情報処理学会論文誌 Vol. 52 No. 3 1348–1356 (Mar. 2011)

内部ネットワーク上のホストを外部から識別するためのMACアドレス中継型NATルータ

山井成良[†1] 村上亮[†2]
岡山聖彦[†1] 中村素典[†3]

IPv4アドレスの枯渇問題の軽減策の1つとして，NAT（Network Address Translation）がある．NATは複数の内部ホストが1つのグローバルIPアドレスを共用できるため，必要なグローバルIPアドレスの数を節約できる．しかし，外部ネットワーク側では個々の内部ホストを識別できないため，たとえば外部ネットワーク側でアクセス制御を行うと，1台の内部ホストが外部ネットワークに対するアクセス許可を受けただけで他の内部ホストまで外部ネットワークにアクセス可能な状態になるなどの問題が生じる．そこで，本論文ではデータリンク層での送信元識別子である送信元MACアドレスが基本的にはレイヤ2機器のMACアドレス学習機能にしか使われていない点に着目し，内部ホストから送信されたフレームに含まれる送信元MACアドレスをそのまま外部ネットワーク側に中継する機能を持つNATルータを提案する．本提案に基づいて試作したNATルータを評価した結果，MACアドレスに基づいて内部ホストを個別にアクセス制御でき，また十分なスループットが得られることを確認した．

A MAC-address Relaying NAT Router for Host Identification from Outside of Internal Network

Nariyoshi Yamai,[†1] Ryo Murakami,[†2]
Kiyohiko Okayama[†1] and Motonori Nakamura[†3]

As an alleviation method against IPv4 address exhaustion problem, NAT (Network Address Translation) has been commonly used. Since NAT allows many internal hosts to share one single global IP address, it can save the number of required global IP addresses. However, with NAT, each internal host cannot be identified from the external network. Consequently, if access control system on external network would permit network access from one internal host, it automatically would permit all network access from any other internal hosts as well, for example. In this paper, we propose a NAT router with MAC address relaying function that copies the source MAC address of receiving frames sent by internal hosts into frames sent to the external network since source MAC addresses, which are the sender identifiers in data link layer, are basically unused except for MAC address learning function of layer 2 switches. According to the results of experiments, we confirmed that the prototype NAT router with MAC address relaying function allows access to external networks by internal hosts to be controlled individually based on MAC address and obtains high throughput as well.

1. はじめに

最近，インターネットの急速な普及にともない，IPv4（Internet Protocol version 4）アドレスの枯渇が問題となってきている．この問題の根本的な解決策として，大きなアドレス空間を持つIPv6（Internet Protocol version 6）の導入がある．しかし，IPv6はIPv4と互換性がなく，また技術面や運用面で様々な課題が残されているため，あまり導入が進んでいないのが現状である．これに対して，この問題の軽減策としてネットワークアドレス変換（NAT：Network Address Translation）[1)]がよく用いられている[⋆1]．この技術を用いれば，プライベートIPアドレスを持つネットワーク（内部ネットワーク）に接続された複数のホスト（内部ホスト）がグローバルIPアドレスを持つネットワーク（外部ネットワーク）上の任意のホスト（外部ホスト）と通信する際に1つのグローバルIPアドレスを共用することが可能となり，これにより必要なグローバルIPアドレスの数を節約することができる．

ところが，NATには，(a) 利用できるプロトコルに制限があったり内部ホストへの通信が行えなかったりするなど，NAT機器を経由した通信に制限が生じる（通信制限問題），(b) 複数の内部ホストが同一のグローバルIPアドレスを共有しているため，外部ネットワーク側からみると個々の内部ホストを識別することが困難である（アドレス隠蔽問題），などいくつかの問題が存在する．このうち，アドレス隠蔽問題はネットワーク管理上重大である．すな

†1 岡山大学情報統括センター
Center for Information Technology and Management, Okayama University
†2 岡山大学大学院自然科学研究科
Graduate School of Natural Science and Technology, Okayama University
†3 国立情報学研究所
National Institute of Informatics

⋆1 ネットワークアドレスだけでなくポート番号も変換する技術はNAPT（Network Address Port Translation）と呼ばれる場合があるが，本論文ではNATとNAPTを総称して単にNATと呼ぶ．

わち，外部ネットワーク側で IP アドレスや MAC アドレスに基づいてアクセス制御を行っている場合，個々の内部ホストを識別できないため，1 台の内部ホストが外部ネットワークに対するアクセス許可を受けると他の内部ホストまで外部ネットワークにアクセス可能な状態になる．以下，本論文ではアドレス隠蔽問題に焦点を絞って議論を進める．

この問題へ対処する従来の方法として，NAT 機能を持つ機器（NAT ルータ）でアクセス制御を行う方法（方法 1），アプリケーション層プロトコルの認証機能を用いる方法（方法 2）などが存在する．このうち，方法 1 は通常用いられる方法であるが，アドレスの節約効果が高い大規模なネットワークでは多数の NAT ルータを個別に管理する必要があるため，管理コストが増大する点が問題となる．また，方法 2 は HTTP におけるアクセス認証[2] や cookie 認証[3] などが該当する．しかし，この方法は特定のアプリケーションのみに適用可能であり，すべての通信には適用できない点が問題である．このように，従来の方法はいずれも問題がある．

