dr inż. Dariusz Chaładyniak
wykładowca w Warszawskiej Wyższej Szkole Informatyki
dchalad@wwsi.edu.pl

mgr inż. Jacek Grzybowski
słuchacz studiów podyplomowych w Warszawskiej Wyższej Szkole Informatyki
j_grzybowski@poczta.wwsi.edu.pl

Wybrane metody diagnozowania nieprawidłowości działania sieci teleinformatycznych

Selected methods of diagnosing of telecommunication networks malfunctioning

Streszczenie

Sieci teleinformatyczne są efektywne, jeżeli działają prawidłowo, tzn. w pełni realizują swoje funkcje we wszystkich warstwach logicznego modelu ISO/OSI.
W realnym świecie jednak z różnych przyczyn występują awarie, które powodują różnego rodzaju problemy z poprawnym działaniem sieci. Opierając się na warstwowym modelu ISO/OSI można sklasyfikować problemy występujące w sieciach teleinformatycznych w odniesieniu do poszczególnych warstw modelu. Większość problemów związanych z niedziałaniem sieci teleinformatycznych przypisane jest do niższych warstw modelu ISO/OSI. Są to warstwy związane z fizycznymi nośnikami danych sieciowych, urządzeniami sieciowymi oraz podstawowymi mechanizmami sterującymi przepływem danych w sieciach teleinformatycznych. Powyższym zagadnieniom poświęcony jest ten artykuł.

Słowa kluczowe: model ISO/OSI, sieci teleinformatyczne, warstwa fizyczna, warstwa łącza danych, warstwa sieciowa, analizator sieci

Abstract

Telecommunication networks are efficient when they operate correctly, i.e. they fully carry out their functions in all layers of the logical ISO/OSI model. In the real world for various reasons, there are failures that cause problems and improper operation of networks. Based on the layered ISO/OSI model, we can develop a classification of the problems encountered in data communication networks for the individual layers of the model. Most of the problems related with networks malfunctioning are attributed to lower layers of the ISO/ OSI model. These are related to the network data storage medium, network devices and the basic mechanisms of data flow control in data communication networks. The article presents these issues.

Keywords: ISO/OSI model, telecommunication networks, physical layer, data link layer, network layer, network analyzer

1. TYPOWE NIESPRAWNOŚCI SIECI TELEINFORMATYCZNYCH

Poniżej przedstawiono typowe niesprawności sieci pogrupowane według logicznych warstw modelu ISO/OSI, w których występują.

Warstwa fizyczna będąca najniższą warstwą modelu ISO/OSI, jest odpowiedzialna za przesyłanie bitów danych z jednego komputera na inny i regulację transmisji strumieni bitów przez nośnik fizyczny, jakim są przewody miedziane i światłowodowe, interfejsy fizyczne kart sieciowych oraz anteny dla sieci bezprzewodowych. Awarie i nieoptymalne warunki występujące w warstwie fizycznej mogą mieć wpływ na pracę firmy, korporacji czy instytucji. Sieci, w których występują usterki w warstwie fizycznej zazwyczaj nagle przestają funkcjonować. Najczęściej występującymi problemami i usterkami w warstwie fizycznej są:

- **Utrata łączności** - będąca wynikiem zaprzestania działania urządzenia lub niesprawnego kabla sieciowego. Objawem jest utrata połączenia między urządzeniami, które komunikują się przez to samo łącze albo przez nieczynne urządzenie lub interfejs. Przyczyną utraty łączności mogą być obluzowane lub utlenione połączenia.
- **Wskaźniki błędów** - czyli komunikaty błędów wyświetlane w konsoli urządzenia oznaczają problem w warstwie fizycznej. Informować o tym mogą również diody znajdujące się na urządzeniach sieciowych.
- **Duża liczba kolizji** - może to być problem w sieciach ethernetowych ze współdzielonymi nośnikami, w których średni wskaźnik kolizji przekracza 5%. Przyczyną problemów związanych z kolizjami może być zły kabel albo interfejs. Jeżeli wskaźniki kolizji mają zbyt wysokie wartości i urządzenie sieciowe jest przeciążone to sieć może przestać działać.

Najczęściej spotykanymi przyczynami usterek w warstwie fizycznej sieci teleinformatycznej są:

- **Awarie zasilania** – jest to jeden z podstawowych powodów niesprawności sieci występujący zarówno lokalnie (w obrębie konkretnego urządzenia sieciowego) jak i globalnie typu awaria zasilania w obrębie dzielnicy lub całego regionu.
- **Wadliwy sprzęt** – w tym przypadku głównym „podejrzanym" stają się karty sieciowe (NIC), które mogą być przyczyną błędów w transmisjach sieciowych ze względu na różne kolizje, krótkie ramki i zakłócenia typu „jabber" (tzw. „rozwlekanie").
- **Wadliwe okablowanie** – jest to częsta przyczyna awarii sieci, którą rozwiązuje się poprawiając kable, a właściwie obluzowane albo źle zarobione wtyki na kablach. W przypadku sieci Ethernet dla kabli miedzianych typu UTP i STP jest to wtyk RJ-45. Oprócz tego, podczas diagnostyki należy szukać uszkodzonych lub niewłaściwych kabli (pod kątem niewłaściwego standardu zarobienia końcówek lub nieodpowiedniej długości). W przypadku kabli światłowodowych spotykamy się z problemami związanymi z zanieczyszczonymi złączami, zbyt mocnymi wiązaniami albo zamienionymi połączeniami RX/TX przy polaryzacji.
- **Tłumienie** – usterka powstająca na skutek zbyt dużego tłumienia sygnału w medium transmisyjnym. Przyczynami powstawania zbyt dużego tłumienia może być zbyt długi kabel przekraczający limit przewidziany dla danego nośnika (np.: dla skrętki kat 5E poprawna transmisja jest gwarantowana dla długości poniżej 100 metrów), słabe połączenie wynikające z luźnego kabla albo utlenione styki.
- **Szum** – jest to zjawisko występowania lokalnej interferencji elektromagnetycznej (EMI), której wyróżniamy 4 podstawowe typy mające największe znaczenie dla sieci teleinformatycznych: szum impulsowy, szum losowy (tzw. biały), przesłuch obcy oraz przesłuch zbliżny (tzw. NEXT).
- **Błędy w konfiguracji interfejsu** – źle skonfigurowane interfejsy szeregowe.
- **Przeciążenie procesora** routera spowodowane intensywnym ruchem na jednym bądź kilku interfejsach routera.

