ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 1996

Seria: INFORMATYKA z. 30 Nr kol. 1315

Adam DOMAŃSKI
Piotr KASPRZYK

PROSTE METODY TESTOWANIA SIECI ROZLEGŁYCH

Streszczenie. Artykuł przedstawia kilka prostych metod testowania sieci rozległych. Tematyka artykułu dotyczy sieci Internet, szczególnie jej fragmentu, który składa się z linii szeregowych, sieci Ethernet oraz linii światłowodowych. Przedstawiono kilka urządzeń sprzętowych oraz programy, spełniające różne role przy testowaniu sieci. Podano także w ogólnym zarysie sposób szukania błędów w sieciach.

SIMPLE METHODS FOR WIDE AREA NETWORK TESTING

Summary. This article presents several simple methods for wide area networks testing. The point of this article relates to the Internet network, particularly its part that is composed of leased-lines, Ethernet and fiber optics. A few hardware devices and programs that serve various purposes in network testing were presented. A simple method of error finding in networks was also presented.

TESTE DES RESEAUX ETENDUS PAR DES SIMPLES METHODES

Résumé. Cet article présente quelques simples methodes testant les réseaux étendus. Le sujet suivant concerne le réseau Internet, et en particulièrement son fragment qui se compose des lignes RS-232 mis en series, le réseau Ethernet ainsi que les fibres optiques. Ils sont présentés aussi quelques appareils et programmes réalisant des differents roles lors du teste de ces reseaux. Il a été donné en general la manière de decouvrir les erreurs dans les réseaux.

1. Wstęp

Sieć komputerowa to zbiór wzajemnie połączonych komputerów. Połączenia między komputerami są realizowane przez fizyczne środki transmisji (kable, światłowody, fale radiowe) oraz protokoły komunikacyjne - oprogramowanie działające na poszczególnych węzłach sieci. W trakcie eksploatacji sieci zdarzają się sytuacje, kiedy pewien element sieci ulega awarii - możemy wtedy zwykle zaobserwować jej skutki (np. tracimy łączność z niektórymi komputerami). Wtedy należy przystąpić do lokalizacji uszkodzenia. Taka lokalizacja jest szczególnie skomplikowana w przypadku sieci rozległych, gdyż wykorzystują one różne media transmisji. Administratorowi takiej sieci potrzebna jest wiedza obejmująca zasady działania i możliwości diagnozowania połączeń między komputerami oraz oprogramowania działającego na komputerach sieci.

Opisane poniżej metody i narzędzia były wykorzystywane przy eksploatacji fragmentu sieci Internet, łączącego przy użyciu łączy szeregowych, sieci lokalnej Ethernet i łączy światłowodowych komputery klasy IBM PC oraz serwery pracujące pod systemami UNIX.

Istnieje warstwowy model sieci komputerowej (np. ISO/OSI), dzięki któremu można podejść metodycznie do zagadnienia testowania sieci. Najniższą warstwą są fizyczne łącza danych, nad nimi znajdują się protokoły komunikacyjne, a na samej górze działają aplikacje wykorzystujące sieć. Ogólna metoda testowania sieci polega na znalezieniu najwyższej warstwy sieci, która jeszcze poprawnie realizuje swoje działania, a następnie należy zlokalizować przyczynę błędnego działania (lub braku działania) wyższej warstwy. Testowanie różnych warstw sieci jest wykonywane w celu osiągnięcia różnych rezultatów:

- dla warstwy fizycznej chcemy sprawdzić, czy potrafi ona przesyłać dane bez zakłóceń lub przy zakłóceniach o tolerowalnej wartości. W tej warstwie dla każdego miedium transmisyjnego należy stosować specyficzne dla tego medium metody;
- dla warstwy logicznej interesuje nas, czy sieć jest w stanie poprawnie nadawać i odbierać ramki protokołu IP;
- dla warstwy aplikacyjnej sprawdzamy poprawność konfiguracji i działania wybranych aplikacji.