そこで，本論文では上記の問題を解決するために，送信元ホストのデータリンク層での識別子である送信元 MAC アドレスが一部の用途にしか使われていない点に着目し，内部ホストから送信されたフレームに含まれる送信元 MAC アドレスをそのまま外部ネットワーク側に中継する機能（MAC アドレス中継機能）を持つ NAT ルータ（MAC アドレス中継型 NAT ルータ）を提案する．これにより，外部ネットワーク側では IP アドレスの代わりに MAC アドレスにより送信元内部ホストを特定できるようになり，外部ネットワーク側で集約的にアクセス制御を行うことが可能になる．

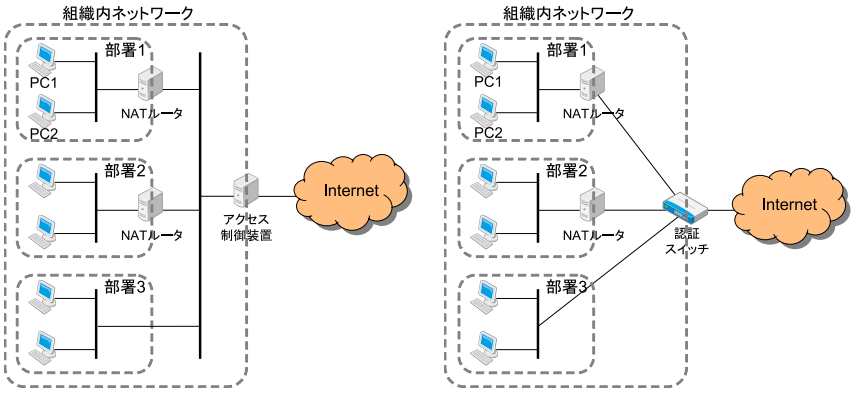
以下，2 章では，想定するネットワーク環境を示し，従来の NAT ルータの問題点について述べる．また，3 章では MAC アドレス中継型 NAT ルータの設計とその実装について述べた後，4 章でその機能および性能の評価結果について述べる．最後に，5 章で本論文をまとめる．

2. NAT ルータとその問題点

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

本論文で想定するネットワーク環境を**図 1** に示す．図 1 (a) は複数の部署から構成される組織において部署ごとに LAN を設置し，すべてあるいは一部の部署が NAT ルータを用いて上位の組織内ネットワークに接続されているような環境を表している．また図 1 (b) は



(a) アクセス制御装置を用いた環境　　(b) 認証スイッチを用いた環境

図 1　対象となるネットワーク環境
Fig. 1　Target network environment.

図 1 (a) のアクセス制御装置の代わりに認証機能付きレイヤ 2 スイッチあるいは同機能付きレイヤ 3 スイッチ（以下，両者をまとめて認証スイッチと表記）が存在し，すべてあるいは一部の部署が NAT ルータを用いて部署内の LAN を上位の組織内ネットワークに接続されているような環境を表している．このような構成の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比較的多く見られる．たとえば大学の学科においてアクセス制御装置を含む組織内ネットワークの共通部分は学科の管理者が管理運用し，研究室単位で管理される内部ネットワークを NAT ルータを介して組織内ネットワークに接続しているような場合がこれに該当する．なお，このようなネットワーク環境では NAT ルータはアクセス制御装置や認証スイッチと管理主体が異なる場合がある点に注意する．すなわち，アクセス制御装置や認証スイッチは組織内ネットワークの管理者が運用を行うのに対して，NAT ルータは部署内ネットワークの管理者が導入および運用を行い，組織内ネットワークの管理者が NAT ルータの存在に気付かない場合もある．

このようなネットワーク環境において，アクセス制御装置や認証スイッチは何らかのユーザ認証機能を持ち，ユーザ認証に成功したホストからの通信のみを MAC アドレスあるいは IP アドレスに基づいて許可するように動作するものとする．MAC アドレスや IP アドレスは偽装が比較的容易であるため，セキュリティ的に強いアクセス制御方法とはいえず，不正アクセスを許す可能性がある．しかし，ユーザ認証と組み合わせることにより，認証前

にアドレスを偽装したとしても偽装されたアドレスと認証されたユーザ名を関連付けることにより不正アクセスを行ったユーザを特定することが可能であり，またユーザ認証後に認証済みの他のホストの持つ MAC アドレスや IP アドレスに偽装した場合でも，同一のアドレスを持つホストが同時に複数存在することになり，容易に検出可能であることから，セキュリティ的にそれほど弱いアクセス制御方法ともいえず，実際にこのようなアクセス制御は多くの組織で広く用いられている．

2.2　アクセス制御における NAT ルータの問題点

図 1 の環境では 2 つの図でアクセス制御を行う位置が異なるが，機能的にはどちらも同じであるため，以下の議論では特に断りのない限り図 1 (a) の環境について議論する．この図において部署 1 に所属する 2 台の端末 PC1，PC2 が同時期に外部ネットワークにアクセスする場合を考える．簡単化のため，各端末から外部ネットワークへのパケットについてのみ議論の対象とする．

