

# SaaS 型提供モデルに基づく仮想 Linux 環境を用いたネットワーク構築演習システムの開発

井口 信和 近畿大学理工学部情報学科教授

## 1 はじめに

近年、社会へのインターネットの浸透とネットワーク技術の進歩に伴い、ネットワーク技術者の需要が増加している。ネットワーク学習は書籍や資料による基礎知識の習得と、習得した知識をもとに実習を繰り返すことで、実践経験を積み重ねることが重要である。シスコネットワーキングアカデミー1)においても、Web教材と実機を用いたネットワーク学習方法が取り入れられており、世界的に広く普及している。

実機による演習は、ネットワークの構築経験による実践的な知識が身につくため学習効果が高い。しかし、複数のネットワーク機器を用意しなければ演習できないため、学習者が手軽に繰り返し演習できる環境を整えることは困難である。また実機によるトラブルシューティングは、技術者が通信の障害箇所の特定、修復などネットワークトラブルを早期に解決する能力を養う上で重要な学習である。しかし、ネットワークの障害として考えられる要因は多種多様であり、その全ての事例を実機によって再現することは困難である。

書籍やWeb資料による学習では、通信プロトコルの仕様や通信の処理手順に関する知識について学ぶ。しかし、実機の操作を伴わない学習であることや、例として用いられるネットワークの構成が固定であることから、学習内容がパターン化し実践的なスキルを習得できないといった問題がある。

そこで、これまでに仮想Linux環境をネットワーク機器として動作させ、1台のPC上で動作する仮想的なネットワークを構築することで、ネットワークの構築手順や通信の処理手順について演習するシステム(以下、e-Netlab)を開発してきた2)。

e-Netlabは、仮想Linux環境を活用することで、ネットワーク構築の演習環境を学習者に提供する。実機による演習では、機器が故障した場合の復旧作業が指導者にとって作業負担となるが、仮想環境の利用により指導者の負担の軽減が可能となった。しかし、e-Netlabを利用するために必要となる、仮想ネットワークの構築環境の導入作業が、学習者の負担となっていた。

そこで、今回、e-NetlabをSaaS(Software as a Service)モデルに基づいて開発した。SaaS型e-Netlabでは、仮想ネットワークの構築に必要なソフトウェアをサーバで動作させる。学習者は、サーバで動作する仮想ネットワークの構築環境を、実ネットワークを介して利用する。本システムにより、学習者は使用するPCにJavaの実行環境と今回開発したクライアントプログラムを導入するだけで、演習の実施が可能となった。

## 2 関連研究

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)–9)。本研究に関連する研究として、立岩らの開発したシステムがある10)。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。これに対して本システムは、ルータやスイッチなどネットワークの構成に深く関係する機器を学習の対象とする。荒井らは、実ネットワークの通信データを取得し可視化することで教材として利用し、データ構造と通信処理の手順について学習するツールを開発している11)。しかし、学習者が使用しているPCが送受信したデータを取得し可視化するツールであるため、ルータやスイッチなどネットワークを構成する機器が送受信したデータを学習者に提示できない。また、ツールの性質上、ネットワークの構成を学習者が任意に変更できない。中川らは、仮想マシン環境ソフトウェアVMware Workstationを利用して、個々の学習者がLANの設計から構築・運用までを学習するシステムを開発している12)。しかし、システムを利用するために実機のルータが必要である。また、通信を可視化する機能を備えていない。

### 3 開発したシステムの機能

#### 3-1 システムの概要

本システムは、仮想 Linux 環境である User Mode Linux(以下, UML)をネットワーク機器として利用したネットワーク構築演習システムである。学習者は仮想ネットワーク機器で構成されるネットワークを設計・構築することで、実践経験に基づくネットワークの知識を習得する。演習はサーバで動作する仮想ネットワークの構築環境を実ネットワークを介して利用することで実施する。図 1 にシステムのモデルを示す。

