Vol.2019-CSEC-85 No.2
Vol.2019-IOT-45 No.2
2019/5/23

未使用IPアドレススキャンによるルータの負荷増加への対策法の実現

佐藤 聡[1,a)]　玉林 亜喬[1]　三宮 秀次[1]　登 大遊[2]　松本 智[2]

概要：ネットワーク機器の性能向上により，ルータに直接接続されているサブネット数は増加している．この未使用 IP アドレスに対する ARP 解決処理がルータの負荷を増加させている．我々は，未使用だとわかっている IP アドレスに対して，特定の 機器の MAC アドレスをルータの ARP テーブルに書き込むことにより，必要以上の ARP 解決が行われない方法を提案している．本研究では，提案方法の実装方法を提案し，プロトタイプシステムを用いた実験を行い，提案手法の有効性を示す。

キーワード：PING スィープ，ネットワーク管理，ルータ，ARP

Implementation of a counter method of unused IP address sweep for router

Abstract: The number of subnetworks direct-connected to a router is increased by performance improvement of network equipment. The load of a router by which ARP resolved processing to the unused IP address is also increasing. We have proposed a method witch the route adds an entry for the unused IP address with specific MAC address in order to reduce the number of times of the processing for APR packet. In this paper, we propose an implementation method of the proposed method, perform experiments using a prototype system, and show the effectiveness of the proposed method.

Keywords: PING Sweep, Network system operation, router, arp

1. はじめに

ルータの処理能力の向上により，多くのサブネットワークを 1 つのルーターに接続するネットワーク構成を採用することが可能となった．ルータ数を削除することによりコストを削減できるため，組織内のネットワーク構成においては，一つのルータに接続されるサブネットワーク数は増加している．

IP アドレス設計では，サブネットマスクの大きさは，そのサブネットに接続できる機器数の上限値を定めることになる．IP アドレス設計時に，接続される機器数を見積もることが難しい場合は，サブネットマスクの大きさは大きめに設計される．そのため，運用時には，未使用 IP アドレスが存在することになる．

したがって，一つのルータにおいて，管理する IP アドレスの中に，未使用 IP アドレスが多数存在する．ルータにおいては，何らかの理由により未使用 IP アドレス宛のパケットを受け取ると，ARP 解決 [2] を行う処理が実行される．そのため，未使用 IP アドレス数が多くなると，ARP 解決処理の実行回数も多くなり，その結果，ルータが過負荷になってしまう．

このような状況において，未使用 IP アドレスに対するスキャンが頻繁に行われると，ルータに対して未使用 IP アドレス宛のパケットが多数到達することになり，その結果ルータが過負荷状態となる．

我々は，未使用 IP アドレスに対して必要以上に行われているルータの ARP 解決の回数を削減する方法として，未使用だとわかっている IP アドレスに対して，特定の機器の MAC アドレスをルータの ARP テーブルに書き込む方法を提案した [3].

[1] 筑波大学
University of Tsukuba, Tsukuba, Ibaraki, 305–8577, Japan
[2] 情報処理推進機構
Information-technology Promotion Agency
[a)] akira@cc.tsukuba.ac.jp

本研究では，その提案に基づいたシステムの実装方法を示し，プロトタイプシステムによる実験結果、および、その時に新たにわかった問題点を示す．

2. 問題定義

本研究が対象とするネットワーク環境では以下に示す要件を想定している．

- サブネットワークに接続できる情報機器（ IP アドレスが割り振られる情報機器）の数に余裕を持たせる方針でサブネットワークの大きさを決定している．
- ネットワーク機器数を減らすために，ルータ数が減っている．そのために一つのルータに直接接続されるサブネットワーク数が増加している．
- ルータは，直接接続されている全てのサブネットワークにおいて，全ての IP アドレスが使われたとしても十分に処理できるだけの性能を有している．具体的には全ての IP アドレスが使われた時の ARP エントリーを全て収容できるだけの ARP テーブルの大きさを有している．
- ルータが制御（ルーティング）する IP アドレスは IP v4 アドレスとする．
- ARP 解決処理はハードウェア処理されていないため，スイッチング処理・ルーティング処理と比較して，ルータにとって負荷のかかる処理である．