2. Testowanie warstwy fizycznej

Testowanie warstwy fizycznej sieci rozleglej wymaga specyficznych metod dla danych mediów transmisji. W tym opracowaniu skupiono się na liniach szeregowych oraz na odmianach sieci Ethernet. Inne media transmisji będą prawdopodobnie wymagać innego rodzaju metod testowania, aczkolwiek doświadczenie zdobyte przy testowaniu jednego rodzaju medium transmisji może się przydać dla innego medium.

2.1. Łącza szeregowe według standardu RS-232

Pierwszą rzeczą, którą możemy sprawdzić, jest zmierzenie oporności kabli łączących modemy przy użyciu miernika oporności. Jest to możliwe przy liniach dzierżawionych (zwykle kable), zaś dla linii komutowanych nie stosuje się takich pomiarów. Po sprawdzeniu kabli można podłączyć modemy i obserwować, czy modemy będą potrafiły nawiązać między sobą łączność. Dla linii komutowanych trzeba jeden modem ustawić tak, aby odbierał przychodzące telefony, zaś dla linii dzierżawionych jeden modem należy ustawić w stanie "Originate" (to jest modem zaczynający połączenie), zaś drugi modem w stanie "Answer" (ten modem będzie odpowiadał na żądania pierwszego modemu). W przypadku braku łączności trzeba próbować zmieniać konfigurację modemów aż do uzyskania połączenia. Następnie trzeba sprawdzić konfigurację modemów dotyczącą wymiany danych z komputerem. Jest to szczególnie ważne w przypadku połączeń wykorzystujących protokoły SLIP/PPP, które wymagają przeźroczystego kanału transmisji, tzn. takiego, który potrafi przesłać wszystkie bajty danych bez zmian. W miarę możliwości należy ustawić w oprogramowaniu komunikacyjnym transmisję z potwierdzeniem sprzętowym przy użyciu linii RTS/CTS, a nie za pomocą znaków XON/XOFF (wykorzystywane w połączeniach terminalowych - jako emulacja terminala), gdyż powoduje to przekłamania przy transmisjach binarnych. Trzeba sprawdzić przy użyciu miernika oporności, czy kable modemowe przenoszą wszystkie używane sygnały, a także ustawić w konfiguracji modemu, by używał on linii RTS/CTS. Jeśli chcemy obserwować zachowanie się linii sterujących i linii danych w kablu modemowym, przydatny może okazać się prosty przyrząd, wykonany z kilkunastu diod LED i oporników. Pozwala on zaobserwować aktualny stan linii, a także pokazuje, czy w danej chwili zachodzi transmisja danych. Następnie można sprawdzić przy użyciu programów emulujących terminal (np. Kermit), czy w obie strony można przesyłać dane. Brak takiej transmisji może dotyczyć niedopasowania parametrów portu szeregowego komputera i modemu - powinny one mieć ustawione taką samą szybkość transmisji, tyle samo bitów

stopu oraz jednakowo ustawione sprawdzanie parzystości. Później możemy przystąpić do sprawdzania, czy przez połączenie jesteśmy w stanie przesłać dane binarne. Można to zrobić przez uruchomienie programu KA9Q, który ma wbudowaną obsługę protokołów SLIP i PPP. Po odpowiedniej konfiguracji programu (wybranie portu szeregowego, ustawienie parametrów IP, ustawienie domyślnego kierunku wysyłania ramek przez łącze szeregowe) można obserwować zachowanie się łącza przy wysyłaniu ramek kontrolnych poprzez komendę "ping". KA9Q posiada wiele liczników, dzięki którym możemy się zorientować, jakie występują błędy podczas pracy. Wartości liczników możemy zobaczyć za pomocą komend "asystat" i "ifconfig".