本システムで利用可能な仮想ネットワーク機器は、ルータとレイヤ 2 スイッチおよびクライアントやサーバとなるホストである。仮想ルータでは、静的ルーティングと RIP, OSPF, BGP 4 による動的ルーティングの設定が可能である。また仮想スイッチでは、VLAN(Virtual LAN)と STP(Spanning Tree Protocol)の設定が可能である。本システムの機能は、仮想ネットワーク構築支援 GUI と仮想ネットワーク構築機能、および通信可視化機能から構成される。以下では、各機能について説明する。

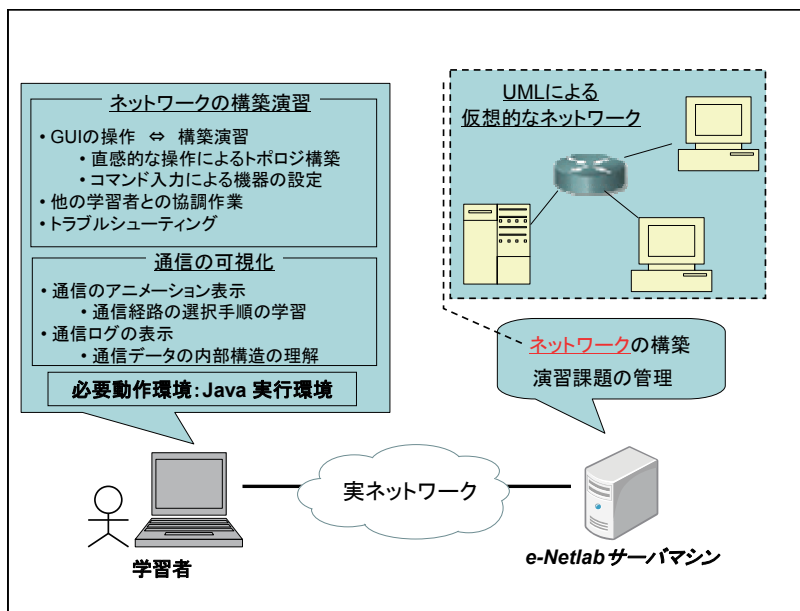


図 1 本システムのモデル

#### 3-2 仮想ネットワーク構築支援 GUI

本システムでは、UML を複数起動し、相互に通信させることで、1 台の PC 上に仮想的なネットワークを構築する。しかし、UML はコンソールアプリケーションであり、UML の起動、設定、確認などの作業はコマンド入力によって行う。このため、ネットワークを構成する各 UML のコンソールから通信の設定を確認できても、ネットワークのトポロジを視覚的に把握できない。そこで、直感的な操作による仮想ネットワークの構築を支援する仮想ネットワーク構築支援 GUI を開発した。本 GUI を用いることで、サーバで動作する仮想ネットワークのトポロジや機器の設定情報を視覚的に確認できる。図 2 に仮想ネットワーク構築支援 GUI を示す。

仮想ネットワーク構築支援 GUI を操作することで、サーバ上に仮想ネットワークが構築される。機器追加ボタンをクリック、または、ネットワーク図にドラッグアンドドロップすることで、仮想ネットワーク機器が仮想ネットワークに追加される。ネットワーク図は、ネットワーク機器を表すアイコン画像と接続を表す直線で描画される。アイコン画像をマウス操作により接続することで、ネットワーク機器同士が通信可能となる。接続を表す直線には、インタフェース名を示す文字ラベルが自動的に表示される。図 3 に機器同士の接続表示例を示す。コンソールへ設定用のコマンドを入力することで、機器の情報を確認、または設定できる。各機器のネットワークに関する設定は、機器情報一覧により確認できる。機器の名前や機器の種類に加えて、IP アドレスやネットマスクなどネットワーク構築に関わる基本的な情報が表示される。

