

1 FD Linux を用いたネットワーク学生実験について

— その 1 — ルーティング実験

南 齊 清巳*

井手尾 光臣**

*小山工業高等専門学校 電子制御工学科

**小山工業高等専門学校 技術室

概要 1 枚のフロッピーディスクで動作する 1 FD Linux を用いて、TCP/IP パケット解析実験、ルーティング実験、パケットフィルタリング実験などの各種ネットワーク実験が行える学生用実験システムの構築を試みた。本報では 1 FD Linux をルータとして使用した時の実験方法等について報告する。

1. はじめに

CPU をはじめ、PC の急速な性能向上と Windows 系の OS が必要とするハードウェアリソースの肥大化の相乗効果により、PC は数年で見向きもされずに廃棄されるケースが多くなってきている。これら一線を退いた PC の有効利用を考えたとき、PC UNIX であればまだまだ十分活用が可能と考えた。そこでフロッピーベースで動作する Linux を用い、学生実験用として、TCP/IP パケット解析実験、ルーティング実験、パケットフィルタリング実験、簡易ファイアウォール実験、サーバ構築実験などの各種ネットワーク実験システムとして利用した。その結果、旧型の PC でもこれらの実験には十分活用できる上、学生個人毎にフロッピーでシステムを管理できるため非常に効果的に実験が行えることがわかった。

2. PC-UNIX のディストリビューションの選定

まずフロッピーベースで動作し、ルータとして利用できる PC-UNIX のディストリビューションを探すことから始めた。旧型の PC とは言え、今回使用した PC は CPU が Pentium 75MHz 以上、メモリは 24MB 以上あるのでルータとしての動作には問題が無い。486 程度の CPU でも利用可能であるためほとんどの旧型 PC の再利用が可能である。一番問題となるのはネットワークカード(以下 NIC と呼ぶ)の対応である。ジャンク品の NIC も利用できるよう、できるだけ幅広い NIC に対応したものが望ましい。特に旧型 PC では拡張バスとして ISA バスが多いため NIC の設定 (IRQ および I/O ポートアドレス) が面倒である。これらの点を考慮して今回の目的にかなう PC-UNIX をインターネットで探した結果、次にあげるも

のが候補として挙がった。

(1)LRP

(2)IPnuts3.4⁽¹⁾

(3)FloppyFW

(4)GNAT Box Light(米国GTA社)

上記(1)~(3)はLinux系、(4)はFreeBSD系である。

この中から、(2)のIpnuts3.4を使用することにした。理由は、Ipnuts3.4の開発は国内の「セサミ有限会社」(<http://www.s-me.co.jp>)が行っており日本語のマニュアルが整備されていること、各種設定をWebベースで行えること、対応するNICカードの種類が幅広いことなどである。尚、Ipnuts3.4自体はLRP 2.9.8をベースにしている。Ipnuts3.4には次のような特徴がある。

- LRP 2.9.8 (Linux Router Project <http://www.linuxrouter.org/>)をベースに開発されており、1枚のFDで動作する
- Webブラウザから各種設定ができる
- NATボックスとして使用でき、CATVやxDSLなどの常時接続環境でIPシェアリングを行い、1つのIPアドレスで複数のPCをインターネットに接続できる
- 簡易ローカルルータとして使用できる
- DHCPクライアント機能がある
- LAN側に対してDHCPサーバ機能があり、パソコンのネットワーク設定を自動化できる
- ADSLで利用されるPPPoEに対応している
- ポートフォワードとフィルタリングの機能で簡易ファイアーウォールとして使用できる
- ポートフォワードでまたはNATで内部サーバを公開することができる
- ネットワークカード3枚までサポートしており、DMZセグメントを作ることができる
- シリアルコンソールがサポートされているので、パソコン本体にキーボードやディスプレイが無くても設定できる
- HDDは必要ない
- RAMディスク上で動作するので、面倒なshutdown操作が必要ない
- FDなどはマウントしないので、起動後抜き取っておける
- ブートディスクのフォーマットはDOSなので、パソコンからパッケージをコピーすることで簡単にアップグレードが可能である

