

LiNeS における仮想ネットワーク間接続機能の開発と実用可能性の検討 A Function for Connecting Virtual Networks in LiNeS and Its Practicability

立岩 佑一郎
Yuichiro TATEIWA

安田 孝美
Takami YASUDA

1. はじめに

インターネットを代表としたコンピュータネットワークが世界に普及し、このような社会的インフラを支えるネットワーク管理者の育成は必要不可欠である。年々、Linux サーバの普及に伴い、Linux サーバ管理者の不足が顕在化してきており、Linux サーバを含むネットワーク（以下 Linux ネットワーク）の管理者の育成が重要となってきた。現に、大学では Linux ネットワーク管理者を育成するための授業が行われつつある。しかし、ネットワーク機器が高価であることから、授業を実施している大学は少なく、また、機器不足のため効果的・効率的な演習を行っていない大学もある。

我々は、ネットワーク管理演習環境提供システム LiNeS (Linux Network Simulator) を User-mode Linux [1]の活用により開発してきた[2][3][4][5][6][7]。LiNeS は、従来の PC 演習室設備でネットワーク管理演習を行えるようにすることを目的としたシステムである。標準的な性能の Linux PC 上で動作し、20 台程度の仮想ネットワーク機器から構成される仮想ネットワークを実現できる。仮想ネットワーク機器は Linux サーバ、ルータ、クライアント、スイッチングハブである。従って、1 台の Linux PC で 1 人の生徒に仮想 Linux ネットワークを管理する演習を行わせることが手軽にできる。

本研究の目的は、LiNeS を拡張し、これまでは各 PC 上に孤立して構築していた仮想ネットワークを外部ネットワークに接続可能にすることによって、外部ネットワークの存在を考慮した以下のようなネットワーク演習を新たに行えるようにすることである。

- ・外部ネットワークを考慮した TCP/IP の設定
- ・外部ネットワークとのアクセス制御
- ・外部ネットワークのネットワーク資源の利用
- ・外部ネットワークへのサービスの提供

この機能によって、LiNeS において、実社会でのネットワーク形態により近いネットワーク演習環境を提供できるようになるため、より実践的なネットワーク管理者育成を行うことができるようになる。

本稿では、この機能実現のためにこれまでに我々が提案してきた手法[8]の実用可能性について、今回新たに行った予備的評価実験の結果をもとに議論する。

2. 関連システム

仮想マシン技術によるサーバ構築演習、およびネットワーク構築演習のためのシステムを取り上げ、本研究との違いを述べる。

Anisetti らは、高性能なサーバ上に仮想マシン技術 Xen により実現した複数の Linux 仮想マシンを、個々の学習者

に割り当てるシステムを開発した[9]。学習者は、遠隔地からサーバにログインし、割り当てられた Linux 仮想マシンにおいてサーバソフトウェアの導入やネットワークプログラミングの演習を行うことができる。後野は、1 台の PC 上に UML により実現した複数の Linux 仮想マシンを、個々の学習者に割り当てることで、各学習者に個別のサーバ構築演習環境を提供するシステムを開発した[10]。これらのシステムは、サーバ構築演習に有用であるが、ネットワーク構築演習を行うための機能を有していない。また、Anisetti らのシステムでは高性能なサーバ設備が新たに必要になるため、従来の演習室設備での手軽な実施を目指す LiNeS の目的を満たすことができない。

中川らは、VMware Workstation により 1 台の PC 上に数台の仮想ネットワーク機器を実現し、その PC 複数台を VLAN 機能を有している実ネットワークによって接続することで、各仮想ネットワーク機器を自由に組み合わせた仮想ネットワークを構築できる演習環境を提供するシステムを開発した[11]。しかし、VMware Workstation と高性能機器による大規模計算機演習室での実環境構築であるため、多大な導入コストが必要となってしまう、LiNeS の目的を満たすことができない。

上田らは、UML と Quagga により擬似的な仮想 Cisco ルータを実現し、1 台の PC で複数の仮想ルータによる仮想ネットワークを構築できる演習環境を提供するシステムを開発した[12]。このシステムでは、Linux サーバ構築やそれを含んだネットワーク構築を演習することができない。

