LAN内PCを外部から識別するための MACアドレス中継型NATルータ

村上 亮[†1] 岡山聖彦[†2] 山井成良[†2]

IPv4アドレスの枯渇問題の一時的な解決策の一つとして，NAT (Network Address Translation) がある．NATは複数のPCでIPアドレスを共用できるため，IPv4アドレスの節減やセキュリティ対策のために広く用いられている．しかし，NATルータより上位のネットワークにおいてIPアドレスなどに基づいてアクセス制御を行っている場合，NATルータの配下にあるPC（LAN内PC）のIPアドレスが隠蔽されるため，LANアクセス制御サーバはすべてのLAN内PCからのアクセスを同一のものと見做してしまう．そこで本研究では，データリンク層レベルでPCを識別するためのMACアドレスに着目し，LAN内PCのMACアドレスを外部に中継するNATルータを提案する．LAN内PCから送出されたパケットの送信元MACアドレスが転送時に保持されるので，上位ネットワークではMACアドレスに基づいて制御できるようになる．

A MAC-address Relaying NAT Router for PC Identification from Outside of a LAN

Ryo MURAKAMI,[†1] Kiyohiko OKAYAMA[†2] and Nariyoshi YAMAI[†2]

NAT(Network Address Translation) is well-known as one of the short-term solutions of IPv4 address exhaustion. NAT is a technique that shares a single IP address in several PCs, and is widely used for alleviating the IPv4 address exhaustion and as a security solution. However, when a backbone network has access control function for PCs based on their IP addresses, it can not identify the PCs under a NAT router since their original IP addresses are hidden by the NAT router. In this research, we focus on MAC address which identifies PC on datalink layer and propose a NAT router which relays the MAC address of PC inside of a LAN to the outside. Since the source MAC addresses of packets sent from PCs are preserved even after being relayed by the router, a LAN access control server outside of the router can still identify these PCs based on their MAC addresses instead of their IP addresses.

1. はじめに

近年のインターネットの普及に伴って，IPv4アドレスの枯渇が問題となっている．根本的な解決として，より大きなアドレス空間を持つIPv6アドレスへの移行が求められているが，既存のIPv4機器の置き換えを要するためさほど進んでいないのが現状である．この問題の一時的な解決策の一つに，NAT（Network Address Translation）[1] がある．NATはIPアドレスの変換技術であり，NAT機能を有するルータ（以下，NATルータ）は，配下のPCから外部に向けて発信されたパケットの送信元アドレスを特定のアドレス（多くの場合はNATルータのグローバルIPアドレス）に変換して中継する．NATルータ配下のPC(以下，LAN内PC) はNATルータのグローバルIPアドレスを共用できるため，グローバルIPアドレスの節減ができる．さらに，NATルータに特別な設定を施さない限り，NATルータの上位ネットワークからはLAN内PCに直接アクセスできないため，LAN内PCを外部から護る手法としても広く用いられている．

しかし，組織の基幹ネットワークなどで認証機能付きLANアクセス制御システムを導入し，送信元PCのIPアドレスなどに基づくアクセス制御を行っている場合，下位ネットワークにNATルータが存在すると問題が生じる．LAN内PCから送出されたパケットの送信元IPアドレスはすべて特定のアドレスに変換されるため，あるLAN内PCが認証に成功するとLANアクセス制御サーバはNATルータのグローバルIPアドレスをアクセス許可リストに登録する．こ

†1 岡山大学大学院自然科学研究科
Graduate School of Natural Science and Technology, Okayama University
†2 岡山大学総合情報基盤センター
Information Technology Center, Okayama University

のため，他の LAN 内 PC はすべて LAN アクセス制御サーバの認証を経ずに外部にアクセスすることが可能となってしまう．この問題は，LAN アクセス制御機能を持つ NAT ルータなどを利用し，NAT ルータ部分で LAN アクセス制御を行うことで回避できるが，大規模なネットワークである場合に管理の手間が増えてしまう．