この想定を満たすネットワーク環境の例としては，2019 年 9 月現在の筑波大学のキャンパスネットワークが該当する．筑波大学では，学内の組織に対して，接続予定の情報機器数に応じて、26 ビットから 24 ビットまでのサブネットワークを割り当てている．ほぼ全てのサブネットワークの 1 つのルータに直接接続する構成となっている．

このようなネットワーク構成では，ルータにおいて，各サブネットワークの中で情報機器に割り当てられいない IP アドレスや，割り当てられていても使われていない IP アドレス（以下，これらのアドレスのことを 未使用 IP アドレスと呼ぶ）の数は増大している．一般的には，ルータにおいて 1 つの未使用 IP アドレスを宛先とするパケットが複数回受信すると，受信の都度 ARP 解決の処理が実行される．未使用 IP アドレス数が増加するとこのような処理が実行される回数も増大することになる．その結果，不要な ARP 解決が短時間に多数実行されることによりルータに負荷がかかる．ルータの負荷が高くなると様々な問題が発生する．問題の一例として，ルータのインタフェースに割り振られた IP アドレスに対する ping 応答が遅くなる・できなくなるといったことが発生する． ping によりサービスの確認を行っている場合には，これによりサービスの障害が発生していると誤検知されることとなる．

本研究では，ルータにおける，未使用 IP アドレスに対して必要以上に行われている ARP 解決の回数を削減することを研究目的とする．

3. 提案手法

本研究では，ルータにおける，未使用 IP アドレスに対して必要以上に行われている APR 解決の回数を削減する方法として，未使用だとわかっている IP アドレスに対して，特定の機器の MAC アドレスをルータの ARP テーブルに書き込む方法を提案する．

提案する方法の概要を以下に示す．

- ルータに直接接続されているサブネットワーク内部に解決装置を接続する．
- ルータからの ARP 要求パケットを解決装置が受信した場合，解決装置自身が ARP 要求パケット内に記載されている IP アドレスが未使用であるかを調査し，未使用 IP と判断した場合には，ルータに対して、未使用 IP アドレスを解決装置が利用しているものとして ARP パケットを送信することにより，ルータの ARP テーブルを制御する．

IP アドレスが未使用であるかの調査については，RFC5227[1] にて定義されている IPv4 アドレス競合検出の方法を用いる．

4. 設計

解決装置は，ルータと接続しているネットワークインタフェース以外に，この装置自身が遠隔監視されるための接続を行うネットワークインタフェースを有することが考えられる．しかし，この章では，解決装置は，ルータと直接接続しているネットワークインタフェース以外のネットワークインタフェースを有していないものとして記述する．

解決装置は，以下に示すルータの基本情報をあらかじめ記憶しておく．

- 直接接続されているサブネットワークのインタフェースに割り振られている IP アドレス．
- 直接接続されているサブネットワークのインタフェースに割り振られている MAC アドレス．

4.1 解決装置にて管理する情報

解決装置では，IP アドレスごとに，管理状態，その IP アドレスを利用されている MAC アドレスを保持することにする．管理状態としては以下の 3 種類を設定する．

- **USED** 当該 IP アドレスが利用中の状態を表す．その IP アドレスを利用している機器の MAC アドレスを記憶しておく．
- **CHECKING** 当該 IP アドレスが利用中であるかどうかを調査している状態を表す．
- **UNUSED** 当該 IP アドレスが未使用の状態を表す．この状態に遷移した場合には，当該 IP アドレスを利用している機器の MAC アドレスを不明とする．この

状態を初期状態とする．

4.2 解決装置が処理するパケット

解決装置は，装置自身のユニキャストパケット，及びブロードキャストパケットを受信できるものとする．解決装置が取り扱うパケットの種類は，ARP パケットのみとする．すなわち，解決装置は，ARP パケット以外のパケットは送受信処理は処理を行わない．