以上の関連研究は、ネットワーク構築演習を行うための機能を有していなかったり、特別な設備を必要としたりするため、LiNeS の目的を達成できない。

3. システム実装

本章では、まず、これまで我々が提案してきた VPN 技術による手法[8]について述べる。そして、インターネット上の PC からも学習に参加できるようにするために行う本システムの公開のために行ったネットワーク設定方法について述べる。

3.1 VPN 技術による仮想ネットワークと外部ネットワークの接続

図 1 は、学習者の仮想ネットワークを外部ネットワークに接続するための手法について示している。

「物理ネットワーク」は実際に使用するネットワーク環境を示している。学習者各々の PC 上に構築される仮想ネットワークは、LAN やインターネットなどの実ネットワークを介して LiNeS ネットに接続される。LiNeS ネットは、擬似的なインターネットという位置づけのネットワークであり、ネットワーク資源として DNS ルートネームサーバやパッケージサーバを保持している。

「実装イメージ」は本手法による通信イメージと実装手法を示す。本研究では LiNeS ネットと学習者の仮想ネットワークを VPN 技術によって接続している。大学の PC 演習室内限定であれば、経路制御の工夫により対応することも可能であるが、LiNeS が自宅での自習利用のほか、将来的に遠隔教育への展開を想定しているため、インターネットを介した接続に対応している必要があるためである。VPN ゲートウェイは VPN ソフトウェア OpenVPN[13]により実装されている。LiNeS ネットの VPN ゲートウェイと学習者の VPN ゲートウェイとの VPN 接続の確立によって、学習者のネットワークは LiNeS ネットおよび、他の学習者のネットワークと通信できるようになる。

以上により、学習者の仮想ネットワークと LiNeS ネットは、「論理ネットワーク」に示されるような実ネットワーク上に独立したネットワークを構成する。このような形態は、既存のネットワークへの悪影響を防ぐだけでなく、学習者の混乱を防げるため、効率的・効果的に学習を進めることを可能にする。

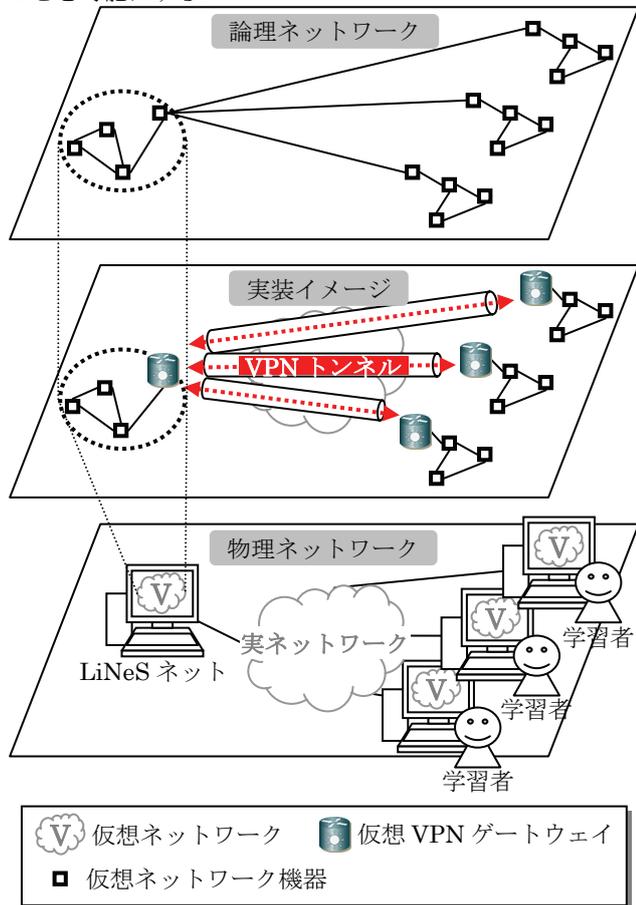


図1 VPN 技術による LiNeS ネットと学習者の仮想ネットワークとの接続

3.2 NAT 技術による仮想 VPN ゲートウェイの公開

LiNeS ネットにインターネット上の PC から参加するためには、VPN ゲートウェイをインターネットに公開する必要がある。LiNeS の VPN ゲートウェイは、Linux 実機の上で UML の仮想機器として動作している。実機ではなく、実機上の仮想機器において VPN サービスを公開するためには、通常、実機と仮想機器にグローバル IP アドレスが