#### 3-3 仮想ネットワーク構築機能

仮想ネットワーク構築機能は、クライアントからの要求により UML による仮想ネットワークを構築する機能である。仮想ネットワーク構築機能は、サーバで動作する。

仮想ネットワークの構築は、仮想ネットワーク構築支援 GUI による操作のほか、ネットワークの情報を記述したファイル(以下、ネットワーク定義ファイル)を用いることでも可能である。ネットワーク定義ファイルは、構築した仮想ネットワークから作成する。ネットワーク定義ファイルには、仮想ネットワークを構成するトポロジや機器の設定値が保存される。定義ファイルを利用することで、学習の一時中断が可能である。また、大規模なネットワークを再現する際に定義ファイルによる自動構築を利用することで、作業負担を軽減できる。図4にネットワーク定義ファイルの例を示す。

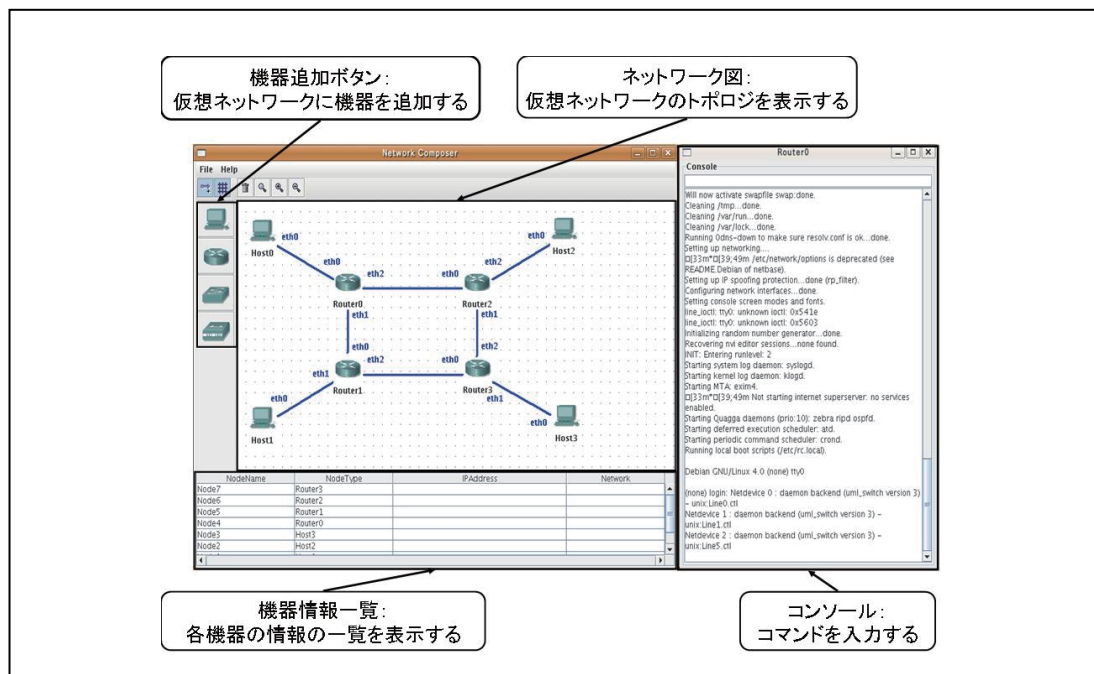


図2 仮想ネットワーク構築支援 GUI

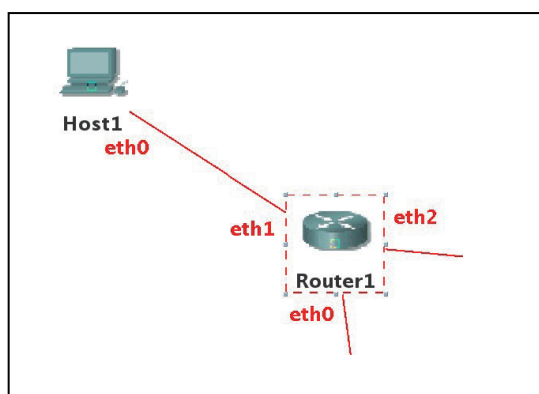


図3 機器同士の接続表示例

### 3-4 通信可視化機能

通信可視化機能を利用することで、通信のログ表示とアニメーション表示が可能である。通信ログ表示機能は、通信ログファイルの内容を解析し、パケットのヘッダ情報を通信プロトコルの仕様に合わせて表示する機能である。この機能により、学習者自身が構築したネットワークの通信情報を用いて、書籍や資料によって得られた通信プロトコルに関する知識の確認が可能となる。

