D-02

仮想 Linux 環境を活用したネットワーク構築演習システムのための仮想スイッチの実装方法の検討

A Study on Implementation of Virtual Switch for Computer Network Construction Training System using Virtual Linux

宮川 祥太† 井口 信和‡
Miyagawa Shouta Iguchi Nobukazu

1. はじめに

ネットワークの構築演習では，ルータなどのネットワーク機器を繰り返し操作することで，ネットワークの構築技能を修得する．実機と Web 教材を用いた教育プログラムとしては，CCNA（シスコ技術者認定）の取得を目的としたシスコネットワーキングアカデミー[1]が世界中の教育機関で実施されている．実機を用いたネットワークの構築演習は，構築するネットワークに応じて機材を用意する必要がある．このため，学習者がいつでも手軽に演習に取り組める環境を用意することは困難である．

そこで，本研究室ではこれまでに，仮想 Linux 環境を活用したネットワーク構築演習システム（以下，本システム）を開発してきた[2]．本システムは，仮想 Linux 環境である User Mode Linux（以下，UML）を用いて，1 台の PC 上に複数の仮想マシンを起動させるものである．本システムでは，この仮想マシンを仮想的なネットワーク機器として動作させ，仮想マシン同士を接続することにより仮想的にネットワークを構築することができる．本システムは，主にルータへのルーティングプロトコルの設定演習を対象としている．本システムにより，実機を用いたネットワークの構築演習と比較して，より手軽に演習を実施することができる．

本研究では，本システムの機能を拡張し，L2 スイッチを用いたネットワーク構築演習の実施を目標とする．L2 スイッチを利用する演習としては，VLAN，スパニングツリープロトコル（以下，STP），L2 セキュリティの設定を行うことを想定している．そこで，本稿では，本システム上で動作する仮想スイッチの実装方法について検討する．

2. 関連技術

仮想化技術を用いた学習環境やソフトウェアのテスト環境の構築を目的とした研究が行われている[3]-[8]．

本システムに関連するシステムとして，立岩らの開発したシステムがある[9]．本システムと同様に，UML を利用したネットワーク学習のためのシステムであり，Web サーバの構築とそのトラブルシューティングを学習の対象としている．このため，立岩らの開発したシステムでは，仮想スイッチの設定は重視されておらず，単純なスイッチング・ハブとなっている．これに対して本システムは，ルータやスイッチなどのネットワークの構成に深く関連する機器を学習の対象とする．

Web サーバ等の構築学習は，一般的な PC でも実現できる．しかし，ルータやスイッチといったネットワーク構成要素を用いた学習では，高価な実習用機材が必要であり，多数を準備することは難しい．さらに，実機を使った実習中にルータやスイッチに障害が発生した場合，障害からの復旧には一定の知識が要求される．したがって，学習環境の整備と保守・運用面から，ルータやスイッチを対象としたネットワークの学習に仮想化技術を利用することのメリットは大きい．

仮想スイッチを提供する仮想化システムとして，VMware ESX，Hyper-V，XenServer がある．これらのシステムでは VLAN を用いたネットワークを構築することができる．しかし，仮想スイッチに IP アドレスを設定する必要があるなど，実機のスイッチでの設定手順とは異なるため，ネットワークの構築演習としては利用できない．本稿で提案する仮想スイッチでは，実機のスイッチと同様の設定手順を実現することで，ネットワークの構築演習として利用することができる．

3. ネットワーク構築演習システム

3.1 システムの概要

本システムでは，仮想 Linux 環境である UML を用いて，仮想マシンを作成する．そして，仮想マシンをネットワーク機器として動作させることで，仮想的にネットワークを構築する．さらに，本システムにはネットワークの構築演習を支援するための機能を実装している．本システムを使用することで，学習者は実機を用いた演習と比較して，より手軽にネットワークの構築演習を実施できる．

3.2 仮想ネットワーク機器

本システムにおいて利用可能なネットワーク機器について記述する．UML により実現する仮想マシンは，それぞれ個別の Linux マシンとして動作する．この仮想マシンに対して，ネットワーク機器として動作するために必要なソフトウェアをインストールすることでネットワーク機器を実現している．

本システムで利用可能なネットワーク機器は，ルータ，およびクライアントやサーバとして動作するホストである．ルータは，仮想マシン上でルーティングプロトコルデーモンである Quagga を動作させることで実現している．これにより，ルータは静的ルーティングに加え，RIP，OSPF，BGP による動的ルーティングを設定できる．ホストは Linux マシンとして Debian を動作させ，標準的な Linux コマンドを扱うことができる．