Problemy występujące w warstwie łącza danych, będącej drugą warstwą modelu ISO/OSI, cechują się rozpoznawalnymi objawami a ich identyfikacja pozwala ograniczyć liczbę możliwych przyczyn. Do typowych objawów problemów sieciowych w warstwie łącza danych możemy zaliczyć:

- **Brak funkcjonowania lub brak łączności w warstwie sieci albo wyższej** – przy identyfikacji braku łączności bardzo pomocne są wskaźniki na urządzeniach sieciowych występujące w postaci diod, zazwyczaj w kolorze bursztynowym.
- **Sieć działa poniżej poziomów wydajności określonych w linii bazowej** – takie nieoptymalne działanie w warstwie 2 możemy podzielić na dwa typy:

- Ramki docierające do celu nielogiczną drogą powodują spadek wydajności sieci. Przykładem problemu powodującego takie działanie może być źle zaprojektowana topologia drzewa rozpinającego w warstwie drugiej. W tym przypadku na łączu, które nie powinno mieć takiego poziomu ruchu, można zaobserwować wysokie wykorzystanie szerokości pasma.
- Niektóre ramki są odrzucane – taki problem można zidentyfikować na podstawie statystyk błędów i komunikatów o błędach na konsoli przełącznika lub routera.

- **Nadmierna liczba rozgłoszeń** wynikająca z tego, iż obecne systemy operacyjne używają bardzo intensywnie komunikatów rozgłoszeniowych do wykrywania usług sieciowych i innych hostów. Przyczyną powstawania nadmiernej liczby rozgłoszeń może być:

  - źle napisane lub źle skonfigurowane aplikacje;
  - duże domeny rozgłoszeniowe warstwy 2;
  - niewidoczne problemy sieciowe, np.: pętle protokołu STP (Spanning Tree Protocol) albo niestabilność trasy.

- **Komunikaty na konsoli** – najczęściej wysyłane przez routery na konsole informujące o problemie w warstwie drugiej.

Najczęściej spotykanymi przyczynami usterek w warstwie łącza danych sieci teleinformatycznej są:

- **Błędy enkapsulacji** – występują wtedy, jeżeli enkapsulacja po jednej stronie łącza WAN zostanie inaczej skonfigurowana niż enkapsulacja po drugiej stronie.
- **Błędy mapowania adresów** – polegają na niedopasowaniu informacji z warstw 2 i 3 czyli nieprawidłowego mapowania adresów warstwy drugiej i trzeciej.
- **Błędy ramkowania** – takie błędy mają miejsce, gdy ramka nie kończy się na granicy ośmiu bitów.
- **Awarie lub pętle STP** – są to awarie związane z nieprawidłowym działaniem protokołu STP.

Problemy występujące w warstwie sieci, będącej trzecią warstwą modelu ISO/OSI, są związane z protokołami warstwy 3, zarówno routowalnymi jak i protokołami routingu. Najczęstszymi objawami problemów w warstwie sieci są awaria sieci i wydajność sieci niższa od linii bazowej. Awaria sieci ma miejsce wtedy, gdy sieć jest prawie lub zupełnie niefunkcjonalna, co bezpośrednio wpływa na wszystkich użytkowników i aplikacje w sieci. W większości sieci trasy statyczne są używane w połączeniu z protokołami routingu dynamicznego. Nieprawidłowa konfiguracja tras statycznych może doprowadzić do nieoptymalnego routingu, a czasami do powstawania pętli routingu lub nieosiągalności niektórych części sieci.

Rozwiązywanie problemów z protokołami routingu dynamicznego wymaga gruntownej znajomości funkcjonowania konkretnego protokołu routingu. Nie istnieje jeden szablon rozwiązywania problemów w warstwie 3. Problemy z routingiem rozwiązuje się metodycznie za pomocą serii poleceń ułatwiających wyizolowanie i zdiagnozowanie problemu.

Problemy występujące w warstwie transportu, będącej czwartą warstwą modelu ISO/OSI, są związane z obszarami, gdzie sieci teleinformatyczne są zabezpieczane i monitorują ruch w sieci. Ma to miejsce w routerach brzegowych bądź kluczowych węzłach sieci.

Do najczęściej spotykanych problemów w tej warstwie możemy zaliczyć:

- przejściowe problemy w sieci;
- problemy z zabezpieczeniami opartymi na ACL;
- problemy z translacją adresów (NAT);
- problemy z konkretnymi typami ruchu.

Kluczowymi spośród nich są usterki wynikające z nieprawidłowej konfiguracji list ACL (Access Control List) oraz problemów z współpracy NAT z innymi technologiami sieciowymi.

Trzy ostatnie warstwy modelu ISO/OSI dostarczają usługi użytkowników za pośrednictwem protokołów takich jak HTTP, FTP, POP3, SNMP, DNS, FTP, SMTP, TFTP czy Telnet. W równoległym modelu warstwowym TCP/IP zostały połączone w jedną warstwę aplikacji. Protokoły tej warstwy są używane do zarządzania siecią, transferu plików, rozproszonych usług plikowych, emulacji terminalu i poczty e-mail, a ostatnio również dodatkowych usług takich jak VPN czy VoIP. Występowanie usterek w warstwie aplikacji dla modelu TCP/IP czy też w warstwach sesji, prezentacji i aplikacji modelu OSI, uniemożliwia dostarczanie usług do programów. Skutkiem tego mogą być nieosiągalne lub nieużywane zasoby mimo działania pozostałych warstw modelu OSI. Przyczynami takich usterek może być nieprawidłowe działanie wymienionych wyżej protokołów warstwy aplikacji bądź też niepoprawna konfiguracja aplikacji hostów korzystających z zasobów sieci.

Izolowanie problemów w tych warstwach odbywa się wg tych samych ogólnych procedur co w warstwach niższych, jednak w tym przypadku dotyczą obszarów takich jak przekroczony czas połączeń, listy dostępu czy problemy z DNS.

2. METODY I NARZĘDZIA DO DIAGNOZOWANIA NIEPRAWIDŁOWOŚCI DZIAŁANIA SIECI TELEINFORMATYCZNYCH

Rozwiązywanie problemów z sieciami teleinformatycznymi jest praktycznie niemożliwe bez diagramu sieci z naniesionymi adresami IP, adresami sieciowymi, domenami routingu i urządzeniami infrastruktury, takimi jak routery, ściany ogniowe, przełączniki, punkty dostępowe czy serwery danych. Praktycznie dostępne powinny być dwie mapy sieci teleinformatycznej: topologia fizyczna oraz topologia logiczna.

Fizyczny diagram sieci przedstawia fizyczne rozmieszczenie urządzeń połączonych z siecią. Wiedza o sposobie fizycznego połączenia urządzeń w sieci pozwala rozwiązywać problemy w warstwie fizycznej, takie jak problemy z okablowaniem albo sprzętem. Na takim diagramie powinny znajdować się następujące informacje:

- typ urządzenia,
- model i producent,
- wersja systemu operacyjnego,
- typ kabla i identyfikator,
- typ złącza,
- punkty końcowe okablowania.

