

知能情報工学実験 II-4 ネットワークの構築

担当: 徳久雅人(tokuhisa@ike.tottori-u.ac.jp)
実験場所: 7452室(大学院棟4階)
実験日: 平成16年4月20, 27日 / 6月15, 22日(3~5限目)
準備: フロッピーディスク1枚(実験結果等の運搬用)

1. 実験の目的

計算機ネットワークを構築する際、次の3つが重要である。

- 1) 通信が行えること
- 2) ネットワークを介したサービスが授受できること
- 3) 不正なアクセスを排除すること

知能情報工学実験 II では、これらの3点について2週ずつ実験・演習を行う。

本実験では、TCP/IP による計算機ネットワークの通信の確立に主眼をおいたネットワークの構築を目的とする。具体的には、まず、TCP/IP によるネットワークの基本的な用語について確認し、次に、IP アドレスおよびルーティングに関する設定を実習する。

2. 用語説明

2.1. TCP/IP プロトコル

データ通信で運ばれる単位的なものを**パケット**という。通信先などが記述されたヘッダ部分と通信内容の部分から成る。パケットの読み方・作り方ははじめ通信のための手順などの規約を**プロトコル**という。プロトコルでは、機能のレベルで分類されている。この分類の標準として、OSI(Open Systems Interconnection)参照モデルがあり、7階層が定義されている。しかし、本実験では、実践的な入門として **TCP/IP プロトコル**^{*1} の4階層のモデルについて取り上げる。

TCP/IP プロトコルには、**ネットワーク層**、**インターネット層**、**トランスポート層**、および、**アプリケーション層**という4つがある。表1に機能とプロトコルの例をまとめる。

表1: TCP/IP プロトコルの機能とプロトコルの例

プロトコル階層	規約の内容	プロトコルの例
アプリケーション層	アプリケーションのための規約	HTTP, SMTP, POP, FTP
トランスポート層	データを正しく送信するための規約	TCP, UDP, SSL
インターネット層	通信相手を保証するための規約	IP, DHCP
ネットワーク層	物理的な通信媒体ごとの規約	Ethernet, PPP, アナログモデムの規約

プロトコル階層の名称に OSI 参照モデルと重複があり混乱しやすいので、十分に注意すること。

2.2. 通信経路の確立

表1の各階層のプロトコルは、下の層の機能を前提にして設計されている。ネットワーク層およびインターネット層の設定が完了すれば、基本的には通信経路の確立ができたことになり、通信内容の伝達漏れなどはトランスポート層の問題となる。本節では、ネットワーク層およびインターネット層について説明する。

イーサネットによるネットワークを構築する際、ネットワーク層に関する機器には、イーサカード(ネットワークカード)、ネットワークケーブル、ハブなどがある。イーサカードには、**MAC アドレス**というカードに固有の番号が付けられている。

*1TCP/IP プロトコルとは、幾つかのプロトコルの総称である。文献によってはプロトコルの意味の混乱を避けるために、TCP/IP アーキテクチャとよんでいるものもある。

インターネット層に関しては、やはりイーサカードごとに **IP アドレス** という固有の番号が付けられる。MAC アドレスがハードウェアに付けられた番号であることに対して、IP アドレスは、ネットワーク上の場所ごとにつけられた番号と理解してよい。IP アドレスは、ある計算機と通信をするために使われる。通信データは、パケットの単位に分割され、パケットリレーのようにしてネットワーク上の計算機から計算機へと転送される。計算機は、パケットに記載された送信先の IP アドレスを見て、わかる範囲で次の転送先を決める。このことを **ルーティング** という。転送に関する情報は **ルーティングテーブル** に記載しておく。ネットワーク上の計算機は、グループで管理される。これを **ドメイン** という。同一のドメインでは、IP アドレスの上位桁の数が共通である。これを **ネットワークアドレス** という。どの桁が共通であるのかを表すものに **ネットマスク** がある。ドメインの異なる計算機と通信するには、**ルーター** という仲介役の計算機(あるいは専用機)を経由する。ここで、プロトコルの異なるドメイン間の仲介が必要な場合がある。この場合の仲介役は **ゲートウェイ** という。ゲートウェイは機能面でいえばルーターを含むので、実際の場面では、ルーターの機能しか使っていないくてもゲートウェイと呼ぶことがある。