NAT ルータは内部ネットワーク側からパケットを受信すると，送信元 IP アドレス[*1]を NAT ルータの外部ネットワーク側 IP アドレス（外部側 IP アドレス）IP_{NATOUT} に変換して外部ネットワーク側に中継する．その際，NAT ルータが送出するフレームでは送信元 MAC アドレスとして NAT ルータの外部ネットワーク側インタフェースの MAC アドレス（外部側 MAC アドレス）MAC_{NATOUT} が使われる．したがって，**図 2** に示すように，アクセス制御装置から見ると NAT ルータが中継したパケットの発信元（PC1 あるいは PC2）を送信元 IP アドレスや送信元 MAC アドレスに基づいて識別することができない．その結果，部署 1 内の端末のうちいずれか 1 台が利用者認証などにより外部ネットワークへのアクセスを許可されると，他の端末は認証を受けなくても外部ネットワークにアクセスできるようになる．

この問題は，アクセス制御機能を NAT ルータ自身に持たせることにより回避することができ，たとえば Opengate[4] など NAT 機能付きアクセス制御装置が実際にいくつか存在する．しかし，図 1 のような環境では，各部署で個別に NAT 機能付きアクセス制御装置を導入する必要があり，組織内ネットワーク全体を対象とした集中的なアクセス制御が困難になる点が新たな問題になる．また，これによりアクセスログなどの管理情報も分散化するため，特に NAT ルータの管理者と組織内ネットワークの管理者が異なる場合にはたとえばインシデント発生時の追跡調査に管理者間の協調が必要になるなど，組織全体での管理の手間が増大する点も問題である．

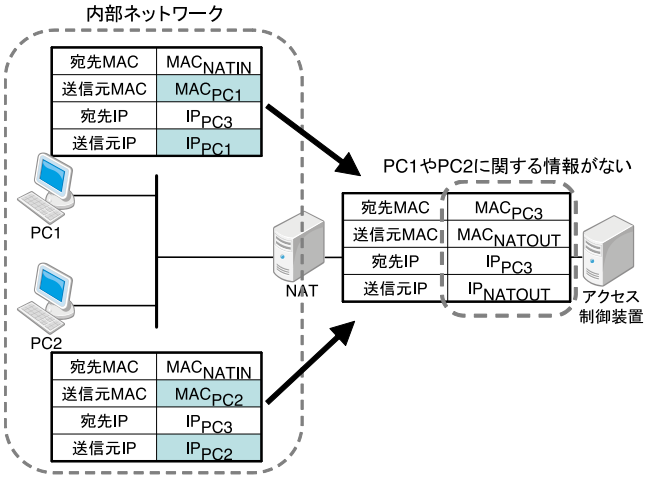


図 2　従来の NAT ルータの動作
Fig. 2　Process of conventional NAT router.

3. MAC アドレス中継型 NAT ルータ

2 章で述べたように，従来の NAT ルータでは外部ネットワーク側でアクセス制御を行う場合に様々な問題が生じる．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

上記の問題の根本的な原因は，NAT ルータが外部ネットワーク側に送出するフレームではアドレス変換により内部ホストを識別可能な情報が失われてしまう点にある．そこで，NAT ルータが内部ホストの識別情報を何らかの形式で付加したうえでパケットを中継すれば上記の問題を解決できると思われる．

内部ホスト識別情報を付加する方法はいくつか考えられるが，これらは以下の 2 種類に分類できる．

(1)　フレームやパケットの形式を拡張して新たに内部ホスト識別子を設定するフィールドを設ける方法．
(2)　フレームやパケットの既存フィールドを流用して内部ホスト識別子を設定する方法．

⋆1 NAPT では送信元ポート番号も変換の対象であるが，以下の議論では簡単化のため省略する．

このうち，(1) はたとえば IP ヘッダの新たなオプションとして内部ホスト識別子を設定する方法が考えられる．しかし，その場合 NAT ルータが外部ネットワーク側に中継するパケットでは付加されるオプションの分だけ内部ホストに対する見かけ上の MTU（Maximum Transfer Unit）が減少し，その結果フラグメンテーションが必要になったりスループットが低下したりするなどの問題が発生する可能性がある[5),⋆1]．また，内部ホスト識別子を設定したフレームやパケットを扱えなかったり，あるいはそれらを廃棄したりする機器が存在する可能性もある．一方，(2) は流用する既存フィールドを本来の目的で使用しないか，あるいは流用しても本来の目的に悪影響を及ぼさないことを保証する必要があるが，パケットサイズはまったく増大せず，上記の問題は発生しない．流用可能なフィールドとしては VLAN タグあるいは送信元 MAC アドレスがあげられるが，前者はネットワークの構成によっては流用できないのに対して後者は事実上レイヤ 2 機器における中継先ポートの学習にしか利用されておらず，このフィールドを流用しても大きな影響がないと思われる．

