# ネットワーク構築*

## 1 目的

ネットワークを構成する機器にはいくつかの種類がある。ネットワーク同士を接続するにはルータ (router) と呼ばれる機器を用いる。

本実験では IPv4 ネットワークアドレスの設計を行った後、実際に 2 台のルータの機能を持つレイヤ 3 スイッチを用いて、シンプルなネットワークを構成する。これにより、ネットワーク機器の基本的な働きと設定方法を学ぶ。

## 2 事前準備

### 2.1 持ちもの

ルータのマニュアルを読むために、ノートパソコンまたはタブレットを持参すること（スマートフォンは不可）。実験結果を持ち帰るために、USB フラッシュメモリを持参すること。

### 2.2 予習事項

1. 用語の整理
   以下の用語の意味を調べて、予習ノートに簡潔にまとめて、実験前にチェックを受けること:

   パケット、IP アドレス、サブネットマスク、ブロードキャストアドレス、ルーティングテーブル、デフォルトゲートウェイ、ping、OSI 参照モデル、最上位 bit、DHCP、VLAN, 802.1Q、レイヤ 3 スイッチ、Ethernet

2. マニュアルの確認
   付録 B のコマンド一覧に従い、各コマンドの用法を参考文献 [1] マニュアルにより確認しておくこと。

*version 1.1

3. インターネットに接続された PC を用いて，Windows のコマンドプロンプト等により下記コマンドを発行し，印刷した実行結果を実験ノートに貼付し提出すること．また，実行結果は何を意味しているか実験ノートに説明すること．

```
ping www.cis1.c.dendai.ac.jp
```

4. なぜ IP アドレスではなく URL を用いて予習 1 の実行結果が得られるか，実験ノートに説明すること．

# 3 原理

## 3.1 TCP/IP

プロトコルとは、通信の手順を表す。TCP/IP(Transmission Control Protocol/Internet Protocol) はインターネットの中核のプロトコルである。

コンピュータ間の通信で重要なのはファイルの転送であるが、これを司るのがもともとの TCP であった。そのうち、TCP の中でネットワーク間のパケット転送のみを取り出し、中継装置にはその転送機能のみをインストールするようになった。このネットワーク間の転送機能を実現するプロトコルを Internet Protocol と呼び、ここから Internet という言葉が生じた。したがって、現在の TCP はコンピュータからファイルを受け取って IP にファイルを渡す機能と、IP から受け取った情報を元に、ファイルを構築してコンピュータに渡す機能、つまり、送信者と受信者間のファイルの交換を司るプロトコルになっている。

TCP を利用して様々なサービスプロトコルが開発されている。最初に広く使われるようになったのが電子メールのプロトコル SMTP(Simple Mail Transport Protocol) である。さらに、現在世界的にもっとも使用されているのが World Wide Web のプロトコルである HTTP(Hyper Text Transport Protocol) である。

## 3.2 プロトコルレイヤ

ネットワーク概念を整理するモデルとして OSI 参照モデルがある (表 1)。しかし、インターネットはすべての階層に一対一でプロトコルが対応しているわけではない [2, 3]。例えば、セッション層にはインターネットアプリケーションも関与するが、TCP も関与する。但し、ネットワーク層に IP が含まれ、トランスポート層に TCP が対応している。

先に述べた SMTP や HTTP のようなサービスプロトコルは、5,6,7 層に対応するが、一般には単純にアプリケーション層と呼ばれることが多い。

一方、Ethernet や無線 LAN などはデータリンク層に区分されるが、実際の定義では物理層（使用ケーブルなど）と一体で定義されることが多い。

表 1: OSI 参照モデル

| レイヤ | 層 | インターネットとの関係 |
|---|---|---|
| 7 | アプリケーション層 | アプリケーション層 |
| 6 | プレゼンテーション層 | |
| 5 | セッション層 | |
| 4 | トランスポート層 | トランスポート層 (TCP, UDP など) |
| 3 | ネットワーク層 | インターネット層 (IP) |
| 2 | データリンク層 | リンク層 |
| 1 | 物理層 | |

## 3.3 IP アドレス

通信で、送信者や受信者を区別するためにはアドレスが必要である。インターネットは、ネットワーク間を接続するため、さらに各ネットワーク自体を識別する必要がある。そのため、インターネットではネットワークアドレスと、コンピュータを識別するホストアドレスの対を IP アドレスとして用いる。

### 3.3.1 IPv4 アドレス空間

IPv4 のアドレス空間は 32 bit である。通常は、これを 8bit ごとに 10 進数にし、.(ピリオド) で区切って表示する。したがって、 IPv4 アドレス (以下、IP アドレス) は 0.0.0.0 から 255.255.255.255 までとなる。

IP アドレスにおけるネットワークアドレスは以下のように可変長になっている。

1. IP アドレスの最上位 bit が 0 の時、ネットワークアドレスは最上位 bit から 8 bit 分 (そのうち最上位は 0) で表すので、ネットワークアドレスは 0 から 127 までとなる。これをクラス A と言う。

2. IP アドレスの最上位 bit から 2bit が 10 の時、ネットワークアドレスは最上位ビットから 16 bit 分で表すので、 128.0 から 191.255 までがクラス B のネットワークアドレスになる。

3. IP アドレスの最上位 bit から 3bit が 110 の時、ネットワークアドレスは最上位ビットから 24 bit 分で表すので、 192.0.0 から 223.255.255 までがクラス C のネットワークアドレスになる。

4. IP アドレスの最上位 bit から 4bit が 1110 の時、ネットワーク内の放送 (一対多通信) に使用される。これをクラス D と言う。

5. IP アドレスの最上位 bit から 4bit が 1111 の時、特殊な用途を除いて使用されない。これをクラス E と言う。

インターネットに接続する際には、接続する機器の IP アドレスはネットワーク上で唯一になっている必要がある。そのため、IP アドレスは世界的に管理されている。インターネットに接続する各組織は IP アドレスの管理組織からアドレスを交付してもらい、それを使用する。東京電機大学は日本の JPNIC からアドレスを交付を受けている。

