RL-001

IPv6 環境におけるネットワーク認証のための マルチキャストフィルタリングイーサネットスイッチ
A Multicast Filtering Ethernet Switch for Network Authentication in IPv6 Networks

布目 淳† 平田 博章† 柴山 潔†
Atsushi Nunome Hiroaki Hirata Kiyoshi Shibayama

1. まえがき

大学のコンピュータ自由演習室のように，不特定多数の利用者が個人所有のノート PC を持ち込み，学内ネットワークに接続するような環境では，そのユーザがネットワークに接続する権限を有しているかを確認する必要がある．現在ではこの方式として，IEEE 802.1X 認証方式[1]（以下，802.1X 方式）や認証 VLAN 方式[2]が広く用いられている．802.1X 方式は，端末上で動作する認証用ソフトウェア（サプリカント）と認証 LAN スイッチ，RADIUS[3]認証サーバが連携することでネットワーク認証を実現している．認証フレームを用いた認証が成功した時点で端末に IP アドレスを割り当てるため，未認証端末が IP 通信によって攻撃できないという点で安全である．しかし，基本的に認証 LAN スイッチのポート単位で制御を行うため，認証 LAN スイッチとサプリカントとの間に集線装置（ハブ）を設置して，収容端末数を一時的に増やそうとすると問題が生じる．例えばリピータハブを設置した場合，リピータハブに接続した端末のうち 1 台が認証に成功すると，他の未認証端末も認証済みとして扱われてしまう．多くの製品はこの問題を MAC アドレスフィルタによって回避しているが，他にも，リピータハブに接続した端末が送受信するフレームを悪意ある端末が盗聴できてしまうという問題もある．このフレーム盗聴問題は，さまざまなスキルのユーザが同時に利用する環境では大きな問題になる可能性がある．一方，スイッチングハブを設置した場合は，フレームの盗聴は避けられるが，通常のスイッチングハブは認証フレームに用いられる特殊なフレームを他のポートに転送せずに破棄してしまうため，認証フレームが認証 LAN スイッチまで到達できない．これらの理由から，ネットワーク認証システムとして 802.1X 方式を用いる場合は，基本的にすべての端末が認証 LAN スイッチと直接接続するようにネットワークを構築しなければならない．

認証 VLAN 方式では，未認証端末にも一時的な仮 IP アドレスを割り当てるため，未認証端末を収容するデフォルト VLAN において，管理者の連絡先といった限られた情報を Web ページとして提示したり，Web インタフェースでユーザ認証を行うことができる．しかし，デフォルト VLAN 内での相互通信は制御されないため，悪意ある未認証端末が他の未認証端末を攻撃したり，通信を妨害する可能性がある．

これらの問題に対し，我々は認証前後で VLAN を切り替えるのではなく，未認証端末の通信可能範囲を必要最小限に制限する放送範囲可変型イーサネットスイッチを提案した[4]．このイーサネットスイッチと認証を受ける端末は直接接続しておく必要がないため，幅広いネットワーク環境に適用できる．また，未認証端末にも IP アドレスを付与するものの，未認証端末間の IP 通信は禁止するため，認証前の段階であっても一定のセキュリティレベルを提供できるという特長がある．

しかし，提案したイーサネットスイッチはブロードキャストフレームのみに注目して制御を行うため，そのままではマルチキャスト通信を多用するネットワーク環境には適用できない問題があった．そこで本稿では，端末の認証状況に応じてマルチキャストフレームの到達範囲を適切に制御するイーサネットスイッチを提案する．

†京都工芸繊維大学大学院工芸科学研究科情報工学部門
Dept. of Information Science, Kyoto Institute of Technology

2. IPv4 環境に対応する放送範囲可変型イーサネットスイッチ

文献[4]で提案したイーサネットスイッチでは，未認証端末が送信するブロードキャストフレームを複数個のユニキャストフレームに変換する．それらのフレームを，Web インタフェースによりユーザの個人認証を行う認証サーバや DHCP[5]サーバのような，認証に必要な通信先にのみ送信する．その後，認証が成功した時点で初めて端末の通信可能範囲が拡がるよう，イーサネットスイッチがブロードキャストフレームの到達範囲を制御する．このように，提案したイーサネットスイッチはブロードキャストフレームだけを制御の対象とするため，DHCP や ARP[6]といったブロードキャスト通信を多用する IPv4 環境に適している．

