社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2007－ＤＳＭ－45（２）
2007／5／10

複数VLANアクセスによるユーザ指向ネットワークシステムの検討

小澤 洋司† 沖田 英樹†

† 株式会社 日立製作所 中央研究所 〒185-8601 東京都国分寺市東恋ヶ窪 1-280
E-mail: †{yoji.ozawa.zp,hideki.okita.pf}@hitachi.com

あらまし 企業で利用されているテレビ会議や電話等，多くの業務サービスがIPネットワークへ統合されてきている．これらの業務用のサービスをユーザが快適に利用するためには，ネットワークがサービス品質を管理し，ユーザに応じてサービスを提供する，ユーザ指向ネットワークシステムが必要である．本研究では，VLANによるサービス毎の専用ネットワークと，ユーザのサービスへのアクセスを制御する複数VLANアクセス方式を提案した．複数VLANアクセス方式は，1台のユーザ端末への異なるMACアドレスの仮想インターフェースの配備により，複数サービスへのアクセスを可能とし，管理サーバのサービス・ユーザ対応関係の管理により，運用を容易化する．さらに，提案方式について実用性を検証するために，仮想インターフェースを実現するネットワークデバイスドライバを開発し，1台のユーザ端末から複数VLANへアクセスできることを確認した．
キーワード ネットワーク運用管理，自律運用，VLAN，MAC-VLAN，仮想ネットワークインターフェース，ネットワークデバイスドライバ

User-Oriented Network System using Multi-VLAN Access Method

Yoji OZAWA† and Hideki OKITA†

† Hitachi, Ltd.,Central Reseach Laboratory Higashi-koigakubo 1-280, Kokubunji-shi, Tokyo, 185-8601 Japan
E-mail: †{yoji.ozawa.zp,hideki.okita.pf}@hitachi.com

Abstract Many enterpises promote to integrate various services into IP network. Those services are TV conference, telephony, and so on. The network system is needed for users to utilize those services properly. We call this network system "User-Oriented Network System". User-Oriented Network System manages service quality and provides services corresponding to each user's property. We propose VLAN based dedicated network and Multi-VLAN access method to control service access from users. We equip an user terminal with multiple virtual interfaces. And each virtual interface has unique MAC address. In this way we realize multiple service access. The management server manages service - user mapping table, which realizes easy management. Forthermore to examine the feasibility of the proposed method we develop the network device driver which realizes the virtual interface and find multiple VLAN access is realized.
Key words Network management, Autonomous Operation, VLAN, MAC-VLAN, Virtual network interface, Network device driver

1. まえがき

1.1 研究の背景

近年，企業においてテレビ会議やIP電話，E-mailなど，業務を行うための様々なサービスがIPネットワークに統合されてきている．さらに，ユーザ毎に提供するサービスの種類を変えたり，同じサービスであっても，ユーザに応じて異なる通信品質のサービスとして提供する必要がある[1]～[3]．例えば，図1に示すように同じテレビ会議であっても，会社役員向けの役員会議用テレビ会議や一般社員向けのチームミーティング用テレビ会議が存在する．

このようにネットワークを介し，様々なサービスをユーザに応じて提供する時に，現在の企業ネットワークには，次のような問題がある．

- ネットワークにおけるサービス間のトラフィックの干渉：現在のネットワークは，サービス毎のトラフィックを区別できないため，サービス間で干渉が起こり，リアルタイム性が必要なテレビ会議などのサービスの通信品質が劣化する．

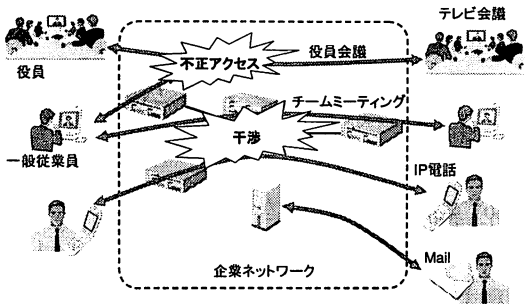

図 1　企業におけるサービスのネットワークへの統合
Fig. 1　Service integration for network in enterprises.