2.2. Sieć ETHERNET

Najczęściej obecnie stosowaną odmianą sieci Ethernet jest 10base2, która wykorzystuje kabel koncentryczny (RG58A/U) zakończony dwoma terminatorami, każdy o rezystancji 50 Ω. Najczęściej spotykanymi uszkodzeniami jest przerwa lub zwarcie w obrębie jednego ze złączy. Do znalezienia miejsca wystąpienia uszkodzenia możemy użyć miernika oporności. Dobrze działający kabel jest w uproszczeniu układem dwóch równolegle połączonych rezystorów 50 Ω, więc rezystancja w miejscu podłączenia karty sieciowej ma wartość 25 Ω. Jeśli gdzieś nastąpiło zwarcie, miernik pokaże 0 Ω, zaś przy przerwie - 50 Ω. Rozpinając kolejno segmenty sieci i mierząc ich rezystancję możemy znaleźć wadliwe łącza.

Inną, coraz częściej stosowaną odmianą Ethernetu jest 10base-T. Jako medium transmisyjne jest wykorzystana 8-przewodowa skrętka (4 pary). Do sprawdzenia poprawności budowy kabla można użyć miernika oporności, ale jest to niewygodne. Znacznie lepiej wykorzystać prosty układ generujący napięcie na kolejnych parach skrętki, zaś z drugiej strony kabla można podłączyć diody świecące LED. Jeśli kabel jest poprawnie wykonany, cztery diody powinny się po kolei zapalać. Nieuporządkowana kolejność zapalania się diod świadczy o złym połączeniu przewodów, zaś brak świecenia diody sygnalizuje uszkodzenie kabla.

W sieciach Ethernet jest także wykorzystywana technologia kabli światłowodowych - odmiana 10base-F. W tym przypadku jedyną prostą metodą testowania jest obserwowanie urządzeń podłączonych do kabla - są one zwykle wyposażone w diody LED, sygnalizujące transmisję ramek i wystąpienie kolizji. W momencie uszkodzenia samego kabla światłowodowego trzeba zastosować drogi, specjalistyczny sprzęt pomiarowy. Do informowania o braku działania elementów sieci służą także diody LED umieszczone w hubach i koncentratorach. Umożliwiają one szybką orientację, jeśli chodzi o rejon wystąpienia uszkodzenia.

3. Testowanie warstwy logicznej - programy narzędziowe

Podstawową metodą sprawdzania, czy węzel jest w stanie poprawnie wymieniać informację z pozostałą częścią sieci rozległej, jest wysyłanie ramek protokołu ICMP przy użyciu komendy "ping". Polecenie to wysyła ramkę ECHO_REQUEST do podanego węzła, który powinien przy poprawnej pracy sieci odpowiedzieć ramką ECHO_RESPONSE. Przy braku odpowiedzi można sprawdzić, czy odległy węzeł otrzymał ramkę, czy odpowiedział na nią oraz czy ramka ECHO_RESPONSE została wysłana we właściwym kierunku. Podstawową informacją, jaką daje komenda "ping", jest czas otrzymania odpowiedzi. Oprócz tego można wymusić zapamiętanie w przesyłanej ramce numerów węzłów, przez które przechodzi dana ramka. Przy zwykłym wywołaniu pakiety są wysyłane w ustalonych odstępach czasu (wersja komendy w systemie operacyjnym HP-UX), a można także wymusić masowe wysyłanie ramek, co pozwala ocenić, jak sobie dają radę poszczególne węzły sieci przy dużym obciążeniu linii. Inną ciekawą opcją (w implementacji komendy w ramach pakietu KA9Q) jest możliwość wysyłania ramek protokołu ICMP do węzłów o kolejnych numerach IP. Może ona służyć do wyszukiwania aktualnie działających węzłów. Za pomocą komendy "ping" można także okresowo (np. co 10 minut) sprawdzać, czy są osiągalne ważniejsze obszary sieci. Jest to łatwe do zaimplementowanie w systemie operacyjnym UNIX, gdzie istnieją mechanizmy okresowego wykonywania poleceń. Po wykryciu niedostępności jakiegoś węzła sieci skrypt może o tym natychmiast powiadomić administratora sieci, używając poczty elektronicznej bądź wypisując odpowiedni komunikat na konsoli.