3. パケットアナライザ

ネットワーク実験を行う場合、TCP/IPパケットを目に見える形で表示してくれるプロトコルアナライザがあると非常に効果的である。Linux等で使用されているtcpdumpの利用は手軽であるが初心者にとっては表示形式が分かりにくいものとなっている。ここではパケットを非常にわかりやすい形で表示してくれ、しかも広範囲なプラットフォームに対応している「Ethereal」(<http://www.ethereal.com/>)というフリーソフトのプロトコルアナライザを利用した。このソフトを利用するためには「WinPcap」(<http://winpcap.polito.it/>)というフリーのネットワークキャプチャドライバのインストールも必要となる。これらのソフトはWindows95にも対応しているため、旧型のノートPC(Pentium120, メモリ40MB, Windows95)

I FD Linux を用いたネットワーク学生実験について—その1—ルーティング実験

にインストールしてプロトコルアナライザ専用機として利用することにした。ただし、Windows95で使用した場合、パケット取り込み時間の表示が一部正しく表示されない。原因は不明であるが、実験には大きな支障が無いのでそのまま使用している。

4. 機器およびソフトウェア構成

使用したPC、HUB等はすべて一線を退いた旧型の機器ばかりである。PCは故障してもすぐに代用機に替え、フロッピーで立ち上げられるので安心して実験が行える。

- PC(ルータ用2台、通信確認用2台)
- NIC(NE2000互換、sis900他)
- IPnuts 3.4 (1 FD Linux)
- ノートPC(Pentium120, メモリ40MB)
パケットキャプチャー用
- パケットアナライザ(Ethereal)
- HUB(リピータハブ)3台

5. Ipnuts3.4の基本設定

(1) Ipnuts3.4のIPアドレス、ネットマスク等の設定を行う。Ipnuts3.4でWebadminを使用することにより、ブラウザから簡単に設定が行える。図1にWebadminの基本設定画面を示す。

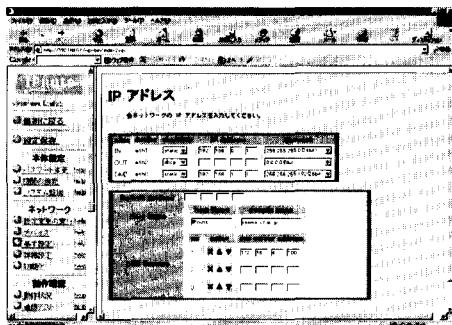


図1 Webadminの基本設定画面

(2) ネットワーク設定の確認

現在のIpnuts3.4のネットワーク設定、ルーティングテーブル、パケットフィルタ等の設定状況はWebadminによって確認することができる。図2にWebadminによる現在のネットワーク設定状況の表示例を示す。

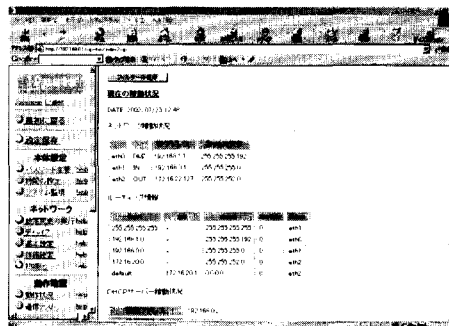


図2 現在のネットワーク設定状況の表示

6. 実験内容

実験1 簡単なLANの構成

目的

単純なLANを構成することによって、TCP/IPにおけるIPアドレスとネットマスクの意味とその設定方法を学習する。また、PCの設定内容を確認するためのipconfigコマンドと通信確認のためのpingコマンドの使用方法について学習する。