- サービスへの不正アクセス：全サービスが同一のネットワーク上で提供されているため，アクセス権限のないユーザが本来許可されていないサービスにアクセスし，そのサービスでやりとりされる情報を取得する可能性がある．例えば，役員会議用テレビ会議とチームミーティング用テレビ会議が提供されている時，一般社員が役員会議の情報を盗聴する．

したがって，ユーザに応じたサービスを提供するために，ネットワークはこれらの問題を解決する必要がある．

1.2　研究の目的

本研究の目的は，上記の問題を解決し，ユーザに応じたサービスを提供するネットワークシステムを開発することである．このようなユーザに応じたサービスを提供するネットワークシステムを以下「ユーザ指向ネットワークシステム」と呼ぶ．

上記の問題を解決するために，ユーザ指向ネットワークシステムは，次のような特徴を持つ．また，その特徴を図 2 に示す．

- サービス毎の専用ネットワーク：ネットワークを分割し，サービス毎の専用ネットワークを構築する．その専用ネットワーク上で，1 つのサービスを提供することで，サービス間の干渉を防止する．
- ユーザ毎のサービスへのアクセス制御：ユーザ毎に，サービス毎の専用ネットワークへのアクセスを制御することで，ユーザに応じたサービスを提供し，アクセス権限のないユーザのアクセスを防止する．

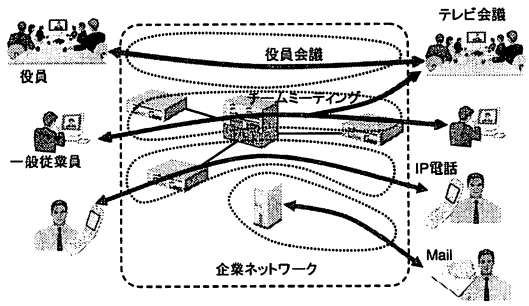

図 2　ユーザ指向ネットワークシステム
Fig. 2　User-Oriented Network System.

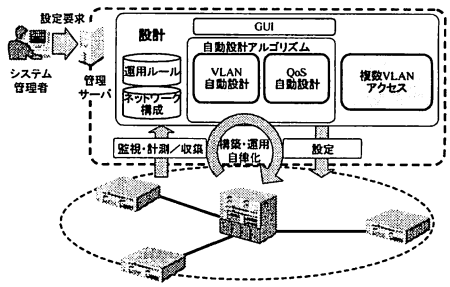

図 3　ネットワーク自律運用フレームワーク
Fig. 3　Framework for network autonomous operation.

1.3　ネットワーク自律運用フレームワーク

我々は，ネットワーク自律運用技術の研究を進めてきた．我々は，まず図 3 に示すネットワーク自律運用技術のフレームワーク [4] を提案した．このフレームワークは，管理対象ネットワークを監視・計測し，情報を収集する機能，運用ルール，ネットワーク構成を元に VLAN，QoS 保証設定などを自動的に設計する機能 [5]，設計した内容をネットワーク装置に反映する設定機能から構成される．そして，それぞれを連動して自動的に動作させることで，ネットワークの自律的な管理，および制御を実現する．

ユーザ指向ネットワークシステムの実現に必要なサービス毎の専用ネットワーク，サービスへのアクセス制御のためには，ネットワークの管理，および制御が必要である．そこで，このネットワーク自律運用フレームワークをベースにして，ユーザ指向ネットワークシステムを実現する．

本研究では，サービス毎の専用ネットワークを実現するために，VLAN を利用する．そして，サービスを提供する VLAN へのアクセスを制御するための「複数 VLAN アクセス」方式を提案する．本報告では，「複数 VLAN アクセス」方式について，主に述べる．

2.　VLAN によるユーザ指向ネットワークシステム

本研究では，ユーザ指向ネットワークシステムを実現するために VLAN を利用する．本章では，まず VLAN を用いた，サービス毎の専用ネットワークの実現方法について述べ，次に，サービス専用ネットワークへのアクセス制御方法について述べる．