Logiczny diagram sieci pokazuje, w jaki sposób dane są przesyłane przez sieć. Do zobrazowania urządzeń sieciowych, takich jak serwery, routery, koncentratory, hosty, koncentratory VPN i urządzenia bezpieczeństwa, na diagramach logicznych stosuje się symbole graficzne. Diagramy zawierają następujące informacje:

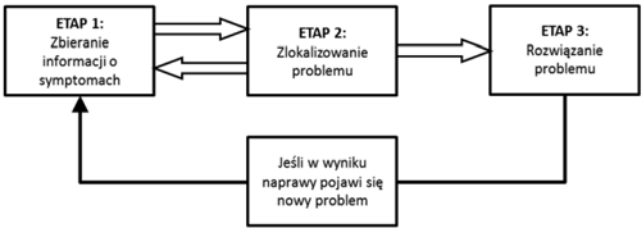
- ✓ identyfikatory urządzeń,
- ✓ adresy IP i maski podsieci,
- ✓ identyfikatory interfejsów,
- ✓ typy połączeń,
- ✓ numery DLCI obwodów wirtualnych,
- ✓ sieci VPN typu stanowisko-stanowisko,
- ✓ protokoły routingu,
- ✓ trasy statyczne,
- ✓ protokoły warstwy łącza danych,
- ✓ używane technologie WAN.

Znane są dwa ekstremalne podejścia do rozwiązywania problemów z sieciami teleinformatycznymi. Jedną z nich jest metoda teoretyczna polegająca na dogłębnej analizie teoretycznej problemu aż zostanie znalezione źródło problemu i błąd zostanie usunięty. Proces ten jest niezawodny jednak bardzo czasochłonny, co staję się jego sporą wadą. Bardzo rzadko jest dopuszczalne, aby sieć była niesprawna przez bardzo długi okres czasu potrzebny na wykonanie drobiazgowej analizy. Drugą z metod jest metoda siłowa polegająca na wymianie podejrzanych o niesprawność elementów sieci, takich jak karty sieciowe, kable, urządzenia i programy, do momentu, aż sieć ponownie zacznie działać. Nie jest to równoznaczne z tym, że sieć działa poprawnie, jednak łączność została przywrócona. Metodę siłową cechuję szybkość działania, jednak nie jest ona niezawodna i nie odkrywa oraz nie eliminuje rzeczywistej przyczyny powstałego problemu.

Obie wskazane metody stanowią dwa ekstremalne podejścia do tematu niesprawności sieci teleinformatycznych i żadna z nich nie jest preferowana. Najlepszym rozwiązaniem jest działanie pośrednie, łączące w sobie cechy obu powyższych podejść. Istotna jest analiza sieci jako całości, a nie tylko jej poszczególnych fragmentów. Podejście takie można określić jako metodę systematyczną, która pozwoli skrócić czas na poszukiwanie problemu. W tej metodzie wykorzystuje się modele warstwowe ISO/OSI i TCP/IP, które pozwalają na rozdzielenie funkcji sieci na modularne warstwy ułatwiające proces poszukiwania.

Ogólną procedurę rozwiązywania problemów można podzielić na następujące etapy:

- Etap 1: Zbieranie informacji o symptomach
- Etap 2: Zlokalizowanie problemu
- Etap 3: Rozwiązanie problemu



Rys. 2.1. Etapy rozwiązywania problemów z sieciami [1].

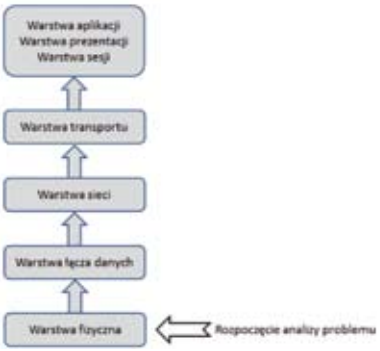
Etap 1 zakłada rozpoczęcie procesu od zbierania danych i udokumentowania objawów w sieci, w systemach końcowych i od użytkowników. W tym kroku administrator ustala także, których komponentów sieciowych dotyczy problem i jak zmieniło się funkcjonowanie sieci w odniesieniu do posiadanej linii bazowej. Objawami mogą być alarmy z systemu zarządzania siecią, komuniskaty na konsoli lub skargi od użytkowników. Podczas 2 etapu administrator sieci bada cechy problemów w logicznych warstwach sieci, aby zlokalizować najbardziej prawdopodobną przyczynę awarii. W 3 etapie administrator przechodzi do pracy nad wyeliminowaniem problemu przez implementację, testowanie i dokumentowanie rozwiązania problemu sieciowego.

Przedstawione etapy nie wykluczają się wzajemnie. W dowolnym momencie procesu może okazać się koniecznym powrót do poprzedniego etapu, np.: celem zebrania dodatkowych danych do analizy. Może się też okazać, że w trakcie rozwiązywania problemu zostanie wygenerowany kolejny. W skutek tego będzie potrzebny powrót do zbierania objawów, a następnie lokalizacja i rozwiązanie bieżącego problemu.

Można wyróżnić trzy podstawowe metody rozwiązywania problemów w sieciach teleinformatycznych:

- metoda analizy ISO/OSI od dołu do góry (bottom-up),
- metoda analizy ISO/OSI od góry do dołu (top-down),
- metoda analizy „dziel i zwyciężaj” (divide-and-conquer).

Pierwsza z wymienionych metod zwana również „bottom-up” zakłada rozpoczęcie analizy sieci od komponentów fizycznych czyli warstwy 1 modelu ISO/OSI, a w następnej kolejności przechodzenie przez kolejne warstwy aż do znalezienia przyczyny problemu.

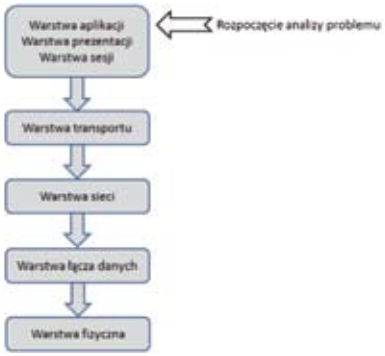


Rys. 2.2. Metoda analizy ISO/OSI od dołu do góry [1].

Rozwiązywanie problemu tą metodą jest dobre jeżeli istnieje podejrzenie, że problem dotyczy warstwy fizycznej. Większość problemów sieciowych ma swoje źródło na niższych poziomach więc analiza metodą „bottom-up" często jest jedną z najbardziej efektywnych.