そこで本研究では，この問題を解決するためにデータリンク層レベルで PC を識別するための MAC アドレスに着目し，LAN 内の PC から送信されたパケットに含まれる送信元 MAC アドレスをそのまま LAN 外へ中継する NAT ルータ（以下，MAC アドレス中継型 NAT ルータという）を提案する．通常であれば NAT ルータがパケットを外部に送出する際の送信元 MAC アドレスは NAT ルータの MAC アドレスとなるが，これを送信元 PC のものに変更することにより，上位ネットワークにある LAN アクセス制御サーバは LAN 内 PC を送信元 MAC アドレスに基づいて制御できるようになる．

以下，2 章では，想定するネットワーク環境を示し，従来の NAT ルータの概要と問題点について述べる．3 章で MAC アドレス中継型 NAT ルータの設計とその実装について述べた後，4 章でその動作確認実験について述べる．最後に，5 章で本論文をまとめる．

2. 従来の NAT ルータの問題点

本章では，想定するネットワーク環境を示した後，従来の NAT ルータの概要と問題点について述べる．

2.1 想定ネットワーク環境

本論文では，**図 1** のように組織のネットワークを各部署ごとなどで LAN を構築し，ある部署では NAT ルータを用いて部署内の LAN を構築しているような環境を想定する．この環境において，組織内にある全ての PC はコアルータを通じて組織外にアクセスするものとし，コアルータと各部署 LAN の間にルータまたはレイヤ 3 スイッチが存在しないものとする．このようなネットワーク環境は部署ごとにネットワークを構築している組織ではよく見られる．たとえば，コアルータを学部ごとに設置し，学科単位の LAN を NAT ルータを用いて構築しているような場合がこれに該当する．

2.2 NAT の概要

NAT は，1 つまたは複数の IP アドレスを LAN 内の PC で共用する技術である．特に，IP アドレスとポート番号の変換を行うものは NAPT（Network Address Port Translation）と呼ばれる．NAPT は，1 つの IP アドレスを同時に共用することができるため，一般的によく用いられている．

また，変換前アドレスと変換後アドレスの組情報を持つアドレス変換表にあらかじめ変換アドレスの組を

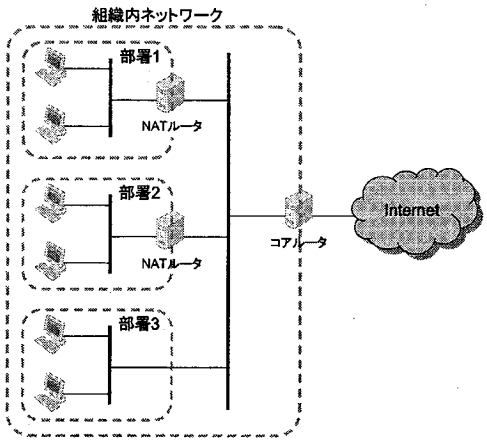

図 1 想定ネットワーク環境
Fig. 1 Assumed network environment

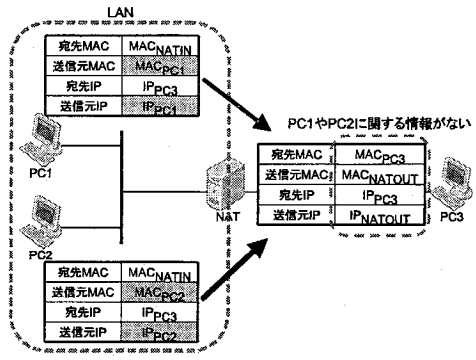

図 2 従来の NAT ルータの動作
Fig. 2 Process in conventional NAT router

登録することにより変換を行う NAT は静的 NAT と呼ばれる．静的 NAT を用いることで，アドレスが固定化されるため，LAN 外から LAN 内 PC にアクセスすることが可能となる．これに対し，LAN 外へのアクセス時に，動的にアドレス変換の登録を行う NAT は動的 NAT と呼ばれ，セッション終了と同時にその登録の解除を行う．そのため，LAN 外から LAN 内 PC へ直接アクセスすることができない．

