

Specyfikacja The cake router

Ryszard Michalski

Paweł Polak

Jacek Strzałkowski

29 kwietnia 2021

The cake router

UWAGA Polecamy zapoznać się z HTMLową wersją niniejszej specyfikacji dostępnej w repozytorium [Repozytorium Github](#).

Trasowanie cebulowe

Trasowanie cebulowe jest techniką służącą do anonimowej komunikacji w sieci komputerowej. Komunikacja odbywa się przy wykorzystaniu trzech rodzajów jednostek: klienci, węzły pośredniczące i końcowe. Połączenie klienta z odbiorcą wygląda następująco. W pierwszej kolejności klient wybiera listę węzłów P_1, P_2, \dots, P_N, WK po których chce dotrzeć do adresata. Następnie nadaje paczkę informacji $\{dane, adres[P_2-ADRESAT]\}$ do P_1 . Dalej P_1 zapisuje adres klienta i wysyła paczkę $\{dane, adres[P_3-ADRESAT]\}$ do P_2 . Proces się powtarza aż węzeł końcowy - WK - wyśle pakiet do adresata.

URZĄDZENIE	OPERACJA	PAMIĘĆ
KLIENT		
P1		
P2		
P3		
WK		
ADRESAT		

Figure 1: Trasowanie cebulowe

Droga w kierunku przeciwnym jest następująca: adresat wysyła odpowiedź do WK. Z kolei z WK jest wysyłana ta odpowiedź do P_N , do WK zapisał adres. Dalej P_N przesyła odpowiedź do P_{N-1} itd., aż odpowiedź wróci do klienta.

Funkcjonalności

Nasz program będzie spełniał następujące wymagania: - umożliwi przesyłanie komunikatów UDP (*user datagram protocol*, protokół bezstanowy, nie zapewnia retransmisji danych, umożliwia przesyłanie danych do wielu użytkowników). - możliwość sprawdzenia poprawności danych przy użyciu sumy kontrolnej (np. *sha256sum*) - Klient będzie posiadał

listę wszystkich węzłów pośredniczących (P_i oraz WK). - Z poziomu klienta będzie możliwy wybór trasy przez N węzłów pośredniczących (na podstawie powyższej listy). Liczba N będzie dowolna, ale mniejsza od ilości dostępnych węzłów pośredniczących. - Komunikaty będą zawierały paczkę złożoną z informacji przesyłanych oraz adresów - Możliwe będzie przesłanie paczki do innego hosta (który również «oferuje» swoje usługi jako węzeł pośredni) i otrzymanie od niego odpowiedzi. - Sieć będzie w stanie obsłużyć równolegle przynajmniej dwóch klientów.

Opis działania programu

Klient będzie uruchamiał program poprzez prosty alias. Na potrzeby robocze założymy, że będzie to cake-router. Zakładamy, że program będzie mógł być używany w następujący sposób

```
usage: cake-router [options]
```

```
options:
```

```
-l --list                               Wyświetla listę dostępnych hostów.
```

Mogą posłużyć do wyboru węzłów pośrednich przy próbie wysłania

```
-s --send [address] [trasa] [num]      Wsyła komunikat na podany adres.
```

W przypadku gdyby adres nie został podany, użytkownik ma możliwość wyboru adresu z listy. Ewentualnie wyświetli mu się taka lista, na podstawie której będzie mógł wybrać adres.

Gdyby trasa nie została podana, to program - o ile to możliwe - użyje domyślnej (wczyta z pliku). Jest możliwość wyboru ilości węzłów pośredniczących [num]. Wówczas te węzły są losowe.

```
--set-trasa                             Ustala domyślną trasę.
```

```
--listen                                Nasłuchuj komunikatów.
```

```
--help                                  Wyświetla ten komunikat.
```

Rozpatrujemy możliwość zadeklarowania trasy poprzez specjalny plik lub odpowiednio zadeklarowaną przy wywołaniu programu listę. ## Obsługa programu Klient uruchamia program cake-router w bashu poprzez wpisanie

```
$ cake-router
```

Wyświetla mu się informacja o możliwych opcjach. Następnie uruchamia program z opcją list

```
$ cake-router -l
```

Dostaje informacje o możliwych węzłach pośrednich (i docelowych). Przygotowuje trasę i wysyła komunikat np na adres lokalny 192.168.1.03 poprzez 3 węzły pośredniczące

```
$ cake-router -s 192.168.1.02 3
```

dalej użytkownik programu oczekuje na odpowiedź od nadawcy.