2.1　VLAN によるサービス毎の専用ネットワーク

VLAN は，仮想的な LAN であり，1 つの物理ネットワーク上に互いが独立した複数の仮想的な LAN を構築できる [6]〜[8]．本研究では図 4 に示すように，物理ネットワーク上にサービス毎に VLAN を作成し，その VLAN にサービスを対応付けることで，サービス毎の専用ネットワークを実現する．図 4 では，2 つの VLAN を作成し，それぞれの VLAN で，役員会議用テレビ会議とチームミーティング用テレビ会議を提供する場合を示す．

また，VLAN を利用することで，複数のサービスを統一され

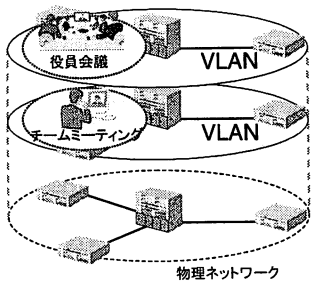

図 4　VLAN によるサービス毎の専用ネットワーク
Fig. 4　Service dedicated network with VLAN.

た識別子（VLAN ID）で制御できるため，複数のサービスの通信品質の管理が容易である．

2.2　サービスへのアクセス制御

ユーザ指向ネットワークシステムは，ユーザからのサービスを提供する VLAN へのアクセスを制御する必要がある．具体的には，図 5 に示すように，ユーザ端末を収容するネットワーク端のエッジスイッチが，ユーザ端末からのパケットを適切な VLAN に転送する必要がある．この際，企業内の様々な業務に実際に適用するためには，ユーザ指向ネットワークシステムが，以下の要求条件を満たす必要がある．

- 1 台のユーザ端末から複数のサービスへの同時アクセスを実現する
- アクセス制御のためのネットワーク管理を容易化する

既存の VLAN 転送方式には，以下の 2 方式がある．

- Tag 方式
- MAC 方式

本報告では，既存の転送方式の特徴を検討し，ユーザからのサービスへのアクセスを制御する　複数 **VLAN** アクセス方式を提案する．

3.　複数 VLAN アクセス方式

3.1　既存方式の検討

本節では，既存の VLAN 転送方式である Tag 方式と MAC 方式について述べる．

3.1.1　既存方式の概要

(1) Tag 方式

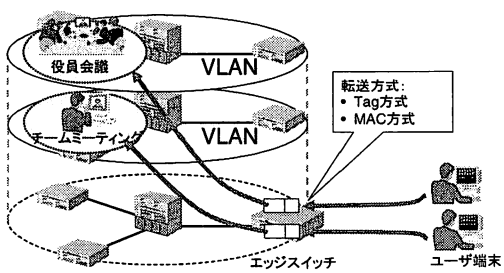

図 5　VLAN へのパケット転送
Fig. 5　Packet forwarding for VLAN.

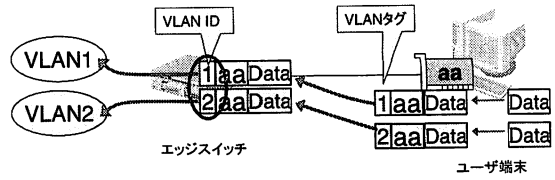

図 6　Tag 方式
Fig. 6　Tag method.

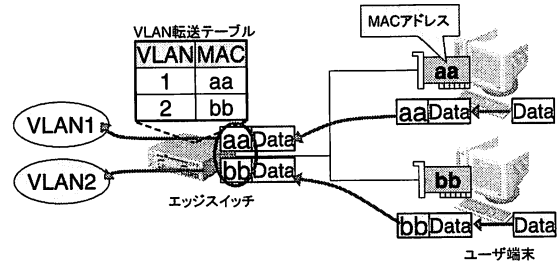

図 7　MAC 方式
Fig. 7　MAC method.

