

## 第 10 章 IP ルーティング

# Exam Topics との対応

- ・ **3.0 IP** コネクティビティ
  - **3.1** ルーティング テーブルを構成する要素の解釈
    - ✧ **3.1.a** ルーティング プロトコル コード
    - ✧ **3.1.b** プレフィックス
    - ✧ **3.1.c** ネットワーク マスク
    - ✧ **3.1.d** ネクスト ホップ
    - ✧ **3.1.e** アドミニストレーティブ ディスタンス
    - ✧ **3.1.f** メトリック
    - ✧ **3.1.g** ラスト リゾート ゲートウェイ
  - **3.2** ルータがデフォルトでフォワーディング デシジョンを行う方法の決定
    - ✧ **3.2.a** 最長一致
    - ✧ **3.2.b** アドミニストレーティブ ディスタンス
    - ✧ **3.2.c** ルーティング プロトコルのメトリック
  - **3.3 IPv4** および **IPv6** でのスタティック ルーティングの設定および確認
    - ✧ **3.3.a** デフォルト ルート
    - ✧ **3.3.b** ネットワークルート
    - ✧ **3.3.c** ホスト ルート
    - ✧ **3.3.d** フローティング スタティック

# ルータ

## ポイント

- ・ ルータはネットワークを相互接続し、ネットワーク間のデータの転送を行います。
- ・ ルータがデータを転送するには、IP パケットの宛先 IP アドレスとルーティングテーブルを参照します。

## ルータの役割

ルータは複数のネットワークを相互接続し、ネットワーク間のデータ転送を行うためのネットワーク機器です。企業の社内ネットワークは、部署ごとなどで複数のネットワークとして構成しています。それら複数のネットワークを相互接続するためにルータを利用しています。企業の社内ネットワークにかぎらず、インターネットにも膨大な数のネットワークがあり、それらがルータによって相互接続されています。

そして、ルータは相互接続したネットワーク間のデータの転送を行います。ルータによるネットワーク間のデータ転送を「ルーティング」と呼びます。また、ルータにとってのデータは IP パケットです。IP は OSI 参照モデルではネットワーク層のプロトコルです。IP パケットを転送するネットワーク機器なので、ルータは OSI 参照モデルのネットワーク層レベルのネットワーク機器です。

## ネットワークの接続は IP アドレスを設定する

これまでも述べていますが、「ネットワークに接続するということは IP アドレスを設定する」ということです。ルータが複数のネットワークを接続するのも、ルータに対して IP アドレスを設定することになります。ルータがネットワークを相互接続するには、ルータのインタフェースの物理的な配線に加えて、インタフェースに IP アドレスを設定します。たとえば、ルータのインタフェース 1 の物理的な配線を行なってそのインタフェースが有効になり、IP アドレス 192.168.1.254/24 を設定すると、ルータのインタフェース 1 は 192.168.1.0/24 のネットワークに接続していることになります。ルータには複数のインタフェースが備わっていて、それぞれのインタフェースの物理的な配線と IP アドレスの設定を行うことで、ルータは複数のネットワークを相互接続することになります。

図の R1 には 3 つのインタフェースがあります。インタフェース 1 の物理的な配線を行なって IP アドレス 192.168.1.254/24 を設定すると、ルータ 1 のインタフェース 1 はネットワーク 1 の 192.168.1.0/24 に接続しています。同様にインタフェース 2 とインタフェース 3 にも IP アドレスを設定することで、R1 はネットワーク 1、ネットワーク 2、ネットワーク 3 を相互接続しています。

ネットワーク 3 には R1 だけではなく R2 も接続されています。R2 の 3 つのインタフェースにも R1 と同様に物理的な配線をして IP アドレスを設定することで、R2 はネットワーク 3、ネットワーク 4、ネットワーク 5 を相互接続しています。

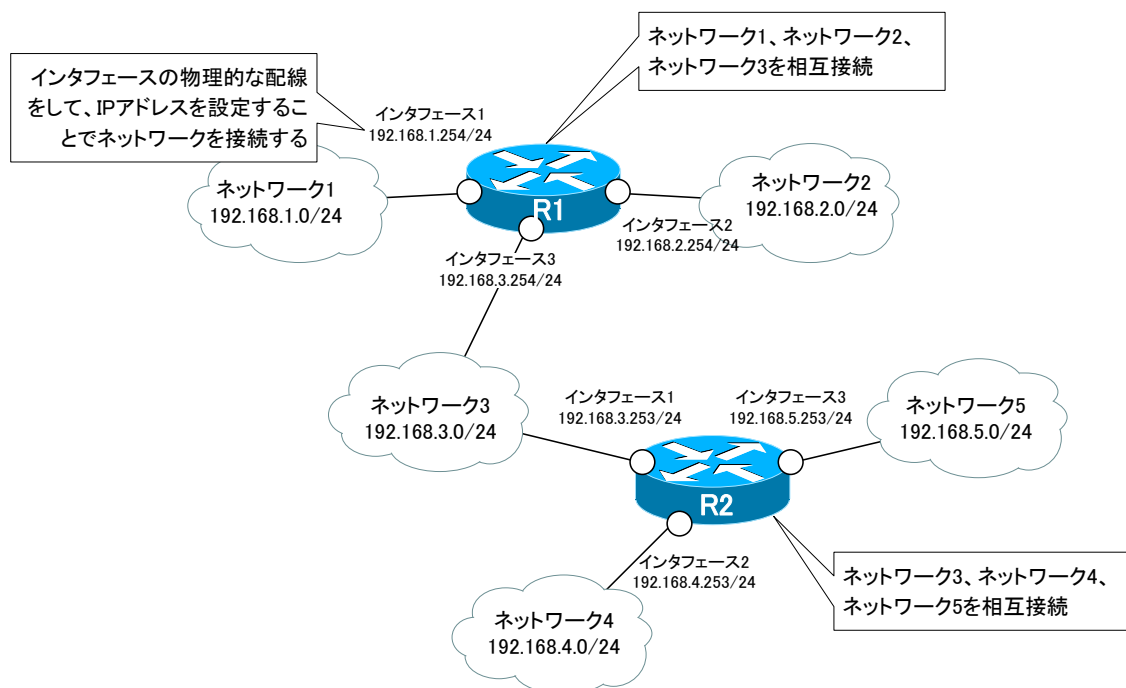


図 1 ルータでのネットワークの相互接続

## ルーティングの概要

ルータは IP アドレスに基づいてデータ(IP パケット)を適切なネットワークへ転送します。ただし、そのためにはルータにはあらかじめルーティングテーブルに転送先のネットワークの情報が登録されている必要があります。ルーティングするためには、まず、ルータのルーティングテーブルを作成することが大前提です。

ルータに IP パケットがやってくると、IP ヘッダに記されている宛先 IP アドレスとルーティングテーブルから次に転送すべきルータ(ネクストホップ)を判断して、IP パケットを転送します。ルーティングテーブルに登録されていないネットワーク宛での IP パケットは転送することができずに破棄されます。ルーティングテーブルにネットワークの情報を登録するということは、ルーティングを考える上でとても重要なことです。この点がレイヤ 2 スイッチの動作と大きく異なります。レイヤ 2 スイッチは「わからなければとりあえずフラッディング」という動作です。一方、ルータは「わからなければ破棄する」という動作です。

レイヤ 2 スイッチとルータのデータ転送の動作の違いは、転送範囲の違いによるものと考えるとよいでしょう。レイヤ 2 スイッチの転送範囲は同じネットワーク内だけです。とりあえずフラッディングしてもそれほど大きな影響は出ません。一方、ルータはネットワーク間のデータ転送です。わからないからとりあえず転送するようなことをしてしまうと、不要なデータ転送が多発する可能性が大きくなってしまいます。

図の R1 と R2 はルーティングテーブルに IP パケットを転送したいすべてのネットワークの情報を登録しておく必要があります。この図では、ネットワーク 1(192.168.1.0/24)～ネットワーク 5(192.168.5.0/24)の 5 つのネットワークです。そして、ホスト(192.168.1.100)からサーバ(192.168.5.100)へデータを転送するときには、宛先 IP アドレスは 192.168.5.100 が指定されます。R1 は宛先 IP アドレスに一致するルーティングテーブル上のネットワークの情報を検索します。すると、ネクストホップが R2 となっているので R2 へ IP パケットを転送します。「ホップ」とは多くの場合、ルータを

# 基礎からの CCNA(200-301)攻略テキスト

## 第 10 章 IP ルーティング

意味していて、ネクストホップは次に転送すべきルータです。

続いて、**R2** でも **IP** パケットに記されている宛先 **IP** アドレスとルーティングテーブルを見て、直接接続されているネットワーク **5(192.168.5.0/24)** 上のサーバへと **IP** パケットを転送します。

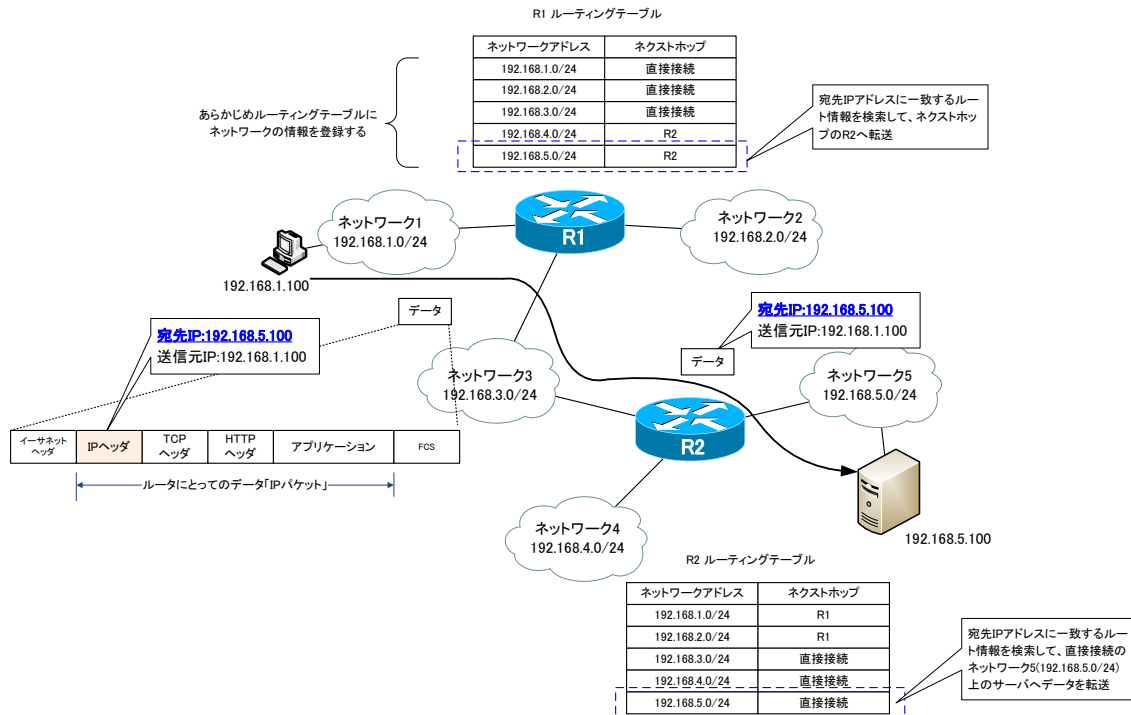


図 2 ルーティングの概要

## ネットワークの「分割」

ルータはネットワークの「分割」を行うためのネットワーク機器とも言えます。ルータはブロードキャストを通しません。そのため、ルータによってブロードキャストドメイン、すなわちネットワークを分割することができます。分割したネットワークは、ルータで相互接続されているので、分割されたネットワーク間の通信が可能です。

