社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

利用者の多重帰属を実現する VPN のプロトタイプ実装

本田　治† 原　義博†† 大崎　博之††† 今瀬　真††† 丸吉　政博†††† 松田　和浩††††

† 大阪大学 大学院基礎工学研究科　〒 565-0871 大阪府吹田市山田丘 1-5
†† 大日本印刷株式会社　〒 162–0062 東京都新宿区市谷加賀町 1–1–1
††† 大阪大学 大学院情報科学研究科　〒 565-0871 大阪府吹田市山田丘 1-5
†††† 日本電信電話株式会社 NTT 情報流通プラットフォーム研究所
〒 180-8585 東京都武蔵野市緑町 3-9-11
E-mail: †o-honda@ics.es.osaka-u.ac.jp, ††y-hara@dev.cio.dnp.co.jp, †††{oosaki,imase}@ist.osaka-u.ac.jp,
††††{maruyoshi.masahiro,matsuda.kazuhiro}@lab.ntt.co.jp

あらまし　我々はこれまで、利用者が、複数の VPN に対して同時に接続（多重帰属）できる、新しい VPN アーキテクチャの提案を行った。本稿では、我々は利用者が複数の VPN に多重帰属できる VPN アーキテクチャの実現可能性を示し、多重帰属サービスのサービス像を明確にするために、既存のネットワーク技術を組み合わせたプロトタイプ実装を行う。このプロトタイプでは、端末が、VLAN で実現した 複数の VPN に対して多重帰属可能である。
キーワード　VPN、プロトタイプ実装、VLAN, 多重帰属、アクセス制御

A Prototype Implementation of VPN Enabling User-Based Multiple Association

Osamu HONDA†, Yoshihiro HARA††, Hiroyuki OHSAKI†††, Makoto IMASE†††, Masahiro MARUYOSHI††††, and Kazuhiro MATSUDA††††

† Gradauate School of Engineering Science, Osaka University,
Yamadaoka 1-5, Suita, Osaka 565-0871, Japan
†† Dai Nippon Printing Co.,Ltd.
1–1, Ichigaya Kagacho 1-chome, Shinjuku-ku, Tokyo 162-8001, Japan
††† Graduate School of Infomation Science and Technology, Osaka University,
Yamadaoka 1-5, Suita, Osaka 565-0871, Japan
†††† NTT Information Sharing Platform Laboratories, NTT Corporation,
3-9-11 Midori-cho, Musashino, Tokyo 180-8585, Japan
E-mail: †o-honda@ics.es.osaka-u.ac.jp, ††y-hara@dev.cio.dnp.co.jp, †††{oosaki,imase}@ist.osaka-u.ac.jp,
††††{maruyoshi.masahiro,matsuda.kazuhiro}@lab.ntt.co.jp

Abstract　In our previous work, we have proposed a new VPN architecture for enabling user-based multiply associated VPNs. In this paper, we implement a prototype system of a VPN enabling users to be associated with multiple VPNs using existing network technologies to show feasibility of our architecture and to clarify service image of a multiple association service. Our prototype system enables hosts to be simultaneously associated with multiple VPNs, each of which is constructed using a VLAN technology.
Key words　VPN, prototype, VLAN, multiple association, access control

1. はじめに

近年のネットワーク技術の発展に伴い、WEB サービスの発展 [1] による購買や流通のネットワーク化、行政機能のネットワーク化 [2]、テレワークや SOHO など労働のネットワーク化 [3] が進行している。これにより、様々な社会活動が地理的な要因から開放され、社会構造の広域分散化が進行すると考えられる。このような社会構造では、近い将来、ネットワーク上に仮想組織が形成されると考えられる。我々は、これら仮想組織群をサイバーソサエティと称している。サイバーソサエティにおける「人」は、セキュリティを維持しながら、複数の仮想組織と通信可能な関係を確立 (多重帰属) する必要がある。我々

は、仮想組織を VPN (Virtual Private Network）を用いて実現することを想定している。

既存の VPN 技術としては、PPVPN（Provider Provisioned VPN) [4]〜[6] やエクストラネット [7], [8] などがある。しかし、これらでは、利用者が、利用者単位で多数の VPN に同時に多重帰属することができない。

そこで、我々は、仮想組織への多重帰属をネットワークサービスとして実現するために、利用者が多数の VPN に対して多重帰属できる新しい VPN 技術の検討を行っている [9], [10]。我々は、このような新しい VPN を、MAVPN（Multiply-Asocciated VPN）と呼んでいる。