解決装置にて送受信する ARP パケットを Gratuitous ARP [1] を参考にして，以下の種類に分類する．

(1) ルータによる要求パケット．「sender IP address (送信元 IP アドレス)」にルータの IP アドレスが，「sender hardware address (送信元ハードウェアアドレス) 」にルータの MAC アドレスが設定されている ARP 要求 (ARP Request) パケット．
(2) 使用中パケット．「sender IP address (送信元 IP アドレス)」 に IP アドレスされている ARP 要求 (ARP Request) もしくは ARP 応答 (ARP Reply) パケット．ただし，ルータによる要求に分類されるパケットは除く．
(3) 探知パケット．RFC 5337 にて記載されている ARP Probe と同じ．「sender IP address (送信元 IP アドレス) 」 をすべてゼロに設定した ARP 要求 (ARP Request) パケット．
(4) ルータへの設定パケット．「sender IP address (送信元 IP アドレス)」に当該 IP アドレスを設定した ARP 要求パケット．

受信した ARP パケットのうち，処理を行うパケットは「ルータによる要求パケット」「使用中パケット」のみとし，パケットの種類に応じて上記の状態を遷移させるとともにいくつかの処理を行う．それ以外の ARP パケットを受信しても処理はしない．

送信するパケットは「探知パケット」と「ルータへの設定パケット」のみとする．

4.3 解決装置の処理

解決装置は，「ルータによる要求パケット」もしくは「使用中パケット」を受信した時に処理を実行する．処理の詳細を以下に示す．

4.3.1 「ルータによる要求パケット」に対する処理

解決装置が「ルータによる要求パケット」を受信した時は，ルータがそのパケットの「target IP address (送信先 IP アドレス) 」に設定されている IP アドレス に対して ARP 解決を行おうとしていると理解することができる．サブネットワークにて，当該 IP アドレスを利用している機器が存在する場合には，当該機器から ARP 応答があり，ルータの ARP テーブルに適切なエントリーが設定される．存在しない場合には，エントリーが設定されない．エントリーが設定されない時に，ルータが当該 IP アドレスへのパケットを受信する度に，転送するために ARP 解決を行うこととなる．

以上より，解決装置が「ルータによる要求パケット」を受信すると，そのパケットの「target IP address (送信先 IP アドレス) 」に設定されている IP アドレスが利用されているかどうかを調査するために，以下の処理を行う．ただし，当該 IP アドレスの管理状態が CHECKING である場合には何も処理を行わない．

(1) 管理状態を CHECKING に推移させる．
(2) 当該 IP アドレスが未使用であるかを調査する．

ここで，当該 IP アドレスが未使用であるかを調査する方法については，RFC 5227 の 2.1.1 節 ”Probe Details” [1] にて定義されている IP アドレスの利用の検知方法を用いる．その概要を以下に示す．

(1) 当該 IP アドレスを 「target IP address (送信先 IP アドレス)」に設定した「探知パケット」を PROBE_NUM 回送出する．ただし, 個々の送出の間に, PROBE_MIN 〜 PROBE_MAX の範囲から偏り無く選んだランダムな秒数だけ、待ち時間を設ける．
(2) 最後に「探知パケット」を送出して ANNOUNCE_WAIT 秒間待っていても，利用中パケットが届かない場合，この IP アドレスが未使用であると判断する．

ここで, PROBE_NUM, PROBE_MIN, PROBE_MAX, ANNOUNCE_WAIT の値は，RFC 5227 にて定義されている値を用いる．具体的には，PROBE_NUM は 3 回，PROBE_MIN は 1 秒，PROBE_MAX は 2 秒，ANNOUNCE_WAIT は 2 秒とする．なお，この調査方法により不要な ARP パケットを送出しないようにするために, 当該 IP アドレスの管理状態が CHEEKING となっている場合にのみ「検知バケット」の送出する．

この方法により未使用であると判断した場合には，以下の処理を行う．

(1) 管理状態を UNUSED に推移させる．
(2) IP アドレスを利用している MAC アドレスを不明とする．
(3) 「target IP address （送信先 IP アドレス)」にルータの IP アドレスを，「sender IP address (送信元 IP アドレス)」に当該 IP アドレスを設定した「ルータへの設定パケット」をルータに対してユニキャストで送信する．

4.3.2 「使用中パケット」に対する処理

解決装置が「使用中パケット」を受信した時は，そのパケットの「target IP address (送信先 IP アドレス) 」に設定されている IP アドレスが何らかの ARP 解決に対して応答を行なっている，あるいは，RFC 5227 によって当該 IP アドレスの利用の公知が行われていると解釈すること