以下，本論文では NAT/NAPT を総称して NAT と呼ぶことにし，動的 NAT を対象とする．

2.3 NAT ルータにおける問題点

NAT ルータが LAN 内の PC から外部へ向かうパケットを中継する際の，ヘッダ内の MAC アドレスと IP アドレスの変更の流れを**図 2** に示す．

NAT ルータは LAN 内の PC から受け取ったパケットを LAN 外へ送出する際，自身のネットワークインタフェースを利用するため，送出されるパケットに付与されるイーサネットヘッダの送信元 MAC アドレス

はNATルータの外向きインターフェースのMACアドレス（MAC_{NATOUT}）になる．PC1とPC2のアドレス変換前のヘッダ情報は互いに異なっているが，アドレス変換後にNATルータが送出するヘッダ情報には，PC1やPC2に関する情報が一切なく，NATルータ自身が送出するパケットとして全く同じものとなってしまう．結果的に，NATルータはLAN外に対してLAN内のPCに関する情報を隠すことになる．

このため，組織の基幹ネットワークなどの上位ネットワークでLANアクセス制御サーバを導入し，IPアドレスあるいはMACアドレスに基づくアクセス制御を行っている場合，以下のような問題が生じる．ここで，LANアクセス制御サーバとはPCのネットワーク接続時に利用者認証を行い，認証に成功したPCのみに対してアクセスを許可するサーバであり，ファイアウォール機能を動的に利用してアクセス制御を行う．

例えば，図2のPC3がLANアクセス制御サーバである場合，LAN内のPC1が外部にアクセスしようとすると，PC3で認証が行われ，認証に成功すれば通常はPC1のIPアドレスあるいはMACアドレスがPC3のアクセス許可リストに登録されるが，途中にNATルータが介在しているため，実際に登録されるのはNATルータのグローバルIPアドレスあるいはMACアドレスである．さらに，PC2が外部へのアクセスを試みると，PC2から送信されるパケットの送信元IPアドレスおよびMACアドレスはNATルータのものに変換されるため，PC3は許可済であると見做して認証することなくパケットを通過させてしまう．この問題は，LANアクセス制御機能を持つNATルータなどを利用し，NATルータの部分でLANアクセス制御を行うことで回避できると考えられる．しかし，上位ネットワークにおいて組織内の全PCのアクセスを集中的に管理するような場合，組織内の全NATルータに対してアクセスログなどの管理を委ねることになったり，ログ転送機能を利用してもトラフィックが増加したりするため，大規模なネットワークでは管理をする上で好ましくない．

3. MACアドレス中継型NATルータの設計と実装

2章で述べたように，従来のNATルータは上位ネットワークにおいてLANアクセス制御を行う場合に問題が生じる．そこで，本章では，この問題点を解決するためのMACアドレス中継型NATルータの設計とその実装について述べる．

3.1 実現方針

前章で述べた問題を解決するためには，LAN外に配置されたサーバがLAN内PCからのアクセスを正しく識別する仕組みが必要となる．

そこで本論文では，**図3**のようにLAN内のPCから受け取ったフレームのイーサネットヘッダ内にある送信元MACアドレスを変更せずに，そのままLAN外へ中継するNATルータを提案する．LAN外へ送出するフレームにLAN内のPC（PC1, PC2）のMACアドレス（MAC_{PC1}, MAC_{PC2}）が付与されることにより，LAN外にあるPC（PC3）はそのMACアドレスを参照することで，LAN内のPC（PC1, PC2）のアクセスを識別することができる．逆方向，つまりLAN外からLAN内へ向かうフレームに対してはこのMACアドレスの中継は行わず，通常のNATルータと動作は変わらない．これにより，NAT機能の利点である，LAN内PCの外部ネットワークからの保護とグローバルアドレスの節減を提供しつつ，LAN外からLAN内PCの識別を実現することができる．