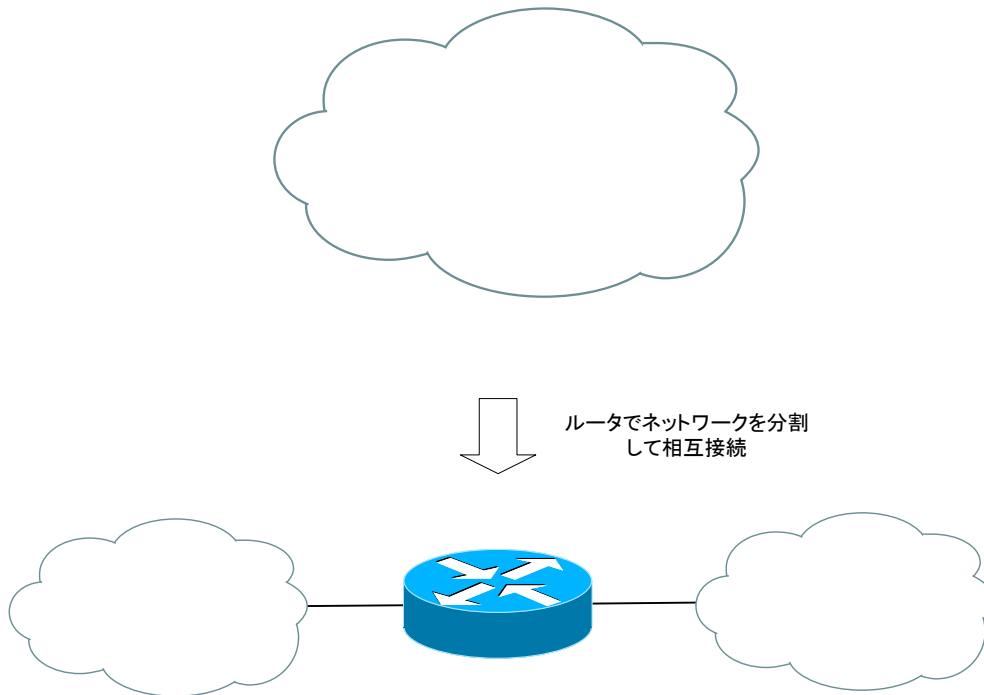


図 3 ルータによるネットワークの分割

## ネットワークを分割する理由

ルータでネットワークを分割できますが、なぜ、ネットワークを分割する必要があるのでしょうか？  
ネットワークを分割する主な理由は、次のとおりです。

- ・ 不要なデータの転送を制限する
- ・ セキュリティを確保する
- ・ 管理を効率化する

どのようにネットワークを分割するかについて、明確な基準はありません。ネットワークを設計する際にケースバイケースでネットワークの分割を考えていきます。企業の社内ネットワークであれば、多くの場合、

- ・ 部署などの業務単位での分割
- ・ フロアなどの物理的な配置による分割
- ・ 上記の組み合わせ

といった基準でネットワークの分割を検討します。

## 不要なデータ転送の制限

レイヤ 2 スイッチだけで構成する 1 つのネットワークにいろんな機器を接続するのが最もシンプルなネッ

ネットワーク構成です。ただし、このようなネットワーク構成では、不要なデータの転送がたくさん発生してしまうことになります。典型的な例が **ARP** でのアドレス解決です。**ARP** は **IP** アドレスから **MAC** アドレスを求めるためのプロトコルで、ブロードキャストを利用しています。

たとえば、同じレイヤ 2 スイッチに接続されているすぐ近くのホストの **MAC** アドレスを求めるために **ARP** リクエストを送信すると、他のレイヤ 2 スイッチも含めて同じネットワーク上のすべてにフラッディングされてしまうことになります。**ARP** リクエストは **MAC** アドレスを問い合わせる対象のホスト以外にとってはまったく関係ないのですが、**ARP** リクエストを受信して、自身が問い合わせ対象でないと判断して破棄します。この際、ホストに余計な処理が発生します。つまり、1 つのネットワークだと、ネットワーク上に **ARP** リクエストの余計なデータ転送も発生しますし、関係のないホストに対して余計な処理負荷をかけてしまうことになります。

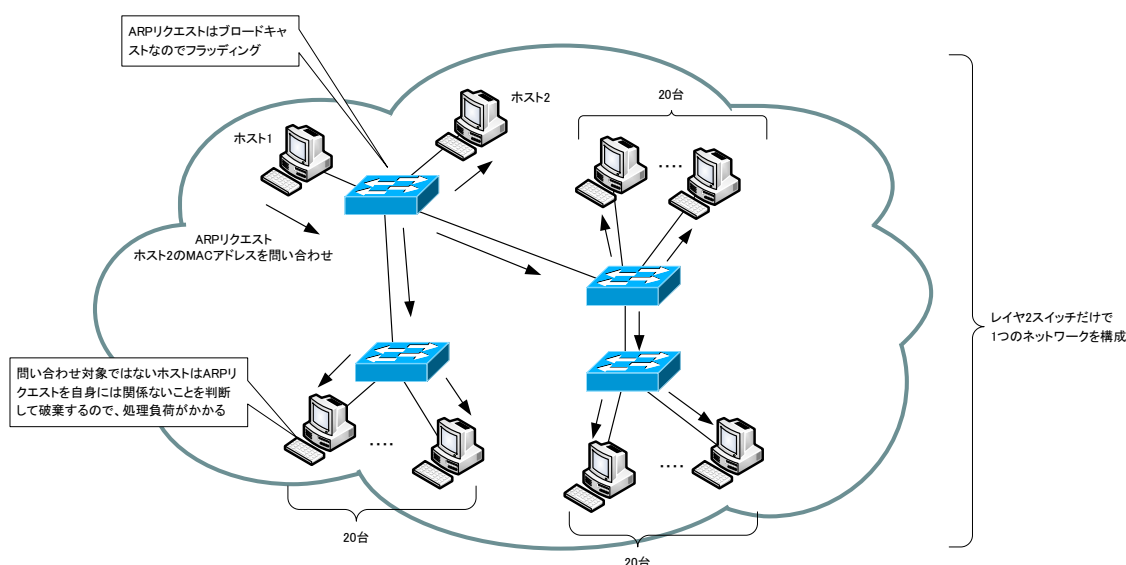


図 4 不要なデータ転送の例' (ARP リクエスト)

**ARP** リクエストのようなブロードキャストだけではなく、マルチキャストや **Unknown** ユニキャストもフラッディングされて、余計なデータ転送が発生してしまいます。

こうした余計なデータ転送やそれに伴うホストの処理負荷を軽減するため、適切な範囲でネットワークを分割します。

## セキュリティの確保

ネットワークを分割すると、ネットワーク間のデータは必ずルータを経由して行われます。ルータで転送するデータが正規の通信のデータであるかを追加でチェックすることができます。ルータという「関門」を設けることで、不正な通信を遮断してセキュリティの確保ができるようになります。

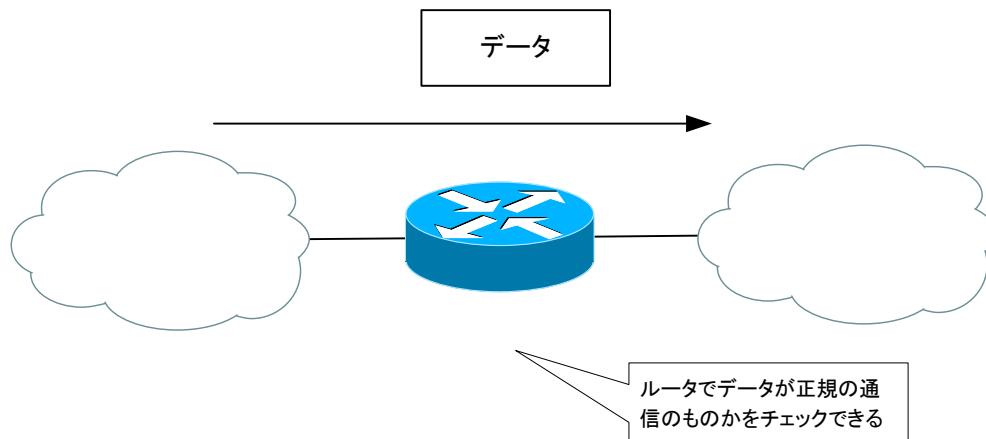


図 5 ルータでのデータのチェック

- ※ ルータで転送する際にセキュリティのチェックを行うためには、追加の設定が必要です。特別な設定をしていないと、ルーティングテーブルに載っている宛先でありさえすれば、転送します。**Cisco** のルータでは主にアクセスコントロールリストの設定を行います。
- ※ 企業向けのレイヤ 2 スイッチであれば、転送するデータのチェックを行うこともできる製品がありますが、ルータほど柔軟なチェックができないことがほとんどです。

## 管理の効率化

企業の社内ネットワークを複数の拠点にもまたがるような 1 つのネットワークとして構成すると、管理が煩雑になってしまいます。適切な範囲でネットワークを分割することで、管理する対象のネットワークの範囲を限定して、管理を効率よく行うことができます。



## レイヤ 3 スイッチ

### ポイント

- ・ ルータの機能を組み込んだレイヤ 2 スイッチがレイヤ 3 スイッチです。
- ・ ルータと同じような役割、目的で利用されることが多く、ルータ≒レイヤ 3 スイッチと考えて差し支えありません。
- ・ CCNA 試験ではあまり重要ではなく概要だけ知っておけば OK ですが、現在のネットワークでは幅広くレイヤ 3 スイッチが利用されています。

### レイヤ 3 スイッチの役割

レイヤ 3 スイッチは、VLAN によってネットワーク構成を柔軟に決めることができ、主に企業ネットワークで複数のネットワークを相互接続するために利用します。

レイヤ 3 スイッチは、レイヤ 2 スイッチにルータの機能を追加しているネットワーク機器です。そのため、レイヤ 2 スイッチのようなデータの転送もできますし、ルータのようなデータの転送もできます。レイヤ 3 スイッチの外観は、レイヤ 2 スイッチとよく似ています。レイヤ 2 スイッチと同じようにたくさんのイーサネットインタフェースを備えたネットワーク機器です。

ここで、レイヤ 2 スイッチとルータのデータの転送の特徴をあらためて以下の表にまとめています。

表 1 レイヤ 2 スイッチとルータのデータ転送の特徴

特徴	レイヤ 2 スイッチ	ルータ
データ	イーサネットフレーム	IP パケット
データの転送範囲	同一ネットワーク内	ネットワーク間
転送するためのテーブル	MAC アドレステーブル	ルーティングテーブル
転送するときに参照するアドレス	MAC アドレス	IP アドレス
テーブルに必要な情報がないときの動作	データをフラッディング	データを破棄

レイヤ 3 スイッチは、ルータと同じようにネットワークの相互接続ができます。そして、同一ネットワークのデータの転送のときはレイヤ 2 スイッチ同じように MAC アドレスに基づいて転送します。一方、ネットワーク間のデータ転送のときはルータと同じように IP アドレスに基づいてデータの転送を行います。