図 6 に Tag 方式を示す．Tag 方式では，ユーザ端末がパケットを送信する時に，VLAN タグを付加する．この VLAN タグには VLAN の識別子である VLAN ID が含まれる．エッジスイッチは，VLAN ID により，該当する VLAN へパケットを転送する．

(2) MAC 方式

図 7 に MAC 方式を示す．MAC 方式では，パケットに付加された送信元のユーザ端末の MAC アドレスを利用する．MAC アドレスは，ユーザ端末のネットワークインターフェース（以下，IF）固有の値である．エッジスイッチは，MAC アドレスとその転送先の VLAN を対応付ける VLAN 転送テーブルを保持しており，パケットを受信すると，この VLAN 転送テーブルに従い，パケットを VLAN に転送する．

3.1.2　既存方式の比較

管理上の観点から Tag 方式と MAC 方式を比較する．サービスへのアクセスを制御するためには，ユーザからサービスの制御情報である VLAN ID を隠蔽する必要がある．

図 8 に Tag 方式と MAC 方式で用いるサービスの識別子を示す．Tag 方式は，サービスの識別子として，ネットワークからユーザ端末まで，VLAN ID を利用している．そのため，制御情報である VLAN ID がユーザから隠蔽されていない．よって，Tag 方式は，サービスのアクセス制御には適さない．

一方，MAC 方式は，サービスの識別子として，ネットワーク内では VLAN ID を，エッジスイッチからユーザ端末では，MAC アドレスを利用する．そのため，制御情報である VLAN ID はユーザから隠蔽されている．したがって，本研究では MAC 方式を用いたサービスアクセス制御方式を提案する．

3.2　**MAC** 方式の課題

本節では，MAC 方式を用いたサービスへのアクセス制御における要求条件「複数サービス同時アクセス」と「管理の容易

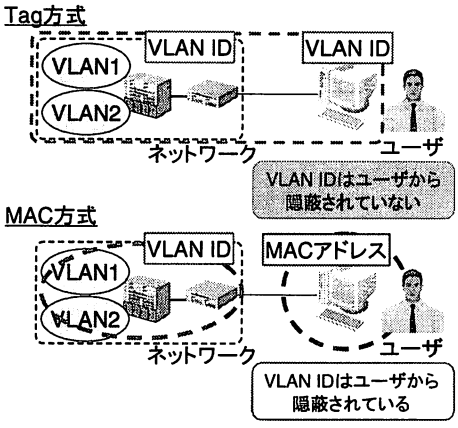

図 8 Tag 方式と MAC 方式の比較
Fig. 8 Comparison between Tag method and MAC method.

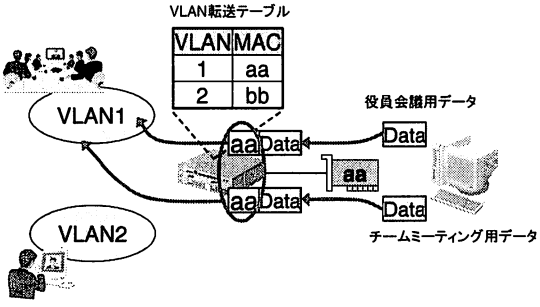

図 9 MAC 方式の課題（複数サービス同時アクセス）
Fig. 9 Issue of MAC method (Multiple service access).

化」の 2 つの項目について検討する．

3.2.1 複数サービス同時アクセス

複数サービスへの同時アクセスの例として，会社役員がテレビ会議による役員会議とチームミーティングの両方に参加したい時，1 台のユーザ端末から複数のサービスに同時にアクセスする場合が考えられる．

しかし，図 9 に示すように，1 台のユーザ端末から送信されるパケットの送信元 MAC アドレスは同一であるため，あるユーザ端末からの全てのパケットは 1 つの VLAN に転送される．したがって，MAC 方式には，1 台のユーザ端末から複数のサービスに同時にアクセスすることが出来ないという課題がある．

3.2.2 管理の容易化

MAC 方式では，エッジスイッチがユーザ端末の MAC アドレスとその MAC アドレスのパケットの転送先 VLAN を対応付ける VLAN 転送テーブルを保持する必要がある．そして，エッジスイッチ毎に収容しているユーザ端末が異なるため，VLAN 転送テーブルの内容も異なる．例えば，図 10 に示すように，エッジスイッチ 1 とエッジスイッチ 2 では，VLAN 転送テーブルの内容が異なる．管理者は，多数のエッジスイッチの VLAN 転送テーブルを管理する必要があり，この管理コストが大きくなるという課題がある．

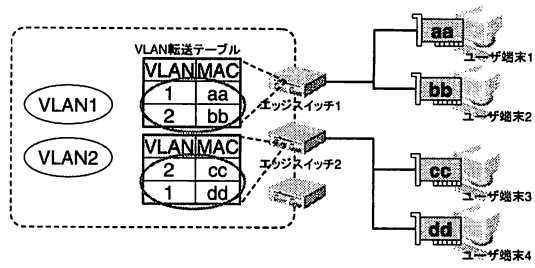

図 10 MAC 方式の課題（管理の容易化）
Fig. 10 Issue of MAC method (Easy management).

