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[†] 二串信弘[††]
河野圭太[†] 岡本卓爾[†††]

VLAN（Virtual LAN）は，論理ネットワークをその物理的形状に依存することなく構成することができる技術である．VLANによれば，VLAN対応スイッチ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ため，会議室などの共通スペースからユーザの所属部署への一時的なVLAN接続を実現可能である．しかし，一般的なVLAN構成手法では，VLANは管理者によって静的に管理されるので，一時的なVLANを構築しようとすると管理の手間が大きいという問題がある．さらに，VLANが部署ごとに独自管理されるような大規模組織においては，一時利用のためのVLAN-IDが不足したり，部署間で衝突したりするといった問題が発生する．そこで本論文では，会議室などの共通スペースに設定された一時利用のためのVLANを，ユーザの所属するVLANに相互接続するための方式を提案する．提案方式では，共通スペースにおいて一時利用のためのVLAN-IDを動的に割り当てるとともに，ユーザが所属部署で使用しているVLAN-IDと相互変換することにより，ユーザが共通スペースから所属部署のVLANにシームレスに接続する機能を実現する．提案方式の有効性は，この方式に基づいて実装したVLAN管理サーバ，VLAN-ID変換サーバおよび認証サーバを用いて性能評価実験を実施することにより確認している．

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

Kiyohiko Okayama,[†] Nariyoshi Yamai,[†] Nobuhiro Nikushi,[††]
Keita Kawano[†] and Takuji Okamoto[†††]

VLAN (Virtual LAN) is a technology which can configure logical networks independent of the physical network structure. With VLAN, users in common spaces (such as meeting rooms) can access to their department networks temporarily because changing of logical network structure is achieved only by configuration of VLAN switches. However, in the general configuration method, because VLANs are managed statically by administrators, various problems such as high administrative cost and conflict or insufficiency of VLAN-IDs may arise especially in large scale organizations where VLANs are managed by each department. To solve these problems, we propose a method which provides an interconnection between a temporary configured VLAN in a common space and a VLAN of a user's department. In the proposed method, a user in a common space can access to his/her department network seamlessly by converting a temporary VLAN-ID in the common space and a VLAN-ID used in his/her department each other automatically. The effectiveness of the proposed method is confirmed by the experiment on the actual network using VLAN managers, VLAN-ID converters and authentication servers based on the proposed method.

1. はじめに

VLAN（Virtual LAN）は，物理ネットワークの形状に依存することなく論理ネットワークを構成するための技術である．VLAN技術によれば，VLAN対応スイッチ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，本論文では，組織のネットワーク内部において，会議室などの共通スペースから，ユーザが所属する部署ネットワークへの一時アクセスをするという用法を考える．

一時的なアクセスを実現する方法として，インターネットを介して遠隔サイトにアクセスするための技術である仮想プライベートネットワーク（Virtual Private Network，以下VPNという）をそのまま適用す

† 岡山大学総合情報基盤センター
Information Technology Center, Okayama University
†† 岡山大学大学院自然科学研究科
Graduate School of Natural Science and Technology, Okayama University
††† 岡山理科大学工学部
Faculty of Engineering, Okayama University of Science

ることが考えられる．ただし，VPN では安全な仮想ネットワークを構成するためにトンネリング技術や暗号技術が用いられるので，通信パケットのカプセル化や通信データの暗号化により，スループットが犠牲になるという側面がある．このため，VLAN 対応スイッチ（以下，単にスイッチという）で構成されるような組織のネットワーク内では，所属部署ネットワークの VLAN を共通スペースに延長するなどして，VLAN の高速性を活かせる方が望ましいといえる．

しかし，一般的な VLAN 構成手法では，(1) VLAN は管理者によって静的に管理されるため，一時的な VLAN の管理（VLAN の設定や解除）にかかる手間が大きいという問題や，(2) IEEE802.1Q[1] によれば，VLAN 識別子（以下，VLAN-ID という）のアドレス空間は 12 ビットしかなく，スイッチによってはさらに制限される場合があるため，一時利用のための VLAN-ID の不足が懸念されるという問題がある．さらに，大規模な組織において VLAN が部署ごとに独自管理されるような場合には，(3) 部署をまたがるような一時的 VLAN を構築しようとすると，部署間で VLAN-ID が衝突するといった問題も生じる可能性がある．

このような問題を解決するため，本論文では，共通スペースで一時的に構築する VLAN と，ユーザの所属部署 VLAN を動的に相互接続するための方式を提案する．提案方式では，共通スペースのユーザに対して一時利用のための VLAN-ID を動的に割り当てて一時的な VLAN を構築するとともに，ユーザの所属部署との境界上で共通スペースの VLAN-ID と所属部署の VLAN-ID を相互変換することにより，共通スペースのユーザに対して所属部署へのデータリンク層レベルでの接続を実現する．上述した処理は自動的に行われるので，一時的な VLAN の構築や解除にともなう管理の手間は生じることがなく，一時利用のための VLAN-ID を動的に割り当てることにより，限られた VLAN-ID 空間を効率良く利用することができる．さらに，部署ネットワークの境界上で VLAN-ID を相互変換することにより，部署間での VLAN-ID の衝突や，これを回避するための管理者間の調整も不要である．

以下，2 章では，本論文が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整理する．3 章では本論文で提案する VLAN 相互接続方式について述べ，4 章では提案方式の実装と実用性を確かめるための性能評価実験について述べる．5 章で考察と今後の課題，6 章で本論文をまとめる．