本稿では、我々の提案する MAVPN の実現可能性を示し、多重帰属のサービス像を明確にするために、既存のネットワーク技術を用いてプロトタイプ実装を行う。

2 章 では、実装を行うにあたって、目標とする MAVPN のサービス像について説明する。3 章では、本プロトタイプの基本的な方針を説明する。4 章では本プロトタイプの各要素の設計について説明する。5 章では具体的な実装方法を説明し、動作を確認する。6 章でまとめと今後の課題について述べる。

2. MAVPN のサービス像

利用者の視点から見た MAVPN のサービス像を述べる。利用者が MAVPN を利用する手順は以下のようなものになる。

（1） 利用者は端末を手元のネットワーク機器に接続する。

（2） 利用者は端末上で MAVPN 端末ソフトウェアを起動する。

（3） 利用者は、端末ソフトウェアに表示される、帰属が許可されている VPN の名前リストから、接続する VPN を複数選択する (もしくは端末ソフトウェアを起動すると、あらかじめ定めておいた複数の VPN に自動的に接続される)。

（4） 利用者やアプリケーションは、通信相手の端末名を指定して通信を行う。

（5） 利用者は、端末ソフトウェアから、切断する VPN を選択して切断する (もしくは端末ソフトウェアを終了すると全ての VPN から切断される)。

このように、利用者は、端末をネットワークに接続し、端末ソフトウェアを起動して利用者 ID とパスワードを入力するだけで複数の VPN に接続されることが望ましい。また、端末ソフトウェアに表示される VPN のリストから、接続や切断を行う VPN を随時指定できることが望ましい。

3. 実装の方針

2. のようなサービスを実現することを目標として、実装を行う。今回は、2. で述べたサービス要求のうちの一部を実現することを目的としている。具体的には、以下の要求を満たすものを構築する。

- 利用者は、複数の VPN を意識せず通信を行える
- VPN を論理的な名前で指定できる
- 利用者端末のアドレスが自動的に設定される
- 利用者単位で VPN へのアクセス制御が可能である

その他の要求を満たす実装については、今後の課題である。

本プロトタイプでは、既存の標準的な技術のうち、容易に利用できるものを用いて実装を行う。我々は、[10] において、既存の技術を用いて MAVPN を実装する場合、基盤となるネットワークをレイヤ 2 技術で実現し、その上に VPN をレイヤ 2 技術で実現し、利用者の複数 VPN へのアクセスをレイヤ 3 技術を用いて制御するというアーキテクチャが最も優れていると判断した。本稿では、このアーキテクチャに基づいて実装を行う。具体的には、基盤となるネットワークを Ethernet で、VPN を IEEE 802.1Q VLAN で、利用者の VPN へのアクセスを IP を利用して制御する。

本プロトタイプは、認証 VLAN [11] と呼ばれる既存技術を参考に実装を行う。認証 VLAN は既存の VLAN に認証機能を追加し、利用者単位のアクセス制御を実現するものである。本プロトタイプは、利用者が複数の VLAN を同時に利用できる認証 VLAN を目標とする。また、認証 VLAN と同程度のセキュリティ水準を実現することを目標とする。具体的には、同一のサイト (LAN) に接続されている端末同士は信頼し合うという前提を置く。このため、同一サイト内の端末による盗聴は想定外とする。また、MAC アドレス詐称も想定外とする。

4. プロトタイプの設計

4.1 ネットワーク構成

まず、プロトタイプのネットワーク構成について説明する。プロトタイプの論理的なネットワークは図 1 のように構成する。

利用者に提供する VPN (図 1 の User VPN) は IEEE 802.1Q VLAN [12] で実現する。IEEE 802.1Q は、Ethernet フレームに 12 ビットの VLAN ID を含むタグを付加することで Ethernet を仮想的に分割する技術である。本プロトタイプでは、実装を簡単にするために、各 VLAN はそれぞれひとつの IP サブネットを構成するものとし、各 IP アドレス空間は重複しないものとする。

端末は MAVPN ゲートウェイ (図 1 の MAVPN Gateway) という機器を介して VLAN に接続する。端末から MAVPN ゲートウェイ間へのアクセス回線を IEEE 802.1Q で多重化し、MAVPN ゲートウェイがこのアクセス回線を IEEE 802.1Q VLAN による VPN へブリッジする。これにより端末は複数のレイヤ 2 VPN を利用できる。また、MAVPN ゲートウェイは利用者の認証機能を持ち、VPN への帰属を許可された利用者の端末からのアクセス回線のみを VPN に接続する。端末がどの VPN にも帰属していない初期状態では、サイト (図 1 の Site) 内でのみ通信可能とする。このため、サイトを初期 VPN (図 1 の Default VPN) と呼ぶ。

利用者の端末が用いる IP アドレスは、各 VLAN 内に設置された DHCP サーバにより、VLAN の IP アドレス空間から割り当てられる。ただし、サーバなどの IP アドレスは、各 VLAN の IP アドレス空間から静的に割り当てる。