ログ表示機能は簡易表示画面、詳細表示画面、16進数表示画面を実装した。簡易表示画面では、宛先 IP アドレスや使われているプロトコルなど基本的な情報を確認できる。詳細表示画面では、パケットの全ての情報できる。16進数表示画面では、パケットのヘッダ情報を16進数で表示し項目ごとに色分けすることで、プロトコルによって定められたデータ構造と合わせて確認できる。また、それぞれのログ表示画面において、

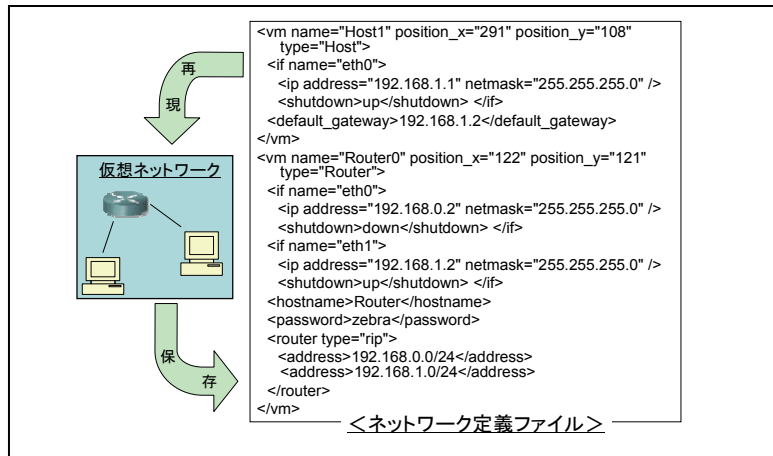


図4 ネットワーク定義ファイル

プロトコルやレイヤ，入出力の方向でフィルタリングしてログ表示できる．図5にパケットログの表示例を示す．

アニメーション機能は，通信ログファイルからパケットの一連の流れを生成し，ネットワーク図上にアニメーションを表示する機能である．パケットを表すアイコン画像がネットワーク図上を移動することで，パケットの通信経路を視覚的に確認できる．また，各ネットワーク機器を通過する際に，パケットのヘッダ情報をダイアログ表示する機能も備えている．この機能により，ルータやスイッチのルーティングの設定変更による通信経路の変化を確認できる．

また，各ネットワーク機器を通過する際に，パケットの情報をダイアログ表示する機能も備えている．ダイアログには，宛先IPアドレス，送信元IPアドレス，宛先MACアドレス，送信元MACアドレスが表示される．このダイアログ表示により，機器を通過するごとに宛先情報がどのように変化するかを確認できる．図6に，通信のアニメーション機能とダイアログ機能の例を示す．

No.	タイプ	方向	Protocol	IN	OUT	1 / 18	前へ	次へ	再生
18	ICMP		ICMP						
17	ICMP		ICMP						
16	ICMP		ICMP						
15	ICMP		ICMP						
14	ICMP		ICMP						
13	ICMP		ICMP						
12	ICMP		ICMP						
11	ICMP		ICMP						
10	ARP		ARP						
9	ARP		ARP						
8	ICMP		ICMP						
7	ICMP		ICMP						
6	ICMP		ICMP						
5	ICMP		ICMP						
4	ICMP		ICMP						
3	ICMP		ICMP						
2	ICMP		ICMP						
1	ICMP		ICMP						

レイヤ別	フィールド別	564E538A	3542564E
<input checked="" type="checkbox"/> dstMac	<input checked="" type="checkbox"/> srcMac	531C57A4	08004500
<input checked="" type="checkbox"/> version	<input checked="" type="checkbox"/> IPlen	00540000	40004001
<input checked="" type="checkbox"/> id	<input checked="" type="checkbox"/> flag	AF55C0A8	0502C0A8
<input checked="" type="checkbox"/> sum	<input checked="" type="checkbox"/> strIP	05010800	5C57FE03
<input checked="" type="checkbox"/> data	<input checked="" type="checkbox"/> dstIP	0001BC28	0348E72F
		0C000809	0A0B0C0D
		0E0F1011	12131415