各々必要になる。本研究ではグローバル IP アドレスの浪費を防ぐため、NAT 技術によりグローバル IP アドレス 1 つで運用可能にした。具体的には、図 2 に示す設定を LiNeS ネットの稼働している PC に施している。実機の IP アドレスがグローバル IP アドレスの 133.X.Y.Z であり、TCP ポート 1194 番に来た VPN のための通信データを UML の VPN サーバのプライベート IP アドレス 172.0.0.2 に転送するための設定である。

```
# iptables -t nat -A PREROUTING -d 133.X.Y.Z \
-p tcp --dport 1194 -j DNAT --to 172.0.0.2
```

図2 NAT 技術によるグローバル IP アドレスの節約

4. 実行例

図3は LiNeS ネットと学習者 2 人によって構築されたネットワークである。学習者 A および学習者 B の仮想ネットワークは、LiNeS ネットとの VPN 接続を各々の VPN ゲートウェイを通じて確立している。学習者 A と学習者 B の仮想ネットワークは LiNeS ネットを経由してお互いに通信可能である。

学習者 A が自身のネットワーク内のウェブサーバに公開したテスト用ウェブページを、学習者 B が自身のネットワークの仮想クライアントから閲覧できるか確認している。もし、学習者 B が図に示すようにウェブページを閲覧できれば、学習者 A と学習者 B が各々のネットワークを正確に

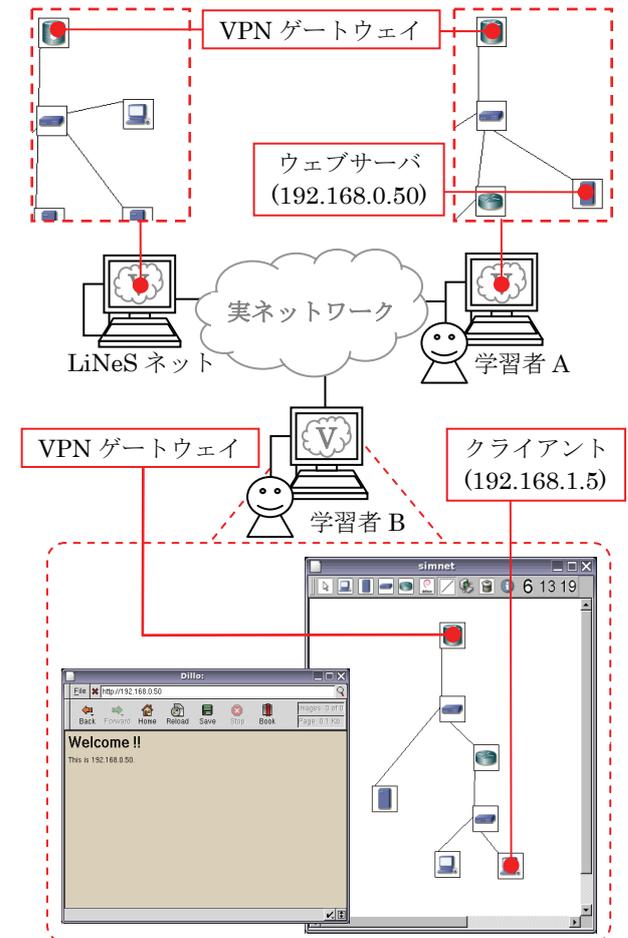


図3 VPN 技術による仮想ネットワーク間通信

構築し外部に公開できていることになる。そうでなければ、学習者 A または学習者 B がネットワークを正しく構築できていないことになるため、2 人は協力してミスを探し修正していくことになる。

5. 予備的評価実験

本手法において、ボトルネックとなりうるのは LiNeS ネットの VPN ゲートウェイである。学習者の外部ネットワークへの通信は、すべてこの VPN ゲートウェイを経由する。従って、多数の通信データが VPN ゲートウェイを同時に経由する場合のネットワークパフォーマンスを測定することで、本手法の性能の下限を明らかにし、その結果をもとにシステムの実用可能性について考察する。

図 4 に測定環境を示す。測定するネットワークは、2 台、8 台、14 台の学習者用 PC にそれぞれ 1 台の LiNeS ネット用 PC を加えたもので、3 パターンである。各パターンのうち 1 台をインターネット上に設置し、その他を LiNeS ネット用 PC と同じ LAN 内に設置した。LiNeS ネット用 PC の性能は Pentium4 2.8GHz、メモリ 512MB であり、学習者用 PC は同程度かやや低い性能である。

