rozwiązaniem jest satelitarny system szerokopasmowy platformy cyfrowej DVB-S (ang. *Digital Video Broadcasting-Satellite*) wyznaczający nowe standardy radiodyfuzji satelitarnej i świadczenia usług multimedialnych w zakresie

specyfikacji metod kodowania sygnałów MPEG 2/4 (ang. *Moving Picture Experts Group*), dołączenia dodatkowych informacji (konfiguracja i synchronizacja dekodera, ang. *Service Information*, SI), rozsiewczej transmisji danych (ang. *DVB Data Broadcasting*) oraz metod zabezpieczenia sygnału przed zakłóceniami za pomocą kodowania kaskadowego.

Niezawodność procesu realizacji usług jest osiągana poprzez trasowanie pakietów w rozległej sieci szkieletowej (router, centrala) i dostępowej (punkt dostępowy, przełącznik, abonenckie zespoły liniowe, itp.). Krytycznymi wartościami technicznymi gwarancji usług są opóźnienie i jego zmienność, utrata pakietów, (ITU-T G.1541 [5], ITU-T G.1010 [6]) itd. Parametry te determinują jakość dostarczanych usług w sieci (tab. 1).

Tabela 1

Przykładowe metryki służące do oceny usługi

Przykładowe metryki służące do oceny jakości usługi		
1	IPTD (IP Packet Transfer Dely)	Opóźnienie to czas upływający między chwilą wysłania pierwszego bitu a momentem odebrania ostatniego bitu danego pakietu w mierzonej sieci lub jej części.
2	IPDV (IP Packet Delay Variation)	Zmienność opóźnienia przekazu *k*-tego pakietu jest zdefiniowana jako różnica *k*-tego pakietu odniesienia.
3	IPLR (IP Packet Loss Ratio)	Poziom strat pakietów to stosunek liczby pakietów straconych do liczby pakietów wysłanych w danym okresie pomiarowym (maksymalny czas oczekiwania 3 s).
4	IPPT (IP Packet Throughput)	Przepływność na poziomie pakietów IPPT to stosunek liczby pakietów odebranych w danym okresie pomiarowym do długości tego okresu pomiarowego.
5	Dostępność usługi IP (IP service availability)	Usługa jest uważana za dostępną, jeśli w danym okresie pomiarowym wartość IPLR jest mniejsza od założonego progu.
6	MOS (Mean Opinon Score)	Subiektywna ocena użytkownika.

Większość użytkowników sieci nie jest zainteresowana tym, w jaki sposób dany typ usługi jest zaimplementowany i realizowany w systemie, ale z pewnością przywiązuje dużą wagę do porównania sposobu zrealizowania tego samego typu usługi przez różnych dostawców usług sieciowych, za pomocą uniwersalnych miar wydajnościowych związanych z daną usługą (tab. 2) [6].

Współczesny użytkownik wymaga od sieci telekomunikacyjnych nie tylko dostępu do usług tradycyjnych, ale także usług szerokopasmowych. Do współczesnych, szerokopasmowych usług multimedialnych zaliczane są m.in.: wideotelefonia, wideokonferencja, wideotekst, biblioteka wideo, teleedukacja, telezakupy, usługi bankowe, poczta elektroniczna oraz dostęp do Internetu i usług tej sieci,

gry komputerowe, wideo na żądanie lub prawie na żądanie, serwis informacyjny i reklamowy (rys. 2).

Tabela 2

Wybrane oczekiwania użytkownika końcowego dotyczące interaktywnych usług jednokierunkowych

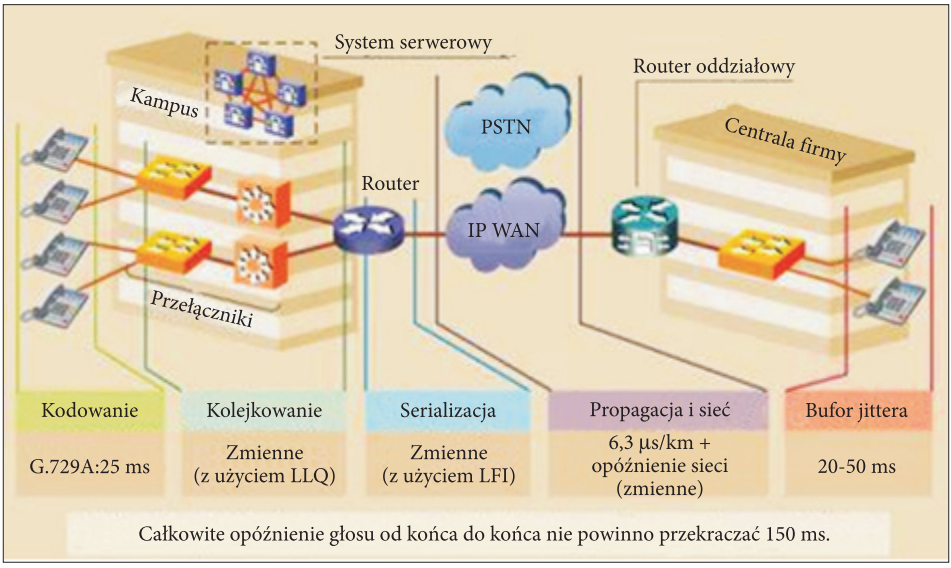
Usługa	Aplikacja/Szybkość transmisji	Parametry		
		Opóźnienie	Odchylenie opóźnienia	Straty informacji
Dane	HTML/10 kB	< 2 s/stronę – preferowane < 4 s/stronę – akceptowane	Nie określono	0
Dane	e-mail/10 kB			
Dane	e-mail (serwer-serwer)/10 kB	kilka minut	Nie określono	0
Audio	Poczta głosowa 4-32 kb/s	< 1 s – odtwarzanie < 2 s –nagrywanie	< 1 ms	< 3%

Rys. 2. Przyszłościowe usługi multimedialne

Komputerowe sieci lokalne (ang. *Local Area Network*, LAN) i rozległe (ang. *Wide Area Network*, WAN), transportujące pakietowo dźwięki, są w stanie zapewnić przekaz głosu (ang. *Voice over Internet Protocol,* VoIP) o jakości porównywalnej z analogiczną udostępnianą w publicznych sieciach z komutacją kanałów. Zadeklarowany QoS usług VoIP wymaga parametrów w postaci:

1. Opóźnienia:
   — zalecana poniżej 80 ms,
   — średnio (80-170) ms,
   — nieakceptowane powyżej 170 ms.
2. Zmienność opóźnienia w czasie (ang. *jitter*) rozumianego jako deterministyczne lub losowe zmiany wartości opóźnienia, które nie powinny przekroczyć 20 ms lub połowy czasu transmisji pakietu dla relacji *end-to-end* (rys. 3).
3. Straty pakietów są wynikiem występowania wielu narażeń środowiskowych i niewydolności sieci IP, grupuje się je w zbiory jakości, tj.:

— wysoka do 1%,
— dobra dla sektora biznesowego do 3%,
— akceptowalna od 3% do 10%,
— niska (głos staje się niezrozumiały) powyżej 10%.



