大規模ネットワークにおけるVLAN管理システム

宮本貴朗[†1] 田村武志[†1] 鈴木亮司[†2]
平岡大樹[†3] 松尾英普[†3]
泉正夫[†4] 福永邦雄[†4]

パソコンの性能向上やインターネットの普及によるデータ伝送量増加にともなって，ネットワークの伝送容量を有効に使用することができるスイッチが普及しつつある．また，計算機の小型軽量化にともなって，モバイルコンピューティングが急速に普及してきている．そのため，端末を容易に移設することができるVLAN（Virtual Bridged Local Area Networks）機能を備えたスイッチが数多く製品化され，低価格化が進んでいる．しかしながら，VLANを構成するためには，各スイッチに対して複雑な設定を行う必要があり，スイッチの台数が多くなるとネットワーク管理者の負担が指数関数的に大きくなるという問題点が指摘されている．本稿では，VLAN構成情報を含めたスイッチの設定情報を一元的に収集/設定するとともに，複数のスイッチ間のVLAN設定の整合性を検証する機能を有するネットワーク管理システムを提案する．本手法に基づくネットワーク管理システムを実装し，実際に稼働している大規模ネットワークに適用して評価を行った結果，設定ミスが事前に検知できることによりネットワーク障害をなくし，ネットワーク管理者が行う各種の設定作業が大幅に軽減できることが確認された．また，管理システムの処理性能としては，VLAN構成の変更，スイッチ全体の設定に対してそれぞれ最大で20秒/台，2秒/台であり，実用上十分な性能であることも明らかにしている．

VLAN Management System on Large-scale Network

Takao Miyamoto,[†1] Takeshi Tamura,[†1] Ryouji Suzuki,[†2]
Taiki Hiraoka,[†3] Hideyuki Matsuo,[†3] Masao Izumi[†4]
and Kunio Fukunaga[†4]

With the massive growth of Internet and mobile computing, broader bandwidth and easier management are required, and switches have become more and more popular in the LAN environment. They not only increase the bandwidth available to end users but also offer flexibility for configuration changes such as moving of terminals. This is achieved by their VLAN (Virtual Bridged Local Area Networks) capability. To construct VLAN, however, complicated switch configuration might put the network administrators under the great overload. In this paper, we propose a network management system whose all-inclusive functions gather and set up the switch configuration including VLAN topology configuration and also check the integrity of VLAN configuration between switches. The proposed system has been evaluated on an actual large-scale operating network and we have obtained a satisfactory results. As the setting errors are found in advance, every setup task, usually done by the network administrators, can be greatly reduced without network error. As for the performance of the management system, the time for VLAN and switch configuration changes are maximum 20 seconds and 2 seconds per terminal respectively, which is good for real use.

†1 大阪府立大学総合情報センター
Library and Science Informaton Center, Osaka Prefecture University
†2 日立電線株式会社オプトロシステム研究所
Optoelectronic System Laboratory, Hitachi Cable Limited
†3 日立電線株式会社高砂工場
Takasago Works, Hitatchi Cable Limited
†4 大阪府立大学大学院工学研究科電気・情報系専攻
Electrical Engineering and Information Science, Graduate School of Engineering, Osaka Prefecture University

1. はじめに

近年のパソコンの性能向上と低価格化により，大学や企業などでは，デスクトップパソコンやノートブックパソコンの台数が急増している．大学や企業では，そのほとんどがLANに接続され，インターネット利用やマルチメディアコンピューティング端末として利用されている．このようにネットワークを介した動画をはじめとするマルチメディア情報を伝送するために，

より高速な LAN が求められ，最近では LAN の伝送容量の有効利用と高速化のため，従来のように受信フレームをすべてのポートに中継するハブに代わって，フレームを必要なポートのみに中継するスイッチングハブ（以下，スイッチと略す）が利用されるようになってきた．現在，スイッチは伝送容量不足の課題を解決する有効な手段として，急速に普及している．

さらに，携帯性に優れたノートブックパソコンなどの普及にともない，物理的な接続関係にとらわれず自由に端末をグループ化することができる VLAN（Virtual Bridged Local Area Networks）[1)~3)]の技術が開発され，ISO/IEC/IEEE などで標準化が進められている．VLAN 技術を利用すれば，端末を移設してもブロードキャストフレームの中継範囲を VLAN グループ内に制限でき，伝送容量を有効に利用できるなど多くの利点がある．

しかしながら，LAN の構築および運用管理の側面から見ると，スイッチ数の増加とともに各種設定項目数が飛躍的に増大して複雑になり，ネットワーク管理者（以下，管理者と略す）の負担がますます増大する傾向にある．VLAN を構成するためには，その VLAN に関するすべてのスイッチに対して設定を行う必要があり，VLAN を構成するスイッチの台数が多い場合やネットワーク構成が複雑な場合には，VLAN 設定も複雑になり設定ミスが生じやすい．しかも，VLAN 設定にミスがあっても容易に気づかないことが起こりうる．たとえば，プロトコル VLAN を構成している場合には，通信に用いるプロトコルによって通信可能であったり通信不可能であったりすることが考えられる．したがって，複雑・大規模化するネットワークにおいては，なおさら各スイッチに対する VLAN の設定は正確を期する必要がある．