Jeśli pakiety wysyłane za pomocą komendy "ping" nie wracają, można spróbować ustalić, jaką drogą ramki próbują dotrzeć do odległego węzła. W tym celu można użyć komendy "traceroute" (w pakiecie KA9Q nosi ona nazwę "hop check"). Wysyła ona ramki protokołu UDP, w których specjalne znaczenie ma pole TTL (Time-to-Live - czas życia ramki). Wartość tego pola określa, przez ile węzłów sieci może przejść ramka, zanim zostanie ona zniszczona. Ten mechanizm pozwala usuwać ramki, które powstały w wyniku przekłamań lub awarii sieci. Na początku jest wysyłana ramka z wartością pola TTL równą 1. Pozwala to ustalić numer sąsiedniego węzła. Następnie wartość pola TTL jest zwiększana o 1, co powoduje uzyskiwanie adresów kolejnych węzłów. Zwiększanie wartości pola TTL trwa aż do osiągnięcia docelowego węzła (sygnalizowane ramką protokołu ICMP o treści PORT_UNREACHABLE) lub do osiągnięcia maksymalnej wartości tego pola (zwykle jest to 30). Jeśli w pewnym momencie przestają przychodzić odpowiedzi od węzłów, to w tym rejonie można szukać przyczyny awarii sieci. Komenda "traceroute" ma tę wadę, że nie potrafi śledzić drogi powrotnej ramki. Ma to znaczenie, gdy istnieje więcej niż jedna

możliwa droga ramki między węzłami i ramka wędruje różnymi drogami dochodząc do odległego węzła i wracając.

Innym mechanizmem, który pozwala na testowanie sieci, jest protokół ARP. Pozwala on w sieciach Ethernet dokonywać konwersji adresów IP (32 bity) na adresy w sieci Ethernet (48 bitów). Za pomocą zlecenia ARP (zaimplementowanego w pakiecie KA9Q i w systemie operacyjnym UNIX) można zobaczyć, jakie są zapamiętane adresy IP - pozwala to ustalić, czy np. niedostępny węzeł był wcześniej widziany, czy była nawiązana z nim łączność. Po wyłączeniu węzła i jego ponownym uruchomieniu (lub po użyciu komendy kasującej zapamiętane wartości - "arp -d") tablice konwersji adresów protokołu ARP są tworzone od nowa, co pozwala na odnotowanie aktualnie używanych adresów IP, widzianych w obrębie lokalnej sieci Ethernet (w obrębie tego samego segmentu sieci). Istnieją także programy pozwalające na analizę pracy sieci. Pozwalają one na obserwację typu i adresów używanych przez ramki. Mechanizmy takie są zawarte w pakiecie KA9Q i są uruchamiane za pomocą zlecenia "trace". Pozwala to obserwować treść ramki razem z jej interpretacją - ustalane są adresy nadawcy i odbiorcy, typ użytego protokołu oraz poprawność sum kontrolnych CRC. Ta komenda może być używana tylko w trakcie rozruchu sieci, gdyż zbyt duża liczba transmitowanych ramek uniemożliwia odczyt i interpretację otrzymanych wyników.

