SSH と 802.1Q による ユーザ認証 VLAN の構築と運用

奈古屋広昭、松村芳樹、入来院ひさ子、鈴木令子、鷹野三千代
一橋大学総合情報処理センター†

概要
SSH と IEEE 802.1Q の組み合せによるユーザ認証 VLAN の構築をおこない、キャンパスネットワーク上での実運用をおこなった事例を報告する。

A user authenticated VLAN by SSH and IEEE 802.1Q

Hiroaki Nagoya, Yoshiki Matsumura, Hisako Irikeen, Reiko Suzuki and Michiyo Takano
Computer Center, Hitotsubashi University

Abstract
We implement the user anthenticated VLAN using by SSH and 802.1Q, and the example which performed real campus network is reported.

1 はじめに

一般的に大学のような研究教育機関には様々なカテゴリの人々が出入りし研究教育活動に従事している。そして今日においてはあらゆる分野の研究教育においてコンピュータネットワークの利用が必須であるため、キャンパスネットワークは誰もが必要に応じて容易に利用できるよう設計・構築・運用されなければならない。大学におけるネットワークユーザの多様性 (研究教育分野・国籍など) を鑑みるに、(ユーザによる独自環境が構築されている) クライアント端末レベルの自由度を最大限に確保し、ユーザおよび端末単位での肌理細かな制御が可能であり、しかもキャンパスネットワークの可用性やセキュリティを妨害しないネットワークシステムが有効である。

このような要求を満たすために、いわゆるユーザ認証 VLAN と呼ばれるカテゴリのネットワークシステムを採用する事例が多いと思われる。ユーザ認証 VLAN の実装としては各社から市販されている商用製品が多数あり、またさまざまな独自方式も公開されている [1, 2, 3, 5, 6]。

一橋大学では 2002 年春から SSH と IEEE 802.1Q VLAN を用いたゲートウェイ方式によるユーザ認証 VLAN を構築・運用しているので、本稿ではその事例報告をおこなう。

なお以下、イーサネットおよび無線ネットワークの接続点を「アクセスポイント」、利用者認証によりアクセス制御をおこなうゲートウェイを「認証ゲートウェイ」、アクセスポイントに接続するパーソナルコンピュータを「クライアント端末」、本稿で報告するユーザ認証 VLAN を「本システム」と呼ぶことにする。

2 構築・運用の概要

2.1 構築方針

2002 年春に本システムの運用を開始するに当っては次のような方針にしたがった。

- 小規模なプロトタイプからスタートするため構築と運用の手軽さを重視する。
- ネットワーク側およびクラインアント端末に対するプラットホーム依存性はなるべく減らす。
- ユーザ認証によるネットワークレベルでのアクセス制御をおこなう。

上記の方針および運用上・予算上などの制約を前提に、市販製品や当時公開されていた複数の独自実装方式を比較検討した結果

†email: nagoya@cc.hit-u.ac.jp

- イーサネットおよび無線ネットワーク (IEEE 802.11a/b/g) での接続性を提供する。
- DHCP により IP アドレスなどのネットワーク情報を、クライアント端末へ自動設定する。
- VLAN によるブロードキャストドメインの局所化をおこなう。
- 各 VLAN に対して認証ゲートウェイにより外部との通信を制御する形でのアクセス制御をおこなう。
- 802.1Q VLAN を用いることにより、認証ゲートウェイの集中を図る。
- 認証ゲートウェイ上で SSH を利用したユーザ認証をおこなう。
- ユーザ認証には総合情報処理センター発行の既存アカウントを流用する。

というで形での (一般に流通している既成部品を活用した) 独自実装をおこなうことになった。

2.2 運用経過

2002 年 6 月に本システムの運用を開始した段階では

- 認証ゲートウェイ (Linux 2.4.17, 100BASE-TX x 2) × 1
- アクセスポイント (VLAN) × 10
- 使用アドレス空間はプライベートアドレスのみ。
- 月毎 (ユニーク) 利用者数は 100 人弱。
- 最大同時利用者数は 20 人前後。

という状況であった。その後に発生した

- 学内からのアクセスポイント設置要請。
- 研究棟の新築。

といった事情により、本稿執筆時点の 2004 年 10 月時点では

- 認証ゲートウェイ (Linux 2.4.26, 1000BASE-TX x 2) × 2
- アクセスポイント (VLAN) × 108
- プライベートアドレス・グローバルアドレスの双方を利用。
- 月毎 (ユニーク) 利用者数は 1200 人程度。
- 最大同時利用者数は 150 人前後。

まで拡大している。

3 実装の概略

以下、現時点での実装についての概略を述べる。詳細については一橋大学総合情報処理センターの WWW サイト [7] にて公開しているので、必要に応じて参照されたい。

