1D-01

IPv6における内部側ネットワークでのアドレス重複を許容する方式の提案

橋口匠† 入江智和†
鹿児島工業高等専門学校情報工学科†

1. はじめに

IPv4では、通常DHCPサーバがアドレスを管理することによりIPアドレスの一意性を確保していた。一方IPv6では、膨大なアドレス空間を有するため各ノードでIPアドレスの生成を行い、一意性を確保するためにDAD(Duplicate Address Detection)が備わっている。しかし、アドレスの手動設定や生成方式などにより重複は一定確率で発生するほか、公衆Wi-Fiなどでは直接通信が禁止されていることでDADが有効に機能しないことがある。アドレス重複が発生するとアドレスの使用不可や再生成が必要となるが、ユーザ側では把握できないため即時に通信を開始したい場合の障害となる。そのため、アドレス重複時にこれを検出できない。ノードでも非重複時と同等の通信が可能になれば利便性が向上する。

本研究では、ポート番号やMACアドレスをノードの識別に用いることで、IPアドレスが重複していても通信を行える手法を提案する。ネットワークへの変更を最小化するためにルータのみに機能を実装し、機能の有用性を検証する。

2. DAD(Duplicate Address Detection)

2.1 DADの概要

DADとは自身で生成したアドレスが他ノードに既に使われていないか検出する機能のことである。同一リンク内の全ノードに対しマルチキャストで重複を検出するためのNS(Neighbor Solicitation)を送信し、一定時間応答を待つ。同一アドレスを使用中のノードが存在する場合、そのノードがNA(Neighbor Advertisement)を送信し、アドレスが使用されていることを知らせる。DADを行っているノードは、一定時間内に応答がないとアドレスを使用することができるが、応答があった場合は重複しているとみなし、アドレスは使用できず、再生成が必要となる。

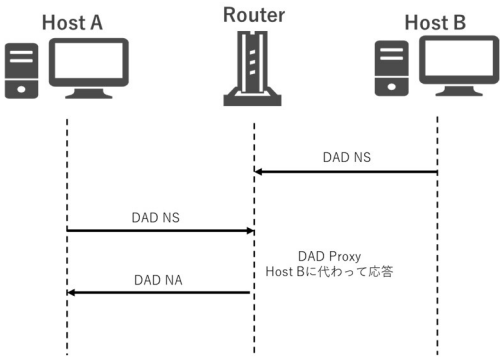

図1 従来手法(DAD Proxy)の動作

2.2 DADの課題

公衆Wi-Fiといった不特定多数のユーザが使用する環境のAP(Access Point)では、プライバシーセパレータが有効になっていることが多い。プライバシーセパレータとは接続している無線端末間の直接通信を制限する機能のことである。機能が有効な場合、本来リンク上の全ノードに重複検出のNSが届かなければならないが、APで制限さることでアドレスの一意性が保証されない問題が生じる。この問題に対しては、従来手法として特にDAD Proxy[1]が存在する。図1はHost BとHost AがDADを行う際のDAD Proxyの動作である。

また、無線接続の場合、各ノードとAPとの距離や周囲環境によって通信に時間がかかることや各ノードの処理状態によってDADの応答待ち時間内にNS、NAの送受信が完了しない問題もある。この問題にはDAD Proxyでは処理が他ノードの状態に依存しているため、有意な対策にならない。

その他、近年のセキュリティへの関心向上に伴い、様々な研究が行われている。例えば、Unified Multiplex[2]がある。Unified Multiplexは IPv6の膨大なアドレス空間を利用し、短時間で多くのアドレスを生成、使用する。多数のアドレスを使用するため、より重複が発生しやすい。

Proposal of a method to allow address duplication that occurs in the internal network in IPv6
†Takumi Hashiguchi, †Tomokazu Irie
Information Engineering, National Institute of Technology, Kagoshima College

表 1　通信の識別

送信元 IP アドレス	送信元 MAC アドレス	送信元ポート番号	宛先 IP アドレス	宛先ポート番号	一意な送信元ポート番号
fd00::2	00-11-22-33-44-55	49654	fd00:0:0:1::2	80	49654
fd00::1	01-12-23-34-45-56	52379	fd00:0:0:1::2	80	53218
fd00::2	55-44-33-22-11-00	49654	fd00:0:0:1::2	22	51786