図5 パケットログの表示

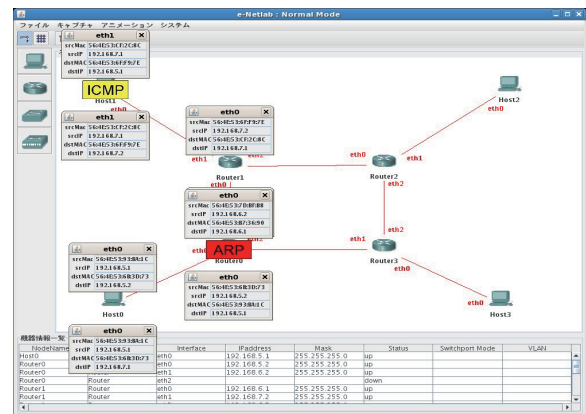


図6 アニメーション機能とダイアログ表示

#### 4 システムの実装方法

本システムはJavaによって開発しており，仮想ネットワークを構成する仮想ネットワーク機器の実装と仮想機器間の接続の処理は，UMLを用いた．また，クライアントサーバ間は，メッセージを交換することで通信する．

仮想ネットワーク構築機能は，メッセージ管理部，仮想ネットワーク定義部，仮想ネットワーク監視部および，仮想ネットワークを制御する仮想マシン起動部，仮想マシン間接続処理部，仮想マシン設定部から構成される．

通信可視化機能は，サーバで動作する通信ログ取得部と仮想ネットワーク構築支援 GUI 上で動作する通信

ログ表示部、アニメーション表示部、およびダイアログ表示部より構成される。通信ログ取得部より送信された通信データは、通信ログ表示部、またはダイアログ表示部により処理され、通信の様子が GUI 上で視覚的に表示される。

