IPネットワークシステムにおけるセキュアかつスケーラブルなユーザ収容方式の検討

押海 卓志† 北村 雅一† 小田 孝和‡ 西尾 修一† 本野 智治†

†NTT 西日本研究開発センタ ‡NTT 西日本技術部

概要

ユーザにIPアドレスを固定的に割り当てる常時固定IPネットワークでは、加入者のIPアドレス詐称やユーザ間の盗聴を防止することが重要である。加えて、ユーザへ効率的にIPアドレスを割り当てる必要がある。本稿では、従来のユーザ収容方式を比較検討することで、これらのユーザ収容方式がセキュリティもしくはスケーラビリティ上の課題を有することを示す。さらに、RFC3069で規定された論理構成にARPフィルタ機能を追加した新たなユーザ収容方式を提案する。

A New Method for Subscriber Aggregation with Security and Scalability.

Takashi Oshiumi † Masakazu Kitamura † Yoshikazu Oda ‡ Shuichi Nishio † Tomoharu Motono †

†NTT-West Research & Development Center ‡NTT-West Technology Department

Abstract

With the population of broadband IP connections, more and more users are connected to the network, 24 hours a day, with fixed IP addresses. This population of stable connectivity is also causing some serious matters on user information security. Thus, on designing career-class subscriber networks, concerns should be made not only on system scalability, but also on security between each subscriber.

In this paper, we first compare various traditional methods for subscriber aggregation, and show that each method has weakness either in security or scalability. Thus, we propose a new method for subscriber aggregation, based on RFC3069, which satisfies both security and scalability issues.

1 はじめに

近年、広帯域IP通信サービスの普及は著しい。数Mbps程度のインターフェースを提供するxDSLのユーザ増加だけではなく、光ファイバーを利用して100Mbpsのインタフェースを提供するIPサービスも普及しつつある[1]。このような広帯域なネットワークを安価に提供できる背景には、ビット単価の低廉化が大きく寄与している。特にEthernetを利用した技術はその傾向が著しく、今後も低コストでIPネットワークを構築する手段の一つとして利用されることは容易に想像できる。本稿では、IPアドレスを固定的にユーザに割り当てる常時固定IPネットワークを想定している。常時固定IPネットワークでは、ユーザをIPアドレスから一意に識別することができるので、認証や課金などへの展開を容易に行うことができる。常時固定IPネットワークを通信事業者が提供する場合、通信事業者はIPアドレスを効率的にユーザへ割り当てることが必要である。また、ユーザが不正なIPアドレスを端末に設定して通信を行うIPアドレス詐称問題やブロードキャストパケットの盗聴問題などを防止することは、重要な課題である。

そこで、本稿では、Ethernet技術を利用してアクセ

ス回線を構築した場合に発生する課題を明らかにするとともに、これらの問題点を解決した、セキュアでかつスケーラブルなユーザ収容方式の提案を行う。

2　従来のユーザ収容方式の概要

Ethernet 技術を利用してアクセスラインを構築した場合、L2 スイッチや PON[2]などに加入者を収容して回線を集約したのち、ルータや L3 スイッチなどのユーザ収容装置へ接続する形態が考えられる。本節では、このような物理構成を有した常時固定 IP ネットワークを前提とする。

2-1 ブロードキャストドメインを共有したユーザ収容方式

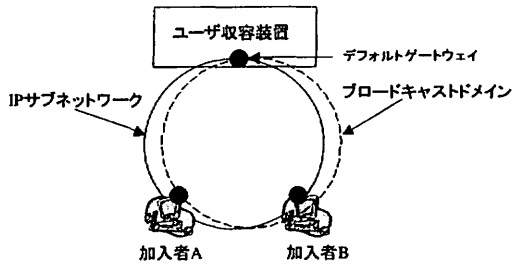

図 1　ブロードキャストドメインを共有したユーザ収容方式

本方式を、以下 L2 方式と呼ぶ。

このユーザ収容方式は以下の(a)および(b)に示した論理構成を有している。

(a)Ethernet のブロードキャストドメインを複数の加入者が共有する。

(b)ブロードキャストドメイン境界と IP サブネットワーク境界が一致しており、一つの IP サブネットワークを複数の加入者が共有する。

この構成では、図 1 で示されたすべての加入者端末またはユーザ収容装置から送出されるブロードキャストパケットが、ブロードキャストドメイン全体にフォワーディングされる。