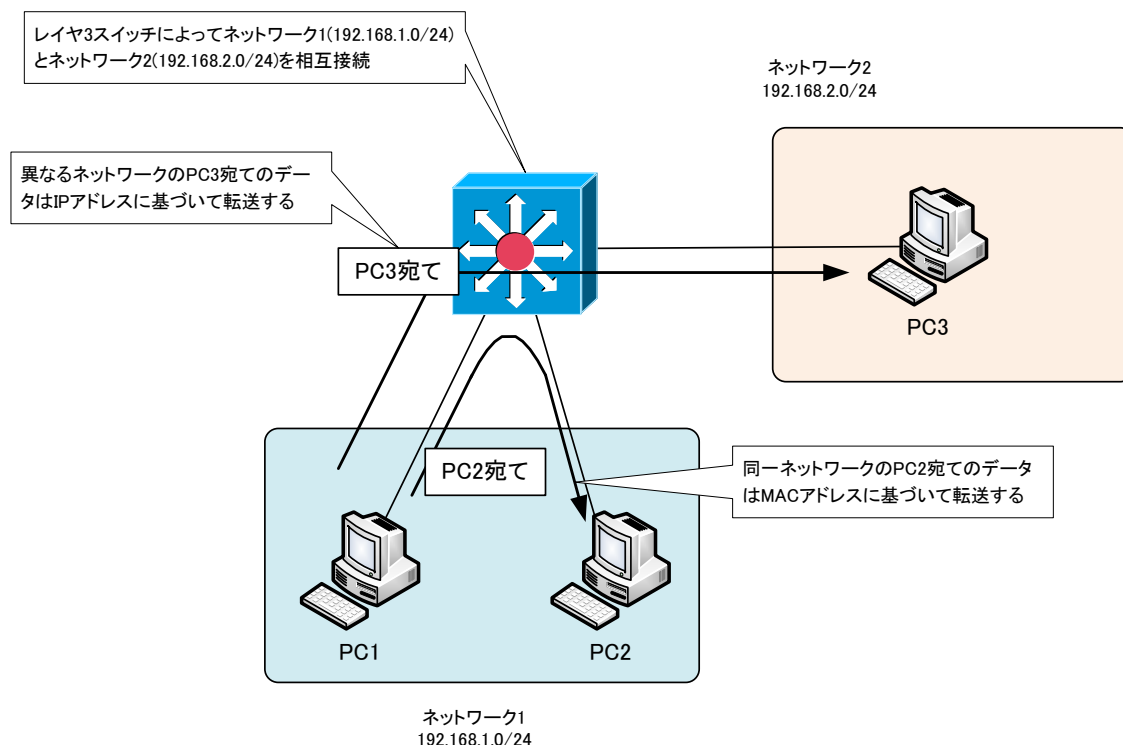


図 6 レイヤ 3 スwitch の概要

この図で、レイヤ 3 スwitch はネットワーク 1 (192.168.1.0/24) とネットワーク 2 (192.168.2.0/24) を相互接続しています。そして、PC1 と PC2 は同じネットワークとなり、PC3 は違うネットワークとしています。このようなネットワーク構成を取るために、レイヤ 3 スwitch で VLAN (Virtual LAN) の機能を利用します。レイヤ 3 スwitch の仕組みを知る上では、VLAN を理解することが必須です。

## レイヤ 3 スwitch の用途

レイヤ 3 スwitch は、企業の社内ネットワークで複数のネットワークを相互接続して、ネットワーク間の通信ができるようにする用途で利用されることが多いです。つまり、レイヤ 2 スwitch としてよりも、ルータとしての用途がメインです。

企業の社内ネットワークは、レイヤ 2 スwitch とレイヤ 3 スwitch で構成されることがほとんどです。オフィスのフロアのクライアント PC はまず、レイヤ 2 スwitch に接続します。ネットワークの入り口に相当するレイヤ 2 スwitch は「アクセスス위치」と呼ばれます。

そして、フロアのレイヤ 2 スwitch を集約するためにレイヤ 3 スwitch を利用します。レイヤ 3 スwitch でフロアのネットワーク間の通信ができるようにします。フロアのアクセスス위치を集約するレイヤ 3 スwitch は「ディストリビューションス위치」と呼ばれます。

アクセスス위치とディストリビューションス위치で 1 つの建物のネットワークを構成します。大規模な社内ネットワークであれば、敷地内に複数の建物が存在します。当然ながら、建物のネットワーク同士も相互接続しなければいけません。建物のネットワークの相互接続にもレイヤ 3 スwitch を利用します。こうした建物のネットワーク間の相互接続のためのレイヤ 3 スwitch は「コアス위치」または「バックボーンス위치」

と呼ばれます。

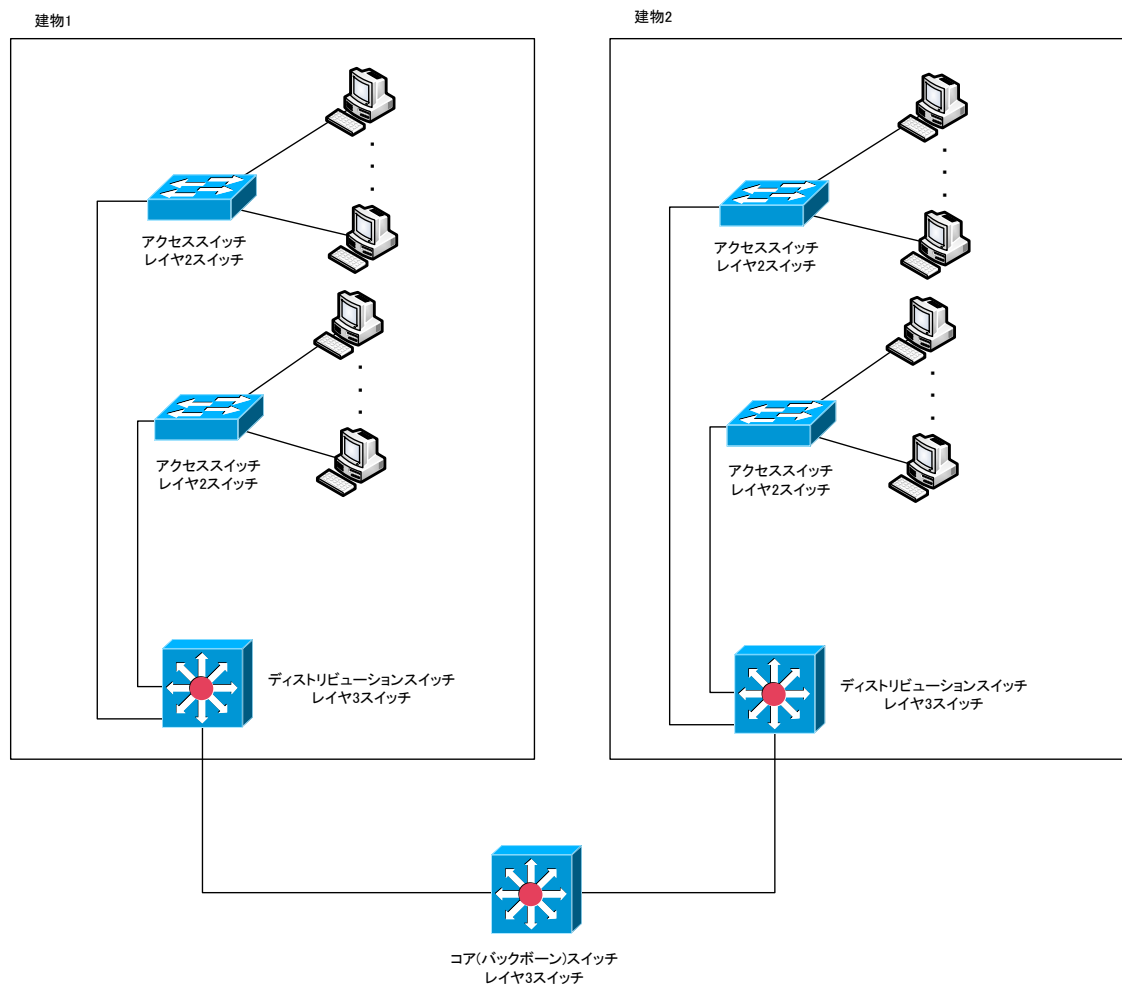


図 7 レイヤ 3 スwitchの用途の例

※ ある程度規模が大きくなると、ディストリビューションスイッチやコアスイッチのレイヤ 3 スwitchは冗長化します。上記の図は、シンプルにするためにレイヤ 3 スwitchの冗長化は考慮していません。

## レイヤ 3 スイッチ≒ルータ

レイヤ 3 スイッチはルータと同じような用途で利用されているので、レイヤ 3 スイッチ≒ルータと考えて差し支えありません。一応、ルータとレイヤ 3 スイッチの特徴の違いとして以下のようなことが挙げられます。

表 2 ルータとレイヤ 3 スイッチの特徴の違い

特徴	ルータ	レイヤ 3 スイッチ
インタフェースの種類	イーサネット以外にもいろんなインタフェースを利用可能	基本的にイーサネットのみ
インタフェースの数	それほど多くの数のインタフェースを備えていない	製品によっては数百以上の数のインタフェースを備えている
機能の拡張性	ソフトウェアのアップデートで機能拡張が可能	機能拡張があまりできない
データの転送性能	あまり高くない	理論的な最大の転送性能を発揮できる

ただ、現在ではこの表にまとめたルータとレイヤ 3 スイッチの特徴の違いは、ほとんどなくなっています。

レイヤ 3 スイッチにも製品によって、イーサネット以外のインタフェースを搭載できるものも増えています。イーサネットインタフェースだけで用が足りることがほとんどなので、対応するインタフェースの種類はあまり問題になりません。たくさんのイーサネットインタフェースを備えたルータも増えています。

レイヤ 3 スイッチでもソフトウェアのアップデートであとから機能拡張できるようになってきています。また、ルータのデータの転送性能も高くなってきていて、理論的な最大の転送性能を発揮できる製品も多くあります。

先にも述べましたが、「ルータ」と「レイヤ 3 スイッチ」というネットワーク機器の種類として分類されますが、現在ではほとんど同じだと考えて差し支えありません。

## ルーティングの動作

### ポイント

- ・ ルータがルーティングするにしたがって、レイヤ 2 ヘッダは書き換わっていきます。
- ・ ルーティングするときのレイヤ 2 ヘッダの書き換えの仕組みは CCNA 試験でとても重要です。

### ルータのデータ転送の流れ

ルータのデータ(IP パケット)の転送の流れは以下のようになります。

1. ルーティング対象の IP パケットを受信する
2. 宛先 IP アドレスからルーティングテーブル上のルート情報を検索して、転送先を決定する
3. レイヤ 2 ヘッダを書き換えて IP パケットを転送する

なお、ルータが IP パケットを転送するには、あらかじめルーティングテーブルに転送先のネットワークの情報(ルート情報)が登録されていることが大前提です。ルーティングテーブルの詳細やルーティングテーブルにルート情報を登録する方法は、次項で解説します。

以下のネットワーク構成でホスト 1 からホスト 2 に IP パケットを送信する場合を例にして、ルータが IP パケットを転送していく様子を解説していきます。

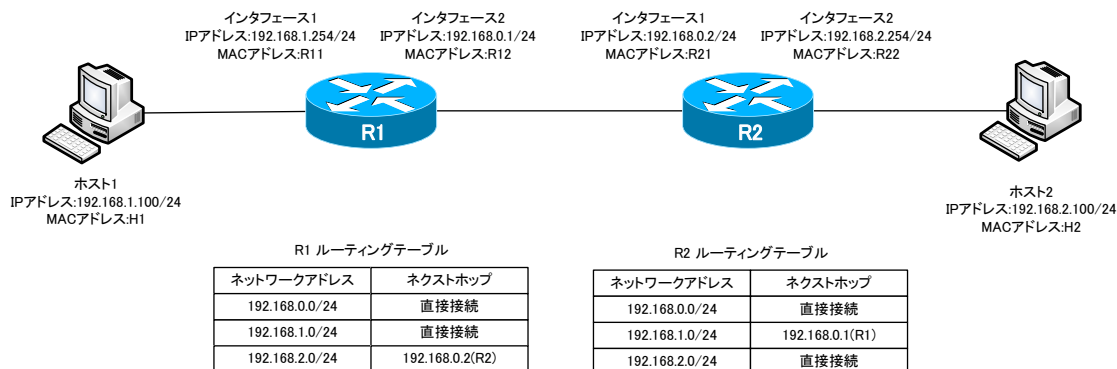


図 8 ルータのデータ転送 ネットワーク構成例

※ すべてのイーサネットインタフェースとしています。また、ネットワーク構成を簡単にするために、レイヤ 2 スイッチを介さずに各イーサネットインタフェース間を直接接続しているものとします。