一方で、実験などで、直接インターネットには接続しないが、インターネットの仕組みを利用したい場合等のために、申請不要な IP アドレスが定められている。この IP アドレスをプライベートアドレスと呼ぶ。プライベートアドレスは表 2 にあるように、クラス A,B,C それぞれに定義されている。

表 2: プライベートアドレス

| クラス | IP アドレス | 個数 |
|---|---|---|
| A | 10.0.0.0 | 1 |
| B | 172.16.0.0 ～ 172.31.0.0 | 16 |
| C | 192.168.0.0 ～ 192.168.255.0 | 256 |

### 3.3.2 サブネット

一般に、組織は IP のネットワークアドレスを 1 つしか受け取れない。しかし、一方で、レイヤ 2 を構成する Ethernet などの機器において、接続可能な台数は 100 台程度と言われている。そのため、大きな規模の組織では受け取ったネットワークアドレスを分割して使用する必要がある。

サブネットとは組織内で定義された、分割されたネットワークである。サブネット同士を認識するため、サブネットにもアドレスを割り当てる。但し、外部から、サブネット内の機器に、アドレス変換なしで通信をするため、IP アドレスの上位のネットワークアドレスは共通にする必要がある。つまり、IP アドレスは、組織のネットワークアドレス、サブネットアドレス、ホストアドレスの 3 つ組で構成される。

前章で述べたように、ネットワークアドレスの長さは IP アドレスの上位 bit を見ると分かるようになっている。一方、サブネットアドレスは組織内で自由に定めてよい。そのため、組織内での利用を意識した IP アドレスではサブネットアドレスの長さの情報を付加する必要がある。ネットワークアドレスと、サブネットアドレスの部分の bit を 1, ホストアドレスの bit を 0 とした 32bit の bit 列をサブネットマスクと呼び、IP アドレスと同じように 10 進数 4 組で表す。例えば、133.20.160.1 という IP アドレスはクラス B なので、ネットワークアドレスは上位 16bit である。したがって、ネットワークアドレスは 133.20 となる。ここで、サブネットアドレスが 8 bit で 160 だとすると、サブネットマスクは上位 $16+8=24$ ビットが 1 になるので、 255.255.255.0 となる。そして、サブネットアドレスを明示する表記としては、 IP アドレスの後ろに/(スラッシュ) をつけて、サブネットマスクを表記するか、サブネットマスクに含まれる 1 の bit 数を付ける。つまり、この例だと次のように表示する。

- 133.20.160.1/255.255.255.0　または

- 133.20.160.1/24

### 3.3.3 様々な IP アドレス

ネットワークや、サブネットを表すために、ホストアドレスの bit がすべて 0 となった IP アドレスをネットワークアドレスとして使用する。

また、サブネット内すべてのホストへの一対多通信のための IP アドレスとして、ホストアドレスの bit すべてが 1 となった IP アドレスをブロードキャストアドレスとして使用する。なお、これに対して、通常の一対一通信用の IP アドレスをユニキャストアドレスと呼ぶ。

なお、255.255.255.255/255.255.255.255 が自分の所属しているサブネットすべてへのブロードキャストアドレスとして定義されている。また、自分自身を表す IP アドレスをループバックと言い、127.0.0.1/255.0.0.0 が定義され、 localhost と呼ばれている。

インターネットすべてを表すネットワークアドレスは 0.0.0.0/0.0.0.0 で、これをデフォルトとも呼ぶ。

表 3: 様々な IP アドレスの例

| 種類 | IP アドレス |
|---|---|
| ユニキャストアドレス | 133.20.160.1/255.255.255.0 |
| ブロードキャストアドレス | 133.20.160.255/255.255.255.0 |
| ネットワークアドレス | 133.20.160.0/255.255.255.0 |
| ループバックアドレス | 127.0.0.1/255.0.0.0 |
| 制限ブロードキャストアドレス | 255.255.255.255/255.255.255.255 |
| デフォルト | 0.0.0.0/0.0.0.0 |

## 3.4 ルータ

ルータはネットワーク同士を接続する装置である。ルータには 2 つ以上のネットワークインタフェースがあり、それぞれが異なるネットワークに接続する。

ルータの基本的な機能として次の 2 つがある。

1. IP フォワーディング
2. IP ルーティング

### 3.4.1 IP フォワーディング

フォワーディングはルーティングテーブルに基づいて、受信したパケットを転送することである。

ルーティングテーブルはルータや PC などのネットワーク対応の OS に一つあり、概ね、ネットワークアドレス、サブネットマスク、転送か直接通信か否かのフラグ、インターフェイスによって構成される表である (表 4)。

表 4: ルーティングテーブルの例

| ネットワーク | マスク | ゲートウェイ | フラグ | インターフェイス |
|---|---|---|---|---|
| 133.20.160.0 | 255.255.255.0 | 0.0.0.0 | U | FE0/1 |
| 133.20.161.0 | 255.255.255.0 | 0.0.0.0 | U | FE0/2 |
| 0.0.0.0 | 0.0.0.0 | 133.20.160.254 | UG | FE0/1 |

ルーティングテーブルは優先順位がある。各パケットの宛先について、テーブルの各行について上から、以下の処理を行う。

1. 受け取ったパケットの宛先アドレスとテーブルのマスクを AND 演算を行う
2. 演算の結果とネットワークが一致してなければ次の行に進む。次の行が無ければ Destination Unreachable Message の ICMP エラーを発生して終了する。
3. 属しているネットワークの行のフラグを見て、転送か直接送るかを判断する
4. 転送の場合は、指定されているゲートウェイに送る。直接送る場合は、インターフェイスを選択して、宛先に直接送る。

### 3.4.2 ルーティング

ルーティングとは、ルーティングテーブルを作成することである。管理者の入力によるスタティックルーティングの他、インターフェイスの定義による自動登録、ルーティングプロトコルによるダイナミックルーティングがある。