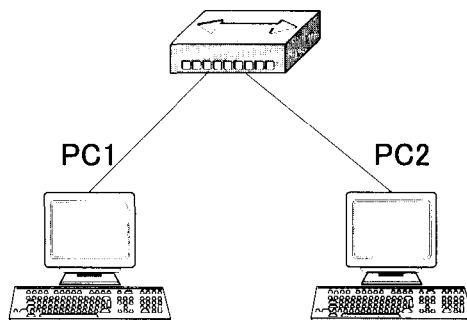
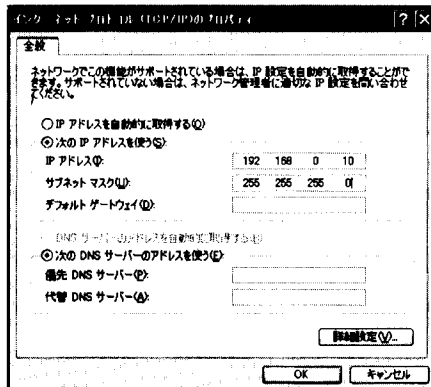
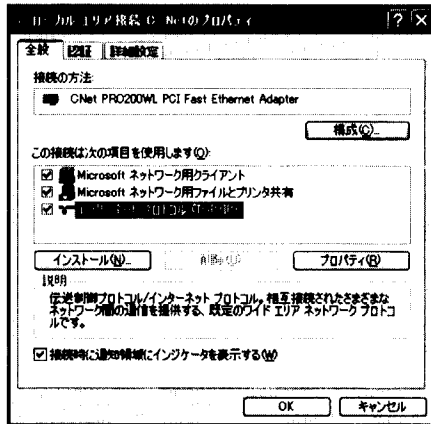


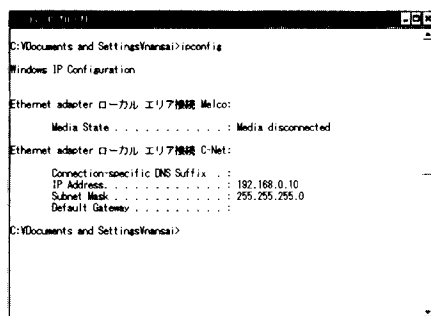
図3 簡単なLANの構成

実験方法

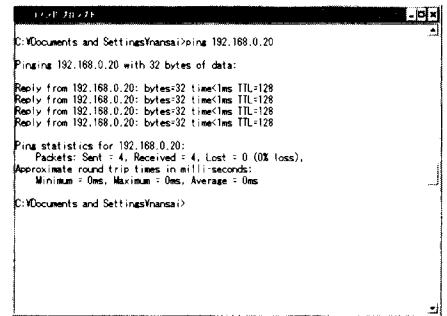
- (1) 図1に従いPCとHUBを接続する
- (2) PC 1およびPC 2にIPアドレスおよびネットマスクを設定する。



- (3) それぞれのPCの設定が終わったら ipconfig コマンドを用いて設定内容を確認する。



- (4) PC 1 から PC 2 に対して ping コマンドを用いて通信確認を行う。



- (5) 同様に PC 2 から PC 1 に対して通信確認を行う。

発展課題

- (6) PC 1 のネットマスクと PC 2 のネットマスクが異なった場合、通信が行えるかどうか試してみよ。
- (7) 正しく通信が行えるためには IP アドレスとネットマスクはどのように設定したらよいのか考えてみよ。

実験 2 LAN 同士の接続

目的

ネットワークアドレスの異なる LAN 同士を相互接続し、通信が行えるようにするためにはパケットの経路選択を行うためのルータが必要となる。ルータは TCP/IP ネットワークにおける最も重要な役割を持つネットワーク機器である。この実験ではルータの基本的な働きを学習するとともに PC にデフォルトゲートウェイアドレスを設定する方法を学習する。