2. 前提とするネットワーク環境と問題点の整理

1 章で述べたように，本論文では，部署ごとに VLAN が独自管理され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．

そこで本論文では，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 つ以上のスイッチで構成される．複数のスイッチをまたがる通信については，IEEE802.1Q で定められた VLAN タギング機能を用いて各 VLAN に固有の VLAN-ID を割り当てるものとし，VLAN-ID の割当てを含めた VLAN の運用管理は各ネットワークで独自に行うものとする．また，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，組織内のユーザが，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-ID は静的に管理されるので，上述した一時利用を実現するには以下の 2 つの方法が考えられる．

方法 1 ユーザ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

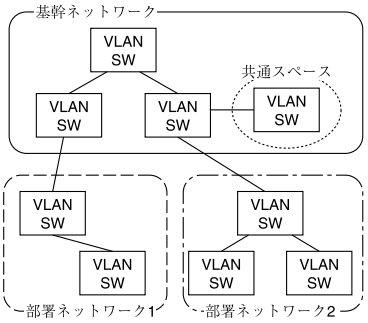

図 1 組織ネットワークの構成例
Fig. 1 An example of target network structure.

管理システムを用いることにより，一時利用の開始・終了にともなう 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 が各部署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-ID 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-ID を確保する必要があるため，部署ネットワーク間で VLAN-ID の衝突が発生しないように調整しようとすると，割当て可能な VLAN-ID に制約が生じる可能性がある．さらに，IEEE802.1Q では VLAN-ID 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，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．

また，地理的に離れた 2 拠点間を，VLAN の管理主体が異なる組織を介して VLAN 接続するために，IEEE802.1Q の VLAN タグ付きフレームを別のフレームでカプセル化する方式[7),☆☆]が提案されている．この方式は，ある VLAN を別の VLAN のトンネルとして利用する技術であり，プロバイダなどが顧客のネットワークの 2 拠点間を VLAN 接続するために用いることが多い．これを図 1 のネットワークに適用すると，基幹ネットワークの VLAN をトンネルとして利用することにより，共通スペースの VLAN と特定の部署ネットワークの VLAN とを相互接続することが可能である．しかし，この方式では，トンネル両端のネットワークで同一の VLAN-ID 空間を共有する必要があるため，VLAN の管理主体が異なる部署のユーザが集まる共通スペースには適用できない．

☆ “認証 VLAN” あるいは “Dynamic VLAN” と呼ばれる．
☆☆ “nested VLAN” あるいは “double-tagged VLAN” と呼ばれる．

3. VLAN の相互接続方式

3.1 VLAN-ID の動的割当てと相互変換

1 章で述べた問題点（1）および（2）を解決するためには，スイッチの VLAN 自動設定機能と，共通スペース内のユーザに対する一時的な VLAN-ID の動的割当て機能が必要である．前者については，多くのスイッチが TELNET や HTTP，SNMP などのリモート設定機能を備えているので，これらにより実現できると考えられる．後者については，基幹ネットワークにおいてあらかじめ一時利用のための VLAN-ID を確保しておき，共通スペースのユーザからの要求に応じて空き VLAN-ID の 1 つを割り当てればよい．

一方，基幹ネットワークでユーザに割り当てられた VLAN-ID は，ユーザの所属する部署ネットワークの VLAN-ID とは異なる可能性があるため，そのままでは接続することができない．そこで本論文では，基幹ネットワークとユーザの所属する部署ネットワークの境界上において，それぞれの VLAN-ID を相互変換する機能を導入する．これにより，ネットワーク間での VLAN-ID の衝突や，これを回避するための調整を行うことなく，共通スペースからユーザの所属部署のネットワークに対してデータリンク層レベルでの接続が可能となる．

3.2 ユーザ認証と接続先の決定

会議室などの共通スペースは部外者を含む様々なユーザが利用する可能性があるので，不正アクセスを防ぐにはユーザ認証が必須である．このとき，共通スペースのスイッチに接続するユーザの PC には，一時的な VLAN の確立後に DHCP などを利用して部署ネットワークの IP アドレスを割り当てることが多いため，IP アドレスの再割当てを必要としないデータリンク層レベルのユーザ認証方式を用いる必要がある．

一方，基幹ネットワークでは，ユーザの所属部署ネットワークの境界まで一時的な VLAN を構築する必要がある．このため，本論文では，基幹ネットワー

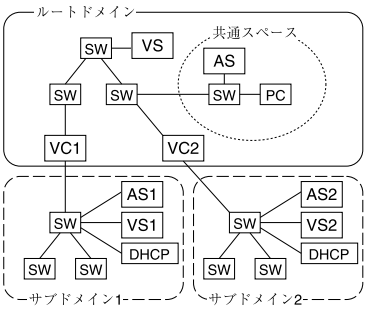

図 2 システム構成例
Fig. 2 An example of system structure.