Rys. 3. Opóźnienie VoIP [7]

Minimalizację strat pakietów osiąga się przez mechanizmy zarządzania wspierane przydzielaniem priorytetu i etykietowaniem oraz buforowaniem w węzłach (routerach) sieci IP, np. w kolejkach FIFO (ang. *First In First Out*).

Wdrażanie technologii VoIP wymaga instalacji na styku sieci pakietowej i publicznej (np. *Public Switch Telecommunication Network*, PSTN) bram głosowych MGW (ang. *Media Gateway*), MGCP (ang. *Media Gateway Control Protocol*) i MEGACO (ang. *Media Gateway Control*). Są to kluczowe elementy zapewniające dwukierunkowe translacje między siecią o charakterze pakietowym a siecią publiczną PSTN. Ich zadanie polega na „przezroczystej" komunikacji między wszystkimi typami terminali komunikacji głosowej.

Druga grupa usług jest związana z transmisją informacji wideofonicznej w postaci skompresowanych sygnałów fonicznych i wideo, której jakość zależy także od prawdopodobieństwa strat oraz wartości i wariancji opóźnienia ITU-T G.114 [8], tj.:

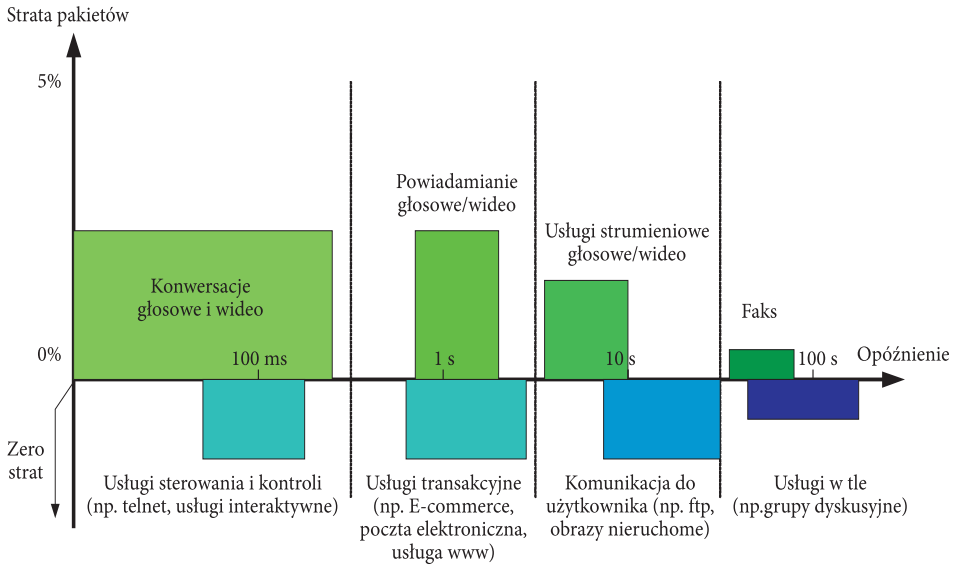
— zalecana do 150 ms,
— średnio (150-400) ms,
— nieakceptowane powyżej 400 ms.

Kompensacja braku synchronizacji między sygnałem wideo i fonią następuje przez buforowanie informacji.

Akceptowany poziom strat lub błędów jest trudny do oszacowania i wymaga uwzględnienia wielu czynników, tj. trybu transferu, czasu trwania sesji, jakości danych źródłowych, zawartości przechwytywanych scen oraz strat i błędów w sygnale odtwarzanym.

Z powyższego wynika, że do podstawowych wymagań sieciowych zaliczamy efektywny multicast, gwarancje jakościowe usługi, małą nierównomierność opóźnienia i pożądaną przepustowość.

Krytyczne dla usług czasu rzeczywistego opóźnienia i jego zmienność usuwa się przez wydajne algorytmy przetwarzania danych i zaawansowane mechanizmy kolejkowania. Wartości dopuszczalnych opóźnień i strat pakietów przedstawiono na poniższym rysunku (rys. 4).



Rys. 4. Dopuszczalne granice strat pakietów oraz opóźnień

Oddzielnym zagadnieniem są straty pakietów i odmowa dostępu do zasobów sieciowych wynikające z błędów transmisyjnych w sieci, przepełnienia buforów wejściowych/wyjściowych w węzłach sieci IP, przekroczenia możliwości kanału transmisyjnego sieci, zbyt dużego obciążenia elementów szkieletowych, braku sterowania translacją adresów i trasowania pakietów oraz niewłaściwej konfiguracji urządzeń i aplikacji.

Możliwych do wydzielenia usług sieciowych jest wiele, lecz zbiór podstawowych usług zawarto w tabeli (tab. 3).

Tabela 3

Ogólne wymagania usług multimedialnych w funkcji parametrów sieci

Typ usługi	Nazwa usługi	Przepustowość	Opóźnienie	Stopa utraty pakietów
Audio	Transmisja głosu	(4-64) kbit/s	< 400 ms	< 3%
	Strumieniowe audio	16 kbit/s	< 10 s	< 1%
Wideo	Wideotelefon	(16-384) kbit/s	< 400 ms	< 1%
	Strumieniowe wideo	(16-284) kbit/s	< 10 s	< 1%
Dane	Transfer danych	nie dotyczy	nie dotyczy	0%
	Przeglądanie stron WWW	nie dotyczy	< 10 s	0%

Z wnioskowania o zjawiskach zachodzących w sieci wynika, że występują problemy zapewnienia QoS usług rozwiązywanych przedsięwzięciami natury administracyjno-organizacyjno-technicznej. Problemy te rozwiązuje się na etapach projektowania lub skalowalności w procesie symulacji modeli [9, 10].