PC では通常は一つのネットワークのみに接続するので、内蔵インタフェースの自動登録と、デフォルトゲートウェイの設定のみで終了する。

一方、ルータは 2 つ以上のネットワークに接続するので、常に適切なルーティングテーブルの設定が必要である。本実験では主にスタティックルートのみを扱うが、発展実験として、 RIP v2 と OSPF による経路制御を行うことができる。

## 3.5 VLAN

Ethernet はブロードキャストが可能である。10Base-T より HUB が導入されたが、当初の HUB は入ってきたパケットがすべてのポートにブロードキャストがされていた。これだと、管理するネットワークが増える度に別々の HUB を接続することになる。それよりも、ポート数の多い HUB のポートを設定により分割して利用できる方が便利である。さらに、HUB を複数接続し、それら同士で協調して異なるブロードキャストの範囲を設

定できるとさらに便利である。このため、実際のネットワークの接続とは別の、想定するブロードキャストエリアを VLAN(Virtual Local Area Network) という概念で考える。

VLAN という考えを導入するために、ブロードキャストエリアに番号を与えることを考える。これを VLAN 番号と呼ぶ。そして、各ポートがどの VLAN に属するかを VLAN 番号で指定することで実現する。さらに、従来の Ethernet の通信と互換性を失うが、Ethernet のフレームに VLAN 番号を与えた拡張されたフレームを直接やりとりすることで、一つのポートで複数の VLAN を扱うこともできるようになる。

従来の Ethernet フレームをタグ無し、VLAN 番号を付加した拡張した Ethernet フレームをタグ付きと呼ぶ。VLAN 番号は 12bit で、1 から 4095 までが利用できる。但し、タグ無しのフレームとタグ付きのフレームは共存できないので、HUB のポートはタグ無しかタグありを設定する必要がある。さらにタグ無しのポートには複数の VLAN は共存できないので、タグ無しポートには所属する VLAN 番号が必要である。一方、タグありのポートにタグ無しのフレームが来た場合は VLAN1 のフレームと解釈する装置が多い。用語をまとめると次のようになる。

**タグ無し** 通常の Ether フレーム、1 つだけ指定した VLAN のみと接続できる。access モードとも呼ばれる。

**タグあり** 拡張した Ether フレーム。複数の VLAN で共有できる。通常の Ether フレームは VLAN1 のフレームとして扱われることが多い。trunk モードとも呼ばれる

HUB には内部構造として共通のバスを持ち、入力パケットをすべてのポートにブロードキャストするリピーター HUB と、交換機を持ち、ユニキャスト時に直結して通信するスイッチング HUB がある。一方、VLAN が扱えるスイッチング HUB をスマートスイッチ、またはレイヤ 2 スイッチと呼ぶ。さらに、ルーティング機能のあるスイッチング HUB をレイヤ 3 スイッチという。

## 3.6 レイヤ 3 スイッチ

レイヤ 3 スイッチは、外見上は HUB と似ているが、内部で VLAN に対してルーティング機能を持つため、従来のルータを置き換える装置となる。

レイヤ 3 スイッチの各ポートは、ポート毎にタグ無しポートかタグありポートかを設定により変えることができる。さらに、タグ無しポートはどの VLAN かを設定する。一方、タグありポートでは、扱える VLAN の集まりを設定する。レイヤ 3 スイッチの多くは、工場出荷時にはすべてのポートがタグ無しで、VLAN1 に所属するように設定されている。したがって、何も設定しない状態では通常のスイッチング HUB と同等である。

ルータではポートに IP アドレスを設定していたが、レイヤ 3 スイッチでは VLAN に IP アドレスを設定する。そして、IP アドレスが設定された VLAN がルーティングの対象となる。従来のルータではポートの数に対応した数だけしかネットワークを接続できなかったが、レイヤ 3 スイッチではタグありポートを使用することで、一つのポートで大量の VLAN に接続できる。そして、さらに、それらの VLAN に IP アドレスを設定すること

で、多くのネットワークに接続したルータと同等のルーティングを行うことができるようになる。

## 3.7　ネットワークトポロジ

ネットワーク技術の進歩とともに、ネットワークの構造も変化してきた。

ネットワーク機器に種類が無かった時代は、すべての機器を一筆書きのようにつなげていた。そのため、バス型ネットワークなどと呼ばれていた。

その後、高価で高速なネットワークが生まれると、バックボーンと呼ばれる高速なネットワークを構築し、各拠点はバックボーンとルータで結び、拠点内にサブネットを分配するような構造になった。バックボーンは冗長構造としてリング型のネットワークとなっていることが多かった。

VLAN が開発されて、大きな変革が生じた。trunk モードがあるので、サイト内のあらゆる VLAN は集約できる。そのため、従来は拠点やサブネット毎にルータが必要であったが、これがすべて VLAN として扱うことができる。その結果、すべての VLAN を、コアスイッチと呼ばれる高性能なレイヤ 3 スイッチに集約し、ルーティングを行うような構成が可能になった。このように、近代のネットワークは多数のレイヤ 2 スイッチが数少ないコアスイッチに集約されるように構成される。このような形状のネットワークを、スター型ネットワークと呼ぶ。スター型ネットワークは、安価な上に、管理が容易で、セキュリティも高い。VLAN に対応した冗長技術なども開発されているため、現代のネットワークは多重化されたスター型ネットワークがスタンダードになっている。

# 4　Allied Telesis AT-AR2050V ブロードバンドルータ

AT-AR2050V はアライドテレシス社の中小規模向け VPN ルーターとして位置づけられているルータである (図 1)。これは、ルーティングなどの基本機能に加え、外部の脅威からネットワークを守るファイアウォール、拠点間通信において盗聴、改ざん、成りすましからデータを保護するトンネリング機能、さらには 1 本の WAN 回線で機器を冗長化し、ダウンタイムを最小限に抑えることが可能なバイパスシステムなどを装備している。

