WEB アプリでのネットワークシミュレータの開発

最首和雄

The Implementation of Network Simulator in WEB Application

Kazuo Saishu

キーワード： WEB アプリケーション，ネットワーク，パケット送信

1. はじめに

情報ネットワークの授業は講義だけでなく、学生１人につき数台の PC、ハブ、LAN ケーブルなどのネットワーク環境を用意し実際にネットワークを構築するのが望ましい。しかし、学生の人数や部屋の広さによってはそれが不可能な場合もある。そこで、本研究ではスマートフォンを利用した情報ネットワーク基礎教育システム[1]をもとに、JAVA による WEB アプリケーション上でシステムを開発中なのでその中間報告をする。

本システムを利用することでネットワーク環境が用意できない場合でも学生はネットワークについてシミュレーションで学ぶことができる。ネットワーク構築実験では、ネットワークの構築時に本システムの補助機能で設定コマンドを確認するなどして実験に利用できる可能性がある。

2. システムの概要

本システムは情報ネットワークをシミュレーションする WEB アプリケーションである。以下のような構成でシステム開発を行っている。

以下の 3 種類のネットワークに対する教育を行う。

①ネットワーク 1

②ネットワーク 2

③実験指導用ネット

論文作成時にはネットワーク１のシステムについてほぼ完成して、教育システムとして使用できるかを検討している。以下がシステムのトップページである。

「実験指導用ネット」については設計段階である。

ネットワーク１が汎用のネットワークである。ネットワーク構成を変えた場合も簡単に対応できるようにしたいが、現在はそのようになっていない。ネットワーク２は MASQUERADE を教えるためのネットワーク、実験指導用ネットは実験のときに実行するコマンドを使って設定し、シミュレートするシステムにすることを目指している。MASQUERADE を教えるにはゲートウェイに３個以上のイーサがあることが望ましいので、ネットワーク 2 を設けた。

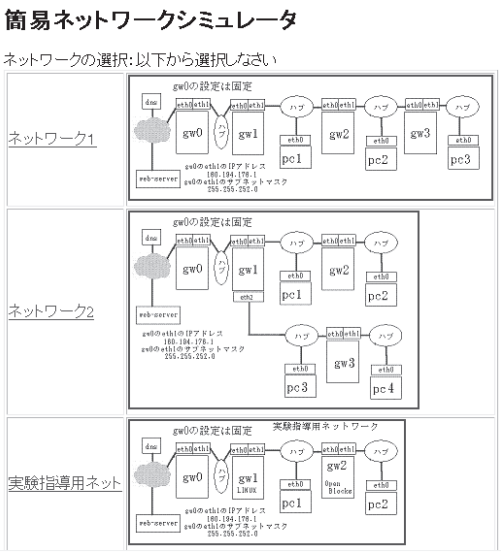

図 1. システムトップページ

各ネットワークでプライベートアドレスを使ったネットワークとグローバルアドレスを使ったネットワークの間にあるゲートウェイをゲートウェイ１(GW1)と呼んで、このゲートウェイだけがファイアウォール機能を持ち、他のホストは持たないとする構成である。

上記の３つのネットワークは設定部とシミュレーション部の２つの要素で構成されている。設定部は

デフォルトの設定値を使う場合と、利用者が設定する場合がある。

シミュレーションはパケットを送信元ホストから送信先ホストにその間のホストを中継して送る。TCP,ICMP パケットについては、戻るパケット（SYC/ACK、エコー応答）のシミュレーションも行う。

3. ネットワーク１を使ったシステム

ネットワーク１の構成は３つのゲートウェイ、３つの端末 PC、WAN 側の DNS、HTTPD で構成されている。

LAN と WAN をつなぐゲートウェイ１の WAN 側のイーサと外部の DNS サーバとＷＥＢサーバのホストには最初から IP アドレスは設定されており設定を変えることはできない。プライベートアドレスを使用する所で、以下の値を設定する。

設定１：IP アドレス等の設定

設定２：ルーティングテーブルの設定

設定３：その他の設定（マスカレード、NAT、パケットフィルター、IP フォアワード）

以下がネットワーク１を選んだときの最初の画面である。

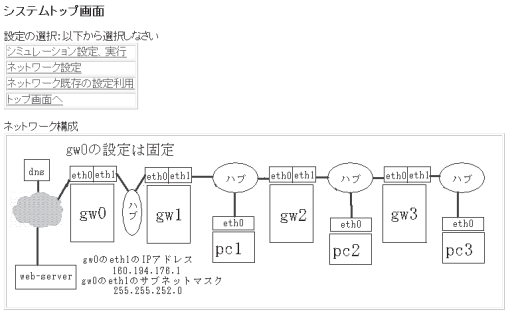

図 2. ネットワーク１のトップページ

「ネットワーク既存の設定利用」を選択すると、各イーサの IP アドレスなどの設定、各ホストのデフォルトゲートウェイ、DNS サーバの設定、ルーティングテーブルの設定、ipforwrd の設定でデフォルト値が設定される。以下がその画面の一部である。