Innym pakietem do obserwacji pracy sieci Ethernet jest EtherDump. Pozwala on na zapisanie ograniczonej liczby bajtów ramki do pliku, łącznie z adresami nadawcy i odbiorcy. Dzięki temu można analizować kolejność pojawiania się ramek w sieci, co jest istotne np. przy uruchamianiu aplikacji sieciowych. Dzięki temu programowi można zaobserwować, jak działa nawiązywanie połączenia "telnet" między komputerem PC i serwerem UNIX, gdzie jest zainstalowany protokół sprawdzania tożsamości użytkowników - "auth". Kiedy użytkownik łączy się z serwerem UNIX za pomocą zlecenia "telnet", UNIX próbuje w tym samym czasie połączyć się za pomocą protokołu "auth" z komputerem PC w celu sprawdzenia tożsamości użytkownika. Długie oczekiwanie użytkownika na wejście do systemu UNIX jest związane z faktem, że serwer UNIX czeka na dokonanie autoryzacji, co nie kończy się pomyślnie - komputer PC nie jest wyposażony w odpowiednie oprogramowanie. Dane generowane przez program EtherDump podczas próby ich analizy wymagają dużej wiedzy osoby analizującej szczegóły implementacji protokołów, gdyż do pliku są zapisywane bajty w postaci liczb szesnastkowych. Poza tym warto określić adresy węzłów, które w czasie zbierania danych generowały niepotrzebne dane i usunąć ramki przez nie generowane - przy dużym ruchu w sieci bardzo szybko rośnie wielkość pliku z zapisaną zawartością ramek, co jest trudne do analizy. Ten program wymaga komputera o dużej wydajności, gdyż w przeciwnym razie może dojść do pomijania niektórych ramek, co utrudnia prawidłową analizę pracy sieci.

Istnieją też specjalizowane produkty (np. LANanalyzer firmy Novell), które potrafią zapisywać do pliku treść ramek razem z ich interpretacją, ale ich działanie ogranicza się do wybranych protokołów.

Programem o innej koncepcji działania jest EtherLoad. Pracuje on w sieciach Ethernet i Token Ring. Jego zadaniem jest gromadzenie różnego rodzaju statystyk dotyczących pracy sieci. Potrafi analizować ramki różnych protokołów (NetBEUI, TCP/IP, OSI, DECnet i inne) oraz pozwala śledzić występowanie ważniejszych zdarzeń zachodzących w obrębie sieci: jakie protokoły są w użyciu, pozwala obserwować sekwencje BOOTP i TFTP (przy uruchamianiu węzłów), pokazuje zawartość tablic protokołu ARP, podaje statystykę wielkości odebranych ramek, zlicza błędy i ich rodzaje (np. zbyt krótkie lub zbyt długie ramki). Pozwala także na obserwowanie, jakie opcje protokołu IP są używane w przesyłanych ramkach. W sposób semigraficzny pokazuje liczbę ramek używających określonych typów protokołów, pozwala zlokalizować węzeł, który nadaje i odbiera największą liczbę ramek.

Wszystkie wymienione programy wymagają bardzo szybkich komputerów w celu uniknięcia zagubienia odczytywanych ramek z sieci, zaś analiza uzyskanych wyników wymaga wiedzy na temat budowy i działania sieci komputerowych.

4. Aplikacje sieciowe

Kolejnym poziomem, na którym można testować sieci rozległe, są aplikacje sieciowe. Elementy sieci Internet, takie jak protokoły RIP (rozpowszechnia informacje o doborze tras ramek w sieci) i serwery nazw (name server) mają organizację hierarchiczną, co powoduje, że błędy konfiguracji w jednym miejscu sieci mogą mieć rezultaty w zupełnie innym miejscu. Przykładem może być sytuacja, kiedy pewnego dnia przestają się uruchamiać terminale graficzne (X Terminal) podłączone do serwera pracującego pod kontrolą systemu UNIX. Takie terminale są specjalizowanymi komputerami, zoptymalizowanymi pod kątem szybkości realizacji operacji graficznych oraz sieciowych. Terminale graficzne po włączeniu zasilania próbują odczytać z serwera UNIX (przy użyciu sieciowego protokołu NFS) kod realizowanych przez siebie programów. W tym konkretnym przypadku próba realizacji tego zadania zakończyła się niepowodzeniem. Konfiguracja terminali była poprawna, nic nie tłumaczyło kłopotów przy uruchamianiu. Kilka godzin później okazało się, że nie działają także usługi pocztowe - nie da się pobrać z serwera UNIX poczty za pomocą protokołu POP3 (pozwala na wygodne nadawanie i odbieranie poczty z serwera UNIX bez uruchamiania sesji terminalowej). Program obsługujący żądania protokołu POP3 jest dostępny w wersji źródłowej, co pozwoliło krok po kroku znaleźć miejsce w programie, które było przyczyną kłopotów - wywołanie funkcji gethostbyname(), której realizacja trwała ponad minutę.