また、人間が計算機を扱う上で、数字の羅列では理解し難くなるので、IP アドレスには **ホスト名** や **ドメイン名** が対応付けられている。

ネットワークの構築者は、IP アドレスの割り当て、デフォルトの転送先などルーティングの設定、ホスト名やドメイン名の割り当て、あるいはこれらの自動割当てのための設定を行う。

2.3. ネットワーク上のサービス

ネットワークサービスは、ネットワークの管理・運営のためのサービスから一般ユーザのためのサービスまで広範にある。前者の例を幾つかあげる。

- **DHCP** : IP アドレスを計算機に自動的に割り当てる。
- **DNS** : ホスト名、ドメイン名から IP アドレスを検索する。あるいは、逆にホスト名などを検索する。
- **routerd** : ルーティングテーブルを自動生成する。
- **YP** **あるいは NIS** : ログインアカウントの共通化

後者の例を幾つかあげる。

- **NFS** : ネットワークを介したファイルの共有
- **HTTPD** : WWW によるデータの公開

これらのサービスの多くは、**サーバ&クライアント**の関係で成り立っている。クライアントはサービスの恩恵を受ける側、サーバはサービスを提供する側である。単純なサーバは、計算機上で常にプログラムが動いており、クライアントから要求の通信が入ることを待っている。この要求を受ける窓口を **ポート** という。ポートは、OS のインストール時に既に定義されたものがある。/etc/services ファイルからその定義が一覧できる。

2.4. セキュリティー

ネットワーク上の計算機は、同ドメイン内の計算機からの不正アクセス、および、外部ドメインの計算機から、あるいは外部計算機への不正アクセスがある。同ドメイン内の場合、/etc/hosts.deny ファイルによるリモートアクセスの制限や、不要なサーバ(デーモン)の停止などにより自衛がある。外部ドメインとの関係の場合、特定パケットの遮断やポートの開閉などの対策があり、**ファイアウォール**が使われる。

ファイアウォールは、外部ドメインと内部ドメインの境界に設置される。

- **パケットフィルタリング**: パケットの発信元 IP アドレス・ポート、および、発信先 IP アドレス・ポートに基づき、特定のパケットの転送を中止させる。
- **プロキシ**: http や ftp などのネットワークサービスを特定のユーザだけに提供する。ユーザは目的のホストからサービスを受けているように見えるが、プロキシが代理で目的のホストからサービスを受けてユーザに伝える。

3. ネットワークの構築方法

3.1. ネットワーク層とインターネット層から見たネットワーク

本実験に関連する事柄について、図1を参照しながら概説する。詳細は次節以降で述べる。

図1は、LAN-1 という局所ネットワーク(LAN; Local Area Network)と外部ネットワーク接続の構築例である。影付きのボックスは、インターネット層の情報であり、それ以外はネットワーク層の情報である。

LAN-1 には、PC10、PC11、PC12 という3台の計算機と2つのハブがある。

PC10とPC11には、それぞれ1枚のイーサカードが装着されている。PC12には、2枚のイーサカードが装着されている。イーサカードの1枚目、2枚目にeth0、eth1というラベルがつく。イーサカードごとに、IPアドレスとネットマスクが設定されている。

計算機とハブは、LANケーブルで接続されている。また、ハブとハブもLANケーブルで接続されている。ハブは、ネットワーク層で接続する装置であり、これをリピータという。

PC10はeth0を通じてHUB1と接続されている。PC10が出力するパケットが、「192.168.1.xx」宛てならば単にeth0から出力する。また、その他に送信する場合は「default」とされるIPアドレスのある計算機に送られる。このように、送信先、IPアドレス、および、イーサカードのラベルとの関係は、ルーティングテーブルに表され、各計算機に設定されている。