図 7 に本システムの構成図を示す。以下では、本システムの各機能の処理方法と実装方法について述べる。

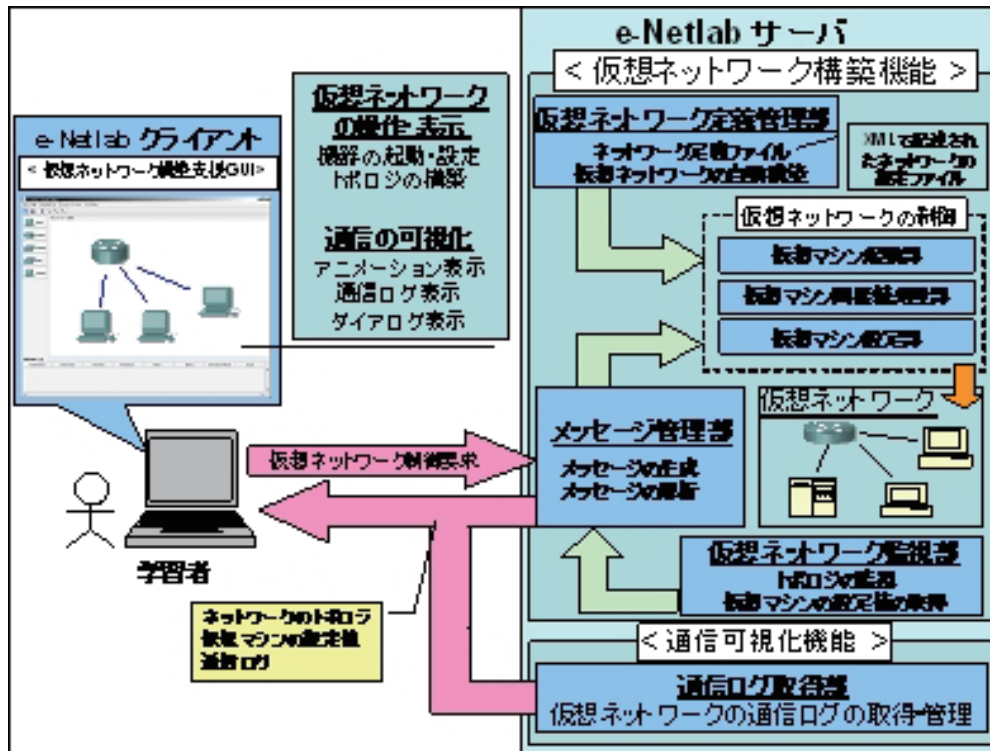


図 7 システム構成図

#### 4-1 仮想ネットワークの制御

仮想ネットワークは、仮想マシン起動部、仮想マシン間接続処理部、仮想マシン設定部によって制御される。仮想ネットワーク構築支援 GUI を操作し、ネットワーク図上に機器が追加されると、仮想マシン起動部によって対応する仮想ネットワーク機器が起動する。GUI 上で機器同士を接続すると、仮想マシン間接続処理部によって仮想機器同士が接続され、相互に通信できる状態となる。GUI のコンソールからコマンドが入力されると仮想マシン設定部により、仮想機器の設定が変更される。

仮想ネットワークを構成する各仮想機器のプロセスの管理は、Process クラス、および ProcessBuilder クラスを用いた。これらのクラスは、Sum Microsystems 社が提供する Java SE 6 に標準で導入されている。ProcessBuilder クラスによって、ソフトウェアやアプリケーションを実行することで起動するプロセスを Process クラスのインスタンスとして管理できる。Process インスタンスの入力ストリームに与えた文字列は、Process インスタンスが管理するプロセスへの入力として処理される。このため、入力ストリームに設定用のコマンドを入力すると、仮想機器上でコマンドが実行され、仮想機器の設定を変更できる。また、仮想機器からの出力は、Process インスタンスの出力ストリームを読み込むことで確認できる。

#### 4-2 メッセージ管理部

メッセージ管理部では、仮想ネットワーク監視部から仮想ネットワークの設定変更の通知を受け取ると、設定の変更を通知するメッセージをクライアントに送信する。

クライアントから仮想ネットワークの操作要求を受け取った場合、その操作要求が存在しない機器に対する操作や、不正なクライアントによる操作でないことを確認する。問題のない操作要求であることを確認できた場合、仮想ネットワークを操作する。

通信方式は、メッセージ交換方式のほかに、Java RMI などの RPC (リモートプロシジャコール) が挙げられる。しかし、メッセージによる通信ではサーバ、またはクライアントを別の言語で再開発する際、通信処理についてはメッセージの解析処理を実装するだけでよい。さらに、複数のクライアントからの要求をメッセージとして管理することで、排他制御を容易に実装できる。そのため、拡張性と移植性の高さから、メッセージ交換による通信方式を採用した。

#### 4-3 仮想ネットワーク監視部

UML の起動時、設定情報を管理するファイル(以下、設定情報ファイル)が作成される。仮想機器はネットワークの設定が変更されると、設定情報を設定情報ファイルに書き込む。仮想ネットワーク監視部は、仮想ネットワークを構成する各仮想機器の設定情報ファイルを監視し、設定情報ファイルの更新を検出すると、クライアントへのメッセージ送信をメッセージ管理部に要求する。

設定情報ファイルは、UML を実行する実マシン側のファイルディレクトリに保存される。実マシンが管理するファイルへのUMLによる仮想マシンからのアクセスは、UMLの機能である fs\_host 機能を用いた。fs\_host 機能を用いることで、実マシンが管理するファイルディレクトリを仮想マシン上にマウントできる。

#### 4-4 仮想ネットワーク定義管理部

仮想ネットワーク管理部では、学習者が構築した仮想ネットワークやトラブルシューティングの演習課題用の仮想ネットワークの情報を保存したネットワーク定義ファイルを管理する。クライアントから仮想ネットワークの構築要求を受け取ると、対応するネットワーク定義ファイルを読み込み、ネットワークの情報を解析する。解析したネットワークの情報は仮想マシン起動部、仮想マシン間接続処理部、および仮想マシン設定部によって処理され、設定情報が反映された仮想ネットワークが構築される。