一方，今後普及が加速すると見られている IPv6[7]環境においては，開発当初からマルチキャスト通信を活用するよう，各種のプロトコルが設計されている．例えば，ネットワークパラメータを配布する DHCPv6[8]では DHCPv6 サーバを探索する際にマルチキャスト通信を行う．また，IP アドレスのステートレス自動設定[9]では，あるノードが作成した IP アドレスが他のノードと重複していないことをマルチキャスト通信によって確認する．通信先の MAC アドレスを解決するという，IPv4 環境における ARP に相当する処理もマルチキャスト通信で行う．

このように IPv6 環境で常用されるマルチキャストフレームは，放送範囲可変型イーサネットスイッチでは一切制御しないため，未認証端末からマルチキャスト通信によって攻撃や妨害を受ける可能性がある．逆に，未認証端末からのマルチキャストフレームを単純に破棄してしまうと，IP アドレスを自動設定する時に他のノードとアドレスが重複するといった問題や，認証サーバの MAC アドレスが取得できずにアクセスができないといった問題が生じる．

そこで以下では，放送範囲可変型イーサネットスイッチにマルチキャストフレームの処理機構を付加することで，未認証端末からのマルチキャストフレームが必要な範囲だけに到達するよう制御する．このように，IPv6 環境においても，未認証端末が送信するフレームの到達範囲を最小限に制限できることを示す．

3. IPv6 環境におけるマルチキャスト通信

IPv6 環境において，未認証端末が必要とするマルチキャスト通信を以下に述べる．

3.1 IP アドレスの自動設定

IPv6 環境では，ネットワークインタフェースの MAC アドレス[10]や乱数[11]を用いることで，端末自身が IP アドレスを作成できる．このステートレス自動設定方式により，端末はネットワークリンク内だけで有効な IP アドレスであるリンクローカルアドレス（Link Local Address; LLA）を作成でき，それを用いて同一リンク内のノードにアクセスできる．他にも，ルータがマルチキャストするルータ広告（Router Advertisement; RA）のパラメータを組み合わせてグローバル IP アドレスを作成することや，DHCPv6 サーバをマルチキャスト通信で探索し，明示的に IP アドレスを付与してもらうステートフル自動設定方式を用いることもできる．

3.2 重複アドレスの検出

前節で述べたどの方式で IP アドレスを設定したとしても，端末はその IP アドレスの一意性を確認するために，ICMPv6[12]の機能の 1 つである近隣探索プロトコル[13]を用いて，「重複アドレス検出（Duplicate Address Detection; DAD）」を行わなければならない．未認証端末が独自に作成した IP アドレスについても DAD を行う必要があるため，そのために必要なフレームがネットワーク内に適切に流れるようにしなければならない．

DAD では，確認する IP アドレスの一部から作成したマルチキャストアドレスに向けて，近隣要請（Neighbor Solicitation; NS）フレームを送信（マルチキャスト）する．もし，この NS フレームを受信したノードが自分の IP アドレスと重複していることを検知した場合は，近隣広告（Neighbor Advertisement; NA）フレームをマルチキャストすることで，アドレスの重複を通知する[9]．DAD のために NS フレームを送信したノードは，1 秒以内に NA フレームで通知されなければ，その IP アドレスは重複していないものと判断できる[13]．

ここで，「未認証端末が送信した」という理由で，すべてのマルチキャストフレームを破棄したり，放送範囲可変型スイッチにおけるブロードキャストフレームと同様に，認証に必要な特定のノードのみに転送してしまうと，IP アドレスの一意性が確認できずに，他のノードと IP アドレスが重複してしまう可能性がある．特にグローバル IP アドレスが重複すると，認証後の通信で障害が生じる．