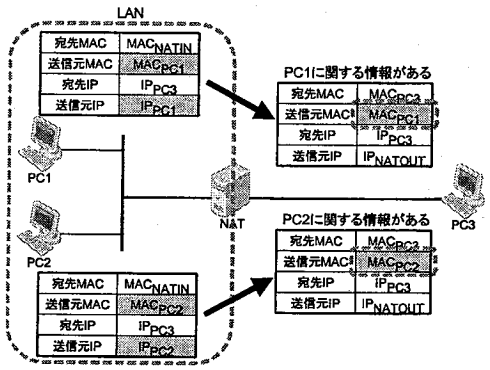

図3 MACアドレス中継型NATルータの動作
Fig. 3 Process in MAC address relaying NAT router

NATはIPデータグラムのIPアドレスおよびTCP/UDPポート番号を変換する技術なので，一般的にデータリンク層の情報（MACアドレス）を保持していない．そのため，提案するMACアドレス中継型NATルータには，以下の機能が必要となる．

- 送信元MACアドレスの取得機能
- イーサネットヘッダへの書込み機能

まず，送信元MACアドレス取得機能を使用してLAN内PCから受信したフレームのイーサネットヘッダ内から送信元MACアドレスを取得する．そして，アドレス変換を行った後，取得したMACアドレスをイーサネットヘッダへの書込み機能を使用してイーサネットヘッダ内の送信元MACアドレスに代入し，宛先PCに対してこのフレームを送出する．

本研究では，FreeBSDにNAT機能を提供する標準的なプログラムであるnatd[2]にMACアドレスを中継する機能を追加した．以下，実装したMACアドレス中継型NATルータについて詳しく述べる．

3.2 送信元MACアドレス取得機能

FreeBSDではNATルータのインタフェースが受信したフレームは，インタフェースドライバからカーネルを経由してファイアウォールモジュールに渡される．

次に，ファイアウォールモジュールによって NAT 機能を提供するプログラムへ IP データグラムがリダイレクトされる．このとき，natd がファイアウォールモジュール（IPFW[3]）から IP データグラムを受信する時点でイーサネットヘッダが取り除かれているので，受信したフレームから直接に送信元 MAC アドレスを取得することができない．一方，libpcap[4] と呼ばれる UNIX 系 OS 用のパケットキャプチャライブラリを用いるとイーサネットヘッダの情報の読み書きが出来るが，受信する全てのフレームを取得すると処理に時間がかかり，スループットが極端に低下してしまう．

そこで，本実装では natd が IP データグラムを受信する機構とは別に，送信元 MAC アドレスを取得するために必要最小限のフレームを libpcap により取得する機構を追加した．natd にはセッション毎の情報をまとめているアドレス変換表が用意されているため，取得した送信元 MAC アドレスをこのアドレス変換表に追加登録しておき，フレームの送出時にはこれを参照することで適切な送信元 MAC アドレスを求めることが出来る．

上述した必要最小限のフレームとは，送信元 MAC アドレスの取得とセッションの特定のみに利用するフレームのことである．TCP の場合ではコネクション確立要求時のフレーム，つまり TCP ヘッダ内に SYN フラグを有するフレームのみ取得すればよく，セッションの特定にはトランスポート層ヘッダまでを取得できればよい．libpcap によるフレームの取得を必要最小限にすることで，オーバヘッドの大幅な削減を図っている．

3.3 イーサネットヘッダへの書込み

一般的に，PC が送出する IP データグラムは，カーネルによる経路制御を経てインタフェースのドライバに渡されるが，このとき，カーネルは送出するインタフェースに割り当てられた MAC アドレスをイーサネットヘッダ内の送信元 MAC アドレスフィールドに書き込む．

通常，NAT ルータは送信元 MAC アドレスとして自身の MAC アドレスを使用するため，これを LAN 内 PC の MAC アドレスに変更する必要があるが，natd は FreeBSD の divert[5] を利用して IP データグラムを送出するプログラムなので，そのままではイーサネットヘッダを直接的に操作することができない．そこで本実装では，前節の送信元 MAC アドレス取得機能と同様にイーサネットヘッダへの書込み機能として libpcap を利用した．