3.1 アクセスポイント

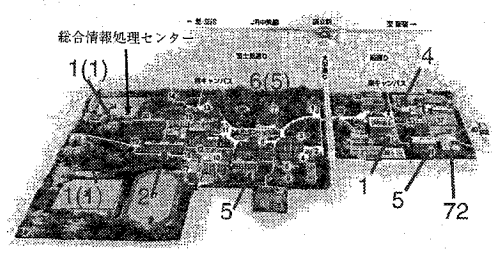

図 1: 数字は建物内の VLAN 数、括弧内は無線 LAN 化されている VLAN 数 (内数)

一橋大学では 2000 年度末の補正予算により IEEE 802.1Q VLAN 対応のキャンパスネットワークが構築・運用されており、その後の追加工事などを含めて、キャンパス内に約 1500 個の「情報コンセント」が設置されている。これらの情報コンセントは 802.1Q VLAN 対応スイッチングハブのイーサネットポートに (ほぼ) 1 対 1 で直結されている。本システムではこの情報コンセントを利用して有線および無線のアクセスポイントを設置した。本稿執筆時点でのアクセスポイントのキャンパス内での配置については図 1 を参照されたい。

3.1.1 有線

講義室やゼミ室には、1〜2 個程度の情報コンセントが既に設置されているので、これをそのまま有線アクセスポイントとして提供している。

また、附属図書館内のように情報コンセントの数に比べて同時利用者がかなり多いと想定される場所では、小型のイーサネットスイッチングハブを情報コンセントにカスケード接続し、このハブのイーサネットポートをアクセスポイントとして提供している。

いずれも MAC アドレスによるフィルタなどは一切かけていない。

3.1.2 無線

IEEE 802.11a/b/g Wi-Fi 準拠の無線アクセスポイントをフロアごとに設置し、最寄りの情報コンセントに接続している。セキュリティレベル低下とユーザ側設定の容易さのトレードオフを検討した結果、現時点では ESS-ID ANY による接続を許可し、WEP や MAC アドレスフィルタリングなどは一切おこなっていない。

また附属図書館のカウンターにて、無線 LAN クライアント用の PC カードの貸し出しサービスをおこない、ユーザへの便宜を計っている。

3.1.3 VLAN

基本的には、情報コンセントごとに異なる VLAN を割り振っている。したがって異なるアクセスポイントは、異なる VLAN に属していることになる。本稿執筆時点では 108 個の VLAN を本システム用に利用している。

3.2 認証ゲートウェイ

認証ゲートウェイはキャンパスネットワークへ接続しているインターフェースと、各 VLAN へのインターフェース (物理的には 1 本のイーサネットインターフェース) を持つルータであり、以下の機能を有している。

- DHCP サーバ: IP アドレスの割り当てをおこなう。
- WWW サーバ: 利用者手引の公開と SSH2 クライアントの提供をおこなう。
- SSH2 サーバ: 利用者認証およびクライアントのヘルスチェックをおこなう。
- パケットフィルタ: 各 VLAN と外部の間のアクセス制御および NA(P)T をおこなう。

3.2.1 プラットホーム

運用開始当初はファストイーサネット (100BASE-T) インターフェースを 2 口持つ PC/AT 互換機上で実装をおこなった。その後、2004 年春以後は、ギガビットイーサネット (1000BASE-T) インターフェースを 2 口持つ PC/AT 互換機上で実装をおこなっている。OS には Debian GNU/Linux(以下、Debian と略す) と (CONFIG_VLAN_8021Q および Netfiter を有効にした) Linux kernel 2.4.26 を利用している。

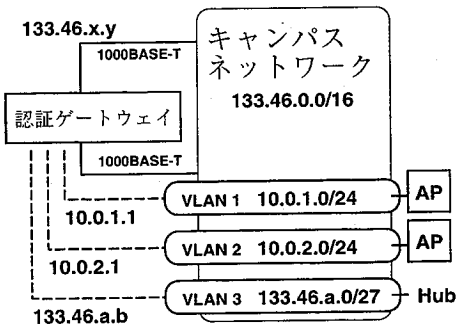

図 2: 接続概念図

3.2.2 DHCP サーバ

Debian にパッケージングされている ISC DHCP を利用している。DHCP サーバは各 VLAN インターフェースからの DHCP リクエストに対して対応するネットワークアドレスの IP アドレスを割当てる。MAC アドレスによる利用制限などはおこなっていない。

3.2.3 WWW サーバ

本運用実験についての利用者手引などを掲載している。また Mindterm などの Java Applet SSH2 クライアントを提供している。これによ

り、Java インタプリタ内蔵の WWW ブラウザ (Internet Exproler 5.x/6.x や Netscape Navigator 4.x/7.x など) が利用できるクライアント端末であれば、特別な設定をおこなわなくても後述の認証ゲートウェイへの接続と認証が可能である。