ができる．前者には，4.3.1 節にて述べた IP アドレスが未使用であるかの調査方法における ARP 解決の応答が含まれる．解決装置がこの応答を受信した際には，調査により当該 IP アドレスが利用されていると判断できるため，その調査の処理を終了させる．

サブネットワーク内に「使用中パケット」が送出されている場合には，ルータもそのパケットを受信しており，ルータの ARP テーブルには正しいエントリーが設定されている．すなわち，解決装置はルータに対して新たな処理を行う必要はない．

以上のことから， 解決装置が「使用中パケット」を受信した時は，以下に示す処理を行う．

(1) 管理状態を USED に推移させる．
(2) 当該 IP アドレスについて，受信した「使用中パケット」の「 sender hardware address（送信元 MAC アドレス)」を MAC アドレスとして記憶する．

5. 実装

設計に基づいて，解決装置を Linux 上で動作可能なプログラムとして C 言語を用いて実装を行なった．

提案方式において，解決装置はルータに直接接続されている全てのサブネットワークに配置することになる．想定条件を考えると，多数の解決装置が必要となる．しかし，ルータと解決装置間の接続を IEEE 802.1 Q の Tagged-VLAN により接続し，解決装置が Tagged-VLAN を解釈することにより，1 台の解決装置にて問題を解決可能となる．本実装では，このための機能を取り入れた．

具体的には，解決装置が管理する IP アドレスごとの情報に，管理状態，MAC アドレスに加えて VLAN ID を加えた．ルータによる要求パケットを受け取り，このエントリーの管理状態が CHECKING に変更される際に，受け取ったパケットの VLAN ID を記憶する．また，解決装置が探知パケット，もしくは，ルータへの設定パケットを送信する際には，当該エントリーに格納されている VLAN ID をパケットにつけて送信する．

6. 実験

実装したプログラムを搭載した解決装置のプロトタイプシステムを用いて，提案方式の有効性を検証するための実験を行う．

実験を行う環境は，提案方式が想定している環境を模した環境とした．具体的には，24 ビットセグメントのサブネットが 11 個接続されているルータを実験の対象とした．実験の環境の概要を**図 1** に示す．

ルータは，Juniper Networks 社製 EX2200-48P-4G を用いた．11 個のサブネットはそれぞれルータの 1 ポート (ge-0/0/0 から ge-0/0/10 まで）を割り当てた．また，これらのポートのトラフィック量を SNMP を用いて採取し，

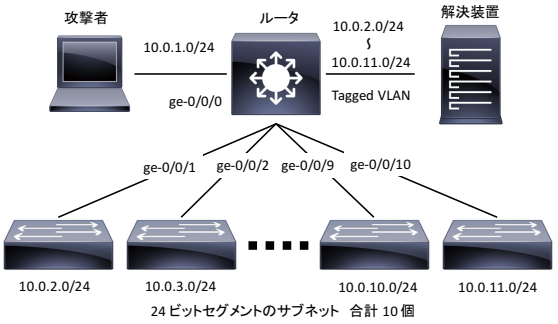

図 1 実験環境
Fig. 1 Experiment environment

```
#!/bin/bash

for c in {1..5}
do
  for i in {1..254}
  do
    for j in {2..11}
    do
      ping -c 1 -w 1 "10.0.$j.$i" &
      sleep 0.1
    done
  done
done
```

図 2 ルータへの攻撃の擬似シェルスクリプト
Fig. 2 Pseudo shell script for attacking routers

グラフにできるように設定した．

各サブネットワークにおいて，ルータに割り当てる IP アドレスは第 4 オクテットが 255 となるように設定した．11 個のサブネットのうちの 1 つサブネット（ 10.0.1.0/24 ）については，アップリンクという想定とし，ルータへの攻撃を行う機器（以下，攻撃者とよぶ）を接続した．攻撃者は残りの 10 個のサブネット（ 10.0.2.0/24 から 10.0.11.0/24 まで）に対して攻撃を行うこととした．またルータと解決装置は直接接続をし，これら 10 個のサブネットごとに VLAN ID を割り当てて Tagged VLAN として接続した．

攻撃者からは、設定した 10 個のサブネットのすべての IP アドレス宛に PING を送信するようにした。擬似攻撃として用いたシェルスクリプトを **図 2** に示す．このプログラムから，擬似攻撃は攻撃を開始してから終了するまでの時間は約 21 分間である．