VLAN 設定作業を個別に行う場合，ネットワーク規模が大きくなると膨大な作業量になり，管理者に大きな負担となる．また，VLAN 技術を用いて構築・運用されているネットワークにおいては，設定を誤るとリモートでの管理が行えなくなることもあり，実際にスイッチが設置されている場所に出向いて作業をしなければならないことも考えられる．構内が広い場合や広域網などでは，管理者の移動だけでも大変な作業ロスになるだけでなく，各設置場所で作業環境を整える必要があり，設備上また人員配置上も大きな問題となる．

この作業を軽減するため，各スイッチメーカは簡単なマウス操作で自社スイッチの管理を行うことができるネットワーク管理ソフトウェア（SNMP[4)]マネージメントソフトウェア）を製品化しているが，スイッチ単体での管理しか行えないものが多い．また，VLAN 管理に関していえば，各スイッチの VLAN 設定情報を個別に収集し画面に表示することやユーザからの指示に従い VLAN 設定の変更を行うことはできるが，多数のスイッチにまたがる VLAN 設定情報を一括して管理することができない．したがって，各スイッチの VLAN 設定が相互に矛盾なく設定されているかどうかの判定は行えず，設定に誤りがないかどうかはネットワーク管理者が確認する必要があった．

本稿では，Web ブラウザから複数のスイッチに対して一括して各種の項目を設定することにより，管理者が行う各種設定作業を大幅に軽減し，管理者を支援するシステムを提案している．特に，複数のスイッチにまたがる VLAN の運用を必要とする大規模なネットワークに対して VLAN 構成一括管理機能を提供することを目的としている．

本システムは次のような特徴を有する．

(1) ネットワーク構成画面内で，グループ化するポートを複数選択し，VLAN 構築に必要な属性を入力すると，選択された複数のスイッチに対して VLAN 設定の整合性を検査することができる．
(2) 複数のスイッチの VLAN 設定情報を含むすべての設定情報をデータベースに一括して保存し，ネットワーク全体の構成管理を行うことができる．
(3) 複数のスイッチのファームウェアなどのバージョンアップ作業を一括して行うことができる．

このように，複数のスイッチの VLAN 設定の整合性を検査する機能を持ち，設定・管理を一元的に効率良く行うシステムはこれまでほとんど実現されていない．また，この機能を管理サーバとして実装し，実証実験を行った結果，作業が大幅に軽減できることが明らかになり，本システムの有効性が確認できた．

2. VLAN 構築と管理

2.1 VLAN 管理

VLAN は，スイッチにより構成されるネットワークに接続されている各種端末を目的に応じてグループ化する技術である．VLAN の構成例を**図 1** に示す．VLAN を構成すると，異なるスイッチに接続されている端末を同一グループにしたり，同じスイッチに接続されている端末を異なるグループに分割するなど物理的な配線に拘束されずに柔軟に設定できる利点がある．

一般に，スイッチの VLAN 機能を使用するためには，各スイッチに VLAN の定義情報を作成し，各ポートをどの VLAN に所属させるかを設定する必要があ

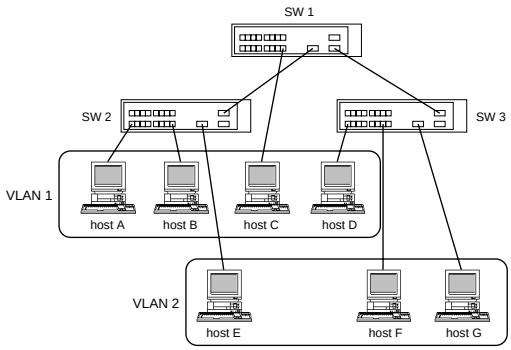

図 1 VLAN の構成例
Fig. 1 Network example using VLAN.

表 1 VLAN 属性
Table 1 VLAN configuration.

Configuration item	Description
Switch name	switch name of this VLAN
vlan_id	vlan_tag number
type	type of this VLAN
vlan_name	name of this VLAN
protocol	protocol of this VLAN
qos	class of QoS
stp_run	configuration of STP
stp_dom	domain name of STP
ip_addr	IP address of this VLAN
subnet_mask	subnet mask of this VLAN

る．VLAN 作成のために設定が必要な VLAN 属性を**表 1** に示す．

VLAN に所属するポートにはトランクリンクポート（trunk link port）とアクセスリンクポート（access link port）とがあり，スイッチを対向で接続するポートはトランクリンクポートに設定し，端末を接続するポートはアクセスリンクポートに設定する．スイッチがトランクリンクポートにフレームを中継する場合，そのフレームがどの VLAN のフレームであるかなどの情報を含む 2 byte の tag を挿入して中継する．また，スイッチがアクセスリンクポートにフレームを中継する場合，その tag を取り除いて中継する．

また，VLAN を構築して運用するには，次のような設定/確認作業が必要である．

(1) スイッチと端末の物理的配線を確認する．
(2) VLAN を作成する．そのために，表 1 に示したような vlan_id などの識別子やプロトコル，QoS（Quality of Service），スパニングツリー（STP）などの VLAN 属性を設定する．
(3) 端末が接続されているポートは，送受信フレームに vlan_id を付加しないアクセスリンクポートに設定し，VLAN を割り当てる．
(4) スイッチを対向で接続するポートは，送受信フレームに vlan_id を付加するトランクリンクポートに設定し，そのポートで中継が必要なすべての VLAN を割り当てる．

