

Studia stacjonarne
Kierunek: Inżynieria Biomedyczna

Instrukcja do zajęć laboratoryjnych z przedmiotu

Telematyka medyczna

Kod przedmiotu: MKIB2S01005M

Ćwiczenie 3: Narzędzia sieciowe w systemie Windows

Opracował: dr inż. **Andrzej Zankiewicz**

1. Ogólna charakterystyka ćwiczenia

Praktycznie każdy ze współcześnie używanych systemów operacyjnych posiada możliwość pracy w środowisku sieciowym (ang. *networking*) i jest wyposażony w szereg narzędzi umożliwiających konfigurowanie, diagnozowanie i nadzorowanie danego urządzenia w zakresie jego współpracy z siecią. Oprócz narzędzi zawartych w systemie operacyjnym dostępnych jest też zazwyczaj wiele dodatkowych programów rozszerzających zakres funkcji udostępnianych przez narzędzia systemowe.

Obecnie jednym z najszerszej używanych systemów operacyjnych przeznaczonych dla komputerów PC i serwerów jest system *Windows* firmy Microsoft. Wraz z tym systemem dostarczanych jest wiele programów narzędziowych służących do rozwiązywania problemów z siecią. W większości przypadków są to narzędzia pracujące w trybie tekstowym (uruchamianie z wiersza poleceń) i będące odpowiednikami analogicznych programów zawartych w systemie *UNIX*.

Celem niniejszego ćwiczenia jest ugruntowanie posiadanych wiadomości z zakresu konfigurowania usług sieciowych w systemie Windows 2000 oraz poznanie sieciowych programów narzędziowych zawartych w tym systemie, a także programów typu „analizator protokołów” stanowiących jedno z podstawowych narzędzi do obserwacji i analizy ruchu sieciowego.

Wiadomości i umiejętności uzyskane w trakcie wykonywania tego ćwiczenia będą stanowiły niezbędną podstawę do kolejnych ćwiczeń z przedmiotu „Systemy i sieci telekomunikacyjne”.

2. Przygotowanie do zajęć

Przed przystąpieniem do wykonywania ćwiczenia należy zapoznać się z następującymi materiałami:

- Całość niniejszej instrukcji
- Informacje o narzędziach sieciowych używanych w ćwiczeniu z dowolnego podręcznika dotyczącego sieci TCP/IP (np. w [1] odpowiednie fragmenty rozdziałów 2, 3, 4, 5)
- Dokumentacja programu *Wireshark*

Informacje zawarte w podanych powyżej źródłach stanowią minimum wiedzy teoretycznej **niezbędnej** do przystąpienia i prawidłowego wykonania ćwiczenia.

3. Podstawowe informacje o używanych w ćwiczeniu narzędziach

1. Polecenie `ipconfig`

Umożliwia ono wyświetlenie informacji o konfiguracji protokołów TCP/IP oraz interfejsu sieciowego (karty sieciowej), a także odświeżenie parametrów

przypisywanych stacji sieciowej dynamicznie. W systemach Windows 95 i Windows 98 narzędzie to nosi nazwę `wiipcfg` i pracuje w oknie graficznym.

2. Polecenie ping

Służy do testowania połączenia między stacjami na poziomie protokołu IP (warstwa 3 modelu OSI) poprzez wykorzystanie komunikatów *echo request* i *echo replay* protokołu ICMP.

3. Polecenie tracert

Umożliwia ono realizację procedury *traceroute* służącej do określenia trasy (w sensie kolejnych węzłów sieci IP) pomiędzy stacją na której wykonano to polecenie, a stacją której nazwa domenowa lub adres IP zostały podane jako parametr polecenia `tracert`.

4. Polecenie netstat

Umożliwia wyświetlenie bieżących połączeń TCP/IP stacji oraz statystyk ruchu protokołów TCP/IP.

