2V－3

# 広域ネットワーキングサービスプラットフォームにおけるVLANサービス

針生 剛男、 有永 憲一、 佐藤 基、 村山 純一
NTTマルチメディアネットワーク研究所

## 1．はじめに

近年、イントラネットが急速に普及し、企業は自社オフィス内のイントラネットでグループウェアやデータベースを運用して、生産性を向上させている。しかし、オフィスが広範囲に点在する企業では、全社的なイントラネットを築くのは容易ではない。各オフィスを専用線で接続するのはコストがかかり、小規模な企業には負担が重い。また、各オフィスをインターネット経由で接続する方法は、それぞれのオフィスで複雑なルータの設定が必要になり、さらにセキュリティの問題も生じる。

インターネットユーザの急増やアプリケーションの高速化に応えるため、ATMを用いた広域ネットワーキングサービスプラットフォームの検討が行われている[1,2]。広域ネットワーキングサービスプラットフォームでは、グローバルなインターネット接続だけでなく、パケットのルーチング機能とフォワーディング機能の分離により、物理的位置に依存しない広域VLAN（Virtual LAN）を実現することも目標にしている。広域VLANは従来のLANと同等の環境を広域で実現するため、企業ユーザは低コストで広域のイントラネットを容易に構築できる。本稿では、サービスの観点から、企業ユーザの広域イントラネット構築に必要なVLANの形態と、ネットワークに必要になる機能について述べる。

## 2．VLAN

一般にVLANは、構内で、フロアや部屋等の物理位置単位ではなく、組織単位にサブネットを構築したり、組織の移動に設定だけで対応したりするために用いられる。物理的位置ではなく組織を単位とする理由は、

・組織を単位としたサブネット管理が可能
・組織を単位としたセキュリティ管理が可能
・組織内端末移動が可能

等である。

LANスイッチによるVLANはIEEE802.1Qにおいて規格化が進められている。またIP over ATMやLAN Emulationを用いてVLANを実現することも可能である。VLANを構成する際のグルーピング単位の観点から、スイッチングハブのポート等を単位とするレイヤ1 VLAN、端末のMACアドレスを単位とするレイヤ2 VLAN、IPアドレス、ATMアドレス等レイヤ3アドレスを単位とするレイヤ3 VLANがある。また、ユーザから見えるVLANの形態は、イーサネット等のレイヤ2 LANセグメントと、レイヤ3サブネットがある。

表1．VLANの分類

| 形態＼構成単位 | レイヤ1（ポート） | レイヤ2（MACアドレス） | レイヤ3（IPアドレス等） |
|---|---|---|---|
| レイヤ2 LANセグメント | スイッチングハブ（ポート単位VLAN） | スイッチングハブ（MACアドレスVLAN） | LAN Emulation |
| レイヤ3 サブネット | | | レイヤ3VLAN-SW IP over ATM MPOA |

## 3．広域VLAN

広域ネットワーキングサービスプラットフォームでは、VLANを広域で提供する。インターネット接続と比較すると、

・組織単位のサブネット管理が可能
・組織単位のセキュリティ管理が可能
・組織内端末移動が可能
・プライベートアドレス、マルチプロトコルが利用可能
・ブロートキャストパケットを利用したアプリケーションが使用可能

といったメリットがある。

グルーピングの単位は基本的に構内と同じで、ポート、つまり加入者収容点を単位とするレイヤ1 VLAN、MACアドレスを単位とするレイヤ2 VLAN、IPアドレス等を単位とするレイヤ3 VLANが可能である。しかし、様々なユーザが使用する広域ネットワーキングサービスプラットフォームにおいてレイヤ2 VLAN、レイヤ3 VLANを用いると、部外者にアドレスを詐称され侵入される危険性があるため、端末認証機能を付加することが必須になる。本稿では、以降レイヤ1 VLANについて述べる。

ユーザから見た広域ネットワーキングプラットフォームで実現されるVLAN形態として、以下に示すバリエーションが考えられる。

(1) 広域LANセグメント

広域で仮想的なイーサネット等のLANセグメントを提供する。ネットワークは仮想的なスイッチングハブ、またはブリッジとして動作し、イーサネットフレームを転送する。ユーザはTCP/IP以外にもAppleTalk、NetBEUI、IPX等様々なプロトコルを利用できる。各オフィスが小規模である場合にはオ

---

VLAN service on a Global Networking Service Platform
Takeo Hariu, Kenichi Arinaga, Motoi Sato, Junichi Murayama
NTT Multimedia Networks Lab.