ファイアウォールの設定は LINUX(Red Hat9)の iptables コマンドの機能を参考にした。マスカレード、SNAT,DNAT、パケットフィルターのデフォルト値の設定を選ぶと、デフォルト値でシミュレーションできる。

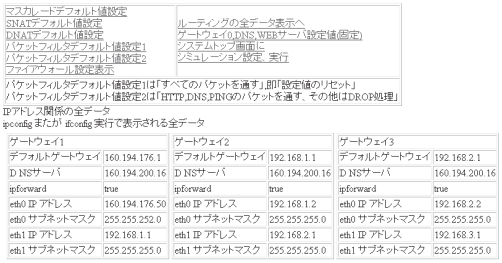

図 3. デフォルト値を設定するページ

3.1　ネットワーク設定

図２で「ネットワーク設定」を選択すると前記　設定１、設定２、設定３　を利用者が行うページとなる。以下がその画面である。

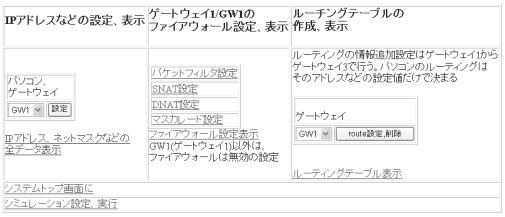

図４．ネットワーク設定画面

3.1.1　IP アドレス等の設定

図４で「IP アドレスなどの設定、表示」では、ホストを指定して設定する。ゲートウェイ２の設定画面の一部は以下である。

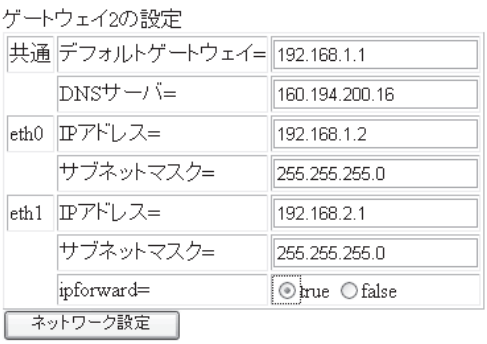

図５．ゲートウェイ２の設定画面の一部

ネットワークの設定では最初に各端末のイーサネットの IP アドレスなどを設定する。

3.1.2　ルーティングテーブルの設定

図 6 の「ルーティングテーブルの設定画面」でも、ホストを指定して設定する。ゲートウェイ 2 の設定画面の一部は以下である。追加と削除がある。

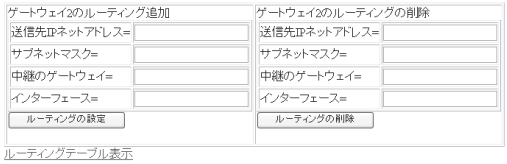

図 6．ルーティングテーブル設定画面

ルーティングテーブルはすべてのゲートウェイ、端末で設定できる。設定に必要な情報は送信先ネットワークアドレス、ネットマスク、中継ゲートウェイ、インターフェースであり、ユーザーが設定可能なのは 3 つまでとした。Default のルーティングとそのホストのイーサと同じネットワークのルーティングは自動で設定される。

3.1.3　その他の設定

本システムではマスカレード、NAT、パケットフィルターの設定ができるのは LAN と WAN をつなぐゲートウェイ(ゲートウェイ 1)だけである。

図 4 で「ゲートウェイ 1/GW 1 のファイアウォールの設定、表示」では、以下の設定を選択して行う。

パケットフィルタ設定、SNAT 設定

DNAT 設定、マスカレード設定

以下は「マスカレード設定」の画面である。設定可能なのは 3 つとした。

なお、Masquerade,SNAT,DNAT ではポート番号の変更は行わない、ポート番号は送信先のみを指定することとした。

パケットフィルタは 5 つまで指定できることとした。指定がない場合はすべてのパケットを通すとした。

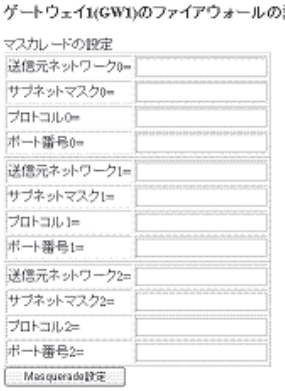

図 7．MASQUERADE 設定画面

パケットフィルタでの設定項目は送信元ホストと送信先ホストでのネットワークアドレス、サブネットマスク、送信先ポート番号、プロトコル(all を含む)、可否情報である。可否情報とは ACCEPT,REJECT,DROP がある。