5. Polecenie arp

Służy do wyświetlenia zawartości pamięci podręcznej protokołu ARP zawierającej pary adresów logicznych (numerów IP) stacji przyłączonych do danej sieci lokalnej oraz ich adresów fizycznych (MAC). Umożliwia też usuwanie wpisów z tej pamięci oraz ręczne dokonywanie wpisów statycznych.

6. Polecenie nslookup

Służy do testowania systemu obsługi nazw domenowych (DNS). Jest to dość rozbudowany program będący przedmiotem jednego z następnych ćwiczeń.

7. Programowy analizator protokołów (Wireshark)

Jest to jedna z wielu aplikacji umożliwiających realizację funkcji programowego analizatora protokołów. Podstawą ich działania jest możliwość przełączenia karty sieciowej w tryb, w którym odbiera ona wszystkie ramki przesyłane w dołączonym do karty medium transmisyjnym (w normalnym trybie karta przyjmuje tylko ramki z jej adresem fizycznym MAC oraz ramki z adresem rozgłoszeniowym). Tryb ten określany jest mianem *promiscuous mode*.

Jedną z ważniejszych funkcji tego programu jest rejestracja ramek przesyłanych w przyłączonym do karty medium oraz dekodowanie i przedstawianie w czytelnej postaci informacji przesyłanych w tych ramkach. Ważną cechą jest też możliwość określenia warunków (filtrów) jakie muszą spełnić ramki aby były rejestrowane. Dzięki temu można wyodrębnić wśród przesyłanych informacji tylko te, które z określonych względów nas interesują. Na podstawie odebranych ramek tworzone są też statystyki ruchu w przyłączonym medium.

4. Plan wykonywania ćwiczenia laboratoryjnego

Informacje pomocnicze

Komendy systemu operacyjnego takie jak *ipconfig*, czy *ping* wygodnie jest wykonywać w osobno otwartym oknie linii komend. Okno takie można otworzyć wybierając ikonę *Start*, a następnie opcję *Uruchom* i wpisując *cmd*.

Zawartość okna komend można skopiować do schowka systemowego w postaci tekstowej. W tym celu należy ustawić kursor myszy w obrębie okna linii komend, wyświetlić prawym klawiszem myszy menu kontekstowe i z tego menu wybrać opcję *Oznacz*. Następnie za pomocą myszy, przytrzymując wciśnięty lewy przycisk, zaznaczyć tekst do skopiowania i po zwolnieniu lewego przycisku myszy nacisnąć klawisz *Enter*. Wówczas zaznaczony tekst zostanie skopiowany do schowka systemowego i może być wklejony do dowolnego dokumentu (np. w *Notatniku*).

Wykonanie ćwiczenia

1. Uruchomić wiersz poleceń systemu Windows 2000.
2. Zapoznać się z opcjami dostępnymi w oknie konfiguracji sieci systemu Windows 2000 (właściwości połączenia sieciowego). Odczytać adresy fizyczne (MAC) oraz logiczne (IP) danej stacji.

Adres fizyczny (MAC) danego interfejsu sieciowego może być odczytany następującymi sposobami:

- poprzez wykonanie polecenia `ipconfig` z opcją `/all`
- poprzez wybranie karty właściwości danego interfejsu i wskazanie na niej kursorem myszy nazwy interfejsu (pole *Połącz używając*)

Adres logiczny (IP) przypisany do danego interfejsu sieciowego może być odczytany następującymi metodami:

- jeżeli dany interfejs jest aktywny jego adres IP wyświetlany jest po wykonaniu komendy `ipconfig`
- poprzez wybranie karty właściwości danego interfejsu, a następnie wyświetlenie właściwości składnika *Protokół internetowy (TCP/IP)*

Uwaga: Jeżeli adres IP jest przypisany w sposób dynamiczny (poprzez protokół DHCP), to może on być wyświetlony tylko pierwszą z wymienionych powyżej metod.

