Wydział Elektroniki i Telekomunikacji – POLITECHNIKA POZNAŃSKA
ul. Piotrowo 3a, 60-965 Poznań
fax: (+48 61) 665 25 72
tel: (+48 61) 665 22 93

LABORATORIUM SIECI KOMPUTEROWYCH

(compnet.et.put.poznan.pl)

Narzędzia sieciowe Windows

Opracował: *dr inż. Sławomir Hanczewski*

Katedra Sieci Telekomunikacyjnych i Komputerowych

Poznań 2014

W kolejnych wersjach systemu Windows pojawiały się programy, które są niezbędne do rozwiązywania problemów z siecią (są one częścią oprogramowania związanego z obsługą stosu protokołów TCP/IP). System operacyjny Windows 7, oprócz narzędzi dostępnych w trybie graficznym, oferuje również narzędzia dostępne w wierszu poleceń (**Menu Start ->Uruchom -> `cmd`**). Narzędzia te były dostępne również w poprzednich wersjach systemu Windows. Są one odpowiednikami programów stosowanych od lat w różnych odmianach systemu UNIX. W systemie Windows dostępne są między innymi następujące narzędzia:

- **`ipconfig`**;
- **`ping`**;
- **`tracert`** (**`traceroute`**);
- **`nslookup`**;
- **`netstat`**;
- **`arp`**.

Listę opcji (wraz z krótkim opisem) wymienionych poleceń można uzyskać uruchamiając dany program z parametrem **`-?`** (**`/?`**).