利用者の認証に用いる利用者のアカウント情報は、RADIUS サーバ (図 1 の RADIUS Server) によって全ての MAVPN ゲートウェイに提供される。RADIUS サーバは管理用の特別な VPN (図 1 の Management VPN) に設置される。また、RADIUS サーバに保存されるアカウント情報は、利用者の ID、帰属が許可されている VPN の名前、パスワードの 3 つからなる。すなわち、利用者は、帰属が許可された VPN の数だけアカウントを持つ。

4.2 通信の方式

次に、本プロトタイプにおける通信の方式について説明する。端末は、最初にサイトに接続された時に、初期 VPN 用のインタフェースを作成し、サイト内の DHCP サーバから初期 VPN 用の IP アドレスを取得する。

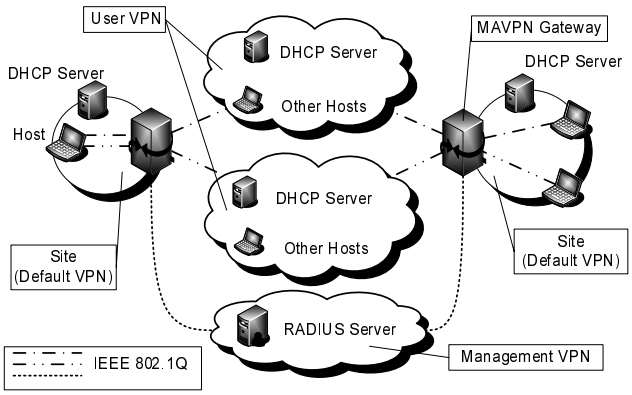

図 1　プロトタイプの論理的ネットワーク構成

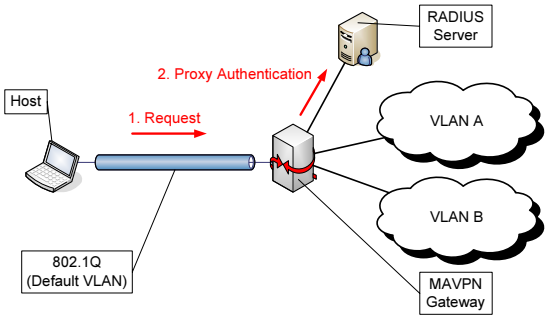

図 2　利用者の VPN への帰属手順 1

4.2.1　帰 属 処 理

利用者が VPN に帰属する場合、以下の手順 (図 2 および図 3 参照) で処理が行われる。

（1） 端末 (図 2 の Host) 上の利用者は、初期 VPN を用いて、MAVPN ゲートウェイ (図 2 の MAVPN Gateway) に対して利用者 ID と帰属したい VPN の名前 (「会社の VPN」というような論理的な名前)、パスワードを入力する。(図 2 の 1. Request)

（2） MAVPN ゲートウェイは、利用者 ID、VPN 名、パスワードを RADIUS サーバ (図 2 の RADIUS Server) に問い合わせる。(図 2 の 2. Proxy Authentication)

（3） RADIUS サーバから応答を受け取り、利用者が VPN の利用を許可されているか確認する。(図 3 の 3. Authentication Reply)

（4） MAVPN ゲートウェイは、利用者の VPN 利用許可が確認されたら、端末からのフレームを VPN にブリッジするように、フィルタリング規則を変更する。このとき、VPN の名前を、実際の通信で利用する IEEE 802.1Q における VLAN ID に変換して利用する。 (図 3 の 4. Change Configuration)

（5） 端末に対し、VPN への帰属が許可されたことを通知する。(図 3 の 5. Reply)

（6） 端末は帰属する VPN のための IEEE 802.1Q インタフェースを作成し、VPN 内の DHCP サーバから IP アドレスを取得する。(図 3 の 6. Create Interface)

