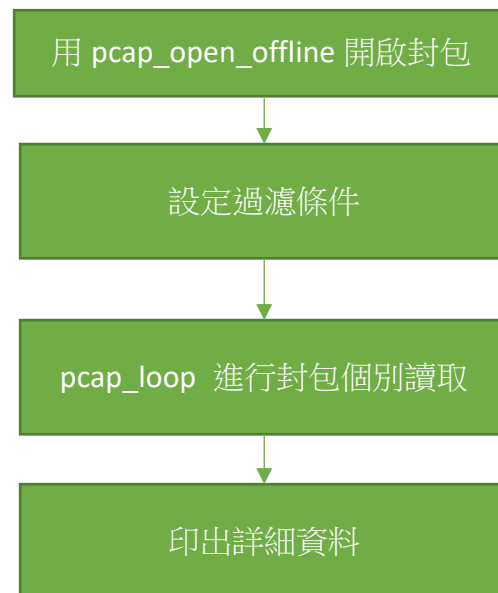


# 網路程式設計作業三 pcap 讀取程式

數學三 405210011 黃伯丞

## (1) 程式流程圖



chat server 流程圖

## (2) 實作技巧描述

本次作業中需要設計一支 pcap 封包檔的讀取程式，可以讀入 pcap 檔，並列出檔案中每個封包的來源/目的 IP 位址、來源/目的 port 號碼、封包長度、時間(以年、月、日、時、分、秒等單位顯示)。另外，command line 當中可以設定過濾條件(BPF 語法的條件)。函式可以從定義好的標頭檔 pcap.h 拿出使用，需要 pcap\_open\_offline (打開存在的封包檔)、pcap\_compile (編譯過濾條件)、pcap\_setfilter (設定過濾條件)、pcap\_loop (個別讀取封包)。個別讀取封包時利用 my\_packet\_handler 來印出所有需要的資料。

## (3) 重要的資料結構

### 1. Ethernet header

```
typedef struct eth_hdr
{
    u_char dst_mac[6];
    u_char src_mac[6];
```

```
        u_short eth_type;
    }eth_hdr;
```

## 2. IP header

```
typedef struct ip_hdr
{
    int version:4;
    int header_len:4;
    u_char tos:8;
    int total_len:16;
    int ident:16;
    int flags:16;
    u_char ttl:8;
    u_char protocol:8;
    int checksum:16;
    u_char sourceIP[4];
    u_char destIP[4];
}ip_hdr;
```

## 3. TCP header

```
typedef struct tcp_hdr
{
    u_short sport;
    u_short dport;
    u_int seq;
    u_int ack;
    u_char head_len;
    u_char flags;
    u_short wind_size;
    u_short check_sum;
    u_short urg_ptr;
}tcp_hdr;
```

## 4. UDP header

```
typedef struct udp_hdr
{
    u_short sport;
    u_short dport;
    u_short tot_len;
    u_short check_sum;
}udp_hdr;
```