ネットワーク定義ファイルは、XML により記述されており、各仮想ネットワークの情報は、ひとつのネットワーク定義ファイルにより保存される。

#### 4-5 通信ログ取得部

仮想ネットワークを構成する各仮想機器には、パケットキャプチャプログラムが動作しており、インタフェースからパケットが送受信されると、通信データが通信を記録するためのファイル(以下、通信ログファイル)に書き込まれる。通信ログ取得部では通信ログファイルを定期的に読み込み、パケットキャプチャプログラムによって書き込まれた通信データを取得することで、通信の発生を検出する。

パケットキャプチャプログラムの実装には、パケットキャプチャ用ライブラリである libpcap を使用した。

### 5 評価実験と考察

本システムによるネットワーク学習の効果を調査するため、本学の情報学科の学生を対象に、本システムの評価実験を実施した。評価実験の対象者は、本学で開講しているシスコネットワークングアカデミーの受講生である。実験内容は、シスコネットワークングアカデミーで用いられている演習課題を利用し、実機による演習と本システムによる演習を比較し、アンケートによりシステムの有用性を評価した。

実験で使用した課題例を図8に示す。各課題の内容を表2に示す。課題1と課題2では、実機による実習と本システムによる実習とで課題終了までの所要時間を比較した。実機による実習では課題1に平均17分35秒、課題2に平均19分25秒を要した。これに対して本システムによる実習では、課題1に8分45秒、課題2に9分9秒を要した。実機による実習では、機器の設置や起動に多くの時間を要したことが、所要時間に大きな違いが出た原因として挙げられる。

課題実習後に実施したアンケートでは、システムの操作性や実装した機能について、以下のような意見を得た。

- ・ 実機に近い操作によるネットワーク学習ができ、予習・復習ができる
- ・ 直感的な GUI の操作により、容易に演習ができる
- ・ パケットの内容が変化する様子を確認できる
- ・ パケットの経路を視覚的に確認できる

これらより、本システムを構成する各機能は目的通りに動作しているといえる。しかし、ネットワークを構成する機器の台数の増加に伴い、サーバで動作する仮想マシン

の処理量が増加するため、反応速度の低下を感じたという意見も得られた。

仮想環境を利用するメリットとして、機材の確保や機器を設置するための作業スペースを確保する必要がないこと、機材の数に制限されない演習環境を提供できることが挙げられる。また、ネットワーク機器に誤った設定を施した場合に、機器やネットワーク全体にどのような影響が出るかといった実験的な実習は、実機による実習で実施した場合、正常な設定に戻す作業や副次的な機器の故障などが懸念される。本システムは1台のPC上に仮想的なネットワークを構築して学習するシステムであるため、このような実験的な実習や多くの機器を使用する実習を安全かつ効率的に実現できる。さらに、仮想環境を実行するためのソフトウェアをサーバに動作させることで、学習者は手軽に学習環境を導入できる。

通信可視化機能によって、ホストだけでなくルータやスイッチの通信もキャプチャし可視化することで、パケットの情報や通信経路がプロトコルの仕様通りであることを確認できる。仮想環境である利点を活用した機能を実装することで、ネットワーク構築経験を伴う知識の体得につながると考える。実機による実習では、ルータやスイッチのインタフェースを通過したパケットをキャプチャするために専用の機器が必要となるが、1台のPC上でこのような学習環境を構築できることも仮想環境を利用するメリットの1つである。

評価実験の結果、通信可視化機能によって、機器の設定と通信内容の関係を視覚的にとらえることで、ネットワークプロトコルによる通信手順の理解を支援できることが分かった。また、ネットワーク定義ファイルによって、学習の一時中断や再開、またトラブルシューティングの学習が可能となった。

本システムの仮想ネットワーク機器は、実機よりも起動時間が短い。さらに、ネットワーク定義ファイルを用いることで設定を容易に複製できる。多数のネットワーク機器を必要とする学習では、これらの仮想ネットワーク機器の利点が学習効果に影響する。特に、使用する機器の多い複雑なネットワーク構成の課題に対して有効であると考えられる。

