異種セグメント端末による分散型仮想 LAN 構築機構の設計と実装

青柳 禎矩[1] 滝澤 允[2] 斉藤 匡人[2] 間 博人[2] 徳田 英幸[1,2]

[1] 慶應義塾大学 環境情報学部 [2] 政策・メディア研究科

1 はじめに

情報共有・協調作業を目的として、Local Area Network (LAN) は企業や学術機関などにおいて広く利用されている。遠隔の LAN に接続する手段として以前はダイアルアップや専用線が一般的であったが、コストが非常にかかるという欠点があった。そこでインターネットなどの公衆ネットワークを利用してあたかも専用線のように遠隔の LAN に接続する技術が多数開発され、これらの技術を用いて構築されたネットワークは Virtual Private Network (VPN) と呼ばれる。遠隔端末が LAN に参加することや、地理的に分散した LAN 同士を接続するといったことを、VPN は既存の公衆ネットワークを利用することで容易に低コストで実現する。しかし既存の VPN 構築手段は通信内容全てが VPN サーバを経由するため、VPN サーバは負荷が多大で単一故障点となる。

本稿は地理的に分散あるいは異種セグメント端末同士による分散型仮想 LAN 構築機構を提案する。既存の VPN 構築技術とは異なり、各端末が自律協調して Peer-to-Peer (P2P) ネットワークトポロジを形成し、仮想的な LAN 構築を可能にする。

2 ELA

本稿では ELA (Everywhere Local Area network) を提案する。ELA は VPN 構築機構の一つであるが、既存の機構にはない特徴がある。本機構によって構築された仮想的な LAN を “仮想 LAN” と呼ぶものとする。

2.1 特徴

ELA の特徴は以下の二点である。

- 自律分散協調

  ELA の仮想 LAN におけるネットワークトポロジは P2P モデルである。

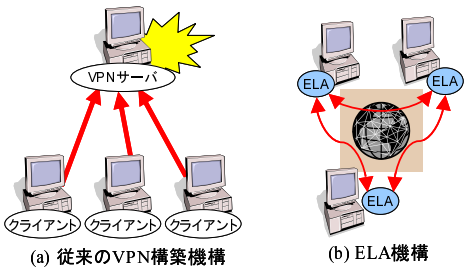
  従来の VPN 構築機構は図 1(a) のようにサーバ・クライアントモデルで、ハブの役割をする VPN サーバにクライアントが接続する。しかし、全ての通信内容がサーバを経由するためサーバへ負荷が集中し、サーバにトラブルが発生すると全ての端末が通信不可能になるという単一故障点となる二つの問題がある。

  この問題を解決するため ELA は図 1(b) のように P2P モデルで、サーバのような中心的存在が存在せず、端末同士が自律協調して仮想 LAN を構築する。そのため本機構は特定へ端末の負荷集中がなく、単一故障点が存在しない。

- 導入の容易さ

  ELA は導入が容易である。既存の VPN 構築技術は設定が煩雑で、ネットワークの深い知識を要求するものも少なくない。ELA はこのような手間を必要としない。

  また VPN 構築技術によってはカプセル化したパケットを配送する特殊なプロトコルを、端末やルータに導入する必要がある。しかし ELA は TCP を利用するため、新たなプロトコル導入を必要としない。



(a) 従来のVPN構築機構　(b) ELA機構

図 1: 従来の VPN 構築機構との違い

2.2 利用例

二台の端末で Windows Network によるファイル共有を行いたいが、ネットワークセグメントが各々異なるため利用できない場合がある。ELA を用いて仮想 LAN を構築すると、二台の端末は Windows Network によって通常と同じようにファイル共有を行える。

2.3 利用手順

- 仮想 LAN 管理者の決定

  仮想 LAN の新規構築時は、最初に仮想 LAN 管理者を決定する。仮想 LAN 管理者は各ユーザの仮想 LAN 構築許諾・禁止などのユーザ管理と、仮想 LAN における通信ポリシ（特定のポートの使用禁止、帯域制限等）決定を行う。