2.2 設計目標

本システムでは，上述した問題点を解決しネットワーク管理者の負担を軽減するために，次に示す機能を実現することを目標とした．

(1) ネットワーク構成画面上で，アクセスリンクポート/トランクリンクポートに設定するポートをそれぞれマウスで複数選択し，vlan_id を入力するだけで，VLAN 設定の整合性を検証し，選択したすべてのスイッチに必要かつ十分な VLAN 設定を一括して行うことができること．
(2) 各スイッチの VLAN 設定情報を中心となるサーバ上でデータベースの形で保存し，統合的な管理が行えること．また，ネットワーク全体の VLAN 構成を含む設定情報が一覧表示できること．このことにより，全体の見通しの良さを保ちながら管理作業を容易に行うことができること．
(3) 複数のスイッチのファームウェアなどのバージョンアップ作業を一括して行うことができること．
(4) 実際のネットワーク管理においては，障害などが発生した場合に管理装置が設置されていない場所での作業も必要になる．そのため，管理装置を限定せず，Web ブラウザを有する任意の端末からでもネットワーク経由で管理操作ができること．

3. システムの機能

3.1 VLAN 設定機能の概要

VLAN を構築する場合には，矛盾なく vlan_id, vlan_name, IP address, プロトコルなどの設定を設計し，VLAN を構成するすべての機器に対して同じような設定作業を行う必要がある．

本システムでは，次のような手順で複数機器への VLAN 同時設定を実現する．

(1) 管理端末画面上へネットワーク構成図を表示する．
(2) 設定を行う機器およびポートを 1 つ，または複数台選択する．
(3) ネットワーク管理サーバは，指定されたすべての機器に対し，必要に応じて以下の操作を行う．
  (a) 新たに VLAN を作成する場合には，VLAN の名前，VLAN 方式，プロトコ

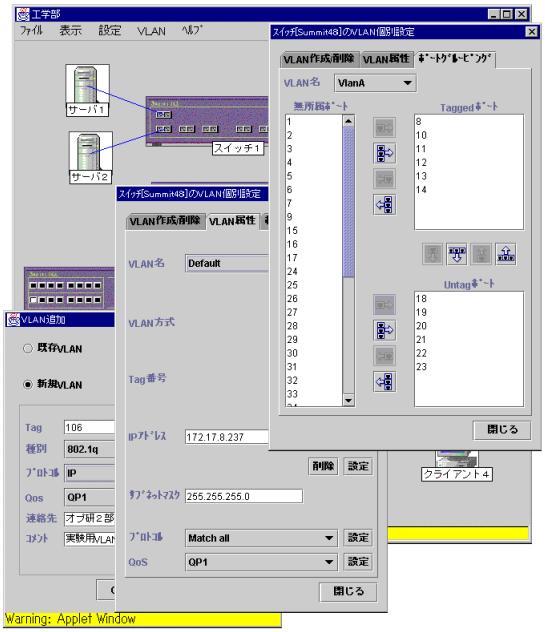

図 2 VLAN 設定インタフェース
Fig. 2 User interface for VLAN configuration.

ル，スパニングツリー動作状況など，表 1 に示した定義情報を設定し，VLAN を作成する（**図 2**）．

（b） VLAN 属性の設定変更を行う．

（c） VLAN に機器を追加/削除する場合には，選択されている機器の選択されているポートを VLAN に追加/削除する（図 2）．

（d） VLAN を削除する場合には，VLAN 属性を削除するとともに，その VLAN に所属しているポートを VLAN から削除する．

同時設定機能は，複数機器への設定を同時に実施するため，管理者の負担が軽減できるというメリットのほか，各機器の設定が異なったり，矛盾したりすることを防ぐことができる．

一般的に VLAN の種類として，port-based VLAN，MAC Address VLAN，プロトコル VLAN，IEEE 802.1Q VLAN などがある．本システムでは，スイッチが持つすべての種類の VLAN に対する参照・設定機能を有しているが，複数機器にまたがった VLAN の整合性の検出を行う VLAN ポート設定検証機能については，IEEE 802.1Q VLAN を対象としている．

3.2 初期設定および設定情報の収集

まず，VLAN 管理サーバにネットワークを構成するスイッチを登録し，各スイッチの IP アドレス，SNMP コミュニティ名，登録ユーザ名，パスワードを設定する．次に，SNMP および telnet を用いて VLAN 設定情報を含むネットワークを構成するすべてスイッチの設定情報を VLAN 管理サーバに収集する．スイッチ間の物理的な接続関係は，収集されたスイッチの設定情報だけでは自動的に生成することは困難であるので，管理者が画面を参照しながら登録を行う．

表 2 VLAN 属性検証項目
Table 2 Verification items of VLAN configuration.

Item	Description
protocol	kind of protocol (IP, IPX, etc.)
IP address	consistency of IP address
subnet mask	consistency of IP subnet mask
STP status	consistency of STP status
STPD name	consistency of STP domain name

3.3 VLAN 設定検証機能

3.3.1 VLAN 属性検証機能

複数機器により VLAN を構成する場合，各機器に設定した VLAN 属性が一致していないと正常に通信できない可能性がある．そこで，**表 2** の項目について，同一 VLAN に属している機器の VLAN 属性の整合性の検証を行い，VLAN 属性について設定ミスがあれば，画面上に設定ミスの可能性のある機器およびポート番号，現在設定されている条件およびその原因を表示する．