2. Narzędzia wsparcia diagnostycznego

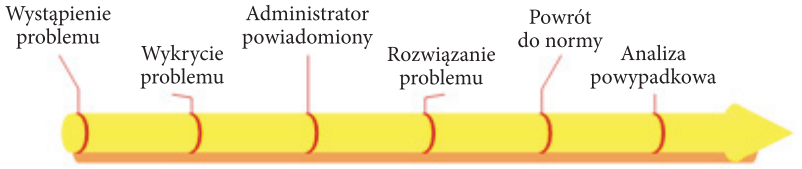
Gwarancją utrzymania prawidłowego funkcjonowania środowiska sieciowego jest zarówno współdziałanie i integracja służb informatycznych (np. administratorów sieci, systemów, baz danych, backupów, serwerów itp.) jak i prowadzenie dokumentacji technicznej, będącej rodzajem przewodnika po sieci. W niej zawarty jest schemat sieci, rodzaj używanego sprzętu, bieżąca konfiguracja, wprowadzone zmiany, hasła administracyjne itp. Ponadto w dokumentacji tej możemy znaleźć wszystkie niezbędne wiadomości potrzebne do przeprowadzenia procesu administrowania czy planowanej rozbudowy systemu [11, 12].

Najważniejszym problemem sieci jest utrzymanie zdatności funkcjonalnej, zgodnej z określonymi wymaganiami technicznymi. Użytkownicy oczekują sygnału zgłoszenia centrali lub osiągalności radiowych i przewodowych punktów dostępowych, za pomocą których są w stanie wykorzystywać oferowane usługi. Operatorzy zaś starają się przedstawiać szeroki zakres konkurencyjnych usług, ale z redukcją ponoszonych nakładów finansowych przy zwiększonej wydajności. Niebagatelne znaczenie ma także wzrost zapotrzebowania na pasmo. Wymagania te najlepiej spełnia transport pakietowy IP z mechanizmami wsparcia usług czasu rzeczywistego.

Zasadnicze znaczenie posiada jednak właściwie prowadzony proces diagnozowania zasobów sieciowych w ujęciu systemu antropotechnicznego [13]. Pierwszym

przedsięwzięciem jest ciągła analiza procesu monitorowania wydajności sieci i poszukiwanie niezdatności oraz „wąskich gardeł" na podstawie analizy czasu przydatności elementu, natężenia ruchu, opóźnienia i czasu oczekiwania oraz wykorzystania zasobów.

Podstawową kwestią przy rozwiązywaniu problemów w sieci jest metodyka postępowania (rys. 5) podczas zaistnienia problemu (incydentu).



Rys. 5. Postępowania przy wystąpieniu problemu w sieci

Zidentyfikowany incydent zostaje zakwalifikowany do grupy problemów i nadaje się mu priorytet obsługi. Tego typu działania pozwalają na wychwycenie potencjalnie groźnych sytuacji, zanim jeszcze obejmą one użytkownika. Poza błędnymi implementacjami i konfiguracjami, wyróżnia się także inne niezdatności, tj.:

— błędy konfiguracji protokołów aplikacji,
— niewłaściwy dobór protokołów routingu,
— błędy sum kontrolnych,
— kolizje i zbyt duży poziom nasycenia ramkami,
— retransmisje i duplikowane adresy sieciowe,
— wprowadzanie ramek niedozwolonych,
— zbyt wielką liczbę ramek rozgłoszeniowych.

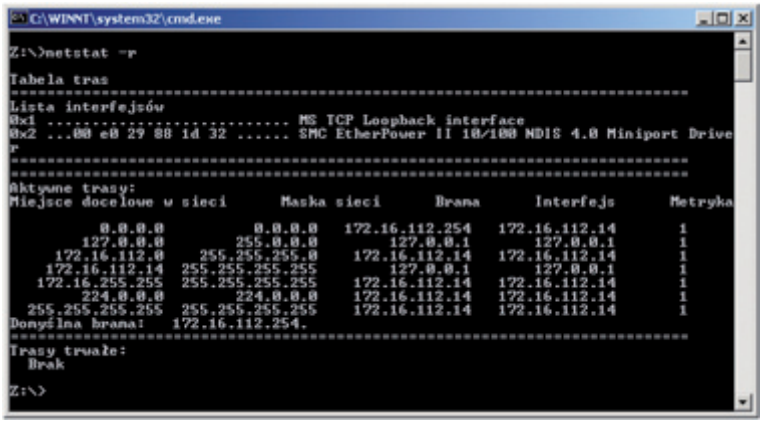
Przyczynami niezdatności są zdarzenia sprzętowo-programowe i/lub postępowanie ludzi. Waga każdego z tych narażeń jest zmienna w czasie. Wykonanie szybkiej i właściwej diagnozy jest trudne. Dlatego też konieczne jest, aby administrator dysponował metodyką postępowania z wykorzystaniem dedykowanych narzędzi analizy i testowania zasobów sieciowych w następujących warstwach:

— łącza danych: lista stacji generujących najwięcej błędów i największy ruch usługowy (rozgłoszeniowy), parametry (wykorzystanie pasma, natężenie ruchu pakietów i ramek typu broadcast i multicast, kolizje, ramki błędne), procentowy rozkład ramek o różnej wielkości, zaobserwowane typy ramek;
— sieciowej (protokół IP): pod względem liczby transmitowanych bajtów i ramek;
— sieciowej i transportowej (TCP/IP): natężenie i analiza ruchu ARP, procentowy rozkład ruchu TCP, stacje generujące największy ruch, wpływ protokołów TCP/IP na wielkość ramek, wpływ ruchu zewnętrznego na lokalny, występowanie komunikatów ICMP, natężenie ruchu IPX RIP, wpływ protokołów IPX/SPX na wielkość ramek, stacje generujące największy ruch IPX/SPX.