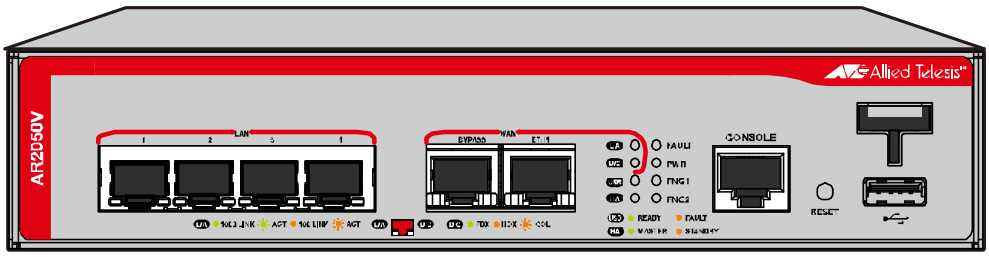


図 1:  AT-AR2050V

ルータの前面パネルに LAN と書かれている 4 ポートの口がある。これはレイヤ 3 スイッチとなっている。これらの各ポートは access モードか trunk モードかを設定できる。ま

た、それ以外のポートは外部接続用の冗長性のあるポートである。内部構造として、VLAN をルーティングするようになっている。基本的なレイヤ 3 スイッチでルーティングするには、次のようにする。

1. VLAN を定義する
2. ルーティングするには VLAN の接続点のアドレスを設定する
3. ポートを設定する
   (a) access モードに設定する時は、どの VLAN か指定する
   (b) trunk モードにするときは、 allowed vlan all など、通せる VLAN を指定する。
4. ルーティングテーブルの管理をする

# 5 実験

## 5.1 ネットワークモデル

本実験では 2 台の AT-AR2050V を使用し、レイヤ 3 スイッチとして活用した場合の接続実験を行う (図 2)。実験は 2 名で行う。

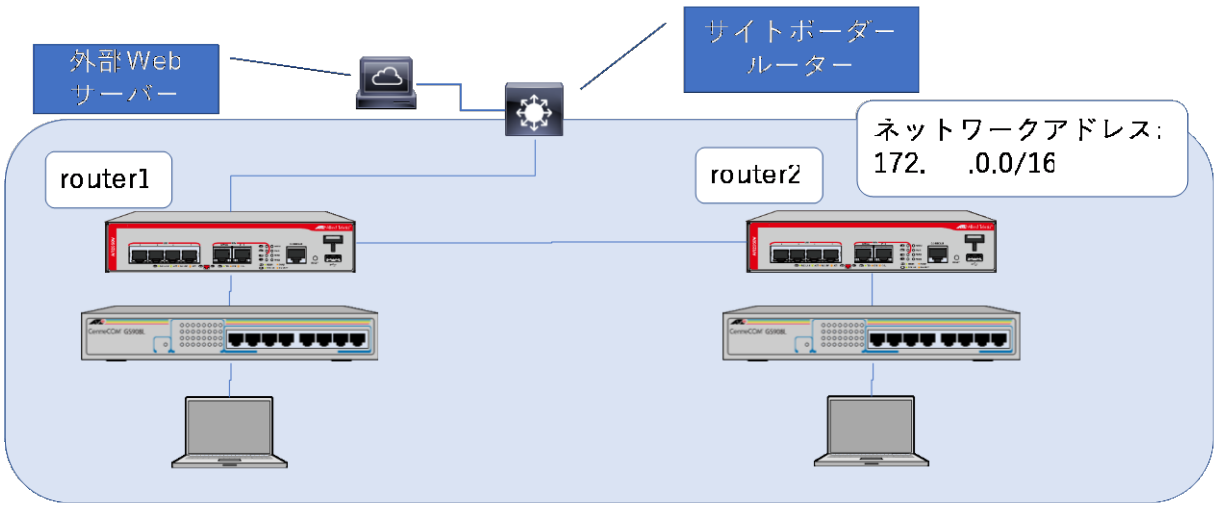


図 2: ネットワーク構成図

1. それぞれにサブネットを設定し、PC を接続する。
2. サブネット間のルーティングを行う。
3. 外部ネットワークと接続し、デフォルトルートを設定する。

## 5.2 準備

各グループは実験指導者から、グループのネットワークアドレスと本日の 外部 Web サーバの IP アドレスを受け取る。例えば、ネットワークアドレス 172.xxx.0.0/16, 外部 Web サーバーの IP アドレス 172.yyy.0.10 などという形式になる。

また、VLAN 設計用紙、ネットワークアドレス用紙も受け取る。

## 5.3 ネットワーク設計

### 5.3.1 VLAN 設計

以下を VLAN 設計用紙に記入すること

1. ポートレイアウト
   はじめに、ルータの接続の構成を確認する。ルータから HUB へは LAN1 または 2 ポートを使用する。ルータ同士は LAN3 ポートで接続する。以上を接続図を見て確認する。

2. VLAN 設計
   本実験ではルータから出る線は全て異なる VLAN とし、各線はそれぞれ一つだけ VLAN が載るように設計する。VLAN 番号として、2 から 4090 までの値を選ぶ。[1] 設計用紙上の線に VLAN 番号を記入する。

3. サブネット設計
   異なる VLAN ではブロードキャストアドレスが異なるようする。各 VLAN 毎にサブネット番号、サブネットマスク を決める。ブロードキャストアドレスを決める。決めたアドレスなどを設計用紙に記入する。

### 5.3.2 アドレス設計

ネットワークアドレス用紙を使い、定めたサブネットなどのアドレスなどを元に各サブネットワークに接続しているルータとパソコンについて、ホスト番号を決め、IP アドレスを決める。また、設定しやすいように、各アドレスにサブネットマスクを決める。決めたアドレスなどをアドレス用紙に記入する。

