パケットづくりではじめる ネットワーク入門

第30回 UDPパケット解析ツールを作る

坂井 弘亮

本連載はネットワーク上を流れるパケットを直接扱うようなツールを自作しつつ，ネットワークの仕組みを勉強していきます．テーマは「自作」，「現物ベース」，「動く感動」の3つです．ネットワークにはイーサネットとIPを想定しています．

今回行うこと

● UDP解析機能をパケット・ライブラリに追加

前回はネットワーク上で動作するサーバやクライアントのプログラムを作成するための準備として，UDPのパケットを作成する機能をパケット・ライブラリに追加しました．

今回はその逆で，受信したUDPのパケットを解析するための機能をパケット・ライブラリに追加します．これにより，UDPのパケットを直接扱うことができるようになります．

さらに機能追加を今回行ったパケット・ライブラリを利用して，UDPのパケットを受信して解析する「UDP解析ツール」を作ってみます．

調べるUDPパケットのヘッダ

● 構造

イーサネット上を流れるUDPのパケットは，**図1**のような構造になっています．先頭にはイーサネット・ヘッダ，続いてIPヘッダとUDPヘッダがあり，最後にデータがあります．

イーサネット・ヘッダ(14バイト)	IPヘッダ(20バイト以上)	UDPヘッダ(8バイト)	データ(任意のサイズ)

図1 UDPパケットの構造

● その1：イーサネット・ヘッダ

UDPのパケットを解析する際には，**図1**に従ってまず先頭のイーサネット・ヘッダを参照し，続くヘッダが何であるのかを判断します．イーサネット・ヘッダは**図2**のような構造になっています．

図2の「タイプ」の位置に，後続のヘッダの種別が格納されています．ここに格納される値は，一般に/usr/include/net/ethernet.hで定義されています．**リスト1**はFreeBSDの/usr/include/net/ethernet.hでの定義です．

● その2：IPヘッダ

続くヘッダがIPである場合には，タイプが0x0800という値になっていることで判断できます．この場合にはIPヘッダが後続しているため，続くヘッダをIPヘッダとして参照します．IPヘッダは**図3**のような構造に

リスト1 イーサネット・ヘッダ(図2)の「タイプ」に格納される値は/usr/include/net/ethernet.hで定義されている(FreeBSDの場合)

```
#define ETHERTYPE_IP            0x0800
                                  /* IP protocol */
:
#define ETHERTYPE_ARP           0x0806
                        /* Address resolution protocol */
:
#define ETHERTYPE_IPV6          0x86DD
                              /* IP protocol version 6 */
```

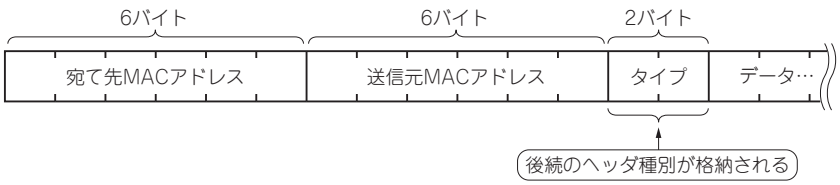

図2 イーサネット・ヘッダの構造

本連載のプログラムのソースコードは以下の筆者のホームページからダウンロードできます．ライセンスはKL-01というもので，組み込み機器などでも自由に利用することができます．
http://kozos.jp/books/interface/ethernet2/