## ルーティング対象の IP パケットの受信 R1

ルータがルーティングする対象の IP パケットは、以下のようなアドレス情報のパケットです。

宛先レイヤ 2 アドレス(MAC アドレス):ルータ

宛先 IP アドレス:ルータの IP アドレス以外

ホスト 1 からホスト 2 宛ての IP パケットは、まず、R1 へ転送されます。そのときのアドレス情報は、以下のようになっています。

宛先 MAC アドレス:R1 I

送信元 MAC アドレス:H I

宛先 IP アドレス:192.168.2.100

送信元 IP アドレス:192.168.1.100

宛先 MAC アドレスが R1 のもので、宛先 IP アドレスは R1 ではなくホスト 2 の IP アドレスです。受信した IP パケットはルーティング対象の IP パケットです。

## ルーティングテーブルの検索 R1

R1 はルーティング対象のパケットの宛先 IP アドレスに一致するルーティングテーブルのルート情報を検索します。宛先 IP アドレス 192.168.2.100 に一致するルート情報は 192.168.2.0/24 です。そのため、転送先のネクストホップ(次のルータ)は 192.168.0.2、すなわち R2 であることがわかります。

# 基礎からの CCNA(200-301)攻略テキスト

## 第 10 章 IP ルーティング

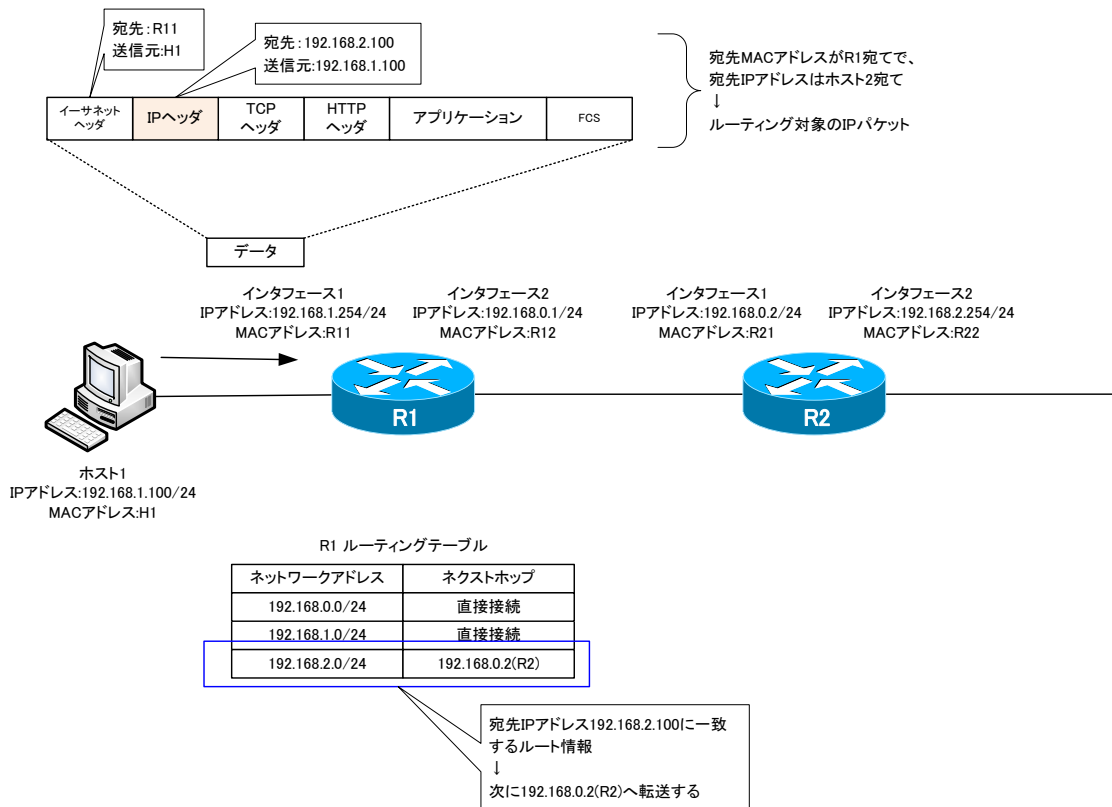


図 9 R1 ルーティング対象 IP パケットの受信とルーティングテーブルの検索

※ 図では、例として HTTP のデータとしています。ルータは単純なルーティングを行うときにはトランスポート層以降の部分はチェックしません。

### レイヤ 2 ヘッダを書き換えて IP パケットを転送 R1

R1 はルーティングテーブルのルート情報から受信した IP パケットを 192.168.0.2(R2)へ転送します。そのために、R2 の MAC アドレスが必要です。ルーティングテーブル上の一致するルート情報のネクストホップアドレスである R2(192.168.0.2)の MAC アドレスを求めるために ARP を行います。ARP で宛先 MAC アドレス R21 がわかれば、新しいイーサネットヘッダに書き換えて IP パケットをインタフェース 2 から転送します。レイヤ 2 ヘッダであるイーサネットヘッダはまったく新しくなります。しかし、IP ヘッダの IP アドレスはまったく変わりません。

※ IP ヘッダでは、TTL を -1 して、それとともなってヘッダチェックサムの再計算を行います。

※ ルータで NAT を行うときには IP アドレスが書き換えられます。単純なルーティングを行うときには、IP アドレスは変わりません。

# 基礎からの CCNA(200-301)攻略テキスト

## 第 10 章 IP ルーティング

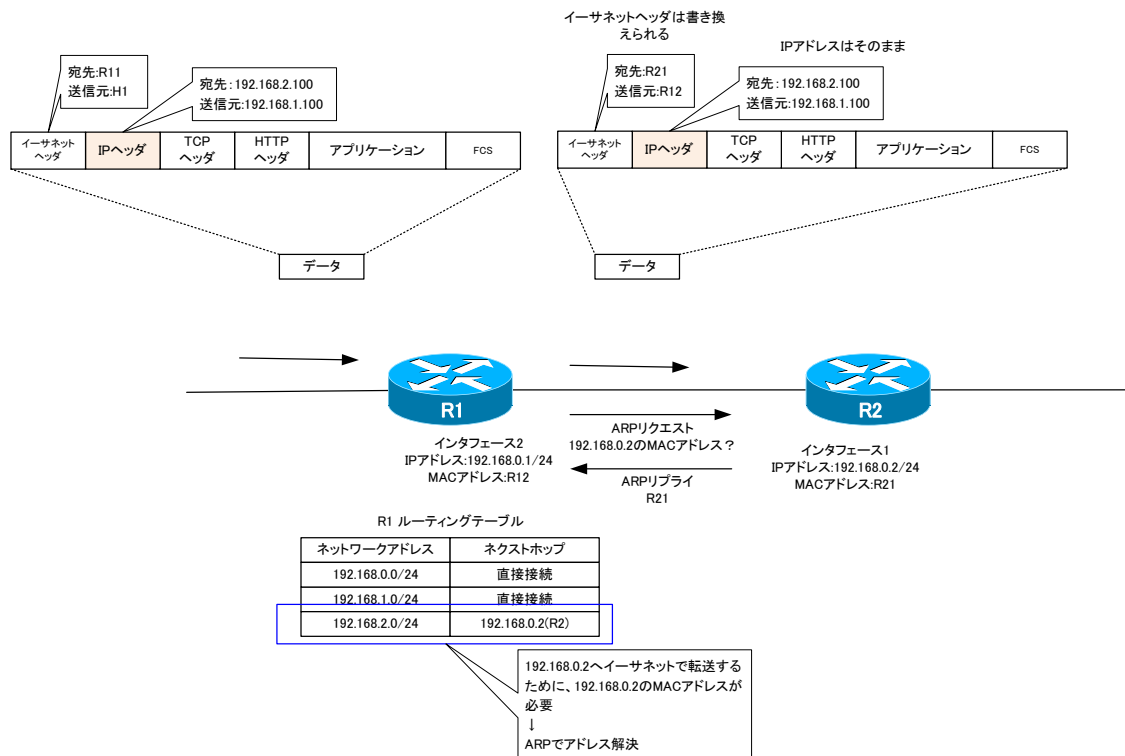


図 10 R1 レイヤ 2 ヘッダを書き換えて IP パケットを転送

### ルーティング対象の IP パケットの受信 R2

R1 から転送された IP パケットは R2 で受信します。このときの IP パケットのアドレス情報は以下のとおりです。

宛先 MAC アドレス:R21

送信元 MAC アドレス:R12

宛先 IP アドレス:192.168.2.100

送信元 IP アドレス:192.168.1.100

ホスト 1 が送信したものと MAC アドレスは書き換わっていますが、IP アドレスは同じです。宛先 MAC アドレスが R2 の MAC アドレスで宛先 IP アドレスは R2 の IP アドレスではありません。これはルーティング対象の IP パケットです。

### ルーティングテーブルの検索 R2

R2 はルーティングするために宛先 IP アドレス 192.168.2.100 に一致するルート情報を検索します。すると、192.168.2.0/24 のルート情報が見つかります。ネクストホップは直接接続となっていて、最終的な宛先 IP アドレス 192.168.2.100 は R2 と同じネットワーク上だということがわかります。