また、クライアント端末への SSH2 クライアント導入を容易にするため Windows ユーザ向けには PuTTY [12] とレジストリダンプを組み合わせた簡単なバッチファイルを作成し提供している。これにより、ユーザはダウンロードとデスクトップ上への LHA アーカイブ展開のみで、必要な設定済みの SSH2 クライアント実行環境を入手できる。

3.2.4 SSH2 サーバ

認証関係で若干のコード修正をおこなった OpenSSH [11] を利用している。総合情報処理センター既存の LDAP システムよるユーザ認証をおこなっている。

ユーザ者認証 クライアント端末上の SSH2 クライアントからの接続が確立後、ユーザからのアカウントとパスワードの入力を受けて LDAP 経由での認証をおこなう。認証に成功した場合は (ユーザのアカウントに依存しないある特定の) 擬似ユーザの権限で、この擬似ユーザのログインシェルが起動する。ログインシェルは setuid-root perl スクリプトで、以下の機能を有する。

- 起動時に次項のパケットフィルタと連動して、クライアント端末の VLAN 外への通信を許可する処理をおこなう。
- 利用者に対して、利用時間などの情報を送信する。
- 終了時に次項のパケットフィルタと連動して、クライアント端末の VLAN 外への通信許可を取り消す処理をおこなう。

ヘルスチェック OpenSSH のヘルスチェック機能 (sshd の設定ファイル内で `ClientAliveInterval` と `ClientAliveCountMax` キーワードにより制御される) を有効にすることにより、クライアント端末のアクセスポイントからの切り離しをチェックしている。

その他 ポートフォワーディング機能は無効にしている。

3.2.5 パケットフィルタ

Linux 2.4.x に標準搭載されている Netfilter[9] を用いている。

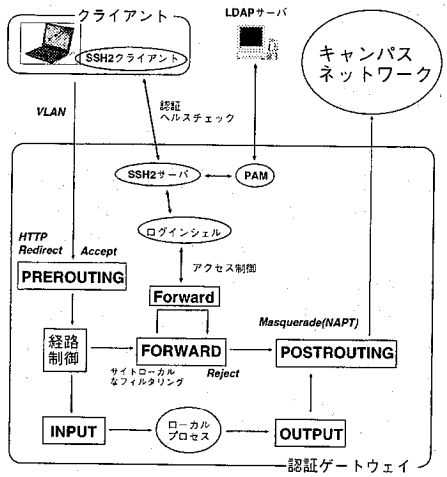

図 3: パケットフィルタの挙動

初期状態 基本的には各 VLAN から入ってくるパケットに対しての IP フォワーディングはすべて拒否する設定となっている。また TCP ポート 80 宛のセッションについては、SNAT により、すべて特定の Web ページへリダイレクトされる。

利用者認証成功 ログインシェルからクライアント端末の IP アドレスと MAC アドレスの対を受け取り、VLAN 内から入ってくる、送信元が該当クライアント端末と一致するパケットに対しての IP フォワーディングを受理するよう設定を変更する。

クライアントの切り離し ログインシェルの終了時 (SSH のセッション終了) に、クライアントの IP アドレスと MAC アドレスの対を受け取り、送信元が該当クライアントと一致するパケットに対しての IP フォ

ワーディングを拒否するよう設定を変更する。

その他 Windows update 用などいくつかの特定サイトに対しては、無条件で IP フォワーディングをおこなうよう設定している。パケットフィルタリングは IP アドレスベースであるが、サイトの特定は DNS ベースであるため定期的 (現在は 5 分毎) に名前解決を実施しフィルタリングルールを変更している。

3.3 モニタリング

DHCP サーバおよび SSH サーバのログは syslog サーバ経由でゲートウェイ内のファイルシステム上に保存される。これにより過去に遡っての利用状況の把握ができる。いずれのログにも VLAN 情報が含まれているため、細かく VLAN を切っておくことにより、物理的な接続個所の特定が可能となる。

また、リアルタイムでの利用状況を把握するために、ゲートウェイ内の wtmp や arp テーブルを参照して、どこ (VLAN) に・誰 (ユーザ) が・何 (IP アドレスと MAC アドレス) で接続しているかをチェックできる管理用 Web インターフェースを用意している。

4 利用状況

本稿執筆時点ではプライベートアドレス用 (28VLAN) とグローバルアドレス用 (80VLAN) に、各々1 台ずつの認証ゲートウェイを割り当てて運用している。