3.3.2 VLAN ポート設定検証機能

- 不十分な VLAN 設定

あるスイッチ A にある VLAN（以下，対象 VLAN と呼ぶ）のアクセスリンクポートが存在し，別のスイッチ B にも対象 VLAN のアクセスリンクポートが存在する場合，スイッチ A とスイッチ B を結ぶ物理的経路上のすべてのポートが対象 VLAN のトランクリンクポートに設定されている必要がある．物理的経路上のいずれかのポートがトランクリンクポートに設定されていない場合や物理的経路のいずれのポートもトランクリンクポートに設定されていない場合には，スイッチ A のアクセスリンクポートに接続されている機器とスイッチ B のアクセスリンクポートに接続されている機器とは正常に通信できない可能性がある．

ここでは，VLAN 設定ミスの例として**図 3** に示すようなネットワークを考え，その構成において各スイッチから収集した VLAN 設定情報を**表 3** に示す．

図 3 のネットワーク構成について考えると，表 3 のような VLAN 設定がなされている場合には，SW 3 の port 18 が VLAN 1 のトランクリンクポートに設定されていないため，host A や host B から送出される

表 3 VLAN 設定ミスの例
Table 3 An example of fault configurations of VLAN.

Switch	port No.	neighbor SW / port No.	VLAN 1	VLAN 2
SW 1	p1	none	none	access link
	p5	none	access link	none
	p18	SW 2 / p17	trunk link	trunk link
SW 2	p1	none	none	access link
	p17	SW 1 / p18	trunk link	trunk link
	p18	SW 3 / p17	trunk link	trunk link (error)
SW 3	p1	none	access link	none
	p17	SW 2 / p18	trunk link	none
	p18	SW 4 / p17	none (error)	none
SW 4	p1	none	access link	none
	p17	SW 3 / p18	trunk link	none

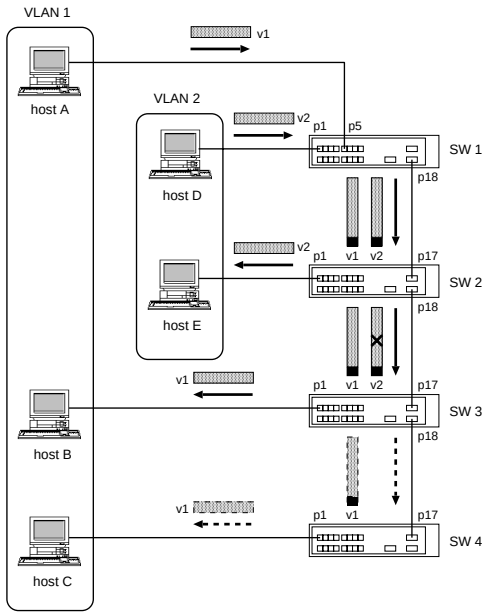

図 3 VLAN 設定ミスの例
Fig. 3 Network example of fault configurations of VLAN.

VLAN 1 のパケットが SW 4 には到達しない．そのため，host C にも VLAN 1 のパケットは到達しない．このような設定に不十分な VLAN があれば，画面上に設定ミスの可能性のある機器およびポート番号，現在設定されている条件およびその原因を表示する．

- 不要な VLAN 設定

あるスイッチ A にある対象 VLAN のトランクリンクポートが存在する場合，そのトランクリンクポートに物理的に接続されているスイッチ B にスイッチ A との接続ポート以外に対象 VLAN のトランクリンクポートまたはアクセスポートが存在するかどうかを判定する．トランクリンクポートもアクセスリンクポートも存在しない場合，スイッチ B に接続されているスイッチ A のポートは，対象 VLAN のトランクリンクポートに設定する必要がないのに対象 VLAN のトランクリンクポートに設定されていると判断する．

図 3 のネットワーク構成について考えると，表 3 のような VLAN 設定がなされている場合には，SW 2 の port 18 が VLAN 2 のトランクリンクポートに設定されているが，SW 3 には VLAN 2 のトランクリンクポートもアクセスリンクポートも存在しない．そのため，host D や host E から送出される VLAN 2 のパケットが届く必要のない SW 3 にも届いてしまう．このような不要な VLAN 設定があれば，画面上に設定ミスの可能性のある機器およびポート番号，現在設定されている条件およびその原因を表示する．

3.3.3 VLAN ポート設定検証手順

具体的な VLAN ポート設定の検証は，以下の手順で行う．

step1 管理サーバに登録されている VLAN（IEEE 802.1Q VLAN）を検索し，VLAN ごとに所属しているアクセスリンクポート（以下，ALP と略す）およびトランクリンクポート（以下，TLP と略す）のスイッチとポート番号を取得する．

step2 得られたすべての ALP に対し，スイッチ内の同じ VLAN に属している TLP を検索する．TLP が存在しない場合には，スイッチに直接接続している他のスイッチの VLAN 設定を検索し，もし直接接続されているポートに TLP が設定されていればその ALP に「不十分な VLAN 設定」があると判定する．

step3 得られたすべての TLP に対し，以下の条件について調べる．

条件 A TLP が存在するスイッチに直接接続しているスイッチの VLAN 設定情報をすべて検索し，直接接続しているポートに ALP もしくは TLP が設定されているか？

条件 B TLP が存在するスイッチに直接接続し

表 4 VLAN ポート設定の検証結果
Table 4 Results of verification of VLAN port assignment.