基礎からの CCNA(200-301)攻略テキスト  
第 10 章 IP ルーティング

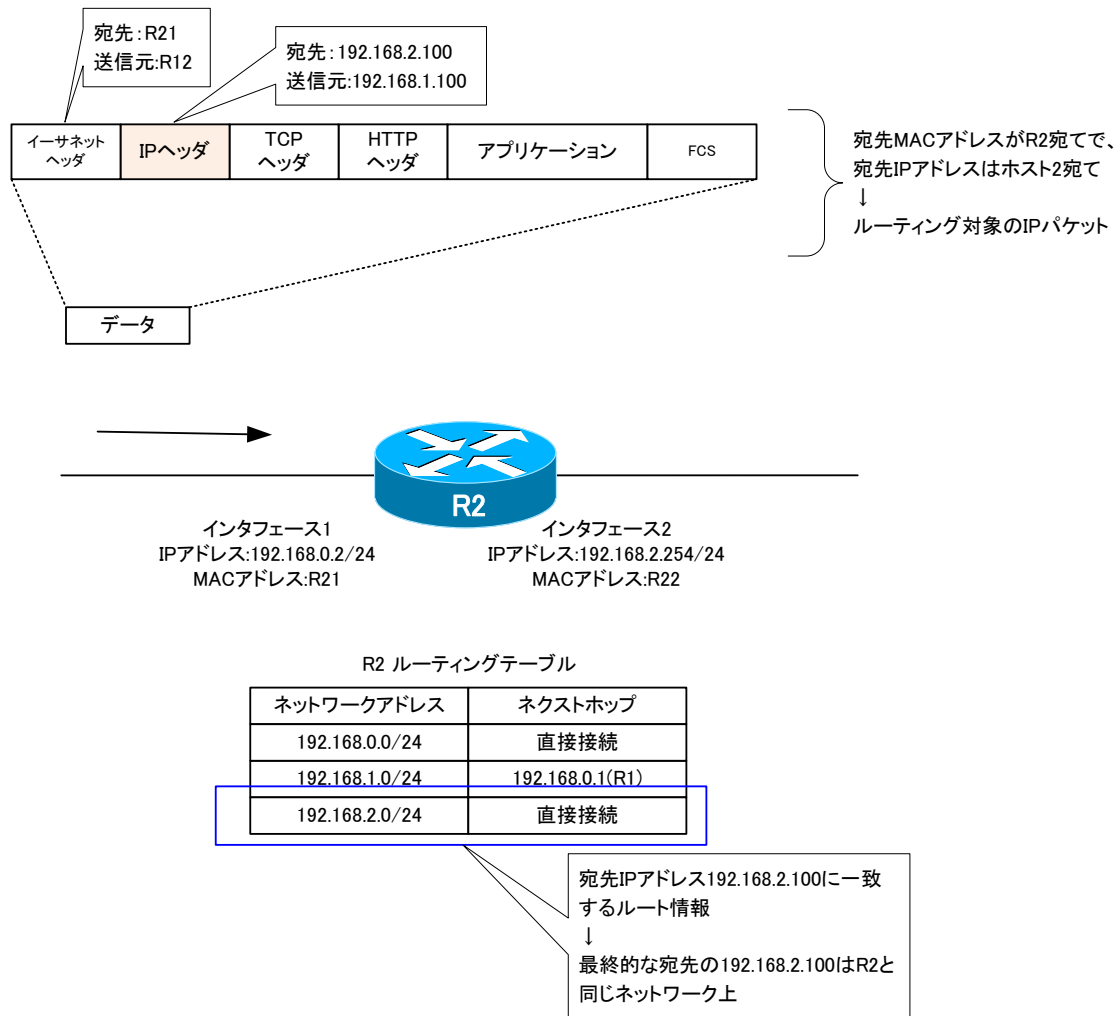


図 11 R2 ルーティング対象 IP パケットの受信とルーティングテーブルの検索

## レイヤ 2 ヘッダを書き換えて IP パケットを転送 R2

R2 はルーティングテーブルのルート情報から、IP パケットの最終的な宛先である 192.168.2.100(ホスト 2)は、R2 のインタフェース 2 と同じネットワーク上にあることがわかります。ホスト 2 へ IP パケットを転送するためには、ホスト 2 の MAC アドレスが必要です。そこで、IP パケットの宛先 IP アドレス 192.168.2.100 の MAC アドレスを求めるために ARP を行います。

ARP でホスト 2 の MAC アドレス H2 がわかれば、新しいイーサネットヘッダを付けて、R2 のインタフェース 2 から IP パケットを転送します。やはり、R2 で受信したときとは MAC アドレスは変わりますが、IP アドレスは同じです。

# 基礎からの CCNA(200-301)攻略テキスト

## 第 10 章 IP ルーティング

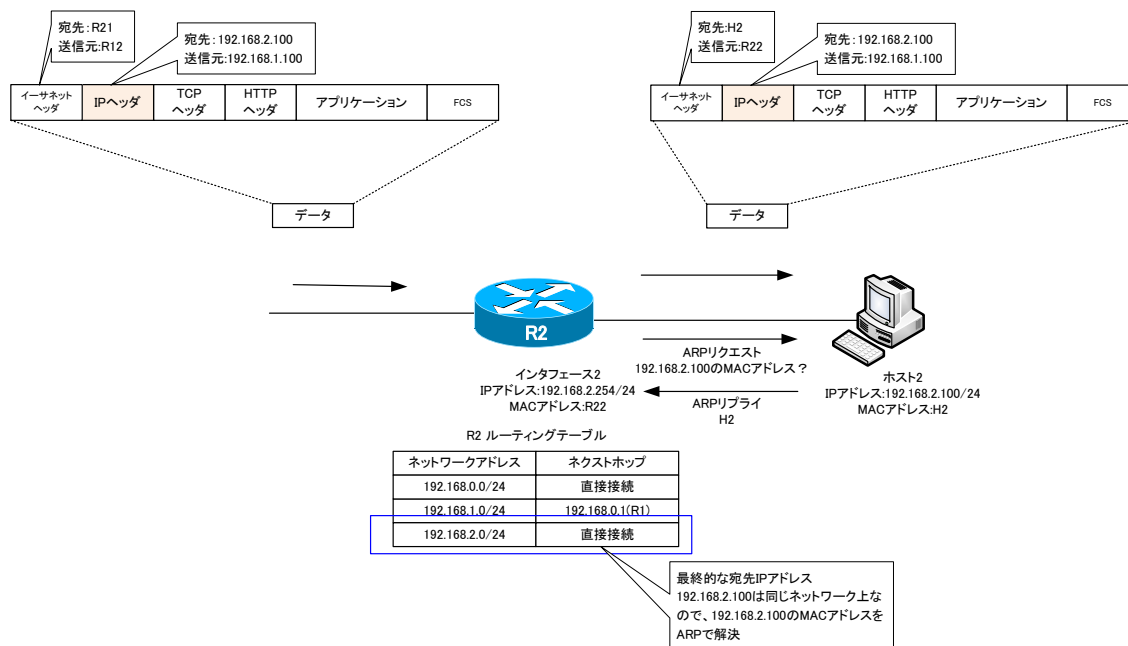


図 12 R2 レイヤ 2 ヘッダを書き換えて IP パケットを転送

R2 で転送した IP パケットは無事に最終的な宛先となっているホスト 2 まで届くことになります。

また、以降の解説は省略しますが、通信は原則として双方向であるということをあらためて思い出してください。ホスト 1 からホスト 2 へ何かデータを送信すると、その返事としてホスト 2 からホスト 1 へデータの送信が発生します。ホスト 2 からホスト 1 へ送信するデータも同じようにルータが宛先 IP アドレスとルーティングテーブルから転送先を判断します。そして、レイヤ 2 ヘッダを書き換えながら転送していくことになります。

こうしたルータのルーティングの動作は、前述のように

「ルーティングテーブルが完成していることが大前提」

です。ルーティングにおいてとても重要なルーティングテーブルについて、次項で見ていきましょう。

## ルーティングは電車の乗り換えのようなイメージ

ルータが IP パケットをルーティングするときに、イーサネットヘッダなどのレイヤ 2 ヘッダが書き換わっていきます。レイヤ 2 は同じネットワーク上のデータの転送を行う役割があります。ルータを超えるとネットワークが変わるので、レイヤ 2 ヘッダも書き換わっていきます。このようなルータを超えると、レイヤ 2 ヘッダが書き変わっていくことは、電車の乗り換えのようなイメージで考えてください。

ネットワークの通信で最終的な宛先が他のネットワーク上に接続されているというのは、電車で行きたい駅が最寄駅とは電鉄会社または路線が違ようなイメージです。電鉄会社や路線が違うと、直通で目的の駅までは行けません。ターミナル駅で乗り換えしなければいけません。ターミナル駅がルータに相当します。

TCP/IP 通信では、最終的に IP パケットを宛先のホストまで届けるようにします。そのために、同じネットワーク上の転送をどんどん繰り返します。同じネットワーク上の転送のために、イーサネットなどのレイヤ 2 ヘッダを付けていきます。ルータを超えてネットワークが変わると、レイヤ 2 ヘッダも変わっていきます。

IP パケットに相当するのが、目的の駅まで行きたい人です。電鉄会社が違うと、一本で目的の駅には行けないので、ターミナル駅で電車を乗り換えていきます。レイヤ 2 ヘッダが電車が相当するイメージです。

そして、ルーティングでも電車の乗り換えでも大事なことは、きちんと宛先を知っていることが大前提です。ルーティングではルータのルーティングテーブルがきちんと完成していなければいけません。目的の駅まで到達するためには、どこでどの電気に乗り換えればよいかかわかっていなければいけないのと同じです。

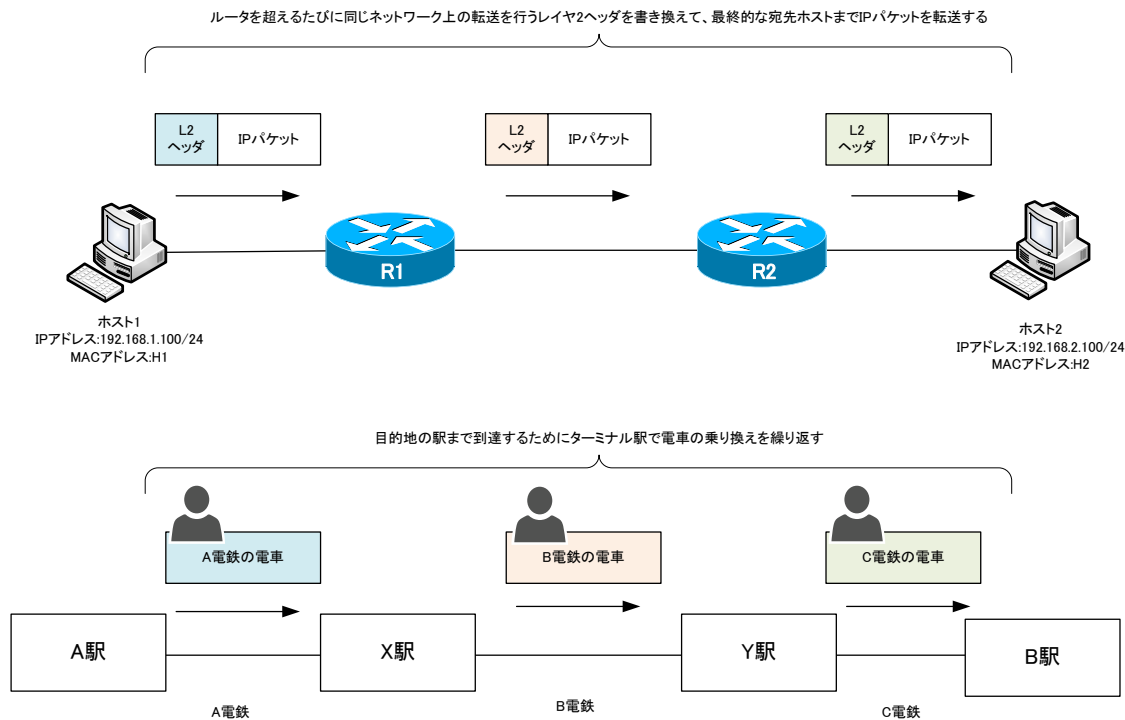


図 13 ルーティングと電車の乗り換え

# ルーティングテーブル

## ポイント

- ・ ルータがルーティングするための大前提は、ルーティングテーブルにデータを転送したい宛先ネットワークのルート情報が登録されていることです。
- ・ ルーティングテーブルに登録されていない未知のネットワーク宛てのデータは破棄します。

## ルーティングテーブルとは

ルーティングテーブルとは、ルータが認識しているネットワークの情報をまとめているデータベースです。

あるネットワークへ IP パケットを転送するためにどのような経路であるかが登録されています。経路とは、具体的には、次に転送するべきルータ(ネクストホップ)です。ルーティングテーブルに登録されているネットワークの情報をルート情報や経路情報と呼びます。

## ルート情報の内容

ルーティングテーブル上のルート情報にどのようなことが記載されているかは、ルータの製品によって若干異なります。企業向けのルータでよく利用されている **Cisco Systems** 社のルータでは、ルート情報として次のような内容が含まれています。

- ・ ルート情報の情報源

どのようにしてルータがルート情報をルーティングテーブルに登録したのかを示しています。ルート情報の情報源として、大きく次の 3 種類あります。

- 直接接続
- スタティックルート
- ルーティングプロトコル

- ・ ネットワークアドレス/サブネットマスク

IP パケットを転送する宛先のネットワークです。IP パケットの宛先 IP アドレスをキーにして、ルート情報のネットワークアドレス/サブネットマスクを検索します。このときの検索は、最長一致検索です。最長一致検索の詳細は、後述します。