このような手順で通信が行われるように、MAVPN ゲートウェイおよび端末を実装する。

4.2.2　離 脱 処 理

また、利用者が VPN から離脱する場合、以下の手順 (図 4 および図 5 参照) で処理が行われる。

（1） 利用者は初期 VPN を用いて、MAVPN ゲートウェイ

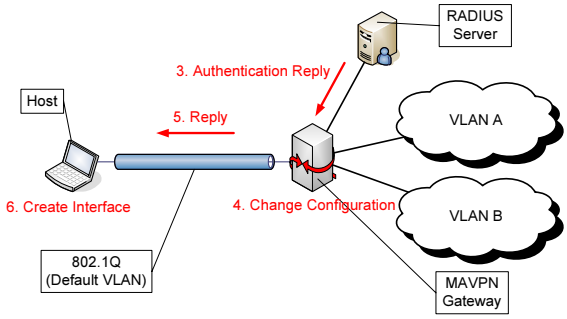

図 3　利用者の VPN への帰属手順 2

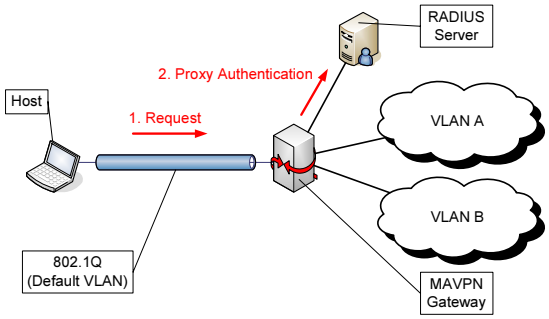

図 4　利用者の VPN からの離脱手順 1

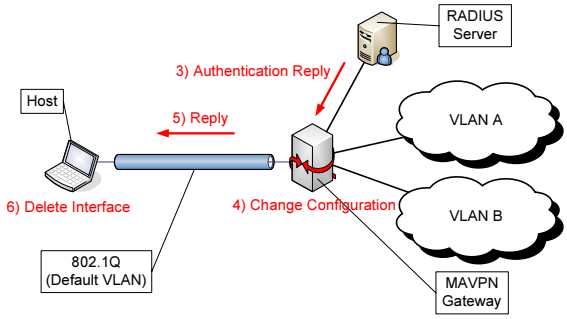

図 5　利用者の VPN からの離脱手順 2

に対して利用者 ID と離脱する VPN の名前、パスワードを入力する。(図 4 の 1. Request)

（2） MAVPN ゲートウェイは、利用者 ID、VPN 名、パスワードを RADIUS サーバに問い合わせる。(図 4 の 2. Proxy Authentication)

（3） RADIUS サーバから応答を受け取り、利用者が VPN の利用を許可されているか確認する。(図 3 の 3. Authentication Reply)

（4） MAVPN ゲートウェイは、利用者の VPN 利用許可が確認されたら、端末からのフレームを VPN にブリッジするようなフィルタリング規則を削除する。このとき、VPN の名前を、実際の通信で利用する IEEE 802.1Q における VLAN ID に変換して利用する。 (図 3 の 4. Change Configuration)

（5） 端末に対し、VPN から離脱したことを通知する。(図 5 の 5. Reply)

（6） 端末は、離脱した VP のための IEEE 802.1Q インタフェースを削除する。(図 5 の 6. Delete Interface)

4.3　端末の設計

端末の設計について説明する。端末は VLAN に帰属するために、MAVPN ゲートウェイに対して帰属の認証要求を行わなければならない。このため、認証要求を行う端末ソフトウェア