3.3 MAC アドレスの解決

IPv6 環境では，通信先ノードの MAC アドレスを解決するために，近隣探索プロトコルで定められたマルチキャスト通信を行う．未認証端末であっても，認証サーバへアクセスする際には，その MAC アドレスを解決する必要があるため，このマルチキャスト通信は不可欠である．そこで，提案するイーサネットスイッチは未認証端末が送信するこうしたマルチキャストフレームを，認証サーバへ転送しなければならない．

以上のように，未認証端末が送信するマルチキャストフレームの中には，近隣探索プロトコルのように，正しく処理しなければ，認証の過程だけでなく認証が完了した後の通信にも問題を生じさせるものが存在する．

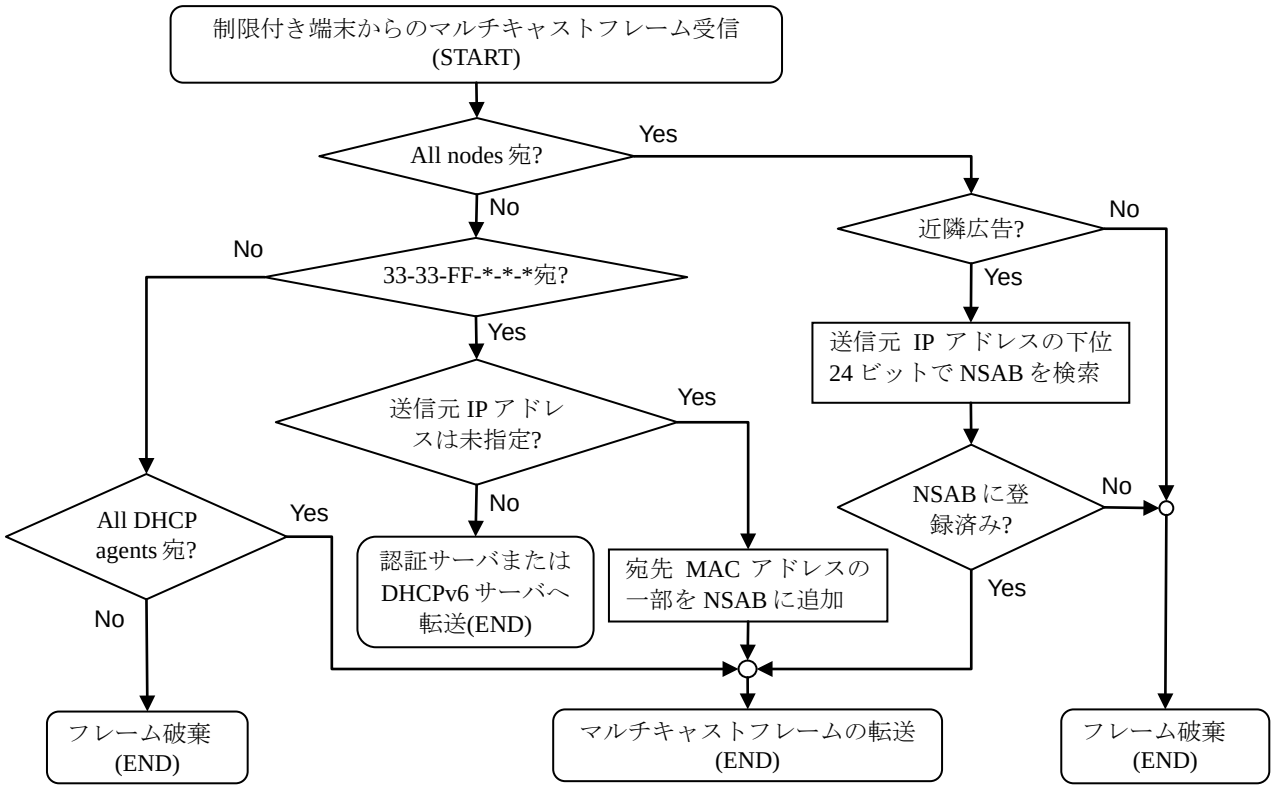

図 1　制限付き端末からマルチキャストフレームを受信した時の処理手順

4. マルチキャストフィルタリングイーサネットスイッチ

4.1 概要

本稿で提案するマルチキャストフィルタリングイーサネットスイッチ（以下，本スイッチと表記）では，放送範囲可変型イーサネットスイッチに対し，必要な範囲だけにマルチキャストフレームを転送する機構を付加する．これにより，IPv6 環境への対応を図る．