また、図 1 で示されたすべての加入者は、ブロードキャストドメインに割り当てられた IP サブネットワークに含まれるどのような IP アドレスを設定しても、それが IP サブネットワーク内で一意であれば、通信することができる。

2-2 加入者ごとに IP サブネットワークを割り当てたユーザ収容方式

本方式を以下、L3 方式と呼ぶ。

このユーザ収容方式は以下に示す論理構成を有している。

(a)加入者ごとにブロードキャストドメインを割り当てる。

(b)加入者ごとに割り当てたブロードキャストドメインに IP サブネットワークを割り当てる。一つの IP サブネットワークに含まれる加入者は唯一である。

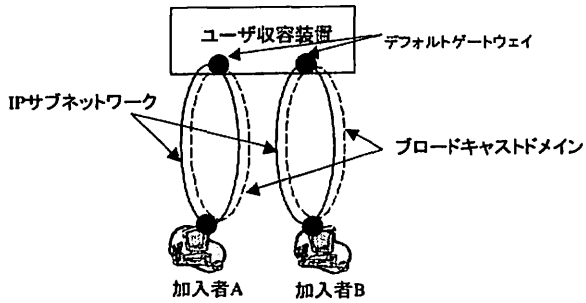

図 2　加入者ごとに IP サブネットワークを割り当てたユーザ収容方式

(a)および(b)から L3 ユーザ収容方式は、以下に示す(1)～(3)の特徴を有する。

(1)加入者端末が送出するブロードキャストパケットは、他の加入者へフォワーディングされない。

(2)加入者は割り当てられた IP サブネットワークにおける IP ホストアドレスを、自身の端末の IP アドレスとして利用できる。それ以外の IP アドレスを設定した場合は、通信を行うことができない。

(3)加入者ごとに IP サブネットワークを割り当てているので、前述の L2 方式と比較して多大な量の IP アドレスが必要となる。その差は、加入者数と加入者に割り当てる IP サブネットワークの大きさにに依存する。図 3 に、クラス C の IP（サブ）ネットワークに複数の加入者を収容した L2 方式と 30 ビットマスクの IP サブネットワークを加入者ごとに割り

当てたL3方式に必要なIPアドレス数の関係を示す。

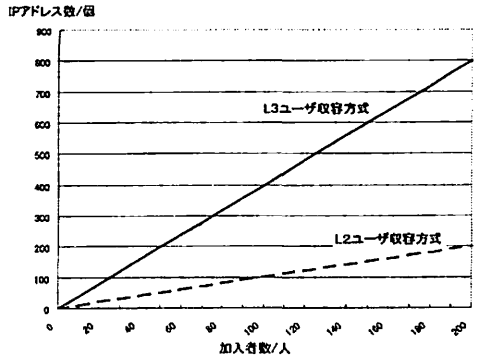

図3　加入者数と必要なIPアドレス数の関係

このように、L2方式と比較して、L3方式で多くのIPアドレスが必要になるのは、L3方式では、加入者に割り当てるIPアドレスの他に、加入者数に等しい数のデフォルトゲートウェイアドレス、ネットワークアドレスおよびブロードキャストアドレスが必要となるためである。

2-3 VLAN　Aggregationによるユーザ収容方式

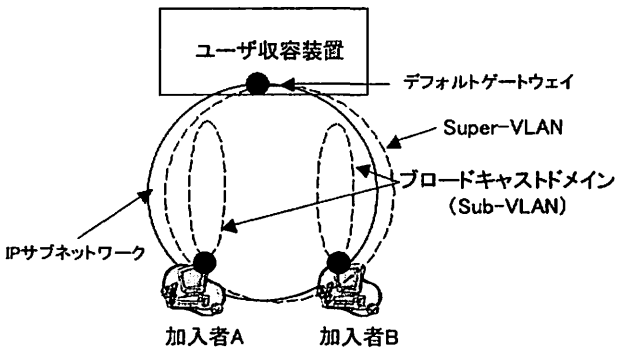

図4　VLAN　Aggregationによるユーザ収容方式

本方式を以下、VLAN　Aggregation方式と呼ぶ。

本方式は、RFC3069[3]において規定されている論理構成に基づいたユーザ収容方式である。RFC3069では、Sub-VLANによってブロードキャストドメインを分割し、分割した複数のSub-VLANを一つのSuper-VLANに所属させて、IPサブネットワークをSuper-VLANに割り当てる論理構成を提案している。

