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.

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 wyświetlenia dostępnych interfejsów sieciowych poleceniami

```
$> ip link
$> ip addr
```

Aktywne interfejsy oznaczone są napisem `UP`, nieaktywne — `DOWN`. Drugie z tych poleceń wyświetla dodatkowo przypisane do interfejsów adresy IP. Podobną informację można również uzyskać za pomocą starszego polecenia

```
#> ifconfig -a
```

Interfejsy `enp1s0`, `enp3s0` i `enp4s0` odpowiadają trzem ethernetowym kartom sieciowym, zaś interfejs `wlp5s0` odpowiada karcie sieci bezprzewodowej. Karty `enp3s0` łączą wszystkie komputery z pracowni z przełącznikiem sieciowym, który jest również podpięty do routera łączącego pracownię z Internetem. Natomiast karty `enp1s0` są spięte parami (łączą sąsiadujące ze sobą w ławce komputery).

Jaki adres IP jest przypisany do interfejsu `enp3s0`? Jak bardzo ten adres różni się od adresu IP Twojego sąsiada? Poleceniami

```
#> ethtool enp1s0
#> ethtool enp3s0
#> ethtool enp4s0
```

sprawdź status warstwy fizycznej poszczególnych kart. Zwróć uwagę na pole `Link detected`, określające czy danym łączem można przesyłać dane (w szczególności, czy z drugiej strony kabla jest aktywna karta sieciowa) oraz pola `Speed` i `Duplex`.

Na komputerze sąsiada uruchom polecenie

```
$> iperf -s
```

zaś na swoim komputerze polecenie

```
$> iperf -c adres_IP_interfejsu_enp3s0_sąsiada
```

Jaką ilość danych udaje Ci się przesłać przez jednostkę czasu? Z czego może wynikać różnica między tą wartością a deklarowaną przez `ethtool` przepustowością kanału (100 Mbit)?

Uaktywnij interfejs `enp1s0` i nadaj mu odpowiedni adres IP poleceniami:

```
#> ip link set up dev enp1s0
#> ip addr add 192.168.0.x/24 dev enp1s0
```

gdzie x jest numerem Twojego komputera. Wartość `/24` jest tzw. maską podsieci i jej znaczenie zostanie wyjaśnione na kolejnych zajęciach. Poleceniem `ethtool enp1s0` sprawdź, że Twój komputer jest połączony z komputerem sąsiada łączem o przepustowości 1 Gbit = 1000 Mbit. Uruchom ponownie na komputerze sąsiada polecenie `iperf -s`, zaś na swoim komputerze polecenie

```
$> iperf -c adres_IP_interfejsu_enp1s0_sąsiada
```

Porównaj faktyczne przepustowości kanałów odpowiadającym połączeniom `enp1s0` (łącze 1 Gbit bezpośrednim kablem) i `enp3s0` (łącze 100 Mbit poprzez przełącznik sieciowy).

Poleceniem

```
#> ethtool -s enp1s0 speed 100 duplex full
```

zredukuj prędkość interfejsu `enp1s0` do 100 Mbit. Sprawdź teraz przepustowość łącza `enp1s0` za pomocą programu `iperf`. Czy jest ona mniejsza, większa czy taka sama jak przepustowość łącza `enp3s0`?

Zadanie 2. Polecenie `ping` służy do testowania warstwy sieciowej. W polu danych pakietów IP wysyłane są wtedy specjalne komunikaty protokołu ICMP. Wykonaj polecenia

```
$> ping adres_IP_interfejsu_enp1s0_sąsiada
$> ping adres_IP_interfejsu_enp3s0_sąsiada
```

Jak różnią się czasy odpowiedzi? Ile milisekund opóźnienia powoduje znajdujący się pomiędzy kartami `enp3s0` przełącznik sieciowy?

Uruchom program Wireshark i włącz w nim obserwację wszystkich interfejsów. Obejrzyj wysyłane przez `ping` pakiety. 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 poleceniem

```
$> man hosts
```

Zmodyfikuj ten plik związując 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

```
$> cp /etc/hosts.bkp /etc/hosts
```

Zadanie 3. Uruchom przeglądarkę Firefox. Z menu wybierz polecenie *View — Sidebar — Live HTTP Headers* wyświetlające w pasku bocznym przeglądarki wysyłanych i odbieranych nagłówków HTTP. Wejdź przeglądarką na stronę http://www.ii.uni.wroc.pl/~mbi/dyd/sieci_17s/ i obejrzyj przesyłane nagłówki protokołu HTTP.

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

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

Niech *w.x.y.z* będzie tym adresem IP. Uruchom program Wireshark i włącz w nim obserwację interfejsu `enp3s0`. 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_17s/ 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_17s. 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. 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_17s/ 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 Bieńkowski