3. 提案手法

本稿ではルータで転送するパケット毎に通信ノードの識別を行う手法を提案する。

具体的には、ルータが内部側から受信した場合には送信元 MAC アドレス、送信元 IP アドレス、送信元ポート番号、宛先 IP アドレス、宛先ポート番号を用いてノードの識別を行い、識別情報に対して一意な送信元ポート番号を割り当て、記憶する。ルータから外部に送信するときには送信元ポート番号を割り当てた一意な送信元ポート番号に変換し送信する。その際、送信元 IP アドレスの変更は行わず、可能な限り送信元ポート番号と一意な送信元ポート番号が同一となるよう調整する。表 1 のように IP アドレスが重複しているノードが存在しても列の要素が異なることで識別を行う。外部側から受信した場合には宛先ポート番号からルータが記憶している情報を元に内部側のノードを特定する。内部側へ送信する際に宛先ポート番号を元の送信元ポート番号に変換し、宛先 MAC アドレスを指定した上で送信する。概略を図 2 に示す。

4. 概念実証実験

提案方式の有用性を確認するために概念実証実験を行う。

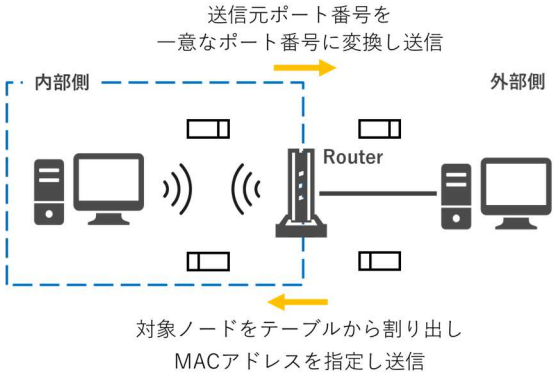

図 2　提案手法

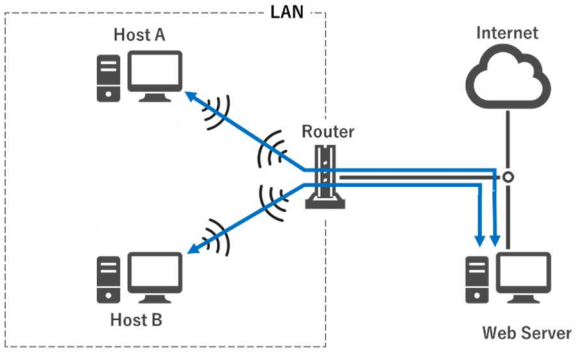

図 3　ネットワーク構成

実験用ネットワークの構成を図 3 に示す。AP はルータ型であり、そのルータに提案方式を実装している。また、AP はプライバシーセパレータが有効である。Host A、Host B、Router には Raspberry Pi を用い、提案手法の実装には Python 3、Scapy を使用した。AP 配下の二台のホストに同一のアドレスを設定し、同時に二台の端末から図中の Web サーバにアクセスを行う。その際の Web サーバ、AP のログと各ホストでの表示を元に評価を行う。

Web サーバのログには同一の接続アドレスとしてのアクセスログが一秒差で二つ残っていた。また、各ホストにおいてそれぞれ非重複時と同じ出力がされた。

5. 結論

本研究では、アドレス重複時にも通信を可能とする手法を提案した。実験により提案手法はアドレス重複時においても重複していないかのように通信でき、この手法が有用であることを確認した。

今後の課題として、提案手法の実装における処理時間の改善やより具体的な検証が挙げられる。まず、処理時間の改善については、変換データの保持方法の見直し、Linux カーネルの BPF を用いて実装するなどが考えられる。また、検証については、暗号化通信や様々な OS での動作についてより詳しく検証していく必要があると考える。

参考文献

[1] F. Costa, X. Pougnard, H. Li, “Duplicate Address Detection Proxy”, RFC 6957, November 2021.
[2] 北村浩, 阿多信吾, 村田正幸, セッション多重化技術の刷新により安心・安全な通信を実現する IPv6 Unified Multiplex 通信アーキテクチャの研究開発, 戦略的情報通信研究開発推進制度(SCOPE) 第 6 回成果発表会(平成 22 年), November 2021.