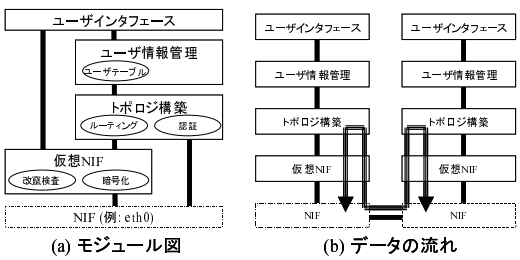
- 仮想 LAN の構築

  仮想 LAN 管理者から仮想 LAN 参加の許諾を受けたユーザ A・B は、以降ユーザ管理者の断りなしに仮想 LAN を構築できる。ユーザ A が構築した仮想 LAN にユーザ B が参加する場合、ユーザ B はユーザ A に対してその要求を行う。ユーザ A・B は互いに認証を行い、互いにそれが妥当と判断されると、ユーザ B は仮想 LAN に参加して通信可能になる。

2.4 設計

ELA の構成を図 2(a) に示す。本機構は実線で囲まれたモジュールの連携により構成される。NIF はネットワークインタフェースを意味する。

仮想 LAN の端末同士による P2P ネットワークトポロジ構築は “トポロジ構築モジュール” によって実現され、他の端末との通信はトポロジ構築モジュールを介して行われる。各参加端末の情報は “ユーザ管理モジュール” によって管理される。“仮想 NIF モジュール” は仮想 LAN におけるネットワークインタフェースの役割を行い、仮想 NIF モジュールは転送するパケットの暗号化とカプセリングを行う。ユーザインタフェースは、各モジュールの状態表示・操作の手段を提供する。



(a) モジュール図　(b) データの流れ

図 2: システム構成図

ELA: Everywhere Local Area network

Sadanori Aoyagi[1], Makoto Takizawa[2], Masato Saito[2], Hiroto Aida[2], Hideyuki Tokuda[1,2]

[1]Faculty of Environmental Information, Keio University

[2]Graduate School of Media and Governance, Keio University

5322, Endo, Fujisawa, Kanagawa 252-8520, Japan

E-Mail: {sada,makoto,masato,haru,hxt}@ht.sfc.keio.ac.jp

ネットワークソフトウェアが仮想LANの他の端末とデータを送受信する時、データの流れは図2(b)のようになる。以下、各モジュールの詳細を述べる。

- ユーザ情報管理
  仮想LANに現在参加している端末の情報を収集・管理し、トポロジ構築の支援をするモジュールである。必要に応じて他の端末と連携して情報の同期を行う。
  ユーザテーブルには仮想LAN参加端末の仮想LANにおけるIPアドレス、実際のネットワークインタフェースのIPアドレス、通信性能（スループット、遅延等）、公開鍵、通信の制約の有無（NAT, ファイアウォール等）が格納される。
- トポロジ構築
  仮想LANに所属する端末が自律協調してP2Pネットワークを構築するモジュールである。
  端末同士はTCP/IPによってコネクションを確立する。このコネクションは仮想LANにおける通信経路という役割のほかに、本機構自身が他の端末と連携する手段として利用される。通信時のスループットを上げ、遅延を減らすために、トポロジ構築モジュールはユーザテーブルを参照して端末同士のコネクションを自律的につなぎかえる。
  またトポロジ構築モジュールは認証を行う。これによって悪意のある第三者が仮想LANに侵入し、不正通信することを防止する。
- 仮想NIF
  LANの端末はネットワークインタフェースを介して通信するように、仮想LANにおいては仮想NIFを介して通信する。また仮想NIFは通信内容のカプセリング、暗号化、改竄検査の機能も有する。
  公衆ネットワークを利用して仮想LANを構築するため、悪意のある人物が仮想LANを攻撃する危険性がある。そのため、カプセリング化した通信内容を途中経路での漏洩防止のため暗号化し、データ完全性を保証するため改竄検査が必要となる。