## 5.4 接続とアドレス設定

1. 設計した通りに、機器の配線する

2. パソコンを起動し、パソコンのアドレスを設定する。

[1] VLAN1 は特別な用途があるので使用しないこと

(a) スタートボタンを右クリックし、ネットワーク接続を選ぶ。左側のイーサネットを選択する (図 3)。あるいは、直接図 4 が表示される場合がある。その場合は (c) へ。


図 3: 設定/ネットワークとインターネット

(b) 「アダプターのオプションを変更する」を押すと、「ネットワーク接続」というウィンドウが表示される (図 4)。

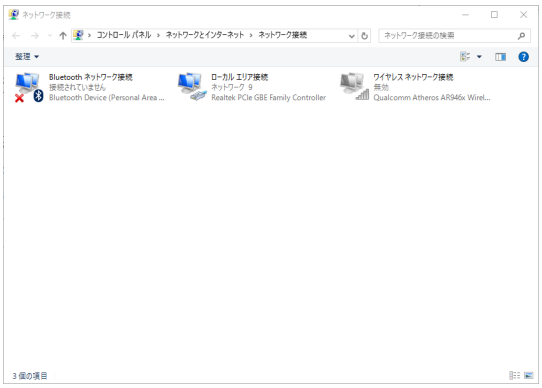


図 4: ネットワーク接続

(c) ローカルエリア接続を右クリックし、「プロパティ」を選ぶ (図 5)。

(d) インターネット プロトコル バージョン 4(TCP/IPv4) を選び、「プロパティ」ボタンを押す (図 6)。「次の IP アドレスを使う」を選択し、IP アドレス、サブネットマスクを設計通りに入れ、さらに、接続しているルータの IP アドレスをデフォルトゲートウェイに入力する。

3. パソコンとルータの設定端子をコンソールケーブルでつなぎ、端末ソフトを起動して、ルータの設定を行う

(a) ログイン名/パスワードは manager/friend

(b) 特権 EXEC モードに入る

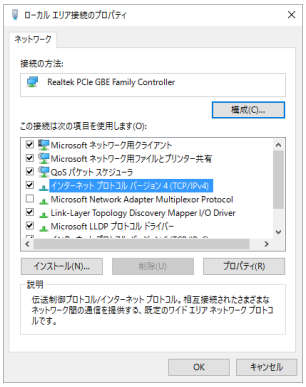


図 5: ローカルエリア接続のプロパティ

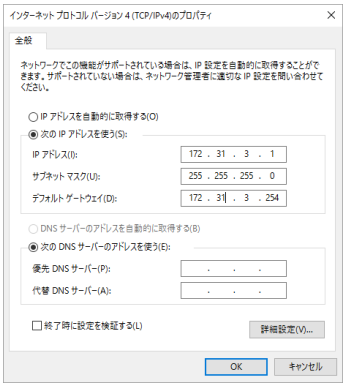


図 6: インターネットプロトコルバージョン 4(TCP/IPv4) のプロパティ

```
AR2050V>enable
AR2050V#
```

(c) グローバルコンフィグモードに入る

```
AR2050V#configure terminal
AR2050V(config)#
```

(d) ルータに名前をつける

```
AR2050V(config)#hostname router1
router1(config)#
```

(e) vlan database モードで vlan を定義する

```
router1(config)#vlan database
router1(config-vlan)#vlan 3
router1(config-vlan)#exit
router1(config)#
```

(f) interface vlan で各 vlan への接続点の IP アドレスを設定する

```
router1(config)#interface vlan3
router1(config-if)#ip address 172.xxx.3.1/24
router1(config-if)#exit
router1(config)#
```

(g) interface port で各ポートに vlan を関連付ける

i. switchport mode access コマンドで各ポートをタグ無しポートに設定する

ii. switchport access vlan コマンドで所属 vlan を指定する

```
router1(config)#interface port1.0.3
router1(config-if)#switchport mode access
router1(config-if)#switchport access vlan 3
router1(config-if)#
```

(h) end コマンドで設定を終了する

```
router1(config-if)#end
router1#
```

(i) show running-config コマンドで設定内容を確認する

4. 表 5 を参考にして、PC, ルータから ping を打ち、設定が正常か確認する。

## 5.5 ルーティング

1. PC において、デフォルトゲートウェイとして、自ルータのポートの IP アドレスを指定する。

2. PC において、ipconfig コマンドでデフォルトゲートウェイが正しく設定されていることを確認する。

3. ルータにて、show ip route でルーティングテーブルを確認する。

4. 設計した全てのサブネットワークと、デフォルト 0.0.0.0/0 について、ルータからの転送先を求め、表 6 に記入する

5. ルータに ip route コマンドにより、必要なすべての経路をスタティックにルーティングテーブルを設定する。

```
router1(config)#ip route 0.0.0.0/0 172.xxx.0.254
router1(config)#ip route 172.xxx.22.0/24 172.xxx.3.2
router1(config)#
```

6. show ip route コマンドにより設計通りにルーティングテーブルが設定されているかを確認する (図 7 参照)。

```
router1#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, D - DHCP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       * - candidate default

Gateway of last resort is 172.xxx.0.254 to network 0.0.0.0

S*      0.0.0.0/0 [1/0] via 172.xxx.0.254, vlan4
C       172.xxx.0.0/24 is directly connected, vlan4
C       172.xxx.3.0/24 is directly connected, vlan3
C       172.xxx.11.0/24 is directly connected, vlan11
C       172.xxx.12.0/24 is directly connected, vlan12
S       172.xxx.21.0/24 [1/0] via 172.xxx.3.2, vlan3
S       172.xxx.22.0/24 [1/0] via 172.xxx.3.2, vlan3
```

図 7: ルーティングテーブルの例

7. 表 7 を用いて ping による接続確認を行う。なお、ルーティングテーブルが正しければ、すべての ping に成功するはずである。

## 5.6 ブラウザによる通信

1. 各 PC のデスクトップ上のアイコンで Web サーバーを立ち上げる
2. ブラウザで http://localhost/ にアクセスし、自分の PC のブラウザにアクセスして、ページが表示するかを確認する。
3. 相手の PC のアドレスを使用して、 http://相手の PC アドレス/ にアクセスし、画面のスクリーンショットを撮る
4. 外部サーバ http://172.yyy.0.10/ にアクセスし、画面のスクリーンショットを撮る (yyy は実験時に指示される)

