

# 組み込み機器を用いた Ethernet フレーム制御端末の検討

佐々木 宏幸<sup>†</sup> 松田 勝敬<sup>‡</sup>

東北工業大学大学院工学研究科<sup>†</sup> 東北工業大学工学部<sup>‡</sup>

## 1. はじめに

我々は、LAN 内部の通信制御に特化したセキュリティシステムを、安価で実現する研究・開発を行っている<sup>[1][2]</sup>。システムは、LAN セグメント毎の通信制御を行う制御端末と、それらを一括管理する管理装置から構成される。制御装置を LAN 内に分散配置する事で、ネットワークを有効に制御し、セキュリティ向上を図っている。

システムの低コスト化を実現する為に、LAN セグメント毎の通信制御を行う端末に、安価な組み込み機器を用いた。これまでに、通信ポートを 1 つ搭載した組み込み機器 2 台をシリアル接続して実装を行い、検証を行った<sup>[2]</sup>。今回は、通信ポートを 2 つ搭載した組み込み機器に制御端末の機能を実装し、検証を行った。

## 2. Ethernet フレーム制御端末

LAN セグメント毎の通信制御を行う端末を Ethernet フレーム制御端末（以下制御端末）と呼ぶ。制御端末は、管理装置の命令に従い MAC アドレスに基づく通信制御を行う。

制御端末で得られたログの管理や、通信制御の判断等、リソースが多く求められる機能を、管理装置に一括して行わせる。これにより、制御端末を組み込み機器等の安価な機器で実装可能となる。その為、最小限の機能として、通過する通信の送受信と通信制御、管理装置へのログ送信、制御命令の受信のみを実装した。概要を図 1 に示す。

### 2.1 通信制御

通信制御として、全ての通信を許可・遮断、指定した送信元・宛先 MAC アドレスの通信を許可・遮断する 4 種類の機能を実装した。

指定した通信を許可・遮断する場合、制御する送信元・宛先 MAC アドレスの組が記録されたフィルタリストと、到着した Ethernet フレームとの比較を行う。送信元・宛先 MAC アドレスをバイト毎に比較し、MAC アドレスが一致しなくなった時点で次のフィルタリストと比較する。

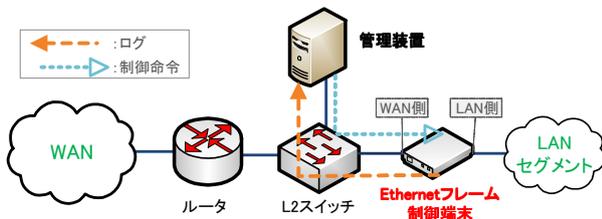


図1 Ethernetフレーム制御端末概要

搭載 CPU	AVR32 (AT32AP7000)
動作クロック	140MHz
Ethernet チップ	National Semiconductor 社 DP83848VV-VBI ×2
Ethernet 規格	10Base-T / 100Base-TX

### 2.2 ログの送信

管理装置へ送信するログは、通過する通信の送信元・宛先 MAC アドレス、タイプ、入出力ポート、フレーム長とした。これらの情報を Ethernet フレームの最小サイズである 64bytes としたデータ部に記述し、制御端末で通信を送受信する度、1 つのログを管理装置に送信する。制御端末を通過した通信の到着時間は、ログが管理装置に到着した時刻とし、管理装置側で時刻をとる。

## 3. 組み込み機器への実装

制御端末の機能を組み込み機器に実装した。実装した組み込み機器には、Atmel 社製の NGW100<sup>[3]</sup>を用いた。構成を表 1 に示す。Ethernet チップが 2 つ実装されており、それぞれ 100Mbps までの通信に対応している。また OS として Linux が実装でき、Atmel 社で提供されている Linux(kernel2.6.27.6.atmel.1)を実装した。

実装にあたって、Linux 上で動作する制御端末のアプリケーションを作成した。このアプリケーションを、AVR32 マイコン向けのコンパイラ avr32-linux-gcc にてコンパイルを行い実装した。コンパイルのオプションとして、最適化レベル 3 を適用した。

