

Warsztaty z Sieci komputerowych

Lista 1

1 Uwagi dotyczące korzystania z pracowni 109

W pracowni 109 nie wolno: przesuwać stołów, komputerów i monitorów (grozi to zerwaniem kabli połączeniowych), przełączać okablowania; zbliżać się do stojaków ze sprzętem sieciowym (wszystkie podłączenia może wykonywać **wyłącznie** osoba prowadząca ćwiczenia).

Przed rozpoczęciem pracy należy: włączyć listwy zasilające znajdujące się na stołach; uruchomić komputery; wydać polecenie `sudo netmode lab`.

Po zakończeniu pracy należy: zamknąć system na obu komputerach w sąsiadujących ławkach wybierając opcję **Shutdown** w menu KDE; wyłączyć listwę zasilającą. Nie wolno wyłączać zasilania przed całkowitym zamknięciem systemu!

Proszę też pozostawić stanowisko w takim stanie, w jakim się je zastało. W szczególności proszę odstawić krzesło, monitor, klawiaturę i mysz na wyjściową pozycję.

2 Zadania

Znak `$>` oznacza wykonanie danego polecenia w konsoli z uprawnieniami zwykłego użytkownika. Natomiast znak `#>` oznacza konieczność wykonania polecenia z prawami administratora: takie polecenie należy poprzedzić komendą `sudo`.

Zadanie 1. Zacznij pracę od wykonania poleceń:

```
#> netmode lab
#> ifup eth0
```

Skonfiguruje to interfejs sieciowy `eth0` na Twoim komputerze; szczegóły tej konfiguracji zostaną wyjaśnione na kolejnych zajęciach. Tymczasem obejrzyj dostępne interfejsy sieciowe:

```
#> ifconfig -a
```

i interfejsy obecnie aktywne:

```
#> ifconfig
```

Interfejsy `eth0` i `eth1` odpowiadają dwóm ethernetowym kartom sieciowym, zaś interfejs `wlan0` odpowiada karcie sieci bezprzewodowej. Karta związana z interfejsem `eth0` łączy Twój komputer z Internetem. Jaki adres IP jest przypisany do interfejsu `eth0`? Jak bardzo ten adres różni się od adresu IP Twojego sąsiada?

Zadanie 2. Poleceniami

```
#> mii-tool
#> ethtool eth0
#> ethtool eth1
```

sprawdź status warstwy łącza danych i warstwy fizycznej. Dla jakich interfejsów warstwa łącza danych jest aktywna? Jaki standard Ethernetu jest wykorzystywany (jaka predkość została wynegocjowana)?

Na komputerze sąsiada uruchom polecenie

```
$> iperf -s
```

zaś na swoim komputerze polecenie

```
$> iperf -c adres_ip_sasiada
```

Jaką ilość danych udaje Ci się przesłać przez jednostkę czasu? Z czego może wynikać różnica między tą wartością a deklarowaną przez `mii-tool` przepustowością kanału?

Zadanie 3. Uruchom przeglądarkę Firefox (Iceweasel). Znajdź i zainstaluj rozszerzenie *Live HTTP Headers* (jeśli jeszcze nie jest zainstalowane). Umożliwia ono wyświetlanie w pasku bocznym przeglądarki wysyłanych i odbieranych nagłówków HTTP (w tym celu wybierz z menu pozycję *View — Sidebar — Live HTTP Headers*). Wejdź przeglądarką na stronę http://www.ii.uni.wroc.pl/~mbi/dyd/sieci_16s/ i obejrzyj przesyłane nagłówki protokołu HTTP.

Sprawdź jaki jest adres IP związany z adresem `ww.ii.uni.wroc.pl` poleceniem

```
$> host -t a www.ii.uni.wroc.pl
```

Niech `w.x.y.z` będzie tym adresem IP. Włącz program `wireshark` i włącz w nim obserwację interfejsu `eth0`. Aby odfiltrować wyświetlanie zbędnych pakietów w polu *Filter* wpisz `ip.src == w.x.y.z || ip.dst == w.x.y.z` i kliknij przycisk *Apply*. W razie potrzeby możesz również kliknąć ikonę *Restart current capture* (jedna z pierwszych ikon od lewej na górze okna programu).

Odśwież przeglądarką stronę http://www.ii.uni.wroc.pl/~mbi/dyd/sieci_16s/ naciskając `Shift + Ctrl + R`. W Wiresharku wśród wysyłanych pakietów znajdź ten zawierający żądanie HTTP. Obejrzyj w tym pakiecie nagłówki warstwy sieciowej (IP) i transportowej (TCP). Klikając poszczególne pola opisu, podświetlasz w widoku szesnastkowym pakietu (na dole okna) odpowiadające im bajty. Które części pakietu zawierają powyższe nagłówki? Jaki jest źródłowy i docelowy adres IP tego pakietu? Jaki jest jego źródłowy i docelowy port?