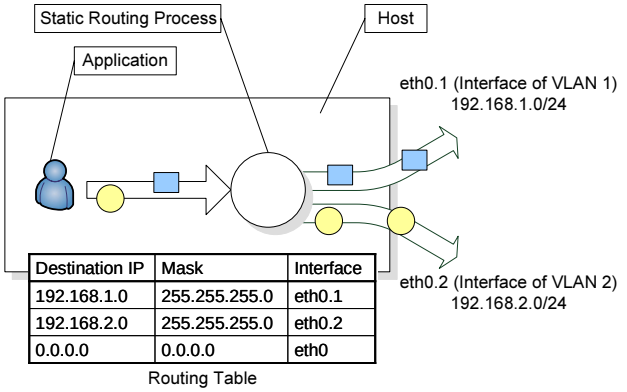

図 6　端末における VLAN インタフェースの選択

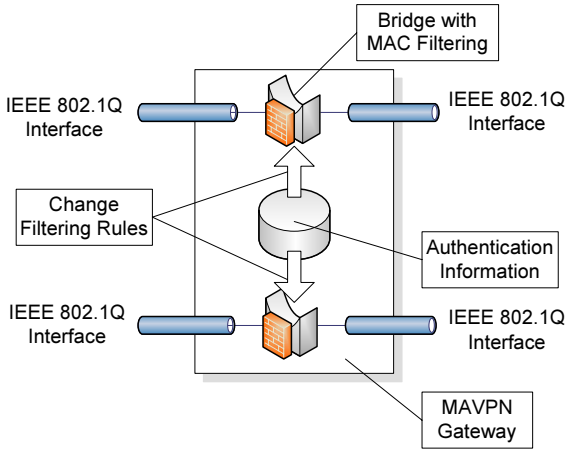

図 7　MAVPN ゲートウェイにおける端末の接続制御

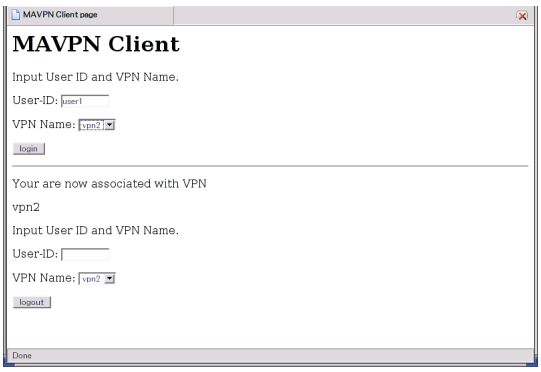

図 8　端末ソフトウェアでの帰属 VPN の選択画面

が必要である。端末ソフトウェアの機能は以下の 3 つである。

- MAVPN ゲートウェイに対して、利用者の ID、帰属する VPN の名前、パスワードを送信する
- VPN への帰属が完了したら VPN アクセスのための IEEE 802.1Q インタフェースを作成し、DHCP 要求を出す
- VPN から離脱したら、VPN アクセスのための IEEE 802.1Q インタフェースを削除する

本プロトタイプでは、各 VPN が一つの IP サブネットを構成し、また IP アドレス空間が重複しないことを前提としている。そのため、端末上のアプリケーションが、パケットをどの VPN の IEEE 802.1Q インタフェースへ渡すかは、端末の持つ静的ルーティングによって決定される。この様子を図 6 に示す。端末の静的ルーティング機能 (図 6 の Static Routing Process) が、パケットの宛先の IP アドレス (図 6 の Destination IP) を元に静的ルーティングテーブル (図 6 の Routing Table) を検索し、適切な IEEE 802.1Q インターフェース (図 6 の eth0.1 や eth0.2) に出力する。

4.4　MAVPN ゲートウェイの設計

MAVPN ゲートウェイの設計について説明する。MAVPN ゲートウェイは、利用者認証によって端末の VLAN への接続制御を行う。

MAVPN ゲートウェイの機能は、大きくわけて以下の 2 つである。

- 利用者からの接続要求を受けて利用者認証を行う
- 認証の結果に応じて端末の接続制御を行う

利用者からの接続要求を受けて利用者認証を行う機能では、利用者から利用者 ID、VPN 名、パスワードを受け取るインタフェースが必要になる。また、利用者から受け取ったこれらの情報を RADIUS サーバに問い合わせ、利用者の VLAN への帰属が許可されているかどうか判定する処理が必要になる。

認証の結果に応じて端末の接続制御を行う様子を図 7 に示す。利用者認証の結果、VPN への帰属を許可された利用者の端末からの IEEE 802.1Q フレームをそれぞれの VPN へブリッジ (図 7 の Bridge with MAC filtering) する。帰属を許可されていない端末からのフレームは、MAC アドレスに基づくフィルタリングにより廃棄する。

5.　プロトタイプの実装

以上で述べた設計をもとに、プロトタイプの実装を行った。

5.1　端末の実装

まず、端末の実装について説明する。本実装では、端末が IEEE 802.1Q をサポートしている必要があるので、今回は Linux カーネル の IEEE 802.1Q 機能 [13] を利用した。

今回は、端末上に WWW サーバを構築し、端末ソフトウェアを PHP スクリプトで実装した。端末ソフトウェアは図 8 のようになっている。利用者は利用者 ID を入力し、帰属したい VPN 名を選択してログインボタンをクリックすると、利用者 ID と VPN 名、端末の MAC アドレスが MAVPN ゲートウェイに送信され、パスワード入力画面が表示される。パスワードを入力すると、認証が行われる。端末ソフトウェアがゲートウェイに情報を送信するために CGI を用いる。今回は、各利用者が、自分が利用できる VPN の名前の一覧を持っているとしている。

認証の結果、VPN の利用が許可された場合、端末ソフトウェアは、Linux の vconfig コマンドを利用して VPN アクセスのための IEEE 802.1Q インタフェースを作成し、DHCP 要求を発してアドレスを取得する。作成する IEEE 802.1Q インタフェースの VLAN ID は MAVPN ゲートウェイから通知される。

また、図 8 の画面で利用者 ID と現在帰属している VPN 名を選択して「Logout」ボタンを押すと、MAVPN ゲートウェイで離脱処理が行われる。そして、端末ソフトウェアは Linux の vconfig コマンドを利用して IEEE 802.1Q インタフェースを削除する。削除する IEEE 802.1Q インタフェースの VLAN ID は MAVPN ゲートウェイから通知される。