- ・ メトリック

メトリックは、ルータから目的のネットワークまでの距離を数値化したものです。距離といっても物理的な距離ではなく、ネットワーク的な距離です。

メトリックの情報は、ルーティングプロトコルによって学習したルート情報の中にあります。ルーティングプロトコルによって、どのような情報からメトリックを算出するかという計算方法が異なりますが、最終的には一つの数値になります。距離は短い方がよりよいルートと考えられるので、メトリック最小のルートが最適ルートです。

メトリックは「コスト」と表現することもあります。

ルーティングプロトコルごとのメトリックとして考えている要素は以下のようになります。

表 3 メトリック

ルーティングプロトコル	メトリックの要素
RIP	経由するルータ台数(ホップ数)
OSPF	累積コスト(ネットワークの通信速度)
EIGRP	帯域幅、遅延、負荷、信頼性、MTU から計算される値

- ・ アドミニストレイティブディスタンス(Cisco)

メトリックはルーティングプロトコルごとに計測している目的のネットワークまでの距離を表しています。ですが、ルーティングプロトコルごとにメトリックとしてどのような要素を考慮しているかが異なります。ルーティングプロトコルごとに異なるメトリックを比較できるように調節するパラメータがアドミニストレイティブディスタンスです。つまり、アドミニストレイティブディスタンスとメトリックによって、ルータは目的のネットワークまでの距離を認識します。

- ・ ネクストホップアドレス

「ホップ」とはルータを指します。目的のネットワークへパケットを送り届けるために、次に転送すべきルータの IP アドレスです。ネクストホップアドレスは、原則としてルータと同じネットワーク内の他のルータの IP アドレスです。

- ・ 出力インタフェース

目的のネットワークへパケットを転送するときに、パケットを出力するインタフェースの情報です。ネクストホップアドレスと出力インタフェースを合わせて、目的のネットワークまでの方向と考えることができます。

- ・ 経過時間

ルーティングプロトコルで学習したルート情報について、ルーティングテーブルに登録されてから経過した時間が載せられます。経過時間が長ければ長いほど、安定したルート情報です。

以下は、Cisco ルータのルーティングテーブルの例です。

図 14 ルーティングテーブルの例

ルーティングテーブルは、ルータが認識しているネットワーク構成ということもできます。例に挙げたルーティングテーブルを持つルータ **R1** がどんな風にネットワーク構成を認識しているかを見ていきます。

- 10.1.1.0/24 FastEthernet0/0
- 10.1.2.0/24 Serial0/1

**| 0-20 |**

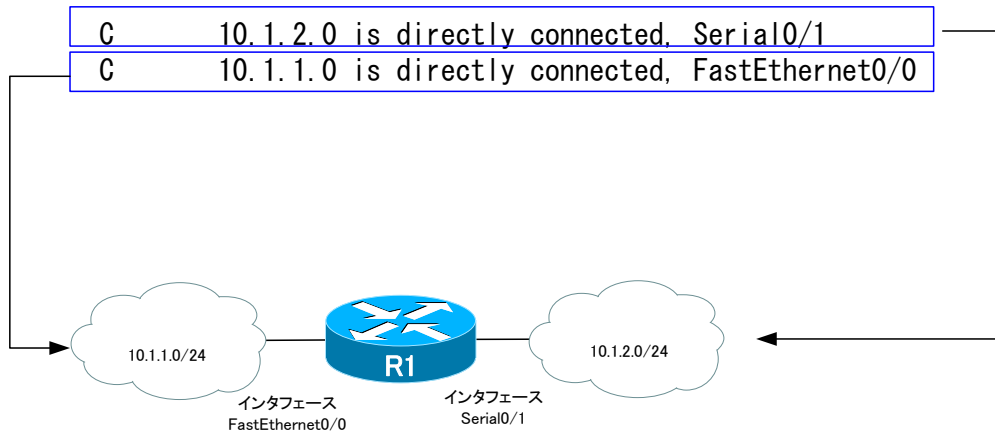


図 15 直接接続のルート情報

次に先頭に「S」と表示されているルート情報が以下の 3 つあります。

- ・ 172.16.0.0/16
- ・ 172.17.0.0/16
- ・ 192.168.1.0/24

これは、スタティックルートの設定によってルーティングテーブルに登録されたルート情報であることを表しています。3 つのルート情報で「via 10.1.2.2」と共通しています。この部分はネクストホップアドレスで次に転送するべき隣のルータの IP アドレスです。10.1.2.0/24 のネットワーク上には 10.1.2.2 という IP アドレスのルータが存在していて、そのルータの向こう側に 3 つのネットワークがあると認識しています。

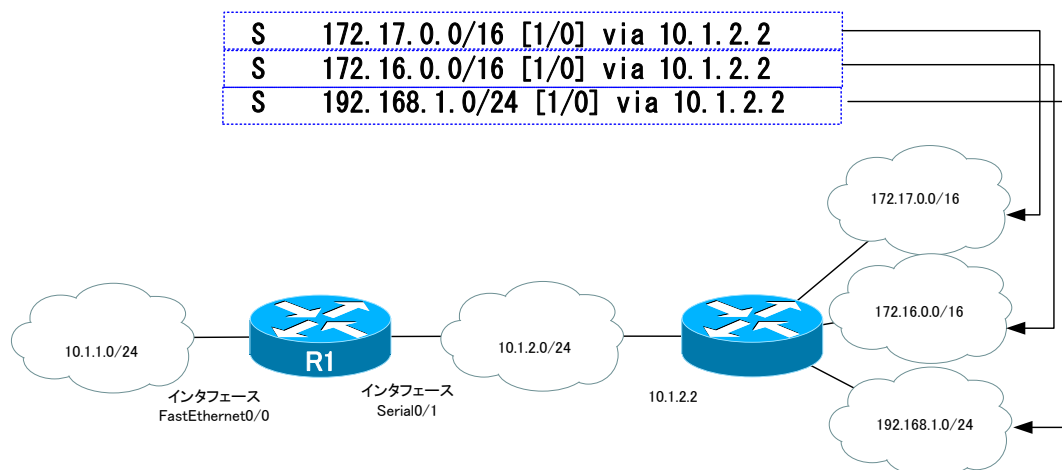


図 16 スタティックルートのルート情報

なお、R1 が認識しているのは 3 つのネットワークが 10.1.2.2 の IP アドレスを持つルータの向う側にあるということだけです。10.1.2.2 のルータに直接接続されているのではなく、さらに他のルータを経由しなければいけないかもしれません。

そして、もう 1 つ「R」と表示されている 10.1.3.0/24 のネットワークがあります。「R」は **RIP** というルーティングプロトコルによってルーティングテーブルに登録されたルート情報であることを意味しています。ネクストホップは「10.1.2.2」で、この IP アドレスのルータの先に 10.1.3.0/24 のネットワークがあります。**RIP** のようなルーティングプロトコルで登録されたルート情報には、距離が載せられています。「[120/1]」の部分が距離です。このルーティングテーブルを持つ R1 から [120/1] だけ離れたところに 10.1.3.0/24 のネットワークがあることがわかります。**RIP** の場合、経由するルータ台数を距離とみなします。つまり、10.1.3.0/24 は 10.1.2.2 のルータに直接接続されているということがわかります。

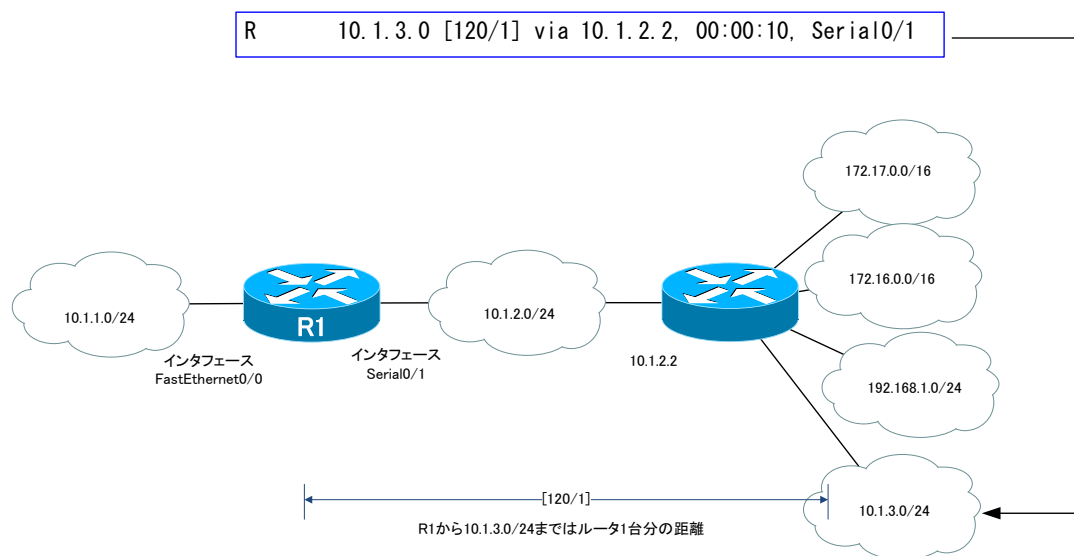


図 17 RIP のルート情報

※ スタティックルートのルート情報には「[1/0]」という距離の情報がありますが、スタティックルートの場合は、基本的に距離は意味がありません。

以上のように、ルーティングテーブルによって、そのルータがどのようなネットワーク構成であるかを認識しています。ただし、ネットワーク全体の詳細な構成ではなく、**自身を中心としてネクストホップ(隣のルータ)の向こう側にどんなネットワークが存在するかというレベルです**。IP によるエンドツーエンドの通信は、同じネットワーク上の転送を繰り返していくわけなので、隣のルータまで転送できればよいです。隣のルータの先のネットワーク構成の詳細まで知っておく必要はありません。

ルーティングテーブル上で認識できないネットワーク宛ての IP パケットはすべて破棄します。そのため、ルータがきちんとルーティングするためにはルーティングテーブルに必要なルート情報をすべてもれなく登録しておかなければいけません。これは 1 台のルータだけではなく、ネットワーク上のすべてのルータです。そして、**ネットワーク上のすべてのルータのルーティングテーブルに必要なルート情報が登録されている状態**を指して「**コンバージェンス(収束)**」と呼びます。



## パケットの転送経路

ルーティングテーブルは、ルータが認識しているネットワーク構成であると同時にパケットの転送経路を表してもいます。ルーティングテーブルには、原則として、宛先ネットワークへの最適ルートのみが登録されます。宛先ネットワークまでのルートが冗長化されている場合、迂回ルートはルーティングテーブルには載せられていません。各ルータのルーティングテーブルをたどっていくことで、パケットが転送される経路がわかります。

