Specyfikacja The cake router

Ryszard Michalski Paweł Polak Jacek Strzałkowski

29 kwietnia 2021

The cake router

UWAGA Polecamy zapoznać się z HTMLową wersję niniejszej specyfikacji dostępnej w repozytorium Github link .

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 P1,P2,...,PN,WK po których chce dotrzeć do adresata. Następnie nadaje paczkę informacji {dane,adres[P2-ADRESAT]} do P1. Dalej P1 zapisuje adres klienta i wysyła paczkę {dane,adres[P3-ADRESAT]} do P2. Proces się powtarza aż węzeł końcowy - WK - wyślę 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 PN, do WK zapisał adres. Dalej PN przesyła odpowiedź do PN-1 itd., aż odpowiedź wróci do klienta.

Funkcjonalności

Nasz program będzie spełniał następujące wymagania: - [X] umożliwi przesyłanie komunikatów UDP (*user datagram protocol*, protokół bezstanowy, nie zapewnia retransmisji danych, umożliwia przesyłanie danych do wielu użytkowników). - [X] Użytkownik otrzymuje instrukcję dotyczącą tego, w jaki sposób może wykonać kontrolę danych. Np. tak

```
$ ./CakeClient.sh --help
```

- [X] Klient będzie posiadał listę wszystkich węzłów pośredniczących (P_i oraz WK) zapisaną w pliku konfiguracyjnym.
- [X] Klient będzie mógł łatwo podejrzeć listę przy pomocy bez znajomości nazwy pliku konfiguracyjnego.
- [X] Klient będzie mógł wygenerować listę węzłów pośrednich za pomocą odpowiedniej funkcji.
- [X] Komunikaty będą zawierały paczkę złożoną z informacji przesyłanych oraz adresów rozdzielonych średnikiem `;`.
- [X] Możliwe będzie przesłanie paczki do innego hosta (który również «oferuje» swoje usługi jako węzeł pośredni) i otrzymanie od niego odpowiedzi. W zasadzie, możliwe będzie wysłanie paczki do każdego hosta (węzła). Program węzła pośredniego i adresata jest ten sam.
- [X] Sieć będzie w stanie obsłużyć równolegle przynajmniej dwóch klientów oraz wielu klientów po sobie.
- [X] Wiadomość powrotna będzie wysyłana każdemu klientowi osobno.
- [X] Adresat nie będzie mógł bezpośrednio zidentyfikować skąd pochodzi wiadomość. Dlatego nadawca powienien się podpisywać w swojej wiadomości.
- [X] Adresat będzie mógł wpisać swoją odpowiedź w terminalu.
- [X] Adresat będzie mógł zapisać komunikat do pliku
- [X] Adresat będzie zabezpieczony przed wpisaniem wiadomości z `;`
- [X] Przed uruchomieniem programu klienckiego, program (z poziomu powłoki) sprawdzi, czy jest zainstalowana java. ## Obsługa programu Klient będzie mógł uruchamiać program poprzez poprzez prosty alias. Na potrzeby robocze załóżmy, że będzie to cake-router. Aby to osiągnąć, wystarczy wykonać na przykład

```
$ sudo echo "export cake-router=./path/to/file/CakeClient.sh" >> ~/.bash_aliases
$ cd ~
$ . .bashrc
```

Klient uruchamia program cake-router w bashu poprzez wpisanie nazwy skryptu np. `./CakeClient.sh` lub (Patrz instrukcja) za pomocą aliasu.

```
$ cake-router --help
```

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

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

Dostaje informacje o węzłach pośrednich z wczytanych z pliku konfiguracyjnego.

Możliwość wygenerowania pliku z adresami pośrednimi będzie realizowana za pomocą opcji

```
$ cake-router --set-trasa
```

Wysyłka odbywać się będzie za pomocą opcji `send`. Załóżmy, że użytkownik chce wysłać msg.txt na adres 192.168.1.1

```
$ cake-router -s 192.168.1.1 msg.txt
```

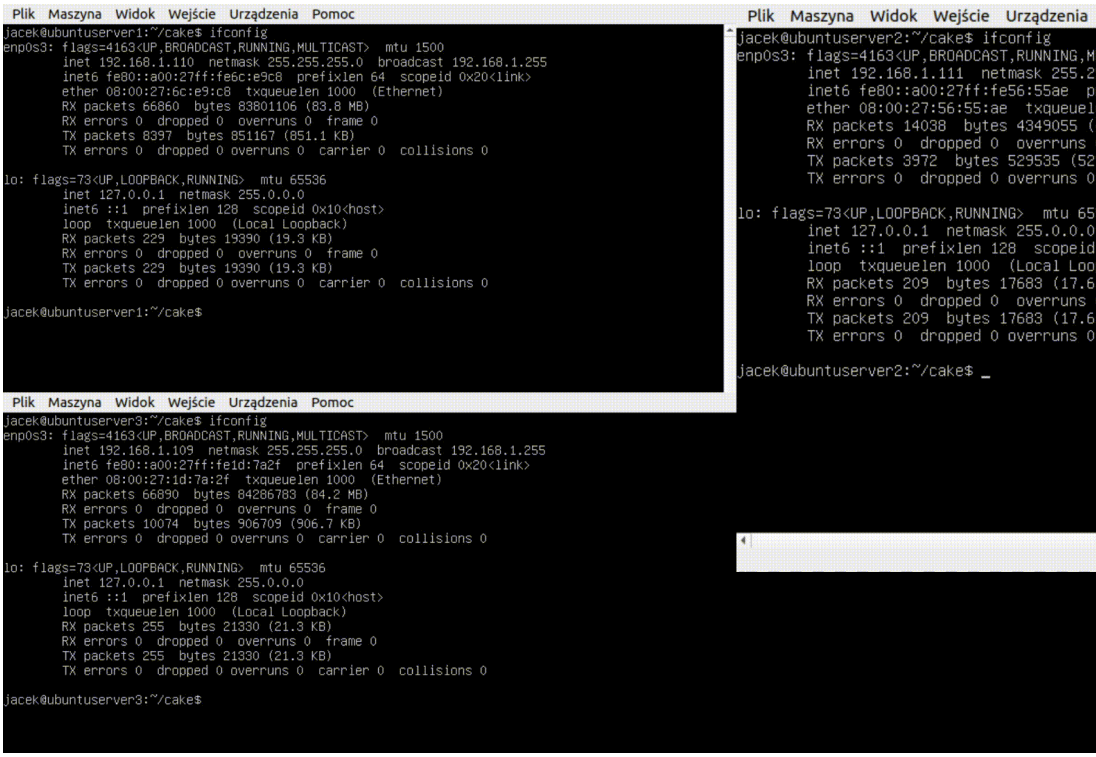
Po wysłaniu użytkownik programu oczekuje na odpowiedź od nadawcy.

Węzeł pośredni będzie uruchamiał swój program w konsoli za pomocą

```
$ ./CakeNode.sh
```

Gdy paczka dojdzie do adresata, będzie miał możliwość zapisania wiadomości do pliku oraz odpowiedzi. ## Działanie

Nadanie wiadomości i wybór trasy



Nadanie wiadomości poprzez dwa węzły pośrednie