3.3 複数 VLAN アクセス方式の提案

以上の既存の転送方式の課題を解決するために，以下の 2 つの機能からなる「複数 VLAN アクセス方式」を提案する．

- 仮想 IF 機能
- マッピング管理機能

以下，「仮想 IF 機能」と「マッピング管理機能」の詳細について述べる．

3.3.1 仮想 IF 機能の提案

本研究では，以下のようにして，MAC 方式の複数サービスに同時にアクセス出来ないという課題を解決する．図 11 に，提案方式を示す．

複数サービスにアクセスするためには，1 台のユーザ端末が複数の MAC アドレスを保持する必要がある．しかし，基本的に 1 台のユーザ端末は，1 つの MAC アドレスのみを持つ．そこで，複数サービスへのアクセスを可能にするために仮想 IF を導入する．そして，複数の異なる MAC アドレスを持つ仮想 IF を 1 台のユーザ端末に割り当てる．

さらに，MAC アドレスの重複を避けるために，管理サーバを設置し，MAC アドレスの管理を行う．この管理サーバは，仮想 IF 用の MAC アドレスとその MAC アドレスを割り当てるユーザ端末の対応テーブル（MAC アドレステーブル）を保持し，仮想 IF 毎に固有の MAC アドレスを割り当てる．

以上により，1 台のユーザ端末は複数の仮想 IF を利用してパケットを送信することで，異なる送信元 MAC アドレスのパ

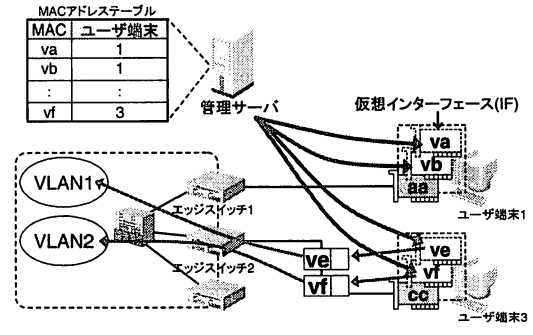

図 11 仮 想 IF
Fig. 11 Virtual interface.

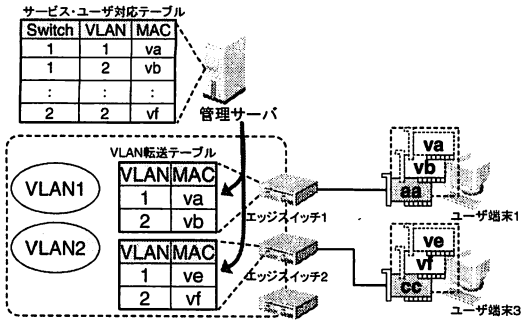

図 12 マッピング管理

Fig. 12 Mapping management.

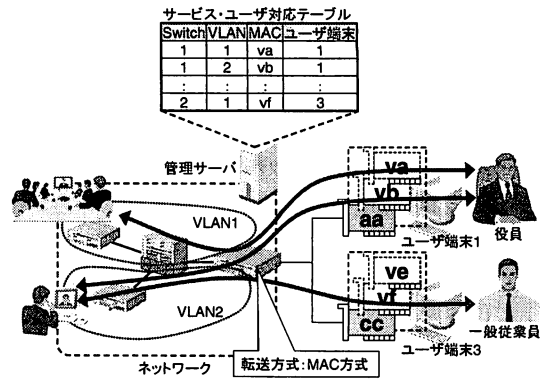

図 13 提案システムの構成

Fig. 13 Proposed system architecture.