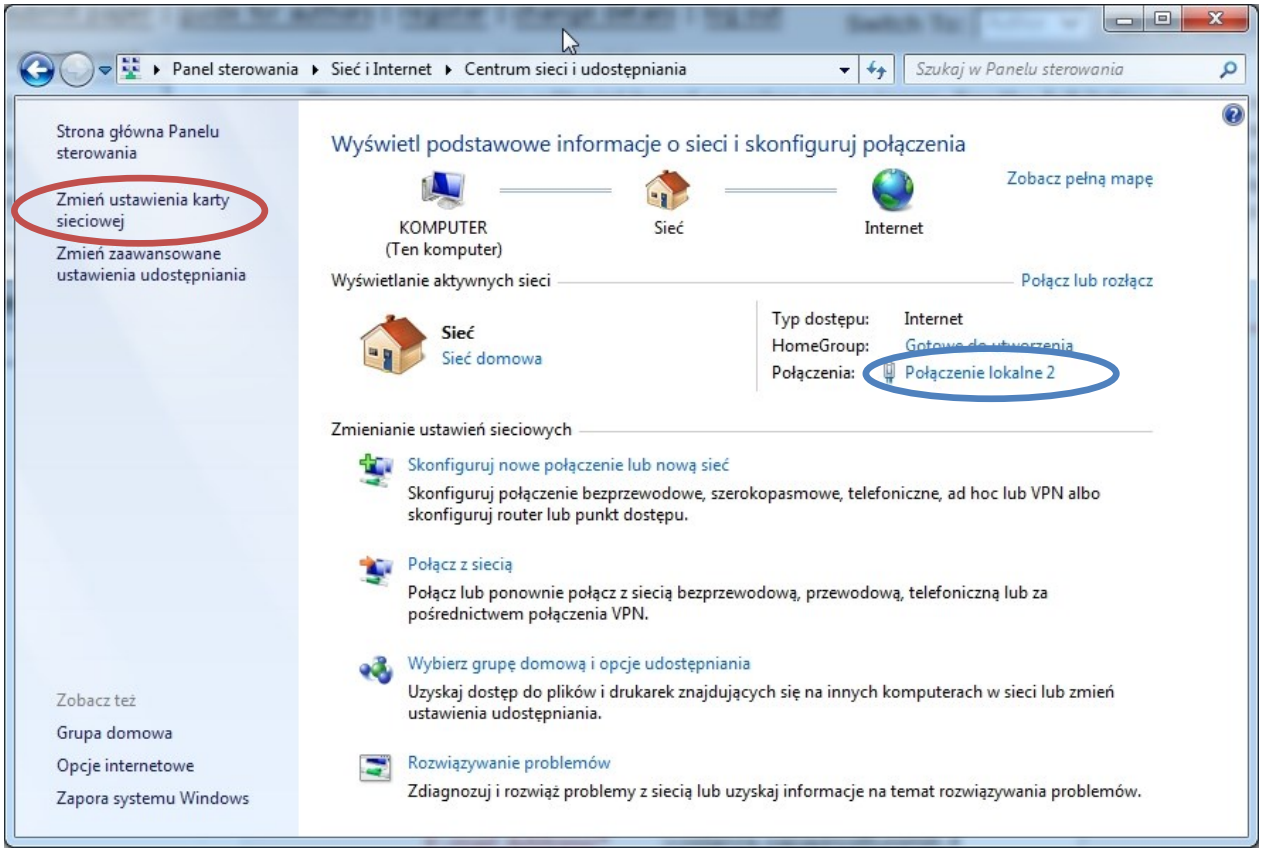
1. Konfiguracja TCP/IP

1.1 Konfiguracja adresów IP

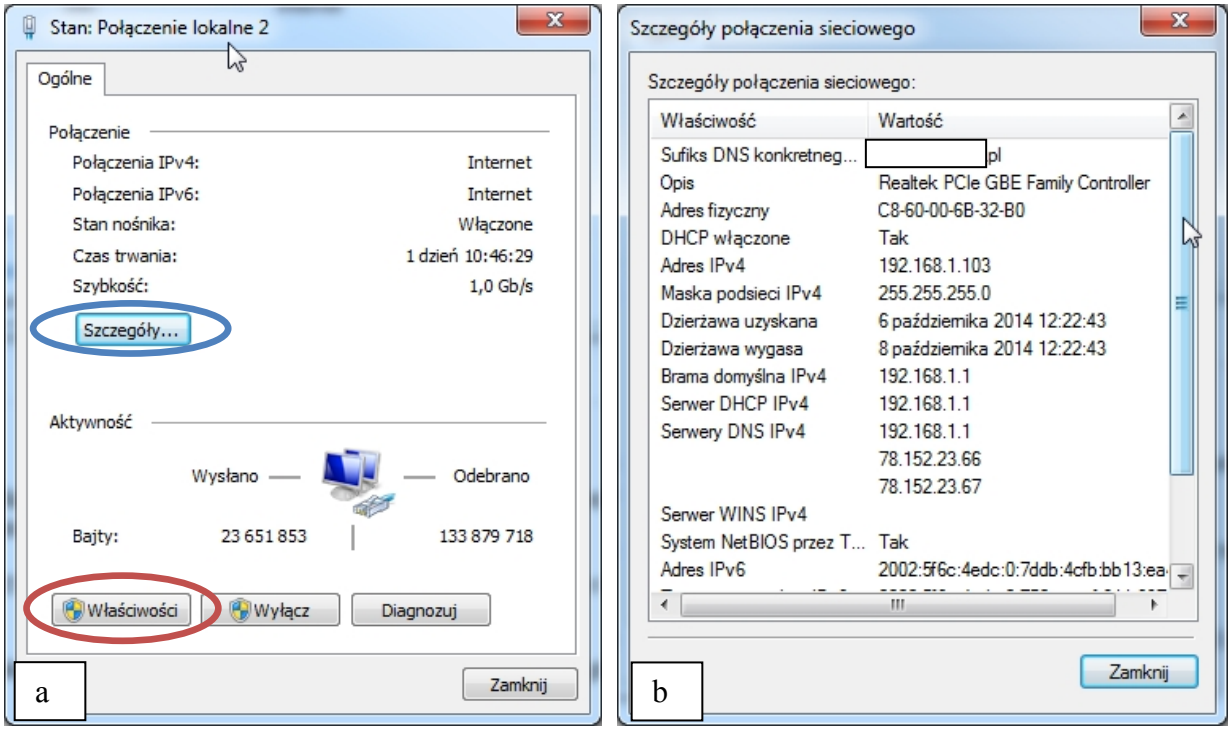
Adres IP może być przydzielony danemu urządzeniu na dwa sposoby:

- automatycznie (adres jest przydzielany przez serwer DHCP - Dynamic Host Configuration Protocol),
- ręcznie (odpowiedni adres IP musi być ręcznie wpisany w odpowiednim polu okna „**Właściwości: protokół internetowy w wersji 4 (TCP/IPv4)**” – Rysunek 3b)

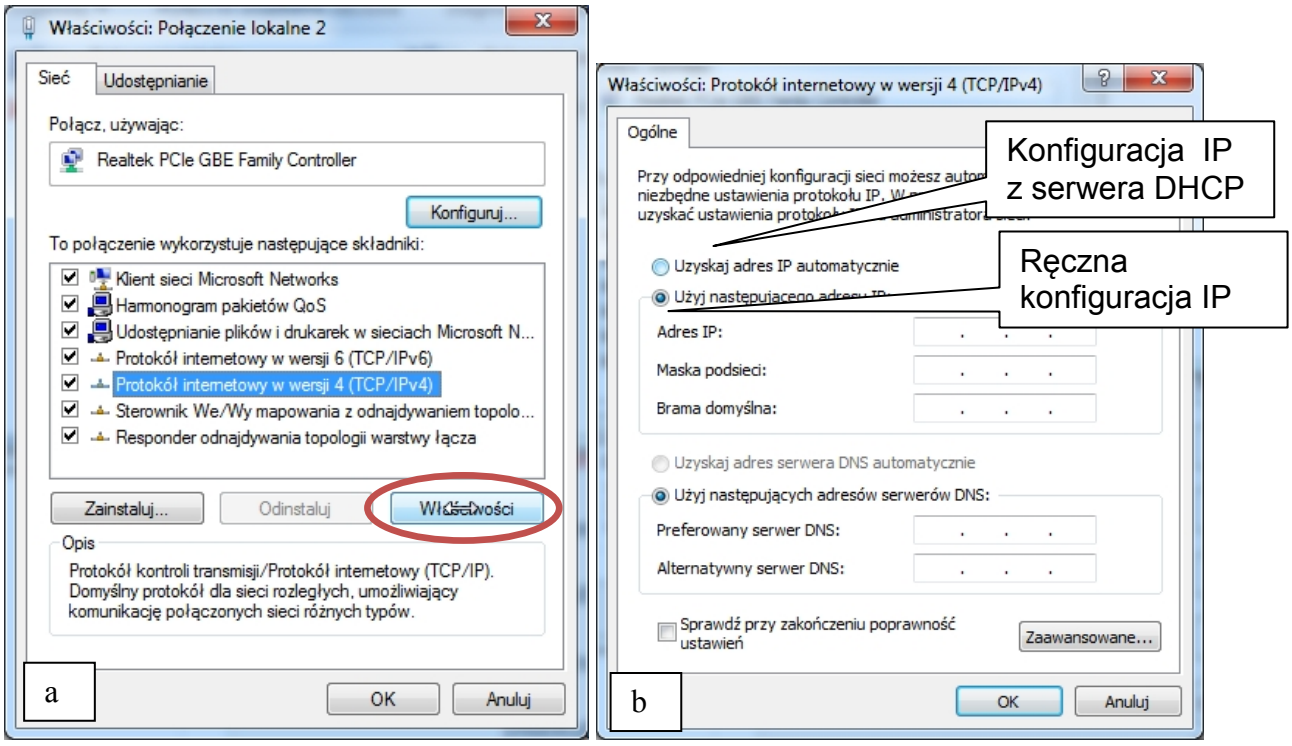
W przypadku automatycznej konfiguracji (ustawienie domyślne), adres IP zostanie przydzielony w trakcie uruchamiania systemu operacyjnego. Informacje o konfiguracji można wyświetlić za pomocą programu **`ipconfig`** dostępnego w wierszu poleceń (punkt 1.2). W trybie graficznym należy otworzyć okno: **Panel sterowania-> Sieć Internet->Centrum sieci i udostępniania** (rysunek 1). Następnie należy kliknąć na wybrane połączenie sieciowe. Wyświetlone zostanie okno zaprezentowane na rysunku 2a. Następnie należy kliknąć na opcję **Szczegóły** w wyniku czego wyświetlone zostanie okno przedstawione na rysunku 2b.
Aby ręcznie ustawić adres IP należy w oknie przedstawionym na rysunku 2a kliknąć przycisk **Właściwości** (pojawi się okno przedstawione na rysunku 3a), następnie należy dwukrotnie kliknąć lewym klawiszem myszy na opcję **Protokół internetowy w wersji 4 (TCP/IPv4)**. Wywołane zostanie w ten sposób okno przedstawione na rysunku 3b. Aby ręcznie ustawić adres IP należy wybrać opcję **Użyj następującego adresu IP**.