クおよび各部署ネットワークにドメイン名を割り当て，ユーザ認証時のユーザ ID にドメイン名を付加するものとする．具体的には，メールアドレスのように“*username*@*domainname*”の形式で表す．ドメイン名の利用により，ユーザ認証時に接続先の部署ネットワークが自動決定できるだけでなく，ユーザの認証情報（ユーザ名とパスワードなど）を各部署ネットワークで管理できるようになる．

なお，本論文で導入するドメインは VLAN の管理範囲を表すものであり，基本的には DNS のドメインとは無関係である．以降では，組織の基幹ネットワークをルートドメイン，各部署ネットワークをサブドメインと呼ぶものとする．

3.3 システム構成

提案方式のシステム構成を**図 2** に示す．図中の SW はスイッチ，PC はユーザが使用する PC，DHCP はサブドメインで IP アドレスの割当てを行う DHCP サーバを示している．3.1 節および 3.2 節で述べた各機能は，既存のネットワークに以下の 3 つの要素を追加することによって実現する．

- VLAN 管理サーバ（図 2 の VS，VS1 および VS2）
- VLAN-ID 変換サーバ（VC1 および VC2）
- 認証サーバ（AS，AS1 および AS2）

以下，それぞれのサーバについて詳述する．

3.3.1 VLAN 管理サーバ

VLAN 管理サーバは各ドメインに設置され，一時利用のための VLAN-ID と，ドメイン内のスイッチを管理する．

まず，VLAN-ID の管理方法は，ルートドメインとサブドメインの VLAN 管理サーバで異なる．ルートドメインの VLAN 管理サーバは一時利用のための VLAN-ID を保持し，共通スペースのユーザからの要求に応じて空き VLAN-ID を割り当てる．このとき，VLAN-ID の空き状況や使用中のユーザ情報などを把握するため，VLAN-ID 管理のためのデータベース（以下，

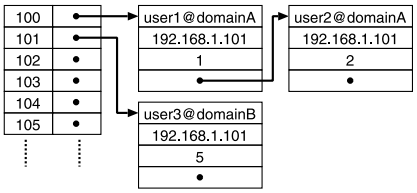

図 3 VLAN-ID データベースの例
Fig. 3 An example of VLAN-ID database.

VLAN-ID データベース）を設ける．VLAN-ID データベースは VLAN-ID をインデックスとする線形リスト構造を持ち，各ノードには以下の情報を格納する．

- VLAN-ID を使用中のユーザ ID
- ユーザが接続している共通スペースのスイッチの IP アドレス
- ユーザが接続している共通スペースのスイッチのポート番号
- 他ノードへのポインタ

図 3 に VLAN-ID データベースの例を示す．user1 および user2 のように，接続先が同一ドメインで，かつ，接続先ドメインで同一の VLAN を使用している場合は，同じ VLAN-ID を割り当てて一時利用の VLAN-ID 数を節減することができる．また，各ノードにスイッチの IP アドレスを格納することにより，同時に使用するユーザ数に応じて共通スペースのスイッチを増やすことも可能である．なお，これらの情報は，共通スペースにおけるユーザ認証成功時に認証サーバから得るものとする．

一方，サブドメインの VLAN 管理サーバは，サブドメインのユーザが通常使用する VLAN-ID を把握する必要がある．このため，ユーザ ID と VLAN-ID の組を VLAN-ID データベースで管理する．

次に，ドメイン内のスイッチを管理するには，スイッチの構成情報を把握する必要がある．ルートドメインの VLAN 管理サーバは，共通スペースから接続先ドメインの境界まで一時的な VLAN を構築し，サブドメインの VLAN 管理サーバは，ユーザが通常使用する VLAN をルートドメインとの境界まで延長する必要があるので，いずれの VLAN 管理サーバもスイッチの物理的な接続関係を把握しておかなければならない．そこで本論文では，各 VLAN 管理サーバにスイッチの接続関係を管理するためのデータベース（以下，スイッチ情報データベースという）を導入する．スイッチ情報データベースには，隣接する各ドメインの境界から共通スペースのスイッチ（サブドメインの場合はユーザが通常使用する VLAN の接続点となるスイッチ）に至るまでの各スイッチの IP アドレスと，隣接

するスイッチへの接続ポート番号を格納する．

3.3.2 VLAN-ID 変換サーバ

VLAN-ID 変換サーバは，ルートドメインと各サブドメインとの境界上に設置され，一方のドメインから送信されたフレームに含まれる VLAN-ID を変換してもう一方のドメインに中継する．ただし，ユーザによっては接続先のサブドメインが同一であっても，同一の VLAN を通常使用しているとは限らないので，複数の変換ルール（一時的な VLAN の構築時に VLAN 管理サーバから与えられる）をテーブルとして保持し，これに従って VLAN-ID の変換を行うものとする．

なお，各サブドメインでは異なる目的のために同一の VLAN-ID が使用される可能性があるため，VC はサブドメインごとに 1 つ配置する必要がある．

また，VLAN-ID 変換サーバを設置する両端のスイッチの空きポートを利用してスイッチ間を直結し，通常の，すなわち VLAN-ID の変換を必要としないトラフィックはこの回線を経由するように設定すれば，通常のトラフィックが VLAN-ID の変換による影響を受けることはないと考えられる．

3.3.3 認証サーバ

認証サーバは共通スペースと各サブドメインに設置され，共通スペースのスイッチに接続するユーザの認証を行う．共通スペースとサブドメインの認証サーバの役割は異なり，前者はユーザ ID に含まれるドメイン名に基づいて認証のための通信を中継し，後者は自ドメイン内のユーザの認証情報を保持する．

また，3.2 節で述べたように，提案方式ではデータリンク層レベルでユーザ認証を行うため，IEEE802.1X[8] を採用する．IEEE802.1X は，Windows2000/XP や Mac OS X が標準でクライアント機能（サプリカント）をサポートしており，フリーの認証サーバが公開されているなど，広く普及している認証方式である．