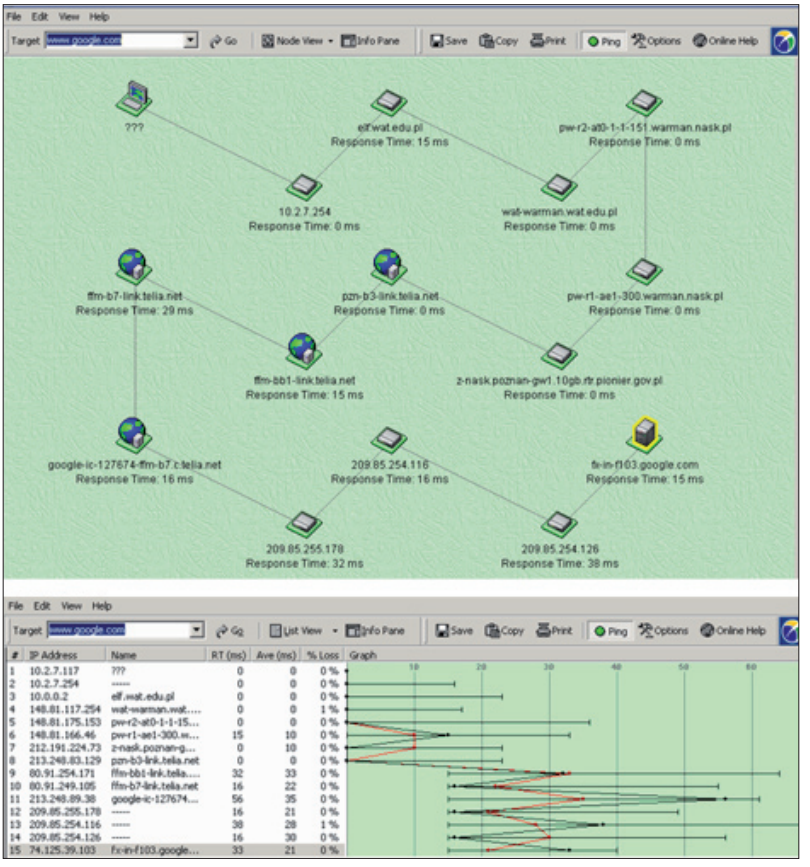
Ocena i identyfikacja stanu sieci w warstwach transmisyjnych realizowana jest przez przegląd architektury sieci pod kątem jej wpływu na wydajność pracy oraz wskazanie obciążonych segmentów, łączy, przełączników i serwerów, dla których przepustowość interfejsu sieciowego staje się „wąskim gardłem" w transmisji.

Wiele komponentów sieciowych zawiera mniej lub bardziej rozbudowany system operacyjny zawierający lub umożliwiający implementację narzędzi diagnostycznych. Podstawowy zbiór aplikacji uruchamianych z wiersza poleceń tworzą [14-20]:

- IPCONFIG (ang. *Internet Protocol Configuration*) pokazuje ustawienia interfejsu sieciowego protokołu TCP/IP i odświeża ustawienia dynamicznej konfiguracji (DHCP).
- PING (ang. *Packet InterNet Groper Utility*) będący narzędziem do sprawdzania dostępności drogi do stacji roboczej w sieci. Problemami są blokada przez firewall odpowiedzi ICMP i duży rozmiar pakietu (> 32 kB). Badanie wydajności sieci jest możliwe przez połączenie *pinga* z innymi narzędziami diagnostycznymi protokołów (np. SLIST w sieci NetWare).
- TRACEROUTE (Unix/Linux) jest efektywny przy lokalizacji miejsca niezdatności sieci, np. przez wskazanie portu niebramkującego urządzenia. *Ping* i *Traceroute* stosowane razem są najbardziej wartościowymi narzędziami programowymi dostępnymi dla administratora sieci TCP/IP.
- TRACERT (Windows) wykonuje tzw. śledzenie marszruty pakietów UDP ze stacji lokalnej do stacji zdalnej na podstawie małych wartości TTL i błędnego numeru portu zmiennego sekwencyjnie o 3. Oferuje on tablicę bram łączących stacje.
- ARP bada problemy związane z translacją między adresami IP i sieci Ethernet przez wyświetlanie i modyfikację oddzielnych tabel translacji adresów IP i adresów fizycznych używanych przez protokół rozróżniania adresów (ARP).
- NETSTAT wyświetla statystyki protokołu, aktywne połączenia sieciowe TCP/IP, porty nasłuchu stacji sieciowej, tabelę routingu, statystykę protokołu IPv4/6 (ICMP/6, TCP/UDP).
- NETUSE testuje chwilowe i trwałe połączenie stacji sieciowej, wyświetla tabelę routingu podobnie jak polecenie„router print" (rys. 6).
- NEOTRACE prezentuje w różnych frmach ścieżkę między stacjami sieciowymi a serwerem WWW lub adresem IPv4. Do istotnych cech wyróżniających ten program należy możliwość tworzenia historii, ciągłe zbieranie danych o transmitowanych pakietach (liczba wysłanych, utraconych, itp.), modyfikacja wysyłanych pakietów, graficzne zilustrowanie węzłów komunikacyjnych na trasie pakietów (rys. 7).



