大規模VLAN環境におけるVLANの相互接続方式

岡山 聖彦† 山井 成良†† 岡本 卓爾‡

概 要

本論文では，部署ごとに独自管理されたVLANで構成される大規模な組織ネットワークにおいて，会議室等の共通スペースに設定された一時利用のためのVLANを，利用者の所属するVLANに相互接続するための方式を提案する．提案方式では，一時利用のためのVLAN識別子を部署ごとに動的に割り当て，さらに，これらの異なるVLAN識別子を相互変換することにより，共通スペースに接続する一時利用者が，自己の所属する部署のVLANにシームレスに接続する機能を実現する．

A Method of Interconnection of VLANs for Large-scale VLAN Environment

Kiyohiko Okayama† Nariyoshi Yamai†† Takuji Okamoto‡

Abstract

In this paper, we propose a method which provides the interconnection between the temporary configured VLAN in the common spaces such as conference rooms and the user's VLAN in the large-scale organization network which is managed independently by departments. In this method, The function of connecting temporary user's VLAN in the common space to the VLAN to which the user belongs seamlessly is achieved by allocating VLAN-ID for temporary use in each department dynamically and converting these VLAN-IDs each other.

1 はじめに

現在，物理ネットワークの形態に依存することなく論理ネットワークを構成することの可能なVLAN技術が急速に普及しつつある．VLAN技術によれば，VLANに対応したスイッチ(以下，VLANスイッチという)の設定変更のみで論理ネットワークの構成を変更できるので，会議室のような共通スペースにおいて，利用者の所属部署のネットワークへの一時的なアクセスが容易に実現できる．

しかし，従来のVLAN構成手法ではVLANが静的に管理されるので，一時利用開始時にすべてのVLANスイッチの設定を手動で行うか，あるいは一時利用に必要なすべてのVLANをあらかじめ設定しておくしかない．このため，前者の場合には管理の手間が大きいという問題があり，後者の場合，VLANが部署ごとに独立して管理されていると，部署間でVLAN識別子の衝突が生じたり，VLANスイッチによっては設定可能なVLAN識別子の数を超過する可能性がある．

そこで，本研究では，VLANが部署ごとに独自管理されている大規模な組織ネットワークを前提とし，上記の諸問題を解決するための，VLAN識別子の動的変換に基づいたVLAN相互接続方式の提案と，これを実現するためのシステムの設計を行う．提案方式では，部署ごとに一時利用のため

†岡山大学工学部, Faculty of Engineering, Okayama University
††岡山大学総合情報処理センター, Computer Center, Okayama University
‡岡山理科大学工学部, Faculty of Engineering, Okayama University of Science

のVLAN識別子をあらかじめ一定数確保し，利用者が共通スペースの情報コンセントへの接続時にVLAN識別子を動的に割り当てる．さらに，部署ごとに独自に割り当てられたVLAN識別子を相互変換することにより，共通スペースから利用者が所属する部署のネットワークへのデータリンク層レベルでの接続を実現としている．

本論文では，前提とするネットワーク環境と従来のVLAN構成手法の問題点について考察した後，提案手法の概要とこれに基づいたシステムの設計について述べる．

2 前提とするネットワーク環境と問題点の整理

1で述べたように，本研究では，部署ごとにVLANが独自管理されている組織ネットワークを対象としている．このとき，規模がある程度大きな組織では，組織の構造と同様に，ネットワークも階層的に構成および運用管理されるのが一般的である．

そこで本研究では，組織ネットワーク全体を統括する部署(計算機センタなど)が管理する基幹ネットワークが階層の最上位にあるものとし，これに各部署が管理するネットワークが接続するものとする．部署によっては，その規模に応じてさらに部署ネットワーク内部を階層的に構成することもあるが，簡単化のため，図1のように2つの階層で構成されるものとする．図1において，基幹および部署ネットワークはそれぞれ1つ以上のVLANスイッチで構成される．複数のVLANスイッチを跨る通信については，IEEE802.1Q[1]で定められたVLANタギング機能を用いて各VLANに固有のVLAN識別子を割り当てるものとし，VLAN識別子の割り当てを含めたVLANの運用管理は各ネットワークで独自に行なうものとする．また，会議室などの共通スペースは，説明の簡単化のために，基幹ネットワークに含まれるものとする．

