VLAN相互接続方式に基づくシステムの設計と実装

二串 信弘† 岡山 聖彦†† 山井 成良†† 谷渕 陽祐‡ 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，VLAN-IDを部署毎に独立して動的に管理し，部署間でVLAN-IDを相互変換することでユーザの一時利用を可能にする方式が提案されており，本研究では，この方式の主要な構成要素であるVLAN管理サーバおよび認証サーバの設計と実装を行った．試作システムの有効性は，これらのサーバを利用した実験ネットワーク上での性能評価実験により確認している．

Design and Implementation of A System Based on the Method of Interconnection of VLANs

Nobuhiro Nikushi† Kiyohiko Okayama†† Nariyoshi Yamai††
Yousuke Tanibuchi‡ 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 arise. 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 describe design and implementation of a VLAN manager and an authentication server which are the major components of this method. The effectiveness of our system is confirmed by the experiment on the actual network using these servers.

1 はじめに

VLN(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技術である．VLAN技術によれば，VLANに対応したスイッチ(以下，単にスイッチという)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を容易に実現できる．

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

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

ごとに独立して管理されていると，部署間でVLAN-IDの衝突が生じたり，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接続した際に，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るVLAN管理サーバおよび認証サーバの設計と実装を行った．VLAN管理サーバは，一時利用のためのVLAN-IDリストを持ち，共通スペースのユーザに対して利用可能なVLAN-IDを動的に割り当てると共に，ネットワーク内のスイッチを自動設定してユーザの所属部署ネットワークまで一時的なVLANを構築する．一方，認証サーバは，一時利用ユーザに対する認証を行い，認証に成功した場合はVLAN管理サーバに対して一時利用のためのVLAN構築を要求する．さらに，これらのサーバと既に実装済みであるVLAN-ID変換サーバ[2]を用いて実験ネットワークを構築して性能評価実験を行うことにより，一時的なVLAN構築にかかる時間が実用上問題ないことを確認した．

以下，2章ではVLAN相互接続方式の概要について述べ，3章ではVLAN管理サーバおよび認証サーバの設計と実装，4章では性能評価実験について述べる．最後に，5章でまとめと今後の課題について述べる．

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，以下，基幹ネットワークをルートドメイン，部署ネットワークをサブドメインということにする．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つ以上のスイッチ(SW)で構成されるものとし，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．なお，原理上はドメインの階層数が3以上であってもよく，共通スペースの設置場所にも制約はないが，説明の簡単化のため，以降では階層数を2とし，共通スペースはルートドメイン内にあるものとして議論する．

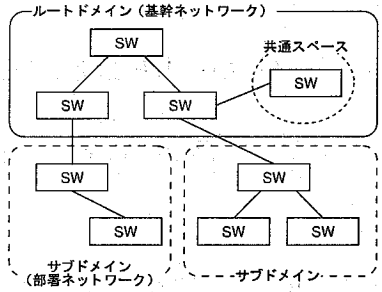

図1: 前提とするネットワーク構成

2.2 VLAN-ID動的割当てと相互変換

図1のネットワーク構成において，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を行うことについて考える．一般的なVLAN管理手法では，VLANが静的に管理されているので，ユーザが一時利用を行う際には管理者が全ての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全てのVLANをあらかじめ設定しておかなければならない．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がドメインごとに独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，スイッチによっては設定可能なVLAN-IDの数を超過する恐れがある．

これらの問題を解決するために，ドメイン毎にVLAN-IDを動的に管理し，ルートドメインとサブドメインの間でフレームに付加されているVLAN-IDの相互変換を行う方式がVLAN相互接続方式である．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 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システム構成例を図2に示す．本システムは，図1のモデルを元にVLAN管理サーバ(VS1，VS2)，VLAN-ID変換サーバ(VC)，認証サーバ(AS1，AS2)により構成される．以下，スイッチ以外の構成要素の役割について述べる．

- VLAN管理サーバ(VS1，VS2)