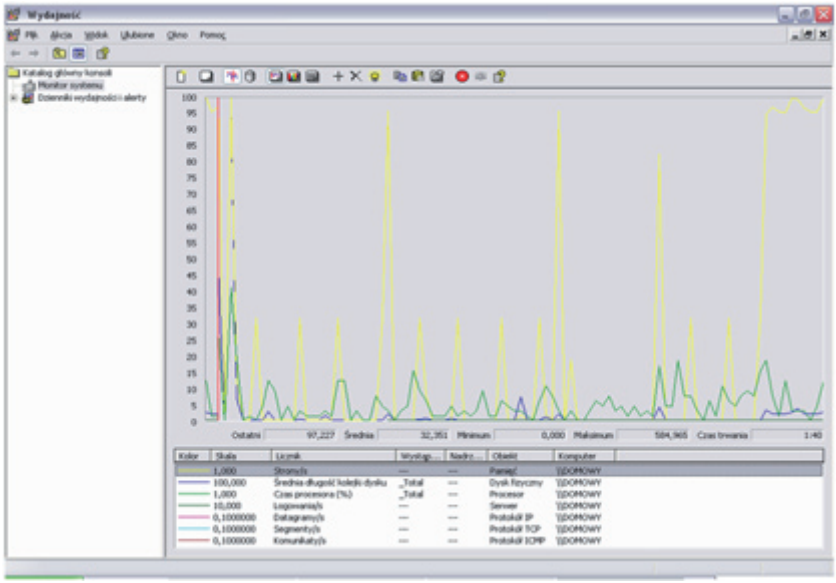
Rys. 6. Opcje programu *netstat –r*



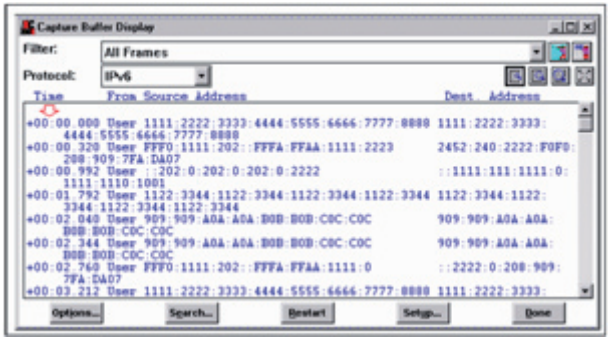
Rys. 7. Opcje programu NeoTracer

- SATAN (ang. *Security Analysis Tool for Analyzing Networks*) to unixowe narzędzie bezpieczeństwa wspierające diagnostykę przy lokalizacji luki w zabezpieczeniach sieci. W wypadku znalezienia problemu *Satan* proponuje rozwiązanie w postaci rekonfiguracji lub aktualizacji oprogramowania, ewentualnie ogranicza dostęp do sieci i wyłącza wadliwą usługę. Gromadzi także informacje dostępne dla wszystkich użytkowników sieci. *Satan* zyskał popularność dzięki wykorzystaniu do wyświetlania raportów możliwości Perla i przeglądarki HTMLa.
- ISS (ang. *Internet Security System*) — funkcjonalnie zbliżony do *Satana*, testuje błędy oprogramowania i konfigurację systemu. Efektem pracy jest raport zawierający szczegółowe instrukcje usuwania wykrytych problemów i luk. Oprogramowanie obsługiwane jest za pomocą przejrzystego i intuicyjnego graficznego interfejsu GUI (ang. *Graphical User Interface*). Zaletą tego programu jest szybki i łatwo zarządzany interfejs i system raportujący, dzięki czemu administrator jest w stanie utrzymać wysoki stan bezpieczeństwa systemu.
- MONITOR SIECI podaje informacje o wejściowo-wyjściowym ruchu w sieci przez przechwyt i analizę ramek (adres nadawcy i odbiorcy ramki, protokoły występujące wewnątrz ramki). Głównymi narzędziami monitorowania w systemie Windows są: Konsola Wydajność i Menedżer Zadań. Menedżer udostępnia dane o aktywności i wydajności systemu, a Konsola umożliwia analizowanie szczegółowych informacji pomocnych podczas wyszukiwania wąskich gardeł i innych problemów. Konsola Wydajność zawiera dwa narzędzia: Monitor Systemu i Dzienniki Wydajności oraz alerty.
  Monitor wydajności umożliwia śledzenie statystyk usług sieciowych, tj. TCP/IP, i innych usług jak np. serwer i stacja robocza. Z analizy wyników tych statystyk określa się „wąskie gardła" sieci, przeciążenie routerów szkieletowych, dysku, procesora. Kolejną zaletą Monitora jest elastyczność w zakresie zbierania danych, ponieważ oglądając statystyki na ekranie „Wykres" (rys. 8), generuje się rejestry wydajności z okresu czasu za pomocą funkcji „Log", lub oglądając „surowe" dane liczbowe na ekranie „Raport" ustawia się alarmy progowe na ekranie „Alarm".
- *RC-100WL*® analizuje zebrane dane i prowadzi obserwację ruchu w dowolnym protokole w łączu przewodowym w trybie pasywnego monitorowania i symulacji zadanych protokołów celem porównania logów (rys. 9). Obserwować można sekwencje wymienianych wiadomości w określonych przez użytkownika warstwach modelu odniesienia na wybranym poziomie szczegółowości. Do jego najważniejszych zalet należy zaliczyć:
  — dekodowanie w czasie rzeczywistym ponad 300 protokołów modelu OSI,

— generowanie raportów graficznych i tekstowych i przechwytywanie zdarzeń co 1 ms,
— równoczesne monitorowanie sieci WAN i LAN oraz wykrywanie problemów sieciowych.

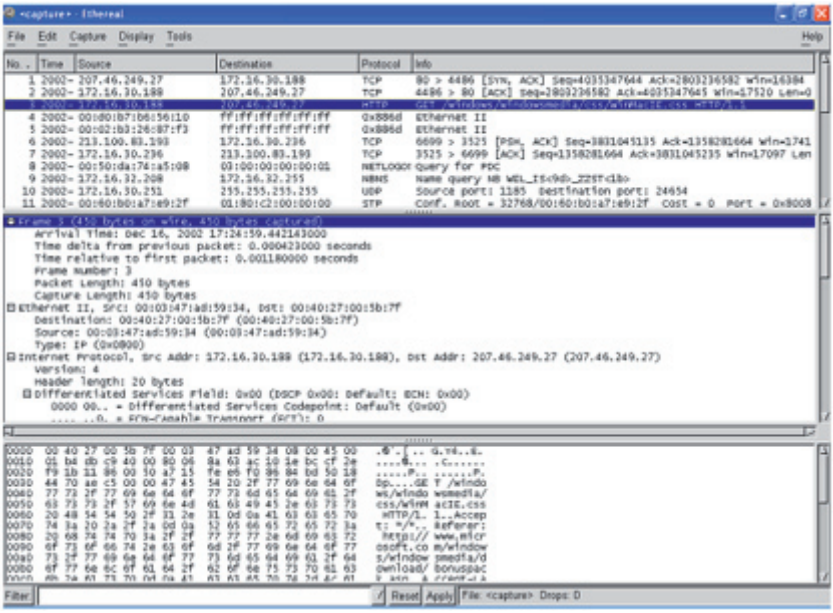


Rys. 8. Okno dialogowe Monitora Wydajności



Rys. 9. Okno dialogowe RC100-WL

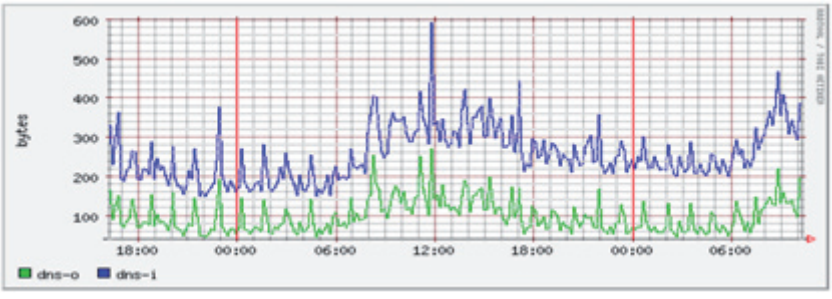
- ETHEREAL umożliwia analizę ponad 250 protokołów od TCP/IPv4i6 po IPX/SPX, SMB i Netbios w środowisku Windows z Winpcap, a w Linuksie to kod źródłowy do kompilacji (rys. 10).
  Okno dialogowe składa się z paneli: listy przechwyconych pakietów, rozkodowanych informacji i nierozkodowanego pakietu.