3.4 動作手順

実装した MAC アドレス中継型 NAT ルータの内部構成を**図 4** に示す．LAN 内 PC からフレームを受信してから LAN 外へ送出するまでの動作手順は以下のようになる．なお，カッコ内は図 4 の番号に対応している．

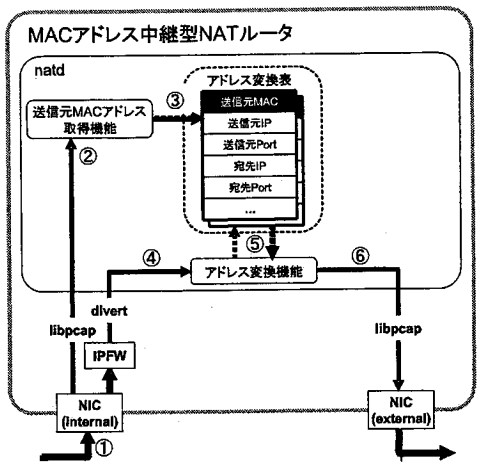

図 4 実装した MAC アドレス中継型 NAT ルータの内部構成
Fig. 4 Inside architecture of MAC address relaying NAT router

(1) LAN 内 PC からのフレームを内向きインタフェースから受信する．(①)
(2) 受信フレームが送信元 MAC アドレスの取得に必要なフレームであれば，libpcap によるフレームの取得を行い，セッションを特定して送信元 MAC アドレスをアドレス変換表に登録しておく．(②，③)
(3) IPFW により divert socket を通過して natd に IP データグラム部分が渡される．(④)
(4) 送信元 IP アドレスおよび送信元ポート番号をアドレス変換表に基づいて NAT 変換を行う．さらに，手順 2 で登録しておいた送信元 MAC アドレスもアドレス変換表から取得する．(⑤)
(5) 手順 4 で取得した送信元 MAC アドレスをイーサネットヘッダの送信元 MAC アドレスフィールドに書き込み，libpcap により外向きインタフェースに送出する．(⑥)

4. 動作確認実験

本章では，試作した MAC アドレス中継型 NAT ルータの動作確認実験について述べる．

4.1 実験環境と方法

MAC アドレス中継型 NAT ルータの動作確認および実用性の検証を行うため，以下の実験を行った．

4.1.1 PC 識別実験

LAN 内 PC を NAT ルータの外部から識別することができるか確認するために，LAN アクセス制御システムとして Opengate[6] を MAC アドレスに基づいてアクセス制御を行うように拡張したものを利用した．本実験では LAN アクセス制御システムと実装し

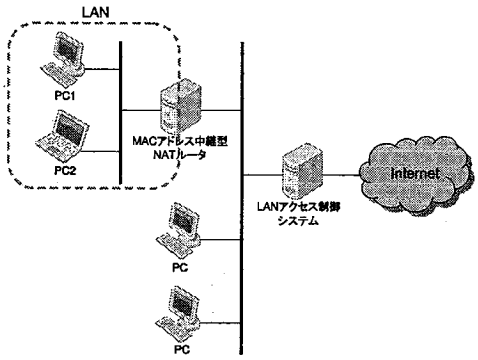

図 5 LAN アクセス制御システムを用いた PC 識別実験環境
Fig. 5 Experimental network for PC identification with LAN access control system

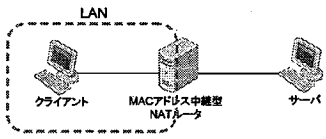

図 6 各種 OS の ARP テーブル確認実験環境
Fig. 6 Experimental network for confirmation of ARP table within various OS

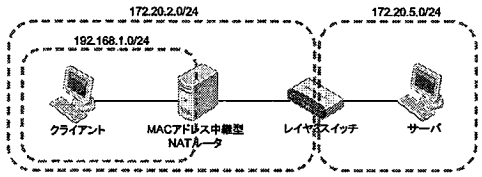

図 7 レイヤ 3 スイッチの ARP テーブル確認実験環境
Fig. 7 Experimental network for confirmation of ARP table within Layer 3 switch