そこで，NAT ルータにおいて内部ネットワーク側インタフェースで受信したフレームに含まれる送信元 MAC アドレスを内部ホスト識別情報として扱い，アドレス変換したパケットを外部ネットワーク側に出力する際にはこれをそのまま中継する方法を提案する．これにより，外部ネットワーク側のアクセス制御装置では送信元 MAC アドレスに基づいて個々の内部ホストを識別し，アクセス制御を行うことが可能になるので，前章で述べた問題を解決できる．また，送信元 MAC アドレスがそのまま中継されることから，同アドレスに基づいて動作する既存のシステムを多くの場合そのまま利用することが可能になる．たとえば図 1 (b) のような環境において，認証スイッチが MAC アドレスに基づいてアクセス制御を行っていれば，組織内ネットワークには何ら変更を加えることなく，ユーザ認証に成功した内部ホストだけにアクセスを許可したり，マルウエアに感染した疑いのある内部ホストを MAC アドレスを指定してアクセスを禁止したりできるようになる．ただし，NAT ルータと認証スイッチとの間（図 1 (a) では NAT ルータとアクセス制御装置との間）に他のレイヤ 3 機器が存在するような環境や IP アドレスのみに基づいてアクセス制御を行う装置においては，本方法を適用しても個々の内部ホストを識別したアクセス制御ができないことに注意する．

⋆1 たとえば，MTU が 1,500 バイトのイーサネット環境において MTU に等しいペイロードを送出した場合，8 バイトの IP オプションの追加によりフラグメンテーションが発生すると，18 バイトのイーサネットヘッダとチェックサムおよび 20 バイトの IP ヘッダが新たに必要になるため，合計で 46 バイト分（約 3%）のオーバヘッドが発生する．

なお，送信元 MAC アドレスの中継により，一般的には通信元ホストが第三者に知られてしまう可能性が生じる．しかし，送信元 MAC アドレスが中継される範囲は NAT ルータの外部ネットワーク側インタフェースと同一のレイヤ 2 ネットワーク内に限られ，図 1 (a) の環境では部署 3 のホストと同一の条件であるため，多くの場合には問題にならないと思われる．もし何らかの理由でこれが許容できない場合には，NAT ルータにおいて内部ホストの MAC アドレスを適当な鍵で暗号化するなど推測困難な別のアドレスに変換し，これを送信元 MAC アドレスとして中継することにより，個々の内部ホストの識別はできるが特定はできないようにすることも可能である．

3.2　MAC アドレス中継型 NAT ルータの動作

MAC アドレス中継型 NAT ルータの動作を以下に示す．

まず，内部ネットワークから外部ネットワーク宛のフレームを中継する場合の MAC アドレス中継型 NAT ルータの動作を**図 3** に示す．内部ホスト PC1 から送出されたフレームを受信すると，NAT ルータは送信元 IP アドレスを NAT ルータの外部側 IP アドレス IP_{NATOUT} に変換し，さらに送信元 MAC アドレスは PC1 のアドレス MAC_{PC1} をそのまま使用したフレームを作成して外部ネットワーク側に送出する．一方，別の内部ホスト PC2 から送出されたフレームを受信すると，NAT ルータは同様に送信元 IP アドレスを IP_{NATOUT}

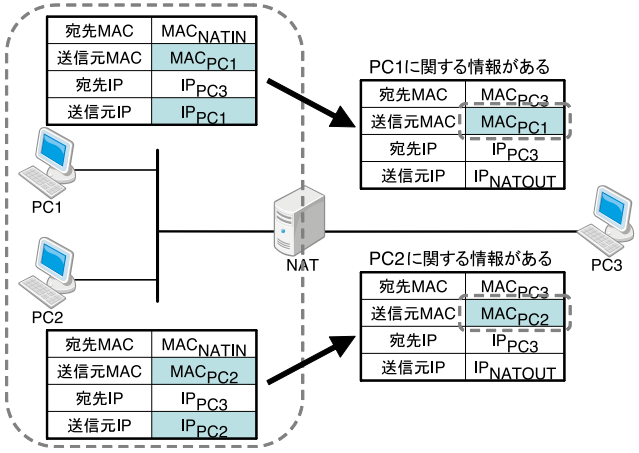


図 3　外部方向中継時の MAC アドレス中継型 NAT ルータの動作
Fig. 3　Process in MAC address relaying NAT router for outbound forwarding.

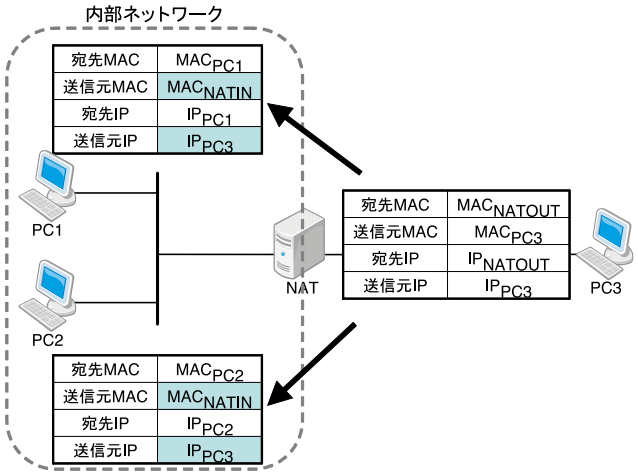


図 4　内部方向中継時の MAC アドレス中継型 NAT ルータの動作
Fig. 4　Process in MAC address relaying NAT router for inbound forwarding.