PC12はルーターである。eth0を通じてHUB2と、eth1を通じて外部ネットワークと接続されている*1。

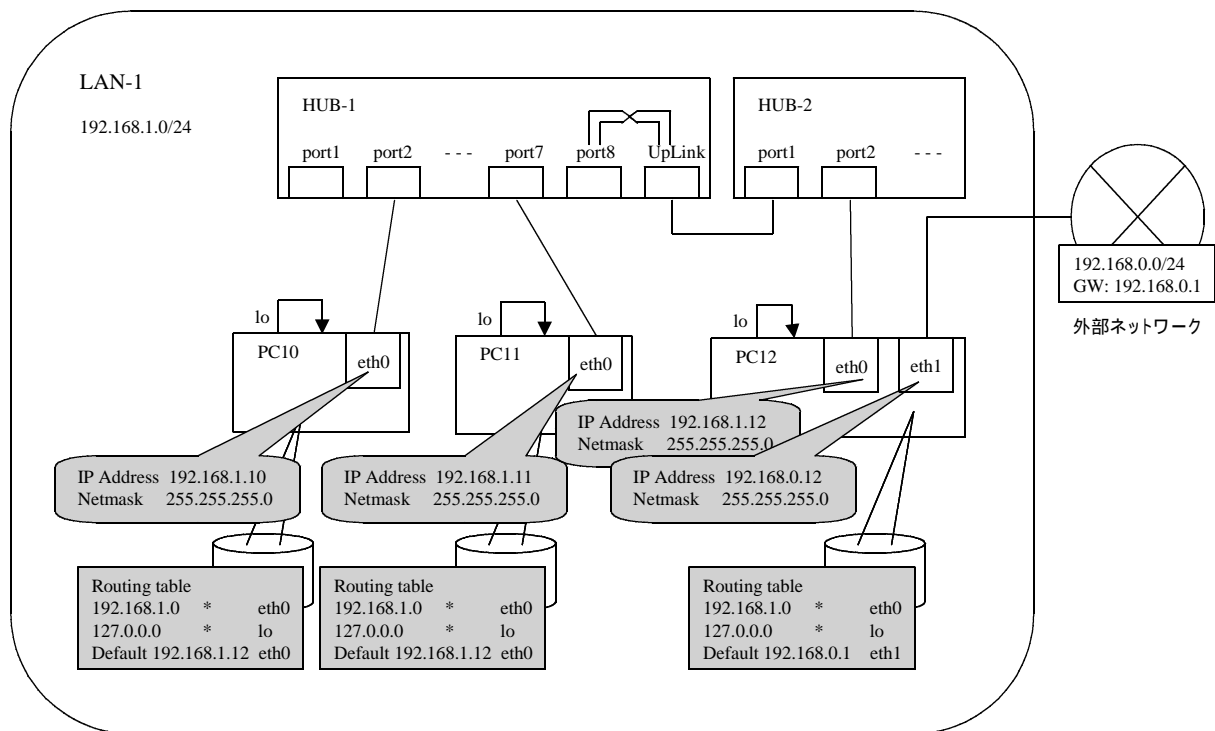


図1: 各種設定・接続の例

3.2. ハードウェアの接続

3.2.1. ネットワークデバイス

計算機をネットワークに接続する装置をネットワークデバイスという。イーサカードが最もポピュラーである。イ

*1 詳しくいうと、外部ネットワーク内のハブに接続される。

ーサカードは、計算機の拡張スロットに接続するタイプ、マザーボードに直接備わっているタイプなどがある。
自分自身に接続する仮想的なネットワークデバイスがあり、lo(Local Loopback Device)という。

3.2.2. ネットワークケーブル・ハブ

ネットワーク層において、機器を接続する装置をリピータという。ハブは、100BASE-TX や 10BASE-T で使用するツイストペアケーブルを集積接続する機器である。

ハブには、**ポート**^{*1}と呼ばれるケーブルの差し込み口が複数個ある。ある1つのポートから入力されたパケットは残りのポートから出力される^{*2}。こうしてハブは、計算機同士を接続することができる。

