

パケットジェネレータの作成 (途中経過)

2015/7/16

藤田将輝

1 はじめに

libnet により作成したパケットが NIC ドライバで正常に処理されていないことを確認した．本資料では，その原因の調査の途中経過について述べる．正常に処理されるパケットと libnet によって作成されたパケットを比較し，原因の調査を行った．この結果，IPv4 ヘッダに差異が多く見られた．IPv4 ヘッダのみを正常に処理されるパケットと同じ値にしたところ，正常に処理されていることを確認した．

2 パケットジェネレータ

本デバッグ支援環境においてパケットジェネレータはデバッグ支援 OS 上で動作するアプリケーションとして実装する．パケットジェネレータはデバッグ対象 OS の NIC ドライバが処理するパケットを作成し，システムコールとして実装しているデバッグ支援機構を呼び出す機能を持つ．本資料において，パケットが正常に処理されるとは，パケットジェネレータを起動してから，デバッグ対象 OS 上の UDP を受信し，メッセージを表示するアプリケーションがメッセージを表示するまでの処理を行うこととする．パケットジェネレータの処理流れを図 1 に示し，以下で説明する．

- (1) デバッグ支援 OS でパケットジェネレータを動作させる．
- (2) パケットジェネレータにより，パケットが作成され，デバッグ支援機構が呼び出される．
- (3) デバッグ支援機構は作成されたパケットを共有メモリに配置する．
- (4) デバッグ支援機構がデバッグ対象 OS に割り込みを発生させる．
- (5) 割り込みハンドラが動作し，NIC ドライバはパケットを共有メモリからソケットバッファに格納する．
- (6) NIC ドライバはソケットバッファを上位層に送信する．
- (7) デバッグ対象 OS 上で動作する UDP の受信プログラムが UDP パケットを受け取る．
- (8) デバッグ対象 OS 上で動作する UDP の受信プログラムがメッセージを画面に出力する．

3 作成したパケットの処理

libnet により作成したパケットをデバッグ対象 OS の NIC ドライバに処理させた．具体的には，以下の流れで，処理を行った．

- (1) パケットを共有メモリに作成した NIC ドライバの受信バッファに配置する．
- (2) 受信ディスクリプタを更新し，デバッグ対象 OS の占有するコアへ IPI を送信する．

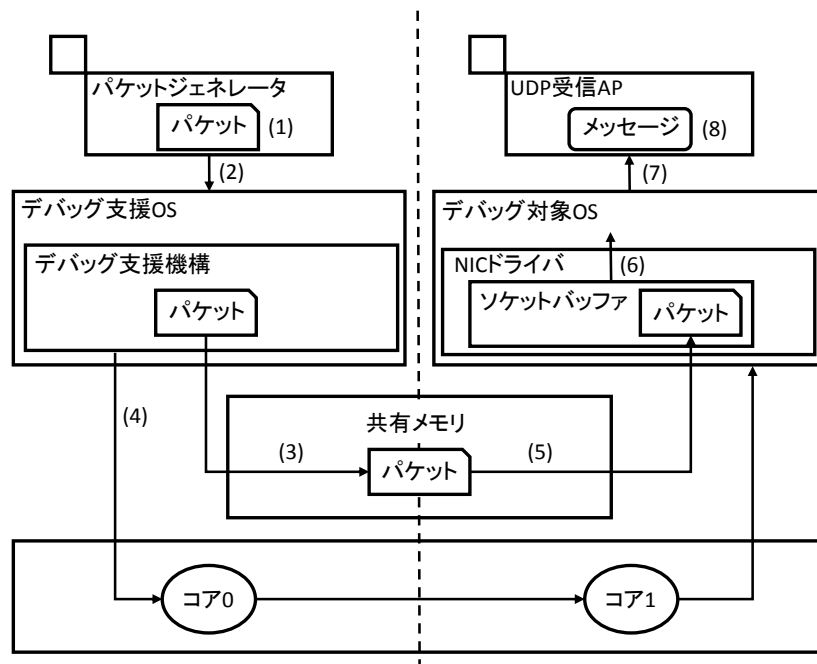


図 1 正常な処理流れ

- (3) デバッグ対象 OS の占有するコアが IPI を受信すると、NIC ドライバの割り込みハンドラが動作する。
- (4) 割り込みハンドラにより、共有メモリからパケットを取得し、パケット受信割り込み処理を行う。

以上の流れで作成したパケットを処理させた結果、正常に処理されていなかった。具体的には、デバッグ対象 OS 上で動作する UDP のメッセージを取得し、表示するアプリケーションに何も表示されていなかった。これにより、パケットは正常に処理されていないと判断した。

4 原因の調査

libnet により作成したパケットが正常に処理されない原因について調査している。本章では、この途中経過について説明する。なお、正常に処理されないパケットと、正常に処理されるパケットの値を比較することで調査を行った。作成したパケットには、以下の 3 つのヘッダが付与されている。

- (1) Ether ヘッダ
- (2) IPv4 ヘッダ
- (3) UDP ヘッダ

これらのヘッダによってパケットの処理が決定するため、これらのヘッダに不具合の原因があると考えた。また、Ether ヘッダと UDP ヘッダについてはヘッダを構成する要素が少なく、作成したパケットと正常に処理されるパケットで大きな差異がなかったため、IPv4 ヘッダの構成に不備があると考え、調査を行った。正常に動作するパケットのヘッダと、正常に動作しないパケットのヘッダで異なっていた

のは以下の要素である．

(1) データグラム長

IP パケット全体のサイズを示す要素である．

(2) ID フィールド

フラグメントが発生した際に使用される識別子をもつ要素である．

(3) フラグフィールド

フラグメントを行うか否かを示す要素である．

(4) チェックサム

IPv4 ヘッダのチェックサムの要素である．

(5) 送信元 IP アドレス

送信元の IP アドレスを表す要素である．

これらの値を全て正常に動作するパケットと同様の値に変更すると，パケットは正常に処理されることを確認した．どの要素が原因で正常に動作しないのかは特定できていない．今後，どの要素が不具合の原因となっているか調査し，その理由について考察する．

5 おわりに

本資料では，libnet によって作成されたパケットが正常に処理されない原因についての調査について述べた．今後は IPv4 ヘッダのどの要素が原因かを特定し，その理由について調査し，考察する．その後，パケットジェネレータを完成させる．