3 関連研究

ELAと目的が同一のVPN構築機構としてSoftEther [3], PPTP [1], L2TP [2] が挙げられる。各機構はカプセリングするOSI階層や、カプセリングしたデータを転送するプロトコルが異なるが、いずれもサーバ・クライアントのネットワークトポロジを形成する。ELAはネットワークトポロジがP2Pであるため、他の機構に存在する特定端末の負荷集中・単一故障点の存在という問題を解決できる。

4 評価

ELAを二つの手法で評価した。

4.1 定量的評価

ELAをRed Hat Linux 9においてプロトタイプ実装し、ELAによって構築した仮想LANにおける端末間のスループットと通常のLANにおける端末間のスループットを計測し、二つを比較した。端末A (CPU: Mobile Pentium 650MHz, Memory 192MB) と端末B (CPU: Mobile Pentium 600MHz, Memory 64MB) を用意し、両端末にELAのプロトタイプを導入した。そして両端末をハブを介して100Base-TXで接続し、通常のLANと仮想LANの物理的な構成は同一のものとした。

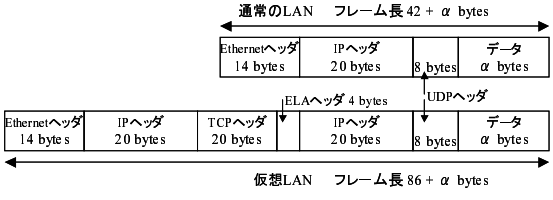


図 3: フレームの構成

表 1: スループットの比較

	スループット
通常のLAN	15.21 Mbps
ELAによる仮想LAN	2.00 Mbps

16バイトのUDPデータグラムを端末Aから端末Bに5秒間可能な限り送信し、1秒当たりのスループットを計測した。図3のように、データを送信する毎に通常のLANでは42バイトのヘッダが付くのに対し、ELAの仮想LANでは86バイトのヘッダが付く。そのため仮想LANのスループットは通常のLANの ((42+16)/(86+16)=)0.569 倍になると仮説を立てた。

しかし結果は表1が示すように、0.131倍のスループットしか得られなかった。ELAは通常に比べ必要な処理の多いことが原因となり、予想を大きく下回る結果になったと考えられる。しかしELAはインターネットを介して利用することを想定している。インターネットのスループットが2.00Mbpsに到達しない通信環境は少なからず存在するため、仮想LANのスループットがさほどボトルネックにならないと考えられる。

4.2 定性的評価

VPN構築手段をVPN参加端末のネットワークトポロジ、単一故障点の有無、データをカプセリングすることによるデータの増加バイト数という観点から比較し、表2にまとめた。トポロジの列にあるS/Cはサーバ・クライアントモデルをLを表す。またL2TPの増加データ長はトンネルモードでIPSecを利用した場合である。

表 2: VPN構築手段の比較

	トポロジ	単一故障点	増加データ長
ELA	P2P	なし	44バイト
SoftEther	S/C	あり	58バイト
PPTP	S/C	あり	38バイト
L2TP	S/C	あり	68バイト

ELAのみP2Pモデルのネットワークトポロジで、単一故障点が存在しない。増加データ長が最小なのはPPTPだが、ELAはPPTPより6バイト多いだけであるため、大きな違いはない。

5 まとめと今後の課題

本稿では異種セグメント端末同士による仮想LAN構築機構としてELAを提案した。ELAを用いると仮想的なLANを柔軟かつ容易に構築でき、通常のLANと同様に、仮想LAN内においてアプリケーションの利用可能になる。これによって情報共有・協調作業がより快適に行える。

今後の課題として多数の端末が仮想LANに参加可能にするためのトポロジ構築モジュールの改良、ブートストラップにおける仮想LANの端末検索手法の改良等が挙げられる。

参考文献

[1] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, G. Zorn. Point-to-point tunneling protocol (pptp). *RFC 2637*, 1999.

[2] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, B. Palter. Layer two tunneling protocol

[3] 登大遊. Softether による Ethernet の仮想化とトンネリング通信. **情報処理学会　プログラミング・シンポジウム**, 2004.