Do istotnych wad tej metody można zaliczyć konieczność sprawdzania każdego urządzenia i interfejsu w sieci, aż do momentu znalezienia przyczyny problemu. Dodatkowym utrudnieniem jest określenie, od którego urządzenia rozpocząć sprawdzanie.

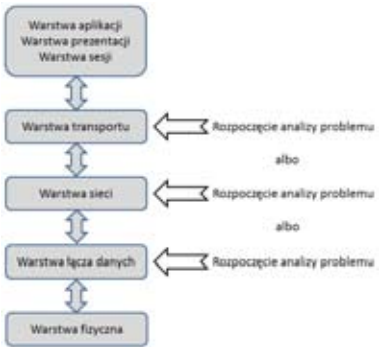
Drugą z przedstawianych metod jest metoda analizy ISO/OSI od góry do dołu nazywana „top-down". Zakłada ona rozpoczęcie analizy problemu od najwyższej, 7 warstwy modelu ISO/OSI, czyli aplikacji użytkownika końcowego, a następnie przechodzenie przez kolejne warstwy modelu w kierunku najniższej warstwy fizycznej do momentu znalezienia przyczyny problemu.



Rys. 2.3. Metoda analizy ISO/OSI od góry do dołu [1].

Przed zbadaniem kluczowych elementów sieci z warstw niższych administrator przeprowadza testy aplikacji użytkowników systemów końcowych. Metoda ta sprawdza się w przypadku prostych problemów albo kiedy istnieje podejrzenie, że występujący problem dotyczy aplikacji. Wadą tej metody jest wymóg sprawdzania każdej aplikacji sieciowej aż do momentu znalezienia możliwej przyczyny problemu. Podobnie jak w poprzedniej metodzie utrudnieniem jest ustalenie, od której aplikacji zacząć sprawdzanie.

Trzecia metoda łączy w sobie cechy dwóch poprzednich. Posługując się metodą „dziel i zwyciężaj" przy rozwiązywaniu problemów w sieci wybieramy warstwę początkową, a następnie przeprowadzamy testy w obu kierunkach.



Rys. 2.4. Metoda analizy „divide-and-conquer" [1].

W tej metodzie działania rozpoczynamy od zebrania od użytkowników informacji o problemie i udokumentowaniu objawów. Następnie na podstawie zebranych informacji decydujemy, od której warstwy modelu ISO/OSI rozpoczynamy badania. Jeżeli okazuje się, że wybrana warstwa działa prawidłowo to zakładamy, że warstwy niższe również działają i przeprowadzamy analizę w górę modelu ISO/OSI. Jeżeli jednak okazuje się, że warstwa nie działa prawidłowo to rozpoczynamy poszukiwanie problemu po kolei w niższych warstwach modelu ISO/OSI. takie działanie pozwala szybciej zlokalizować problem.

3. NARZĘDZIA PROGRAMOWE WSPOMAGAJĄCE ROZWIĄZYWANIE PROBLEMÓW Z DZIAŁANIEM SIECI

Jednymi z podstawowych narzędzi programowych są „ping" i „tracert". Ping testuje połączenie „end-to-end", wysyłając w tym celu pakiet protokołu ICMP (Internet Control Message Protocol). Akcja ta pozwala stwierdzić, czy węzeł lub urządzenie jest włączone i czy reaguje. Jednym z pierwszych kroków w wykrywaniu niesprawności sieci jest użycie do testowania urządzeń lokalnych ogólnego adresu pętli zwrotnej IP ping 127.0.0.1. Ping można użyć do badania maksymalnej jednostki transmisyjnej, to jest maksymalnej ilości danych, które mogą być przenoszone w trybie „end-to-end" w każdym pakiecie.

Ponadto można użyć „ping" do określenia czasu przejścia do innego urządzenia w sieci. „Tracert" wykorzystuje działanie ping przez szacowanie skoków wzdłuż ścieżki i wyliczanie czasu potrzebnego na przejście pakietu z jednego rutera do drugiego. Na przykład, po zleceniu testu ping zdalnemu urządzeniu odpowiedź nadchodzi po upływie długiego czasu. By dowiedzieć się, co jest przyczyną opóźnienia, należy użyć „tracert". Przebada on czasy przejścia do każdego rutera na danej ścieżce, co pozwoli zlokalizować miejsce problemu.

Do narzędzi diagnostycznych z poziomu konsoli możemy zaliczyć takie polecenia jak: nslookup, route, arp czy netstat.

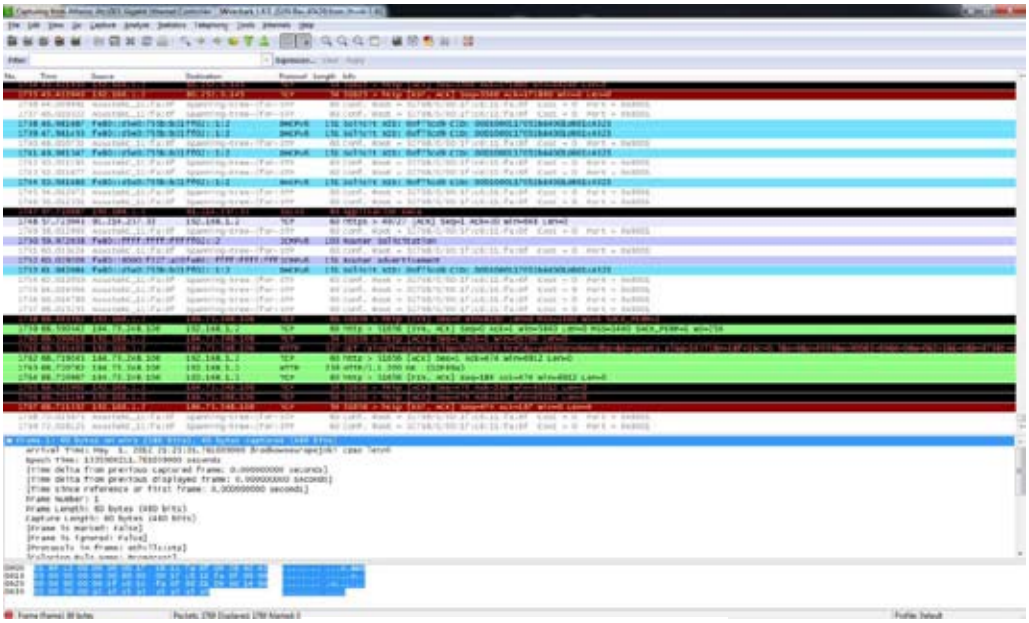
Usługi „nslookup" formułują zapytania do serwerów DNS (Domain Name System). Zapytanie nslookup będzie żądało od domyślnego serwera DNS określenia relacji pomiędzy nazwą hosta a adresem IP. „Route" jest usługą, która pozwala uzyskiwać informacje i manipulować tablicami routingu IP w lokalnym urządzeniu. Tablice ustalają następny skok na ścieżce prowadzącej do hosta lub sieci. Zawierają również domyślne wejście bramy, jeśli takie istnieje. Protokół ARP (Address Resolution Protocol) utrzymuje ścieżkę adresów IP i odpowiadające im fizyczne adresy sieciowe. Dzięki niemu można czytać tablice ARP w celu identyfikacji adresu sprzętu, który wysyła pakiety. Z kolei narzędzie „netstat" dostarcza informacje o konfiguracji i połączeniach.

