Sieci komputerowe – Laboratorium
Ćwiczenie 6

Cel ćwiczenia.

Celem ćwiczenia jest zapoznanie się zasadą działania i obsługą programowego analizatora sieci lokalnych Anasil.

1.2 Wprowadzenie.

Anasil jest aplikacją stworzoną przez katowicką firmę **LF Networks,** programowym analizatorem sieci lokalnych oraz dekoderem protokołów, działającym w sieciach zbudowanych w oparciu o łącza klasy Ethernet. Dzięki swej niebywałej elastyczności jest narzędziem o bardzo szerokich zastosowaniach: od diagnostyki sieci, poprzez monitorowanie krytycznych parametrów, wykrywanie nieautoryzowanego dostępu do łącza, sporządzanie remanentu aż po pomoc we wszelkich projektach informatycznych w jakikolwiek sposób dotykających problematyki sieci lokalnych.

Jest to program adresowany głównie do:

1. **Administratorów sieci lokalnych** - opcje badania rozkładu obciążenia pomogą im znaleźć stacje generujące największy ruch w sieci a testy point-to-point wykryć uszkodzone stacje. Profil sieci i wykrywanie nowych stacji pozwolą na łatwe zauważenie intruzów wpinających się w łącze. Dodatkowo profil sieci ułatwi przeprowadzenie remanentu.

2. **Programistów pracujących w środowisku sieciowym** - przechwytywanie i analiza pakietów które są nieocenionym narzędziem do testowania komunikacji pomiędzy programami działającymi na różnych komputerach. Programowalny dekoder protokołów pozwoli na łatwe stworzenie dekoderów własnych protokołów komunikacyjnych. ANASIL zapewnia też wgląd w status adapterów NetBIOS na zdalnych końcówkach.

3. **Instalatorów i serwisantów sieci i serwerów** - dekoder protokołów i przechwytywanie ramek umożliwią im wykrycie i usunięcie problemów konfiguracyjnych a testy point-to-point pomogą sprawdzić jakość zainstalowanej sieci.

Pomimo faktu, że ANASIL działa w systemie Windows 95/98/NT, analizy przez niego wykonywane nie ograniczają się do systemów firmy Microsoft. ANASIL analizuje również sieciową aktywność systemów spod znaku UNIX'a, Novell'a czy Apple.

1.3 Sposób działania

Do kontaktu z siecią ANASIL używa specjalizowanego drivera. Driver ten umożliwia odbiór wszystkich ramek transmitowanych w sieci. Umożliwia też wysyłanie niestandardowych ramek. Z jego pomocą ANASIL jest w stanie odebrać i zanalizować ruch w całym segmencie sieci Ethernet (w tzw. *domenie kolizji*, czyli w jednym odcinku kabla lub w paru odcinkach połączonych przy pomocy *repeaterów*). Przez *ruch* rozumiemy tutaj ramki WSZYSTKICH typów oraz WSZYSTKICH protokołów sieciowych. Pole "widzenia" ANASILA kończy się jednakże na najbliższym *routerze* lub innym urządzeniu filtrującym pakiety (np. *switch, hub*).

Odebrane ramki ANASIL analizuje i na podstawie tych analiz uaktualnia prowadzone przez siebie **statystyki.** Statystyki te dotyczą zarówno parametrów globalnych całego segmentu sieci (np. wykorzystanie czy sumaryczna liczba przetransmitowanych przez segment ramek) jak i poszczególnych stacji lub protokołów sieciowych.

Odebrane ramki (lub ich podzbiór określony przez **filtr**) mogą być również zapamiętywane w specjalnym buforze a następnie przeglądane w postaci zrozumiałej dla człowieka przy pomocy **dekodera protokołów**).

