調査したバグの再現について

2016/7/13

藤田将輝

1 はじめに

＜new 304-04＞において，RTL8169 の過去のバグについてをまとめた．本資料では，＜new 304-04＞に挙げた 3 つのバグを本開発支援環境で再現する際の設計について述べる．具体的には，各バグを再現するにあたっての課題，対処，およびバグの確認方法について述べる．

2 目的

本環境を用いて NIC を用いず過去に発生した NIC ドライバのバグを再現する．これにより，NIC を用いた場合よりも少ない工数でバグを再現できることを示す．

3 再現するバグ

再現するバグとその概要を以下に示す．

(1) チェックサムを確認するタイミングに関するバグ
受信したパケットのチェックサムを確認するタイミングを誤っているため，チェックサムの確認が不要なパケットであってもすべてのパケットに対してチェックサムを確認してしまうバグである．

(2) 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
アロケートしたバッファサイズよりも大きなパケットの受信を許してしまうことにより，カーネル空間を侵害し，システムをクラッシュさせる可能性があるバグである．

(3) 特定のサイズのパケットを受信できないバグ
パケットのフィルタリング機能とアロケートするバッファサイズの関係に不一致があることにより，受信可能であるはずのサイズのパケットまでフィルタにより破棄されてしまうバグである．

4 各バグを再現する際の開発支援環境の設計

4.1 概要

各バグを再現するには，NIC ドライバをバグが報告されているバージョンに戻し，このバージョンに対して開発支援環境を構築する必要がある．それぞれのバグが発生するバージョンの NIC ドライバに開発支援環境を構築し，バグを再現する際に発生する課題，対処，およびバグの確認方法についてを以

降で示す．

4.2 チェックサムを確認するタイミングに関するバグ

4.2.1 課題と対処

本バグが発生する NIC ドライバのバージョンと開発支援環境を実装した NIC ドライバのバージョンとでは，開発支援環境の構築に関して特筆すべき差異が無かった．このため，現在構築している NIC ドライバのバージョンと同様の改変を加えることにより，バグを再現できると考えられる．

4.2.2 確認方法

本バグは IP 層でチェックサムの確認の必要がないパケットであっても全てチェックサムを確認してしまうバグである．本バグの確認方法を以下に示す．

(**確認方法**) 上位層に送信される直前のソケットバッファをキャプチャし，`skb->ip_summed` が `CHECKSUM_NONE` であることを確認する．これにより，バグが発生していることが分かる．

4.3 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

4.3.1 課題

本バグを再現するにあたっての課題を以下に示す．

(**課題** 1) 受信バッファのアロケート方法の変更

本バグが発生する NIC ドライバのバージョンと開発支援環境を構築している NIC ドライバのバージョンとでは受信バッファのアロケート方法が異なっている．開発支援環境を構築している NIC ドライバのバージョンでは，受信バッファのサイズは固定である．一方，本バグが発生するバージョンでは，指定した MTU によって受信バッファのサイズが変化する．開発支援環境では共有メモリに受信バッファを確保する．この際，開発支援 OS では，受信バッファのサイズは固定されたものとしてパケットを配置する．このため，本バグを再現するには，NIC ドライバが確保したバッファのサイズを開発支援 OS が知る必要がある．

4.3.2 対処

課題に対しての対処について以下に示す．なお，課題番号と対処番号は対応している．

(**対処** 1) 共有メモリを用いたバッファサイズの通知

NIC ドライバが受信バッファを確保した際，そのサイズを共有メモリを用いて開発支援 OS に通知する．開発支援 OS は通知されたバッファサイズに従って受信バッファのエントリを算出し，パケットを配置する．これにより，正しい位置にパケットを配置することができる．

4.3.3 確認方法

本バグは，アロケートした受信バッファサイズよりも大きいサイズのパケットを受信することでシステムがダウンするバグである．バグの確認方法について以下に示す．

(**確認方法**) 開発支援 OS で，受信バッファよりも大きなパケットサイズを指定し，送信する．これにより，システムが停止し，バグが発生することを確認する．

4.4 特定のサイズのパケットを受信できないバグ

4.4.1 課題

本バグを再現するにあたっての課題を以下に示す．

(**課題** 1) 受信バッファのアロケート方法の変更

4.3.1 項の (課題 1) と同じ．

(**課題** 2) レジスタの動作の再現

本バグは，ハードウェアのパケットフィルタの動作によって発生する．パケットフィルタは RxMaxSize レジスタに受信可能なパケットサイズの最大値を指定することで，その値よりも大きなサイズのパケットを破棄する．開発支援環境では NIC ハードウェアを用いないため，RxMaxSize レジスタに値を指定しても，パケットはフィルタリングされない．このため，開発支援 OS でパケットフィルタ機能を再現する必要がある．

4.4.2 対処

課題に対しての対処について以下に示す．なお，課題番号と対処番号は対応している．

(**対処** 1) 共有メモリを用いたバッファサイズの通知

4.3.2 項の (対処 1) と同じ．

(**対処** 2) 共有メモリを用いたフィルタ機能の再現

RxMaxSize レジスタを共有メモリに配置し，開発支援 OS と開発対象 OS で参照可能にする．これにより，開発支援 OS で RxMaxSize の値を確認することができる．開発支援 OS はパケットを受信バッファに格納する際，RxMaxSize の値を確認し，この値よりも格納しようとしているパケットサイズが大きい場合，パケットを格納せず，破棄する．

4.4.3 確認方法

本バグは，指定した MTU と同じサイズのパケットがフィルタ機能によって破棄されてしまうものである．バグの確認方法について以下に示す．

(**確認方法**) 開発支援 OS で MTU と同じサイズのパケットを指定し，動作させた際，NIC ドライバが

パケットを受信しないことを確認することで，バグを確認する．

5 おわりに

本資料では，各バグの再現についての設計を述べた．本資料の設計に基づいてバグを再現し，再現にかかったコードの変更量等を調査する．