3.3 ネットワーク構築支援 GUI

本システムは，ネットワーク機器の追加や設定，機器間の接続を GUI から行う．この GUI を図 1 に示す．学習者

† 近畿大学大学院 総合理工学研究科
‡ 近畿大学 理工学部 情報学科

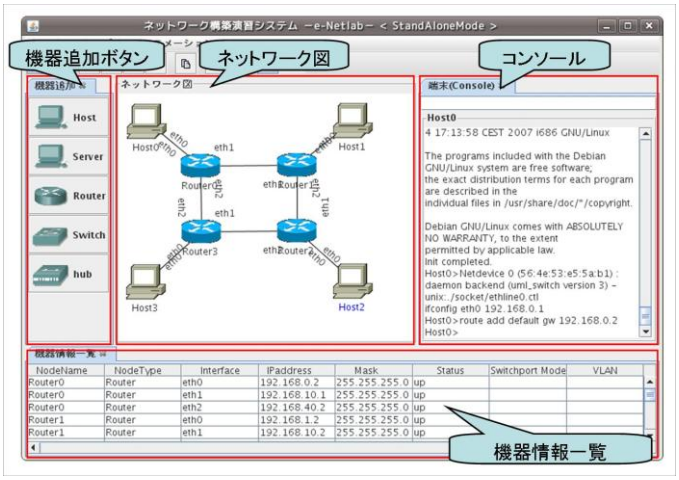

図 1　ネットワーク構築支援 GUI

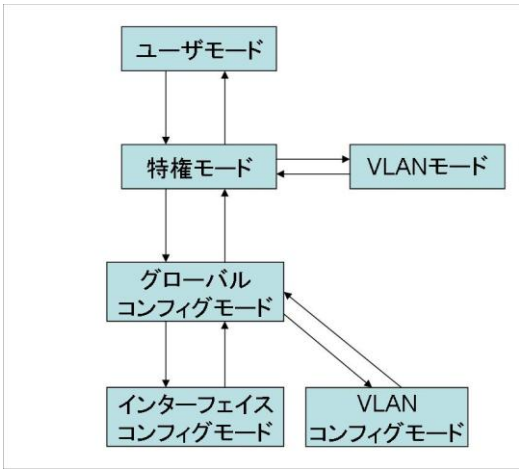

図 2　仮想スイッチのモード遷移図

はこの GUI を用いることで手軽にネットワークを構築することができる．

ネットワーク構築支援 GUI では，機器追加ボタンから，必要な機器を選択し，ネットワーク図にドラッグアンドドロップすることにより，対応するネットワーク機器が起動する．追加された機器はネットワーク図に表示される．ネットワーク図に表示されているネットワーク機器を 2 つ選択することによって，ネットワーク機器同士が接続される．ネットワーク機器の設定はコンソールから行うことができる．機器情報一覧では，設定された機器の名称，IP アドレス，ネットマスク，インターフェイスの状態などが確認できる．

4. 仮想スイッチ

4.1 システムの要件

これまで，本システムでは，パケットをスイッチングし，STP の設定が可能な仮想スイッチを使用していた．しかし，VLAN の設定が不可能なため，スイッチを利用した演習ができなかった．そこで，本稿では，本システム上で動作し，L2 スイッチを利用したネットワークの構築演習を可能とする仮想スイッチの要件と実装方法について検討した．

L2 スイッチを用いたネットワークの構築演習としては，以下のような演習を可能とすることを目標とする．

- VLAN を利用した論理的な LAN セグメントの構築
- 複数スイッチ間での VLAN の設定
- STP を利用した冗長ネットワーキングトポロジの構築
- ポートセキュリティの設定
- ルータを使用した VLAN 間ルーティングの設定

学習者は上記の演習を行うことで，L2 スイッチの動作や設定手順を学習することができる．上記の演習を可能にするためには，仮想スイッチに以下の機能が要求される．

- VLAN
- STP
- L2 セキュリティ

さらに，実機のスイッチと同様の設定手順を可能とするために，実機のスイッチと同様のコマンドラインインターフェイス（以下，CLI）を提供する機能が必要である．

4.2 設計

4.2.1 実機のスイッチと同様の CLI

仮想スイッチの CLI には，実機のスイッチと同様の操作を可能とするために，clish を利用する．clish は，linux システム上で Cisco ネットワーク機器と同様の CLI を実現するためのフレームワークである．clish を利用して，仮想スイッチで使用されるコマンドを定義する．仮想スイッチで使用可能なコマンドの一部を表 1 に示す．仮想スイッチの設定には，実機のスイッチと同様のコマンドが使用できる．