に変換し，送信元 MAC アドレスには PC2 のアドレス MAC_{PC2} を使用したフレームを作成して送出する．なお，外部ホスト PC3 では送信元 IP アドレスが同一（IP_{NATOUT}）で送信元 MAC アドレスが異なるフレームを受信するが，これらのフレームの受信により PC3 内の IP アドレスと MAC アドレスとの対応表[⋆1]は影響を受けない[6] ことに注意する．

次に，外部ネットワークから内部ネットワーク宛のフレームの流れを**図 4** に示す．同図において内部ホスト PC1 から外部ホスト PC3 宛に通信を開始し，PC3 がこれに応答して PC1 にパケットを送出する場合を想定する．このとき PC3 では宛先 IP アドレスとして NAT ルータの外部側 IP アドレスを指定する．また，フレームを作成する際の宛先 MAC アドレスは ARP[7] を用いて取得したものが使用されるため，NAT ルータの外部側 MAC アドレスが使用される．NAT ルータは外部ネットワーク側インタフェースで受信したフレームについては宛先 IP アドレスの変換を行った後，従来のものと同様に送信元 MAC アドレスを中継せずに内部ネットワークに送出する．

以上のように，MAC アドレス中継型 NAT ルータを導入する場合でも内部ホストと外部ホストとの間で通常の NAT ルータと同様の通信を行うことが可能である．

⋆1 いわゆる ARP（Address Resolution Protocol）表と呼ばれるもの．

なお，レイヤ 2 機器への影響については 4.4 節で議論する．

3.3　MAC アドレス中継型 NAT ルータの設計

本来であれば性能を向上させるために MAC アドレス中継機能はハードウェアにより実現すべきであるが，現実的には困難であるため，本研究では PC 上でソフトウェアにより同機能の実現を目指した．本節では試作した MAC アドレス中継型 NAT ルータ（試作 NAT ルータ）の設計および実装について述べる．

NAT はレイヤ 3 以上[⋆2]を対象とした技術であるため，通常ではレイヤ 2 の情報は扱わない．そこで，MAC アドレス中継型 NAT ルータを実現するにはアドレス変換プログラムがフレームをヘッダ付きで直接読み書きする機能が必要となる．PC 用の多くの OS では pcap（packet capture）[8] と呼ばれるライブラリによりこの機能を利用可能であり，試作 NAT ルータでもこのライブラリを用いることにした．

フレーム受信時の処理では，pcap ライブラリを用いてフレーム全体を取得する方法が考えられるが，予備実験でこの方法を評価した結果，オーバヘッドが大きくスループットが大幅に低下することが判明した．そこで，試作 NAT ルータの設計ではアドレス変換表のフロー単位のエントリ[⋆3]に内部側 MAC アドレスを追加し，pcap ではフローを特定するために必要な部分だけを取得してアドレス変換表に記録する手法を用いた．また，TCP については事前のコネクション確立が必須でこの時点で内部側 MAC アドレスが一意に定まるため，内部ネットワーク側から IP ヘッダ中で SYN フラグが設定されているフレームだけを取得するようにした．

フレーム送信時の処理では，内部ネットワーク側インタフェースで受信したパケットに対して通常の NAT ルータと同様のアドレス変換を行った後，アドレス変換表を参照して送信元 MAC アドレスとして内部側 MAC アドレスを設定したフレームを作成し，pcap ライブラリを用いて外部ネットワーク側インタフェースに送出する．

3.4　MAC アドレス中継型 NAT ルータの実装

試作 NAT ルータの実装は，FreeBSD 上で NAT 機能を提供する標準的なプログラムである natd[9] に前節で述べた MAC アドレス取得機能を持つモジュール（MAC アドレス取得モジュール）を追加し，またアドレス変換を行う部分とパケットを出力する部分を一部修

⋆2 FTP（File Transfer Protocol）など一部のアプリケーションプロトコルを対象にペイロードの変換を行う場合がある．
⋆3（内部側 IP アドレス，内部側ポート番号，変換後 IP アドレス，変換後ポート番号，外部側 IP アドレス，外部側ポート番号，トランスポート層プロトコル）の 7 つ組で構成される．

正することにより行った．

試作 NAT ルータの内部構成を**図 5** に示す．また，同図に基づき，内部ネットワーク側インタフェースからフレームを受信してから外部ネットワーク側インタフェースに送出するまでの動作手順を以下に示す．なお，図中の番号は以下の手順の番号に対応している．

(1)　NAT ルータは内部ネットワーク側インタフェースに到着したフレームを受信する．

(2)　MAC アドレス取得モジュールは受信したフレームが送信元 MAC アドレスの取得に必要であれば，pcap ライブラリ（libpcap）を用いてフレームの一部を取得する．

(3)　MAC アドレス取得モジュールは取得したフレームからフローを特定し，アドレス変換表に新しいエントリを作成して送信元 MAC アドレスを内部側 MAC アドレスとして登録する．

(4)　受信されたフレームは IP データグラムとして処理され，OS の IPFW（IP firewall）機能[10] により divert ソケット[11] を経由して natd に渡される．

(5)　natd は受け取った IP データグラムの送信元 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変換する．さらに，手順 (3) で登録された内部側 MAC アドレスもアドレス変換表から取得する．