Rys. 10. Okno dialogowe Ethereala

Ethereal stosuje ten sam silnik co *tcpdump*, a kolejną jego wersją jest *Wireshark* analizujący dane w trybie on-/off-line. Wydobycie loginów i haseł z niezaszyfrowanej transmisji (np. ftp, http) jest prostym zadaniem i sprowadza się do przefiltrowania zebranych pakietów pod kątem specyficznych informacji.

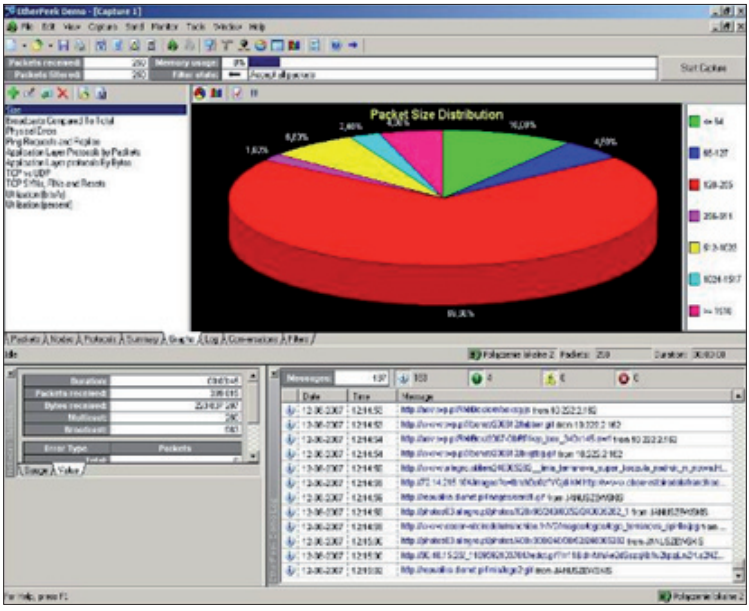
- IPTRAF dostarcza informacji o interfejsach sieciowych dla platform linuksowych, tj. bieżące obciążenie, wielkość pakietów i statystyk portów (rys. 11).



Rys. 11. Okno dialogowe Iptrafa

Praktyczne zastosowanie Iptrafa to tryb interaktywny do przeglądania ruchu sieciowego w czasie RT (ang. *Real Time*). Jednakże posiada on tryb demona, zapisując rezultaty śledzenia w przetwarzalnym pliku (/var/log/iptraf).

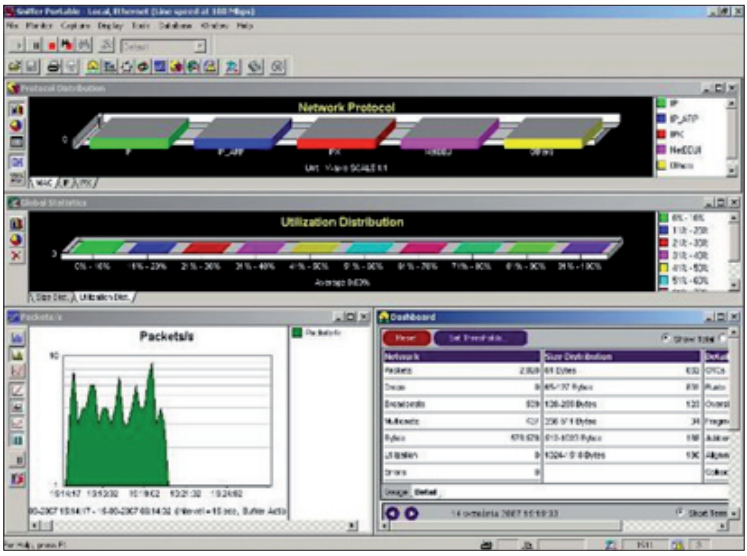
- ETHERPEEK analizuje protokoły i ruch w sieciach wieloprotokołowych i wieloplatformowych, gdyż przechwytuje pakiety, interpretuje warstwy protokołu przechwyconej ramki i udostępnia informacje zawarte w pakiecie (rys. 12). Poprzez monitorowanie, filtrowanie, dekodowanie i udostępnienie danych pakietu identyfikuje błędy protokołów oraz wykrywa wybrane problemy sieciowe. Główną zaletą programu jest równoczesne przechwytywanie kilku sesji na różnych segmentach sieci, niezależnie od typu sprzętu i oprogramowania sieci interpretuje warstwę protokołu przechwyconych pakietów i eksponuje zasadnicze informacje.



Rys. 12. Okno dialogowe EtherPeek w trybie RT

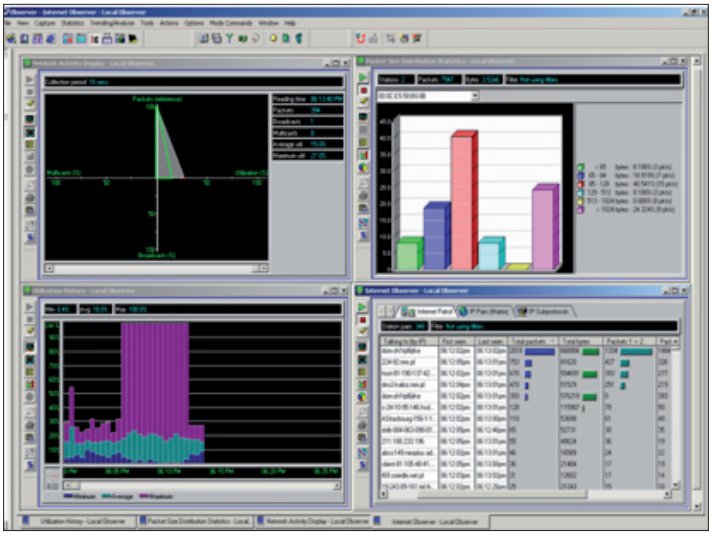
- Sniffer Portable służy do selektywnego wykrywania luk i zwiększenia wydajności sieci przez rozwiązywanie problemów i konfigurowanie sieci niezależnie od topologii i technologii. Analiza Ekspercka czasu rzeczywistego dodaje inteligencję tłumaczenia protokołów sieciowych. Monitorowanie jest idealnym sposobem utrzymywania sieci, wykrywania anomalii oraz zapisywania całkowitej wydajności sieci (rys. 13).
  Program zbiera kompleksowe statystyki celem identyfikacji aktywności sieci przenoszone do bazy danych, arkusza kalkulacyjnego czy też raportowania.