VLAN　Aggregation方式では、加入者ごとにSub-VLANを割り当てる。

しかしながら、この構成では、ARPパケット[4]がSub-VLANを超えてフォワーディングされないため、加入者は他のSub-VLANに所属する加入者端末のMACアドレスを解決できない。この問題を解決するためには、加入者端末が送出するARPリクエストパケットをユーザ収容装置がProxy処理[5]することが必要である。ARPパケットのProxy処理の必要性は、RFC3069でも触れられている。

また、IPサブネットワークがSuper-VLANに対して割り当てられているので、IPマルチキャストはSuper-VLAN全体へ転送される。マルチキャストグループに参加要求を行った加入者へのみマルチキャストトラヒックを転送するためには、ユーザ収容装置がSub-VLANごとのIGMPスヌーピング機能を実装している必要がある。

以上のことから、VLAN　Aggregation方式は、以下に示す(1)～(3)の特徴を有する。

(1)加入者端末が送出するブロードキャストパケットは、他の加入者へフォワーディングされない。

(2)ユーザ収容装置が、加入者端末へ送出するARPリクエストパケットは、Super-VLANに所属するすべての加入者へ送出される。

(3)IPアドレス数は、L2方式と等価である。

3　従来のユーザ収容方式の評価と課題

3-1　セキュリティに関する評価

ネットワークにおけるセキュリティ上の脅威として、DoS攻撃やフラッディング、IPアドレス詐称、盗聴問題などが挙げられる。本項で取り扱うセキュリティは、ユーザ収容方式と深く関連のある、IPアドレス詐称およびブロードキャスト問題をスコープとしている。

(a)IPアドレス詐称問題

加入者が意図的にまたは誤って、割り当てられたIPアドレス以外のIPアドレスを端末に設定して通信を行うことは、重大な問題を発生させる場合がある。特にIPアドレスでユーザを識別して認証などを行うネ

ットワークモデルでは対策が必須である。また、悪意を持った加入者が他の加入者に成りすまして通信を行うという問題がある。

(b)ブロードキャスト問題

加入者またはユーザ収容装置が送出したブロードキャストが、他の加入者へフォワーディングされる環境下では、Ethernet のブロードキャストによる通信が行われる可能性がある。良く知られているところでは、Microsoft 社の NetBIOS の通信がある。

また、ブロードキャストによるデータ通信が、他の加入者までフォワーディングされることによって盗聴されるという問題がある。

(a)の問題は、L2 方式および VLAN Aggregation 方式で発生する。

L2 方式および VLAN Aggregation 方式では、ユーザ収容装置が加入者端末に対する ARP 解決のために送出する ARP リクエストパケットが、同一 IP サブネットワークに所属する全加入者に受信されるため、加入者は、他の加入者に割り当てられた IP アドレスを不正に端末に設定して ARP レスポンスパケットを返すことで、ユーザ収容装置の ARP テーブルに、不正な情報を記録させることが可能になる。これにより、加入者は他の加入者に割り当てられた IP アドレスを使って通信することが可能になる。

一方、L3 方式では、加入者と IP サブネットワークが一意にマッピングされているので、ユーザ収容装置は、ARP リクエストパケットをターゲットとする加入者端末が所属する IP サブネットワークにのみ送信する。したがって、L3 方式では(a)の問題は発生しないことがわかる。

また、(b)の問題は、L2 方式のように複数の加入者が単一の Ethernet ブロードキャストドメインを共有しているために発生する。一方、VLAN Aggregation 方式では、加入者端末から送出されるブロードキャストを加入者ごとに割り当てられた Sub-VLAN 内に閉じこめることができるので、加入者端末が送出したブロードキャストは、他の加入者へフォワーディングされない。しかしながら、ユーザ収容装置が送出する ARP リクエストパケットは、すべての Sub-VLAN へ向けて送出される。ARP リクエストパケットには、ターゲットとなる加入者端末の IP アドレスが含まれているため、Super-VLAN 内に所属するすべての加入者は、この ARP リクエストパケットに含まれている IP アドレスを検知することができる。これは、加入者に関連する情報を不必要に他の加入者に知られることを防ぐ意味で、防止できることが望ましい。