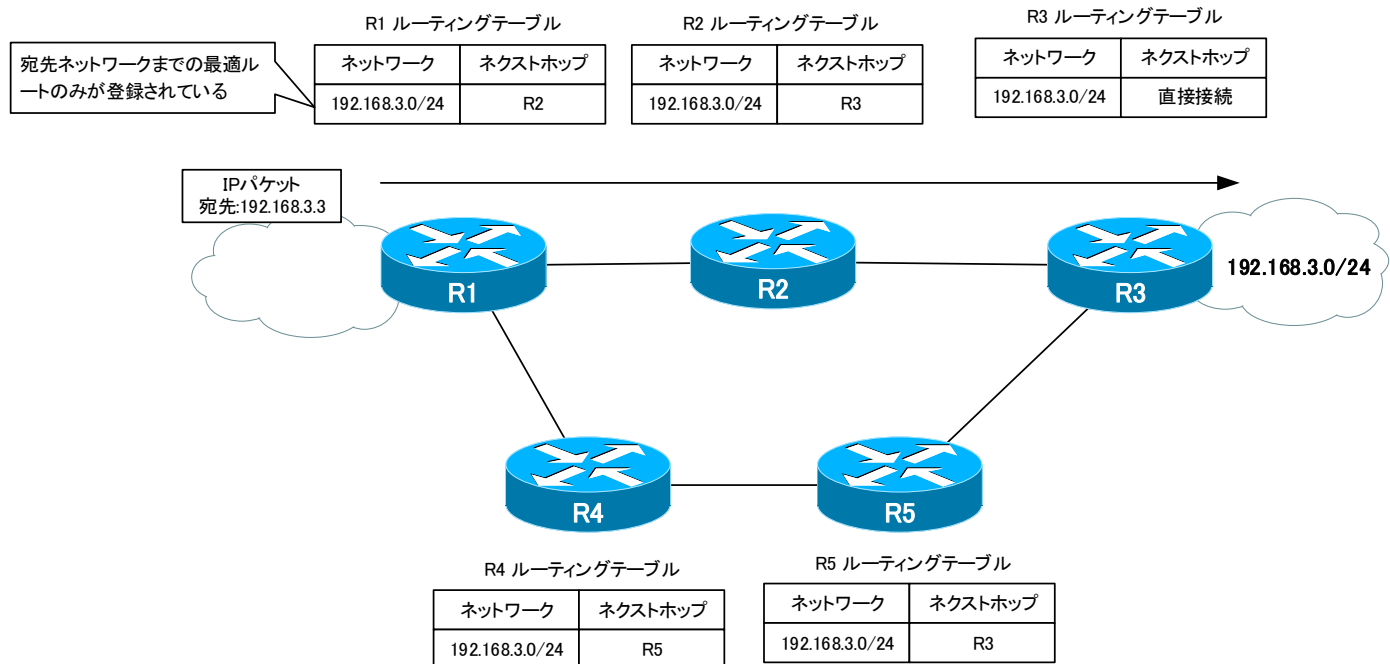


図 18 パケットの転送経路

※ ルーティングプロトコルによっては、迂回ルートもルーティングテーブルに載せられることがあります。

そして、ネットワークの障害などでネットワーク構成が変化した場合は、パケットの転送経路となるルーティングテーブルを更新しなければいけません。ルーティングテーブルの更新もコンバージェンスの一種です。ルーティングテーブルが適切に更新されなければ、パケットのルーティングが正常にできずに通信できなくなってしまいます。

基礎からの CCNA(200-301)攻略テキスト  
第 10 章 IP ルーティング

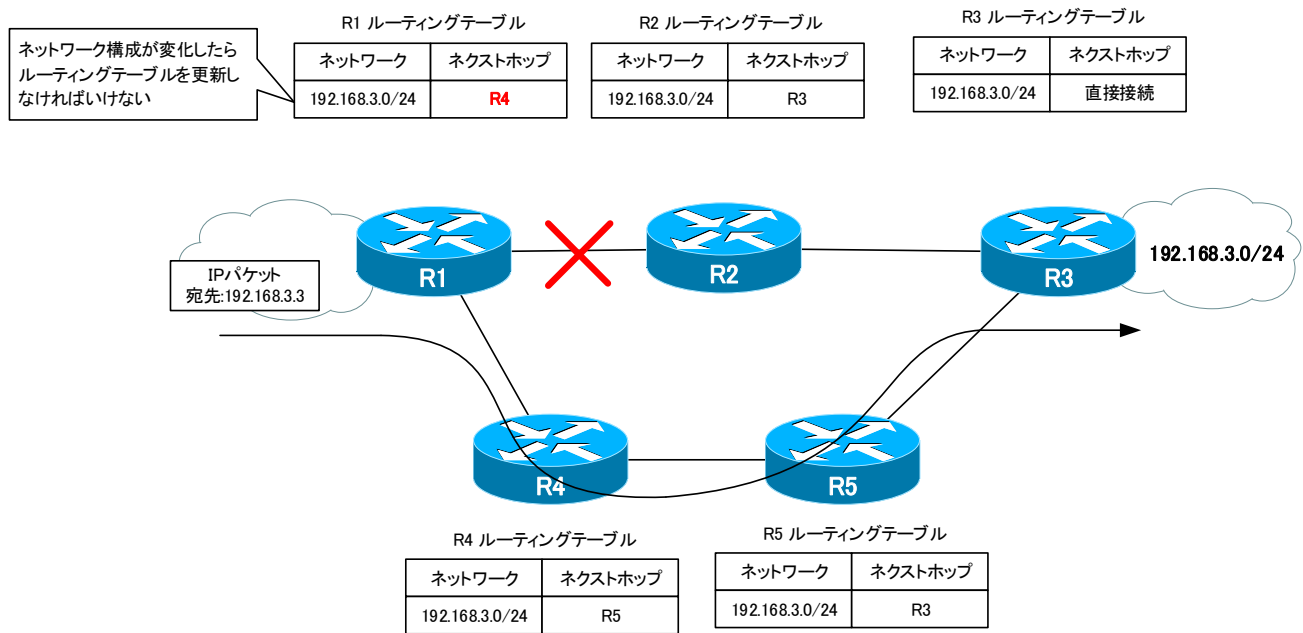


図 19 ルーティングテーブルの更新

ルーティングプロトコルを利用すると、ネットワークの障害発生時のルーティングテーブルの更新を自動的に行うことができます。

## ルーティングテーブルの作り方

ルータに直接接続されていないネットワークのルート情報をスタティックルートまたはルーティングプロトコルによってルーティングテーブルに登録します。

### ルーティングテーブルのルート情報

ルーティングテーブルにルート情報を登録する方法として、次の 3 つの方法があります。

- ・ 直接接続
- ・ スタティックルート
- ・ ルーティングプロトコル

直接接続のルート情報は、最も基本的なルート情報です。ルータにはネットワークを接続する役割があります。直接接続のルート情報は、その名前の通りルータが直接接続しているネットワークのルート情報です。

直接接続のルート情報をルーティングテーブルに登録するために、特別な設定は不要です。ルータのインタフェースに IP アドレスを設定して、そのインタフェースを有効にするだけです。自動的に設定した IP アドレスに対応するネットワークアドレスのルート情報が、直接接続のルート情報としてルーティングテーブルに登録されます。

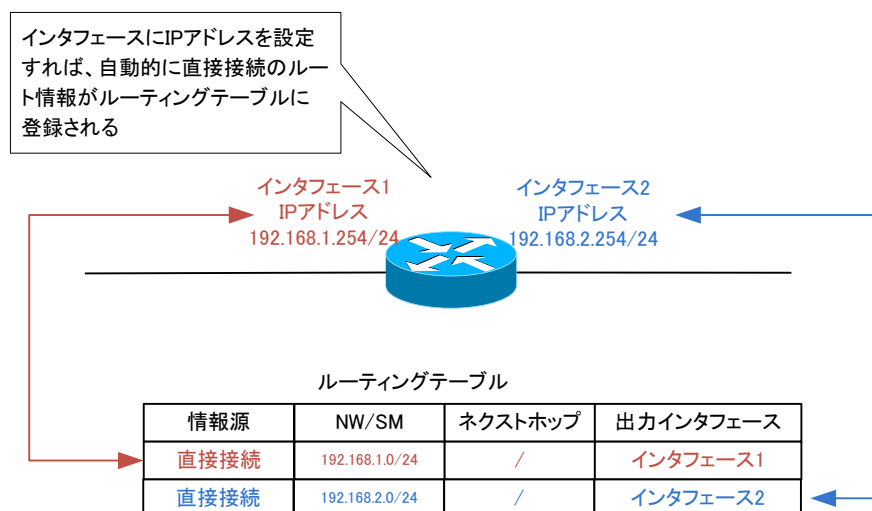


図 20 直接接続のルート情報

Cisco ルータの IOS のバージョンによっては、IP アドレスを設定してインタフェースがアクティブになると直接接続のルート情報に加えて、ローカルのルート情報もルーティングテーブルに登録されます。ローカルのルート情報とは、ルータのインタフェースに設定されている IP アドレス自体の情報で、サブネットマスク /32 で登録されます。

Center#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, 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  
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2  
ia - IS-IS inter area, \* - candidate default, U - per-user static route  
o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.1.0/24 is directly connected, GigabitEthernet0

L 192.168.1.254/32 is directly connected, GigabitEthernet0

※ サブネットマスク/32 の特定の IP アドレスを表すルート情報は「ホストルート」とも呼びます。

ルーティングテーブルに登録されているネットワークのみ IP パケットをルーティングできます。つまり、ルータは特別な設定をしなくても、直接接続のネットワーク間のルーティングが可能です。逆に言えば、ルータは直接接続のネットワークしかわかりません。ルータに直接接続されていないリモートネットワークのルート情報をルーティングテーブルに登録しなければいけません。つまり、ルーティングの設定とは、基本的にリモートネットワークのルート情報をどのようにしてルーティングテーブルに登録するかということです。リモートネットワークのルート情報を登録するための方法が

- ・ スタティックルート
- ・ ルーティングプロトコル

です。

ルーティングが必要なリモートネットワークごとにスタティックルートまたはルーティングプロトコルによって、ルート情報をルーティングテーブルに登録します。それにより、リモートネットワークへの IP パケットのルーティングが可能になります。スタティックルートでリモートネットワークのルート情報を登録することを指して「スタティックルーティング」と呼びます。また、ルーティングプロトコルでリモートネットワークのルート情報を登録することを「ダイナミックルーティング」と呼びます。

スタティックルートはルータにコマンドを入力するなどして、ルート情報を手動でルーティングテーブルに登録します。一方、ルーティングプロトコルはルータ同士でさまざまな情報を交換して自動的にルーティングテーブルにルート情報を登録します。ルーティングプロトコルによって、ルータがルート情報を送信すること

を指して、「アドバタイズ」という表現をよく利用します。

ルーティングプロトコルには、次のような種類があります。

- ・ RIP(Routing Information Protocol)
- ・ OSPF(Open Shortest Path First)
- ・ EIGRP(Enhanced Interior Gateway Routing Protocol)
- ・ BGP(Border Gateway Protocol)

RIP は比較的規模が小さい企業のネットワークでよく利用されるシンプルなルーティングプロトコルです。OSPF は中～大規模な企業のネットワークで利用されるルーティングプロトコルです。EIGRP は Cisco 独自のルーティングプロトコルで大規模な企業ネットワークでよく利用されています。そして、インターネット上のルータは、ルーティングプロトコルとして主に BGP を利用しています。インターネット上には膨大な数のネットワークが存在しています。膨大な数のネットワークのルート情報を効率よく扱うために BGP が必要です。