たMACアドレス中継型NATルータを図5のように構成し，LAN内PCの識別が行えるか実験を行った．

4.1.2 ARP テーブル確認実験

2章で述べたように，LAN内PCが従来のNATルータを介してLAN外へアクセスする際，NATルータのネクストホップに到着するフレームの送信元MACアドレスと送信元IPアドレスはいずれもNATルータのものとなる．しかし，MACアドレス中継型NATルータを介する場合，ネクストホップには送信元MACアドレスはLAN内PCのもの，送信元IPアドレスはNATルータのものであるフレームが到着する．もし，ネクストホップがこのフレームに基づいてARPテーブルのエントリを更新した場合，ネクストホップからMACアドレス中継型NATルータへフレームを送信する際に宛先MACアドレスがLAN内PCのものとなる．ところが，MACアドレス中継型NATルータは宛先が自身のMACアドレスではないためにこのフレームを受け取らず，LAN外からLAN内への通信に支障をきたす恐れがある．

このような不具合がないかを確認するため，以下に示すOSが動作するPCをLAN外にサーバとして用意し，図6のようなネットワークを構成して実験を行った．

- Windows Vista Business Edition
- Windows XP Professional Edition SP3
- Windows XP Home Edition SP3
- Windows 2000 Professional Edition SP4
- MacOS X Version 10.5.1 (Leopard)
- KNOPPIX Edu2 (Kernel 2.4)
- Ubuntu 8.04 (Kernel 2.6)
- FreeBSD 7.0-RELEASE

さらに，NATルータと接続されたLAN外のレイヤ3スイッチ（アラクサラ社のAX3630-24T）を介してアクセスする際に，レイヤ3スイッチのARPテーブルに不具合がないかを確認するため，図7のようにレイヤ3スイッチを配置して実験を行った．

4.1.3 性能評価実験

図6と同様の実験環境を用意し，クライアント（FreeBSD7.0, Pentium4 2.4GHz, メモリ 512MB）からMACアドレス中継型NATルータ（FreeBSD7.0, Pentium4 2.0GHz, メモリ 1024MB）を介してサーバ（Ubuntu8.04, Pentium4 3.0GHz, メモリ 2048MB）へTCPコネクションを確立し，500MBのデータを送信する実験を100回行い，平均転送速度を算出した．なお，全ての機器は100Base-TXのイーサネットで接続しており，データの送信にはnttcp[7]を利用した．

4.2 実験結果と考察

PC識別実験では，LAN内のPC1およびPC2がLAN外にアクセスしようとしたとき，いずれもLANアクセス制御システムから認証を求められることを確認した．これは，LAN外にあるLANアクセス制御システムがPC1およびPC2のMACアドレスに基づいて正しく識別していることを意味する．

次に，ARPテーブル確認実験では，今回使用したすべてのOSおよびレイヤ3スイッチのARPテーブルにMACアドレス中継型NATルータのIPアドレスとMACアドレスの組が登録され，通信に支障をきたさないことを確認した．これは，各カーネルがホスト要求RFC[8]の記述に従って，ARPパケットによりARPテーブルを更新しているためと考えられる．ただし，ARPパケットではなく，各フレームのイーサネットヘッダの送信元MACアドレスを基にARPテーブルを更新するような機器では不具合が出ると考えられるため，今後さまざまな機器を用いて検証する必要がある．

最後に，性能評価実験の結果を表1に示す．通常のNATルータと比して，MACアドレス中継型NATルータを介する場合の転送速度の低下は0.06Mbpsで

表 1 性能評価実験結果
Table 1 Result of performance evaluation

NAT ルータ種別	平均転送速度 (Mbps)
通常の NAT ルータ	93.92
MAC アドレス中継型 NAT ルータ	93.86

あり，MAC アドレス中継による通信速度への影響は誤差の範囲である．

4.3 周辺機器への影響

通常，送信元 MAC アドレスはルータを介すると変更されるため，MAC アドレス中継型 NAT ルータを用いるアクセス制御の適用可能な範囲は MAC アドレス中継型 NAT ルータの内側と外側のセグメントに限られる．さらに上位のネットワークで送信元 MAC アドレスに基づいてアクセス制御を行うには，MAC アドレス中継型 NAT ルータ同様に送信元 MAC アドレスを中継するルータが必要となるが，その実装は容易であると考えられる．

