RTL8169 の過去のバグについて

2016/6/15

藤田将輝

1 はじめに

開発支援環境を用いて，過去あった NIC をドライバのバグを再現することを考えている．Linux カーネルは Git を用いて開発されており，開発過程が全て記録として残っている．本開発環境での開発対象である NIC ドライバ (RTL8169) の開発過程も記録されており，どのようなバグが修正されてきたかを確認可能である．そこで，この記録から修正されたバグを調査した．本資料は，調査したバグについてまとめたものである．

2 調査目的

本研究における開発支援環境は NIC ドライバを対象としており，NIC を用いずに NIC の動作を再現するものである．これを用いて，報告されたバグを再現できれば，本環境がデバッグにおいて有用である可能性を示せる．そこで，過去に修正されたバグを調査し，現在の開発支援環境で再現できるかを考察する．また，現在の開発支援環境にどのような機能を追加すればバグを再現するかを考察する．これらの目的からバグについて調査した．

3 調査方法

本開発支援環境の開発対象としている RTL8169 は Linux カーネルの一部として Git を用いて開発されている．このため，開発工程が全て記録として残っている．この記録はある機能を追加した，あるバグを修正した，といった作業の粒度で記録されており，そのメッセージが残されている．そこで，本開発環境が対象としているバージョンの最新の更新記録から過去 3 年間のバグを調査した．バグを修正したメッセージには「fix: 」という文字列が含まれているため，この文字列を含むメッセージの記録を調査した．この際，ハードウェアに依存した修正や詳細が記述されていない修正は調査対象外とした．

4 発見したバグ

Linux3.0.8 の最新更新記録から過去 3 年間のバグを調査した．その一覧を以下に示す．

(1) チェックサムをチェックするタイミングに関するバグ

NIC ドライバは受信したパケットのチェックサムをチェックし，問題なければ上位層でチェックする必要が無いことを示すフラグをセットする．この処理は受信したパケットがソケットバッファに複写された後に実行されることが期待されているが，パケットの複写前に実行されている

ため，チェックする処理が無駄になっている．

(2) あるサイズ以上のパケットを受信できないバグ
RTL8169 では，MTU は受信バッファのサイズを計算するために使用されている．受信バッファサイズはハードウェアのパケットフィルタを設定するために使用されている．修正前の実装は多くの MTU は 1536B であるのに関わらず，受信バッファサイズも 1536B とされている．Ethe ヘッダが 22B あるため，IP パケットのサイズが 1536-22B のものは全てフィルタで破棄されてしまう．

(3) 大きなサイズのパケットを受信した場合，マシンをクラッシュさせるバグ
受信可能なパケットサイズよりもアロケートしている受信バッファの方が小さいという事があり得る記述をしているため発生するバグである．受信したパケットが受信バッファより大きい場合，アロケートしたメモリを超えて配置してしまい，カーネルの領域を侵害する．

5 考察

5.1 チェックサムをチェックするタイミングに関するバグ

このバグはパケットの処理流れに関するものであるため，再現は容易であると考えられる．現在の実装を変えず実現できると考えられる．このバグを確認するには，バグの発生するコードでパケットを処理させ，全てのデータのチェックサムフラグがセットされていないことを確認することで行える．

5.2 あるサイズ以上のパケットを受信できないバグ

このバグは，ハードウェアのフィルタリングを用いている可能性がある．このため，このフィルタリング機能を開発支援 OS に実装する必要がある．共有メモリを用いて，NIC ドライバの設定を開発支援 OS に渡す方法が考えられる．

5.3 大きなサイズのパケットを受信した場合，マシンをクラッシュさせるバグ

このバグは自由にパケットのサイズを調整可能な本開発環境を用いることで再現可能であると考えられる．受信バッファのサイズを大きく超えるデータを配置することで挙動を確認する．

6 おわりに

本資料では，過去に修正された NIC ドライバのバグについてまとめた．今後は，バグを再現するための具体的な課題や対処について検討する．