(1) コリジョン

複数のポートから同時にデータが入力された場合をコリジョンという。同時に入力されたデータは壊れているので、入力のあったポートからコリジョン信号が返される。

(2) ハブ同士の接続(カスケード接続)

接続する計算機の量が多い場合ポートが不足する。その場合、ハブとハブを LAN ケーブルで接続し、ポート数を増やすことができる。これを**カスケード接続**という。

計算機とハブとを結ぶ LAN ケーブルは、ストレートケーブルを用いる。一方、ハブとハブとを結ぶ場合、通常のポート同士ならばクロスケーブルを用いる。しかし、ストレートケーブルとクロスケーブルは外観から見分け難いため、実際にネットワークを管理する現場では、両ケーブルを同時に用いることは避けたい。そこで、ハブ間をストレートケーブルで結ぶために「カスケードポート(Up-Link ポートともいう)」がある。このポートは内部でクロスケーブルに変換する結線が施され、一般には最終ポートと結びついている。

接続方法は、ハブのカスケードポートにストレートケーブルを差し込み、ケーブルのもう一方をもう1つのハブの通常のポートに差し込む。

カスケード接続には台数の制限がある。10BASE-T の場合、ハブ間のケーブルの距離は 100m まで、接続台数は 4 台までである。100BASE-TX の場合、ケーブルの距離は 100m まで、接続台数は 2 台までである。これは、コリジョンを検出するための時間幅とデータ転送の遅延時間の関係に依る。

3.3. IP アドレス

3.3.1. 一時的な設定と確認

ifconfig コマンドは、イーサカードの設定に使う。表2に一覧を示す。

表2: ifconfig コマンドの使用例

機能	使用例	説明
設定確認	<code>ifconfig eth0</code>	イーサカード eth0 の状態を表示する。割り当てられている IP アドレスは「inet addr:192.168.0.18」のように表示される。稼動中であることは「UP」と表示される。
割り当て	<code>ifconfig eth0 inet 192.168.0.18 netmask 255.255.255.0</code>	イーサカード eth0 に IP アドレスおよびネットマスクを割り当てる。
停止	<code>ifconfig eth0 down</code>	イーサカード eth0 の動作と止める。
再開	<code>ifconfig eth0 up</code>	イーサカード eth0 の動作を開始する。

ifconfig コマンドで設定した IP アドレス等は、計算機をリブートすると失われる。

ping コマンドは、ネットワークにパケットを送ることで、通信状態を確認する。

使用例 `ping 192.168.0.17`

*1 サーバ&クライアントシステムにて TCP や UDP で用いるポートとは同名であるが、異なる物である。

*2 スイッチングハブは、必要なポートにのみ出力する。

表示の意味は以下の通りである。

- 受信したバイト数, 送信シーケンス番号 (comp_seq), 有効期限 (ttl), 応答時間 (ms)
- 送信したパケット数, 受信したパケット数, 受信できなかったパケットの割合 (%), 応答時間の最大値 / 平均値 / 最小値

Ctrl+c で終了する。

3.3.2. 恒久的な設定

Linux には, 幾つかのディストリビューションがある。2年生後期に行った知能情報工学実験 I での OS インストールでは「VineLinux」を用いた。Linux のディストリビューションには Slackware Linux 系, Red Hat Linux 系, Debian GNU/Linux 系などの系列があり, システムの設定ファイルは, 系列ごとに異なるところがある。Vine Linux は, Red Hat Linux 系に属する。本実験書では, Vine Linux をベースに説明する。

計算機のブート時には, 下記の設定ファイルに従って eth0 が設定される。設定項目を表3にまとめる。

- /etc/sysconfig/network-scripts/ifcfg-eth0

表3: ifcfg-eth? ファイルの設定項目

項目名	内容	例
DEVICE	ネットワークデバイス名	DEVICE=eth0
ONBOOT	yes または no	ONBOOT=yes
BOOTPROTO	static または dhcp	BOOTPROTO=static
IPADDR	IP アドレス	IPADDR=192.168.0.47
NETMASK	ネットマスク	NETMASK=255.255.255.0
GATEWAY	IP アドレス	GATEWAY=192.168.0.7