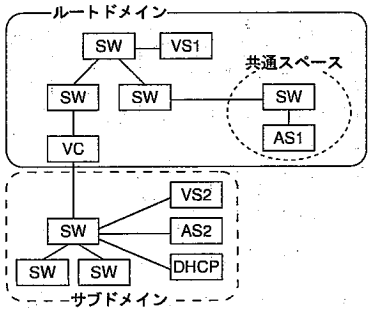

図 2: システム構成例

各ドメインに一つ設置され，一時利用のための VLAN-ID の管理とスイッチの管理を行う．

- VLAN-ID 変換サーバ (VC)
  各サブドメインとルートドメインとの境界に設置され，隣接するルートドメインとサブドメインによってそれぞれ割り当てられた VLAN-ID に基づいて，ドメイン間を通過するフレームの VLAN-ID 変換を行う．
- 認証サーバ (AS1，AS2)
  各サブドメインに 1 つと，共通スペースに 1 つ設置され，共通スペースに接続するユーザの認証を行う．サブドメインの認証サーバ (AS2) はドメインに所属するユーザの情報を保持しており，共通スペースの認証サーバ (AS1) は共通スペース内のユーザとサブドメインの認証サーバの間の通信を中継する．
- DHCP サーバ
  ユーザが所属するサブドメインにそれぞれ設置し，一時利用の設定が全て完了した後，ユーザ計算機に IP アドレスを割り当てる．

2.4 アクセス手順

図 2 において，共通スペース内のユーザが，所属サブドメインへアクセス可能になるまでのシステムの動作を示す．

1. ユーザは共通スペースのスイッチに接続し，AS1 にユーザ ID とパスワードを送信する．なお，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により，ユーザ ID のドメイン情報からユーザの所属するドメインを判別できるようにしている．AS1 はユーザ ID のドメイン名に基づき，サブドメインの認証サーバ (AS2) を決定し，認証情報を中継する．AS2 はユーザの認証を行い，完了した後に AS1 に認証成功の応答を送信する．
2. 認証に成功した場合，AS1 は VS1 に一時利用のための VLAN 設定要求メッセージを送信する．なお，このメッセージにはユーザ ID を含む．
3. VS1 は，一時利用のための VLAN-ID を発行し，ルートドメイン内のスイッチに対して，その VLAN-ID を許可する設定を行う．同時に，VS2 に対して，サブドメイン内の VLAN の設定を行うよう，VLAN 設定要求メッセージ (ユーザ ID を含む) を送信する．
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) スイッチの設定を行い，設定が完了した段階で VS1 に応答メッセージを送信する．この応答メッセージには VS2 が割り当てた VLAN-ID を含む．
5. VS1 は，自己の発行した VLAN-ID と，VS2 から取得した VLAN-ID を含む VLAN-ID 変換要求メッセージを VC に送信する．
6. VC は，VC は自己の保持する変換テーブルにこれらの VLAN-ID を登録し，応答メッセージを VS1 に送信する．
7. VS1 は，AS1 に対して全ての設定が完了したことを伝える応答メッセージを送信する．

ユーザが AS1 からの設定完了のメッセージを受信した時点で，ユーザはユーザの接続するスイッチから部署ネットワークまでデータリンク層レベルで接続可能となり，ユーザはサブドメインの DHCP サーバから IP アドレスを取得することにより，サブドメインにいるときと同様の作業を行うことが可能となる．

3 VLAN相互接続システムの設計と実装

2.3 節で述べたサーバのうち，VLAN-ID 変換サーバについては文献 [2] で報告済みである．したがって，本章では，VLAN 管理サーバおよび認証サーバの設計と実装について述べた後，サーバ間の通信について述べる．

