VLAN相互接続方式に基づいたVLAN-ID変換サーバの実装と評価

濱本 敦† 岡山 聖彦†† 山井 成良‡ 岡本 卓爾‡‡

概 要

VLANが部署ごとに独自管理されるような大規模組織では，組織の構成員が他部署のネットワークを一時的に利用して所属部署のネットワークにデータリンク層レベルで接続しようとすると，VLANの管理の手間に加えて，VLAN-IDの競合や不足などの問題が発生する．これらの問題を解決するため，一時利用のためのVLAN-IDを動的に確保した上で，部署ネットワークごとに異なるVLAN-IDを相互変換する方式が提案されており，本論文では，この方式の主要な構成要素であるVLAN-ID変換サーバの実装を行った．本実装では，ソフトウェアによりVLAN-IDの変換機能を実現しているが，実際のネットワーク環境での性能評価実験により，VPNを利用した接続よりも高速な通信が行えることを確認している．

Implementation and Evaluation of VLAN-ID Converter Based on the Method of Interconnection of VLANs

Atsushi Hamamoto† Kiyohiko Okayama†† Nariyoshi Yamai‡ Takuji Okamoto‡‡

Abstract

In a large-scale organization where VLANs are managed independently by each department, when users attempt to connect temporarily to their departments' network from another location, various problems such as high administrative cost and conflict or insufficiency of VLAN-IDs may occur. To solve these problems, a method of interconnection of VLANs which is able to allocate VLAN-IDs to temporary users dynamically and convert allocated VLAN-IDs of each department network each other has been proposed. In this paper, we implement a VLAN-ID converter which is the major component of this method. Although our VLAN-ID converter is made as a software program, we confirmed that our VLAN-ID converter provides faster communication than VPN software by the experiment on the actual network environment.

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

1 はじめに

近年，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．

この問題を解決するため，文献[1]では，VLAN-IDの動的変換に基づいたVLANの相互接続方式(以下，VLAN相互接続方式という)の提案と，これに基づいたシステムの設計を行っている．VLAN相互接続方式では，部署ごとに一時利用のためのVLAN-IDをあらかじめ一定数確保し，ユーザが共通スペースの情報コンセントへの接続時にVLAN-IDを動的に割り当てる．さらに，部署の境界において，部署ごとに独自に割り当てられたVLAN-IDを相互変換することにより，共通スペースからユーザ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している．

本研究では，VLAN相互接続方式の主要な構成要素であり，部署の境界でVLAN-IDの相互変換を行うVLAN-ID変換サーバの実装を行った．実装には，2つのEthernetインタフェース(以下、インタフェース)を備えたPCを用い，VLAN-IDの変換機能をソフトウェアで実現している．VLAN-ID変換サーバプログラムは，変換前および変換後のVLAN-IDの組を登録するためのテーブルを持ち，インタフェースに対するフレームの入出力を直接的に(すなわち，OSのカーネルを介することなく)行うことにより，一方のインタフェースが受信したフレームに含まれるVLAN-IDを書き換えてもう一方のインタフェースから送信する．遠隔地からユーザの所属するネットワークを安全に利用する手法としては，VPN(Virtual Private Network)技術が広く普及しているが，実験ネットワークを構築し，VLAN-ID変換サーバとVPNソフトウェアの一つであるOpenVPN[2]を用いて性能評価実験を行うことにより，OpenVPNよりも高速に通信できることを確認した．

以下，VLAN相互接続方式の概要について述べた後，VLAN-ID変換サーバの実装と，性能評価実験について述べる．

2 VLAN相互接続方式の概要

2.1 前提とするネットワーク環境

VLAN相互接続方式は，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，大規模な組織では，組織の階層構造に合わせてDNSのドメインを構成していることが多いことに注目し，図1のように，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に各部署のネットワークが接続しているような形態を前提とし，前者をルートドメイン，後者をサブドメインとしている．部署の規模によっては，サブドメイン内部をさらに階層的に構成することもあるが，議論の簡単化のため，ドメインの階層数は2とする．図1において，ルートドメインおよびサブドメインはそれぞれ1つ以上のVLANスイッチ(SW)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[3]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の運用管理は各ドメインで独自に行なうものとする．また，説明の簡単化のため，会議室などの共通スペースはルートドメインに含まれるものとする．