条件 A	条件 B	判定
○	○	設定は正しい
○	×	接続元および接続先の VLAN 設定が不要
×	○	接続元の VLAN 設定が不要
×	×	接続先の VLAN 設定が不十分

ているスイッチの VLAN 設定情報をすべて検索し，直接接続しているポート以外の他のポートに ALP もしくは TLP が設定されているか？

条件 A および条件 B から**表 4** のように判定する．

このように，同じ vlan_id が設定されているスイッチを検索し，物理的な接続関係から VLAN の整合性を網羅的に検証する．そのため，設定ミスが 1 カ所だけの場合には，複雑なネットワークであっても整合性の検証は正しく行われる．しかし，複数のスイッチに複数の設定ミスがある場合には，正しい設定が複数考えられることがあり，設定ミスの特定が困難である．そこで本システムでは，考えられる設定ミスをすべて提示し，管理者が設定ミスを特定する方法を採用している．

3.4 設定情報バックアップ機能

ネットワーク機器に障害が発生した場合，新しい機器に交換することも多い．その場合，その機器に対する設定作業をやり直す必要がある．そのため，一般的に各ネットワーク機器の設定情報をファイルの形で保存しておくことが多い．しかしながら，大規模なネットワークになると設定情報の管理は複雑になり，新たにネットワーク機器の設定を変更するたびに，設定情報の管理が必要になる．そのため，本システムでは，管理サーバに TFTP[5] サーバを搭載し，TFTP により各スイッチの設定情報を管理サーバに転送し，ファイルとして保存する機能を実装した．管理サーバでは，収集された各ネットワーク機器の IP アドレスをキーとするデータとして設定情報をファイルの形で管理する．

3.5 設定情報のログ作成機能

大規模なネットワークにおいては，ネットワーク管理作業を複数人で分担して行うことが多い．その際，他の管理者がネットワーク機器の一般的な設定を変更する場合や，VLAN を新たに作成する場合には，管理者間での連絡確認を行う必要が生じる．本システムでは，ネットワーク機器の一般的な設定に関しての変更作業を管理サーバ上に保存し，ログとして残す機能を搭載した．また，VLAN 設定に関しても，複数のスイッチに対しての設定変更作業をログ化して保存し，HTML への出力を行う機能を実装した．

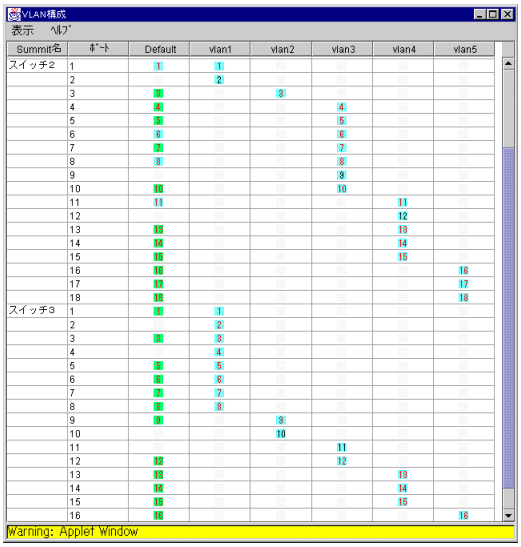

図 4 VLAN 構成表示例
Fig. 4 An example of representation of VLAN port assignment.

3.6 データの保存

本システムでは管理対象機器のパラメータや取得した情報をデータベースに保存する．この場合，データを各機器ごとに保存するとともに，各種のデータの関係をリレーショナルデータベースのリンク情報として格納する．

3.7 VLAN 構成表示機能

ネットワーク全体もしくは指定された VLAN やスイッチ単位での VLAN 構成情報を一覧表示する．このことにより，全体の見通しの良さを保ちながら管理作業を容易に行うことができる．ここでは，ネットワーク全体の VLAN 構成表示例を**図 4** に示す．

3.8 ユーザ認証機能

本システムでは，管理者端末から管理サーバへのアクセスには，ユーザ名とパスワードによる認証を行う．ユーザには一般ユーザと特権ユーザがあり，一般ユーザは設定情報の参照のみ可能であり，特権ユーザはすべての設定情報の参照と変更を行うことができる．また，管理サーバへのユーザの登録は特権ユーザのみが行うことができ，一般ユーザは自分自身のパスワードのみ変更可能である．管理者端末から管理サーバへの特権ユーザのアクセスは同時 1 ユーザに制限し，複数の特権ユーザが同時にスイッチの設定変更を行うことがないよう排他制御を行う．

一般に，ネットワーク機器にも一般ユーザと特権

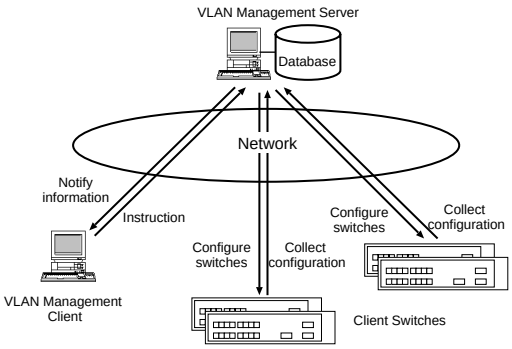

図 5 システムモデル
Fig. 5 System model.

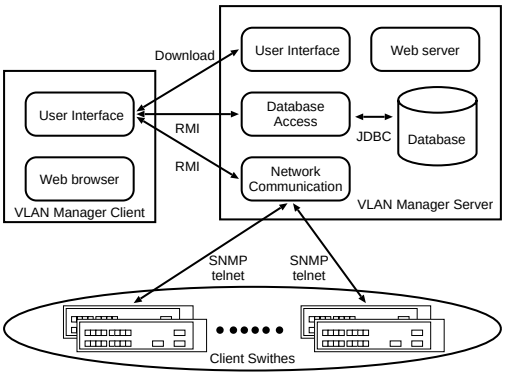

図 6 ソフトウェアシステム構成
Fig. 6 Software system architecture.