MAC アドレス中継型 NAT ルータから多くの異なる送信元 MAC アドレスが送出されるため，上位ネットワークに MAC アドレス学習機能を持つレイヤ 2 スイッチ (スイッチングハブ) が存在する場合，その MAC アドレステーブルには多くの送信元 MAC アドレスが登録されることになる．しかし，最近の市販レイヤ 2 スイッチの MAC アドレスエントリ数は十分大きく，MAC アドレス中継型 NAT ルータが送出する送信元 MAC アドレスの数はレイヤ 2 スイッチに置き換えた場合と同じなので，規模に見合ったレイヤ 2 スイッチであれば，溢れなどの問題は発生しにくいと思われる．また，MAC アドレス中継型 NAT ルータは自身の MAC アドレスを送信元 MAC アドレスとして送らないため，ネクストホップのレイヤ 2 スイッチでは MAC アドレステーブルのキャッシュエントリがタイムアウトし，応答パケットを送る際に全ポートに対して ARP 要求を送るということが発生しやすくなる．この問題は，MAC アドレス中継型 NAT ルータから Gratuitous ARP のようなフレーム (送信元 MAC アドレスが MAC アドレス中継型 NAT ルータのものであればよい) を定期的に送出し，強制的にレイヤ 2 スイッチの MAC アドレステーブルを更新させることで回避できる．

5. むすび

本研究では，NAT ルータ配下の PC を外部ネットワークから識別するために，LAN 内 PC からのフレームに付与されている送信元 MAC アドレスを LAN 外へと中継する NAT ルータを設計した．さらに，PC を利用して MAC アドレス中継型 NAT ルータを実装し，動作確認実験により LAN 外に設置した LAN アクセス制御システムが MAC アドレスを用いて LAN 内 PC を識別できることを確認した．

今後の課題として，さまざまな機器への影響の検証や，今回は小規模な環境での実験であったため NAT ルータ配下および中継先の PC 数を増やしての検証を行うことが挙げられる．また，MAC アドレス中継型ルータの実装を行い，MAC アドレス中継型 NAT ルータと組み合わせた環境での検証も今後行いたい．

参考文献

1) P. Srisuresh, K. Egevang: "Traditional IP Network Address Translator (Traditional NAT)," RFC3022, 2001.
2) Archie Cobbs, Charles Mott, Eivind Eklund, Ari Suutari, Dru Nelson, Brian Somers, Ruslan Ermilov: "natd – Network Address Translation daemon," FreeBSD Kernel Interfaces Manual, 2003.
3) Ugen J. S. Antsilevich, Poul-Henning Kamp, Alex Nash, Archie Cobbs, Luigi Rizzo: "ipfw – IP firewall and traffic shaper control program," FreeBSD System Manager's Manual, 2007.
4) Steven McCanne, Craig Leres and Van Jacobson: "pcap - Packet Capture library," `http://www.tcpdump.org/`.
5) Archie Cobbs: "divert – kernel packet diversion mechanism," FreeBSD Kernel Interfaces Manual, 2004.
6) 渡辺義明, 渡辺健次, 江藤博文, 只木進: "利用と管理が容易で適用範囲が広い利用者認証ゲートウェイシステムの開発," 情報処理学会論文誌, Vol.42, No.12, pp.2802-2809, 2001.
7) Bill Fumerola: "nttcp - new test TCP Program," `http://www.freebsd.org/cgi/url.cgi?ports/benchmarks/nttcp/pkg-descr`.
8) Robert Braden: "Requirements for Internet Hosts," RFC1122, 1989.