Powtórz te operacje dla pakietu zawierającego odpowiedź HTTP (powinien zawierać kod odpowiedzi 200 OK wraz ze stroną w HTML lub kod odpowiedzi 304 Not Modified). Czy dane identyfikujące połączenie (źródłowy/docelowy adres/port) zmieniły się czy są takie same? Dlaczego?

Zadanie 4. Za pomocą Live HTTP Headers obejrzyj jeszcze raz żądanie HTTP wysyłane w momencie pobierania strony http://www.ii.uni.wroc.pl/~mbi/dyd/sieci_16s. Zaznacz myszką wyświetlane żądanie HTTP i wybierając z menu kontekstowego polecenie *Save Selection* zapisz je do pliku `zapytanie`. Upewnij się, że na końcu pliku znajduje się pusty wiersz. Wyślij to zapytanie do serwera WWW (tj. do portu 80 adresu IP związanego z nazwą `www.ii.uni.wroc.pl` poleceniem

```
$> nc -q 3 www.ii.uni.wroc.pl 80 < zapytanie
```

(Opcja `-q 3` czeka 3 sekundy przed zamknięciem połączenia). Obejrzyj przesyłane pakiety w Wiresharku.

Sprawdź, czy uzyskasz odpowiedź, jeśli w pliku `zapytanie` pozostawisz jedynie dwa pierwsze wiersze (zaczynające się od `GET` i `Host:`) i następujący po nich pusty wiersz. Ponownie obejrzyj pakiety w Wiresharku.

Zadanie 5. Polecenie `ping` służy do testowania warstwy sieciowej. W polu danych pakietów IP wysyłane są wtedy specjalne komunikaty protokołu ICMP. Wykonaj polecenie

```
$> ping adres_IP_sąsiada
```

Obejrzyj wysyłane pakiety w Wiresharku. W tym celu usuń bieżący filtr, wpisz nowy: `ip.src == Twój_adres_IP || ip.dst == Twój_adres_IP` a następnie kliknij przycisk *Apply*. Czy znacznik czasowy w wysyłanym zapytaniu i odpowiedzi różnią się, czy są takie same?

Pingnij kilka znanych Ci adresów polskich stron WWW i adresów zagranicznych. Jakie są czasy odpowiedzi w przypadku każdego z nich?

Swoim ulubionym linuksowym edytorem otwórz plik `/etc/hosts` i przeczytaj dokumentację

```
$> man hosts
```

Zmodyfikuj ten plik związuąc adresy IP paru komputerów z pracowni z wymyślonymi przez siebie nazwami komputerów. Uwaga: to przyporządkowanie działa tylko lokalnie, na jednym komputerze. Sprawdź, czy polecenie `ping` działa też z tymi nazwami. W razie problemów początkową konfigurację można przywrócić poleceniem

```
#> restore_hosts
```

Zadanie 6. Poleceniem

```
$> telnet www.ii.uni.wroc.pl 80
```

otwórz strumień danych do serwera WWW na komputerze `www.ii.uni.wroc.pl`. Wpisz tam zawartość pliku `zapytanie`, czyli następujące wiersze

```
GET /~mbi/dyd/sieci_16s/ HTTP/1.1
Host: www.ii.uni.wroc.pl
```

a następnie pusty wiersz. W odpowiedzi otrzymasz kolejny raz powyższą stronę WWW.

Poleceniami

```
#> netstat -4tlpn
#> netstat -4tlp
```

wyświetl uruchomione na Twoim komputerze usługi „przypięte” do konkretnych portów warstwy transportowej. Pierwsze polecenie wyświetla wartości numeryczne, drugie zaś stara się je interpretować wykorzystując m.in. plik `/etc/services` (obejrzyj ten plik). Ponownie korzystając z programu `telnet` połącz się z kilkoma wybranymi z powyższych usług, w tym z usługą FTP i SSH. Przykładowo z portem 22 połączysz się poleceniem

```
telnet localhost 22
```

Sprawdź, czy te usługi wypisują coś po połączeniu. Rozłączyć się możesz naciskając klawisze `Ctrl +]` i następnie wydając polecenie `quit`.

Lista i materiały znajdują się pod adresem <http://www.ii.uni.wroc.pl/~mbi/dyd/>

Marcin Bienkowski