Rysunek 1 Okno **Panel sterowania-> Sieć Internet->Centrum sieci i udostępniania**



Rysunek 2. Wyświetlenie informacji o konfiguracji wybranego połączenia. a) okno z ogólnymi informacjami o wybranym połączeniu b) szczegóły wybranego połączenia sieciowego



Rysunek 3 Ręczne ustawienie adresu IP. a) okno właściwości wybranego połączenia sieciowego, b) okno właściwości protokołu IPv4

1.2 Polecenie `ipconfig`

Wyświetla informacje o konfiguracji stosu protokołów TCP/IP w systemach MS Windows. Polecenie wywołane bez parametrów wyświetla dla każdej karty sieciowej następujące informacje:

- adres IP komputera,
- maskę podsieci oraz
- bramę domyślną.

Po uruchomieniu programu z parametrem **`/all`** wyświetli kompletną informację o konfiguracji sieci (w tym adres MAC każdej karty sieciowej). W przypadku połączenia modemowego parametry zostaną wyświetlone dopiero po jego nawiązaniu połączenia. Program **`ipconfig`** najlepiej uruchamiać w wierszu poleceń (uruchomienie tego programu **Menu Start-> Uruchom-> `ipconfig`** spowoduje, że wynik działanie programu będą widoczne tylko przez chwilę).

```
C:\>ipconfig /?

SPOSÓB UŻYCIA:
    ipconfig [/allcompartments] [/? | /all |
       /renew [karta] | /release [karta] |
       /renew6 [karta] | /release6 [karta] |
       /flushdns | /displaydns | /registerdns |
       /showclassid karta |
```

```
        /setclassid karta [identyfikator_klasy] ]|
        /showclassid6 karta |
        /setclassid6 karta [identyfikator_klasy] ]
```

...

Opcje:

/?	Wyświetla ten komunikat pomocy.
/all	Wyświetla pełne informacje o konfiguracji.
/release	Zwalnia adres IPv4 podanej karty.
/release6	Zwalnia adres IPv6 podanej karty.
/renew	Odnawia adres IPv4 podanej karty.
/renew6	Odnawia adres IPv6 podanej karty.
/flushdns	Przeczyszcza bufor programu rozpoznawania nazw DNS.
/registerdns	Odświeża wszystkie dzierżawy DHCP i rejestruje ponownie nazwy DNS.
/displaydns	Wyświetla zawartość buforu programu rozpoznawania nazw DNS.
/showclassid	Wyświetla wszystkie identyfikatory klas DHCP dozwolone dla karty.
/setclassid	Modyfikuje identyfikator klasy DHCP.
/showclassid6	Wyświetla wszystkie identyfikatory klas DHCP IPv6 dozwolone dla karty.
/setclassid6	Modyfikuje identyfikator klasy DHCP IPv6.

Jeśli dla parametrów **release** i **renew** nie zostanie określona nazwa karty, zwolnieniu lub odnowieniu ulegną dzierżawy adresów IP dla wszystkich kart związanych z protokołem TCP/IP.