測定にはネットワークパフォーマンスの測定ソフトウェア `ttcp`[14]を用いた。2 つの PC でペアを組み、両方の PC から通信データを同時に送受信する。これは、学習者同士がお互いに相手のネットワークからデータをダウンロードしている状態と考えることができる。この通信を各々のパターンにおいてすべてのペアで同時に行うことで、VPN ゲートウェイに最も負荷のかかっている時のネットワークパフォーマンスを測定できる。

測定結果として、LiNeS ネット用 PC の CPU 使用率を図 5 に、学習者用 PC の通信速度の平均を図 6 に示す。通信中の CPU 使用率はすべてのパターンにおいて 100%で、通信速度はネットワーク規模に反比例している。従って、ボトルネックとなっているのは LiNeS ネット用 PC の CPU 性能であると言え、通信データが LiNeS ネット用 PC において転送処理を待っていることが原因であると考えられる。2 台のパターンと比べて、8 台のパターンは 1/3 程度、14 台のパターンは 1/5~1/6 の速度となっており、台数に反比例している。これを基に、本システムの想定する使用条件である 30 台 (学習者 30 人) での結果を推定すると、およそ 13KByte/sec となる。

本機能を使用する演習では、最大で 5MByte 程度のデータを送受信する。このデータを 13KByte/sec で送信あるいは受信するには約 384 秒かかる計算となる。しかし、演習内容を考慮すると、このような負荷のかかった状態 (学習者 30 人が同時かつ双方向に送受信するケース) になる可能性は低い。従って、本手法は本システムの使用目的において大きな問題とならないと考える。また、LAN 上の PC 同士、インターネット上の PC と LAN 上の PC との通信速度はほぼ同じであることから、インターネットを経由した学習も、本手法で大きな問題なく行えると言える。

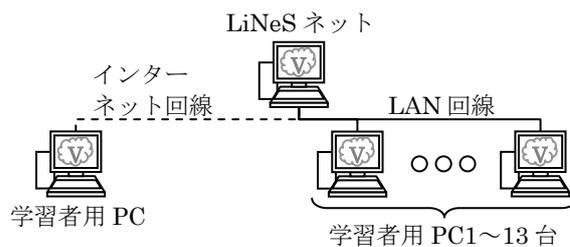


図 4 測定環境

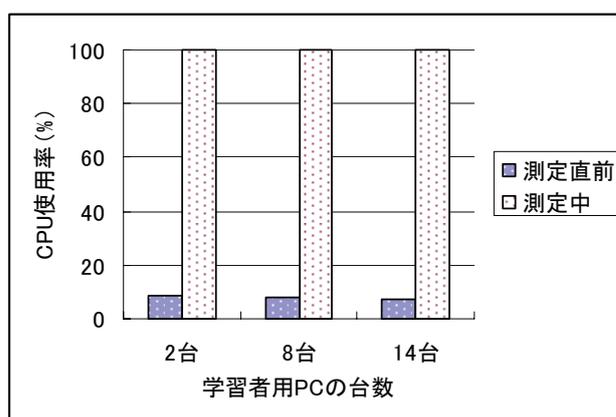


図 5 CPU 使用率測定結果

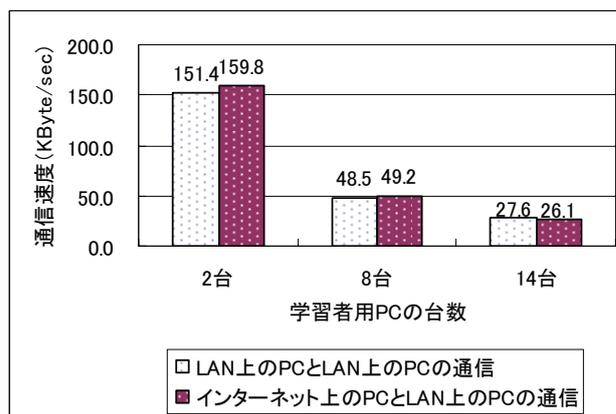


図 6 通信速度測定結果

6. おわりに

本稿では、これまでに我々が提案してきた、学習者の構築する仮想ネットワークを VPN 技術により外部ネットワークに接続する手法について述べた。そして、その実用可能性を、予備的評価実験の結果に基づいて議論した。実験では、ネットワーク間の通信速度と VPN サーバのホスト機の CPU 使用率の測定を行い、その結果から、実際の使用時における性能の下限を推定した。推定結果より、実際の使用において大きな問題なくシステムが動作すると結論付けた。