3.4 接 続 手 順

提案方式による一時的な VLAN の構築手順を，図 2 を例に説明する．提案方式を構成する各サーバは，少なくとも IP による通信が常時可能であるものとする．

(1) ユーザが共通スペースのスイッチに PC を接続すると，PC はスイッチを介して AS との間で IEEE802.1X による認証処理を開始する．認証メッセージにはユーザ ID が含まれており，ユーザ ID に含まれるドメイン名がサブドメイン 1 であったとすると，AS は認証のための通信を AS1 に中継する．

(2) AS が認証成功を検知すると，VS に対して一時的な VLAN の要求メッセージを送信する．このメッセージには，PC が接続されているスイッチの IP アドレスとポート番号，および，ユーザ ID が含まれる．なお，この時点では，認証成功メッセージを PC に送信しない．

(3) VS は VLAN-ID データベースを検索し，空き VLAN-ID の 1 つを割り当てる．そして，ユーザ ID に含まれるドメイン名に基づいてスイッチ情報データベースを検索し，接続先ドメインに至るまでの各スイッチを設定することにより，一時的な VLAN を共通スペースから VC1 まで構築する．スイッチの設定が完了すると，VS は VS1 に対してユーザ ID を送信する．

(4) VS1 はユーザ ID に基づいて VLAN-ID データベースを検索し，ユーザが通常使用する VLAN の VLAN-ID を得る．さらに，スイッチ情報データベースを参照し，ドメイン内のスイッチを設定して VLAN を VC1 まで延長する．スイッチの設定が完了すると，VS1 は延長した VLAN の VLAN-ID を VS に返す．

(5) VS は，自身がユーザに割り当てた VLAN-ID と，VS1 から受信した VLAN-ID の組を VC1 に送信する．

(6) VC1 は受信した VLAN-ID の組をテーブルに登録することにより，VLAN-ID の相互変換を開始する．さらに，VS に対して登録完了メッセージを送信する．

(7) VS は一時的な VLAN の構築完了メッセージを AS に送信する．これを受信した AS は，認証成功メッセージを PC に返す．

以上の手順が完了した段階で，PC はデータリンク層レベルでサブドメインに接続されているので，サブドメインの DHCP サーバから IP アドレスの割当てを受けることができる．

一方，一時的な VLAN の切断手順は以下のようになる．

(1) PC が共通スペースの SW から切断されると，SW がこれを検知して SW のポート番号とともに AS に通知する．

(2) AS はポート番号を切断要求メッセージとして VS に送信する．

(3) VS は受信したポート番号に基づいて VLAN-ID データベースを検索し，ポートを使用していたユーザ ID と，ルートドメイン内でそのユーザに割り当てた一時 VLAN-ID を得る．そして，以下の処理を行う．

- 切断したユーザの情報を VLAN-ID データ

ベースから削除
- スイッチ情報データベースに基づいてスイッチを設定し，共通スペースから VC1 に至るまでの一時的な VLAN を解除
- VS1 にユーザ ID を送信

なお，当該 VLAN-ID を使用する他のユーザが存在した場合，切断したユーザの情報を VLAN-ID データベースから削除するのみであり，他の処理はいっさい行わない．

(4) VS1 はユーザ ID に基づいて VLAN-ID データベースを検索し，ユーザが通常使用する VLAN の VLAN-ID を得る．さらに，スイッチ情報データベースを参照し，ドメイン内のスイッチを設定して VC1 まで延長された VLAN を解除する．スイッチの設定が完了すると，VS1 は解除した VLAN の VLAN-ID を返す．

(5) VS は，自身がユーザに割り当てた VLAN-ID と，VS1 から受信した VLAN-ID の組を VC1 に送信する．

(6) VC1 は受信した VLAN-ID の組をテーブルから削除することにより，VLAN-ID の相互変換を終了する．さらに，VS に対して削除完了メッセージを送信する．

なお，提案方式は，ドメイン階層数が 3 以上の場合や，共通スペースがサブドメインにある場合にも対応している．ドメインの階層数が 3 以上の場合，ユーザ ID に含まれるドメイン名は，一般的なドメイン名表記のように，ユーザが所属するサブドメインからルートドメインに至る各ドメイン名をドットで区切って表現する．一方，共通スペースが設置されたドメインの VLAN 管理サーバは，自ドメインのドメイン名とユーザ ID に含まれるドメイン名との比較により，上位ドメインと下位ドメインのどちらに一時的な VLAN を構築するかを自動的に判断する．そして，次に接続すべきドメインとの間に一時的な VLAN を構築し，そのドメインの VLAN 管理サーバに対して一時的な VLAN の構築要求を行う．また，次に接続するドメインが接続先ドメインでない，すなわち，中間のドメインであった場合も，ドメイン名の比較によってドメイン内に中継のための一時的な VLAN を構築する．

以上のように，提案方式ではドメイン名の比較によって自動的にドメインツリーをたどることが可能であるため，ドメインの階層数が 3 以上の場合や，共通スペースがサブドメインにある場合は，原理的には中継役となるドメインが増えるのみである．

4. 実装と性能評価

4.1 提案方式の実装

提案方式の有効性を検証するため，3.3 節で述べた各サーバを実装した．実装には FreeBSD 4.X を搭載した PC/AT 互換機を用い，C 言語を用いて各サーバを新規作成あるいは拡張した．以下，各サーバの実装について詳述する．

なお，3.4 節で述べたとおり，提案方式はドメイン階層数や共通スペースを設置するドメインに制約はないが，現在の実装では，ドメインの階層数が 2 であるとともに，共通スペースはルートドメインのみに設置されるものとしている．