iptables コマンドでの設定例を以下に示す。

iptables –A FORWARD –p tcp –d 192.168.3.0/24 –dport 80 –j ACCEPT

これは「ネットワーク IP アドレスが 192.168.3.0/24 へ送る TCP パケットで、送信先ポートが 80 のパケットを通す」規則を、FORWARD チェインに加えることを表す。コマンドでの省略はすべてを表す。上記で -s 、-sport オプションはないので、すべての発信元ホストのすべての発信元ポートを表している。

LINUX のコマンドで、iptables コマンドはネットワークアドレス表現に CIDR を使う。route コマンドではサブネットマスクを使う。本システムでは設定をすべてサブネットマスクを使う方法とした。

上記の設定結果を表示する例をを以下に示す。

パケットフィルタの設定
iptable -L で表示される全データ

送信元IP	送信元netマスク	送信先IP	送信先netマスク	protocol	送信元ポート	送信先ポート	可否
null	null	192.168.3.0	255.255.255.0	tcp	null	80	ACCEPT
null	null	160.194.200.20	null	tcp	null	80	ACCEPT
null	null	null	null	udp	null	53	ACCEPT
null	null	null	null	icmp	null	null	ACCEPT
null	null	null	null	null	null	null	null

図 8　パケットフィルタ設定値表示結果の 1 例

3.2　シミュレーション部

設定部で設定した情報を元にパケット送信をシミュレーションする。図 2 の「シミュレーション設定、実行」を選

択して実行する。この最初の処理は接続検査である。以下の 3 項目を検査する。

① Ether の IP アドレス、ネットマスクの設定検査
② 各ネットワークの Ether が同じネットワークアドレスである検査
③ 異なるネットワークが異なるネットワークアドレスである検査

シミュレーション実行では送信元、送信先、プロトコル、ポート番号を入力し送信ボタンを押すとパケットが送信される。その画面が以下である。

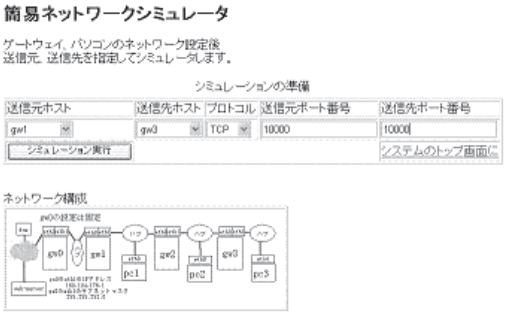

図 9.　シミュレーション設定画面

送信画面では現在のパケットの位置や送信先などの情報が表示され、ボタンを押すごとにパケットが次の中継ゲートウェイを進んでいく。このパケットの動きは画像を利用しユーザーに分かりやすいようになっている。パケットには現在のホスト、送信先、送信元、プロトコル、ポートなどのデータが表示されており、この送信データの設定と設定部で設定したネットワークの設定がマッチしてなければパケット送信に失敗したと画面に出力する。ポート番号に整数値が入っていない場合は再設定のページを表示する。