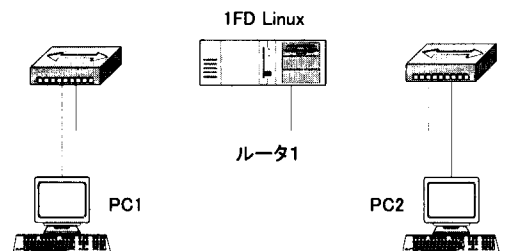


図 4 LAN 同士の接続

1 FD Linux を用いたネットワーク学生実験について—その1—ルーティング実験

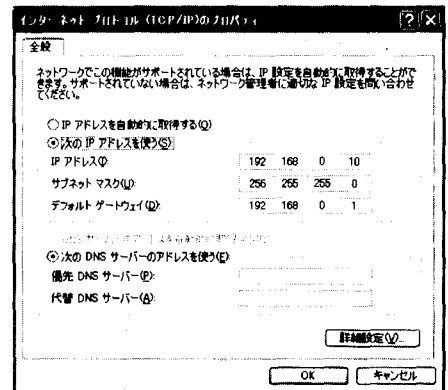
実験方法

- (1) 図4に従い、PC、ルータ1およびHUBを接続する。このときルータとして使用するPCには3枚のインターフェースカード(このうち2枚がアクティブに設定されている)が装着されているので間違えないように接続すること。
- (2) ルータ1のPCにIpnuts3.4フロッピーディスクを挿入し起動する。各インターフェースカードのIPアドレスとネットマスクは次のように設定されている。

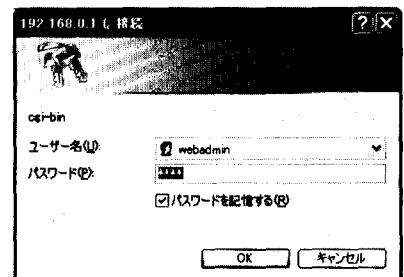
	ルータ1	
	eth 0	eth 1
IPアドレス	192.168.0.1	192.168.1.1
ネットマスク	255.255.255.255	255.255.255.255

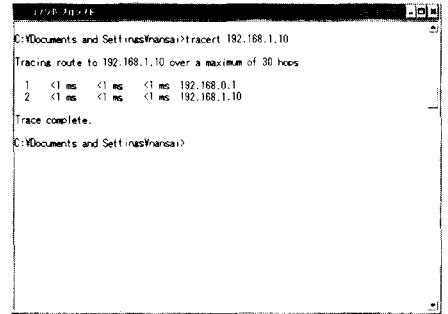
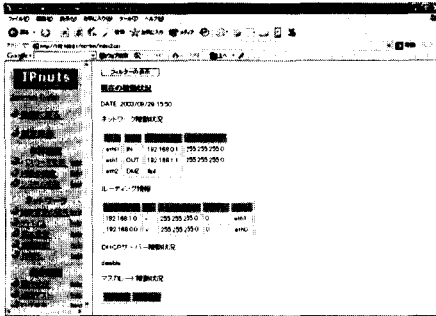
- (3) PC1およびPC2に対して次のネットワーク設定を行う。

	PC 1	PC 2
IPアドレス	192.168.0.10	192.168.1.10
ネットマスク	255.255.255.255	255.255.255.255
デフォルトゲートウェイ	192.168.0.1	192.168.1.1

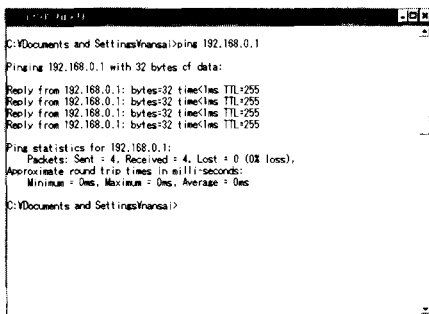


- (4) PC1からルータ1のeth0へpingを打ち、通信可能なことを確認する。同様にPC2からルータ2のeth1へpingを打ち、通信可能なことを確認する(もし、うまく通信できないときはルータのIPアドレスまたはネットマスクが正しく設定されていない可能性がある。このときは別のフロッピーから起動しなおすこと)
- (5) PC1上で「Internet Explorer」を起動しURLhttp://192.168.0.1/に接続するとルータ1の設定画面が表示される。同様にPC2上で「Internet Explorer」を起動しURLhttp://192.168.1.1/に接続するとルータ2の設定画面が表示される。





- (6) ルータの設定画面の左側メニュー上で「動作確認」-「動作状況」をクリックしルータの動作状況を確認する。
- (7) PC 1 のコンソール画面から ping コマンドを使用し、PC 2 と通信できることを確認する。同様に、PC 2 のコンソール画面から ping コマンドを使用し、PC 1 と通信できることを確認する。うまく通信できないときは自分の使用している PC から近い方のインターフェースに対して ping を使用し通信確認を行っていくことによってどのインターフェースの設定が悪いのかを特定することができる。