1.2 Przebieg ćwiczenia

Sprawdzić działanie polecenia **ipconfig** (należy wywołać to polecenie z odpowiednimi, wybranymi opcjami) i odpowiedzieć na następujące pytania:

a) Jakie informacje można uzyskać za pomocą polecenia **ipconfig**, które zostało wywołane bez dodatkowych opcji?
b) Jakie informacje dodatkowe można uzyskać dzięki opcji **/all**?
c) Czy powiodła się próba zwolnienia i ponownego uzyskania adresu IP?
d) Co to jest dzierżawa adresu IP i jak długo trwa?
e) Jakie informacje można uzyskać za pomocą polecenia **ipconfig /displaydns**
f) Czy za pomocą polecenia **ipconfig** można sprawdzić adres MAC karty sieciowej? Jeśli nie, to w jaki sposób można odczytać ten adres.
g) Czy za pomocą polecenia **ipconfig /all** można uzyskać informacje o adresach IPv6? Czy adresy IPv4 i IPv6 różnią się? Jeśli tak, wymień różnice.
h) Czym różni się adres IP (v4 i v6) od adresu MAC?

2. Polecenie **ping**

Narzędzie testowe **ping** wysyła pakiety diagnostyczne ICMP – Internet Control Message Protocol - (typu Echo Request - żądanie odesłania odpowiedzi), aby sprawdzić, czy zdalny host podłączony do sieci jest dostępny. **Ping** podaje również czas odpowiedzi zdalnego komputera na wysyłane zapytania, co pozwala się zorientować, czy diagnozowany problem nie jest związany z szybkością łącza. Jako argument podaje się nazwę zdalnego komputera. Warto pamiętać, że coraz częściej administratorzy serwerów internetowych blokują pakiety ICMP (ping) jako stwarzające potencjalne zagrożenie (systemy operacyjne Windows od wersji Windows XP SP2 domyślnie blokują odpowiedzi na wiadomości Echo request). W takim przypadku **ping** wyświetli komunikat "Request Timed Out" (Upłynął limit czasu żądania), mimo że zdalna maszyna funkcjonuje poprawnie. Wraz z systemem Windows 2000 wprowadzono ulepszoną wersję **ping**-**a** - **pathping**. Potrafi ona określać, który router jest powodem opóźnienia w przesyłaniu pakietów. Podawane są również informacje o liczbie utraconych pakietów.
Użycie polecenia:

```
C:\>ping

Sposób użycia:
ping [-t] [-a] [-n liczba] [-l rozmiar] [-f] [-i TTL] [-v TOS]
[-r liczba] [-s liczba] [[-j lista_hostów] | [-k lista_hostów]]
[-w limit_czasu] [-R] [-S adres_źródłowy] [-4] [-6]
nazwa_obiektu_docelowego

Opcje:
```

-t Odpytuje określonego hosta do czasu zatrzymania. Aby przejrzeć statystyki i kontynuować, naciśnij klawisze **Ctrl+Break.** Aby zakończyć, naciśnij klawisze **Ctrl+C.**

-a Tłumaczy adresy na nazwy hostów.

-n liczba Liczba wysyłanych żądań echa.

-l rozmiar Rozmiar buforu wysyłania.

-f Ustawia w pakiecie flagę "Nie fragmentuj" (tylko IPv4).

-i TTL Czas wygaśnięcia.

-v TOS Typ usługi (tylko IPv4). To ustawienie zostało zaniechane i nie ma wpływu na wartość pola typu usługi w nagłówku IP.

-r liczba Rejestruje trasę dla podanej liczby przeskoków (tylko IPv4).

-s liczba Sygnatura czasowa dla podanej liczby przeskoków (tylko IPv4).

-j lista_hostów Swobodna trasa źródłowa wg listy **lista_hostów** (tylko IPv4).

-k lista_hostów Ściśle określona trasa źródłowa wg listy **lista_hostów** (tylko IPv4).

-w limit_czasu Limit czasu oczekiwania na odpowiedź (w milisekundach).
-R Powoduje użycie nagłówka routingu w celu dodatkowego testowania trasy wstecznej (tylko IPv6).
-S adres_źródłowy Adres źródłowy do użycia.
-4 Wymusza używanie IPv4.
-6 Wymusza używanie IPv6.

np.: **ping www.wp.pl**

Program **ping** dostępny jest również online np. na stronie: **http://centralops.net**

2.1 Przebieg ćwiczenia

a) Sprawdzić działanie polecenia **ping** z opcjami: **-t, -a, –n, -i, -r.** Jako cel należy wybrać:
www.et.put.poznan.pl,
www.wp.pl.