3.4. ルーティング

3.4.1. 一時的な設定と確認

route コマンドで, ルーティングテーブルを編集する。パケットの送信先の IP アドレスに応じて経路を指定する。使用例を表4にまとめる。

表4: route コマンドの使用例

使用例	説明
route -n	現在のルーティングテーブルの内容を表示する。
route add -net 192.168.1.0 netmask 255.255.255.0 eth0	送信先が 192.168.1.?? ならば eth0 から転送する。
route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.0.1	送信先が 192.168.1.?? ならば 192.168.0.1 に任せる。
route add default gw 192.168.0.1	その他の送信先ならば, 192.168.0.1 に任せる。
route del -net 192.168.1.0 netmask 255.255.255.0	192.168.1.?? に対するルーティングの情報を削除する
route del default	デフォルトゲートウェイの設定を削除する

ゲートウェイとなる計算機は, パケットを受信し他へ転送しなければならない。ゲートウェイでない計算機はその必要がない。そこで, パケット転送をするかしないかの設定がある(表5)。

表5:パケット転送の設定例

使用例	説明
echo 1 > /proc/sys/net/ipv4/ip_forward	パケット転送をする.
echo 0 > /proc/sys/net/ipv4/ip_forward	パケット転送をしない.

route コマンドおよび表5の設定は、計算機をリブートすると失われる。

traceroute コマンドは、指定する計算機までのルーティングの情報を出力する。情報の意味は以下の通りである。

- 経路の終点となるホストの名前と IP アドレス, 最大通過ルータ数 (hop 数)
- ルータのレスポンス時間 (3 回分)
途中で止めず, しばらく待つこと。

3.4.2. 恒久的な設定

ルーティングテーブルのうち、デフォルトゲートウェイ以外については、`/etc/sysconfig/static-routes` ファイルに定義する。図2のように設定すると、「`route add -net 192.168.3.0 netmask 255.255.255.0 gw 192.168.11.3`」および「`route add -net 192.168.8.0 netmask 255.255.255.0 gw 192.168.12.8`」を実行するのと同じ効果が得られる。

```
any net 192.168.3.0 netmask 255.255.255.0 gw 192.168.11.3
any net 192.168.8.0 netmask 255.255.255.0 gw 192.168.12.8
```

図2: static-routes ファイルの具体例

デフォルトゲートウェイを指定するには、表3の GATEWAY を記入すればよい。

パケット転送の設定は、`/etc/sysctl.conf` ファイルにおいて、`net.ipv4.ip_forward` の値を書き換えればよい。

3.5. 初期化

linux を起動するとき実行されるプログラムは、`/etc/inittab` に登録されているサブプログラムである。ネットワークの設定を行うサブプログラムは、`/etc/rc.d/init.d/network` である。ネットワークの設定を起動時の状態に変更するためには、以下を実行すればよい。

- `/etc/rc.d/init.d/network restart`

一時的な設定は取り消され、恒久的な設定が有効になる。

ちなみに、ネットワークの機能を停止するには「`stop`」、開始するには「`start`」、を指定すればよい。

4. 実験課題

4.1. 課題1:カスケード接続時の ping の応答時間

3人で1つのグループを作り、図3のネットワークを以下の仕様にしながら構築せよ。

- 設定は一時的とする。
- ハブ間をカスケード接続する。
- PCmi の eth0 を用いる
- PCmi の IP アドレスは、「`192.168.10.mi`」とする。
- PCm3 ダッシュは、PCm3 の LAN ケーブルを差し替えたものとする。