4.1.1 VLAN 管理サーバ

VLAN 管理サーバは，ルートドメインとサブドメインで役割が異なるが，スイッチの自動設定など共通する動作も多いため，同一プログラムとして作成した（設定ファイルでの指定により動作を選択）．3.3.1 項で述べたデータベースのうち，ルートドメインの VLAN 管理サーバが保持する VLAN-ID データベースについては，設定ファイルで指定した空き VLAN-ID リストに基づいて，サーバ起動時に構築するようにした．一方，サブドメインの VLAN 管理サーバが保持する VLAN-ID データベースについては，ユーザ ID と VLAN-ID の組を設定ファイルで与えるようにした．

また，スイッチ情報データベースについては，各スイッチからスパニングツリー情報などを収集して自動的に構築することが望ましいが，今回の実装では，スイッチの接続情報を管理者が設定ファイルに記述するようにしている．

一方，スイッチの自動設定については，多くのスイッチが TELNET によるリモート管理機能を有することから，Expect [9] を用いて実現した．Expect は対話型アプリケーションを自動化するためのスクリプト言語であり，管理者が TELNET を用いて実行する VLAN 設定作業をあらかじめスクリプト化して，VLAN 管理サーバが自動実行できるようにした．

4.1.2 VLAN-ID 変換サーバ

3.3.2 項で述べたように，VLAN-ID 変換サーバは VLAN-ID の変換テーブルを持つ．VLAN 管理サーバのデータベースとは異なり，変換テーブルはフレームの到着ごとに参照されるため，処理の高速性が要求される．そこで本実装では，FreeBSD に付属のデータベースライブラリである gdbm [10] を利用して変換テーブルを構成するようにした．gdbm では，データベースファイルから読み出されたデータはメモリにキャッ

シュされるので，他のデータベースライブラリに比して高速に動作することが期待できる．なお，gdbm を使用する場合はデータベースの逆引きができないため，変換テーブルはルートドメイン側インタフェース用とサブドメイン側インタフェース用の 2 つを用意した．

また，VLAN-ID 変換サーバは，実装の容易さを考慮してユーザ空間で動作するプログラムとして実現している．一般的に，インタフェースが受信したフレームはドライバを経由してカーネルに渡され，カーネルによる経路制御が行われるため，そのままではユーザ空間のプログラムがフレームを直接的に操作することができない．そこで本実装では，FreeBSD の bpf（Berkeley Packet Filter）[11] を利用した．bpf により，インタフェースに対するフレームの読み出しおよび書き込みをユーザ空間のプログラムが直接（カーネルを介することなく）行うことが可能となる．

4.1.3 認証サーバ

本実装では，認証サーバとして IEEE802.1X の一実装である FreeRADIUS [12] を利用した．FreeRADIUS は IEEE802.1X をサポートするだけでなく，3.3.3 項で述べたドメイン名に基づくプロクシ機能を標準でサポートする．ただし，VLAN 管理サーバとの通信機能は含まれていないため，FreeRADIUS のサーバプログラムを拡張した．具体的には，共通スペースの認証サーバとして動作している場合には，認証成功時にユーザ ID，スイッチの IP アドレスおよびポート番号を VLAN 管理サーバに送信し，VLAN 管理サーバからの応答を待ってから認証成功メッセージをユーザの PC に返すようにした．

また，一時的な VLAN の切断を行うため，本実装では，SNMP を用いて共通スペースのスイッチを監視して，リンクダウンを検出する方法をとっている．共通スペースの認証サーバには，これを行うためのプログラムを別途作成し，SNMP のポーリングとトラップを併用したリンクダウンの検出と，リンクダウンが発生したポート番号を VLAN 管理サーバに通知する機能を組み込んでいる．

4.2 性能評価実験

ユーザから見た場合，一時的な VLAN の構築に要する時間と，VLAN-ID 変換サーバのスループットが重要であると考えられる．そこで，4.1 節で述べた各サーバを用いて実験環境を構築し，2 つの指標に関する性能評価実験を行った．

4.2.1 一時的な VLAN の構築時間

一時的な VLAN の構築時間を計測するため，**図 4** に示す実験環境を構築した．VLAN 管理サーバ，VLAN-ID 変換サーバ，および，認証サーバには FreeBSD 4.8-RELEASE を搭載した PC/AT 互換機（Pentium4-3.4 GHz，メモリ 1 GB）を使用し，スイッチには Cisco Systems 社の Catalyst3550，ユーザの PC には WindowsXP を搭載したノート PC を使用した．すべての機器は 100 Mbps の Ethernet で接続している．なお，本実験ではサブドメインに DHCP サーバを置かず，PC には手動で IP アドレスを割り当てている．

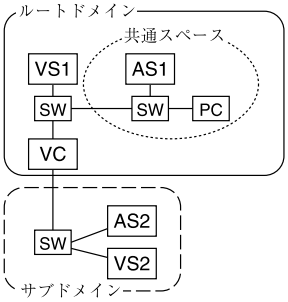

図 4 実験環境 1
Fig. 4 The experiment network #1.

表 1 実験結果 1
Table 1 The result of the experiment #1.