3-2 スケーラビリティ性に関する評価

IP アドレスが貴重なリソースとなるケースでは、加入者へ効率よく IP アドレスを割り当てることが重要な課題である。

L3 方式では、2 節で検討したように、L2 方式や VLAN aggregation 方式と比較して大量のアドレスが必要となる。

3-3 従来のユーザ収容方式の比較

従来のユーザ収容方式の評価を表 1 に示す。

表 1 ユーザ収容方式の評価結果

項目		L2方式	L3方式	VLAN Aggregation 方式
セキュリティ	IPアドレス詐称問題	×	○	×
	ブロードキャスト問題	×	○	△
スケーラビリティ	効率的なIPアドレスの割り当て	○	×	○

表 1 から、セキュリティに関しては、L3 方式が他方式と比較して優れていることがわかる。L2 方式ではセキュリティに関する問題が解決されない。VLAN Aggregation 方式では、加入者端末が送出するブロードキャストパケットは、加入者ごとに割り当てられた Sub-VLAN 内に閉じ込められるので、ブロードキャスト問題の一部が解決している。しかしながら、ユーザ収容装置が送出する ARP リクエストパケットが、す

べての Sub-VLAN へ送出される問題が残る。また、VLAN Aggregation 方式では、IP アドレス詐称問題が解決されない。

スケーラビリティについては、VLAN Aggregation 方式と L2 方式が、L3 方式と比較して優れている。

本検討から、従来のユーザ収容方式は、それぞれに課題を有していることがわかる。そこで、次節では、VLAN Aggregation 方式をベースにセキュリティとスケーラビリティを兼ね備えた、新たなユーザ収容方式を提案する。

4 ARP フィルタ機能を追加した拡張型 VLAN Aggregation 方式

本方式を以下、拡張型 VLAN Aggregation 方式と呼ぶ。本方式は、VLAN Aggregation 方式に ARP フィルタ機能が追加されていることを特徴としている。

4-1 ARP フィルタ機能の検討

本方式における ARP 解決から IP 通信までのシーケンスを図 5 と図 6 に示す。

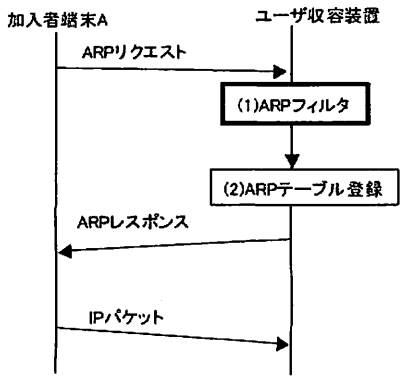

図 5 加入者端末 A が ARP リクエストを送出するシーケンス

ARP フィルタ機能を実現するには、ユーザ収容装置に、加入者ごとに割り当てられた Sub-VLAN の VLAN-id[6]と IP アドレスの対応テーブル（以下、アドレステーブルと呼ぶ）を備える必要がある。

図 5 では、ユーザ収容装置は、加入者端末から送出された ARP リクエストパケットに含まれる加入者 IP アドレスと MAC アドレスの対を ARP テーブルに記録する前に、ARP リクエストパケットに含まれる送信元

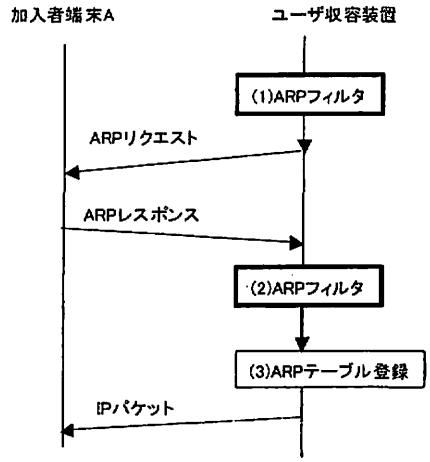

図 6 ユーザ収容装置が ARP リクエストを送出するシーケンス

IP アドレスをキーにして、アドレステーブルを検索し、ARP リクエストパケットに含まれる加入者 IP アドレスが不正な IP アドレスか否かを判定する。そして、不正な IP アドレスの場合は ARP リクエストパケットを廃棄する。図 6 の(1)では、ユーザ収容装置は、ARP リクエストパケットを送出する前に、アドレステーブルを検索し、ARP 解決を行うターゲット加入者端末がどの Sub-VLAN に存在するかを判定して、該当する Sub-VLAN へのみ ARP リクエストパケットを送出する。(2)では、ユーザ収容装置は、加入者端末から送出された ARP レスポンスパケットに対して、図 5 の(2)と同様に、ARP レスポンスパケットに含まれる Sub-VALN の VLAN-id と送信元 IP アドレスを抽出して、アドレステーブルを検索することにより、送信元 IP アドレスが不正に設定された IP アドレスか否かを判定し、不正に設定された IP アドレスの場合は ARP レスポンスパケットを廃棄する。