(6)　natd は手順 (5) で取得した内部側 MAC アドレスを送信元 MAC アドレスとするフレームを作成し，pcap ライブラリを用いて外部側インタフェースから送出する．

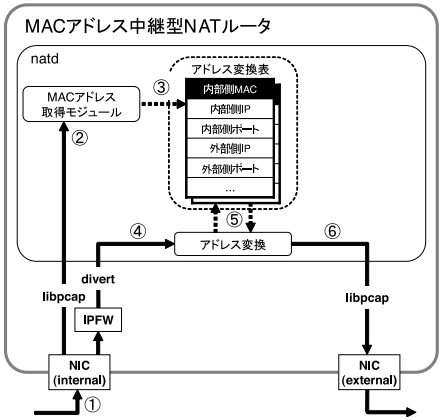


図 5　試作した MAC アドレス中継型 NAT ルータの内部構成
Fig. 5　Inside architecture of prototype MAC address relaying NAT router.

4. 試作 NAT ルータの評価と考察

本章では，試作 NAT ルータの機能や性能を評価するために行った実験について述べる．また，MAC アドレス中継機能が従来の機器に与える影響についても考察する．

4.1 内部ホスト・外部ホスト間通信試験

まず，試作 NAT ルータを経由して内部ホストと外部ホストとの間で通信が行えるかどうかを確認する試験を行った．試験環境を**図 6** および**図 7** に示す．

図 6 は送信元 MAC アドレスが NAT ルータとは異なるフレームを外部ホストが受け取った場合でも外部ホストから内部ホストへの通信が NAT ルータ経由で配送されるかどうかを確認するための試験環境である．この図においてサーバには以下に示す OS をそれぞれ搭載したものを用い，クライアントからサーバにアクセスした場合に正常に通信が行えるかどうかを確認した．

- Windows Vista Business Edition
- Windows XP Professional Edition SP3
- Windows XP Home Edition SP3

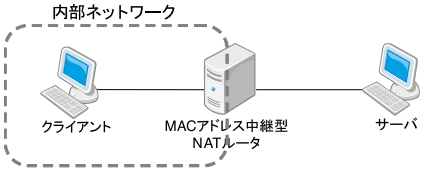


図 6　外部ホストに種々の OS を用いた場合の通信確認実験環境
Fig. 6　Experimental network for communication via prototype NAT router with various OS on the external host.

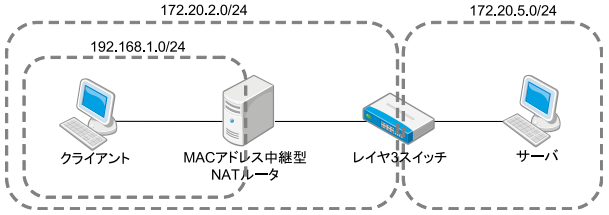


図 7　レイヤ 3 スイッチを経由した場合の通信確認実験環境
Fig. 7　Experimental network for confirmation via prototype NAT router and layer 3 switch.

- 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

試験の結果，いずれの OS の場合でも正常に通信できることを確認した．またサーバの ARP 表を確認した結果，いずれの OS でも NAT ルータの外部側 IP アドレスに対するエントリには NAT ルータの外部側 MAC アドレスが格納されており，NAT ルータによる送信元 MAC アドレスの中継が通信に影響を与えないことを確認した．

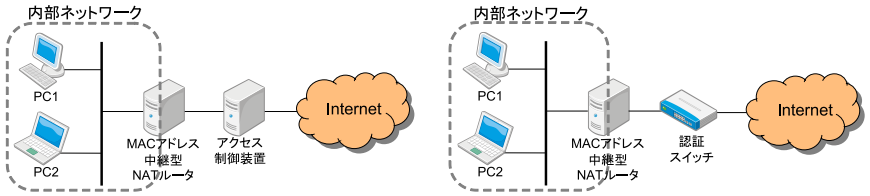
同様に，図 7 は送信元 MAC アドレスが NAT ルータとは異なるフレームをレイヤ 3 スイッチが受け取った場合でも正常に通信を行えるかどうかを確認するための試験環境である．この試験ではレイヤ 3 スイッチとしてアラクサラネットワークス社製 AX3630-24T を用いた．その結果，図 6 の場合と同様に NAT ルータによる送信元 MAC アドレスの中継が通信に影響を与えないことを確認した．

4.2　内部ホスト識別試験

次に，内部ホストを外部ネットワーク側から識別することができるかどうかを確認するための試験を行った．

試験環境を**図 8** に示す．図 8 (a) において，アクセス制御装置には Opengate を IP アドレスの代わりに MAC アドレスに基づいてアクセス制御を行うように改変したものを利用した．また図 8 (b) では認証スイッチとしてアラクサラネットワークス社製レイヤ 3 スイッチ AX3630-24T を利用し，Web 認証によりアクセス制御を行うように設定した．

これらの環境において内部ホスト PC1，PC2 からインターネット側に設置されたサーバに通信を行った結果，いずれの環境でも PC1，PC2 とも認証に成功するまではアクセス制御装置により認証を求められ，また認証に成功した後にはサーバと正常に通信できることを確認した．一方，試作 NAT ルータの代わりに従来の NAT ルータを動作させた場合にはいずれの環境でも PC1，PC2 の一方が認証に成功すると他方は認証なしでサーバと通信できるようになった．さらに図 8 (a) では試作 NAT ルータと改変前の Opengate を用いた場合についても同様であった．



(a) アクセス制御装置を用いた環境　　(b) 認証スイッチを用いた環境

図 8　内部ホスト識別試験環境
Fig. 8　Experimental network for internal host identification with prototype NAT router.