3.1 VLAN 管理サーバ

VLAN 管理サーバに必要な機能は，VLAN-ID の管理機能，およびスイッチの自動設定機能である．本節では，これらの機能の実現方法について述べる．

3.1.1 VLAN-ID の管理

VLAN 管理サーバが保持する VLAN-ID の範囲は管理者によってあらかじめ設定され，VLAN 管理サーバはその範囲内で一時利用を行うユーザに対して VLAN-ID を割り当てる．このとき，VLAN 管理サーバはどの VLAN-ID がどのユーザによって使用されているかという情報や，どの VLAN-ID が割当て可能かといった情報を管理しなければならない．そこで，本研究では VLAN-ID 管理のためのデータベース (以下，VLAN-ID データベース) を導入した．

VLAN-ID データベースは VLAN-ID をインデックスにもつ線形リストとして構成し，ノード (以下，ユーザ情報ノードという) には VLAN-ID を使用中のユーザ情報を格納する．ユーザ情報ノードは以下の 4 つの属性を持つ．

- user_id

  一時利用中のユーザ ID を表す．

- sw_ip_addr

  ユーザが接続している共通スペースのスイッチの IP アドレスを表す．VLAN の設定時および設定解除時にこの値を参照する．

- sw_port

  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を表す．VLAN の設定時および設定解除時にこの値を参照する．

- pointer

  同じ VLAN-ID を利用している他のユーザ情報ノードへのポインタである．接続先ドメインが同じである複数のユーザに対して同一の VLAN-ID を割り当てることができるように，pointer を用いて複数のユーザ情報ノードを連結する．

図 3 に，VLAN-ID データベースの構成例を示す．図 3 では，VLAN-ID:100 以降が一時利用のために確保されていることを意味する．インデックスの VLAN-ID:101，102 は，現在ユーザに割り当てられており，他の VLAN-ID は未割当てであることがわかる．また，VLAN-ID:101 は所属ドメインが等しい 2 ユーザで共有されていることがわかる．

共通スペースの認証サーバから VLAN 設定の要求が到着した際に，VLAN 管理サーバは VLAN-ID の発行処理を行う．VLAN-ID データベースから利用可能な VLAN-ID を検索し，そのインデックス以下にユーザ情報ノードを作成し，VLAN-ID の発行処理が完了する．

3.1.2 スイッチの自動設定

VLAN 管理サーバは，3.1.1 節で自身が発行した VLAN-ID に基づき，ドメイン内に一時利用のため

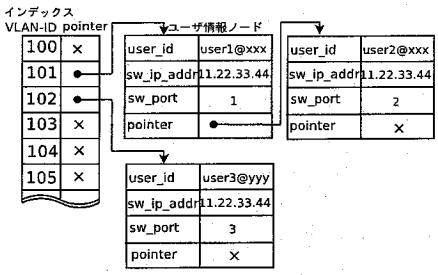

図 3: VLAN-ID データベースの構造例

の VLAN を構築する．VLAN を構築するには，適切なスイッチに対し VLAN の設定を行う必要があるため，VLAN 管理サーバはドメイン内のスイッチの接続関係を把握しなければならない．そこで，本研究では，管理者があらかじめ各隣接ドメインまでのスイッチの接続関係を VLAN 管理サーバに登録するという方法を採用した．

認証サーバから VLAN 管理サーバに VLAN の設定要求が到着した場合，ユーザ ID のドメイン情報を参照し，登録してあるスイッチの接続の関係情報を参照する．そして，発行した VLAN-ID の VLAN を共通スペースからドメインの境界までの間に構築する．

スイッチに対して VLAN の設定を行う一般的な方法は，telnet クライアントを用いてコマンドラインで設定を行う方法である．この処理を自動化するために，実装には対話型アプリケーションを自動化することを目的としたスクリプト言語である expect[3] を用いてバッチ処理化し実現した．

3.2 認証サーバ

本研究では，共通スペースのユーザに対する認証方式として IEEE 802.1X[4] を用いた．IEEE 802.1X は Windows2000/XP が標準でクライアント機能 (サプリカント) をサポートするなど広く使われている認証方式であり，データリンク層レベルで認証を行うので，クライアントが認証のための一時 IP アドレスを必要としないという利点がある．