W jakich granicach zawierają się czasy odpowiedzi zdalnego komputera na wysyłane zapytania?
Jakie informacje można uzyskać za pomocą polecenia **ping**?

b) Sprawdzić działanie polecenia **ping 127.0.0.1**
Proszę o komentarz uzyskanych rezultatów w odniesieniu do wyników uzyskanych w przypadku gdy celem był adres **www.et.put.poznan.pl.**

c) Sprawdzić działanie narzędzia ping dostępnego online.

Jeśli korzystamy ze strony to skąd będą wysyłane wiadomości ICMP?

d) Czy dostępne jest polecenie **pathping**? Jeśli polecenie **pathping** jest dostępne porównaj jego działanie z poleceniem ping (jako cel należy użyć adresu IP: 150.254.29.65).

3. Polecenie **tracert**

Dostępne w systemie Windows polecenie **tracert** jest odpowiednikiem uniksowego polecenia **traceroute.** Program ten pokazuje ścieżkę pokonywaną przez pakiety między dwoma hostami w sieci IP, włączając w to wszystkie routery znajdujące się pomiędzy badanymi hostami. Wyświetlane są również opóźnienia przejścia pakietów pomiędzy nimi. Umożliwia łatwe sprawdzenie, który węzeł jest źródłem największego opóźnienia.

C:\>tracert

```
Sposób użycia:
tracert [-d] [-h maks_przes] [-j lista_hostów] [-w limit_czasu]
        [-R] [-S adres_źródłowy] [-4] [-6] nazwa_celu

Opcje:
-d          Nie rozpoznawaj adresów jako nazw hostów.
-h maks_przes       Maksymalna liczba przeskoków w poszukiwaniu celu.
-j lista_hostów     Swobodna trasa źródłowa według listy lista_hostów (tylko IPv4).
-w limit_czasu      Limit czasu oczekiwania na odpowiedź w milisekundach.
-R          Śledź ścieżkę błądzenia (tylko IPv6).
-S adres_źródłowy   Adres źródłowy do użycia (tylko IPv6).
-4          Wymuś używanie IPv4.
-6          Wymuś używanie IPv6.
```

Program **tracert** dostępny jest również online np na stronie:
http://centralops.net

3.1 Przebieg ćwiczenia

a) Sprawdzić działanie polecenia **tracert** z wybranymi opcjami (jako cel należy podać www.et.put.poznan.pl oraz www.wp.pl).
b) W jaki sposób przedstawiane są informacje o drodze pokonywanej przez pakiet?
c) Sprawdzić działanie narzędzia **traceroute** dostępnego online.
d) Najdłuższa znaleziona ścieżka wyniosła …… węzłów.

4. Polecenie **nslookup**

Każde urządzenie podłączone do Internetu posiada jednoznaczny (niepowtarzalny) adres IP. W przypadku wersji czwartej protokołu IP, adres ten składa się z czterech liczb oddzielanych od siebie kropkami. By ułatwić korzystanie z Internetu, umożliwiono przywoływanie poszczególnych serwerów na podstawie określonych nazw mnemonicznych, np. **www.nss.et.put.poznan.pl**

Natomiast, aby ustalić adres IP serwera, wystarczy skorzystać z polecenia **ping** (należy użyć tego polecenia z odpowiednią opcją). Można również użyć polacenia **nslookup**:

```
nslookup <adres>
```

Aby wyświetlić opcje polecenia należy użyć polecenia **lookup -?**.

Adresy IP i podporządkowane im nazwy są przechowywane w specjalnych serwerach DNS (Domain Name Server). To do nich należy rozkodowywanie nazw wpisywanych przez

użytkowników, którzy chcą nawiązać połączenie z określonymi komputerami w Internecie. Polecenie to również może być dostępne z poziomu strony WWW. Przykładem takiej strony może być: **`http://centralops.net/`**.