このような構成のネットワークにおいて，組織内の利用者が，共通スペースから自己の所属する部署ネットワークに接続して一時利用することを考える．従来のVLAN構成手法では，VLAN識別子は静的に管理されるので，上述した一時利用を

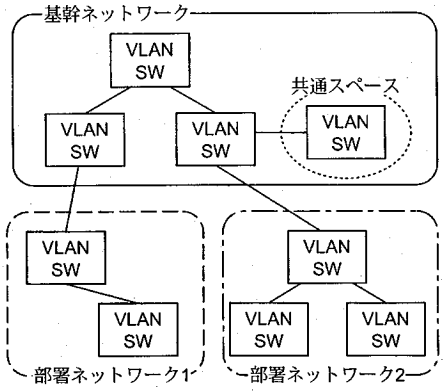

図 1: 前提とする組織ネットワークの構成例

実現するには，以下の2つの方法が考えられる．

方法1 利用者の接続時に各ネットワークの管理者が手動で一時利用のためのVLANを設定

方法2 一時利用に必要と予想されるすべてのVLANをあらかじめ設定

方法1については，文献[2]で提案されているVLAN管理システムを用いることにより，一時利用の開始・終了に伴うVLAN管理の手間をある程度軽減できると考えられる．しかし，文献[2]のVLAN管理システムは，組織全体のVLANスイッチを一元的に管理することを前提としているので，VLANが各ネットワークで独自管理されているような環境にはそのまま適用することができない．さらに，VLANの追加および削除は管理者が管理サーバのデータベースを手動で変更することによって実現されているので，一時利用のようにVLANが頻繁に追加および削除される場合には，管理者にかかる負担が大きいと考えられる．

方法2は，組織全体で一時利用のためのVLAN識別子をあらかじめ確保すると同時に，共通スペースから各部署ネットワークに一時的に接続するためのVLANをあらかじめ設定しておく方法である．しかし，組織全体で同一のVLAN識別子を確保するため，部署ネットワークで割り当て可能なVLAN識別子に制約が生じる可能性がある．さらに，IEEE802.1QではVLAN識別子を12ビットで表現するため，規格上は値0，1，および4095を除

く4093個のVLANが設定可能であるが，VLANスイッチによっては設定可能なVLANの数がこれよりも少ない場合があるので，このような機器が存在すると一時利用のために必要なすべてのVLANを割り当てることができない可能性もある．

一方，共通スペースなどに設置された情報コンセントにおいて，利用者の認証結果に応じてあらかじめ設定された複数のVLANを切り替えることにより，共通スペース外のネットワークとの接続性を確保する方式[3][4]が提案されている．しかし，いずれの方式も，VLANの構成手法という点では方法2と同様であるため，方法2と同様の問題が生じる可能性がある．また，文献[4]の方式は，共通スペース外のネットワークとの接続をNAT[5][6]により実現しているので，利用者が認証時に取得したIPアドレスをそのまま利用できるという利点があるが，IP以外の通信方式に頼るアプリケーションが利用できないなど，利用者から見たネットワークの透過性に制約がある．

3 VLANの相互接続方式

3.1 要求条件

2で述べた問題のうち，VLANの構成手法に起因する問題を解決するためには，以下の条件を満たす必要がある．

条件1 一時利用のためのVLAN識別子の割り当ておよびVLANの設定が自動で行なえること

条件2 一時利用のための共通のVLAN識別子を組織全体で確保する必要がないこと

さらに，共通スペース利用時のセキュリティや利用者に対する利便性を考慮すれば，以下のような条件を満たすことが望ましい．

条件3 一時利用開始時に，利用者認証により接続の可否および接続先の制御が行なえること

条件4 利用者が共通スペースから自己の所属する部署ネットワークに対してデータリンク層レベルで接続できること

3.2 VLAN識別子の動的割り当てと相互変換

3.1で述べた要求条件のうち，条件1を満たすには，文献[2]のようなVLAN管理システムを各ネットワークに導入し，これにVLAN識別子の動的割り当て機能を追加することにより，共通スペースの利用者からの要求に応じて，利用者が所属する部署ネットワークに至るまでの各ネットワークにおいて一時利用のためのVLAN識別子を動的に割り当て，必要なVLANスイッチの設定を自動的に行なう方法が考えられる．しかし，このときに割り当てられるVLAN識別子は各ネットワークで異なるため，そのままではネットワークを跨ぐ通信を行なうことができない．