なお，本研究では 802.1X の一実装である FreeRADIUS[5] を用い，FreeRADIUS のサーバプログラムに VLAN 管理サーバとの通信機能を追加した．共通スペースの認証サーバはサブドメインの認証サーバのプロクシとして動作し (FreeRADIUS のプロクシ機能を利用)，ユーザ情報は各サブドメインごとに管理される．

3.3 サーバ間通信

全てのサーバ間の通信は，1 つの要求に対して 1 つの応答を返す，という単純なやり取りであるため，全てのサーバ間で共通のメッセージフォーマットを用いた．

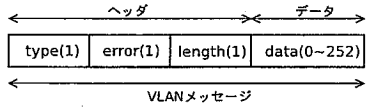

図 4: メッセージフォーマット

表 1: メッセージの type フィールド

type	意味
0	VLAN 設定要求
1	VLAN 設定要求の応答
2	VLAN 設定要求
3	VLAN 設定要求の応答
4	VLAN-ID 変換要求
5	VLAN-ID 変換要求の応答

図 4 にメッセージフォーマットを示す．図中の括弧内の数字はバイト数である．メッセージはヘッダフィールド (*type*, *error*, *length*) とデータフィールド (*data*) に分類され，ヘッダ長 3 バイト，データ長最大 252 バイトの最大 255 バイトのメッセージである．各フィールドの意味を以下に示す．

- type

  メッセージの種類を示すフィールドで，表 1 にフィールドの値とその意味を示す．

- error

  サーバが要求された処理を正常に実行できなかった場合のエラーを要求元のサーバに通知するためのフィールドである．正常な処理が行われた場合には 0 が挿入される．

- length

  1 バイトの length フィールドは，この後のフィールドである data フィールドに含まれるデータのバイト長が格納される．

- data

  メッセージのデータ部である．メッセージの type によって data フィールドに入るデータの種類や長さが異なる．

図 5 に，VLAN 設定時にサーバ間で送受信されるメッセージのフローを示す．各サーバは受信したメッセージの type フィールドの値によって次に行う処理を決定する．

4 実験と考察

本章では，3 章で述べた各サーバと文献 [2] の VLAN-ID 変換サーバを用いたシステム全体の動作確認実験と，本システムの有効性を検証するための性能評価実験について述べる．

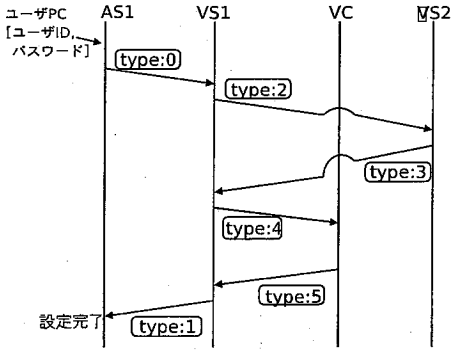

図 5: VLAN 設定時のサーバ間通信

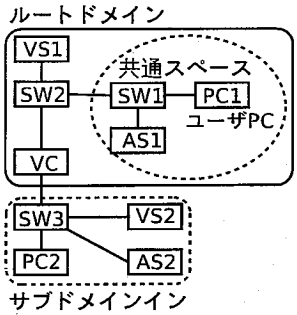

図 6: 実験ネットワークの構成

4.1 実験環境と実験方法

実験ネットワークの構成を図 6 に示す．各サーバには，いずれも FreeBSD4.8R を搭載した PC/AT 互換機 (Pentium4-3.4GHz，RAM1024MB) を使用し，スイッチには Cisco Systems 社の Catalyst3550 を用いた．また，ユーザが使用する端末は WindowsXP 搭載の PC を用い，認証クライアントには WindowsXP 付属の認証サプリカントを用いた．すべての機器は，100Base-TX の Ethernet で接続した．なお，今回の実験では DHCP サーバをサブドメインに設けておらず，ユーザが手動で PC1 に IP アドレスを割り当てた．