解決装置を稼働させていない状態で攻撃者に擬似攻撃をさせたときと，解決装置を稼働させた状態で攻撃者に擬似攻撃をさせたときの双方で，ルータの各インタフェースの

トラフィック量を測定した．解決装置を稼働させていないときの結果を**図 3** に，解決装置を稼働させたときの結果を**図 4** に示す．

この実験では，アップリンクのサブネット以外の 10 個のサブネットについては，ルータに設定されてた　IP アドレス以外は未使用の IP アドレスとなっている．したがって，ルータは攻撃者から擬似攻撃として ping パケットを受け付けると，その IP アドレスを ARP 解決するために，サブネットが割り当てられているポートに対して APR パケットを送信する．解決装置が稼働していない場合には，擬似攻撃の ping パケットを受け付ける度に APR パケットが送信されることになる．

図 3 は，解決装置を稼働させていない場合の結果を示している．右側の一番上のグラフがアップリンクのサブネットワークが割り当てられているポート（ ge-0/0/0 ）のトラフィック量を表している．このブラフから，攻撃は 16 時 16 分ごろに開始し，16 時 38 分ごろに終了していることがわかる．それ以外のグラフは各サブネットワークが接続されているポートのトラフィック量を表している．攻撃が開始してから終了しているまで、1kbps 以上のトラフィックが送信されていることから，ルータが ARP パケットを送信し続けていることがわかる．

図 4 は，解決装置を稼働させている場合の結果を示している．この図でも，右側の一番上のグラフがアップリンクのサブネットワークが割り当てられているポート（ ge-0/0/0 ）のトラフィック量を表している．このグラフから，攻撃は 17 時 34 分ごろに開始し，17 時 55 分ごろに終了していることがわかる．この図でも，それ以外のグラフは各サブネットワークが接続されているポートのトラフィック量を表している．いずれのポートにおいても，17 時 42 分ぐらいにトラフィック量が 0 kpbs 程度となっている．このことから，ルータは　ARP パケットの送信をやめていることがわかる．このことから解決装置が正しく動作していることがわかる．

ただし，図 2 から，各サブネットへの擬似攻撃は約 4 分を単位として 5 回繰り返している．グラフより 2 回目には まだルータが ARP パケットが送信していることから，解決装置は 1 回目の擬似攻撃で対応しきれていないことがわかる．この原因は現在調査中であるが，なんらかの方法により 1 回目の擬似攻撃ですべて対応できるように改善を行う予定である．

7. 考察

プロトタイプシステムを用いた実験を行なうことにより，新たにわかった問題点について述べる．

今回ルータとして用いた機器は，MAC アドレステーブルにエントリーが追加され、設定されているエージングタイムの間，MAC アドレスを記憶している．このエージングタイムが終了する直前に，その MAC アドレス対して ARP パケットを ユニキャストにて送信し、利用されているかどうかを確認することがわかった．現在の設計では，解決装置は，ルータによる要求パケットを受け取ると、ルータはその IP アドレスが利用中であるかどうかわからないためと判断し，管理状態を CHECKING にして，解決装置自身も利用中かどうかの調査を始める．ルータがその IP アドレスが利用中かどうかの再確認を行う場合には ユニキャストで APP パケットを受け取り、利用中であるかの調査の際には，ブロードキャストで APR パケットを受け取るという違いがある．この違いに着目して，ルータからのユニキャストの ARP パケットについては、そのまま ARP 応答パケットを送信することにより、解決装置の負荷を低下させることができる．

8. おわりに

本論文では，すでに点案している未使用だとわかっている IP アドレスに対して，特定の機器の MAC アドレスをルータの ARP テーブルに書き込む方法の実装方法の提案を行い，プロトイプシステムを用いた実験を行い、提案方式の有効性を示した．

今後の課題としては，解決装置が単位時間に解決できる処理を増やす必要がある．今回の実験では，サブネット数を 10 個としたが，上限値がどれぐらいとなるかの調査も行う必要がある．また，ルータが管理している MAC アドレステーブルの維持のために発信する ARP パケットへの対応を行う必要がある．

謝辞

本研究を進めるにあたり，筑波大学学術情報メディアセンターにはネットワーク機器の貸与等，様々な支援を頂いた．ここに感謝の意を表する．

参考文献

[1] Cheshire, S.: IPv4 Address Conflict Detection, RFC 5227 (Proposed Standard) (2008).
[2] Postel, J. and Reynolds, J.: Telnet Timing Mark Option, RFC 860 (INTERNET STANDARD) (1983).
[3] 佐藤聡, 三宮秀次, 登大遊, 松本智：ルータに対する未使用 IP アドレススキャンの対策法，信学技報，Vol. 118, No. 240, pp. 5–8 (2018).