## 4. スループットの検証

組み込み機器に実装した L2 通信制御装置の性能を検証する為、RFC2544<sup>[4]</sup>に基づくスループット測定を行った。

### 4.1 検証環境

図 2 に検証環境を示す。テスターのポート 1、ポート 2 よりテストフレームを 60 秒間送信し、ポート 2、ポート 1 でそれぞれ受信する。これを繰り返し、テストフレームの損失がない最大値を求める。送信するテストフレーム長が 64, 128, 256, 512, 1024, 1280, 1518bytes についてそれぞれ 5 回測定を行い、平均値を DUT(Devices under test)<sup>[4]</sup>スループットとした。

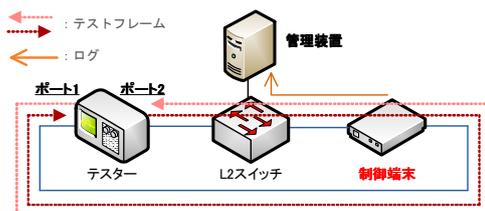


図2 スループットの検証 検証環境

A study of Ethernet Frame Control Terminal Using Embedded System

<sup>†</sup> Hiroyuki Sasaki, Graduate School of Engineering, Tohoku Institute of Technology

<sup>‡</sup> Masahiro Matsuda, Faculty of Engineering, Tohoku Institute of Technology

## 4.2 検証項目

通信制御を行わない場合と、行う場合の2つについて検証を行う。

制御命令を行わない場合は、制御端末に到着した通信を通過させる処理のみを行い、純粋な DUT スループットを測定する。通信制御を行う場合は、指定した通信を遮断する命令を与え、100組の送信元・宛先 MAC アドレスを登録する。この送信元・宛先 MAC アドレスを変化させ、到着した通信と遮断する送信元・宛先 MAC アドレスを1~6bytesまで比較する場合について検証を行う。

## 4.3 検証結果

通信制御を行わない場合の DUT スループットを図3に示す。フレーム長が最小の時は1.18Mbps、最大の時は15.20Mbpsの通信能力を有する。1秒間に処理可能なフレーム数(fps)で見ると、フレーム長が最小の時に、2312個、最大の時は1251個のフレームを処理できる。

図4に、通信制御を行わない時の DUT スループットを基準とし、通信制御を行なった場合の DUT スループット減少率を示す。最大負荷時で14%程の減少率となっている。また単位時間に処理されるフレーム数が多い程、通信制御による影響を受けやすい。

## 5. 実ネットワーク環境での検証

実運用に耐えうる能力であるか、更なる検証を行う為、実ネットワーク環境での検証を行った。

### 5.1 検証環境

図1のLANセグメント内に、インターネットを利用する端末が5台存在する環境を想定する。端末5台から、WANに存在するインターネット上のWebページの閲覧を1分間行い、得られたログを基に検証を行う。閲覧するWebページは、①HD相当の動画を含む、②HDでない動画を含む、③制約なしの3種類とした。

### 5.2 検証結果

#### 5.2.1 フレーム長の分布

得られたログから、それぞれのWebページを閲覧した際のフレーム長の分布を求めた(図5)。どの種類のWebページを閲覧した場合でも、LAN側で0~99、WAN側で1400~1499の区間が殆どを占める。内訳を見ると、LAN側では64bytes、WAN側では1418bytesが9割以上であった。このことから、流れる通信はLAN側で64bytes、WAN側で1418bytesのフレーム長のものが偏って存在している事がわかる。