図 6 において，サブドメイン foo に属するユーザ nikushi が，共通スペースから自己の所属するサブドメインの VLAN を一時利用する実験を行った．このとき，ユーザ nikushi は通常サブドメイン foo 内の VLAN-ID:200 の VLAN に所属するものとする．ユーザ nikushi の情報はあらかじめ AS2 に設定し，AS1 では，サブドメイン foo に所属するユーザの認証要求が到着した場合，AS2 へ中継するように設定した．一方，VS1 では，一時利用のために発行可能な VLAN-ID の範囲を 100 から 150 と設定し，VS2 にはユーザ nikushi が VLAN-ID:200 の VLAN に所属するという設定を施した．なお，サブドメインに

表 2: ユーザの要求の際のシステムの処理時間

区間	時間 [sec]
区間 1	0.01
区間 2	3.71
合計	3.72

アクセスが可能になったかどうかの判断は，PC1 から PC2 へ ICMP エコー要求を送信し，ICMP エコー応答を受信することによって行った．

4.2 実験結果と考察

まず，ユーザ nikushi が PC1 を共通スペースの SW1 に接続し，PC1 が PC2 と通信可能になるまでの動作を確認したところ，2.4 節の手順に沿って認証および一時的な VLAN の構築が自動で行われることを確認した．さらに，VC を通過するフレームに含まれる VLAN-ID を調べたところ，VLAN-ID:100 と VLAN-ID:200 の相互変換が行われていることを確認した．

次に，システムの性能を評価するために，上記の動作確認実験を 10 回繰り返し，サブドメインへの一時利用が可能となるまでの時間の平均値を求めた．システムの処理時間について詳細な考察を行うために，以下に示す区間別に処理時間を測定した．なお，システムの処理時間とは，AS1 が PC1 から認証の要求を受け取り，認証と VLAN 設定などの処理が完了後，AS1 が PC1 に設定完了のメッセージを送信するまでの時間とした．

区間 1 AS1 が SW1 から認証要求のフレームを受信し，AS1，AS2 での認証が完了するまでの時間．

区間 2 AS1 が VS1 に VLAN 設定要求を送信し，AS1 が VS1 から設定の完了応答を受信するまでの時間．

表 2 に実験結果を示す．処理の合計時間は平均 3.72 秒であり，実用範囲内であると考えられる．しかし，所要時間の大部分は VLAN スイッチのリモート設定に要する時間であり，今回の実装では 3 台のスイッチが逐次設定されるため，スイッチ 1 台あたり約 1.2 秒かかったことになる．大規模な組織ではより多くのスイッチを経由することが予想されるため，今後はスイッチ設定の並列化や telnet 以外のリモート設定方法 (例えば SNMP など) を検討するなど，処理の高速化が必要である．

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，VLAN 管理サーバ，および認証サーバの設計と実装を行った．そして，VLAN-ID 変換サーバ含むシステム全体の動作確認実験を行い，一時利用のための VLAN-ID の割当てと，共通スペースからサブドメインの間の VLAN の構築が自動的に行われ，ドメインの境界での VLAN-ID の相互変換により共通スペースのユーザが自己の所属するサブドメインにアクセスできることを確認し，システムの処理時間について考察した．

今後は，通常のトラフィックと一時利用のトラフィックが混在する環境での性能評価や，VLAN 設定時間の短縮化，ドメイン内スイッチ構成の自動検出機能について検討する予定である．また，現在の実装ではスイッチをリモート設定する際のパスワードは expect スクリプト中に平文で指定されているため，安全なリモート設定方法を使用するプロトコルも含めて検討する必要がある．

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，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] 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] 濱本敦，岡山聖彦，山井成良，岡本卓爾: “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”, 情報処理学会 第 9 回分散システム/インターネット運用技術シンポジウム論文集，pp.1-6(2004).

[3] Don Libes, “Expect - Expect - Home Page”, http://expect.nist.gov/ .

[4] IEEE: “802.1X-2001 IEEE Standards for Local and Metropolitan Area Networks: Port-Based Network Access Control”, IEEE (2001).

[5] The FreeRADIUS Project: “FreeRADIUS – building the perfect RADIUS server”, http://www.freeradius.org/ .