Statystyki mogą być wizualizowane na różne sposoby oraz eksportowane przy pomocy **viewerów i form.** Dzięki temu możliwe jest śledzenie tylko tych statystyk na których nam w danej chwili najbardziej zależy. Wybrany zbiór statystyk można **eksportować** z zadanym interwałem do pliku o specjalnym, skompresowanym formacie. Z plików takich można następnie przygotowywać różnego rodzaju **raporty.**

Podstawowe możliwości ANASILa to:

- Pomiary obciążenia łącza, globalne i w rozbiciu na rożne typy adresowania ramek (broadcast'y i multicast'y)
- Pomiary aktywności poszczególnych komputerów w sieci (liczba ramek wysłanych / odebranych)
- Pomiary aktywności połączeń pomiędzy komputerami (liczba ramek przesłanych pomiędzy dwoma komputerami, procentowy udział tych transmisji w obciążeniu łącza)
- Lista i statystyki protokołów sieciowych
- Zdalne sprawdzanie statusów adapterów NetBIOS (oraz nazw NetBIOS) we wszystkich komputerach sieci. Sprawdzane są adaptery działające przy pomocy różnych protokołów transportowych (IPX,TCP/IP oraz NetBEUI).
- Zdalne sprawdzanie do jakich serwerów NetWare zalogowany jest użytkownik na danej stacji.
- Głębsza analiza protokołów: IP, IPX, Appletalk oraz NetBEUI (NBF)
- Globalne filtrowanie i zliczanie przefiltrowanych ramek.
- Przechwytywanie i analiza przechwyconych ramek (packet capture) przy pomocy programowalnego dekodera protokołów. Napisanie dekodera dla własnego protokołu wymaga tylko edytora ASCII. Przechwycone ramki można przeglądać, filtrować oraz zachować do późniejszej analizy albo w formacie binarnym albo w pliku TXT.
- System wizualizacji zbieranych statystyk, pozwalający użytkownikowi na wyświetlenie danych w dogodnej dla niego postaci. Statystyki mogą być prezentowane jako tabele, pojedyncze okienka zawierające tekst, grupy statystyk lub histogramy. Dla wartości numerycznych można dokonywać uśrednień, prezentować tylko maksima lub minima tudzież określać zakresy wartości, po wejściu w które generowany jest komunikat lub zmienia się kolor okna.
- Testy point-to-point dla protokołów IPX, IP, Appletalk oraz NBF. Dla wybranych stacji określany jest minimalny/średni/maksymalny czas odpowiedzi (round-trip) oraz procentowa strata pakietów.
- Eksport danych do clipboardu, pliku TXT (np. dla arkuszy kalkulacyjnych) oraz stron HTML
- Automatyczne tworzenie *profilu sieci*, czyli listy aktywnych stacji. Automatyczne przypisywanie nazw mnemonicznych w oparciu o protokoły DNS, SAP, NBP oraz usługi sieci Microsoft Networking. Stacje nie ujęte w profilu są traktowane jako nieautoryzowane i odpowiednio zaznaczane.
- Podczas tworzenia profilu system próbuje również zidentyfikować system operacyjny każdego komputera.
- Log systemowy z informacjami o przekroczeniu zadanych parametrów.
- Sortowanie tabel po dowolnie wybranej kolumnie.

odbiór wszystkich ramek transmitowanych w sieci. Umożliwia też wysyłanie niestandardowych ramek.

Z jego pomocą ANASIL jest w stanie odebrać i zanalizować ruch w całym segmencie sieci Ethernet (w jednym odcinku kabla lub w paru odcinkach połączonych przy pomocy *repeaterów*). Przez *ruch* rozumiemy tutaj ramki WSZYSTKICH typów oraz WSZYSTKICH protokołów sieciowych. Pole "widzenia" ANASILA kończy się jednakże na najbliższym *routerze* lub innym urządzeniu filtrującym pakiety (np. *switching hub*).
Odebrane ramki ANASIL analizuje i na podstawie tych analiz uaktualnia prowadzone przez siebie statystyki. Statystyki te dotyczą zarówno parametrów globalnych całego segmentu sieci (np. wykorzystanie czy sumaryczna liczba przetransmitowanych przez segment ramek) jak i poszczególnych stacji lub protokołów sieciowych.
Odebrane ramki (lub ich podzbiór określony przez filtr) mogą być również zapamiętywane w specjalnym buforze a następnie przeglądane w postaci zrozumiałej dla człowieka przy pomocy dekodera protokołów).
Statystyki mogą być wizualizowane na różne sposoby oraz eksportowane przy pomocy viewerów i form. Dzięki temu możliwe jest śledzenie tylko tych statystyk na których nam w danej chwili najbardziej zależy.