ユーザがあり，それぞれのパスワードにより認証を行う必要がある．本システムでは，すべてのスイッチのユーザ情報とパスワード情報を管理サーバ上のデータベースに登録し，管理サーバからスイッチへのアクセスには，管理サーバに登録されているパスワードを用いることにより認証を行う．

3.9 その他の機能

その他の機能として，オブジェクトの追加，変更，削除機能およびトポロジー設定機能がある．

4. システム構成

4.1 システム概要

本システムは，管理サーバ，ブラウザを搭載した管理者端末，管理対象スイッチから構成される．システム全体の構成を**図 5** に示す．

図 5 に示したように，管理者は端末（Java が搭載された Web ブラウザが稼働すれば種別は問わない）にて，Web ブラウザを起動して管理サーバの Web サーバにアクセスし，スイッチの設定・管理を行う．この場合，どの端末からでも管理できるようにするため，スイッチとの通信は端末側ではなく，管理サーバ側で行うようにした．管理サーバは，SNMP および telnet を使用して機器の設定情報の参照と変更を行う．本システムでは，実装例として Extreme networks 社のギガビットイーサネットスイッチを管理対象機器として実装を行った．

本システムによりスイッチを管理するための手順は以下のとおりである．

(1) 管理者は，ネットワークに接続されている端末で，Web ブラウザを起動し，サーバプログラムが実装されている管理サーバに接続する．
(2) 管理サーバは，各スイッチから各種情報を収集し，データベースに保存する．
(3) 端末のブラウザ画面には，現在の VLAN 構成や各スイッチの詳細な設定内容が表示される．
(4) VLAN を設定する場合，管理者はブラウザ画面上のマウス操作によって設定内容を指示する．
(5) 管理サーバは，指示に従って複数のスイッチに対して設定項目の設定を行う．

4.2 ソフトウェア構成

ここでは，管理サーバに実装するソフトウェア構成について述べる．**図 6** にソフトウェアの構成を示す．

管理サーバのソフトウェアは，ユーザインタフェース部，通信処理部，データベース処理部の 3 つのプログラムから構成される．これらのプログラムは，Java[6),7)] 言語で記述した．

Java 言語は，Web ブラウザ上でプログラムが実行されることを考慮して設計されており，HTML（HyperText Markup Language）[8),9)]では実現することが困難な高度なユーザインタフェース機能を実現することができる．また，現在広く利用されている主要なブラウザ（Netscape Navigator，Internet Explorer など）には，Java プログラムを解釈，実行する機能が内蔵されている．さらに，Java プログラムは，CPU や基本ソフトウェアに依存しないため，Windows や Macintosh，UNIX などの端末においても実行できるという特徴を有する．

管理者が端末の Web ブラウザを起動して管理サーバに接続すると，Java applet が端末側にダウンロードされ，端末のブラウザ上で実行される．しかし，ユーザインタフェース部は，管理サーバ上で実行される通信処理部とデータベース処理部との間で，指示や情報をやりとりする必要がある．これを実現するため，Java プログラムによる分散処理方式 RMI[10)] を使用した．RMI を使用すると，異なるコンピュータ上で実行されている Java プログラムを連携して動作させる

表 5 実験結果（秒）
Table 5 Experimental results (sec.)

実験方法	5 台	10 台	20 台	40 台	80 台
Firmware の download	32	52	82	157	294
VLAN の追加	105	210	429	857	1,762
VLAN の削除	78	152	301	593	1,201
SNMP データの download	82	159	322	650	1,261
設定情報の upload	10	18	32	62	125

ことができる．ユーザインタフェース部を RMI クライアント，通信処理部とデータベース処理部を RMI サーバとして実装することにより，これら 3 つのプログラムの連携動作が実現できる．

4.2.1 ユーザインタフェース部

ユーザインタフェース部は，データベース処理部から VLAN 設定情報を受け取り，その情報を GUI（Graphical User Interface）を用いて画面に表示を行う．また，管理者からのスイッチ設定指示情報を受け取り，通信処理部に通知する．

4.2.2 通信処理部

通信処理部は，クライアント端末にダウンロードされた RMI クライアントからの指示を受けて，スイッチからの設定情報の取得およびスイッチへの設定を行う．スイッチとの間で情報をやりとりするプロトコルは，SNMP および telnet により行う．

なお，VLAN 設定情報の取得や操作などに関する SNMP の MIB については標準化されておらず，ベンダ独自の拡張 MIB を利用する必要がある．拡張 MIB 情報については，最近では多くのベンダが公開する方針をとっており，本システムでは拡張 MIB の必要部分を各ベンダごとにデータベース化し，機種依存部分の分離を行っている．telnet については，コマンドの引数などが同じ機種でもファームウェアのバージョンにより異なる場合もあり，機種だけでなくバージョンの違いも吸収可能なようにデータベース化を行っている．

4.2.3 データベース処理部

データベース処理部は，クライアント端末にダウンロードされた RMI クライアントから指示を受けて，データベースに情報を保存したり，情報の検索・抽出を行う．リレーショナルデータベースとの通信処理は，SQL（Structured Query Language）を使用した．データベース処理部は，Java プログラムから SQL を使用するためのインタフェース仕様 JDBC（Java Database Connectiviry）に従って実装した．

