

第1章 ネットワーク設計概念

ここでは、本装置を利用してネットワークを設計する際に留意しなくてはならないネットワークの概念と、本装置のネットワーク定義の考え方について説明します。

1.1 ネットワークの概念とルーティング

1.1.1 ネットワークの考え方

ネットワークとは、通信手段を備えたコンピュータ同士が何らかの伝送媒体を介して接続された集合体のことです。例えば、HUB やスイッチなどの装置によって構築されたひとつの LAN はひとつのネットワークとなります。また一般加入線や専用回線などを利用して遠隔地を接続している WAN と呼ばれる部分についても、同様にひとつのネットワークとなります。

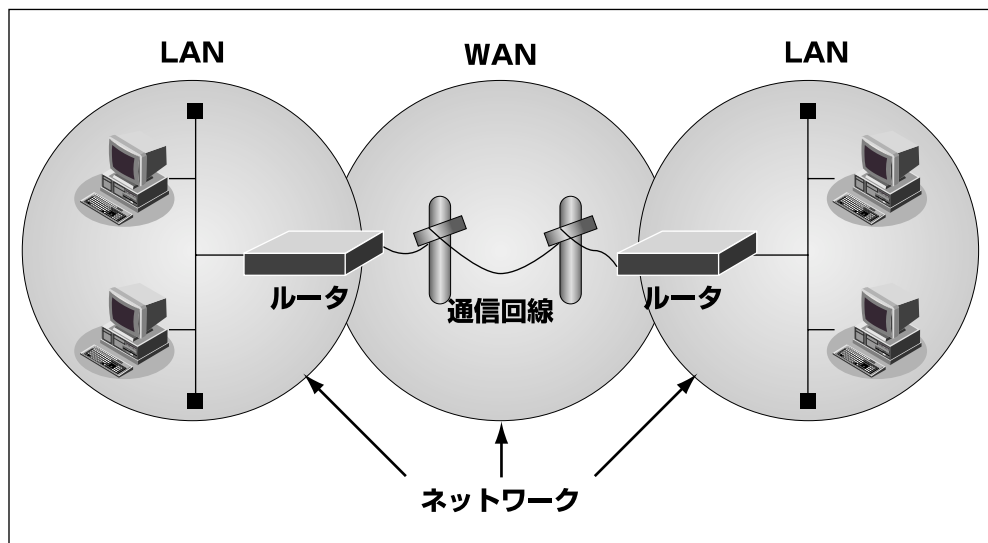


図 1.1 ネットワークの概念

また、広義の意味で、これらひとつひとつのネットワークが接続された全体に対してもネットワークと呼ばれます。

1.1.2 IP におけるネットワーク

IP ネットワークにおいては接続されるすべてのコンピュータ（ホスト）やルータなどのネットワーク機器にそれぞれユニークな IP アドレスを割り当てる必要があります。この IP アドレスは「ネットワーク部」と「ホスト部」から構成されます。