- (8) tracert コマンドを使用して、どのような経路でパケットが PC 1 から PC 2 まで届くかを表示させる。

発展課題

- (1) PC 上のデフォルトゲートウェイが設定されていなかったら(または間違っていたら)どうなるか試してみよ。

実験3 より複雑なネットワークの構成

目的

この実験ではルータ 2 台を使用して、3 つの異なるネットワークを相互に接続し、通信できるようにする。またルータの経路情報を静的(手動)に設定する方法と、RIP プロトコルで動的に設定する方法について実験を行い、その動作を確認するとともに、ルーティングの働きをより深く学習する。

実験方法

- (1) 図 3 に従い、PC、ルータおよび HUB を接続する。このときルータとして使用する PC には 3 枚のインターフェースカード(このうち 2 枚がアクティブに設定されている)が装着されているので間違えないように接続すること。
- (2) ルータ 1 およびルータ 2 の PC に Ipnuts3.4 フロッピーディスクを挿入し起動する。このとき、ルータ 1 用のフロッピーとルータ 2 用のフロッピーを間違えないこと。
- 各インターフェースカードの IP アドレス

1FD Linux を用いたネットワーク学生実験について—その1—ルーティング実験

とネットマスクは次のように設定されている。

	ルータ 1		ルータ 2	
	eth 0	eth 1	eth 0	eth 1
IP アドレス	192.168.0.1	192.168.1.1	192.168.1.2	192.168.2.1
ネットマスク	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

(3) PC 1 および PC 2 に対して次のネットワーク設定を行う。

	PC 1	PC 2
IP アドレス	192.168.0.10	192.168.2.10
ネットマスク	255.255.255.0	255.255.255.0
デフォルトゲートウェイ	192.168.0.1	192.168.2.1

- (4) PC 1 からルータ 1 の eth 0 へ ping を打ち、通信可能なことを確認する。同様に PC 2 からルータ 2 の eth 1 へ ping を打ち、通信可能なことを確認する(もし、うまく通信できないときはルータの IP アドレスまたはネットマスクが正しく設定されていない可能性がある。このときは別のフロッピーから起動しなおすこと)
- (5) PC 1 上で「Internet Explorer」を起動し URL `http://192.168.0.1/` に接続するとルータ 1 の設定画面が表示される。同様に PC 2 上で「Internet Explorer」を起動し URL `http://192.168.1.1/` に接続す

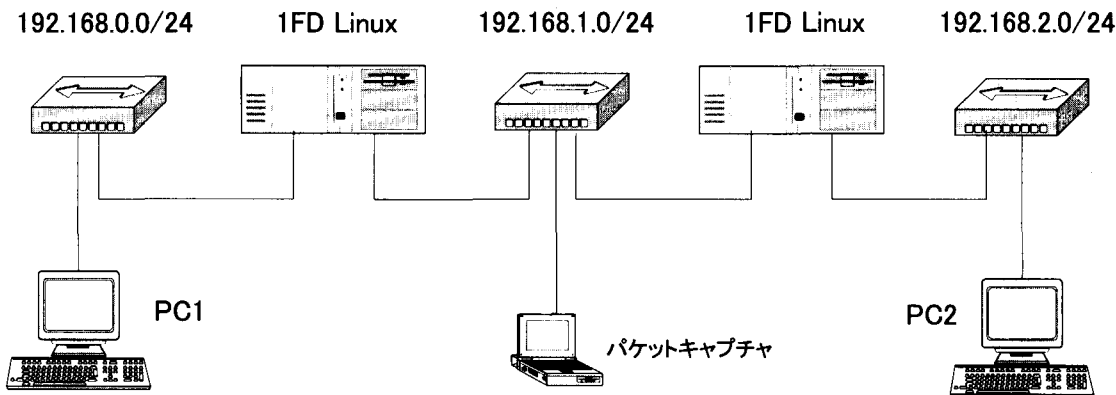


図5 より複雑なネットワークの構成

るとルータ 2 の設定画面が表示される。

- (6) ルータの設定画面の左側メニュー上で「動作確認」-「動作状況」をクリックしルータの動作状況を確認する。

[静的ルーティング]