2.2 VLAN-ID動的割当てと相互変換

図1ような構成のネットワークにおいて，組織内のユーザが，共通スペースから所属部署のネットワークを一時利用することを考える．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者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

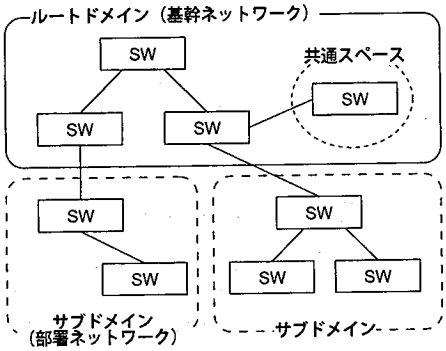

図 1: 前提とするネットワーク構成

立して管理されていると，ドメイン間でVLAN-IDの衝突が生じたり，VLANスイッチによっては設定可能なVLAN-IDの数を超過する可能性がある．

これらの問題を解決するため，VLAN相互接続方式では，VLAN-IDの動的な変換機構を導入している．具体的には，ルートドメインとサブドメインの境界にVLAN-ID変換サーバを設け，各ドメインに設置するVLAN-ID管理サーバからの指示により，各ドメインで独自に割り当てられたVLAN-IDの相互変換を行う．これにより，共通スペースのユーザが所属部署のネットワークにデータリンク層レベルで接続することが可能となる．

2.3 VLAN-ID変換システムの構成

2.2節で述べたVLAN相互接続方式を実現するためのVLAN-ID変換システムの構成例を図2に示す．ユーザ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．

VLAN-ID変換システムは，VLAN-IDの動的割当てを行なうVLAN-ID管理サーバ，VLAN-IDの相互変換を行なうVLAN-ID変換サーバ，および，共通スペースに接続するユーザを認証するための認証サーバを中心に構成される．以下に，VLANスイッチ以外の構成要素の役割を列挙する．

- VLAN-ID管理サーバ (VS1およびVS2)

  各ドメインに一つ設置し，認証サーバからの要求に応じて一時利用のためのVLAN-IDを管理する．

- VLAN-ID変換サーバ (VC)

  ルートドメインとサブドメインの境界に設置し，ルートドメインのVLAN-ID管理サーバからの指示により，フレームに含まれるVLAN-IDの相互変換を行う．

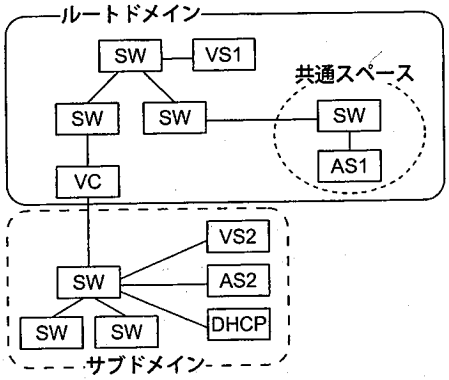

図 2: VLAN-ID変換システムの構成例

- 認証サーバ

  共通スペースと各ドメインにそれぞれ一つ配置する．サブドメインの認証サーバ (AS2)はドメイン内のユーザ情報を管理し，共通スペースの認証サーバ (AS1)を介してユーザの認証を行う．

- DHCPサーバ

  ユーザの所属するネットワークに設置し，ユーザ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，ユーザの計算機にIPアドレスを割り当てる．

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

2.4 アクセス手順

図2において，あるユーザが共通スペースのVLANスイッチに接続し，所属部署のネットワークに接続可能となるまでのアクセス手順は以下のようになる．

1. ユーザは共通スペースのスイッチのポートに接続し，AS1に対してユーザIDを送信する．ここで，ユーザIDは“ユーザ名@ドメイン名”という形式で管理することで，ユーザIDから所属ドメインが判別できるようにしている．AS1