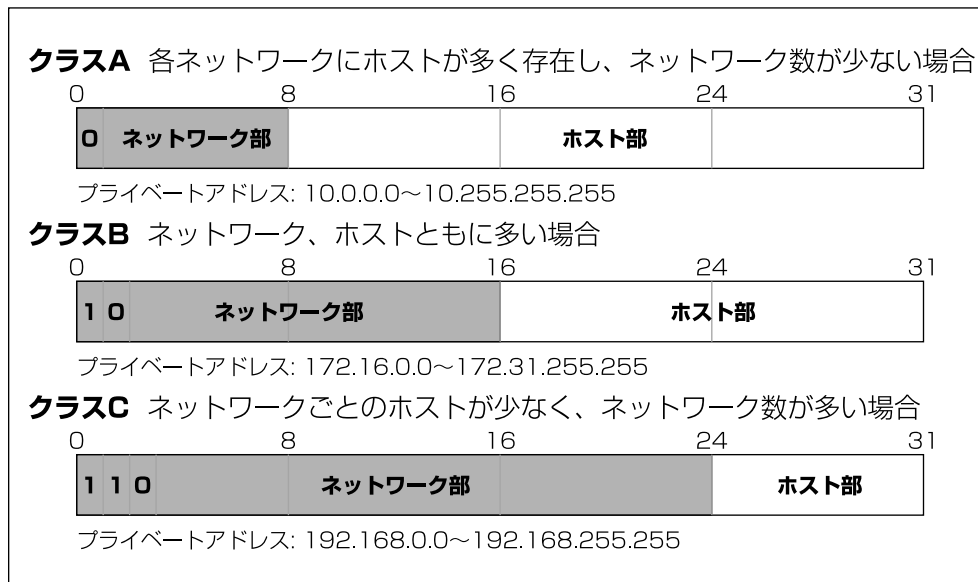


図 1.2 IP アドレスの構造

IP ネットワークにおけるひとつのネットワークとは、IP アドレスのネットワーク部が同一のアドレスを持つ機器の集まりとなります。つまり、同じデータリンクに接続される機器にはすべて同じネットワークアドレスを設定しなければなりません。さらに、他のデータリンクとネットワークアドレスが重ならないように割り当てる必要があります。

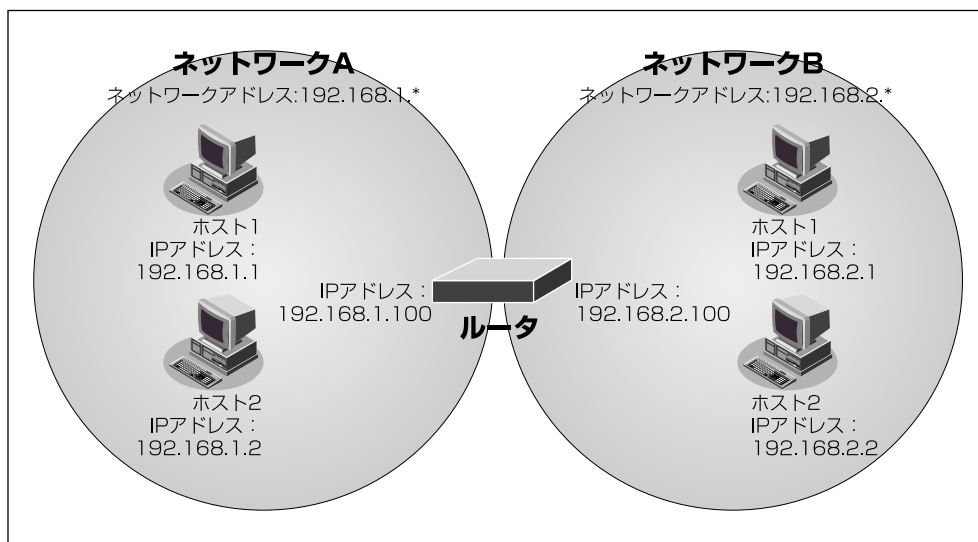


図 1.3 ネットワークとネットワークアドレス

以降、本書で単にネットワークと記述されている場合は IP の同一ネットワーク群のことを言います。また、広義のネットワークについては「ネットワーク全体」と記述します。

1.1.3 ネットワークとルータ

本装置はネットワークとネットワークを相互に接続するルータと呼ばれる装置です。ルータはIPパケットと呼ばれる転送単位ごとに、パケットに付加されているIPアドレスのネットワーク部の情報に従って通信します。他のネットワーク宛のデータであればデータを転送することにより、ネットワーク間での通信を実現しています。この動作をルーティング（経路制御）と言い、この時にどのネットワークがどこにあるのかを知るために必要な情報がルーティング情報です。ルータはあらかじめ作成されたルーティング情報の集まりであるルーティングテーブル（経路制御表）によって動作します。ルーティングテーブルの作成方法には、管理者があらかじめ装置ごとに設定しておくスタティックルーティングと、接続されているルータ同士で情報を交換しあって自動的に作成するダイナミックルーティングの2種類の方法があります。