4.1 Przebieg ćwiczenia

a) Proszę sprawdzić dostępność tego polecenia.
Z jakimi opcjami można wywoływać to polecenie, jakiego typu informacje można dzięki opcjom uzyskać? (jeśli opcji jest dużo sprawdź działanie polecenie z 3 – 4 opcjami – przedstaw wyniki).

5. Polecenie **`netstat`**

Polecenie to umożliwia wyświetlenie statystyk protokołu oraz bieżących połączeń sieciowych TCP/IP.
Użycie polecenia **`netstat`**:

```
NETSTAT [-a] [-e] [-n] [-s] [-p protokół] [-r] [odstęp]
```

Opcje:

`-a` wyświetla wszystkie połączenia i porty oczekujące.

`-e` wyświetla statystyki Ethernet-u. Ta opcja może być używana razem z opcją -s.

`-n` wyświetla adresy i porty w postaci liczbowej .

`-p protokół` wyświetla połączenia dla określonego protokołu; może to być protokół TCP lub UDP. Jeżeli ta opcja użyta jest razem z opcją -s, do wyświetlenia wybranego protokołu, protokół może mieć wartość TCP, UDP lub IP.

`-r` wyświetla tabelę routingu.

`-s` wyświetla statystykę wybranego protokołu. Domyślnie jest to statystyka protokołów TCP, UDP i IP;

`odstęp` Wyświetla wybraną statystykę, odczekując zadaną ilość sekund pomiędzy każdym wyświetleniem. Naciśnij CTRL+C, aby przerwać wyświetlanie statystyk. Jeżeli ta zmienna nie zostanie określona, program **`netstat`** wydrukuje raz informację o konfiguracji.

5.1 Przebieg ćwiczenia

Sprawdzić jakie informacje są możliwe do uzyskania za pomocą polecenia **`netstat`** użytego z wybranymi opcjami (przedstawić uzyskane informacje).

6. Polecenie **`arp`**

Protokół ARP (Address Resolution Protocol) umożliwia powiązanie adresu IP z adresem MAC.

Użycie polecenia:

```
ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]
```

-a Wyświetla bieżące wpisy protokołu ARP przez odpytywanie bieżących danych protokołu. Jeżeli **inet_addr** jest określony, to wyświetlany jest adres IP i fizyczny dla określonego komputera. Jeżeli więcej niż jeden interfejs sieciowy korzysta z protokołu ARP, to wyświetlane są wpisy dla każdej tabeli protokołu ARP.

-g To samo co **-a.**

-v Wyświetla bieżące wpisy protokołu ARP w trybie pełnym. Zostaną pokazane wszystkie nieprawidłowe wpisy oraz wpisy interfejsu pętli zwrotnej.

inet_addr Określa adres internetowy.

-N if_addr Wyświetla wpisy protokołu ARP dla interfejsu sieciowego określonego przez **if_addr.**

-d Usuwa hosta określonego przez inet_addr. W inet_addr można użyć symbolu wieloznacznego * do usunięcia wszystkich hostów.

-s Dodaje hosta i kojarzy adres internetowy **inet_addr** z fizycznym adresem internetowym **eth_addr**. Adres fizyczny jest reprezentowany przez 6 szesnastkowych bajtów oddzielonych znakami łącznika. Wpis dokonywany jest na stałe.

eth_addr Określa adres fizyczny.

if_addr Jeżeli jest określony, to wskazuje adres interfejsu, którego tabela translacji powinna zostać zmieniona. Jeżeli nie jest określony, zostanie użyty pierwszy odpowiadający interfejs.

```
Przykłady:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .... Dodaje
statyczny wpis.
  > arp -a  .... Wyświetla tabelę arp.
```

6.1 Przebieg ćwiczenia

Proszę odpowiedzieć na następujące pytania:

a) Do czego służy protokół **arp**?
b) Jakie informacje można uzyskać za pomocą polecenia **arp**?
c) Jakie opcje są dostępne dla tego polecenia? (proszę podać 3-4).
d) Czy informacje uzyskane za pomocą protokołu ARP są zapamiętywane w systemie operacyjnym.

Literatura:
- pomoc systemowa omawianych poleceń;
- opisy narzędzi sieciowych systemu Windows dostępne w sieci Internet