サーバ上に複数の仮想マシンを動作させた場合、増大する処理量によってクライアントへの反応速度が低下する。この問題を解決するため、より小さな処理量で動作するように、仮想マシンの設計を見直す必要がある。

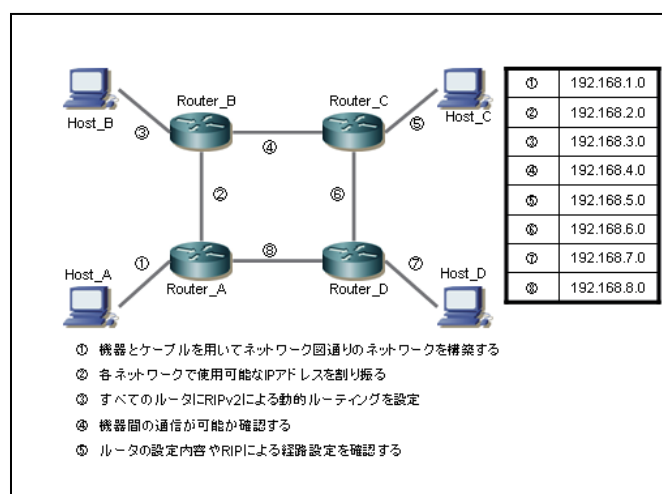


図8 実験に用いた課題例

表1 各課題の内容

課題	内容	必要な機材
課題1	機器の基本設定 静的ルーティングの設定 機器同士の接続 IPアドレスの割り当て	PC2台 ルータ2台
課題2	機器の基本設定 動的ルーティング (RIP) の設定 機器同士の接続 IPアドレスの割り当て	PC2台 ルータ2台
課題3	機器の基本設定 動的ルーティング (RIP) の設定 機器同士の接続 IPアドレスの割り当て	PC4台 ルータ4台

## 6 まとめ

ネットワーク学習支援のために、仮想Linux環境を用いて1台のPC上に仮想的なネットワークを構築することで、通信プロトコルやネットワークの構築手順について学習するシステムを開発した。仮想環境を利用することで、規模に制限されないネットワークの構築環境を提供し、教材作成や故障した機器の復旧などによる指導者の負担を軽減できた。さらに、SaaS型とすることによって、仮想環境によるネットワークの構築機能をすべてサーバで動作させるため、学習者に対して実習環境を容易に提供することが可能となった。今後の課題として、仮想機器の排他的制御とGUIの操作性の向上があげられる。

### 【参考文献】

- 1) Cisco Systems: 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, DICOM02008
- 3) 早川正昭, 丹野克彦, 山本洋雄, 中山 実, 清水康敬: LAN構築シミュ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 security centerhandson 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 Net-working 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) Benjamin, A. and Thomas, E.D.: Xen Worlds:Xen and the Art of Computer Engineering Education, *Proceedings of 2006 ASEE Annual Conference and Exposition* (2006).
  - 10) 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).
  - 11) 荒井正之, 田村尚也, 渡辺博芳, 小木曾千秋, 武井恵雄: TCP/IP プロトコル学習ツールの開発と評価, 情報処理学会論文誌, Vol.44, No.12, pp.3242-3251 (2003).
  - 12) 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, 教育システム情報学会誌, Vol.24, No.2, pp.126-136 (2007).

#### 〈発 表 資 料〉

題 名	掲載誌・学会名等	発表年月
仮想 Linux 環境を活用した SaaS 型ネットワーク構築演習システムの開発	DICOMO2009 シンポジウム	2009 年 7 月
仮想 Linux 環境を活用したネットワーク構築演習システムへの自動採点機能の実装	情報処理学会第 72 回全国大会	2010 年 3 月
仮想 Linux 環境に基づくネットワーク構築演習システムへの実ネットワークとの通信機能の開発	情報処理学会第 72 回全国大会	2010 年 3 月