4-2 提案方式の評価

VLAN Aggregation 方式の課題は以下の 2 点である。

(a)IP アドレス詐称問題

(b)ARP に関するブロードキャスト問題

以下、(a), (b)について評価を行う。

(a)に関しては、図 5 で加入者 A が加入者 B の IP ア

ドレスを端末に設定して（IPアドレス詐称）、ARPリクエストパケットを送出すると、ユーザ収容装置は、ARPフィルタ機能によって加入者端末Aから送出されたARPリクエストパケットを廃棄する。これにより加入者AのIPアドレス詐称を防止できる。図6で加入者Aが加入者BのIPアドレスを端末に設定（IPアドレス詐称）していても、ユーザ収容装置は加入者Bをターゲットとする ARP リクエストを加入者Aが所属する Sub-VLAN には送出しないので、加入者Aは加入者Bとして通信を行うことができない。これによりIPアドレス詐称を防ぐことができる。また、(b)は、ユーザ収容装置が ARP リクエストパケットをすべての Sub-VLAN へ送出するために、加入者が他の加入者の IP アドレスとある程度の通信状況を知ることができる問題である。これは、加入者に関連する情報を不必要に他の加入者に知られることを防ぐ意味で、防止できることが望ましい。本提案方式では、図6で示したように、ユーザ収容装置は、ARP リクエストパケットをターゲットととする加入者端末が存在するSub-VLAN へのみ送出するので、この問題は発生しない。

5 まとめ

本稿では、IP ネットワークシステムにおける従来のユーザ収容方式を比較検討し、従来のユーザ収容方式では、セキュリティまたはスケーラビリティに関してそれぞれ課題を有することを明らかにした。さらに、課題を解決し、セキュリティとスケーラビリティを兼ね備えた拡張型VLAN Aggregation方式を提案した。本提案方式は、IPアドレス数を加入者に効率的に割り当てることができる RFC3069 で規定された論理構成に、セキュリティを強化するために ARP フィルタ機能が追加されていることを、特長とする。ARP フィルタ機能により、割り当てられたIPアドレス以外のIPアドレスを送信元IPアドレスとするARPリクエストパケットおよび ARP レスポンスパケットを廃棄することを可能にした。さらに、ユーザ収容装置が送出するARP リクエストパケットをターゲット加入者端末が所属するSub-VLANへのみ送出することで、L3方式と同等のセキュリティ機能を実現した。これらの結果、IPアドレス詐称問題、ブロードキャスト問題が解決した。

本稿で述べた、拡張型VLAN Aggregation方式を実現するための機能を、現在実装している市販製品としては、今回検証を行った古河電気工業株式会社製のルータ、FITELnet-Gシリーズがある。実機による検証の結果から、提案方式が本稿で示した問題を解決することを確認した。

謝辞

本検討にあたりご協力いただいた安田圭一様、福富昌司様を始めとする古河電気工業株式会社の皆様に感謝します。

参考文献

[1] 総務省：平成13年版 情報通信白書 http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h13/index.htm, 2001

[2] 三木 哲也, 青山 友記 監修, マルチメディア通信研究会 編, "xDSL/FTTH 教科書", アスキー, 1999

[3]D. McPherson and B. Dykes," VLAN Aggregation for Efficient IP Address Allocation", Feb. 2001, RFC3069

[4] David C. Plummer, "An Ethernet Address Resolution Protocol -- or -- Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware", RFC826, Nov.1982

[5] Smoot Carl-Mitchell and John S. Quarterman, "Using ARP to Implement Transparent Subnet Gateways", RFC 1027, Oct. 1987

[6]IEEE Std 802.1Q-1998, "Virtual Bridged Local Area Networks", IEEE, 1998