本スイッチでは，受信したフレームの送信元 MAC アドレスをもとに，端末を以下の 2 種類に区別して管理する．

- ［制限付き（Restricted）］認証を受けておらず，通信可能範囲が制限されている端末．未認証端末．
- ［制限無し（Authenticated）］認証が済んでおり，通信可能範囲に制限がない端末．

「制限付き」端末から受信したフレームは，認証に必要な通信先だけに到達するよう，本スイッチが制限する．このため，認証を済ませていない段階でも一定の範囲内であれば IP 通信が可能である．

「制限付き」端末が送信するマルチキャストフレームの中には，3.2節や3.3節で述べたような役割のフレームがあるため，近隣探索プロトコルに関連するフレームは単純に破棄することができない．本スイッチが「制限付き」端末からマルチキャストフレームを受信した際の処理手順を図1に示す．受信したマルチキャストフレームについて，フレームヘッダ上の宛先 MAC アドレスや，必要に応じて IPv6 ヘッダと ICMPv6 ヘッダを調べることで，これらのフレームの到達範囲を制御する．なお，ブロードキャストフレームやユニキャストフレームを受信した場合は，放送範囲可変型イーサネットスイッチと同様の処理を行う．

次節では，図 1に従って，マルチキャストフレームを受信した時の処理手順を詳しく述べる．

4.2 マルチキャストフレーム受信時の処理

本稿では以降， MAC アドレスを 8 ビットずつ区切り，各々の 16 進数をハイフン（-）でつないで表記する．

近隣探索プロトコルで用いられるマルチキャストフレームの宛先 MAC アドレス[14][15]を表 1に示す．ここで，NS フレームの宛先 MAC アドレスは，下位 24 ビットの部分（*-*-*部）に宛先 IP アドレスの下位 24 ビットを取り込むため，他の用途のマルチキャストフレームとは容易に区別できる．

一方，NA フレームと RA フレームの宛先 MAC アドレスは，「リンク内の全ノード（All nodes）宛」を意味しており，到達範囲は IPv4 環境におけるブロードキャストフレームと同じである．この宛先 MAC アドレスは，近隣探索プロトコル以外でも用いられるため，NS フレームのように宛先 MAC アドレスだけでフレームの用途を判断することはできない．そこで，IPv6 対応スイッチの多くが対応している MLD（Multicast Listener Discovery）[16]スヌーピング機能のように，必要に応じてフレーム内の IPv6 ヘッダおよび ICMPv6 ヘッダを解釈する機能を実装することで，マルチキャストフレームの用途を特定できるようにする．

表 1　近隣探索に用いられるマルチキャストフレームの宛先 MAC アドレス

用途	宛先 MAC アドレス
近隣要請 (NS)	33-33-FF-*-*-*
近隣広告 (NA)	33-33-00-00-00-01
ルータ要請 (RS)	33-33-00-00-00-02
ルータ広告 (RA)	33-33-00-00-00-01

4.2.1 近隣要請フレームの処理

通信先MACアドレスの解決とDADにはNSフレームを用いる．このうち，DADのためのNSフレームでは，送信元IPアドレスとして「未指定（All 0）」が設定される [1]．そこで，本スイッチが「制限付き」端末からNSフレーム（宛先MACアドレスの上位 24 ビットが 33-33-FFであるフレーム）を受信した場合は，まずIPv6 ヘッダ上の送信元IPアドレスを確認する．ここが未指定であればDADのためのNSフレームと判断し，そのフレームを当該マルチキャストグループに参加している端末が接続しているポートに送信する．この時，送信したNSフレームに対する応答（NAフレーム）を判別するために，宛先MACアドレスの下位 24 ビット [2]をスイッチ内部の近隣要請アドレスバッファ（Neighbor Solicitation Address Buffer; NSAB）に保存する．3.2節で示したように，端末がNSフレームを送信した後，NAフレームによる重複通知を待つ時間は 1 秒間だけなので，NSABに情報を追加してから 1 秒以上が経過したエントリは削除して構わない．