## 5.7 まとめ

ルータで show running-config により、設定を表示させ、レポートに報告すること。なお、レポートにはルータ 2 台とも設定を報告すること。

## 5.8 発展事項: NAT

ネットワークセキュリティが唱えられてから久しい。ネットワークのセキュリティを高めるために、外部からのアクセスを禁止し、内部からのアクセスは許すような、ネットワークごとの通信の行き来を制御する firewall という技術がある。さらに、内部からのアクセスに対しては、外部から返信のパケットがやってくるので、そのパケットを受け付ける必要がある。そのため、内部と外部の境界において、伝言を成立させるような意味合いで、内部アドレスを外部との境界ルータのアドレスと変換を行う NAT(Network Address Translation) という技術を用いる。

ここで、「内部」「外部」というキーワードを使用して議論したが、実際にルータにおいてもこの「内部」や「外部」などの概念を使用する必要がある。これを実現するは、ネットワークの集合に名前をつけて扱えれば良い。この扱いについては、ルータの各社によって色々ある。CISCO 社はアクセスリストと呼んでいる。Allied Telesis 社では UTM(Unified Threat Management)[4] という概念を導入し、その中で、ネットワークの集合は zone で定義するようになっている。

例えば、router1 の LAN1 ポートにこのファイアーウォールを設定することを考える。新たなネットワークとして 192.168.1.0/24 を定義する。つまり、まず以下のように設定を行う (ここで DHCP を使い、アドレスも配布する)。

```
vlan database
vlan 111
exit
interface vlan111
ip address 192.168.1.1/24
exit
interface port1.0.1
switchport access vlan 111
exit
service dhcp-server
ip dhcp pool pool111
network 192.168.1.0/24
range 192.168.1.65 192.168.1.126
default-router 192.168.1.1
end
```

この定義したネットワークを private, その他のネットワークを public という zone で定義するには次のようにする。

```
zone private
network private1
ip subnet 192.168.1.0/24
exit
exit
```

```
zone public
network public1
ip subnet 0.0.0.0/0 interface vlan4
ip subnet 172.xxx.0.0/16 interface vlan12
ip subnet 172.xxx.0.0/16 interface vlan3
end
```

private ゾーンから public ゾーンへのアドレス変換は次のようにする。

```
nat
rule 10 masq any from private to public
enable
end
```

各ゾーン間の IP フォワーディングのルールはホワイトリストにより次のように定義する。

```
firewall
rule 10 permit any from private to private
rule 20 permit any from private to public
rule 30 permit any from public to public
protect
end
```

## 5.9 発展事項: VLAN ルーティング

図 8 のように、すべての VLAN を router1 に集め、ルーティングを router1 だけにする。現代のネットワークは基本的にスター型と呼ばれる、

```
hostname router1
vlan database
vlan 4,11,12
exit
interface vlan4
ip address 172.xxx.0.1/24
exit
interface vlan11
ip address 172.xxx.1.1/24
exit
interface vlan12
ip address 172.xxx.2.1/24
exit
ip route 0.0.0.0/0 172.xxx.0.254
interface port1.0.1
```

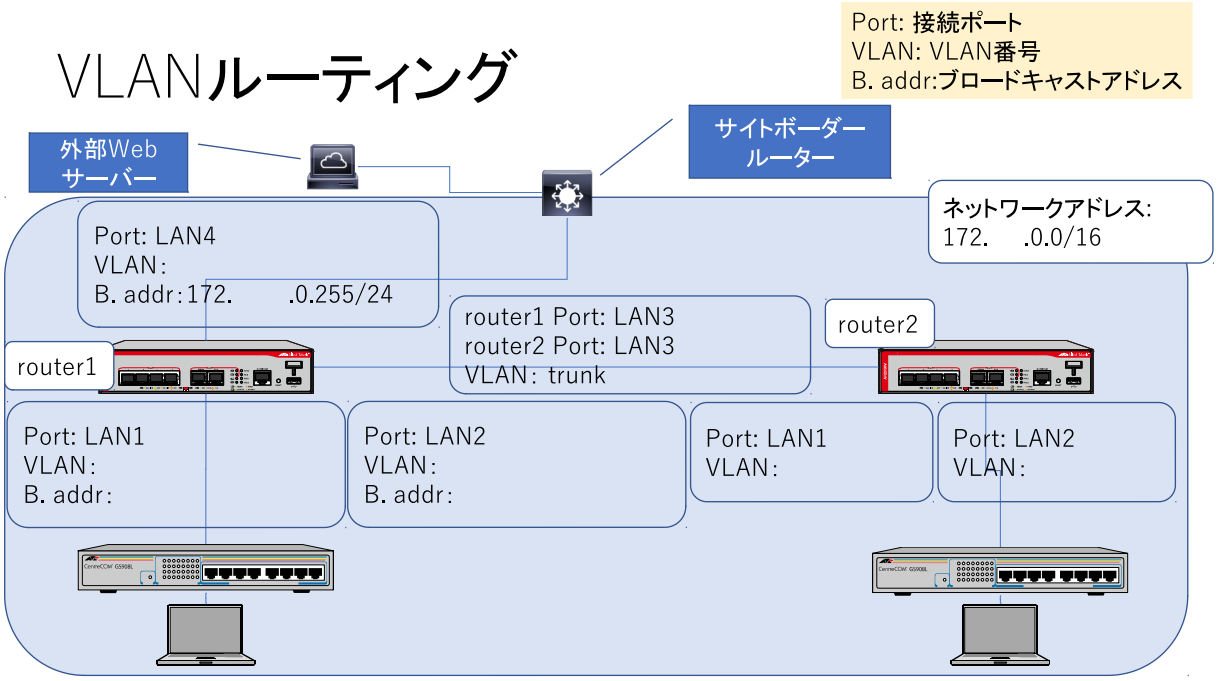


図 8: VLAN ルーティング

```
switchport mode access
switchport access vlan 11
exit
interface port1.0.2
switchport mode access
switchport access vlan 12
exit
interface port1.0.3
switchport mode trunk
switchport trunk allowed vlan all
exit
interface port1.0.4
switchport mode access
switchport access vlan 4
exit
```