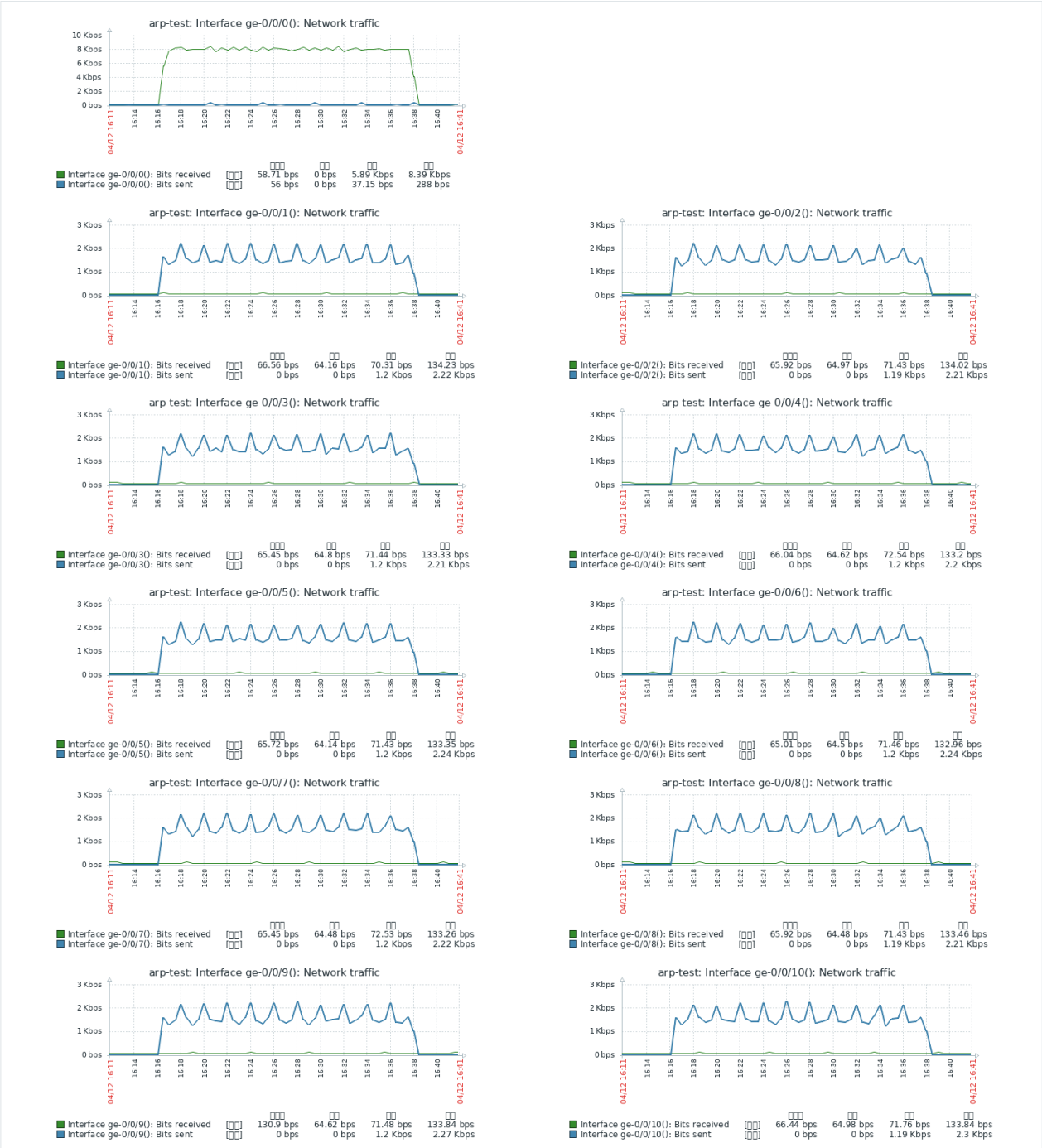

図 3 解決装置を使わない場合の実験結果

Fig. 3 Experiment Results without using Proposed System