#### 5.2.2 通信量とDUTスループットの比較

5.2.1の結果から、LAN側は64bytes、WAN側では1418bytesの通信に注目する。得られたログから、LAN側

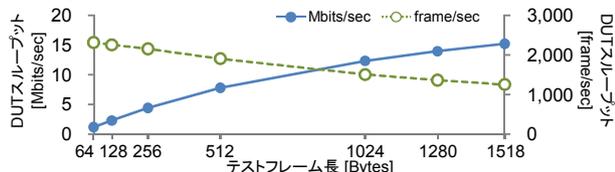


図3 通信制御を行わない場合のDUTスループット

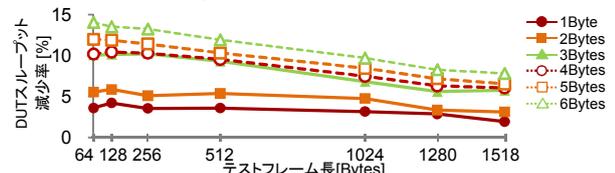


図4 通信制御を行った場合のDUTスループット減少率

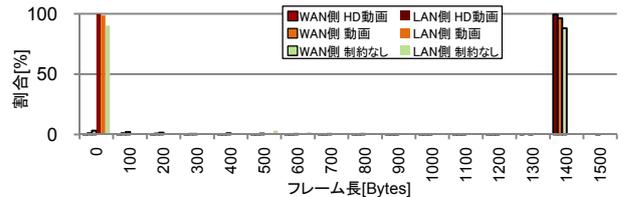


図5 Webページ閲覧時におけるフレーム長の分布

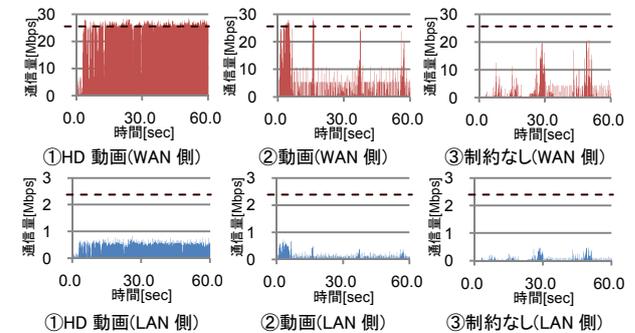


図6 通信量とDUTスループットの比較

は64bytes、WAN側は1418bytesのフレーム長の通信の0.1秒毎の通信量を求め、DUTスループットとの比較を行う。比較するDUTスループットは、図2においてテストフレームを片側から送信した時の値とし、64bytes時は2.2Mbps、1418bytes時は25.8Mbpsとなっている。図6に結果を示す。点線は、それぞれのDUTスループットを表す。動画閲覧時のWAN側では、HD動画閲覧時はほぼ常に、HDでない動画閲覧時にはバースト的にDUTスループットを上回っている事がわかる。制約なし閲覧の時は、WAN側、LAN側共にDUTスループットを上回る通信量は観測されなかった。

### 5.3 考察

数台の端末でHD動画閲覧の場合、制御端末の無い状態で端末のDUTスループットを超える40~60Mbpsの通信量がある。図6の①HD動画(WAN側)のグラフから、DUTスループットを超える通信量が発生していると、常にDUTスループット前後の通信量となっており、端末がボトルネックとなっている事がわかる。しかし、この状態でも実際のWeb閲覧には支障がなく、数台の端末からなる環境では十分な性能であると考えられる。

## 6. まとめ

LANセグメント毎の通信制御を行う制御端末を、安価な組込み機器で実装し、性能の検証を行った。検証の結果、通信ポートを2つ搭載した組込み機器では、数台の端末からなる環境であれば、実運用可能であると思われる。

### 参考文献

- [1] 佐々木宏幸, 松田勝敬: 分散型通信制御セキュリティシステムの開発, 第8回情報科学技術フォーラム第4分冊, pp.133-134(2009).
- [2] 佐々木宏幸, 松田勝敬: 分散型通信制御セキュリティシステムの組込み機器への実装に関する考察, 情報処理学会創立50周年記念(第72回)全国大会 講演論文集(分冊3), pp.379-380(2010).
- [3] Atmel Corporation: Atmel Products-AVR Solutions-Mature NGW100 Network Gateway Kit, Atmel(オンライン), 入手先<[http://www.atmel.com/dyn/products/tools\\_card.asp?tool\\_id=4102](http://www.atmel.com/dyn/products/tools_card.asp?tool_id=4102)>.
- [4] S.Bradner, J.McQuaid: RFC2544 - Benchmarking Methodology for Network Interconnect Devices, IETF,IETF(オンライン), 入手先<<http://www.ietf.org/rfc/rfc2544.txt>>.