一方，送信元 IP アドレスが指定されている NS フレームは通信先 MAC アドレスを解決するための NS フレームであり，「制限付き」端末が認証サーバの MAC アドレスを調べるために必要である．また，認証が成功する前にその他のノードの MAC アドレスを調べる必要はないので，この種の NS フレームは認証サーバが接続されたポートにのみ送信する．これにより，「制限付き」端末が認証に無関係のノードと通信を行わないように制御する．

4.2.2 近隣広告フレームの処理

DAD においては，IP アドレスの重複を検知したノードは NA フレームによって通知するため，このフレームをスイッチが破棄してしまうと，DAD が機能しなくなる．特に，「制限付き」端末からの NA フレームをすべて破棄してしまうと，ほぼ同時に複数の端末がネットワークに接続した場合，これらの端末間で IP アドレスが重複していても検出できなくなる．そのため，「制限付き」端末がマルチキャストした NA フレームは，本スイッチで単純に破棄することはできない．

しかし，先に述べたように，フレームヘッダの情報だけからそのフレームが NA フレームであると判定することはできない．そこで，「制限付き」端末からマルチキャストフレームを受信した場合は，以下の手順で NA フレームと判定し，そのうち必要なフレームだけを中継する．まず，宛先 MAC アドレスが「リンク内の全ノード宛」であるかを調べ，一致した場合は，ICMPv6 ヘッダのタイプフィー

[1] この場合でも，イーサネットのフレームヘッダには送信元 MAC アドレスが記録されているため，送信した端末の認証状態を判断できる．

[2] これは重複を検査する IP アドレスの下位 24 ビットに等しい．

ルドが NA フレームを示す 136 であるかを調べる．フレームが NA フレームであれば，以前転送した NS フレームへの応答であるかを調べるために，送信元 IP アドレスの下位 24 ビットと NSAB に保存していた宛先 MAC アドレスの下位 24 ビットを照合し，一致するエントリが存在するかを調べる．一致するエントリがあれば，以前に転送した NS フレームに対する応答である可能性があるため，その NA フレームを転送する．一致するエントリが存在しない場合は，「制限付き」端末からの攻撃である可能性があるので，その NA フレームは転送せずに破棄する．

こうすることで，「制限付き」端末同士の IP アドレスが重複することを回避し，同時に「制限付き」端末が近隣要請とは無関係な NA フレームを大量に送信して DAD を妨害することを防ぐ．

4.2.3 全 DHCP エージェント宛フレームの処理

ステートフル自動設定方式によって IP アドレスを設定する場合，「制限付き」端末は「全 DHCP エージェント（All DHCP agents）宛」のマルチキャストフレームを送信して，DHCPv6 サーバに IP アドレスの割当を依頼する．この時の宛先 MAC アドレスは「33-33-00-01-00-02」であり，他の用途では用いられない．そこで，「制限付き」端末からこの MAC アドレス宛のフレームを受信した場合は，既知の DHCPv6 サーバが接続しているポートに転送処理を行う．

4.2.4 その他のマルチキャストフレームの処理

「制限付き」端末が送信する可能性のあるルータ要請（Router Solicitation; RS）フレームは，端末による LLA の自動設定や DAD には不要なため，本スイッチで破棄する．特に，RS フレームの宛先 MAC アドレスは「リンク内の全ルータ（All routers）宛」であるため，悪意のある端末からルータへの攻撃を防ぐ観点からも，こうしたフレームは破棄すべきである．なお，RS フレームを破棄した場合でも，正規のルータが定期的にマルチキャストする RA フレームは「制限付き」端末にも届くため，ネットワークのサブネット情報のような基本的な情報は「制限付き」端末にも問題なく通知できる．

その他のIPv6 マルチキャストフレームおよびIPv4 マルチキャストフレーム [1]を本スイッチが受信した場合，「制限付き」端末が送信したフレームに関しては破棄する．これにより，「制限付き」端末からの認証処理に無関係なフレームがネットワーク内に流れることを防止する．