	Time（秒）
認証時間	0.01
スイッチ設定時間	1.31

ユーザが PC を共通スペースのスイッチに接続すると，3.4 節で述べた手順により一時的な VLAN の構築が開始される．本実験では，一時的な VLAN の構築を 10 回試行し，AS1 がスイッチから認証要求メッセージを受信してから，VS1 から一時的 VLAN の構築完了メッセージを受信するまでの平均時間を算出した．

実験結果を**表 1** に示す．表 1 のうち，認証時間は，AS1 がスイッチから認証要求メッセージを受信してから VS1 に一時的な VLAN の要求メッセージを送信するまでの時間であり，スイッチ設定時間は，VS1 が AS1 から一時的な VLAN の要求メッセージを受け取ってから構築完了メッセージを返すまでの時間である．後者には VC の VLAN-ID 変換テーブルに変換ルールを登録する時間なども含まれるが，無視できる値であり，ほとんどがスイッチのリモート設定に要する時間で占められていた．

認証時間およびスイッチ設定時間の合計は約 1.32 秒であり，実用上問題ないといえる．今回の実装では，VLAN 管理サーバはドメイン内の各スイッチを並列的にリモート設定しているので，並列処理のためのオーバヘッドを無視すれば，設定すべきスイッチ数にかかわらずスイッチ設定時間はほぼ一定である．一方，

図 5 実験環境 2
Fig. 5 The experiment network #2.

ドメイン間については，VS1 がルートドメイン内のスイッチ設定を完了してから VS2 に要求メッセージ（ユーザ ID）を送信しているため，この順序を入れ替えることにより，スイッチ設定時間は表 1 の約半分になると考えられる．

4.2.2 VLAN-ID 変換サーバのスループット

3.3.2 項で述べた VLAN-ID 変換サーバを用いて，VLAN-ID の相互変換によるスループットへの影響を測定した．VLAN と同じく仮想ネットワークを構築する技術である VPN を用いた場合と比較するために，OpenVPN [13] を用いた場合についても実験を行った．

実験環境を**図 5** に示す．本実験では，一時的な VLAN 構築後のスループットを計測すればよいので，VLAN 管理サーバおよび認証サーバは省略し，VLAN-ID 変換ルールを手動で VLAN-ID 変換サーバのテーブルに登録した．サーバ，クライアント，および VLAN-ID 変換サーバには，いずれも FreeBSD バージョン 4.9-RELEASE 搭載の PC/AT 互換機（Pentium4-3 GHz，メモリ 1 GB）を使用し，スイッチとして Cisco Systems 社の Catalyst2950 を用いた．すべての機器は，100 Mbps の Ethernet で接続した．

この環境において，VLAN-ID 変換サーバを用いた場合（VC）と OpenVPN を用いた場合，および，いずれも用いない場合（直接接続）のそれぞれについて，クライアントからサーバへ TCP コネクションを確立して 500 MB のデータを送信する実験を 100 回行い，平均スループットを算出した．OpenVPN については，暗号化通信およびパケット認証の有無を指定できるため，さらに以下の 3 つの場合について実験を行った．

- 暗号化通信とパケット認証の両方を行う場合（OpenVPN1）
- パケット認証のみを行う場合（OpenVPN2）
- 暗号化通信とパケット認証のいずれも行わない場合（OpenVPN3）

なお，データの送信には，nttcp [14] を利用した．nttcp は指定した大きさのデータをクライアントからサーバに対して（逆方向も可能）送信するソフトウェアであり，ディスクへのアクセスをまったく行わないため，ftp などのファイル転送ソフトウェアよりも精確なスループットを測定することができる．また，OpenVPN および直接接続の場合には，図 5 の実験環境から VLAN-ID 変換サーバを取り除き，2 台のスイッチを直接接続している．

表 2 実験結果 2
Table 2 The result of the experiment #2.

	Throughput (Mbps)
OpenVPN1	65.46
OpenVPN2	83.53
OpenVPN3	85.37
VC	88.39
直接接続	89.74

実験結果を**表 2** に示す．直接接続に比して，VLAN-ID 変換サーバを使用した場合のスループットの低下は約 1.4 Mbps であり，VLAN-ID の変換による影響は比較的小さいといえる．これに対し，OpenVPN により暗号化通信とパケット認証の両方を行う場合（OpenVPN1）は直接接続に比して約 24 Mbps の低下が見られ，パケット認証のみを用いた場合（OpenVPN2）でも約 6.2 Mbps 低下しているので，スループットの面では VLAN-ID の変換が有効であるといえる．

一方，OpenVPN で暗号化通信もパケット認証も行わない場合（OpenVPN3）は，直接接続に比して約 4.4 Mbps の低下にとどまっている．このため，組織内では OpenVPN を用いて暗号化通信やパケット認証を行わずに運用する方法も考えられるが，途中のスイッチに対して MAC address flooding 攻撃を許した場合，同じ VLAN-ID が割り当てられたすべてのポートから通信内容が漏洩する危険性がある．したがって，不必要なポートからの通信内容漏洩を防ぐには，組織内であっても暗号化通信およびパケット認証は必須である．これに対し，提案方式では，一時利用のための VLAN-ID は接続に必要なポートのみに割り当てられるので，少なくともルートドメイン内では MAC address flooding 攻撃によって通信内容が漏洩する可能性は低くなると考えられる．

以上のことから，本論文が前提とするようなネットワーク環境では，提案方式によって安全かつ高速な通信が実現できると考えられる．なお，提案方式は，組織のネットワーク内部での利用を前提としている．一般に，組織内部ではネットワーク機器に対する物理的な安全性が確保しやすいことから，インターネットを介した通信に比してスイッチの TAP などによる盗聴の危険性が低いと考えられる．これをふまえたうえで，提案方式はユーザに対する高速なアクセスの提供を指向しているが，高速性よりも安全性を要求するアプリケーションに対しては，必ずしもデータリンク層レベルのアクセスを提供する必要はなく，VPN などの既