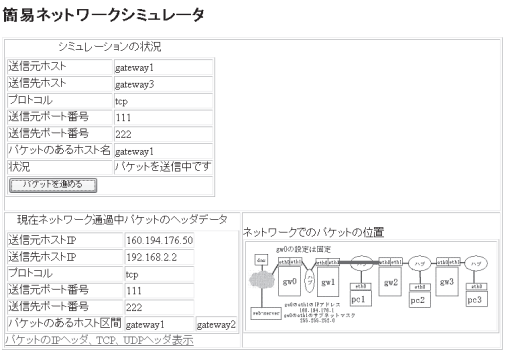

図 10.　シミュレーション実行中の画面 1

パケットは IP ヘッダ、TCP/UDP ヘッダの表示をできる機能を持たせた。図 11 はパケットが送信先ホストに達したときの表示である。

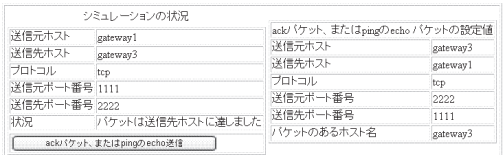

図 11　パケットが送信先ホストに到達した画面

4　システムの詳細

4.1　設定部の詳細

システム全体の動作に必要な情報は DataStore クラスのオブジェクトに持たせている。クラスは以下のように分類できる。

① データ保存用のクラス
② データ処理用クラス
③ シミュレーション用クラス
④ ツール用クラス

データ保存用クラスは以下のようになっている。

DNAT, Ether, GateWatTerm,GateWay,
Terminal, Masquerade, Network,
Packet, PacketFilter, Route, RouteTable, SNAT,
IP,TcpUdp

GateWatTerm クラスは,GateWay クラスと Terminal クラスのスーパークラスとした。

データ処理用クラスは以下に分かれる。

① 全体のデータを管理するクラス　DataStore
② デフォルト値を設定するサーブレット
DNATdefaultServlet,SNATdefaultServlet,
MasqDefaultServlet,SetAllDataServlet

SetAllDataServlet クラスは、各 Ether の IP アドレス、ネットマスクの設定が中心である。

③ JSP ファイルの設定値をオブジェクトに取り込むサーブレットは以下である。

NetData,GetRouteData,DNATservlet,
Masqueradeservlet,SNATservlet,
PacketFilterservlet,SetFireWall

JSP のページで利用者は設定値を入れる。

④　シミュレーション用クラス
シミュレーションの最初のクラスはネットワークのデータの初期化を行う。NetWork1 クラス
パケットを送るシミュレーションクラスは SimyurateExe2 クラス、SYC/ACK または応答パケットを送る SimyurateExe3 クラスである。

4.2　シミュレーション部の詳細

シミュレーション部の遷移を表す図を図 11 に示す。TCP プロトコルによる接続では、①要求元から相手先へ SYN フラグをセットしたパケットを送信、② SYN パケットを受け取った相手先は、要求元に SYN/ACK フラグをセットしたパケット(SYN/ACK パケット)を送信、③ 相手先から ACK フラグがセットされたパケットを要求元が受け取る　という 3 ウェイハンドシェークの処理の、①、②のパケットの流れをシミュレーションする。TCP パケットは TcpUdp クラスの SYN,ACK フィールドの値が設定される。

ICMP プロトコルによる通信では、送信元ホストが PING コマンドを送信先ホストに送り、送信先ホストから ICMP メッセージを送信元ホストに送られる(エコー応答パケット)ときの状態をシミュレーションする。これらは ICMP のエコー要求、エコー応答と呼ばれる。

UDP プロトコルによる通信では送信元ホストから送信先ホストにパケットが送られる状態をシミュレーションする。以下がこれらの 3 つのシミュレーションをまとめた流れである。

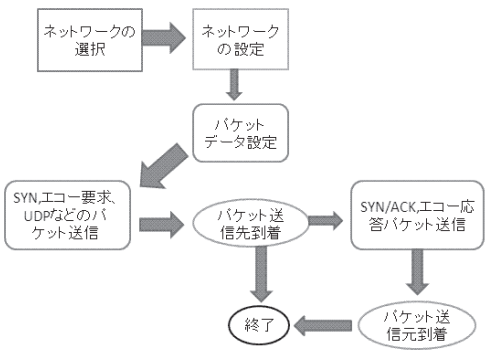

図 12　シミュレーション部の Packet の遷移を表す図

シミュレーション部の先頭は「パケット設定」画面である。ここでパケットの送信元、送信先のホスト名、プロトコル、ポート番号などを設定して「シミュレーション実行」ボタンを押す。(図 9)

図 13 は「パケット送信」画面である。画面の下側には簡単なネットワーク図が表示される。パケットは GW1 から GW3 に送る例である。ここで「パケットを進める」ボタンを押すと、この画面になり、パケットが GW2 に達したことを示す。図 13 の GW1 と GW2 の間のリンクが赤色になり、ここをパケットが通ったことを示す。