仮想スイッチのモード遷移について図 2 を用いて説明する．ユーザモードでは，ping の実行や仮想スイッチの設定の一部を表示することが可能である．特権モードでは仮想スイッチの設定の表示や，VLAN モードとグローバルコンフィグモードへの遷移が可能である．VLAN モードでは，VLAN の定義や設定が可能である．グローバルコンフィグモードでは，機器の名前を設定することや，インターフェイスコンフィグモード， VLAN コンフィグモードへの遷移が可能である．インターフェイスコンフィグモードでは，STP の設定，アクセスポート・トランクポートの設定，セキュリティの設定が可能である．VLAN コンフィグモードでは，VLAN モードと同様に VLAN の設定が可能である．

4.2.2 VLAN

仮想スイッチで実装する VLAN の要件を述べる．VLAN の方式としては，ポートベース VLAN とタグ VLAN を可能にする．

ポートベース VLAN は，スイッチのポートをグループ化することによって，ブロードキャストドメインを分割する．そのため，VLAN を利用した論理的な LAN セグメントを構築することができる．ポートベース VLAN の設定は，インターフェイスコンフィグモードで「switchport access」コマンドを使用することにより設定できる．

ポートベース VLAN ではスイッチ間接続のために，設定した VLAN の数だけポートを確保する必要がある．そのため，仮想スイッチにタグ VLAN を実装する．VLAN のタグ付け方式には，IEEE802.1Q を使用する．この方式では，Ethernet フレームに 4 オクテットの識別情報を付加する

表 1　仮想スイッチで使用可能なコマンドの例

ユーザモード	enable	特権モードに遷移する
特権モード	configure terminal	グローバルコンフィグモードに遷移する
	copy running-configuration startup-configuration	現在の設定ファイルを スタートアップファイルにコピーする
	erase startup-configuration	スタートアップファイルを削除する
	show running-configuration	現在の設定ファイルを表示する
	vlan database	VLAN モードに遷移する
VLAN モード	show	VLAN の設定を表示
	vlan 10	VLAN10 を定義する
グローバル コンフィグモード	hostname VSwitch	機器の名称を VSwitch に変更する
	interface eth0	eth0 のインターフェイスコンフィグモードに 遷移する
	spanning-tree priority 1	bridge priority を 1 に設定する
インターフェイス コンフィグモード	shutdown	インターフェイスをシャットダウンする
	switchport access vlan 10	インターフェイスを VLAN10 の アクセスポートに設定する
	switchport mode access	インターフェイスをアクセスポートに設定する
	switchport mode trunk	インターフェイスをトランクポートに設定する
	switchport port-security maximum 1	ポートに関連付ける MAC アドレス数を 1 に設定する
	switchport port-security violation shutdown	セキュリティに違反した場合にインターフェイスを シャットダウンする

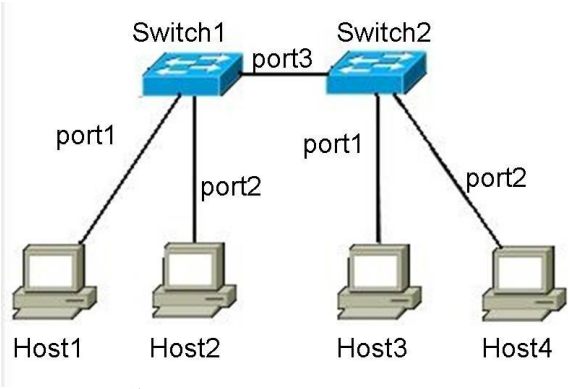

図 3　複数スイッチ間での VLAN の設定演習

ことによって，任意のポートを複数の VLAN に所属させることができる．　タグ VLAN の設定は，インターフェイスコンフィグモードで「switchport mode trunk」コマンドを使用することにより設定できる．

異なる VLAN 間で通信を行うには，ルータが必要になる．そこで、本システムの仮想ルータで IEEE802.1Q の使用，サブインターフェイスの作成を可能にする．この仮想ルータと仮想スイッチを組み合わせることで VLAN 間ルーティングが可能になる．

4.2.3 STP

STP はスイッチで構成された冗長ネットワークにおいて，ブロードキャストストームなどのループによる問題を回避するためのプロトコルである．そこで，仮想スイッチでは，STP の設定やスイッチのプライオリティの変更を可能にする．スイッチのプライオリティは，グローバルコンフィグモードで「spanning-tree priority」コマンドを使用することにより設定できる．