DHCP を設定する場合はさらに次を router1 のみに設定する。

```
ip dhcp pool p1
network 172.xxx.1.0/24
range 172.xxx.1.10 172.xxx.1.20
subnet-mask 255.255.255.0
default-router 172.xxx.1.1
```

```
exit
ip dhcp pool p2
network 172.xxx.2.0/24
range 172.xxx.2.10 172.xxx.2.20
subnet-mask 255.255.255.0
default-router 172.xxx.2.1
exit
```

route2 には次の設定をする。

```
hostname router2
vlan database
van 11,12
exit
interface port1.0.1
switchport mode access
switchport access vlan 11
exit
interface port1.0.2
switchport mode access
switchport access vlan 12
exit
interface port1.0.3
switchport mode trunk
switchport trunk allowed vlan all
exit
```

1. PC の IP アドレス設定を自動に設定する。
2. 各ルータの LAN1 または LAN2 ポートに PC をつなぐ。
3. コマンドプロンプトで ipconfig を実行し、IP アドレスの設定がされていることを確認する。
4. ping コマンドで通信が正常に行われることを確認する。
5. ブラウザで Web ページが正常に表示されることを確認すること

# 6 報告事項

報告書には次の項目を含めること。また、実験中はこれらの項目について、その都度担当教員に報告し、確認を得ること

1. VLAN 設計図
2. アドレス設計図
3. ルータ、HUB、PC の機種名、OS やファームウェアの名前とバージョン
4. 入力したコマンド
5. ルータのルーティングテーブルの内容
6. PC の ipconfig のイーサネットアダプターの内容
7. 表 5 〜 7
8. 2 台のルータの内容

### 発展事項

1. NAT の実験を行った場合、その設定内容と動作結果をレポートに報告すること
2. VLAN ルーティングの実験を行った場合、その設定内容と動作結果をレポートに報告すること
3. 外部 Web サーバのページを参照して、OSPF の実験を行った場合、その設定内容と動作結果をレポートに報告すること
4. 外部 Web サーバのページを参照して、RIP の実験を行った場合、その設定内容と動作結果をレポートに報告すること
5. 外部 Web サーバのページを参照して、DHCP の実験を行った場合、その設定内容と動作結果をレポートに報告すること

## 7 検討事項

1. IP フォワーディングと IP ルーティングの違いについて説明しなさい。
2. スタティックルーティングとダイナミックルーティングの長所、短所についてまとめよ
3. ブロードキャストアドレスの設定を間違えると、どのような症状が出るか？実験あるいは考察せよ。
4. ping コマンドとは何か、説明しなさい

## 発展事項

1. 発展事項で VLAN ルーティングを行った場合、正課の実験で構築したネットワークとの長所、短所をまとめよ
2. 802.1Q VLAN とは何か、説明しなさい
3. 外部接続スイッチがどのような設定になっているか考えてみよ
4. 実験で使用している PC でインターネットに接続してマニュアルを読みながら実験を行う場合、どのような操作が必要か？（ヒント：DHCP、 デフォルトルート、route コマンド）

# A　表

(凡例) ○:接続, ×:到達不能, -:タイムアウト

表 5: 通信確認

| 対象機器 | アドレス | 自PCからping予想 | 自PCからping結果 | 自ルータからping予想 | 自ルータからping結果 |
|---|---|---|---|---|---|
| 自 PC | | | | ○ | |
| 自ルータ | | | | ○ | |
| 自ルータ | | | | ○ | |
| 対向ルータ | | | | ○ | |
| 対向ルータ | | | | × | |
| エリアボーダルータ | 172.　　.0.254 | | | ○ or × | |
| 外部 Web サーバー | 172.　　.0.10 | | | × | |

表 6: ルーティングテーブル設計

| ネットワークアドレス | サブネットマスク | 転送先 |
|---|---|---|
| 0.0.0.0 | 0.0.0.0 | |
| | | |
| | | |
| | | |

表 7: 通信確認 2

| 対象機器 | アドレス | 自PCからping予想 | 自PCからping結果 | 自ルータからping予想 | 自ルータからping結果 |
|---|---|---|---|---|---|
| 自 PC | | ○ | | ○ | |
| 自ルータ | | ○ | | ○ | |
| 自ルータ | | ○ | | ○ | |
| 対向ルータ | | ○ | | ○ | |
| 対向ルータ | | ○ | | ○ | |
| エリアボーダルータ | 172.　　.0.254 | ○ | | ○ | |
| 外部 Web サーバー | 172.　　.0.10 | ○ | | ○ | |

# B　コマンド

以下に有用なコマンドを列挙するので、マニュアルで用法を確認しておくこと。余白にメモすると良い。

## B.1　PC コマンド

ネットワーク管理を行うための Windows10 で使うコマンドを挙げる。help ユーティリティでは用法が出力されないので、 ipconfig /? などにより、コマンド自体が出力する用法を確認すること。

1. ipconfig
2. ipconfig /renew
3. ping
4. tracert
5. arp -a
6. arp -d *
7. route print
8. route add
9. route delete

## B.2　ルータコマンド

AT-AR2050V のマニュアルは web で公開されている (参考文献 [1])。

### B.2.1　モード切り替え

1. enable
2. configure terminal
3. exit
4. end
5. reload
6. hostname

### B.2.2 EXEC モード

1. show running-config
2. show ip interface
3. show interface switchport
4. show interface
5. show interface brief
6. show interface status
7. show ip route