5.2　MAVPN ゲートウェイの実装

次に、MAVPN ゲートウェイの実装について説明する。本プロトタイプでは、MAVPN ゲートウェイを、物理的なネットワークインタフェースを 2 つ持った計算機で実装する。ゲートウェイには次の 3 つの機能を実装することになる。

a) インタフェース機能

端末の端末ソフトウェアと情報を交換するインタフェース機能を実装する。この機能は、MAVPN ゲートウェイ上の WWW サーバで動作する、PHP で作成したゲートウェイ処理プログラムとして実装した。ゲートウェイ処理プログラムは CGI を介して端末ソフトウェアと通信を行う。具体的には、ゲートウェイ処理プログラムは、端末ソフトウェアから利用者 ID、VPN 名、パスワード、端末の MAC アドレスを受け取る。また、端末が VPN との通信に用いる IEEE 802.1Q インタフェースの作成または削除を端末ソフトウェアに指示し、作成するインタフェースの VLAN ID を伝える。

ここで、VPN 名を、IEEE 802.1Q の通信で利用する VLAN ID に変換する必要がある。よって MAVPN ゲートウェイにその対応表を持たせる。

b) 利用者認証機能

次に、利用者認証機能を実装する。端末ソフトウェアから受け取った利用者 ID、VPN 名、パスワードからなるアカウント情報に基づいて認証を行う。認証は利用者が VPN に帰属する際と、離脱する際に行う。今回、アカウント情報は MAVPN ゲートウェイ上に保存されているものとし、複数の MAVPN ゲートウェイ間でアカウント情報の同期が取れているものと仮定する。認証は、受け取ったアカウント情報とゲートウェイに保存されたのアカウント情報を比較することで行う。

c) ブリッジ機能

最後に、認証された利用者からの VLAN フレームを VPN へブリッジする機能を実装する。本プロトタイプでは、Linux の Ethernet Bridge 機能 [14] を利用する。認証が完了し、利用者が VPN に帰属する場合、まずその VPN に対応する VLAN 用の IEEE 802.1Q インタフェースを、端末が接続されている側、VPN が接続されている側の両方に対して作成する。そして、2 つの IEEE 802.1Q インタフェース間を接続する Ethernet ブリッジを作成する。

このように、VPN ごとにブリッジを作成し、ブリッジを通過する Ethernet フレームに対して MAC アドレスフィルタリングを行う。フィルタリングには MAC アドレスフィルタリングツールである ebtables [15] を用いる。基本的なフィルタリング規則は以下の 2 つである。

- 端末から VPN へのフレームは全て廃棄する
- VPN から端末へのフレームは全て廃棄する

利用者の認証が完了し、VPN に帰属する場合には次のような規則を追加する。

- 認証された端末の MAC アドレスから VPN へのフレームは全て通過させる
- VPN から、認証された端末の MAC アドレスへのフレームは全て通過させる

また、利用者が VPN から離脱する場合には、追加した 2 つの規則を削除する。

5.3 プロトタイプの動作確認

以上のように端末と MAVPN ゲートウェイの実装を行い、動作確認を行った。動作確認用ネットワークの物理的な構成は、図 9 の通りである。

プロトタイプのネットワーク中には 2 つのサイトが存在する。サイト 1 は MAVPN ゲートウェイ 1、端末 1 と端末 2 で構成されている。サイト 2 は MAVPN ゲートウェイ 2 と端末 3 で構成されている。VPN は IEEE 802.1Q VLAN で構成される。

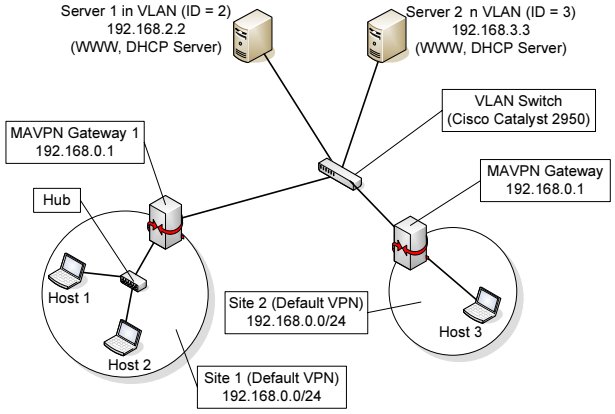

図 9　動作確認に用いたネットワークの物理構成

表 1　プロトタイプの動作確認に用いたアカウント情報

利用者 ID	帰属が許可された VPN	パスワード
user1	vpn2	xxx
user1	vpn3	xxx
user2	vpn3	yyy
user2	vpn4	yyy
user3	vpn4	zzz