- (7) ルータ設定画面の左側メニュー上で「ネットワーク」-「詳細設定」を選択し、さらに上部メニューから「Routing」を選択する。IP Routing 設定画面で次のように設定する。

192.168.2.0	192.168.1.2	255.255.255.0	0	eth1
192.168.1.0	x	255.255.255.0	0	eth1
192.168.0.0	x	255.255.255.0	0	eth0

- (8) ルータ設定画面の左側メニュー上で「ネットワーク」-「詳細設定」を選択し、さらに上部メニューから「Routing」を選択する。IP Routing 設定画面で「 rip enable」にチェックを入れる。
- (9) OK ボタンを押してから画面左側メニュー上の「ネットワーク」-「設定変更の実行」をクリックする。この操作を行わないと設定内容が反映されないので注意すること。
- (10) PC 1 のコンソール画面から ping コマンドを使用し、PC 2 と通信できることを確認する。同様に、PC 2 のコンソール画面から ping コマンドを使用し、PC 1 と通信できることを確認する。うまく通信できないときは自分の使用している PC から近い方のインターフェースに対して ping を使用し通信確認を行っていくことによってどのインターフェースの設定が悪いのかを特定することができる。

- (11) tracert コマンドを使用して、どのような経路でパケットが PC 1 から PC 2 まで届くかを表示させる。

[動的ルーティング RIP]

- (12) ルータ設定画面の左側メニュー上で「ネットワーク」-「詳細設定」を選択し、さらに上部メニューから「Routing」を選択する。IP Routing 設定画面で「 rip enable」にチェックを入れる。
- (13) OK ボタンを押してから画面左側メニュー上の「ネットワーク」-「設定変更の実行」をクリックする。この操作を行わないと設定内容が反映されないので注意すること。
- (14) ルータの動作状況を表示させルーティングテーブルの状態を確認すること。RIPでは経路情報は30秒毎に更新されるので、最初は正しいルーティングテーブルが表示されないことがあるので注意すること。
- (15) PC 1 のコンソール画面から ping コマンドを使用し、PC 2 と通信できることを確認する。同様に、PC 2 のコンソール画面から ping コマンドを使用し、PC 1 と通信できることを確認する。うまく通信できないときは自分の使用している PC から近い方のインターフェースに対して ping を使用し通信確認を行っていくことによってどのインターフェースの設定が悪いのかを特定することができる。
- (16) tracert コマンドを使用して、どのような経路でパケットが PC 1 から PC 2 まで届くかを表示させる。

1 FD Linux を用いたネットワーク学生実験について—その1—ルーティング実験

発展課題

- (1) 動的ルーティングの実験の際に HUB 2 にパケットキャプチャー用 PC を接続してルータ 1—ルータ 2 間に流れるパケットをキャプチャしてみる
- (2) RIP パケットが定期的に流れるがその時間間隔を調べてみよ。

実験 4 パケットフィルタリング

目的

ルータにはパケットを中継する際に IP アドレスやポート番号を基にパケットをフィルタリングする機能がある。ネットワークのセキュリティを向上させるためには欠かせない機能である。この実験では telnet のアクセスを制限するようなフィルタリングルールを設定し動作を確認するとともにフィルタリングの考え方を学習する。

実験方法

- (1) ネットワーク構成は実験 3 で使用したものをそのまま使用する。
- (2) ルータ 1 の設定画面で画面左側メニュー上で「ネットワーク」-「詳細設定」を選択する。さらに画面上部のメ