### B.2.3 VLAN コマンド

1. vlan database
2. vlan

### B.2.4 Interface

1. interface vlan 番号
2. ip address
3. interface port1.0. 番号
4. switchport mode access
5. switchport access vlan 番号
6. switchport mode trunk
7. switchport trunk allowed vlan all

### B.2.5 ルーティング

1. ip route
2. router ospf
3. network
4. redistribute static
5. default-information originate

# C　トラブルシューティング

うまく動作しない場合に有用な調査の定石を示す。

1. 分割統治法
   ネットワークはすべての条件が満たされて始めて通信が可能になる。そこで、状況を分割できる場合は分割し、個別に条件が完璧かどうかを確認する。

2. レイヤーの低い順
   「ブラウザで画面が表示されない」などのアプリケーションレイヤにおけるトラブルの場合、アプリケーションレイヤでのトラブルだけではなく、物理レイヤまですべてのレイヤのうちのどこかに原因があることが考えられる。下位レイヤでトラブルがある場合、上位レイヤでの通信は必ず失敗するので、上位レイヤから調べるのは時間の無駄となる可能性がある。

3. 背理法
   「全体が通信できているのに、一部が通信できないのはおかしい」など、想定できる故障状態を排除するのに、現状と矛盾するようなものを排除していく。そして、否定すると矛盾するような条件を積み上げていく。

4. 対照実験法
   一つだけ条件を変えて、状況が変わるかを観測する。状況が変化すれば、その条件が関係あることになり、変化しなければ関係ないことが分かる。なお、同時に 2 つ以上条件を変えると、対照実験法が成立しなくなり、どの条件と関係あるかが分からなくなる

トラブルの原因は探すのにどれだけ時間がかかっても、最終的には大抵はどこか一ヶ所の不具合が原因である。したがって、そこを発見し、対処するしかない。本実験においては、教材はチェック済みなので、基本的には設定ミスがもっとも大きい可能性のある原因である。しかし、その他にも配線ミスや、場合によっては機器の故障などもある。

なお、コンピュータ系の実験では、ミスがあるかどうかの確認を人がチェックするより、場合によっては実際に試した方が早い場合もある。場合により効率的な方法は変わるので、経験などを積んで判断する必要がある。

なお、少ない可能性ではあるが、完全な考え間違いなどによる設計の誤りであることもある。この場合は微調整では直らない。ただし、完全な考え間違いの場合でも、すべての設定項目が異なっていることはさらにまれなので、すべて消してやり直すのは最終手段とし、なるべく修正箇所を求めて直すようにする。

## C.1　レイヤ 1

1. 機器の電源ランプの確認

2. 配線の確認、接続ランプの確認

3. 接続を外し、つなぎ直す。端子は酸化するので、つなぎ直しで酸化膜が取れて、接続が良好になる場合がある。但し、つなぎ直しをきっかけにして、上位プロトコルが接続プロセスを再起動することもあるので、つなぎ直しに対応する上位プロトコルの確認が必要なこともある。

## C.2 レイヤ 2

1. 接続機器で、インターフェイスが有効になっているか？
2. 接続機器においてインターフェイスの状況が正常に稼働中となっているか？
3. 接続機器のドライバは正常か？(授業の実験では検証済みだが、実際の運用ではドライバーの最新性の確認なども重要)
4. 場合によっては、起動や接続に時間がかかったり、 arp テーブルなどの内部情報の更新時間など時間が関与する場合もあるので、一定時間様子を見ることも必要。

## C.3 レイヤ 3

1. アドレス違い、ネットマスク違い、ブロードキャストアドレス違い、デフォルトゲートウェイアドレス違いで、それぞれどのような症状が出るか、想像や体験しておくと対処が早い
2. インターフェイスの設定項目の確認
3. ping による通信確認
4. ルーティングテーブルの確認
5. ファイヤウォール、セキュリティの設定の確認

## C.4 ヒューマンエラー

1. 確認を怠っている
2. デフォルト設定値の確認ミス
3. 機器に設定されているものと、設定すべき値が食い違っている
4. 設計が間違っている
5. 機器の制限事項により、設定ができないため、回避法をとらなければならない
6. 時として廃止されるプロトコルもあるため、場合によっては互換性を無視した機器のバージョンアップで使用不能になる場合もある

# D　設定例

```
no spanning-tree rstp enable
hostname router1
vlan database
vlan 3,4,11,12
exit
interface vlan3
ip address 172.31.3.1/24
exit
interface vlan4
ip address 172.31.0.1/24
exit
interface vlan11
ip address 172.31.11.1/24
exit
interface vlan12
ip address 172.31.12.1/24
exit
interface port1.0.1
switchport mode access
switchport access vlan 11
exit
interface port1.0.2
switchport mode access
switchport access vlan 12
exit
interface port1.0.3
switchport mode access
switchport access vlan 3
exit
interface port1.0.4
switchport mode access
switchport access vlan 4
exit
ip route 0.0.0.0/0 172.31.0.254
ip route 172.31.21.0/24 172.31.3.2
ip route 172.31.22.0/24 172.31.3.2
end
```

# 参考文献

[1] アライドテレシスホールディングス株式会社. AT-AR2050V/AT-AR3050S/AT-AR4050S コマンドリファレンス, 第 5.4.7 版, 2015–2018. https://www.allied-telesis.co.jp/support/list/awp/rel/5.4.7-2.4/613-002107_R/.

[2] R. Bush and D. Meyer. Some Internet Architectural Guidelines and Philosophy. RFC 3439 (Informational), December 2002.

[3] OSI model. Wikipedia. https://en.wikipedia.org/wiki/OSI_model#Comparison_with_TCP/IP_model.

[4] アライドテレシスホールディングス株式会社. UTM/概要, 第 5.4.7 版, 2015–2018. AT-AR2050V/AT-AR3050S/AT-AR4050S コマンドリファレンス https://www.allied-telesis.co.jp/support/list/awp/rel/5.4.7-2.4/613-002107_R/docs/overview-194.html.