5. システムの実装と評価

5.1 システムの実装

これまで述べた方式に基づき，VLAN 構成管理のためのネットワーク構築/管理システムを実装し評価を行った．VLAN 管理サーバには Pentium II 400 MHz 256 MB RAM の PC/AT 互換機を使用し，OS には Windows NT 4.0 を用いた．また，WWW Server には Microsoft 社の IIS（Internet Information Server），Database には Sybase 社の Adaptive Server Anywhere，Java と Database とのインタフェース部には Sybase 社の JConnect を用いた．

ソフトウェア開発は Visual C++および JDK 1.1.8 で行い，総ステップ数は約 50,000 である．

5.2 実 験 方 法

本システムを用いて，実稼働している大規模ネットワーク環境で以下の実験を対象スイッチの台数を変えながら行った．そのときの実行時間を計測したものを**表 5** に示す．

(1) ファームウェアのダウンロード
管理サーバに搭載した TFTP サーバ機能を用いて，スイッチのファームウェアのバージョンアップを行う．転送するファームウェアのサイズは約 1.8 MB である．

(2) 新たな VLAN の作成
新たな VLAN を生成し，各スイッチのうちの 2 ポートをその VLAN に追加する．

(3) 既存の VLAN の削除
各スイッチのうち，既存の VLAN に属するポートをすべて削除し，VLAN 設定情報の削除を行う．

(4) SNMP データのダウンロード
スイッチが保持しているすべての SNMP データを取得する．取得するデータのサイズは約 500 KB である．

(5) 設定情報のアップロード
各スイッチへの設定情報の転送を TFTP を用いて行う．スイッチの設定情報のサイズは約

8.5 KB である．

計測結果をみると，VLAN の追加/削除では実行時間と台数はほぼ線形に近い関係があり，その他の作業においては線形よりも少ない時間で設定作業が終了することが分かる．実際，VLAN の追加/削除に関しては，手慣れた作業員が手作業で同じ作業を行った場合に，設定ミスがなかったとしても 80 台のネットワーク機器に対して VLAN 追加を行うためには，確認作業を含めるとほぼ半日の時間を要することから，管理者の負担が大幅に軽減できることが確認できる．

6. 考　　察

本システムの特徴は，以下のとおりである．

(1)　複数のスイッチに対して一度にまとめて設定する機能を持ち，設定作業の簡略化を実現した．複数機器への設定が一度に実施できるため，管理者の負担が大幅に軽減できる．

(2)　VLAN 設定作業の検証機能を実装しているので，複数のスイッチに対して複雑な VLAN を構築する際にも設定ミスを回避できる．また，複数機器に対して同じ設定を行うため，各機器の設定が異なったり，矛盾したりすることを防ぐことができる．

(3)　複数のスイッチから構成されるネットワーク機器の設定情報を一括して保存・管理できる．このことにより，大規模なネットワークにおいても設定情報の世代管理ができる．また，ネットワークの設定状況や運用状況などの全体像を容易に把握することができる．さらに，設定情報をファイルの形でデータベース化して保存しているので，機器単位での再設定が必要なときに容易に設定を行うことができる．

(4)　Java が稼働する一般的なブラウザを搭載していれば，どの端末からでも管理作業を可能とした．このことにより，実際にネットワーク機器が設置されている場所に出向いて作業を行う必要がある場合に，現場にある端末を安全に管理端末として利用することができる．

(5)　管理サーバから行われた設定変更は，管理サーバにログの形で保存する．また，VLAN 設定に関しても複数のスイッチに対して行われた設定の変更作業情報をログ化し保存・出力する機能を実装している．このことにより，ネットワーク管理作業を複数の管理者が行う場合に，他の管理者が行った作業を時系列的に把握し，ネットワークの全体の運用を容易に把握することができる．

本システムでは，対象機器として特定のベンダの機器に限定して実装し評価を行っているが，一般にネットワークは多くのベンダの機器で構成されていることが多い．マルチベンダ対応について考えると,「標準」である SNMP 準拠のネットワーク機器においても，ベンダ独自の拡張や制約を設けている場合が多く，開発コストを低減するためにネットワーク管理システムのためのフレームワークを構成する方法[11),12)]やベンダ独自の拡張 MIB の対応関係を記述し，その参照プログラムを自動生成する手法[13)]が提案されている．

本システムは，システム構成の章で述べたとおりユーザインタフェース部，通信処理部およびデータベース処理部から構成され，各部分は可能なかぎり独立かつ階層的な構成とし，ソフトウェアのモジュール化を行っている．そのため，異なるベンダの機器への対応には，通信処理部の機種依存部分のカスタマイズを行えば対応可能な構成としている．VLAN 管理においては，管理技術の標準化は未完了であり，現状では SNMP 以外のベンダ独自の管理プロトコルを使用せざるをえないが，VLAN 管理技術が標準化が行われれば対応は容易であると考えられる．

7. む　す　び

Java を利用して Web サーバとデータベースを連携させることにより，複数スイッチによって構成される VLAN を容易に一括管理するネットワーク管理システムを開発した．本システムでは，複数機器に対して同じ設定を行うため，各機器の設定が異なったり，矛盾したりすることを防ぐことができる．また，VLAN 構成の整合性を検証する機能を実装し，複雑な VLAN を構成する場合にも設定ミスを防ぐことができる．