System zawiera również predefiniowane raporty klasy menedżerskiej w łatwym do interpretacji stylu. *Sniffer Portable* może wysyłać alarmy na email, pager, drukarkę itp.



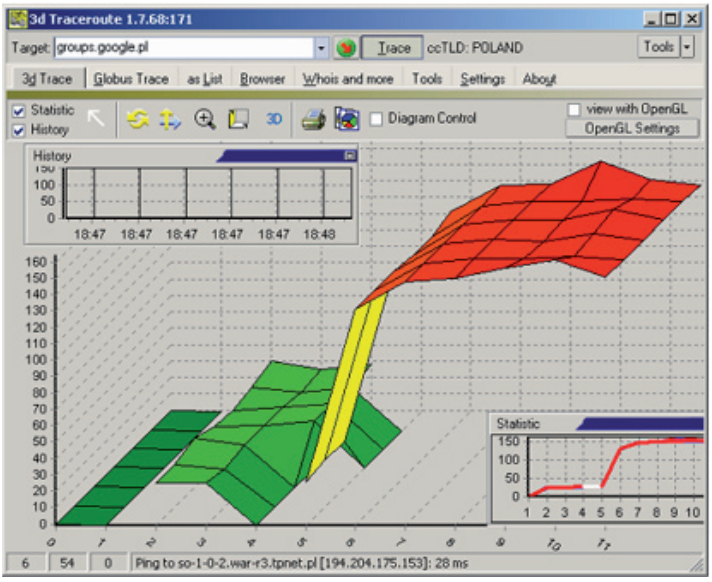
Rys. 13. Okno dialogowe Sniffera Portale

- OBSERVER ukierunkowany jest na analizę aktywnych węzłów trasujących i dostępowych w zakresie statystyk protokołów i konwersacji par węzłów oraz wykorzystania Internetu. Dodatkowo umożliwia wykrycie błędów warstw fizycznej i transportowej, statystyki routerów i przełączników, wykorzystanie sieci i trendy w funkcji czasu (rys. 14). Raporty aktywności węzłów obejmują listę węzłów uszeregowaną według stopnia wykorzystania pasma, całkowitą liczbę pakietów, transmisje rozsiewcze (ang. *broadcast*) i grupowe (ang. *multicast*). Raport protokołów klasyfikuje ruch w sieci zarówno w tabelarycznej, jak i graficznej postaci. Raport konwersujących par śledzi węzły wymieniające komunikaty sieciowe, kreśląc linie między węzłami.
  Przykładowo moduł *Router Observer* monitoruje liczbę pakietów i bajtów oraz wykorzystanie routera. Analizator może także pokazać ruch danych serwera webowego, w tym liczbę połączeń internetowych i udział procentowy ruchu lokalnego w sieci, średnie i maksymalne wykorzystanie pasma, liczbę pakietów, błędy CRC, błędy uszeregowania, błędny rozmiar pakietów i kolizje. Dodatkowo analizuje kolizje w sieci Ethernet i rozpoznaje 10 ich najważniejszych przyczyn.



Rys. 14. Okno dialogowe Observera

- 3D TRACEROUTE rozszerza możliwości *pinga i tracerta* oferując skaner portów i adresów IP, listy aktywnych połączeń z lokalnego komputera, badanie serwera HTTP, zapytania do serwerów DNS, analizę nagłówków poczty elektronicznej oraz klienta protokołu Telnet (rys. 15).



Rys. 15. Okno dialogowe 3D Tracerout

Przedstawiona powyżej charakterystyka różnego rodzaju analizatorów sieciowych wykorzystywanych do wsparcia procesu diagnozowania posiadanych zasobów umożliwiła przeprowadzenie oceny ich przydatności w zakresie powszechności zastosowań w środowisku IP. Uogólnione porównanie bardziej rozbudowanych analizatorów zaprezentowano w poniższej tabeli (tab. 4). Wszystkie z testowanych analizatorów są przydatnymi narzędziami, ale to EtherPeek imponuje zakresem dekodowanych protokołów, łatwą nawigacją między ekranami, jasnością raportów. Nadaje się do powszechnego zastosowania dla administratorów sieci.

Tabela 4

Ocena analizatorów w skali (1-5)

Nazwa	Dokładność (20%)	Protokoły (20)	Raporty (20%)	Łatwość użycia (20%)	Dokumentacja (10%)	Instalacja (10%)	Ocena ogólna
EtherPeek	4	4	4	4	3	3	3,8
3D Tracerout	4	3	4	3	4	3	3,5
Sniffer	4	4	3	2	3	3	3,2
Observer	4	2	3	3	3	3	3,0
Ethereal	4	2	3	3	3	3	3,0

Wnioski

Ewolucja zapotrzebowań użytkowników na usługi telekomunikacyjne wynika z popularyzacji procesu konwergencji głosu i danych we współczesnych środowiskach sieciowych. Prym wśród nich wiodą mobilne rozwiązania WLAN/GSM/UMTS oferujące usługi dostępne z telefonów komórkowych (smartfonów) i komunikatorów (pocketów). Liczność bezprzewodowych implementacji technologii Wi-Fi w zasięgu hot-spotów, dostęp do portali WWW, technologia p2p stymulują ewolucję w sieciach komputerowych. Z punktu widzenia administratorów, czy też pracowników działów telekomunikacyjnych, zintegrowana komunikacja zwiększa efektywność wykorzystania sieci i przekłada się także na zyski przedsiębiorstwa (organizacji).