そこで本論文では，VLAN識別子の動的割り当て機構に，VLAN識別子の相互変換機構を組み合わせたVLANの相互接続方式を提案する．具体的には，基幹ネットワークと部署ネットワークの境界にVLAN識別子変換サーバを設け，各ネットワークを跨って送受信されるフレームに含まれるVLAN識別子の相互変換を行なう．これにより，一時利用のために確保するVLAN識別子の番号や数は各ネットワークで自由に決めることができるので，条件2を満たすことができる．

さらに，共通スペースの情報コンセント利用時の認証については，既存の認証システム[3][4][7]を適用することができる．これにより，利用者認証を行なうと共に，利用者が接続するVLANスイッチのポートに基幹ネットワークで割り当てられた一時利用のためのVLANを設定することにより，条件3および条件4も満たすことができると考えられる．

4 VLAN相互接続システムの設計

4.1 システムの構成

3で述べたVLAN相互接続方式を実現するための，システム構成例を図2に示す．図中の“SW”はVLANスイッチを示しており，利用者が一時利用を行なう場合には，共通スペース内のVLANスイッチのポートに計算機を接続する．

本システムは，VLAN識別子の動的割り当てを

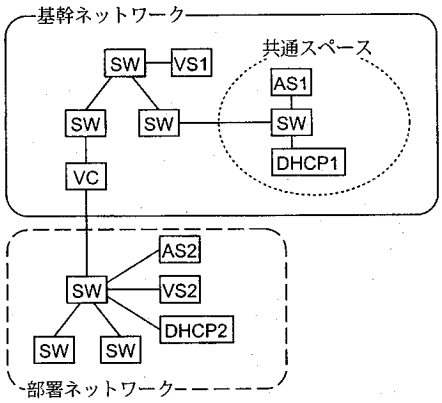

図 2: VLAN相互接続システムの構成例

行なうVLAN管理サーバと，基幹ネットワークと部署ネットワーク間でVLAN識別子の相互変換を行なうVLAN識別子変換サーバを中心に構成される．以下に，VLANスイッチ以外の主要な構成要素の役割を列挙する．

- 認証サーバ (AS1およびAS2)

  共通スペースと部署ネットワークにそれぞれ一つ設置し，利用者の認証を行う．

- DHCPサーバ (DHCP1およびDHCP2)

  共通スペースと部署ネットワークに一つ設置する．共通スペースのDHCPサーバ (DHCP1) は認証時に必要なIPアドレスを利用者の計算機に割り当て，部署ネットワークのDHCPサーバ (DHCP2) は認証に成功して一時利用のためのVLAN設定が完了した後に，利用者の計算機にIPアドレスを割り当てる．

- VLAN識別子管理サーバ (VS1およびVS2)

  基幹ネットワークと部署ネットワークにそれぞれ一つ設置し，認証サーバからの要求に応じて一時利用のためのVLAN識別子を管理する．

- VLAN識別子変換サーバ (VC)

  基幹ネットワークと部署ネットワークの境界に設置し，基幹ネットワークのVLAN識別子管理サーバからの指示により，フレームに含まれるVLAN識別子の相互変換を行う．

なお，利用者が共通スペースのVLANスイッチに接続する計算機を除き，本システムを構成する各サーバ間では，少なくともIPによる通信が行なえるように設定されているものとする．

4.2 認証情報の管理と接続先の決定方法

利用者が共通スペースから接続する部署ネットワークを決定するためには，文献[4]の方式のように，利用者認証時のユーザ識別子に接続先となるVLAN識別子を埋め込む方法がある．しかし，本論文では基幹ネットワークと部署ネットワークで独自にVLANが管理されるので，共通スペースの認証サーバが利用者の所属する部署ネットワークのVLAN識別子を把握するのは困難である．また，大規模な組織では利用者数が多いので，共通スペースに設置する認証サーバですべての利用者の認証情報を管理するのは困難であるという問題もある．