Uzupełnieniem tych narzędzi jest wiele poleceń diagnostycznych dla systemów Cisco IOS znajdujących się w najbardziej popularnych urządzeniach sieciowych. Pomagają one w lokalizacji problemu już na konkretnym urządzeniu Cisco.

Tabela 3.1. Wybrane polecenia diagnostyczne urządzeń sieciowych CISCO [2].

Polecenie systemu IOS CISCO	Opis działania
Show interfaces	Wyświetla dane statystyczne dotyczące wszystkich interfejsów routera lub przełącznika
Show controllers serial x/x	Wyświetla specyficzne informacje dotyczące sprzętu interfejsu. W poleceniu należy podać port lub numer gniazda/portu interfejsu szeregowego.
Show arp	Wyświetla tablicę ARP routera lub przełącznika
Show protocols	Wyświetla status wszystkich skonfigurowanych protokołów warstwy 3 w ujęciu globalnym i z uwzględnieniem konkretnych interfejsów.
Show ip route	Wyświetla zawartość tablicy routingu routera
Show ip interface brief	Wyświetla informacje na temat stanu interfejsów
Show startup-configuration	Wyświetla zawartość startowego pliku konfiguracyjnego z pamięci NVRAM
Show running-config	Wyświetla zawartość aktualnego pliku konfiguracyjnego urządzenia
Show hosts	Wyświetla przechowywaną w pamięci podręcznej listę nazw i adresów hostów
Show users	Wyświetla nazwy wszystkich użytkowników podłączonych do routera
Show history	Wyświetla historię wprowadzonych poleceń

Kolejnymi narzędziami programowymi pomocnymi przy diagnozowaniu sieci są analizatory protokołu, czasem nazywane analizatorami sieci. Takie programy pozwalają zrozumieć, co dana sieć robi. Analizatory przechwytują wszystkie lub specjalnie zdefiniowane w filtrach pakiety i umieszczają je w buforach. Analizator dekoduje pakiety w celu ukazania ich zawartości w czytelnej postaci. Jednym z najbardziej znanych analizatorów jest Wireshark.



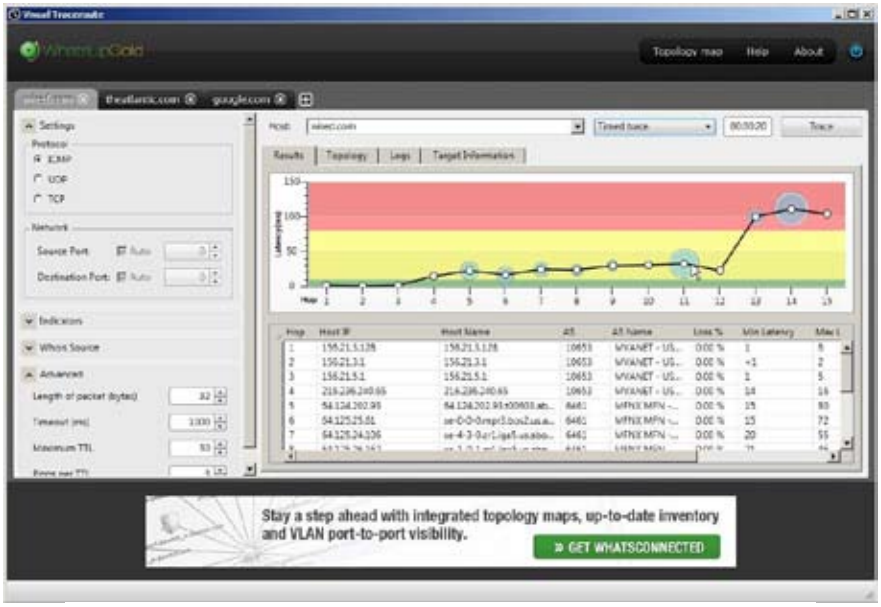
Rys. 3.1. Analizator sieci Wireshark.

Pozwala on na przechwytywanie ruchu sieciowego przechodzącego przez wskazany interfejs. Ruch ten jest wyświetlany w przystępnym formacie pozwalającym zobaczyć zawartość ramek, pakietów

i segmentów oraz rodzaje protokołów uczestniczących w ruchu sieciowym. Wireshark potrafi również filtrować ruch według określonych kryteriów, np. kiedy jest potrzeba śledzenia całości ruchu do określonego urządzenia albo kiedy potrzebujemy śledzić konkretny strumień pakietów.

Drugim ze znanych analizatorów sieciowych pomocnym przy rozwiązywaniu problemów z niezawodnością lub wydajnością sieci jest Sniffer Pro firmy Network Associates. Pozwala on dodatkowo interpretować macierze komunikacyjne w celu zapewnienia alarmów i zaleceń dotyczących niesprawności.

W procesie badania i eliminowania błędów można też wykorzystać tzw. systemy zarządzania siecią NMS (z ang. Network Management System). Są to narzędzia do monitorowania urządzeń, konfiguracji i zarządzania błędami. Programy do monitorowania sieci prezentują urządzenia sieciowe w trybie graficznym, co pozwala administratorom sieci monitorować zdalne urządzenia bez nawiązywania fizycznych połączeń. Przykładem takiego oprogramowania jest „WhatsUp Gold" firmy Ipswitch, Inc.



Rys. 3.2. System zarządzania siecią WhatsUp Gold 15 [3].

Dysponując właściwymi narzędziami, możemy być pewni, że wykrywanie usterek w sieciach TCP/IP będzie łatwiejsze.

4. URZĄDZENIA WSPOMAGAJĄCE ROZWIĄZYWANIE PROBLEMÓW Z DZIAŁANIEM SIECI

Oprócz programów, w rozwiązywaniu problemów z siecią pomocne mogą być urządzenia do diagnozowania niesprawności i monitorowania sieci teleinformatycznych. Można wyróżnić następujące kategorie takich urządzeń:

- Mierniki cyfrowe
- Testery połączeń kablowych
- Testery sieci bezprzewodowych
- Analizatory kabli
- Moduły analizowania sieci (NAM) firmy CISCO
- Przenośne analizatory sieci

Jedną z podstawowych grup narzędzi wykorzystywanych w rozwiązywaniu problemów z sieciami teleinformatycznymi stanowią mierniki cyfrowe (ang. Digital Multimeter). Są to urządzenia służące do bezpośredniego pomiaru wartości elektrycznych takich jak napięcie, natężenie prądu czy rezystancja. W procesach diagnostyki niesprawności sieci wykorzystywane są do sprawdzania poziomów napięcia zasilaczy i identyfikacji problemów z zasilaniem. Przykładowe profesjonalne mierniki do zastosowań przemysłowych pokazano na rysunkach poniżej.