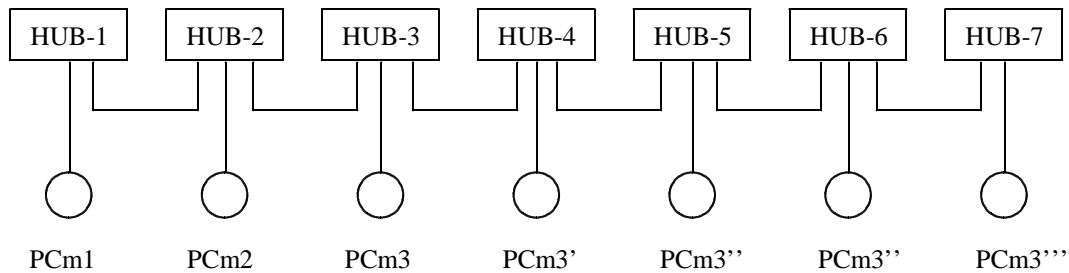


図3:課題1ネットワーク

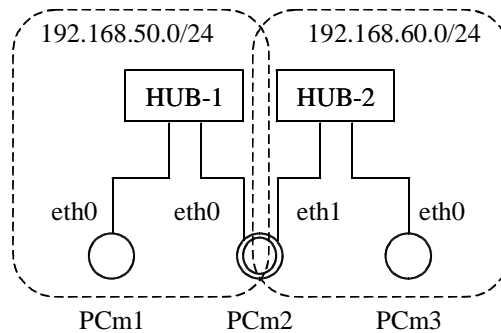
報告事項1

- (1) PCm1 の ifconfig eth0 の結果
- (2) PCm1 から PCm3 への ping の結果
- (3) PCm1 から PCm3 への ping および PCm2 から PCm3 への ping を同時に実施した際の ping の応答時間
- (4) PCm1 から PCm3', PCm3'', PCm3'''へのそれぞれの ping の応答時間

4.2. 課題2:ゲートウェイ経由での ping の応答時間

3人で1つのグループを作り,図3のネットワークを以下の仕様にしたがって構築せよ.設定は一時的とする.

- 一時的な設定とする.
- 2つのLANを構築する.LAN1は「192.168.50.0/24」,LAN2は「192.168.60.0/24」とする.
- PCm2をゲートウェイとする.eth0はLAN1と接続し,eth1はLAN2と接続する.
- PCm1およびPCm3は,eth0を使う.



192.168.50.m1 192.168.50.m2 192.168.60.m2 192.168.60.m3

図4:課題2ネットワーク

報告事項2

- (1) PCm1, PCm2, PCm3 の route -n の結果
- (2) 次の3つの条件での ping の結果
 - PCm1 から PCm2(eth0)へ
 - PCm1 から PCm2(eth1)へ
 - PCm1 から PCm3 へ
- (3) (2)と同じ条件での traceroute の結果

4.3. 課題3 : 小規模 LAN の構築

以下の仕様にしたがって、5人で1つの LAN を構築する。

- 図5は実験室の配置と対応し、図5の左側が実験室の西側になる。各 LAN は、図の左側から順に LAN-1, LAN-2, LAN-3, ..., LAN-6 とよぶ。
- 恒久的な設定とする
- LAN-n のネットワークアドレスは「192.168.n.0/24」とする。
- ホストの IP アドレスは、PCm に従い、「192.168.n.m」とする。eth0 に割り当てる。
- LAN-1 から LAN-6 まで、「192.168.10.0/24」のドメインで接続する。つまり、ゲートウェイの eth1 にはこのドメインを割り当てる。また、LAN-n のゲートウェイの IP アドレスは、「192.168.10.n」として、eth1 に割り当てる。