そこで，本システムでは，DNSのドメインが組織の構造に合わせて構成されることが多いことに注目し，基幹ネットワークを組織ネットワークの最上位ドメイン，部署ネットワークをサブドメインとして構成する．そして，利用者の認証情報は各部署ネットワークに設置する認証サーバが分散管理し，利用者認証時のユーザ識別子を “(ユーザ名)@(ドメイン名)” という形式で管理することにより，共通スペースの認証サーバがユーザ識別子のドメイン名に基づいて部署ネットワークの認証サーバに認証のための通信を中継することが可能となると共に，認証成功後に利用者が接続すべき部署ネットワークを自動的に決定することが可能となる．部署ネットワークの規模が大きい場合には，ドメイン名からVLAN識別子が一意に定まらないことも考えられるが，この場合には，部署ネットワークのVLAN識別子管理サーバが，ユーザ名とVLAN識別子の対応表を管理することによって解決できる．

なお，ユーザ識別子に含まれるドメイン名から部署ネットワークの認証サーバやVLAN識別子管理サーバを決定する方法については，DNSのSRVレコード [8] を利用して，サブドメインごとにこれらのサーバを登録することにより，サブドメイン名をキーとしてDNSサーバに問い合わせを行なうことにより，サブドメインに対応した認証サーバ

やVLAN識別子管理サーバを自動的に決定することが可能となる.

4.3 アクセス手順

図2において，ある利用者が共通スペースのVLANスイッチに接続し，自己の所属する部署ネットワークに接続可能となるまでのアクセス手順の概略は以下のようになる.

1. 利用者は共通スペースのDHCPサーバ(DHCP1)から認証用のIPアドレスの割り当てを受けた後，共通スペースの認証サーバ(AS1)に対してユーザ識別子を送信する．これを受けた共通スペースの認証サーバ(AS1)は，ユーザ識別子に含まれるドメイン名から部署ネットワークの認証サーバ(AS2)を決定し，認証のための通信をAS2に中継する．なお，この時点では，利用者がアクセスできるのはDHCP1およびAS1のみに制限されているものとする.

2. 認証に成功した場合，AS1は基幹ネットワークのVLAN識別子管理サーバ(VS1)に対して一時利用のためのVLAN設定要求メッセージを送信する．このメッセージには，利用者のユーザ識別子が含まれる.

3. VS1は，基幹ネットワークにおける一時利用のためのVLAN識別子を決定し，基幹ネットワーク内のVLANスイッチに対してVLAN設定を行なう．同時に，VS1は部署ネットワークのVLAN識別子管理サーバ(VS2)に対して一時利用のためのVLAN設定要求メッセージ(利用者のユーザ識別子を含む)を送信する.

4. VS2は，ユーザ識別子に基づいて部署ネットワークにおけるVLAN識別子の決定と(必要であれば)VLANスイッチの設定を行ない，設定が完了した段階で割り当てたVLAN識別子を含む応答メッセージをVS1に送信する.

5. 応答メッセージを受信したVS1は，自己の割り当てたVLAN識別子と，VS2が割り当てたVLAN識別子とをVLAN識別子変換サーバ(VC)に送信する.

6. VCは，自己が管理する変換テーブルにこれらのVLAN識別子を登録し，VCを通過するフレームのVLAN識別子の相互変換を開始すると共に，VS1に対して設定完了メッセージを送信する.

7. VS1は，AS1に対して基幹ネットワークで使用するVLAN識別子を含むVLAN設定完了メッセージを送信する．これを受けたAS1は，利用者の接続するVLANスイッチのポートにVLAN識別子を設定後，利用者に対してVLAN設定完了メッセージを送信する.

利用者がAS1からVLAN設定完了メッセージを受信した時点で，利用者の接続するVLANスイッチから部署ネットワークのVLANに対してデータリンク層レベルで接続可能となるので，利用者は部署ネットワークのDHCPサーバ(DHCP2)からIPアドレスの割り当てを受けることにより，部署ネットワークに直接接続する場合と同様に作業を行なうことが可能となる.

なお，これまでの議論では，共通スペースは基幹ネットワークに含まれるものとしたが，共通スペースの認証サーバが，基幹ネットワークのVLAN識別子管理サーバや各部署ネットワークの認証サーバに対してIPによる通信が可能であれば，共通スペースを部署ネットワーク内に置くこともできる.