Kluczową rolę w uzyskiwaniu zintegrowanej komunikacji odgrywają telecentra usługowe i nowoczesne platformy komunikacyjne z aplikacjami integrującymi usługi. Terytorialnie wydzielone systemy *contact*/call *center* są przystosowane do wielousługowych transmisji oraz obsługi różnorodnych kontraktów przez telefon, e-mail, faks, transfer plików i strony WWW. Abonenci poszukują nie tylko bezpiecznej i niezawodnej realizacji usług wyrażonej odpowiednim poziomem jakości SLA, ale przede wszystkim właściwego formatu informacji przekazywanej z pożądaną przepływnością i minimalnym opóźnieniem.

Systemy multimedialne integrują dane, obraz i dźwięk w środowisku sieciowym i determinują wymagania w stosunku do technik wytwarzania, przesyłania, przetwarzania i prezentacji. Usługi multimedialne oferuje się na podstawie dedykowanych systemów, więc ich dostarczenie do adresata musi być wykonane przez system dostępu i wielofunkcyjne terminale sieci zintegrowanej. Jest to szczególnie ważne dla coraz powszechniej oferowanych usług wysokiej rozdzielczości (np. HDTV).

Uwzględniając powyższe, następuje coraz to większe zapotrzebowanie na jakość usługi telekomunikacyjnej dla mobilnego abonenta. Kolejnym i jednocześnie kluczowym wymaganiem jest bezpieczny transport danych. Zapewnienie integralności i poufności to kolejne zadania dla administratorów branży teleinformatycznej. Autoryzacja i uwierzytelnianie stały się w globalnej sieci kluczowymi aspektami zapewniającymi swobodny dostęp do usług realizowanych za pośrednictwem otwartych sieci komputerowych.

Systemy zarządzania i diagnozowania pojedynczych relacji/kanałów telekomunikacyjnych to już przeszłość. Obecnie istnieje konieczność posiadania jednego spójnego systemu, integrującego procesy utrzymania wymaganego stanu zdatności wspierane przez narzędzia identyfikacji i lokalizacji błędów, uszkodzeń i punktów największych obciążeń oraz najmniej wydajnych („wąskich gardeł") [21-23].

Charakterystyka wybranych własności analizatorów wskazuje, iż programy diagnostyczne są „bronią obosieczną". Narzędzia tego rodzaju mogą być zastosowane zarówno przy diagnozowaniu sieci jak i przy wyszukiwaniu jej miejsc potencjalnie wrażliwych na uszkodzenia (np. Satan).

Przedstawiona, w ogólnym zarysie, specyfikacja analizatorów sieciowych przygotowana jest do:

— prowadzenia eksperymentów naukowo-badawczych oszacowujących poziom efektywności ich zastosowań dla zadanych stanów niezdatności sieci IPv4 i 6,
— sprecyzowania metodyki badań,
— przeprowadzenia testów eksploatacyjnych i symulacyjnych.

Wynikiem tych przedsięwzięć badawczych będzie sprecyzowanie metodyki postępowania w zakresie użytkowania i obsługiwania lokalnych (LAN) i rozległych (WAN) sieci komputerowych oraz rekomendacja open source'owych narzędzi wsparcia procesu administrowania.

Artykuł wpłynął do redakcji 14.12.2009 r. Zweryfikowaną wersję po recenzji otrzymano w grudniu 2009 r.

LITERATURA

[1] ITU-T Y.1241, ITU-T Recommendation Y.1241 — Support of IP based Services Using IP Transfer Capabilities.

[2] ITU. *F.700*, Framework Recommendation for audiovisual/multimedia services.

[3] ITU-T H.323, Packet-based multimedia communications systems.
[4] IETF RFC— 3261, SIP: Session Initiation Protocol.
[5] ITU-T G.1541, A Basis for IP Network QoS Control and Traffic Management.
[6] ITU-T G.1010, End-user multimedia QoS categories.
[7] www.cisco.com.
[8] ITU-T G.114, Guidance on one-way delay for Voice over IP.
[9] D. Laskowski, *Symulacyjna metoda wyznaczenia wybranych wskaźników niezawodności sieci teleinformatycznej*, ZNS 2007.
[10] A. Bajda, D. Laskowski, M. Wrażeń, *Symulacyjny testbed diagnostyczny infrastruktury IT*, Diagnostyka maszyn, 36, 2009.
[11] C. Hunt, *TCP/IP Administracja Sieci*, Wydawnictwo RM, Warszawa, 2003.
[12] K. Liderman, *Podręcznik administratora bezpieczeństwa teleinformatycznego*, Wydawnictwo MIKOM, Warszawa, 2003.
[13] T. M. Dąbrowski, *Diagnozowanie Systemów Antropotechnicznych w ujęciu potencjałowo-efektowym*, rozprawa habilitacyjna, Warszawa, 2001.
[14] D. Laskowski, *Wykorzystanie platformy Linux do testowania sieci komputerowych*, Diagnostyka maszyn, 35, 2008.
[15] T. M. Dąbrowski, D. Laskowski, *Metody i narzędzia diagnozowania sieci teleinformatycznych*, ZNS, 2006.
[16] http://network-tools.com/
[17] http://www.linux-magazine.pl
[18] http://www.microsoft.com
[19] http://www.networld.pl
[20] http://www.securityfocus.com/
[21] J. S. Haugdahl, *Diagnozowanie i utrzymanie sieci*, Helion, Warszawa, 2000.
[22] K. Misra, *Reliabilty analysis and prediction*, Elsevier, Amsterdam, 1992.
[23] G. Iresom, *Handbook of reliability engineering and management*, McGraw-Hill, New York, 1996.

D. LASKOWSKI, M. WRAŻEŃ

Tools and mechanisms of diagnostic test used in a process of implementing network service IP 4 & 6

Abstract. Computer networks are complex technical objects containing components characterized by a high level of technical sophistication.
These components operate in an environment of numerous protocols and network interfaces with the primary goal oriented to meet the declared range of services. The achievement of the declared default guarantee of the quality of service offered involves the need of continuous-time diagnosis of selected Web properties.
Open source tools and mechanisms to ensure the testing of IP networks provide reliable information on the state of the network enabling the identification of phenomena, adequately to changes capacity and delay.
Keywords: network, security, computer diagnostic, diagnostic tool
Universal Decimal Classification: 681.324.004.14