ケットを送信することが出来，複数のサービスにアクセスすることが可能となる．

3.3.2 マッピング管理機能の提案

次に，MAC 方式の管理コストが大きいという課題を以下のようにして解決する．図 12 に，提案機能を示す．

提案機能では，管理サーバに，サービス・ユーザ対応テーブルを保持させる．この対応テーブルは，MAC アドレスと転送先の VLAN，そしてそのエントリがどのエッジスイッチのエントリかの情報を含む．

このように管理サーバが，各エッジスイッチの VLAN 転送テーブルのエントリを管理することで，管理サーバはこのサービス・ユーザ対応テーブルに従い，全エッジスイッチの VLAN 転送テーブルに，エントリを登録することができる．管理サーバがこれらの処理を自動的に行うことにより，MAC 方式の課題であった管理コストを削減し，管理の容易化を実現できる．

4. 提案システム

サービス毎の専用ネットワークのための VLAN と，アクセス制御のための複数 VLAN アクセス方式を用いた，ユーザ指向ネットワークシステムを実現する提案システムについて述べる．

4.1 提案システムの構成

図 13 に提案システムの構成を示す．

まず，ネットワークではサービス毎の VLAN を作成し，サービス毎の専用ネットワークを実現する．そして，提案した複数 VLAN アクセス方式により，ユーザからのサービスを提供する専用ネットワークへのアクセスを制御する．ユーザ端末に複数の仮想 IF を持たせることで，1 台のユーザ端末から複数の VLAN へのアクセスを可能にする．また，管理サーバがサービス・ユーザ対応テーブルを保持する．このサービス・ユーザ対応テーブルには，仮想 IF 用の MAC アドレスとその MAC アドレスを割り当てるユーザ端末，そしてその MAC アドレスのパケットの転送先 VLAN ID，さらに，MAC アドレスと転送先 VLAN ID のエントリがどのエッジスイッチのエントリかの情報を含む．管理サーバは，このサービス・ユーザ対応テーブルに従い，エッジスイッチの VLAN 転送テーブルに MAC アドレスと転送先の VLAN のエントリを登録し，さらに，ユーザ端末の仮想 IF に MAC アドレスを登録する．

これにより，ユーザ毎に適切にサービスを提供することができる．図 13 では，役員は，役員会議とチームミーティングにアクセスすることができるが，一般従業員は，チームミーティングにのみアクセス可能となる．提案システムにより，ユーザ指向ネットワークシステムを実現することができる．

5. 仮想 IF 用デバイスドライバの開発

提案方式を実現するために，仮想 IF 用ネットワークデバイスドライバを開発した．そして，1 台の PC から複数の VLAN にアクセスできることを確認した．

以下の特徴を持つ Linux デバイスドライバを開発した．また，表 1 に開発したデバイスドライバの動作環境を示す．

- 1 つの NIC を複数の IF で共有可能．これにより，仮想 IF を実現する．
- IF 毎に MAC アドレスを設定可能．

表 1 デバイスドライバ動作環境

Table 1 Operating environment for the device driver.

対象 NIC	Intel 82557/8/9 [Ethernet Pro 100]
OS	Linux 2.4.27
CPU	Intel Pentium 4 3.2GHz

開発したデバイスドライバをユーザ端末に組込み，図 14 に示すシステムを構築した．このシステムの構成は，以下である．2 つの VLAN（VLAN1，VLAN2）があり，各々の IP アドレス空間は，192.168.10.0/24，192.168.20.0/24 である．ユーザ端末には，開発したデバイスドライバを用いて，2 つの仮想 IF（eth1，eth2）を配備し，異なる MAC アドレスを設定する．なお，本報告では手動で MAC アドレスを設定した．そして，各仮想 IF に VLAN1，VLAN2 内の IP アドレスを割り当てる．エッジスイッチの，ユーザ端末を収容する Port3 を，MAC 方式によりパケットを VLAN に振り分けるポートに設定する．具体的には，eth1 の MAC アドレスが送信元のパケットは VLAN1 に，eth2 の MAC アドレスのパケットは VLAN2 に転送する．

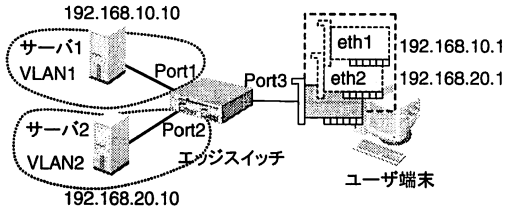

図 14 プロトタイプシステム構成
Fig. 14 Prototype system architecture.