4.4 検討事項

最後に，提案方式を実現するにあたり，今後検討すべき事項を以下に示す.

- IPアドレスの再取得

  提案方式では，利用者が共通スペースから所属する部署ネットワークに対してデータリンク層レベルで接続できることを目標としているため，4.3で述べたように，利用者はまず認証用のIPアドレスを取得し，部署ネットワークに接続可能となった時点で部署ネットワークで使用するIPアドレスを再取得する必要がある.

  IPアドレスの自動取得にはDHCPの利用が一般的であるが，RFC2131[9]で定められたDHCPのプロトコル仕様にはDHCPサーバが能

動的にDHCPクライアントのIPアドレスを変更する機能がない．これに対し，RFC3203[10]ではこの機能を実現するためのプロトコル拡張が提案されているが，実装例がないので，認証用のリース期間を短く設定する方法や，DHCPクライアント(利用者の計算機)にIPアドレスの再取得機能を組み込む方法なども含めて検討する必要がある．

- 認証サーバ

  共通スペースのVLANスイッチに接続する利用者の認証については，3.2で述べた既存の認証システムの利用を検討している．既存の認証システムを提案方式に適用するには，少なくとも，VLAN識別子管理サーバとの連携機能を組み込む必要があり，認証システムによっては，利用者の認証情報を分散管理できるように拡張する必要が生じる場合もある．したがって，どの認証システムを利用するかは，拡張の容易さも含めて今後検討する必要がある．

- VLANスイッチの自動設定

  VLANスイッチに対して一時利用のためのVLANを自動的に追加・削除する方法としては，IEEE802.1Qで規定されているGVRP(GARP VLAN Registration Protocol)の他，文献[2]のVLAN管理システムの利用や，提案方式のVLAN識別子管理サーバにVLANスイッチの設定機能を組み込む方法などが考えられる．ただし，VLANスイッチを遠隔操作する場合には，VLANスイッチに対するアクセス時のセキュリティを確保することが重要であるので，この点を考慮して検討しなければならない．

5 おわりに

本論文では，VLANが部署ごとに独自管理されている組織ネットワークにおいて，会議室などの共通スペースから，利用者の所属する部署ネットワークの一時利用を実現するための，VLAN識別子の動的割り当てと相互変換に基づいたVLAN相互接続方式の提案を行なった．今後は，4.4で述べた検討事項を考慮して設計の詳細化を行ない，提案方式に基づいた試作システムの実装に取り組む予定である．

参考文献

[1] IEEE: "802.1Q-1998 IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridge Local Area Networks", IEEE (1998).

[2] 宮本貴朗, 田村武志, 鈴木亮司, 平岡大樹, 松尾英普, 泉正夫, 福永邦雄: "大規模ネットワークにおけるVLAN管理システム", 情報処理学会論文誌, Vol.41, No.12, pp.3234–3244 (2000).

[3] 久長穣, 北上悟史, 渡邊孝博, 棚田嘉博, 井上裕二: "複数VLANの動的切り替えネットワークの構築について", 情処研報, DSM-22-7, pp.39–44 (2001).

[4] 田島浩一, 西村浩二, 相原玲二: "VLAN選択機能を持つ情報コンセントシステム", 学術情報処理研究, No.6, pp.5–12 (2002).

[5] Srisuresh, P. and Holdrege, M.: "IP Network Address Translator (NAT) Terminology and Considerations", RFC2663 (1999).

[6] Srisuresh, P. and Egevang, K.: "Traditional IP Network Address Translator (Traditional NAT)", RFC3022 (2001).

[7] 石橋勇人, 山井成良, 安倍広多, 阪本晃, 松浦敏雄: "利用者ごとのアクセス制御を実現する情報コンセント不正利用防止システム", 情報処理学会論文誌, Vol.42, No.1, pp.79–88 (2001).

[8] Gulbrandsen, A., Vixie, P. and Esibov, L.: "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782 (2000).

[9] Droms, R.: "Dynamic Host Configuration Protocol", RFC2131 (1997).

[10] T'Joens, Y., Hublet, C. and De Schrijver, P.: "DHCP reconfigure extension", RFC3203 (2001).