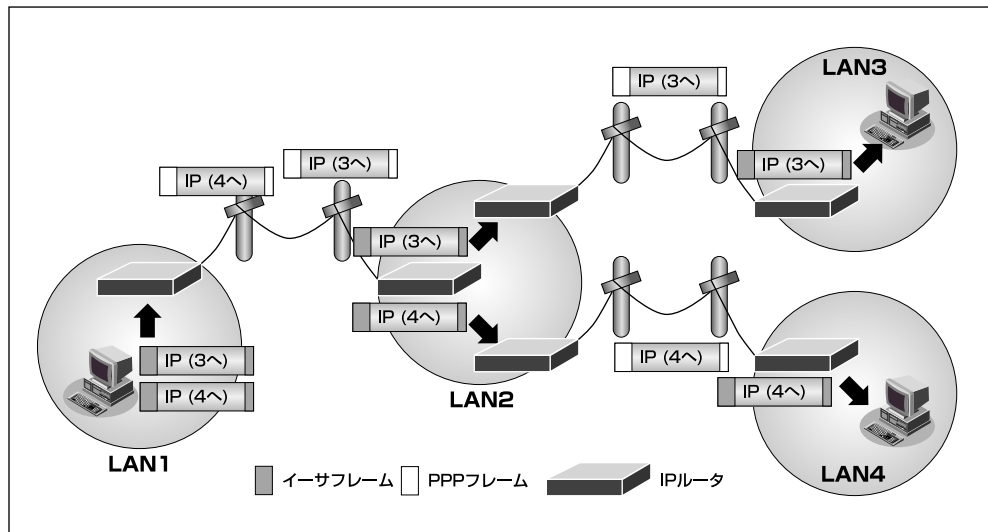


図 1.4 ルータの動作

なお、本装置ではIP以外のパケットを転送する機能であるブリッジについてもサポートしており、IPアドレスを持たないIP以外のパケットについてはEthernetフレームの情報にしたがって適切な相手にデータを転送することもできます。

1.1.4 ネットワークインタフェースの概念

ルータがデータを送信または受信する場合には、論理的な出入り口が必要となります。この出入り口をネットワークインタフェースと呼び、すべてのデータの送受信はネットワークインタフェースを通じて行われます。

基本的にはネットワークインタフェースは物理回線と1対1に対応しますが、PPP通信やtunnel通信などのように物理回線と等価に見える論理的な通信路もあるため、ネットワークインタフェースはパケット転送処理のための論理的な出入り口と考える必要があります。

