第1部

第2章 よくあるMAC＆IPアドレスの重複やデータ誤りなどをサッと発見!

Linuxを使えば楽ショー!

ネットワーク・パケット取り込み＆解析環境の構築

坂井 弘亮

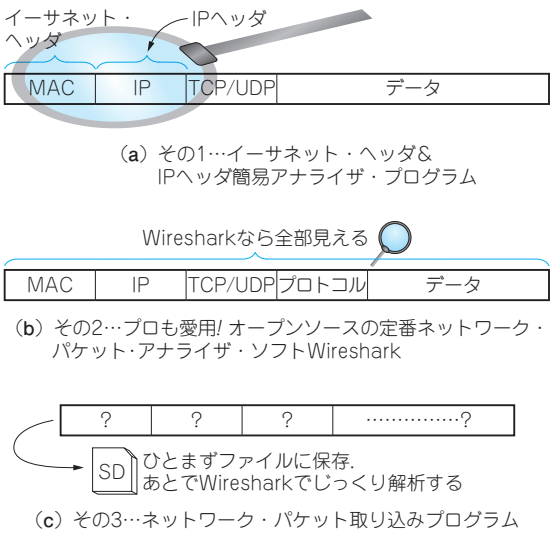

図1 本稿で紹介するネットワーク・パケット解析環境

本稿でやること

● ネットワーク・パケットを解析できると上達するし劇的に便利

自作マイコン基板をネットワークにつなぐとき，応答が出てこなかったり挙動がおかしかったりすることがあります．

例えば，MACアドレスは世界に一つだけのはずですが，自作マイコン基板の場合，サンプルのMACアドレス設定をそのまま利用してしまうことがあります．なんとなく装置の挙動がおかしいことには気づくのですが，解決に時間がかかることがあります．

何らかの問い合わせは届いているのに，マイコン基板からの応答がLAN上に出てこないなどの事象もあり得ます(パルス・トランスの断線などの原因が考えられます)．

原因を探るにはLANケーブル上に流れるパケットを見てしまえれば，手っ取り早く解決できます．

● 紹介するソフトウェア

ここでは，用途に応じて三つのネットワーク・パケット解析用のソフトウェアを紹介します．

▶その1…イーサ＆IPヘッダの自作簡易アナライザ

イーサネット・ヘッダやIPヘッダは，それほど複雑な構造をしているわけではないため，簡単なアナライザならば，自作可能です[**図1**(a)]．プログラムの容量も数Kバイト程度なので，ラズベリー・パイに搭載して持ち歩くこともできます．

▶その2…UDP/TCPもOKでフリー! 定番ネットワーク・パケット・アナライザ・ソフトWireshark

その1の自作簡易アナライザは，イーサネット，IP，ARPの三つのプロトコルにしか対応していません．

世の中には，フリー・ソフトウェアのネットワーク・パケット・アナライザtcpdumpやWiresharkなどといったものがあります．ここでは定番のWiresharkについて紹介します[**図1**(b)]．

Wiresharkは高機能なぶん巨大なツールでもありますので，ラズベリー・パイのような小型CPU基板での動作に不向きな部分もあります

▶その3…自作ネットワーク・パケット・ロガー・ソフト

その1の自作簡易アナライザではもの足りなくて(UDPやTCPも解析したくて)，Wireshark搭載パソコンをいちいち持ち歩きたくない場合，ネットワーク・パケット・ロガーがあると非常に便利です．ひたすらパケットを記録した後，パソコン上で動くWiresharkに読み込んで解析できます[**図1**(c)]．

第3章で示すようにラズベリー・パイで動かせば，非常に便利なネットワーク・パケット取り込み器になります．

その1…イーサ＆IPヘッダの自作簡易アナライザ

● 組み込みではイーサとIPのヘッダが解析できれば事足りる場合も

イーサネットは隣接ノードとの通信，IPはルーティングによる世界中へのパケットの到達性を司ります．