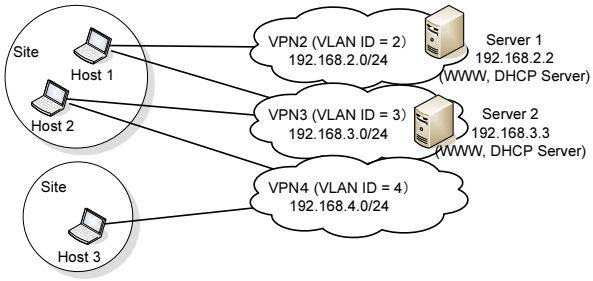

図 10　動作確認に用いたネットワークの論理的構成

サーバ 1 は vpn2 という名前の VPN (VLAN ID は 2) に、サーバ 2 が vpn3 という名前の VPN (VLAN ID は 3) に、常に帰属している。各 VPN のネットワークアドレスは重複しないものとし、vpn2 のネットワークアドレスを 192.168.2.0 とし、vpn3 のネットワークアドレスを 192.168.3.0 とする。また、サーバ 1 とサーバ 2 上には、共に DHCP サーバと WWW サーバが動作している。

このようなネットワーク構成で、端末 1、端末 2 および端末 3 を利用する利用者のアカウント情報を表 1 のように規定した。ここでは、user1 が端末 1 を、user2 が端末 2 を、user3 が端末 3 を利用するものとする。

表 1 ようなアカウント情報に基づき、各端末がそれぞれ許可された VPN に多重帰属すると、論理的なネットワーク構成は図 10 のようになる。このネットワークでは、以下の点が確認できる。

- 端末が複数の VPN に多重帰属できること
- 同一サイト内の各端末がそれぞれ別の VPN に帰属できること
- 端末単位の VPN を動的に構築できること
- 認証されていない利用者端末からのフレームがフィルタリングされること

最初に、端末が複数の VPN に多重帰属できることを確認する。端末 1 から user1 が端末ソフトウェアを用いて vpn2 と

表 2　多重帰属時の端末 1 の静的ルーティングテーブル

Destination	Gateway	Genmask	Iface
192.168.3.0	*	255.255.255.0	eth0.3
192.168.2.0	*	255.255.255.0	eth0.2
192.168.0.0	*	255.255.255.0	eth0
default	192.168.3.1	0.0.0.0	eth0.3
default	192.168.2.1	0.0.0.0	eth0.2

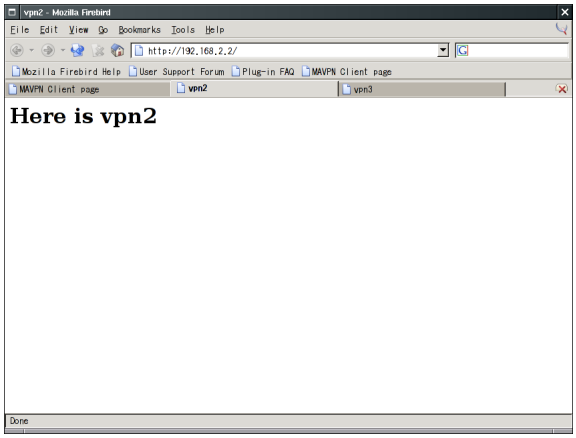

図 11　端末 1 から vpn2 へのアクセス結果

vpn3 に多重帰属すると、user1 の端末の静的ルーティングテーブルは表 2 のようになった。この表では、192.168.3.0/24 宛てのパケットは eth0.3 に出される。eth0.3 は VLAN ID 3 の IEEE 802.1Q インタフェースであり、すなわち vpn3 に通じる。同様に、192.168.2.0/24 宛てのパケットは eth0.2、すなわち vpn2 に出される。この状態で、Host 1 から Server 1、Server 2 に ping や ssh、http によるアクセスが可能であることを確認した。図 11 は Host 1 から vpn2 の Server 1 に http でアクセスした様子である。このように、同一のブラウザで複数の VPN に http アクセスが可能であることを確認した。

次に、同一サイト内の各端末がそれぞれ別の VPN に帰属できることを確認する。端末 1 から user1 が vpn2 のみに、端末 2 から user2 が vpn3 のみにそれぞれ帰属した状態で通信を行った。このとき、端末 1 は vpn2 と、端末 3 は vpn3 とそれぞれ通信が可能であることを確認した。また、端末 1 が vpn3 と、端末 2 が vpn2 と通信できないことも確認した。よって端末 1 と端末 2 はそれぞれ別の VPN に帰属していることがわかる。

次に、端末単位の VPN を動的に構築できることを確認する。端末 2 上の user2 と、端末 3 上の user3 が共に vpn4 に帰属した状態で通信を行った。vpn4 には DHCP サーバが存在しないため、vpn4 のネットワークアドレスを 192.168.4.0/24 と定め、端末 2 と端末 3 にはアドレスを手動で設定した。このとき、端末 2 から端末 3 へアクセスが可能であった。