今後の課題として，ネットワーク機器に障害が発生した場合に，管理サーバに保存されている構成情報と設定情報を用いて，最低限の設定を済ませた代替機器をネットワークに接続するだけで管理サーバから設定情報を自動的に設定する機能を追加することを検討している．また，VLAN の管理技術の標準化が COPS（Common Open Policy Service protocol）などにより行われ，ベンダによる実装が進むことにより，より多くのベンダのネットワーク機器に対応させることが必要になると思われる．

参 考 文 献

1) IEEE Std 802.1Q-1998, IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks (1998).
2) IEEE Std 802.1D-1998, IEEE Standards for Information technology – Telecommunications

and information exchange between systems – Local and Metropolitan Area Networks – Common Specifications Part 3: Media Access Control (MAC) Bridges (1998).
3) IEEE Std 802.1ac-1998, IEEE Standards for Information technology – Telecommunications and information exchange between systems – Local and Metropolitan Area Networks – Specific requirements Part 3: Carrier sence multiple access with collision detection (CSMA/CD) frame extensions for Virtual Bridged Local Area Networks (VLAN) tagging on 802.3 networks (1998).
4) Case, J., Fedor, M., Schoffstall, M. and Davin, J.: Simple Network Management Protocol (SNMP), RFC1157 (1990).
5) Sollins, K.R.: The TFTP Protocol (Revision 2), RFC1350 (1992).
6) Horstmann, C.S. and Cornell, G.: *Core Java 2 Volume I – Fundamentals*, Prentice-Hall (1998).
7) Horstmann, C.S. and Cornell, G.: *Core Java 2 Volume II – Advanced Features*, Prentice-Hall (1999).
8) Berbers-Lee, T., Fielding, R. and Frystyk, H.: Hypertext Transfer Protocol – HTTP/1.0, RFC1945 (1996).
9) Fielding, R., Gettys, J., Mogul, J., Frystyk, H. and Berbers-Lee, T.: Hypertext Transfer Protocol – HTTP/1.1, RFC2068 (1997).
10) Sun Microsystems, Inc.: *Java Remote Method Invocation* (1998). http://java.sun.com/jdk/rmi/index.html.
11) 荒野高志，青野 博，藤崎智宏：ネットワーク管理フレームワークとその開発に関する一考察，情報処理学会論文誌，Vol.38, No.6, pp.1182–1191 (1997).
12) 浜田雅樹，蔭山克禎，藤崎智宏：管理プロトコルへの適応性を有するネットワーク管理システム用フレームワーク構成法，情報処理学会論文誌，Vol.41, No.1, pp.101–109 (2000).
13) 堀内浩規，吉原貴仁，杉山敬三，小花貞夫，鈴木健二：ネットワーク管理のための管理情報ベース（MIB）に対する柔軟なビュー提供方式，情報処理学会論文誌，Vol.39, No.2, pp.367–378 (1998).

(平成 12 年 4 月 28 日受付)
(平成 12 年 10 月 6 日採録)

宮本 貴朗（正会員）

1985 年大阪府立大学総合科学部卒業．1987 年同大学大学院総合科学研究科修士課程修了．1988 年同大学院工学研究科博士後期課程退学．同年同大学計算センター助手．現在，同大学総合情報センター講師．画像処理，情報ネットワークに関する研究に従事．電子情報通信学会，システム制御情報学会，IEEE，ACM 各会員．

田村 武志（正会員）

1966 年東海大学工学部電気工学科卒業．1962 年国際電信電話（株）入社．衛星・海底ケーブルネットワークの運用管理，同社国際電気通信学園にて CAI，遠隔教育システムの研究開発に従事．現在，大阪府立大学総合情報センター教授．工学博士．次世代型遠隔教育，学習システム等の研究に従事．電子情報通信学会，教育システム情報学会，日本ディスタンスラーニング学会各会員．

鈴木 亮司

1992 年東北大学大学院工学研究科電気及通信工学専攻修了．同年日立電線（株）入社．現在，同社オプトロシステム研究所第 2 部に所属．LAN 製品の研究開発に従事．電子情報通信学会会員．

平岡 大樹

1997 年筑波大学第三学群情報学類卒業．同年日立電線（株）入社．現在，同社高砂工場 LAN 機器開発グループに所属．LAN 製品の研究開発に従事．

松尾 英普

1984 年北海道大学工学部電子工学科卒業．同年日立電線（株）入社．同社高砂工場情報ネットワーク部に所属．現在，Hitachi Cable America San Jose 事務所に駐在．LAN 製品の研究開発に従事．

泉　　正夫（正会員）

1983 年大阪府立大学工学部電気工学科卒業．1985 年同大学大学院工学研究科博士前期課程修了．同年シャープ（株）入社．1990 年大阪府立大学工学部助手．現在，同大学大学院工学研究科電気・情報系専攻助教授．博士（工学）．画像認識・理解に関する研究に従事．電子情報通信学会，システム制御情報学会，IEEE 各会員．

福永　邦雄（正会員）

1967 年大阪府立大学工学部電気工学科卒業．1969 年同大学大学院工学研究科修士課程修了．同年同大学工学部電気工学科助手．現在，同大学大学院工学研究科電気・情報系専攻教授．工学博士．コンピュータビジョン，グラフ理論とその応用等の研究に従事．電子情報通信学会，電気学会，システム制御情報学会，IEEE 各会員．