Zadaniem tej funkcji jest zamiana symbolicznej nazwy węzła na adres IP, wyrażony w postaci liczby 32-bitowej. To nasunęło podejrzenie o złej konfiguracji serwera nazw. Okazało się, że serwer nazw był tak skonfigurowany, że wysyłał żądania do sąsiednich węzłów, nawet jeśli nazwy przeznaczone do konwersji mogły być przekształcone przy użyciu tylko lokalnego serwera nazw. Wtedy wystarczyła awaria (lub tylko wyłączenie) jednego z sąsiednich węzłów, aby serwer nazw bardzo długo realizował pewne rodzaje żądań i w konsekwencji niektóre usługi (np. w czasie uruchamiania terminali graficznych występuje żądanie do serwera nazw, tak samo w przypadku protokołu POP3) zwracały informację o błędzie w działaniu. Po zmianie konfiguracji lokalnego serwera nazw sytuacja wróciła do normy. Ten przykład pokazuje, że bardzo ważną rolę przy testowaniu pracy sieci rozległej odgrywa możliwość szczegółowej analizy działania aplikacji na poziomie kodu źródłowego.

5. Podsumowanie

Sieci rozległe są bardzo skomplikowane, składają się z wielu rodzajów środków transmisji i łączą wiele różnych sieci. Testowanie sieci rozległych ma za zadanie sprawdzenie poprawności działania sieci oraz znajdowanie błędów w pracy sieci i określanie sposobów ich usuwania. Podstawowa metoda znajdowania błędów polega na zlokalizowaniu poprawnie działającej warstwy sieci i ustaleniu, dlaczego nie działa warstwa wyższa. Znajdowanie i usuwanie błędów w sieciach rozległych wymaga obszernej wiedzy na temat każdego poziomu działania sieci. Taką wiedzę można nabyć przez lekturę standardów budowy sieci, opisów działania protokołów sieciowych oraz przez analizę aplikacji sieciowych, pod warunkiem że można skorzystać z kodu źródłowego lub dokładnej dokumentacji. Innym, trudniejszym sposobem zdobycia wiedzy może być analiza kodu źródłowego pakietu KA9Q (w języku C). Pakiet ten implementuje szereg podstawowych mechanizmów sieci Internet i pokazuje praktyczne zastosowanie protokołów, zaś praca włożona w analizę treści plików o łącznej długości 1,5 MB na pewno się opłaci.

LITERATURA

[1] Piotrowski J.: Przewodnik po sieciach rozległych. Helion, Gliwice 1993.

[2] Gabassi M., Dupouy B.: Przetwarzanie rozproszone w systemie UNIX. Lupus, Warszawa 1995.

[3] Postel J.: Internet Protokol. Request For Comments 791, 1981.

[4] Plummer D., Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transsmision on Ethernet hardware. Request For Comments 826, 1982.

[5] Malkin G., Traceroute Using an IP Option. Request For Comments 1393, 1993.

Recenzent: Dr inż. Ryszard Winiarczyk

Wplynęlo do Redakcji 27 grudnia 1995 r.

Abstract

This article presents several simple methods for wide area networks testing. The methods of testing were used while working with the Internet network. Various kinds of transmission mediasuch as: leased-lines, the Ethernet net (10base2, 10base-T, 10base-F) are mixed within one network. Suitable measurement instruments were presented for all kinds of media. Examples of programs that operate on IBM PC compatible microcomputers and on UNIX systems were given. These programs analyse the contents of frames and allow to record them in a file. The basic method of error finding in wide area networks was described. The sample when one faulty network piece affected another area of network activity was given. The importance of network manager's knowledge about network architecture and activity was emphasized.