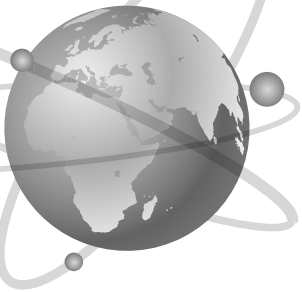
ダウンロード・データあります



パケットづくりではじめる ネットワーク入門

第65回 簡易L2スイッチにポートのミラーリング機能を追加する

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．ネットワークはイーサネットとIPを想定しています．

前回までは簡易L2スイッチに簡易認証機能を実装し，バージョン2まで改版しました．

今回はL2スイッチでネットワークのデバッグ時に重宝される，ポートのミラーリング機能を追加してみます．

ミラーリング機能を実装する

● こんな機能

L2スイッチの重要機能に，ポートのミラーリング機能があります．ミラーリング機能は，L2スイッチの機種によっては，「ミラー・ポート」などと呼ばれることもあります．

ポートのミラーリングは，あるポートから入力されるパケットをそのまま別のポートに出力する機能です．一般ユーザにはさほど必要とされない機能ですが，ネットワーク設計やデバッグの際に重宝されます．

● ケーブルを挿したままで特定ポートを監視できる

パケットの監視のためには，外部にハブを接続してキャプチャするなどの方法も考えられます．そのためにLANケーブルの抜き差しなどを行うと，ポートのリンクダウンが発生し，アラートが上がる可能性があります．もしくは，ネットワークが冗長構成の場合は，バックアップ側に切り替わる可能性もあります．一般にリンク・ダウンの発生は，ネットワーク構成の変更を引き起こす可能性があるので，運用中のネットワークでむやみに起こしてよいものではありません．

特定のポートを監視したいポートのVLANに含めておけば，そちらにも出力されることになりますが，ポート上にパケットが流れたときに入力されてしまう上に，MACアドレスが学習されてしまうこともあります．またそもそもMACアドレスの学習により，宛て先MACアドレスのノードが存在しなければ出力されません．キャプチャ専用の出力だけポートが必要とされるわけですが，そのために利用されるのがポートのミラーリング機能です．

監視したいポートに対して，ミラーリングするポートをあらかじめ設定しておけば，L2スイッチの設定変更やネットワークの構成変更なしに，特定のポートを通過しているパケットを確認できます．また，L2スイッチには，ポートのリンク・ダウンを発生させずにミラーリングの設定追加を可能としている機種も多くあります．

簡易L2スイッチのプログラム

リスト1に示すのは，前回までに作成した簡易L2スイッチ(`l2switch.c`)に，ポートのミラーリング機能を実装したプログラムです．

本プログラムは，説明用の簡易的なサンプルです．バッファやパケットのサイズ・チェックなどが省略されている部分があり，実際にはそれらのエラー対策が必要です．

● ミラーリング先の定義

258～265行目はネットワーク・インターフェースのオプションの定義です．

パケット・ライブラリには送受信インターフェースにオプション領域を指定できる機能がありますが，そこにミラーリング先のインターフェースを追加しています．入力パケットのミラーリングと出力パケットのミラーリングのそれぞれを定義しています．

● ミラーリングの出力処理

480～496行目の`send_packet_mirror_in()`と`send_packet_mirror_out()`は，それぞれ入力パケットと出力パケットのミラーリング先への出力処理です．インターフェースのオプション領域を見

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できます．
`http://kozos.jp/books/interface/ethernet2/`