は，ユーザIDに含まれるドメイン名からサブドメインの認証サーバを(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，ユーザがアクセスできるのはAS1のみに制限されているものとする．

2. 認証に成功すると，AS1はVS1に対して一時利用のためのVLAN設定要求を行う．なお，要求メッセージはユーザIDを含む．

3. VS1は，ルートドメインにおける一時利用のためのVLAN-IDを決定し，ルートドメイン内のVLANスイッチに対してVLAN設定を行なう．同時に，VS1はVS2に対して一時利用のためのVLAN設定要求(ユーザIDを含む)を行う．

4. VS2は，ユーザIDに基づいてサブドメインにおけるVLAN-ID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VS1に応答する．なお，応答メッセージはVS2が割り当てたVLAN-IDを含む．

5. VS1は，自己の割り当てたVLAN-IDと，VS2が割り当てたVLAN-IDの組をVCに送信する．

6. VCは，自己が管理するVLAN-ID変換テーブルにVLAN-IDの組を登録し，VCを通過するフレームのVLAN-ID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に対してルートドメインで使用するVLAN-IDを含むVLAN設定完了メッセージを送信する．

以上の手順が完了した段階で，ユーザの計算機は所属部署のネットワークにデータリンク層レベルで接続されているので，DHCPサーバからIPアドレスの割り当てを受けることにより，所属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うことが可能となる．

3 VLAN-ID変換サーバの実装

VLAN-ID変換サーバはVLAN相互接続方式の重要な構成要素であり，VLAN-ID管理サーバからの指示により，ドメインを跨って送受信されるフレームに含まれるVLAN-IDの相互変換を行う．本実装では，OSとしてFreeBSDバージョン4.9-RELEASEを搭載したPCを用いて，ユーザ空間で動作する変換プログラムを作成した．以下，VLAN-ID変換サーバに必要な機能とその実現方法，および，動作例について述べる．

3.1 必要な機能と実現方法

VLAN-ID変換サーバは2つのインタフェースを持ち，ルートドメインとサブドメインを接続するスイッチ間に挟み込むように接続する．そして，一方のインタフェースで受信したフレームに含まれるVLAN-IDを書き換えた上で，もう一方のインタフェースに書き出すという動作を行う．したがって，このような動作を実現するには以下の2つの機能が必要である．

- VLAN-ID変換テーブル

  VLAN-IDの相互変換は，一方のインタフェースから送られてくるフレームに含まれるVLAN-IDを，もう一方のネットワークで割り当てられたVLAN-IDに書き換えることによって行われる．さらに，複数のユーザによる一時利用に対応するため，変換前および変換後のVLAN-IDの組を複数保持する必要がある．

  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[4]を用いてVLAN-IDの組を管理する．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つを用意する．また，現時点ではVLAN-ID管理サーバが未実装であるため，VLAN-ID変換テーブルへのエントリの追加・変更・削除は専用のプログラムを作成して手動で行っている．

- フレームの入出力

  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．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

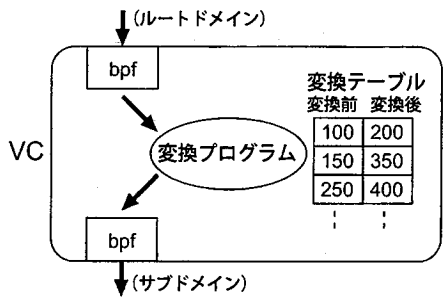

図 3: VLAN-ID変換サーバの動作例

るので，そのままでは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)[5]を利用する．bpfにより，インターフェイスに対するフレームの読出しおよび書込みをユーザプログラムが直接(カーネルを介することなく)行うことが可能となる．

3.2 動作例

VLAN-ID変換サーバの動作例を図3に示す．図3はフレームがルートドメインからサブドメインへ送信される場合を表しており，この場合の変換手順は以下のようになる．

1. 変換プログラムはbpfを用いてルートドメイン側インタフェースが受信したフレームを読み出す．

2. フレームに含まれるVLAN-IDをキーとしてルートドメイン側インタフェース用の変換テーブルを検索し，その結果に基づいてフレーム中のVLAN-IDを書き換える．