最後に、認証されていない利用者端末からのフレームがフィルタリングされることを確認する。具体的には、端末 1 上の user1 が vpn2 (VLAN ID が 2) に帰属している状態で、端末 2 上の user2 が認証を行わずに、不正に VLAN ID 2 の IEEE 802.1Q インタフェースを作成した。このとき、端末 2 は vpn2 と通信できないことが確認された。

6.　まとめと今後の課題

本稿では、サイバーソサイエティの実現に向けた、利用者の多重帰属を実現する VPN のプロトタイプ実装を行った。既存のネットワーク技術を用いたプロトタイプ実装により、我々の提案する、利用者の多重帰属を実現する VPN の実現可能性を示し、またそのサービス像を明確にした。具体的には、VLAN で実現した 複数の VPN に対して、端末が多重帰属できるようなプロトタイプを作成した。このプロトタイプで、端末が端末単位に複数の VPN を透過的に利用できることを確認した。また、認証によって端末単位のアクセス制御が可能であることを確認した。

今後の課題としては、プロトタイプのセキュリティレベル、スケーラビリティを向上させることがあげられる。また、VPN 間でアドレス空間が重複することを許容するプロトタイプや、利用者の VPN からの離脱方法を改良したプロトタイプの作成があげられる。さらに、これらの作成したプロトタイプが、VPN 数や帯域幅に対してどの程度スケーラビリティをもつかを評価することがあげられる。

謝　　辞

本研究の一部は、平成 16 年度科学技術振興調整費「サイバーソサエティを実現する仮想網技術」の援助による。

文　　献

[1] S. J. Vaughan-Nichols, “Web Services: Beyond the Hype,” *IEEE COMPUTER*, vol. 35, pp. 18–21, Feb. 2002.

[2] 大山 永昭, “電子政府の現状と課題,” 情報処理, vol. 44, pp. 455–460, May 2003.

[3] 日本テレワーク協会, “日本テレワーク人口等に関する実体調査,” July 2002. available at `http://www.soumu.go.jp/s-news/2002/020705_4.html`.

[4] M. Carugi *et al.*, “Service Requirements for Layer 3 Provider Provisioned Virtual Private Networks,” *Internet Draft* `<draft-ietf-l3vpn-requirements-00.txt>`, Apr. 2003.

[5] A. Nagarajan, “Generic Requirements for Provider Provisioned Virtual Private Networks,” *Internet Draft* `<draft-ietf-l3vpn-generic-reqts-03.txt>`, Feb. 2004.

[6] R. Callon *et al.*, “A Framework for Layer 3 Provider Provisioned Virtual Private Networks,” *Internet Draft* `<draft-ietf-l3vpn-framework-00.txt>`, Mar. 2003.

[7] 原 博之, 村山 純一, 飯盛 可織, 今井田 伊佐宗, “ポリシーベース IP-VPN 方式,” 電子情報通信学会技術報告 *IN2000-101*, vol. 100, pp. 39–46, Oct. 2000.

[8] 三好 潤, 今井田 伊佐宗, 飯盛 可織, 村山 純 一, 栗林 伸一, “VPN 間通信におけるポリシーに基づくサービス制御方式 の検討,” 電子情報通信学会技術報告 *SSE99-171*, vol. 99, pp. 61–66, Mar. 2000.

[9] 原 義博, 大崎 博之, 今瀬 真, 田島 佳武, 丸吉 政博, 村山 純一, 松田 和浩, “利用者が複数の VPN に多重帰属できる VPN アーキテ クチャの提案,” 電子情報通信学会技術研究報告 (IN2003-50), pp. 47–52, July 2003.

[10] 原 義博, 大崎 博之, 今瀬 真, 田島 佳武, 丸吉 政博, 村山 純一, “利用者が複数の VPN に多重帰属できる階層化 VPN アー キテクチャ,” 電子情報通信学会技術研究報告 (NS2003-107, IN2003-73, CS2003-82), pp. 5–10, Sept. 2003.

[11] Alcatel, “Authenticated VLANs, Secure Network Access at Layer 2,” *An Alcatel White Paper*, Nov. 2002.

[12] IEEE Standards for Local and Metropolitan Area Networks, “Virtual bridged local area networks,” *IEEE Standard 802.1Q-1998*, Dec. 1998.

[13] “802.1Q VLAN implementation for Linux.” `http://www.candelatech.com/~greear/vlan.html`.

[14] “Linux Ethernet bridging.” `http://bridge.sourceforge.net/`.

[15] “ebtables.” `http://ebtables.sourceforge.net/`.