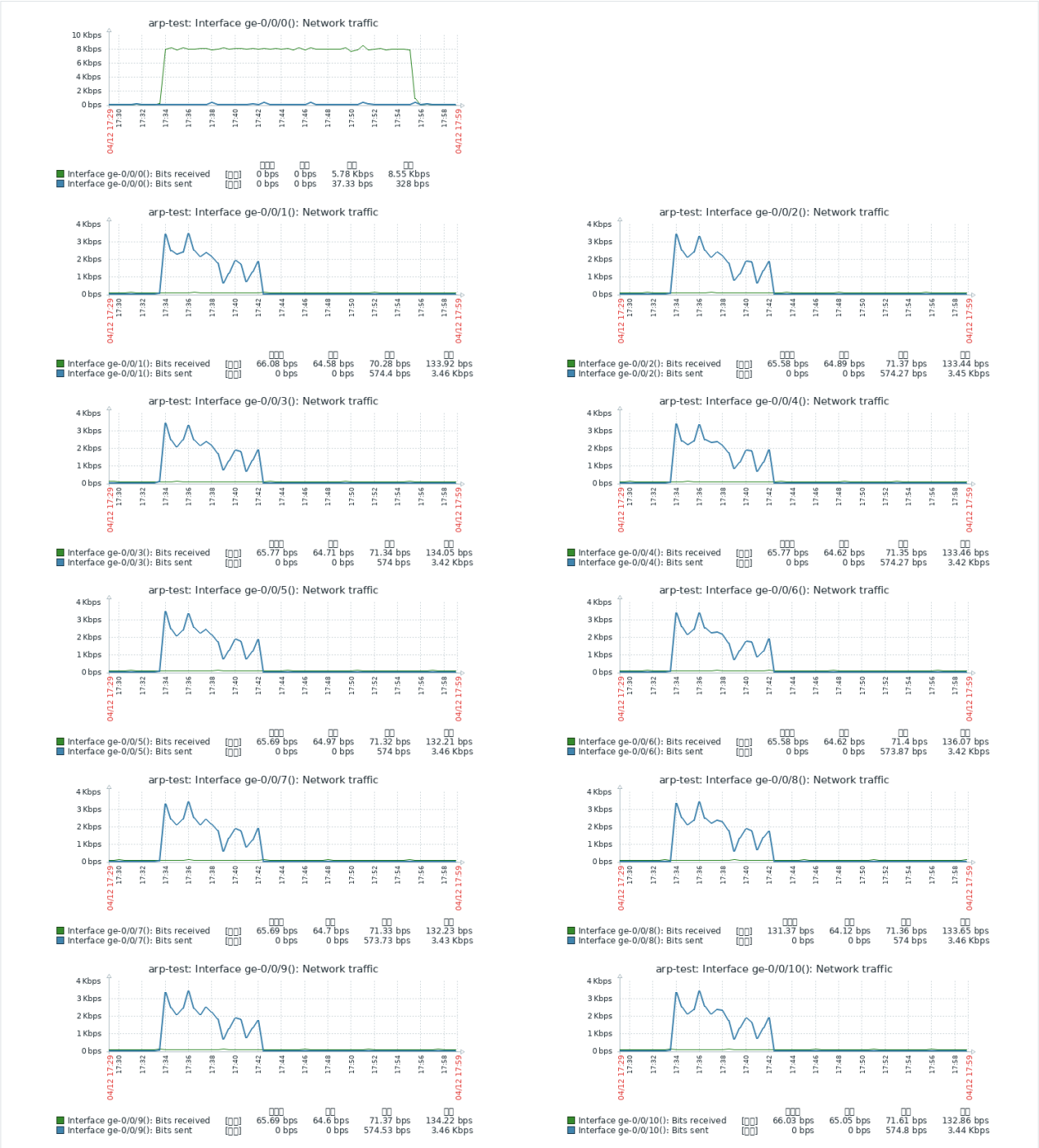

図 4 解決装置を使った場合の実験結果

Fig. 4 Experiment Results with using Proposed System