4.1 利用ユーザ数

表 1 は 2004 年における月毎の本システム (ユニーク) 利用者数を集計したものである (G はグローバルアドレス系の、P はプライベートアドレス系のアクセスポイントのみを集計)。月単位では (最大) 1200 人弱の利用者がおり、一橋大学の規模 (構成員数約 7000 人) からすると、それなりに普及しているサービスであると考えられる。

年/月	G	P	計
2004/01	-	164	164
2004/02	-	133	133
2004/03	-	110	110
2004/04	-	600	600
2004/05	-	770	770
2004/06	-	1042	1042
2004/07	-	1067	1067
2004/08	297	365	662
2004/09	319	366	685
2004/10	365	842	1207

表 1: 月毎の (ユニーク) 利用者数

4.2 最大同時利用者数

統計値については [7] を参照のこと。変動は大きいが、最大同時利用者数は 2 台の認証ゲートウェイで各々 100, 50 程度である。現行のハードウェアであれば同時 100 接続で 90Mbps 程度の実用に耐えうるスループットを確保できている (100BASE-TX インターフェースを持つ PC 2 台を使い nttcp[10] により計測した結果)。

5 まとめ

5.1 評価

以上のような SSH と IEEE 802.1Q VLAN を用いたゲートウェイ方式によるユーザ認証 VLAN の構築・運用をおこなった結果、以下のような利点と難点が得られた。

5.1.1 利点

- アクセスポイントについては、特定ベンダーに依存しない。
- 認証情報は SSH により暗号化された通信路上を流れるため、無線 LAN 環境にも適用可能。
- セッション管理を SSH 通信路上でおこなうため、APR や ping ベースのセッション管理と比較して、クライアント端末に導入済みのパーソナルファイアウォールなどとの干渉が少ない。
- 802.1Q VLAN ベースのネットワークが

敷設されていれば、細かなVLAN設定が可能である。

- VLAN数に関らず、認証ゲートウェイは1〜2台程度に集約可能である。
- クライアント端末への要求はDHCP対応・SSH2クライアント導入程度である。
- ユーザ認証にはNIS/RADIUS/LDAPなどが利用可能である。

5.1.2 難点

- 認証ゲートウェイが性能上・運用上のsingle failure pointとなる。
- 複数のSSHクライアントが存在するため、ユーザインターフェースの統一が難しい。
- クライアントとしてNA(P)Tボックスを接続された場合は、その配下に接続された複数クライアントの区別ができない。
- ユーザを守るための通信路暗号化やVPN導入などは別途検討する必要がある。
- 偽ゲートウェイを立てられた場合への対処が困難(一応はSSHサーバのホスト鍵配布でユーザ側からのチェック可)。
- 複数ユーザが共用するクライアント端末については[4]で指摘されているような、偽認証画面の組込みによる認証情報漏洩という脆弱性がある。

5.2 今後の予定

本稿執筆時点で2年間強の運用実験をおこなっているが、とくに不都合はなく安定したサービスを提供できているので、当面は現状を維持し、必要に応じてアクセスポイントの拡充を図る予定である。また

- クライアント端末のサポート範囲拡大(PDAなど)。
- IDSの導入。
- 検疫機構の実装。

なども検討したいと考えている。

一方、冒頭に述べたようにユーザ認証VLANについては、商用製品を含めてさまざまな実装があり、項目によっては本システムより高度な機能を有しているものも多い。したがって、必ずしも本システムに固執することなく、運用上・予算上その他の前提条件を検討したうえで、現状より有効なものがあれば、乗り換えをおこなうこともありうると考えている。

参考文献

[1] 久長穣、岡田隆、刈谷丈治: 情報コンセントのユーザ認証について, 学術情報処理研究 2 77-88 (1998).

[2] 後藤英昭 他: 公共利用の無線LAN/イーサネット・ジャックのセキュリティ対策, http://www.sc.isc.tohoku.ac.jp/~ehgot/secap.html

[3] 只木真一、江藤博文、渡辺健次、渡辺 義明: 利用者移動端末に対応したネットワークの運用 – 佐賀大学でのOpenGateの運用 –, 情報処理学会シンポジウムシリーズ 2004(3) 85-90 (2004).

[4] 安田伸一 他: Opengateを利用した公開端末の認証および利用記録, 2004-DSM-33 (12) 65-69 (2004).

[5] NoNetCat, http://nocat.net/

[6] PersonalTelco http://wiki.personaltelco.net/

[7] オープンアクセスフロア(仮称)運用実験, http://www.cc.hit-u.ac.jp/monban/

[8] Debian GNU/Linux, http://www.debian.org/

[9] netfilter, http://www.netfilter.ort/

[10] nttcpp, http://www.leo.org/~elmar/nttcp/

[11] openssh, http://www.openssh.com/

[12] PuTTY, http://www.chiark.greenend.org.uk/~sgtatham/putty/