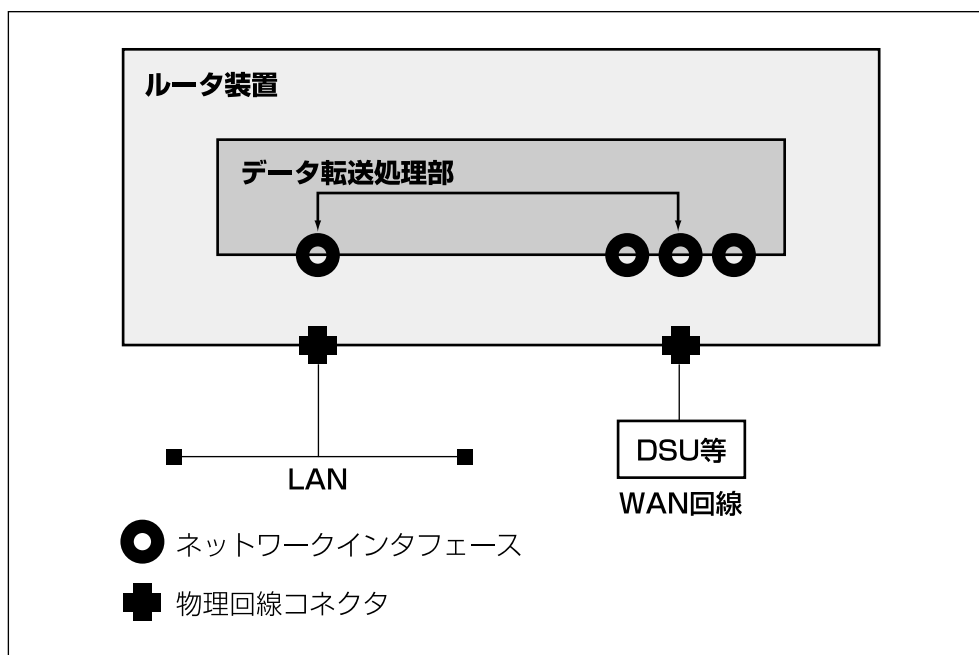


図 1.5 ネットワークインタフェース

1.1.5 ルーティングによる転送

ルーティングはネットワーク層プロトコルの情報によってデータの転送先を決定します。データ転送はパケットと呼ばれる通信単位ごとに転送先を選択し、転送先に対してデータを転送します。この時、転送先を選択するための情報としてルーティングテーブル（経路制御表）を利用します。ルーティングテーブルとは「そのネットワークにデータを転送するためには、次にどの装置に対して転送したらよいか」を管理するテーブルです。ルーティングによる転送においては個々のパケットに含まれる宛先アドレスを元に経路情報を検索し、その経路に従って送出先を決定します。決定される情報は、出口となるネットワークインタフェースと、経由すべき次装置のアドレス（これは存在しない場合もあります）となります。

例： 192.168.2.1 宛のパケットを転送する場合

表 1.1 経路情報

宛先ネットワーク	次装置アドレス	出口インタフェース
192.168.1.0/24	-	lan0
192.168.2.0/24	192.168.1.2	lan0
⋮	⋮	⋮

この経路情報から、192.168.2.1 に到達するための出口となるネットワークインタフェースは lan0 であり、次装置は 192.168.1.2 であると判定されます。

この経路選択による出力先の選定は受信したデータに対してだけでなく、本装置が生成するデータについても同様に適用されます。つまり、経路情報が存在しないと装置からデータを送信することができません。このため、最低でも 1 つの経路情報を設定する必要があります。

1.1.6 ブリッジによる転送

最も簡単なブリッジによる転送の構造は、受信したデータを他のすべてのネットワークインタフェースに対して送信します。しかし、これではトラフィックが膨大になるため、学習機能や制御プロトコルによって適切なネットワークインタフェースだけに転送することが一般的です。ルーティングと同じく、ここでもその出口ネットワークインタフェースの選定処理が行われます。

1.2 ルータ設定の概要

1.2.1 ネットワークと設定の関係

ルータに設定すべき情報としては、接続する回線に関する物理的な情報と、接続するネットワークに関する論理的な情報、そしてデータの振り分け条件であるルーティング情報が必ず必要となります。また、他に装置固有の情報や、付加的なサービスの設定を必要に応じて行います。

本装置ではこれらの情報の設定に関して大きく次のように分類しています。

- wan 定義
本装置に接続する回線に関する物理的な情報を定義する命令群であり、回線の種類や電話番号などの契約に関する情報を定義します。
- lan 定義
本装置に接続する lan に関する論理的な情報を定義する命令群であり、lan のアドレスやネットワークの情報などを定義します。また、DHCP などの lan に固有のサービスに関しても lan 定義によって行います。
- remote 定義
本装置が wan 回線を通じて通信を行う相手に関する論理的なネットワーク情報を定義する命令群であり、PPP に関する情報や相手ネットワークのアクセスポイントに関する情報などを定義します。
- answer 定義
本装置が不特定の相手から接続される場合の情報を定義する命令群であり、必要に応じて定義します。
- その他の定義
装置固有の情報や付加サービスの情報を必要に応じて定義する命令群であり、ネットワーク管理に関する情報や時刻情報などの定義があります。