Rys. 4.1. Profesjonalne mierniki cyfrowe.

Testery połączeń kablowych to kolejna grupa urządzeń przenośnych wspierających wykrywanie niesprawności sieci w warstwie fizycznej. Ich zadaniem jest testowanie różnego rodzaju przewodów komunikacyjnych oraz ich połączeń w sieciach teleinformatycznych. Testery kabli znajdują zastosowanie przy wykrywaniu pękniętych i skrzyżowanych przewodów jak również skróconych i nieprawidłowo sparowanych przewodów (niepoprawnie zarobionych złącz na końcach kabli). Urządzenia te można podzielić na 3 grupy: niedrogie proste testery ciągłości, średnio drogie testery przewodów oraz bardzo drogie reflektometry TDR. Przy opisie urządzeń wspomagających wykrywanie niesprawności sieci posłużę się przykładami urządzeń produkowanych przez wiodącą w tej dziedzinie amerykańską firmę Fluke Networks. Przykładem prostego testera ciągłości kabla sieci teleinformatycznej jest MicroMapper firmy Fluke Networks.

Rys. 4.2. Tester MicroMapper firmy Fluke Networks [4].

MicroMapper to mały podręczny tester kabla, który umożliwia specjalistom sieciowym szybkie i łatwe sprawdzenie integralności skrętki ethernetowej. Urządzenie szybko i łatwo testuje skrętki, dzięki czemu diagnozuje takie usterki jak: pęknięcia przewodu, za krótkie końcówki, skrzyżowane pary przewodów, odwrócone i podzielone pary. Proces testowania polega na podłączeniu urządzenia do jednego końca testowanego przewodu, a przystawki „REMOTE" do drugiego końca i naciśnięciu przycisku TEST. Urządzenie wykona automatyczne skanowanie wszystkich par przewodów a znalezione nieprawidłowości zgłosi za pomocą wyświetlacza diodowego.

Bardziej rozbudowaną wersją testera jest MicroScanner Cable Verifier. Urządzenie to posiada już znacznie szersze możliwości testowania zarówno kabli ethernetowych (skrętka UTP, FTP, SSTP) za-

kończonych złączami RJ-45 lub RJ-11 jak i kabli koncentrycznych o impedancji 75Ω, 50Ω lub 93Ω. Testowane kable ethernetowe mogą być wykonane w standardzie TIA-568A lub B.

Rys. 4.3. MicroScanner Cable Verifier firmy Fluke Networks [4].

MicroScanner został wyposażony w duży wyświetlacz LCD z podświetleniem, na którym może prezentować jednocześnie wyniki przeprowadzonych wszystkich kluczowych badań: mapę połączeń, długość par, odległość do miejsca uszkodzenia (przerwy w ciągłości) przewodu, identyfikator kabla (cable ID) oraz odległość do końca urządzenia. Sposób wykonywania testów jest podobny jak w przypadku prostego testera jednak prezentacja wyników kilku testów na czytelnym wyświetlaczu znacząco skraca czas analizy problemu. Urządzenie pozwala również precyzyjnie zlokalizować praktycznie każdą parę kabla lub przewodu, niezależnie od środowiska pracy dzięki wbudowanemu systemowi IntelliTone w wersji cyfrowej i analogowej. Cyfrowy tryb pracy jest wykorzystywany do znajdowania wysokiej klasy okablowania danych (skrętka Cat5e/6/6a) w wiązkach przewodów, w przełącznikach, krosownicach lub gniazdkach ściennych. Cyfrowy tryb jest szczególnie użyteczny w środowiskach o wysokiej transmisji danych, RF lub z dużą ilością zakłóceń elektromagnetycznych. MicroScanner w połączeniu z IntelliTone 200 Probe Pro może być również używany do weryfikacji mapy połączeń kabli od końca testera lub na końcu sondy. Urządzenie potrafi również wykrywać obecność napięcia POTS i sprawdzać jego polaryzację, a dodatkowo diagnozować złącza typu PoE.

Grupę testerów zamykają najbardziej rozbudowane urządzenia typu TDR. Służą one do dokładnego wskazywania odległości do przerwy albo niedoboru kabla. Przykładem takiego urządzenia jest CableIQ Qualification Tester wspomagający rozwiązywanie problemów z przewodami miedziowymi stosowanymi w technologiach Ethernet 10/100/1000 oraz VoIP.

Rys. 4.4. CableIQ Qualification Tester firmy Fluke Networks [4].

Urządzenia te wysyłają przewodem sygnał i czekają na odbicie. Czas między wysłaniem i odebraniem sygnału jest przekształcany na pomiar odległości. Dzięki dużej dokładności urządzenia można precyzyjnie określić, w którym odcinku przewodu nastąpiła awaria, co również skraca czas usunięcia problemu.

Ze względu na dużą popularność połączeń światłowodowych inżynierowie sieciowi muszą posiadać narzędzia do lokalizacji awarii na tego typu łączach. Pomocne tutaj są testery światłowodowe często nazywane reflektometrami optycznymi OTDR (ang. Optical Time-Domain Reflectometers). Podobnie jak w przypadku kabli miedzianych, tutaj również mamy proste i bardziej skomplikowane testery. Do prostych możemy zaliczyć tester VisiFault Visual Fault Locator, który lokalizuje usterki typu: ciasny zakręt, przerwane włókno, złe złącze oraz łatwo sprawdza polaryzację i identyfikuje włókna.

Rys. 4.5. VisiFault Visual Fault Locator firmy Fluke Networks [4].

Urządzenie obsługuje złącza SFF o średnicach 2,5 mm oraz 1,25 mm, a cała procedura testowania sprowadza się do podłączenia końcówki kabla światłowodowego do testera i wciśnięcia jednego przycisku. VisiFault emituje jasny promień światła czerwonego łatwo widoczny z daleka. Po podłączeniu jednego końca światłowodu możemy łatwo zlokalizować drugi koniec, nawet jeżeli jest to jedno z wielu włókien światłowodu. Bardziej wszechstronnym testerem jednomodowych przewodów światłowodowych jest Fiber OneShot™ PRO firmy Fluke Networks.