存技術を選択的に適用すればよい．

5. 考察と今後の課題

最後に，提案方式に対する性能評価実験以外の考察と，今後の課題を以下にまとめる．

- 提案方式の適用範囲
  2 章で述べたように，提案方式は組織のネットワーク内部が VLAN 対応スイッチで構成されており，かつ，部署など一部のネットワークでの VLAN 管理が基幹ネットワークと独立して行われているような組織が前提となっている．ただし，組織ネットワークの末端部分まで VLAN 対応スイッチで構成される必要はなく，基幹ネットワーク内の部署サブネットを収容する L2 あるいは L3 スイッチ部分までが VLAN に対応していれば，基幹ネットワーク内で動的に一時的な VLAN を構築することにより，共通スペースから部署サブネットに対してデータリンク層レベルの接続を提供することが可能である．
  一方，特に大学などの組織においては，計算機センタなどの部署が組織のネットワーク全体の VLAN を管理する場合であっても，部署（学科や研究室など）の単位で独自にファイアウォールなどを設置して，ファイアウォール内部では外部とは異なる IP アドレス空間（プライベートアドレスなど）を割り当てて独自に運用するケースがよく見られる．この場合，ファイアウォール外部から内部にアクセスする場合には，一般的にはいわゆる NAT 越え（ポート転送など）や VPN といった IP 層以上の技術を用いる必要があるが，ファイアウォール内部のサブネットを収容するネットワーク機器が VLAN に対応していれば，提案方式の適用によりファイアウォール外部から内部に対してデータリンク層レベルの高速なアクセスが可能である．
- 高速かつ大規模なネットワーク環境での性能評価
  4.2 節で述べた性能評価は，クライアント PC が 1 台という状況での実験結果であり，会議や授業のように，多数のユーザが共通スペースで同時接続する場合の各サーバへの負荷や一時的な VLAN 構築時間への影響が考慮されていない．しかし，実験に使用したスイッチでは，管理のための TELNET による同時セッション数が 4 に制限されていることから，スケーラビリティに問題があることが判明している．このため，今後は同一スイッチに対するより並列度の高いリモート設定方法，たとえば，1 つの TELNET セッションで複数の設定作業を実行する方法や，SNMP によるリモート設定方法などを検討する必要がある．さらにそのうえで，大規模なネットワーク環境における性能評価実験を行い，VLAN 管理サーバにおける VLAN-ID データベース操作の負荷や，VLAN-ID 変換サーバにおける変換ルール数とスループットの関係などを定量的に評価する予定である．
  また，最近では基幹ネットワーク部分にギガビットクラスのネットワーク回線を導入する組織が多くなっているため，提案方式の性能評価にも GbE などの高速回線を利用することが望ましい．しかし，今回の実装では VLAN-ID 変換サーバを PC で実現しており，PC での GbE のスループットはたかだか数百 Mbps であることから，スイッチを直結して VPN を利用する場合との比較が困難である．このため，4.2.2 項のスループット測定では，PC でもワイヤレートに近いスループットが得られる 100 Mbps の Ethernet を使用したが，今後はより高速なネットワーク環境での性能評価を念頭に置いて，VLAN-ID 変換サーバの専用機器化を検討したい．
- ユーザによる接続先 VLAN の指定
  現在の実装では，ユーザが所属するサブドメイン内で通常使用する VLAN は VLAN 管理サーバの VLAN-ID データベースで静的に管理されており，ユーザに対して登録可能な VLAN-ID は 1 つである．
  これに対し，あるユーザがサブドメイン内で複数のネットワーク（VLAN）を利用するような場合も考えられるため，ユーザに対して複数の VLAN-ID を登録できるようにしたうえで，共通スペース接続時にユーザがこれらの VLAN-ID を選択できるような仕組みを検討する予定である．
- サーバの配置
  提案方式を構成する各サーバ間および VLAN 管理サーバとドメイン内各スイッチ間では，IP による通信が常時行えればよいため，サブドメイン内の VLAN 管理サーバと認証サーバの機能をルートドメインの各サーバに一本化すれば，サブドメイン管理者にかかるサーバ運用の手間を軽減できると考えられる．また，VLAN-ID 変換サーバについては，ルートドメインと各サブドメインの境界に 1 台ずつ設置する必要があるが，VLAN-ID 変換サーバは VLAN 管理サーバの指示のみによって動作するため，一度設置すれば特別な管理運用の手間は必要ない．

ただし，サーバ機能の集約によってサブドメイン内で管理すべき情報（ユーザのアカウント情報やサブドメイン内のスイッチ構成など）もルートドメインに集約されるため，サーバの配置は各ドメイン管理者にかかる負担のバランスを考慮して決定すべきである．