3. VLAN-IDを書き換えたフレームをbpfを用いてサブドメイン側インタフェースに書き出す．

逆方向，すなわち，サブドメインからルートドメインへ送信されるフレームのVLAN-IDを変換する場合には，サブドメイン側インタフェース用の変換テーブルを用いる．

なお，サブドメインの接続先VLANが同一の端末が共通スペースに複数ある場合には，ルートドメインでもこれらの端末に同じVLANを割り当てることが望ましい．そうでない場合には，これらの端末に対してサブドメインから送信されるフレームは，端末の数だけVLAN-ID変換サーバで複製されることになる．

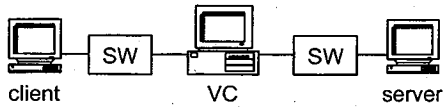

図 4: 実験環境

4 実験と考察

3章で述べたVLAN-ID変換サーバを用いて，VLAN-IDの相互変換による通信速度への影響を測定した．このとき，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を用いた場合についても実験を行った．

4.1 実験方法

実験環境を図4に示す．サーバ，クライアント，およびVLAN-ID変換サーバ(VC)には，いずれもFreeBSDバージョン4.9-RELEASEを搭載したPC/AT互換機(Pentium4-3GHz，メモリ1GB)を使用し，VLANスイッチとしてCisco Systems社のCatalyst2950を用いた．すべての機器は，100Base-TXのEthernetで接続している．

この実験環境において，VLAN-ID変換サーバを使用した場合(VC)と，OpenVPNを使用した場合，および，いずれも使用しない場合(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、500MBのデータを送信する実験を100回行い，平均転送速度を算出した．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[6]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全く行わないため，ftpなどのファイル転送ソフトウェアよりも精確な転送速度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4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．

4.2 実験結果と考察

実験結果を表1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(VC)の転送速度の低下は約1.4Mbpsであり，VLAN-IDの変換による通信速度への影響は比較的小さいといえる．これに対し，OpenVPNを使用した場合，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24Mbpsの速度低下が見られ，パケット認証のみを用いた場合(OpenVPN2)でも約6.2Mbps低下していることから，通信速度の面ではVLAN-IDの変換が有効であると考えられる．

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4.4Mbps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VLAN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，通信の安全性を重視する場合には，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，VLAN相互接続方式では，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いと考えられる．

以上のことから，2.1節で述べたようなネットワーク環境では，VLAN-ID変換サーバ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．

5 おわりに

本論文では，文献[1]のVLAN相互接続方式に基づき，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-IDの変換を行うVLAN-ID変換サーバの実装と評価を行った．本実装ではVLAN-IDの変換機能をソフトウェアとして実現しているが，性能評価実験により十分な通信速度が得られることを確認した．

測定方法	平均転送速度 (Mbps)
直接接続	89.74
OpenVPN1	65.46
OpenVPN2	83.53
OpenVPN3	85.37
VC	88.39

表 1: 実験結果

今後は，VLAN相互接続方式におけるVLAN-ID変換サーバ以外の構成要素である，VLAN管理サーバおよび認証サーバの実現と，これらのサーバの連携機能について検討する予定である．

謝辞 本研究の一部は，文部科学省科学研究費平成16～17年度若手研究(B)課題番号16700071および総務省・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)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] 岡山聖彦，山井成良，岡本卓爾: “大規模VLAN環境におけるVLANの相互接続方式”，情報処理学会 分散システム/インターネット運用技術シンポジウム2003論文集，pp.55-60(2003).

[2] James Yonan:“OpenVPN”, http://openvpn.sourceforge.net/index.html.

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

[4] GNU Project:“GNU Database Manager”, http://www.gnu.org/software/gdbm/gdbm.html.

[5] Steven McCanne and Van Jacobson:“The BSD packet filter: A New Architecture for User-level Packet Capture”, Proc. of The 1993 Winter USENIX Conference, pages 259–269 (1993).

[6] Elmar Bartel:“nttcp: New TTCP Program”, http://www.leo.org/ elmar/nttcp.