Dla lepszego zrozumienia możliwości ANASILA konieczne jest poznanie i przyswojenie pewnych pojęć, które pomogą lepiej zrozumieć budowę i działanie Anasila. Są to:

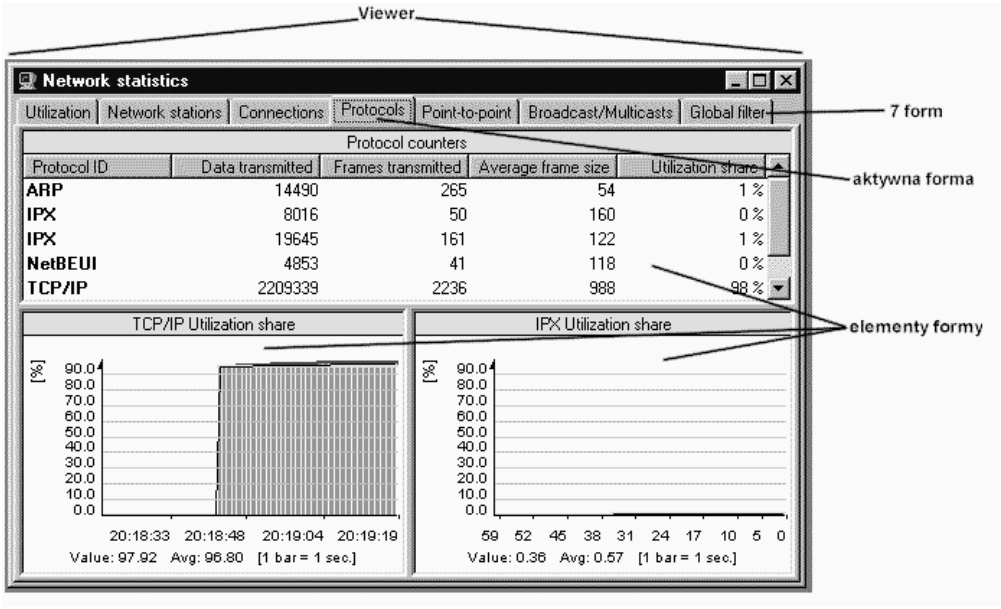
Profil sieci

Dla każdej analizowanej sieci można (i powinno się) zbudować profil sieci. Profil przechowuje dodatkowe informacje o adresach kart sieciowych (MAC) spotykanych w sieci. Każdemu adresowi można w profilu przyporządkować mnemoniczną nazwę, adresy protokołów sieciowych oraz szereg innych przydatnych informacji np. rodzaj i wersję systemu operacyjnego działającego na opisywanej stacji. Profil sieci ma szereg zastosowań. Przede wszystkim pozwala ANASILowi stosować czytelne dla człowieka nazwy mnemoniczne zamiast adresów MAC. Może służyć jako narzędzie wspomagające sporządzanie remanentu. A dodatkowo wspomaga wykrywanie nielegalnie podłączonych do sieci komputerów, które są identyfikowane jako nie należące do profilu i odpowiednio zaznaczane.
Profil sieci można utworzyć ręcznie (wpisując poszczególne stacje) lub automatycznie za pomocą opcji zbierania informacji o sieci.

Viewery i formy

Viewery i formy są podstawowymi mechanizmami wizualizacji statystyk w ANASILu. *Viewer* jest oknem, które może zawierać jedną lub więcej *form*. Forma z kolei jest oknem zawierającym jeden lub więcej *element*. *Element* zaś wizualizuje już konkretne, wybrane przez użytkownika statystyki z **bazy statystyk.**

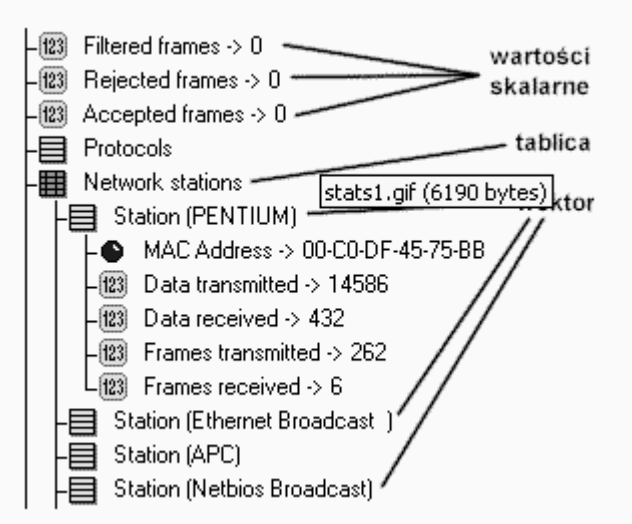
Cały ten (dość skomplikowany) układ ilustruje poniższy rysunek:



Baza statystyk

Wszystkie zbierane przez ANASILa informacje na temat ruchu w sieci są zapisywane w bazie statystyk. Baza ta jest tworzona i aktualizowana "w tle" działania programu. Informacje tam zapisane są wizualizowane przez viewery i formy. W ANASILu zastosowano zalecany przez podręczniki projektowania obiektowego rozdział pomiędzy danymi a ich zewnętrzną, widoczną dla użytkownika reprezentacją. W efekcie dane zbierane w bazie statystyk mogą być wizualizowane na szereg sposobów, zależnie od potrzeb użytkownika.

Elementami tej bazy mogą być wartości skalarne, wektory wartości skalarnych oraz tablice wartości skalarnych:



Wartości skalarne mogą być numeryczne lub nienumeryczne. Na wartościach numerycznych **viewery i formy** mogą wykonywać pewne dodatkowe działania (np. obliczanie maksimum, minimum czy średniej). Wartości nienumeryczne mogą być tylko wizualizowane w sposób bezpośredni.

Każda wartość jest pewnego **typu**. Typ wartości określa dostępne sposoby jej wyświetlania oraz sortowania.

Z bazy statystyk korzystają przede wszystkim **viewery i formy** , których zadaniem jest wizualizować je w postaci dogodnej dla użytkownika.

Szablony form

Wizualizacja szczegółowych danych dotyczących np. stacji sieciowych wymaga czasami skonstruowania identycznych lub bardzo podobnych form dla każdej z obserwowanych stacji. Aby uprościć to zadanie, ANASIL udostępnia możliwość zachowania formy na dysku jako szablonu. Szablon ten można później automatycznie otworzyć jako formę z zadaną np. stacją lub innym elementem tablicy (patrz Opcja "View row with template").

Filtry

Filtry służą do nakładania warunków na analizowane przez ANASILa ramki. Można w ten sposób ograniczyć liczbę ramek łapanych przez ANASILa do bufora, filtrować zawartość samego bufora lub badać liczbę ramek które spełniają kryteria filtra (patrz Opcja "Set-up global filter").

Testy point-to-point

W czasie testów point-to-point badana jest komunikacja pomiędzy komputerem, na którym działa ANASIL a grupą stacji. Komunikacja może odbywać się za pomocą jednego z czterech głównych protokołów sieciowych: IP, IPX, NetBEUI lub Appletalk. W czasie tych testów mierzone są czasy odpowiedzi stacji oraz procentowa "stratność pakietów". Na tej podstawie można określić stan łącza, karty sieciowej (czy np nie "śmieci") a także sprawdzić czy w/w protokoły są poprawnie skonfigurowane.

Bufor i dekoder protokołów

Dogłębna analiza problemów np. konfiguracyjnych, wymaga niekiedy bliższego przyjrzenia się zawartości transmitowanych ramek. ANASIL potrafi złapać część lub całość transmitowanych ramek do tzw. *bufora*. Złapane w ten sposób ramki mogą być następnie wizualizowane przy pomocy *dekodera protokołów*, tłumaczącego ramkę z postaci binarnej do zrozumiałej dla człowieka. Dekoder protokołów w ANASILu jest *programowalny*. Znaczy to, że każdy użytkownik może w języku opisu protokołów zbudować własny dekoder dla np. pisanego przez siebie protokołu.

czyli ANASIL Desktop Agent)

Aby umożliwić programowi dokonywanie bardziej dogłębnych analiz konfiguracji stacji, konieczne okazało się zaimplementowanie części funkcji analizujących na stacjach w sieci. ANASIL Desktop Agent jest niewielkim programem rezydentnym, uruchamianym automatycznie przy starcie systemu, który komunikując się z ANASILem jest w stanie dostarczyć mu szczegółowych informacji na temat konfiguracji stacji, statystyk błędów transmisji, ilości wolnego miejsca na dyskach, otwartych portach TCP/UDP i inne. Agenci umożliwiają również podgląd ekranu oraz udostępniają statystyki wykorzystania aplikacji na danej końcówce. Poza tym, przy pomocy mechanizmu **Wake-up-on-LAN** można zdalnie zgasić lub zrestartować komputer.