今後の課題は、本システムの現場導入に向けて、カリキュラムの構築および教材の作成を行うことである。大学関係者へのヒアリング調査、学習理論に基づく教材の考案をする。

謝辞：本研究を修士課程の研究テーマとして精力的に推進して下さった倉地宏輔氏 (現 日本アイ・ビー・エム株式会社

社 ITS ソリューション・センター中部第一サービス)に感謝します。本研究の一部は(財)電気通信普及財団の研究助成によるものです。

参考文献

- [1] The User-mode Linux Kernel Home Page: <http://user-mode-linux.sourceforge.net/>.
- [2] 立岩佑一郎, 安田孝美, 横井茂樹: TCP/IP 学習のための可視化シミュレータの研究, 第3回情報科学技術フォーラム 情報科学技術レターズ, pp.355-357 (2004).
- [3] 立岩佑一郎, 安田孝美, 横井茂樹: TCP/IP 学習支援のための可視化シミュレータの開発 ~表示用データ収集のための User-mode Linux の拡張~, 第4回情報科学技術フォーラム 一般講演論文集第3分冊, pp.369-372 (2005).
- [4] 立岩佑一郎, 安田孝美, 横井茂樹: 仮想環境ソフトウェアに基づくネットワーク構築トラブルシューティング学習支援システムの開発, 第5回情報科学技術フォーラム 一般講演論文集第4分冊, pp.347-348 (2006).
- [5] Yuichiro TATEIWA, Takami YASUDA, Shigeki YOKOI, "A Network Construction Learning Support System Based on Virtual Network Simulation Using Virtual Environment Software," Poster Paper Notes of the 14th International Conference on Computers in Education (ICCE2006), Beijing, China, pp.21-24 (2006).
- [6] 立岩佑一郎, 安田孝美, 横井茂樹: 仮想環境ソフトウェアに基づく LAN 構築技能と TCP/IP 理論の関連付け学習のためのネットワーク動作可視化システムの開発, 情報処理学会論文誌, Vol.48, No.4, pp.1684-1694 (2007).
- [7] 立岩佑一郎, 安田孝美, 横井茂樹: 仮想環境ソフトウェアに基づくネットワークトラブルシューティング実習環境提供システムの評価, 第6回情報科学技術フォーラム 情報科学技術レターズ, pp.469-470, (2007).
- [8] 倉地宏輔, 立岩佑一郎, 安田孝美, 横井茂樹: LAN 構築実習システムにおける仮想 WAN の VPN による構築とその支援機能の開発, 情報処理学会コンピュータと教育研究会 第92回研究会 情報処理学会研究報告 2007-CE-92, pp.45-50 (2007).
- [9] Anisetti, M.; Bellandi, V.; Colombo, A.; Cremonini, M.; Damiani, E.; Frati, F.; Hounsou, J.T.; Rebecconi, D.; Learning Computer Networking on Open Paravirtual Laboratories, IEEE Transactions on Education, Vol.50, No.4, pp.302-311 (2007).
- [10] 後野隆: 仮想環境を利用した「サーバ構築実習」環境の構築--仮想 OS の UML(User Mode Linux)活用報告, 技能と技術, Vol.2004, 雇用問題研究会, pp.34-39 (2004).
- [11] 中川泰宏, 須田宇宙, 三井田惇郎, 浮貝雅裕: VMware を利用した学習用 LAN 構築支援システムの開発, 教育システム学会誌, Vol.24, 教育システム情報学会, pp.126-136 (2007).
- [12] 上田拓実, 井口信和: 仮想 Linux 環境を用いたネットワーク教育システムのための仮想ルータと GUI の実装, 第6回情報科学技術フォーラム講演論文集, J-026, pp.447-448 (2007).
- [13] OpenVPN-An Open Source SSL VPN Solution by James Yonan: <http://openvpn.net/>.
- [14] ttcp.c : <http://www.netcordia.com/files/ttcp.c>.