以上の結果から，試作 NAT ルータを用いれば外部ネットワーク側でも MAC アドレスに基づいて個々の内部ホストを識別し，個別にアクセス制御を行えることが確認された．

4.3　性能評価実験

最後に，試作 NAT ルータの MAC アドレス中継機能が性能に与える影響を調べるため，性能評価実験を行った．この実験では図 6 と同様の環境を用意し，クライアント（OS：FreeBSD7.3，CPU：Core2Duo 2.93 GHz，メモリ：2 GB）から試作 NAT ルータ（OS：FreeBSD7.0，CPU：Pentium4 2.0 GHz，メモリ：1 GB）を介してサーバ（OS：Ubuntu9.10，CPU：Pentium4 3.0 GHz，メモリ：1 GB）へ TCP あるいは UDP により 60 秒間送信する試行を 10 回行い，平均スループットを測定した．また，比較の対象として従来の NAT ルータを用いた場合についても同様の実験を行った．なお，すべての機器は 100Base-TX で接続されており，スループットの測定には Iperf を利用した．

実験結果を**表 1** に示す．この表より，従来の NAT ルータと比べて MAC アドレス中継型 NAT ルータを介する場合のスループットの低下は TCP の場合で 0.06 Mbps（約 0.06%），UDP の場合は 0.02 Mbps（約 0.02%）にとどまっており，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といえる．

4.4　周辺機器への影響に関する考察

MAC アドレス中継機能は従来のレイヤ 3 機器は有していない機能であるため，従来の機器と MAC アドレス中継型 NAT ルータが混在する環境では同機能が従来の機器に影響を及ぼす可能性がある．以下では，このような影響とその対策について考察する．

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

NAT ルータ種別	TCP（Mbps）	UDP（Mbps）
従来型	93.98	95.50
MAC アドレス中継型	93.92	95.48

4.4.1　大規模ネットワーク環境への適用

送信元 MAC アドレスはレイヤ 3 スイッチやルータなどのレイヤ 3 機器では中継されないため，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 ルータの内部ネットワーク側および外部ネットワーク側インタフェースに直接接続されているセグメントに限られる．このため，大規模なネットワーク環境において，たとえばインターネットとの接続点などで集約的にアクセス制御を行いたい場合には，内部ホストと MAC アドレス中継型 NAT ルータとの間および MAC アドレス中継型 NAT ルータとアクセス制御装置との間に他のレイヤ 3 機器を設置することができず，ネットワークの構成に大きな制約が生じることになる．

この問題に対する解決方法として，他のレイヤ 3 機器にも MAC アドレス中継機能を導入する方法があげられる．同機能は試作 NAT ルータと同様の方法で他のレイヤ 3 機器にも導入可能であり，またハードウェアによる実装も技術的には困難ではないと思われる．

4.4.2　レイヤ 2 機器における無意味な MAC アドレスの学習

今日ではほとんどのレイヤ 2 スイッチやブリッジなどのレイヤ 2 機器が MAC アドレス学習機能を有しており，任意のフレームを受信すると送信元 MAC アドレスと受信インタフェースの対応を MAC アドレス表と呼ばれるデータベースに一定時間登録する．このデータベースはフレーム送出時に参照され，フレームの中継先インタフェースの決定に用いられる．ところが，レイヤ 2 機器が MAC アドレス中継型 NAT ルータの出力したフレームを受信すると，3.2 節で述べたように逆方向の通信には MAC アドレス中継型 NAT ルータ自身の MAC アドレスが用いられ，中継された内部ホストの MAC アドレスは用いられないため，レイヤ 2 機器はまったく参照されない MAC アドレスを多数登録することになる．

この問題に対して，無意味な登録の抑制は困難であるが，登録される MAC アドレス数は NAT ルータの代わりにレイヤ 2 機器を用いた場合と同じであり，また最近のレイヤ 2 機器は数千エントリから数万エントリ程度の十分大きな MAC アドレス表を有するため，ネットワークの規模に見合ったレイヤ 2 機器を用いれば，影響は事実上無視できる．

4.4.3　レイヤ 2 機器における MAC アドレス学習の無効化

MAC アドレス中継型 NAT ルータは通常の動作では自身の外部側 MAC アドレスを送信元 MAC アドレスとして設定したフレームを送出しないため，外部ネットワーク側のレイヤ 2 スイッチでは当該 MAC アドレスを MAC アドレス表に登録する機会が ARP 応答時しかない可能性がある．ところが，レイヤ 2 機器の MAC アドレス表のエントリ有効期間はホストやネットワーク機器の ARP 表のものより短いことが多い[⋆1]ため，レイヤ 2 機器上で登録内容が無効化され，次に MAC アドレス中継型 NAT ルータが ARP 応答を送るまでの間はレイヤ 2 機器が MAC アドレス中継型 NAT ルータ宛のフレームをフラッディングする現象が発生しやすくなる．この問題への対策としては，MAC アドレス中継型 NAT ルータから送信元 MAC アドレスとして外部側 MAC アドレスを設定したフレーム（たとえば gratuitous ARP [12]）を MAC アドレス表のエントリ有効期間より短い間隔で定期的に送出し，強制的にレイヤ 2 機器の MAC アドレス表を更新させる方法があげられる．