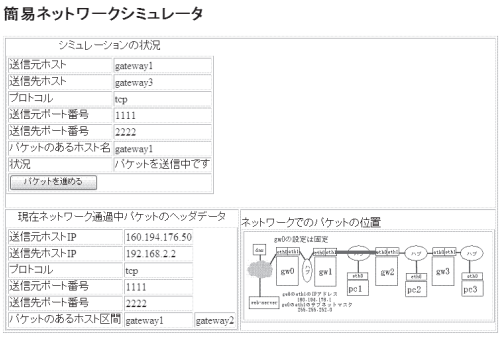

図 13　パケット送信時の画面

パケット送信の処理については、LAN と WAN の境界にあるゲートウェイ 1(GW1)にファイアウォール機能を設定し、他はファイアウォールなしとした。GW1 でのパケットの処理の流れの一部を図 14 に示す。

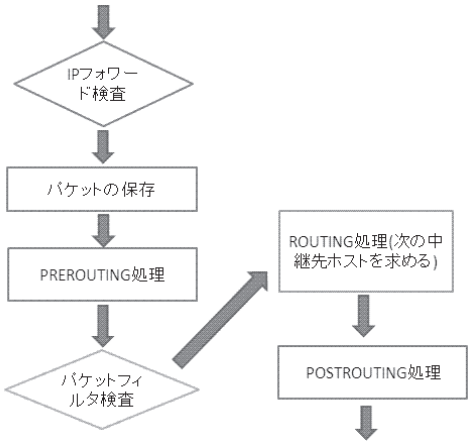

図 14　ファイアウォールの処理

ここでの処理は PREROUTING で DNAT 処理、POSTROUTING で Masquerade 処理、SNAT 処理を行う。その他 FORWARD 処理、パケットフィルターの処理からなる。ここで処理したデータは保存され、TCP の SYC/ACK パケット、ICMP パケットのエコー応答などのパケットの設定に使用される。

SYC/ACK,エコー応答パケットの処理について

これらの戻ってくるパケットについては PREROUTING で Masquerade、SNAT の元に戻す処理、POSTROUTING で DNAT の元に戻す処理を行う。処理方法は以下でシミュレーションした。

ゲートウェイ 1 で受け取ったパケットと変更前のパケットの比較を行う。変更前のパケットとは送信元から送信先に送るとき、ゲートウェイ 1 で受け取ったパケットをいう。

① Masquerade、SNAT が行われた判定：送信先がゲートウェイ 1 で、変更前のパケットの送信元がゲートウェイ 1 でない場合。送信先 IP アドレスを変更前のパケットの送信元 IP アドレスにする。

② DNAT が行われた判定：変更前のパケットの送信先がゲートウェイ 1 で、このパケットの送信元がゲートウェイ 1 でない場合。このパケットの送信元アドレスをゲートウェイ 1 の送り出されるイーサの IP アドレスにする。

戻るパケットの処理

TCP の SYC/ACK パケットの通過許可のルールは、コマンドでは以下で規則が作られる。

iptables …… --state ESTABLISHED,RELATED

上記 state モジュールが、ESTABLISHED・RELATED の状態にあるパケットだけを受け入れる。これは「iptables」のコネクション追跡機能を利用し実現している。(2)　ICMP パケットのエコー応答のパケットの通過許可は ICMP パケット通過許可設定でよい。これらのシミュレーションでは最初に通過したパケットを保存しそのパケットの印と、戻ってくるパケットが同じ印なら通過を許可するとして処理した。このようにコネクション追跡機能のセッションログを模擬した。パケットフィルタでは以下の設定がある場合、戻ってくるパケットを通過させる規則の判定を入れて、処理した。

プロトコルが TCP、オプションが「-m state --state ESTABLISHED,RELATED」

5　おわりに

情報ネットワークをシミュレーションするアプリケーションを制作した。このアプリケーションをネットワークの授業で利用すれば学生はいつでも授業の予習復習を行うことができる。昨年の Android を利用するシステム(1)から改良してシステム開発を行った。

現在はネットワーク 1 だけの動作確認が完了している。ネットワーク 2、実験指導用ネットについても今後開発を進める。実験指導用ネットは LINUX のコマンドを入れて設定するように設計する予定である。

今後ゲートウェイの配置、ハブの配置、ゲートウェイ同士を接続する等の操作を可能にし、ネットワークをユーザー自身が構築できるようにする。昨年開発した Android によるシステムはプログラムが系統だってないという欠点があったので、Android によるシステムの改善も予定している。

（参考文献）

(1) 小俣由太　他 『Android を用いた情報ネットワーク基礎教育システムについて』
教育システム情報学会 全国大会（第 35 回）2010 年 8 月

(2) Iptables チュートリアル 1.2.2 (7 章 ステート機構)
http://www.asahi-net.or.jp/~aa4t-nngk/ipttut/output/index.html