Rys. 4.6. Fiber OneShot™ PRO firmy Fluke Networks [4].

Urządzenie potrafi analizować łącza światłowodowe na długości 23 km w czasie krótszym niż 5 sekund. Proces testowania uruchamiany jest jednym przyciskiem a wyniki testów zapisywane są w pamięci urządzenia. Tester pozwala znaleźć źródła błędów spowodowane przez czołowe zanieczyszczenia lub źle wykonane połączenia światłowodów. Najbardziej wszechstronnym urządzeniem testującym i rozwią-zującym problemy z łączami optycznymi jest OptiFiber® OTDR. Wykorzystując to urządzenie inżynierowie sieciowi mają możliwość wykonywania kontroli, weryfikacji, certyfikacji, szybkiego lokalizowania i eliminowania problemów ze światłowodami oraz dokumentowania okablowania optycznego.

Rys. 4.7. OptiFiber® OTDR firmy Fluke Networks [4].

Mówiąc o urządzeniach wspomagających rozwiązywanie problemów z sieciami teleinformatycznymi nie można pominąć coraz częściej obecnych dzisiaj sieci bezprzewodowych i dedykowanych dla nich testerach. Przykładem urządzenia do przeprowadzania testów poprawności działania sieci bezprzewodowych jest kolejny miernik firmy Fluke Networks o nazwie AirCheck Wi-Fi tester. Tester sieci bezprzewodowych AirCheck potrafi szybko diagnozować i pomagać w rozwiązywaniu problemów z sieciami standardu 801.11 a/b/g/n. Procedura testowa uruchamiana jest jednym przyciskiem, a rezultatem są raporty generowane na wyświetlaczu urządzenia.

Rys. 4.8. AirCheck Wi-Fi tester firmy Fluke Networks [4].

Główne funkcje urządzenia to:

- Szybki test poprawności działania sieci bezprzewodowych i ich współdziałania z kablowymi sieciami teleinformatycznymi;
- Identyfikacja poziomu zabezpieczeń dla sieci otwartych, WEP, WPA, WPA2 oraz pozostałych 802.1x;
- Diagnostyka obciążenia każdego kanału AP przez odbywający się ruch w sieci bezprzewodowej;
- Wykrywanie fałszywych Access Point z wykorzystaniem dodatkowej anteny kierunkowej;
- Sprawdza zasięg, zakłócenia, bezpieczeństwo i możliwość podłączenia do określonych sieci;
- Zbieranie szczegółowych informacji o sieciach bezprzewodowych;
- Lokalizowanie AP i klientów sieci na podstawie poziomu sygnału;
- Szybka identyfikacja problemów z AP na podstawie zebranych szczegółowych informacji, takich jak: poziomy Sygnał/szum/sygnał-szum (aktualna i maksymalna), identyfikatory SSID i BSSID, stan ACL, Bezpieczeństwo/Szyfrowanie, podłączeni klienci;
- Testy połączeń i sprawdzanie dostępności sieci;
- Użycie poszczególnych kanałów;

- Szybkie znajdowanie źle skonfigurowanych klientów AP;
- Szerokie raportowanie wykonanych badań.

Dzięki szerokim możliwością urządzenie staje się bardzo pomocne przy diagnozowaniu problemów z teleinformatycznymi sieciami bezprzewodowymi.

Kolejną grupą urządzeń wspomagających wykrywanie niesprawności sieci są analizatory kabli. Są to wielofunkcyjne niewielkie urządzenia służące do testowania i zatwierdzania kabli miedzianych oraz optycznych w różnych usługach i standardach. Bardziej zaawansowane narzędzia zawierają programy diagnostyczne, które potrafią zmierzyć odległość do miejsca spadku wydajności, podpowiedzieć działania naprawcze i graficznie zaprezentować informacje o przesłuchach i impedancji. Zazwyczaj do analizatorów kabli dołączone jest oprogramowanie PC pozwalające przesyłać dane z urządzenia do komputera PC i raportować wykonane testy. Przykładem takiego analizatora jest Fluke Networks DTX CableAnalyzer.

Rys. 4.9. DTX Cable Analyzer firmy Fluke Networks [4].

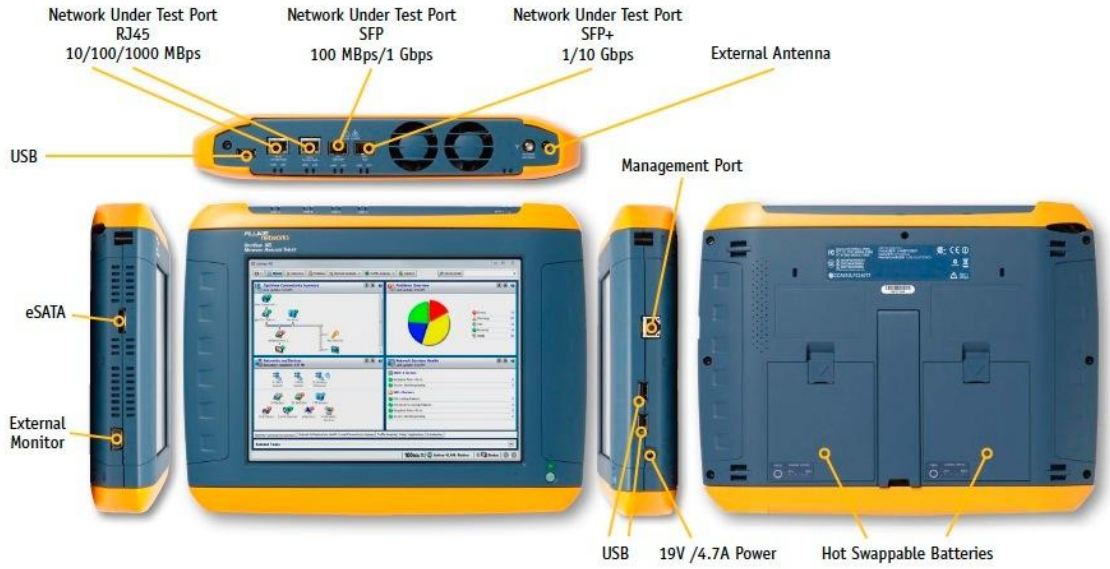
Następną kategorią urządzeń są moduły analizowania sieci NAM firmy CISCO, które można instalować w przełącznikach serii Catalyst 6500 i routerach serii 7600. Moduł pozwala na uzyskanie graficznej prezentacji ruchu z lokalnych oraz zdalnych przełączników i routerów, która jest prezentowana administratorowi z poziomu przeglądarki internetowej. Moduł generuje raporty na temat ruchu pochłaniającego krytyczne zasoby sieciowe, potrafi przechwytywać i dekodować pakiety oraz śledzić czasy odpowiedzi, aby móc zlokalizować problem z aplikacją w danej sieci albo na serwerze.