4.3 認証終了後の処理

認証が成功した場合，本スイッチは認証サーバから完了通知を受け取り，「制限付き」端末として扱っていた端末を以後は「制限無し」端末として扱うよう，内部の管理状態を変更する．これにより通信可能範囲の制限を解除する．

また，「制限無し」端末の無通信時間が一定時間を超えた場合や，「制限無し」端末と接続しているポートのリンクが切断した場合は，スイッチ内部のテーブルから当該端末に関する情報を削除する．これによって，端末に再認証を要求する．

[1] 宛先 MAC アドレスの上位 24 ビットが 01-00-5E で，25 ビット目が 0 のフレーム．

5. むすび

本稿では，未認証端末からのマルチキャストフレームを適切にフィルタリングすることで，通信可能範囲を制限するイーサネットスイッチを提案した．本スイッチは，未認証端末が IPv6 環境で行おうとするマルチキャスト通信のうち，認証を受けるまでの間に必要なフレームだけを転送するよう制御する．802.1X 方式と異なりポート単位の制御ではないため，通常のハブを併用してネットワークを容易に拡張できる．また，未認証端末間の IPv6 通信も必要最小限に制限するため，未認証端末に関しては認証 VLAN 方式よりも安全性が高い．

今後の課題としては，(i)本スイッチと認証サーバおよび DHCPv6 サーバとの間で端末の認証状態を交換するための安全な通信プロトコルを決定すること，(ii)本方式を実装し，動作を検証すること，が挙げられる．

謝辞

本研究の一部は日本学術振興会科学研究費補助金（基盤研究(C)21500053 および同 22500046）の補助による．

参考文献

[1]LAN/MAN Standards Committee of the IEEE Computer Society, “802.1X - Port-Based Network Access Control”, IEEE (2004).
[2]Alcatel Internetworking, Inc., “White paper: Authenticated VLANs, Secure Network Access at Layer 2”, http://enterprise.alcatel-lucent.com/private/active_docs/wp_a-vlans.pdf (2002).
[3]C. Rigney, S. Willens, A. Rubens, W. Simpson, “Remote Authentication Dial In User Service (RADIUS)”, RFC2865, IETF (2000).
[4]布目 淳, 平田 博章, 柴山 潔, “ネットワーク認証のための放送範囲可変型イーサネットスイッチ”, 電子情報通信学会論文誌 D-I, Vol.J88-D-I, No.4, pp.908-911 (2005).
[5]R. Droms, “Dynamic Host Configuration Protocol”, RFC2131, IETF (1997).
[6]D. Plummer, “Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware”, RFC826, IETF (1982).
[7]S. Deering, R. Hinden, “Internet Protocol, Version 6 (IPv6) Specification”, RFC2460, IETF (1998).
[8]R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney, “Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”, RFC3315, IETF (2003).
[9]S. Thomson, T. Narten, T. Jinmei, “IPv6 Stateless Address Autoconfiguration”, RFC4862, IETF (2007).
[10] M. Crawford, “Transmission of IPv6 Packets over Ethernet Networks”, RFC2464, IETF (1998).
[11] T. Narten, R. Draves, S. Krishnan, “Privacy Extensions for Stateless Address Autoconfiguration in IPv6”, RFC4941, IETF (2007).
[12] A. Conta, S. Deering, M. Gupta, “Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification”, RFC4443, IETF (2006).
[13] T. Narten, E. Nordmark, W. Simpson, H. Soliman, “Neighbor Discovery for IP version 6 (IPv6)”, RFC4861, IETF (2007).
[14] R. Hinden, S. Deering, “IPv6 Multicast Address Assignments”, RFC2375, IETF (1998).
[15] D. Eastlake 3rd, “IANA Considerations and IETF Protocol Usage for IEEE 802 Parameters”, RFC5342, IETF (2008).
[16] R. Vida, L. Costa, “Multicast Listener Discovery Version 2 (MLDv2) for IPv6”, RFC3810, IETF (2004).