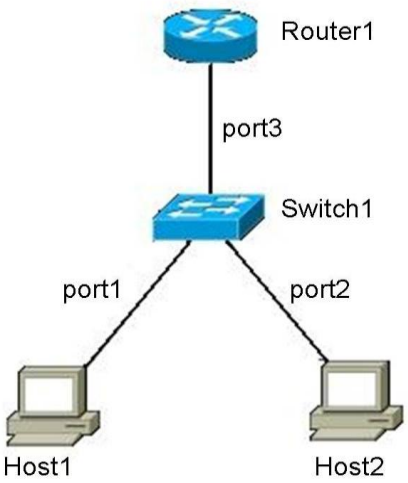

図 4　ルータを使用した VLAN 間ルーティングの設定演習

4.2.4 L2 セキュリティ

L2 スイッチは，ポートセキュリティを設定することにより，ポートに接続するホストのトラフィックを制限する．そこで，仮想スイッチでは，MAC アドレスに基づくポートセキュリティの設定やセキュリティ違反後の違反アクションの設定を可能にする．ポートセキュリティは，インターフェイスコンフィグモードで「switchport port-security」コマンドを使用することにより設定できる．

5. 仮想スイッチを用いた演習例

提案した仮想スイッチを実装することで，以下のような L2 スイッチを用いたネットワークの構築演習が可能となる．

5.1 複数スイッチ間での VLAN の設定

演習課題のネットワークを図 3 に示す．この演習課題では，仮想スイッチで VLAN，アクセスポート，トランクポートの設定を行う．この演習課題により学習者は，複数のスイッチにまたがる VLAN の設定手順を学習することができる．

この演習課題の設定手順を示す．まず，スイッチを 2 台，ホストを 4 台用意する．ホスト 4 台に IP アドレスを設定後，スイッチの設定を行う．スイッチ 1，スイッチ 2 のポート 1 に VLAN10，ポート 2 に VLAN20 を設定する．次に，スイッチ 1，スイッチ 2 のポート 3 をトランクポートとして設定する．これにより，VLAN を利用して，ホスト 1 とホスト 3，ホスト 2 とホスト 4 の論理的な LAN セグメントが構築される．

5.2 ルータを使用した VLAN 間ルーティングの設定

演習課題のネットワークを図 4 に示す．この演習課題では，仮想スイッチで VLAN の設定，トランクポートの設定を行う．仮想ルータでは，サブインターフェイスの作成，VLAN の設定を行う．この演習課題により学習者は，VLAN 間ルーティングの設定手順を学習することができる．

この演習課題の設定手順を示す．まず，ルータ，スイッチを 1 台，ホストを 2 台用意する．ホスト 2 台に IP アドレスを設定後，スイッチとルータの設定を行う．スイッチはポート 1 に VLAN10 を，ポート 2 に VLAN20 を設定する．次に，ポート 3 をトランクポートとして設定する．次に，ルータでは VLAN ごとのサブインターフェイスを作成し，VLAN の対応付けを行う．次に，サブインターフェイスに IP アドレスを設定する．これにより，ルータを利用した VLAN 間ルーティングが可能となり，ホスト 1 とホスト 2 の通信が可能になる．

6. まとめ

本稿では，本システム上で動作し，L2 スイッチを利用したネットワークの構築演習が可能となる仮想スイッチの要件と実装方法について検討した．

今後は，本稿で検討した仮想スイッチを実装し，性能や学習効果について評価する予定である．

参考文献

1) Cisco System:Cisco Networking Academy, http://www.cisco.com/web/learning/netacad.
2) 上田拓実，井口信和，島村博: 仮想Linux 環境を用いたネットワーク教育システムにおける通信可視化機能とネットワーク保存・再現機能の開発，DICOMO2008
3) 早川正昭，丹野克彦，山本洋雄，中山実，清水康敬:LAN 構築シュミレータの開発と教育手法の改善，教育システム情報学会第26 回全国大会講演論文集，Vol.E5-4, pp.367-368(2001).
4) 宮地利幸，三輪信介，知念賢一，篠田陽一:ネットワーク実験支援ソフトウェアの汎用アーキテクチャの提案，情報処理学会論文誌，Vol.48，No.4，pp.1695-1709(2007).
5) Abler, R., Contis, D., Grizzard, J. and Owen, H.:Georgia tech information securitycenter hands-on network security laboratory, Education, IEEE Transactions, Vol.49, No.1, pp.82-87(2006).
6) Bruce, K. and Ilona, B.:A Virtual Learning Environment for Real-World networking, Proceeding of Informing Science + IT Education Conference 2003(2003).
7) Steve, L., Willis, M. and Wei, Z.:Virtual Networking Lab(VNL):its concepts and implementation, Proceedings of the 2001 American Society for Engineering Education Annual Conference & Exposition(2001).
8) Fermin, G. and David, F.:Distributed Virtualization Scenarios Using VNUML, Proceedings of the First System and Virtualization Management Workshop(SVM'07)(2007).
9) 立岩佑一郎，安田考美，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).