⋆1 典型的な例としては，前者の 5 分に対して後者の 20 分．

5. むすび

本研究では，内部ホストを外部ネットワークから識別するために，内部ホストから送信されたフレームに含まれる送信元 MAC アドレスをそのまま外部ネットワーク側に中継する機能を持つ NAT ルータを提案した．また，このような NAT ルータを PC 上で実装し，機能的，性能的に十分動作することを確認した．

今後の課題として，MAC アドレス中継機能を有する他のレイヤ 3 機器を実装し，NAT ルータと組み合わせた環境での検証を行うことがあげられる．また，MAC アドレス中継機能のハードウェア化や OS の改変による高速化を図り，より高帯域のネットワーク環境で性能評価を行うこともあげられる．さらに，ソフトウェア資産管理システムや検疫システムとの組合せなど，他のシステムとの連携についても検討したい．

謝辞　本研究の一部は平成 21〜23 年度科学研究費補助金（基盤研究（C），課題番号 21500075）の補助を受けている．ここに記して感謝の意を表する．

参考文献

1) Srisuresh, P. and Egevang, K.: Traditional IP Network Address Translator (Traditional NAT), RFC 3022, IETF (2001).
2) Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A. and Stewart, L.: HTTP Authentication: Basic and Digest Access Authentication, RFC 2617, IETF (1999).
3) Kristol, D. and Montulli, L.: HTTP State Management Mechanism, RFC 2965, IETF (2000).
4) 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).

5) Savola, P.: MTU and Fragmentation Issues with In-the-Network Tunneling, RFC 4459, IETF (2006).
6) Braden, R.: Requirements for Internet Hosts, RFC 1122, IETF (1989).
7) Plummer, D.C.: Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware, RFC 826, IETF (1982).
8) Jacobson, V., Leres, C. and McCanne, S.: Manpage of PCAP (online), available from ⟨http://www.tcpdump.org/pcap3_man.html⟩ (accessed 2010-06-08).
9) Cobbs, A., Mott, C., Eklund, E., Suutari, A., Nelson, D., Somers, B. and Ermilov, R.: natd – Network Address Translation daemon, *FreeBSD Kernel Interfaces Manual* (2003).
10) Antsilevich, U.J.S., Kamp, P.-H., Nash, A., Cobbs, A. and Rizzo, L.: ipfw – IP firewall and traffic shaper control program, *FreeBSD System Manager's Manual* (2006).
11) Cobbs, A.: divert – kernel packet diversion mechanism, *FreeBSD Kernel Interface Manual* (2004).
12) Cheshire, S.: IPv4 Address Conflict Detection, RFC 5227, IETF (2008).

(平成 22 年 6 月 14 日受付)
(平成 22 年 12 月 1 日採録)

山井　成良（正会員）

昭和 59 年大阪大学工学部電子工学科卒業．昭和 61 年同大学大学院博士前期課程修了．昭和 63 年同大学院基礎工学研究科（物理系専攻情報工学分野）博士後期課程退学．同年奈良工業高等専門学校情報工学科助手．同講師，大阪大学情報処理教育センター助手，同大学大型計算機センター講師，岡山大学総合情報処理センター（現情報統括センター）助教授を経て，平成 18 年より同教授．分散システム，ネットワーク運用管理，ネットワークセキュリティの研究に従事．IEEE，電子情報通信学会各会員．博士（工学）．

村上　　亮（学生会員）

平成 21 年岡山大学工学部通信ネットワーク工学科卒業．現在，同大学大学院自然科学研究科（電子情報システム工学専攻）博士前期課程在学中．分散システム運用管理に興味を持つ．

岡山　聖彦（正会員）

平成 2 年大阪大学基礎工学部情報工学科卒業．平成 4 年同大学大学院基礎工学研究科博士前期課程修了．同年同大学院基礎工学研究科博士後期課程を退学し，同大学工学部助手．奈良先端科学技術大学院大学情報科学研究科助手，岡山大学工学部助手，同大学総合情報基盤センター助教を経て，平成 22 年同大学情報統括センター助教．博士（工学）．インターネットアーキテクチャ，ネットワーク管理，ネットワークセキュリティの研究に従事．電子情報通信学会会員．

中村　素典（正会員）

平成 6 年京都大学大学院工学研究科博士後期課程単位取得退学．立命館大学理工学部助手，京都大学経済学部助教授，京都大学学術情報メディアセンター助教授を経て，平成 19 年より国立情報学研究所教授，現在に至る．博士（工学）．日本ソフトウェア科学会，電子情報通信学会各会員．コンピュータネットワーク，ネットワークコミュニケーション，認証連携等の研究に従事．