ニューから「IP Filter」を選択する。

- (3) 「Packet Filter:」の設定画面で次のように設定する。

フィルタリング条件

PC 1 から 192.168.2.0/24 のネットワークに対して telnet 接続を禁止する。尚 telnet の使用するポート番号は 23 番である。

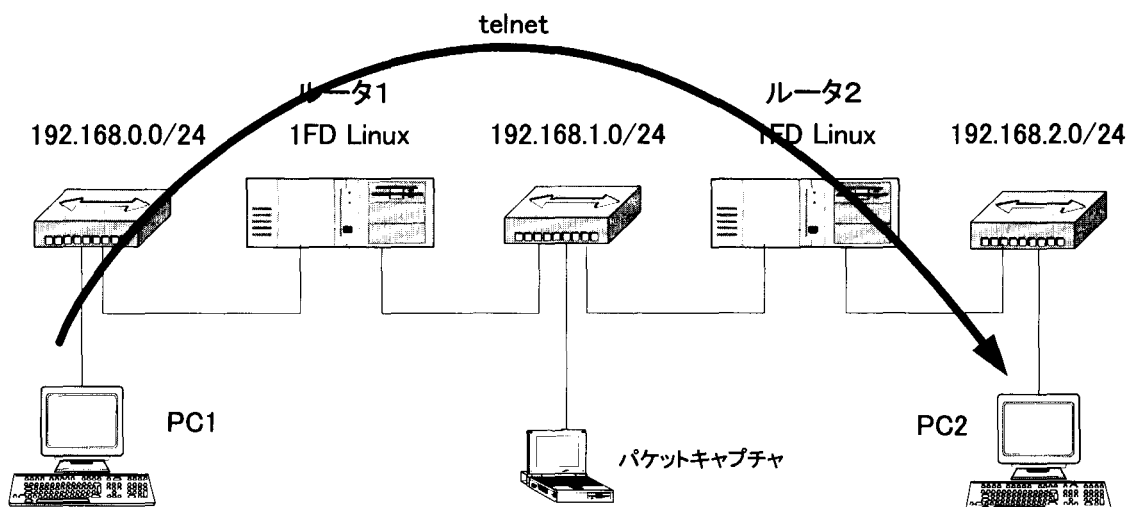
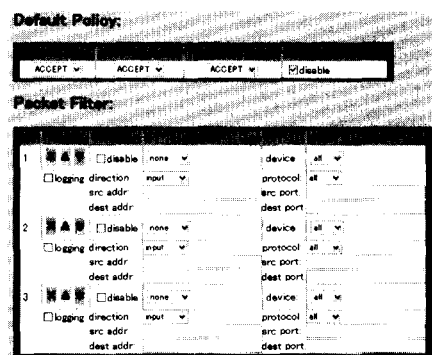
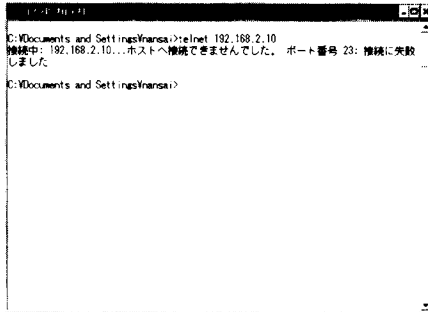


図 6 パケットフィルタリング

- (4) PC 1 から PC 2 に対して telnet 接続する。このときフィルターがかかっているため接続に失敗する。



```
C:\Documents and Settings\masa>telnet 192.168.2.10
接続中: 192.168.2.10...ホストへ接続できませんでした。 ポート番号 23: 接続に失敗
しました
C:\Documents and Settings\masa>
```

7. まとめ

旧型の PC とフロッピーベースで動作する 1 FD Linux を使い、各種ネットワーク実験が行える実験システムの構築を試みた。今回はルーティング実験を中心に実験方法と結果について述べた。旧型の PC でも十分学生実験に利用可能な上、学生個人毎にフロッピーでシステムを管理できるため、非常に効果的に実験が行える。今後はネットワークアドレス変換やファイアーウォール実験も行なっていきたい。

参考文献

「IPnuts 3.4.x マニュアル」セサミ有限会社
オーム社「TCP/IP セキュリティ実験」寺田
真敏・萱島 信

〔受理年月日 2003 年 9 月 30 日〕