3. Sprawdzić listę dostępnych opcji w poleceniu `ping` (`ping /?`). Wykonać polecenie `ping` do wskazanego przez prowadzącego hosta i zarejestrować otrzymane wyniki. Sprawdzić i opisać działanie następujących opcji polecenia *ping*:
 - `-t` - ciągłe odpytywanie określonego hosta
 - `-l` - określenie rozmiaru wysyłanych pakietów
 - `-n` - określenie liczby wysyłanych powtórzeń
 - `-a` - wykonanie tłumaczenia numeru IP na nazwę hosta (opcja istotna tylko w przypadku podania numeru IP jako argumentu polecenia *ping*)

4. Sprawdzić listę dostępnych opcji w poleceniu `tracert` (`tracert /?`). Wykonać polecenie `tracert` do wskazanego przez prowadzącego hosta i zarejestrować otrzymane wyniki. Sprawdzić i opisać działanie następujących opcji polecenia `tracert`:

- -d - wyłączenie rozpoznawania nazw hostów znajdujących się na wyznaczonej ścieżce
- -h - określenie maksymalnej liczby przeskoków na wyznaczonej ścieżce

5. Sprawdzić listę dostępnych opcji w poleceniu `netstat` (`netstat /?`). Zarejestrować i skomentować informacje zwracane przez program `netstat` z następującymi opcjami:

- -a – wyświetlenie oprócz nawiązanych połączeń także portów TCP i UDP znajdujących się w stanie oczekiwania
- -n – wyłączenie rozpoznawania nazw hostów i portów
- -e – wyświetlenie statystyk interfejsu Ethernet

6. Sprawdzić listę dostępnych opcji w poleceniu `arp` (`arp /?`). Wyświetlić i zarejestrować tablicę ARP używanej stacji sieciowej (`arp -a`). Wykonać komendę `ping` do jednego z komputerów w sieci lokalnej i ponownie wyświetlić tablicę ARP. Ponawiając cyklicznie wyświetlanie tablicy ARP określić czas po jakim usuwane są z niej wpisy dynamiczne.

7. Uruchomić program *Wireshark*. Zapoznać się ze strukturą okna programu i rodzajem wyświetlanych informacji. Posługując się programem *Wireshark* wykonać następujące operacje:

- wypróbować działanie funkcji rejestracji ramek
- wykonać zapis zawartości zarejestrowanych ramek do pliku tekstowego
- zapoznać się z dostępnymi możliwościami filtracji ramek. Skonfigurować parametry filtracji ramek według założeń podanych przez prowadzącego.

Filtracja ramek jest bardzo przydatną opcją umożliwiającą zdefiniowanie warunków jakie muszą spełniać ramki, aby zostały umieszczone w buforze odebranych ramek. W celu uaktywnienia filtracji ramek należy wybrać zakładkę *Rules*. W wyświetlonym oknie można określić filtrację na podstawie adresów warstwy drugiej (MAC), trzeciej (IP), czwartej (porty UDP i TCP) oraz m.in. na podstawie protokołów oraz kierunku ruchu (wchodzący, wychodzący, obcy).

Dostępny jest też filtr zaawansowany pozwalający na połączenie prostych filtrów z użyciem operatorów logicznych (np. AND, OR).

Sprawozdanie

W sprawozdaniu należy zamieścić opis wykonania i wyniki zarejestrowane w poszczególnych punktach ćwiczenia wraz z niezbędnymi komentarzami wyjaśniającymi istotę poszczególnych operacji.

5. Wymagania BHP

Zgodnie z podanymi na pierwszych zajęciach i potwierdzonymi przez studentów zasadami obowiązującymi w pomieszczeniu, w którym odbywają się ćwiczenia. Stosowny regulamin BHP jest też wywieszony w pomieszczeniu laboratorium.

6. Literatura

1. J. D. Sloan: *Narzędzia administrowania siecią*. Wydawnictwo RM, W-wa 2002
2. Dokumentacja programu *Wireshark* (www.wireshark.org)
3. Notatki z wykładu *Systemu i sieci telekomunikacyjne 1*