各定義の分類と、実際のネットワークの対応を図 1.6 に示します。

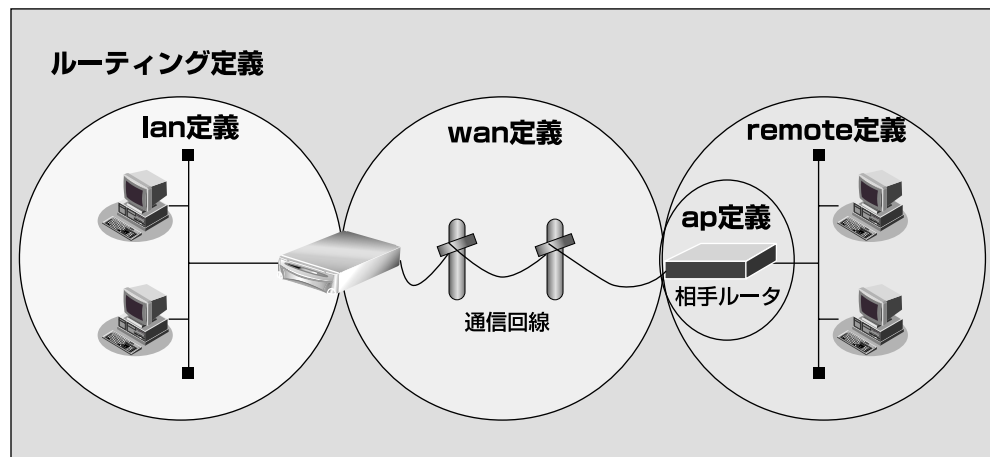


図 1.6 ネットワークと定義の対応

1.2.2 ネットワークインタフェースの定義

データ転送時の出口となるネットワークインタフェースには、その特性や接続されている回線によっていくつかの種別があります。

- lo
ループバックインタフェース
装置の内部プログラムで折返し通信を行う場合に利用されます。外部から利用することはありません。
- lan
Ethernet インタフェース
Ethernet を利用して通信する場合に利用するネットワークインタフェースです。lan 定義によって設定されます。
- rmt
設定済相手用通信インタフェース
ISDN / 専用線 / フレームリレーなどの回線を利用して通信を行う場合、または IPv6-over-IPv4 トンネルを利用して通信を行う場合に、定義された相手システムとの通信において利用されるネットワークインタフェースです。remote 定義によって設定されます。

これらのインタフェース種別にインタフェース番号を付与したものがネットワークインタフェース名となります。

例： lo0, lan0, lan1, rmt0, rmt1, ...

lan および rmt のネットワークインタフェースはそれぞれ lan 定義、remote 定義によって設定されます。lan 定義、remote 定義の定義番号とネットワークインタフェースのインタフェース番号は 1 対 1 に対応します。lo は装置が自動設定しますので、設定項目はありません。

1.2.3 ルーティング情報の定義

ルーティング情報は最終的に出口となるネットワークインタフェースを決定するために必要な情報を定義するものです。本装置では出口インタフェースに対応する定義内でルーティング情報の設定を行います。例えば、lan0 から出力するためのルーティング情報は lan0 内の定義に、rmt0 から出力するためのルーティング情報は remote0 内の定義に分けて設定します。

1.2.4 高度な転送先選定定義

本来の IP ルーティングにおける送信先選定のルールでは出力先インタフェースまでしか選定されません。このため、通常の IP ルーティングでは、一つの経路によって決定される接続先は一つしか利用することができません。しかし、本装置では相手ネットワークの定義である remote 定義の配下に、実際の接続先設定となる ap 定義を複数定義することができます。これは、ルーティング情報によって決定された出力先の remote 定義の範囲で、送信データ内の宛先 IP アドレス以外の情報をルーティング情報の代わりに利用して、さらに送信先を分別するマルチルーティングという機能を利用して実現しています。例えば、Internet と通信するためには default route というルーティング情報が必要ですが、ひとつの remote 定義において default route を設定した場合には、他の remote 定義には default route は設定できません。このため、remote 定義だけでは必要に応じて ISP を切り替えるということは通常の IP ルーティングの機構だけでは不可能です。本装置のマルチルーティングは、決定された remote 定義の範囲内でルーティング機構では参照されない情報を利用して、さらに細分化された送信先の選定を行います。

マルチルーティングは同一の remote 定義内で動作するため、remote 定義によるデータ送信先の分配と、ap 定義 (マルチルーティング) によるデータ送信先の分離は以下のように使い分けます。

- remote 定義による分離
経路情報として分離できる接続先 (つまり、独立したネットワークとして識別できる接続先) は、それぞれ別の remote 定義として定義し、ルーティング機能を用いて分配を行います。
- ap 定義 (マルチルーティング) による分離
経路情報では分離できない接続先 (つまり、独立したネットワークとして識別できない接続先) は、同一の remote 定義内にそれぞれ別の ap 定義として定義し、マルチルーティング機能を用いて分配を行います。