(ang. terminate and stay resident) to program komputerowy, który pozostaje w pamięci operacyjnej po załadowaniu w postaci jawnej lub ukrytej. Programy rezydentne mogą być wielokrotnie ponownie uaktywnione albo przez kombinację naciśniętych klawiszy, albo przez urządzenie peryferyjne. Typowym programem rezydentnym jest Zegarek systemu operacyjnego Microsoft Windows 3.x.

Dzięki ANASIL Desktop Agent, jest możliwe:

- Zdalne wyłączanie i restartowanie stacji
- Zbieranie statystyk na temat błędów transmisji popełnionych przez poszczególne adaptery sieciowe stacji.
- Zbieranie informacji o aktualnie otwartych portach TCP/UDP
- Zbieranie informacji o statusie urządzeń (Windows 95/98) lub serwisów (Windows NT)
- Zbieranie informacji o konfiguracji stacji
- Zbieranie informacji o liczbie dysków i o ilości wolnego miejsca na nich
- Przesyłanie do użytkownika komunikatów
- Pobieranie szczegółowych informacji o konfiguracji adapterów, protokołów i klientów sieci.
- Podglądanie ekranu stacji (w trybie thumbnail i pełnoekranowym)
- Zbieranie informacji na temat aplikacji używanych na danej stacji i ich wykorzystaniu.

Hierarchiczna baza statystyk składa się z kilku głównych części. Są to:

1. **Statystyki globalne** - są to statystyki zbierane dla całej analizowanej podsieci.
2. **Statystyki stacji sieciowych** - są to statystyki dotyczące każdej ze stacji sieciowych, zorganizowane w postaci tablicy statystyk.
3. **Statystyki protokołów** - są to statystyki dotyczące udziału protokołów sieciowych w wypełnieniu łącza, zorganizowane w postaci tablicy statystyk.
4. **Statystyki połączeń** - są to statystyki dotyczące ruchu generowanego poprzez połączenia pomiędzy konkretnymi stacjami, zorganizowane w postaci tablicy statystyk.
5. **Statystyki testów point-to-point** - są to statystyki przechowujące wyniki testów point-to-point.

ANASIL jest narzędziem niezwykle elastycznym pod względem sposobu oraz rodzajów prezentowanych statystyk. Użytkownik ma możliwość samodzielnego określenia, które informacje mają być prezentowane oraz w jaki sposób.

- ANASIL dzięki "agentom" (Anasil Desktop Agent) udostępnia statystyki wykorzystania aplikacji na wybranych stacjach. Dzięki temu narzędziu wiadomo kto i jak długo pracował, a jak długo zajmował się innymi sprawami.
- ANASIL tworzy profil sieci, w którym zapisuje listę stacji w sieci. Dzięki mechanizmowi AUTOMATYCZNEGO uaktualniania listy dołączonych urządzeń, ANASIL sygnalizuje każdy nieautoryzowany dostęp.
- ANASIL dzięki wbudowanemu, programowalnemu dekoderowi ramek potrafi przechwycić wszystkie lub wybrane ramki oraz pokazać ich zawartość.

  ANASIL za pomocą "agentów" (Anasil Desktop Agent) umożliwia podgląd ekranu wybranych stacji, a także dzięki mechanizmowi Wake Up On-LAN pozwala na zdalne wyłączanie i restartowanie wybranych komputerów.
- ANASIL potrafi gromadzić wybrane przez użytkownika statystyki automatycznie i na ich podstawie generować RAPORTY. Dzięki temu narzędziu nawet po okresie nieobecności można dowiedzieć się co działo się w twojej sieci.

  Ponadto, w przypadku przekroczenia zadanych parametrów, użytkownik może być o tym fakcie powiadomiony e-mailem (SMS-em).