ユーザ端末から，仮想 IF eth1，eth2 を用いてパケットを転送し，VLAN1，20 に所属するサーバ 1，2 への IP 到達性を確認した．これにより，開発したデバイスドライバにより，1 台のユーザ端末から複数の VLAN へのアクセスが可能になることを確認できた．

6. おわりに

6.1 結　論

企業において，業務を行うためのサービスが IP ネットワークに統合されてきている．このため，ユーザに応じてサービスを提供するユーザ指向ネットワークシステムが必要とされている．この背景を受け，これまで開発を進めてきたネットワーク自律運用フレームワークに基づき，ユーザ指向ネットワークシステムを実現するネットワークシステム「ユーザ指向ネットワークシステム」を提案した．

ユーザ指向ネットワークシステムを実現するために，VLAN を用いて，サービス毎の専用ネットワークを構築し，以下の特徴を持つユーザからのサービスへのアクセス制御方式「複数 VLAN アクセス方式」を提案した．

- エッジスイッチでの VLAN 転送に MAC 方式を用い，MAC アドレスにより，ユーザとサービスを対応付ける．
- 仮想 IF により，1 台のユーザ端末が複数の MAC アドレスの保持を可能にすることで，複数サービスへのアクセスを可能にする．
- 管理サーバがサービス・ユーザ対応テーブルの管理を行い，エッジスイッチの VLAN 転送テーブルと，ユーザ端末上の仮想 IF に設定することで，容易な管理を実現する．

そして，この複数 VLAN アクセス方式と，VLAN によるサービス毎の専用ネットワークにより，ユーザ指向ネットワークシステムを実現するネットワークシステムを提案した．

さらに，仮想 IF 用デバイスドライバを開発した．このデバイスドライバにより，1 台のユーザ端末から複数の VLAN へアクセスできることを確認した．

6.2 今後の課題

今後，管理サーバ等を実装し，今回開発したデバイスドライバと併せ，複数 VLAN アクセス方式，及び提案システムの実装・評価を行う．また，提案システムの実現のために，既存技術との連携を検討する．

文　献

[1] Wei-Hua Wang, Marimuthu Palaniswami, Steven H. Low, "Application-Oriented Flow Control: Fundamentals, Algorithms and Fairness", *IEEE Trans. Networking*, Vol.14, No.6, pp.1282-1291, Dec. 2006.

[2] Scott Shenker, "Fundamental Design Issues for the Future Internet", *IEEE J. Sel. Areas Commun.*, Vol.13, No.7, pp.1176-1188, Sep. 1995.

[3] T.Eilam, M.H.Kalantar, A.V.Konstantinou, G.Pacifici, " Reducing the complexity of application deployment in large data centers", *Integrated Network Management, 2005. (IM 2005.)*, pp.221- 234, May 2005.

[4] 沖田英樹，小澤洋司，住吉貴志 IP ネットワーク自律運用技術の研究 ネットワーク自律運用フレームワークの提案，信学会 2006 年総合大会，Mar, 2006.

[5] 小澤洋司，沖田英樹，住吉貴志，IP ネットワーク自律運用技術の研究 QoS 保証自動設定システムの提案 信学会 2006 年総合大会，Mar, 2006.

[6] V. Rajaravivarma, "Virtual local area network technology and applications", *29th Southeastern Symposium on System Theory (SSST '97)*, pp.49-52, 1997.

[7] Xiaoying Wang, Hai Zhao, Mo Guan, Chengguang Guo, Jiyong Wang, "Research and Implementation of VLAN Based on Service", *IEEE GLOBECOM '03*, Vol.5, pp.2932-2936, Dec. 2003.

[8] Minli Zhu, Mart Molle, Bala Brahmam, "Design and Implementation of Application-Based Secure VLAN", *29th Annual IEEE International Conference on Local Computer Networks (LCN'04)*, pp. 407-408, 2004.