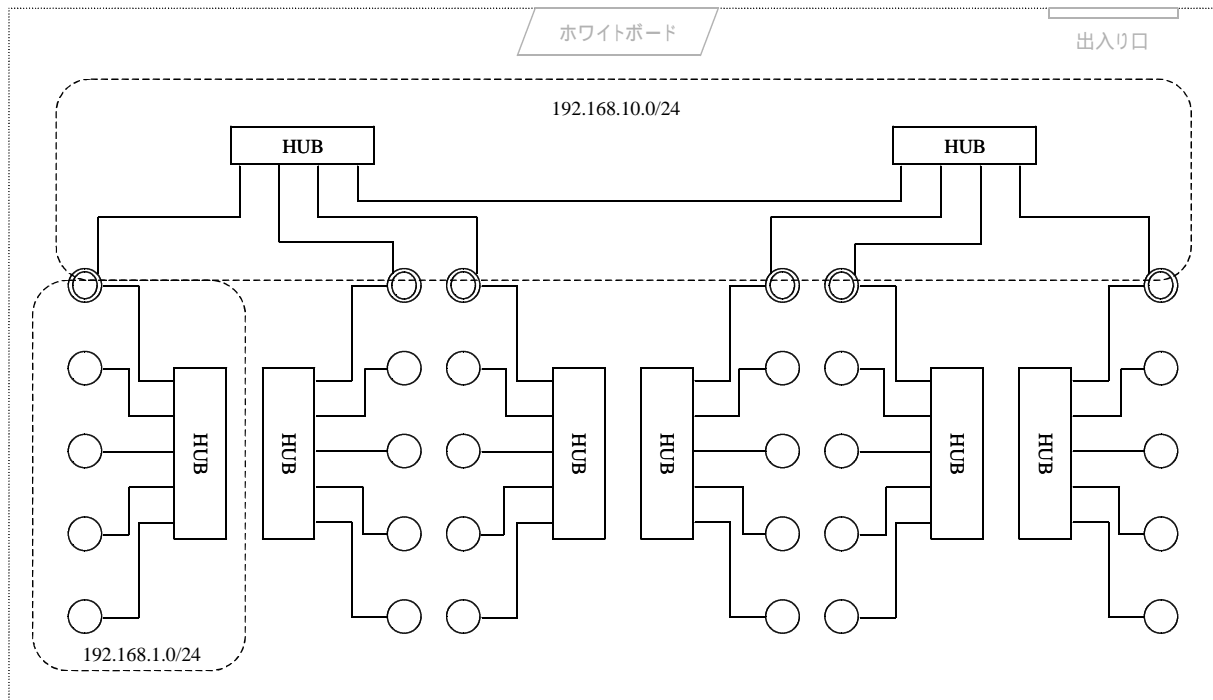


図5：課題3ネットワーク

報告事項3

- (1) ゲートウェイで設定した内容
- (2) ゲートウェイ以外の計算機で設定した内容
- (3) LAN-n 内での ping および traceroute の結果
- (4) となりの LAN 内のゲートウェイ以外の計算機間の ping および traceroute の結果

5. レポートの作成要領

レポートは各自が1部作成する。A4用紙に、鉛筆やボールペンによる手書き、または、ワープロによる印刷とする。枚数制限はない。表紙には、実験テーマ名、実験日、レポート提出日、氏名、学籍番号、班名を書く。左上の一箇所をステープラなどで綴じる。

レポートの章立ての例を以下に示す。

第1章 . 実験の目的

第2章 . 実験機材の説明

第3章 . 課題の概要と結果

第4章 . 考察

参考や引用した文献や Web ページがあれば「参考文献」の章を設けて紹介する .

また , 今後の参考のために「感想」を最後に載せて下さい .

レポートの提出の締め切りは , 4 月 20-27 日に実験をした班は 5 月 6 日 (木) 12:00 , 6 月 15-22 日に実験をした班は 6 月 29 日 (火) 12:00 とする . 提出場所は , 計算機 C 講座前 (1504 室) の提出箱とする . 間違った箱に入れないよう充分注意すること .

実験に欠席したりレポート提出が間に合わない者は , 知能情報工学実験 II 全体が不合格になる場合がある . 病気のため欠席した場合には , 病院で診断書を書いてもらい提出すること . その他のやむを得ない場合もきちんと報告すること . これら正当な理由による欠席の場合には , 予備日を使って実験の補講を行う . ただし , 予備日の都合によっては試験期間と重なる可能性があるため注意しておくこと .

参考文献

國安和廣 : フリー UNIX で作るネットワークサーバ , 秀和システム , 1998 .

@IT : <http://www.atmarkit.co.jp/fsys/>