Rys. 4.10. Moduły NAM dla przełączników i routerów CISCO [5].

Moduły te są instalowane w urządzeniach stanowiących newralgiczne węzły danej sieci, co w przypadku awarii pozwala zawęzić obszar poszukiwań problemu z siecią.

Ostatnią z wymienionych kategorii urządzeń a zarazem najbardziej rozbudowaną są przenośne analizatory sieci. Są to kompleksowe rozwiązania do identyfikacji i rozwiązywania problemów sieciowych w całym obszarze modelu ISO/OSI. Te niestandardowe urządzenia ułatwiają rozwiązywanie problemów w terenowych sieciach przełączanych i VLAN. Podłączając analizator sieci w dowolnym miejscu sieci możemy w czasie rzeczywistym zbierać dane dotyczące średniego i szczytowego ruchu danych na

określonym porcie. Analizator można również wykorzystać do wykrywania konfiguracji sieci VLAN, wykrywania urządzeń generujących największy ruch w sieci, analizy ruchu w sieci oraz przeglądania szczegółowych informacji o interfejsie. Uzyskane dane można przesyłać do komputera PC a następnie analizować i wykorzystywać przy rozwiązywaniu problemów. Przykładem takiego urządzenia jest nowoczesny wielofunkcyjny analizator sieci OptiView® XG Network Analysis Tablet firmy Fluke Networks. Analizator pozwala na szybkie diagnozowanie anomalii pracy przełączników, routerów jak również urządzeń bezprzewodowych.



Rys. 4.11. OptiView® XG Network Analysis Tablet firmy Fluke Networks [4].

Główne funkcje analizatora:

- Możliwość dowolnej konfiguracji pulpitów, co pozwala na przeglądanie aktualnego statusu sieci, krytycznych wskaźników z pracy routerów, przełączników, firewalli, serwerów, usług, aplikacji i innych urządzeń sieciowych;
- Możliwość śledzenia stanu wybranego fragmentu sieci;
- Raportowanie problemów sieci i działających w niej aplikacji;
- Szczegółowa analiza ruchu w sieci i badanie wpływu ruchu na wydajność sieci;
- Automatyczne wyszukiwanie błędów w infrastrukturze sieciowej (np.: problemy z wydajnością, powielane adresy IP, nieprawidłowe maski podsieci, brak odpowiedzi routerów, itp.);
- Centrum wsparcia pomagające w identyfikacji i usunięciu problemu sieciowego;
- Analiza infrastruktury aplikacji sieciowych;
- Pełna analiza VLAN i łącz trunkowych;
- Analiza łączy o przepustowości ponad 10 Gb/s;
- Analiza NetFlow w czasie rzeczywistym.

Szeroka funkcjonalność analizatora sieciowego pozwala na sprawniejsze rozwiązywanie problemów z sieciami teleinformatycznymi.

Wymienione tu narzędzia są tylko pomocą dla inżynierów sieciowych, aby rozwiązywanie problemów z sieciami przebiegało sprawniej i znacznie krótszym czasie, co z kolei zaowocuje mniejszymi przerwami w poprawnej pracy sieci teleinformatycznych.

PODSUMOWANIE

Sieci teleinformatyczne odgrywają dzisiaj znaczącą rolę w naszym codziennym życiu, dlatego ich sprawne funkcjonowanie jest bardzo ważne. Stąd też kluczową rolę odgrywają administratorzy i inżynierowie sieciowi potrafiący szybko i sprawnie diagnozować problemy z sieciami, wykrywać występujące niesprawności, awarie czy problemy z wydajnością sieci teleinformatycznych. Bardzo ważnym aspektem przy zarządzaniu mniej lub bardziej rozległymi sieciami jest odpowiednie przygotowanie merytoryczne. Na skuteczność i szybkość wykrywania niesprawności sieci wpływają następujące elementy:

- Wybrana metoda analizy problemu sieciowego w zależności od złożoności sieci, złożoności problemu oszacowanego na podstawie zebranych danych o awarii oraz priorytetu ustalonego dla awarii;
- Wiedza posiadana na temat zarządzanej sieci bądź jej fragmentu oraz problemów jakie mogą jej dotyczyć;
- Przygotowana wcześniej dokumentacja techniczna sieci, schematy fizycznej infrastruktury sieci jak i logiczny schemat konfiguracji urządzeń i sieci;
- Posiadane narzędzia wspomagające wykrywanie awarii, takich jak: niesprawności fizycznych nośników danych, zakłóceń przemysłowych, niesprawności procesów komunikacyjnych (przekłamania transmisji danych, niedziałających protokołach routingu, problemach z przeciążeniami sieci) czy w końcu błędnej konfiguracji urządzeń sieciowych bądź końcowych hostów i serwerów;
- Doświadczenie administratora lub inżyniera sieciowego pozwalająca wstępnie oszacować skalę problemu.

Dzisiaj dostępne jest wiele narzędzi, które pozwalają precyzyjnie zdefiniować problem sieciowy. Przykłady większości z nich zostały przedstawione w poprzednich rozdziałach niniejszej pracy. Niektóre z nich oprócz analizy podpowiadają inżynierowi możliwe rozwiązania zaistniałego problemu. Metody i środki należy dobierać w zależności od skali problemu sieciowego i jego skutków ekonomicznych. Nie uzasadnionym jest stosowanie bardzo drogich analizatorów sieciowych w małych firmach, gdzie administrowana sieć skupia kilkanaście hostów i kila serwerów usług. Inaczej jest w dużych korporacjach, serwerowniach czy dostawcach usług sieciowych, gdzie awaria sieci powoduje odcięcie od zasobów i usług tysiące hostów i serwerów, w szczególności dużych firm które wymiernie wykorzystują do swojego funkcjonowania sieci teleinformatyczne. W takim przypadku liczy się czas usunięcia problemu, gdyż ma to wymierny skutek ekonomiczny.

BIBLIOGRAFIA

[1] M. A. Dye, R. McDonald, A. W. Rufi, Akademia sieci Cisco CCNA Exploration Semestr 4 – Sieci WAN – zasady dostępu, Wydawnictwo Naukowe PWN, Warszawa, 2011

[2] M. A. Dye, R. McDonald, R. W. Rufi, Akademia sieci Cisco CCNA Exploration Semestr 1 – Podstawy sieci, Wydawnictwo Naukowe PWN, Warszawa, 2011

[3] Serwis www: http://www.whatsupgold.com/products/whatsup-gold-core/

[4] Serwis www: http://www.flukenetworks.com

[5] Serwis www: http://www.cisco.com/web/learning/netacad/