- VLAN-ID 変換機能付きスイッチの導入
  現在の実装では，VLAN-ID の変換をドメインの境界に設置された VLAN-ID 変換サーバでのソフトウェア処理により実現している．このため，同サーバに登録可能な VLAN-ID の変換ルール数に上限はない（IEEE802.1Q の仕様により，VLAN-ID 空間は 12 ビットに制限されるため）が，変換ルールの増加にともなってスループットが低下する恐れがある．一方，既存のスイッチには，任意のポートに対して VLAN-ID の変換ルールを設定できるような機種があるため，このようなスイッチをドメインの境界に設置すれば，VLAN-ID の変換をより高速に行うことができると考えられる．ただし，上述したスイッチのほとんどは，あるポートに設定可能な VLAN-ID の変換ルールは 1 つだけであるため，共通スペースから特定のサブドメイン内の異なる VLAN に対して多数のユーザが接続する場合には，その同時接続数に応じて複数のスイッチを用意する必要がある（たとえば，24 個のポートを備えたスイッチであれば，トランクポートを除くと最大 23 個の変換ルールしか設定できないことになる）．このため，VLAN-ID 変換サーバを既存のスイッチで置き換える場合には，あるサブドメインの異なる VLAN への同時接続数とコストのバランスを考慮しなければならない．
- 無線 LAN への対応
  現在の提案方式は，共通スペースでのユーザの接続方法は有線のみであり，無線 LAN の利用は考慮していない．しかし，大学などの組織では共通スペースに無線 LAN が整備されるなど，無線 LAN への対応は重要であると考えられる．
  現在では，SSID に応じて接続先の VLAN を変更可能なアクセスポイント製品もあるが，設定可能な SSID の数はあまり多くないため，接続先の VLAN 数が非常に限定される恐れがある．そこで，今後は 2 章で述べた認証 VLAN をベースに，認証結果により空き VLAN-ID をユーザごとに動的に割り当てることが可能な仕組みを検討する予定である．

6. おわりに

本論文では，VLAN が部署ごとに独自管理されるような組織のネットワークを対象とした，VLAN-ID の動的割当てと相互変換に基づく VLAN の相互接続方式を提案した．さらに，提案方式を実装して性能評価実験を行うことにより，実用的な時間で一時的な VLAN が自動構築できることと，現在の実装では VLAN-ID の相互変換をソフトウェアで行っているにもかかわらず，既存の VPN ソフトウェアに比してより高いスループットが得られることを確認した．

今後は，5 章で述べた課題について検討するとともに，VLAN 管理サーバがドメイン内のスイッチ構成情報を自動収集する方法や，ドメインの階層数が 3 以上で，かつ，共通スペースがサブドメインにある場合の実装について検討する予定である．

謝辞 本研究の一部は，総務省・戦略的情報通信研究開発推進制度（特定領域重点型研究開発プログラム，課題番号 041108001）の補助を受けている．ここに記して感謝の意を表する．

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，情報処理学会研究報告，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) Cisco Systems: IEEE 802.1Q-in-Q VLAN Tag Termination. http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a-00801f0f4a.html
8) IEEE: 802.1X-2001 IEEE Standards for Local and Metropolitan Area Networks: Port-Based Network Access Control, IEEE (2001).
9) Libes, D.: Expect - Expect - Home Page.

http://expect.nist.gov/
10) GNU Project: GNU Database Manager. http://www.gnu.org/software/gdbm/gdbm.html
11) McCanne, S. and Jacobson, V.: The BSD packet filter: A New Architecture for User-level Packet Capture, *Proc. 1993 Winter USENIX Conference*, pp.259–269 (1993).
12) The FreeRADIUS Project: FreeRADIUS — building the perfect RADIUS server. http://www.freeradius.org/
13) Yonan, J.: OpenVPN. http://openvpn.sourceforge.net/index.html
14) Bartel, E.: nttcp: New TTCP Program. http://www.leo.org/~elmar/nttcp

(平成 18 年 7 月 7 日受付)
(平成 19 年 1 月 9 日採録)

岡山　聖彦（正会員）

平成 2 年大阪大学基礎工学部情報工学科卒業．平成 4 年同大学大学院基礎工学研究科博士前期課程修了．同年同大学院基礎工学研究科博士後期課程を退学し，同大学工学部助手．平成 6 年奈良先端科学技術大学院大学情報科学研究科助手．平成 10 年岡山大学工学部助手．平成 17 年同大学総合情報基盤センター助手．博士（工学）．インターネットアーキテクチャ，ネットワーク管理，ネットワークセキュリティの研究に従事．電子情報通信学会会員．

山井　成良（正会員）

昭和 59 年大阪大学工学部電子工学科卒業．昭和 61 年同大学大学院博士前期課程修了．昭和 63 年同大学院基礎工学研究科（物理系専攻情報工学分野）博士後期課程退学．同年奈良工業高等専門学校情報工学科助手．同講師，大阪大学情報処理教育センター助手，同大学大型計算機センター講師，岡山大学総合情報処理センター（現，総合情報基盤センター）助教授を経て，現在同教授．分散システム，マルチメディアシステム，マルチメディアネットワークの研究に従事．IEEE，電子情報通信学会各会員．博士（工学）．

二串　信弘（学生会員）

平成 17 年岡山大学工学部通信ネットワーク工学科卒業．平成 19 年同大学大学院自然科学研究科博士前期課程修了．現在（株）インターネットイニシアティブ勤務．ネットワーク運用管理技術等に興味を持つ．

河野　圭太（正会員）

平成 12 年大阪大学工学部電子情報エネルギー工学科卒業．平成 14 年同大学大学院工学研究科（情報システム工学専攻）修士課程修了．平成 16 年同大学院情報科学研究科（情報ネットワーク学専攻）博士課程修了．同年岡山大学総合情報基盤センター助手．モバイルネットワーク，分散システムの研究に従事．IEEE，電子情報通信学会各会員．博士（情報科学）．

岡本　卓爾（正会員）

昭和 33 年大阪大学工学部通信工学科卒業．川崎重工業（株），三井造船（株）を経て，昭和 42 年岡山大学工学部奉職．昭和 62 年同大学教授．平成 13 年岡山理科大学工学部教授．主として，論理回路を中心とした計算機ハードウェアの研究に従事．工学博士．電子情報通信学会，映像情報メディア学会，日本エム・イー学会各会員．