フィス間のルータが不要で、全体のネットワーク管理が容易になる。 端末はLANセグメント内を自由に移動することができる。

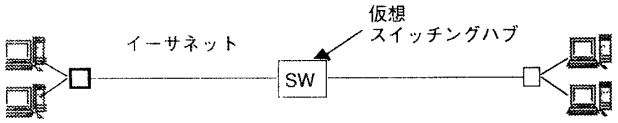


図3-1. 広域LANセグメント

(2) 広域IPサブネット

広域で仮想的なIPサブネットを提供する。ネットワークは仮想的なスイッチングハブ、またはProxy ARPルータとして動作する。後者はIPパケットが転送されるため、マルチプロトコルは利用できないが、オーバヘッドの少ない効率的な転送が可能になる。この場合パケットはIPアドレスによりルーチングされるため、サブネット内であっても端末移動にはProxy ARP設定の変更が必要である。

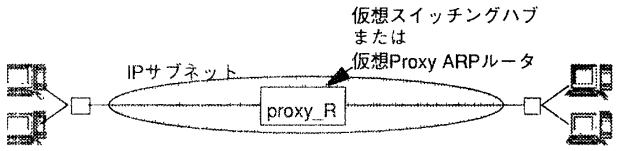


図3-2. 広域IPサブネット

(3) 広域ルータ接続

広域で、サブネット間を直接ルータ接続した環境を提供する。ネットワークは仮想的なプライベートルータとして動作する。ユーザは複数サブネットを接続したグループ内でプライベートアドレスが利用できる。また、グループ内のパケットは外部インターネットを経由しないため、グループ内のセキュリティは外部接続するルータのファイアウォール一箇所で管理できる。プライベートルータにファイアウォール機能を設けることにより、内部サブネット間セキュリティ、外部接続セキュリティの両方を管理可能になる。この形態は、個々のオフィスで既に多数のユーザがいる場合や、エクストラネットのように多段階のセキュリティ管理をしたい場合に有効である。

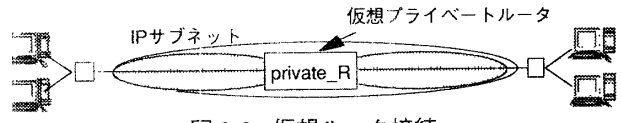


図3-3. 仮想ルータ接続

(4) グローバルインターネット接続

これ自体はVLANではないが、通常のインターネットユーザと同様、インターネット接続を提供する。ネットワークはインターネットのルータとして動作する。

ユーザはこれらのバリエーションのうちひとつを選択するのではなく、オフィスや利用形態に応じて自由に組み合わせて利用できる。利用形態例を図3-4に示す。

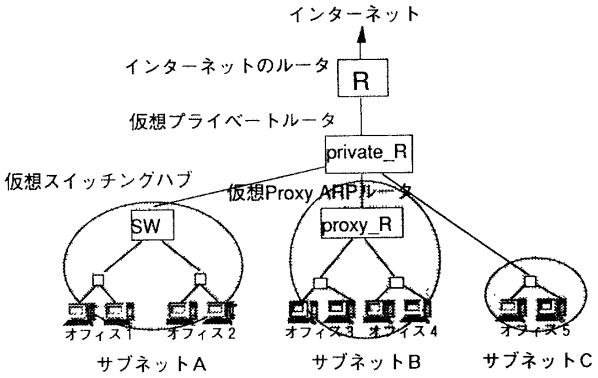


図3-4 VLAN利用形態例（ユーザからの見え方）

## 4．ファイアウォール、NAT (Network Address Translator)

イントラネットをインターネットに接続する場合、セキュリティを保つファイアウォール機能が必要になる。さらに内部のセキュリティ管理を行う場合は、サブネット間ファイアウォール機能も必要になる。また、プライベートIPアドレスを使用している場合、グローバルIPアドレスに変換するNAT機能が必要になる。仮想プライベートルータのユーザには、これらの機能を仮想プライベートルータで提供することにより、ユーザ側でファイアウォールやNATを用意しなくても、セキュリティ確保、アドレス変換が可能になる。これらの機能は、ユーザ側のネットワーク管理者からの設定を可能にするため、設定インタフェースがオープン化され遠隔設定機能が実現されることが望ましい。

## 5．まとめ

広域ネットワーキングサービスプラットフォームにおけるVLANサービスの形態と、必要な機能について検討した。広域LANセグメント、広域IPサブネット、広域ルータ接続の形態があり、ネットワークにはそれぞれ仮想スイッチングハブ、(仮想Proxy ARPルータ、) 仮想プライベートルータとしての機能が必要である。また、インターネット接続のため、仮想プライベートルータにおいてファイアウォール機能、NAT機能の提供が必要になる。

---

[1] K.Koyanagi, T.Saito, T.Kanada, and K.Kitami, "Technology Initiative for the Near Future in Internetworking ", IEEE Communications Magazine, May 1997

[2] 村山 他、"広域ネットワーキングサービスプラットフォームの設計"、信学技報 IN97-39 (1997-05)