## ルーティングテーブル作成の例

次の簡単なネットワーク構成を例にして、スタティックルートとルーティングプロトコルによるリモートネットワークのルート情報の登録を考えます。

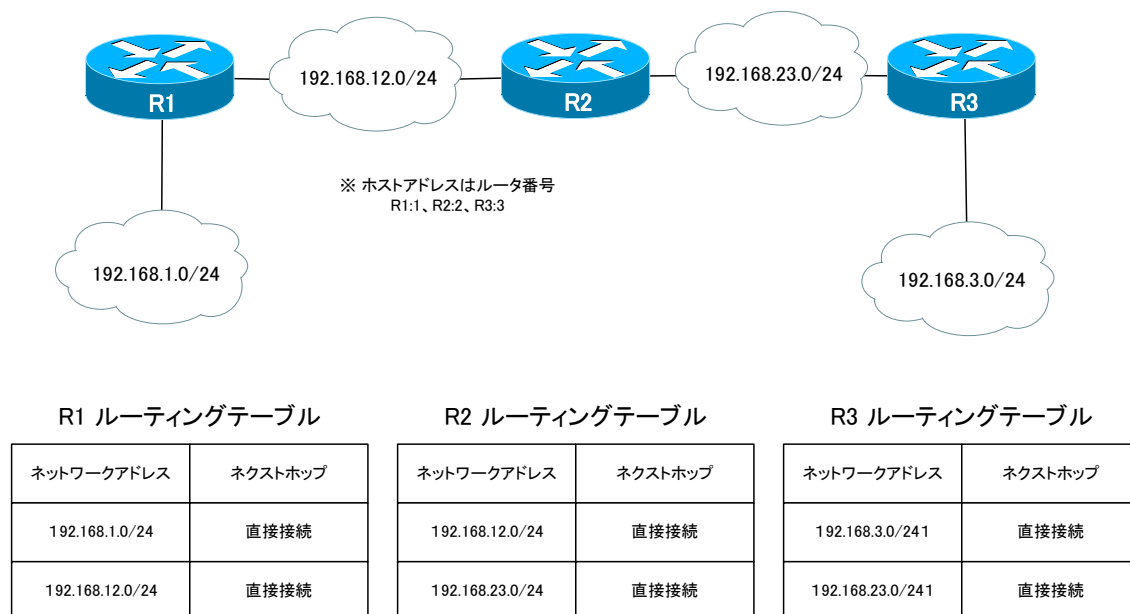


図 21 ルーティングテーブル作成例のネットワーク構成例

R1、R2、R3 の 3 台のルータで 4 つのネットワークを相互接続しています。各ルータのインタフェースに IP アドレスを設定することで、ネットワークを接続していることになり、ルーティングテーブルに直接接続のルート情報が登録されています。

### スタティックルートの設定

スタティックルートを利用する場合、それぞれのルータにとってのリモートネットワークのルート情報をコマンド入力や **GUI** ベースの設定で、管理者が手動でルーティングテーブルに登録します。そこで、まずは、各ルータのリモートネットワークをきちんと把握しておかなければいけません。つまり、スタティックルートの設定を行うためには、各ルータのルーティングテーブルの完成形がわかっていなければいけません。

各ルータのリモートネットワークと指定すべきネクストホップアドレスをまとめると、次の表のようになります。

表 4 リモートネットワーク

ルータ	リモートネットワーク	ネクストホップ
R1	192.168.23.0/24	192.168.12.2
	192.168.3.0/24	192.168.12.2
R2	192.168.1.0/24	192.168.12.1
	192.168.3.0/24	192.168.23.3
R3	192.168.1.0/24	192.168.23.2
	192.168.12.0/24	192.168.23.2

リモートネットワークを把握したら、各ルータで管理者がコマンドラインからコマンドを入力したり、**GUI** の設定画面でスタティックルートのパラメータの指定を行って、リモートネットワークの情報を手作業で登録します。

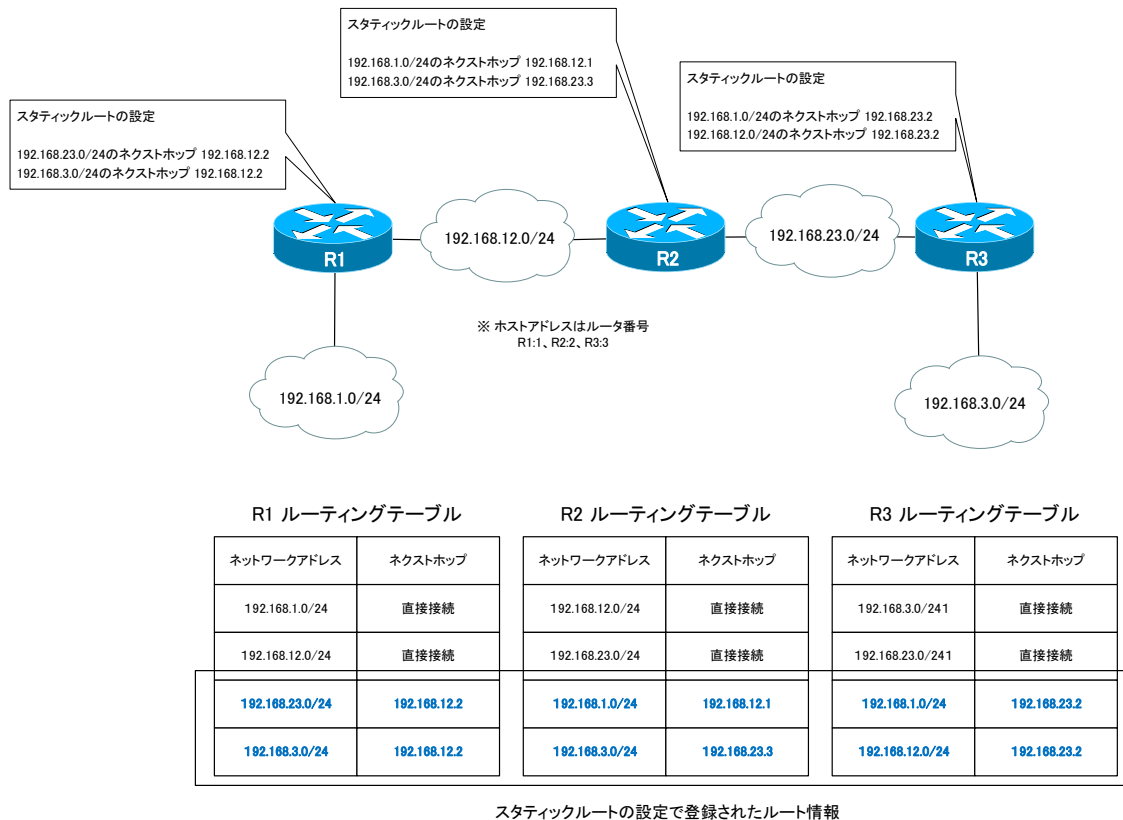


図 22 スタティックルートの設定例

この例のような小規模なネットワークであればそれほど設定の負荷は大きくありませんが、ルータの台数が増え、ネットワークの数も増えてくるとスタティックルートの設定は大変な作業です。

### ルーティングプロトコルの設定例

ルーティングプロトコルの設定例を考えるにあたって、一番シンプルな **RIP** を利用するものとします。設定は、各ルータのすべてのインタフェースで **RIP** を有効化するだけです。特にリモートネットワークを洗い出して、ネクストホップを考えるような作業はいりません。設定するだけなら、各ルータのルーティングテーブルが最終的にどのようなになるかを知らなくても大丈夫です。

ただし、ルーティングプロトコルを使うときにも、リモートネットワークとネクストホップを認識してルーティングテーブルの最終形をわかっておくことは重要です。そうでないと、出来上がったルーティングテーブルが正しいかどうか判断できません。ルーティングプロトコルを設定するときにはリモートネットワークとそのネクストホップの情報は特にいらないという意味です。

※ **RIP** 以外のルーティングプロトコルも基本的な設定は同じです。ルーティングプロトコルをすべてのインタフェースで有効化するという設定を行うだけです。ただし、**BGP** は例外です。**BGP** の設定はインタフェース単位ではありません。

**RIP** を有効化すると、各ルータは **RIP** のルート情報を送受信します。**R1** であれば、**R2** へ **192.168.1.0/24**

の **RIP** ルート情報を送信します。それを受信した **R2** はルーティングテーブルに **192.168.1.0/24** を登録します。また、**R2** から **R3** へ **192.168.1.0/24** と **192.168.12.0/24** の **RIP** ルート情報を送信します。**R3** は受信した **RIP** ルート情報をルーティングテーブルに追加します。

**R3** からは **R2** へ **192.168.3.0/24** の **RIP** ルート情報を送信しています。**R2** はルーティングテーブルに **192.168.3.0/24** を追加します。また、**R2** から **R1** へ **192.168.3.0/24** と **192.168.23.0/24** の **RIP** ルート情報を送信しています。すると、**R1** のルーティングテーブルに **192.168.3.0/24** と **192.168.23.0/24** が登録されます。

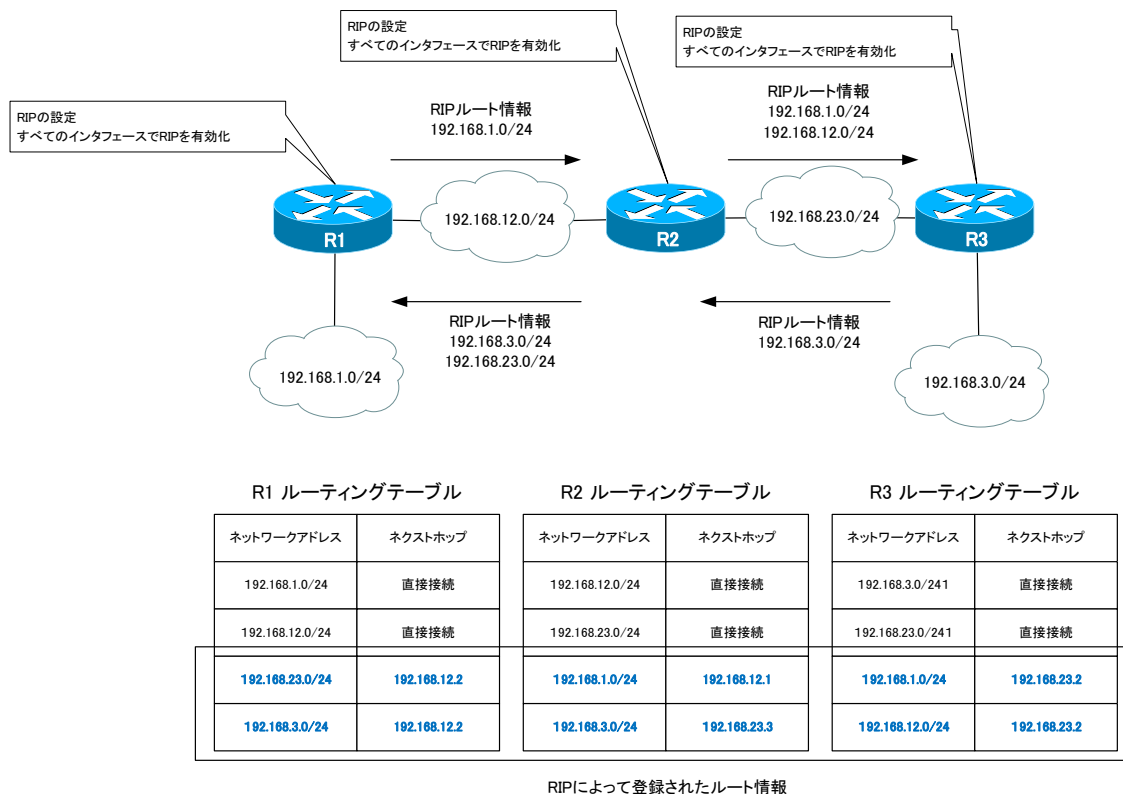


図 23 RIP の設定例

以上のように、各ルータで「すべてのインタフェースにおいて **RIP** を有効にする」という設定をすれば、あとはルータ同士がルート情報を交換して自動的にルーティングテーブルを作ってくれるようになります。



## ルート情報の送信の意味

ルーティングプロトコルでネットワークのルート情報を送信することの意味についてもう少し補足します。

「ルート情報を送信することで、そのネットワークへのアクセス許可を与えている」と考えることができます。

ルーティングプロトコルによって、ルート情報を送信することで以下のような動作になります。

1. ルーティングプロトコルで他のルータにネットワークのルート情報を送信する
2. 他のルータのルーティングテーブルにルート情報が登録される
3. そのネットワーク宛てのパケットをルーティングできる

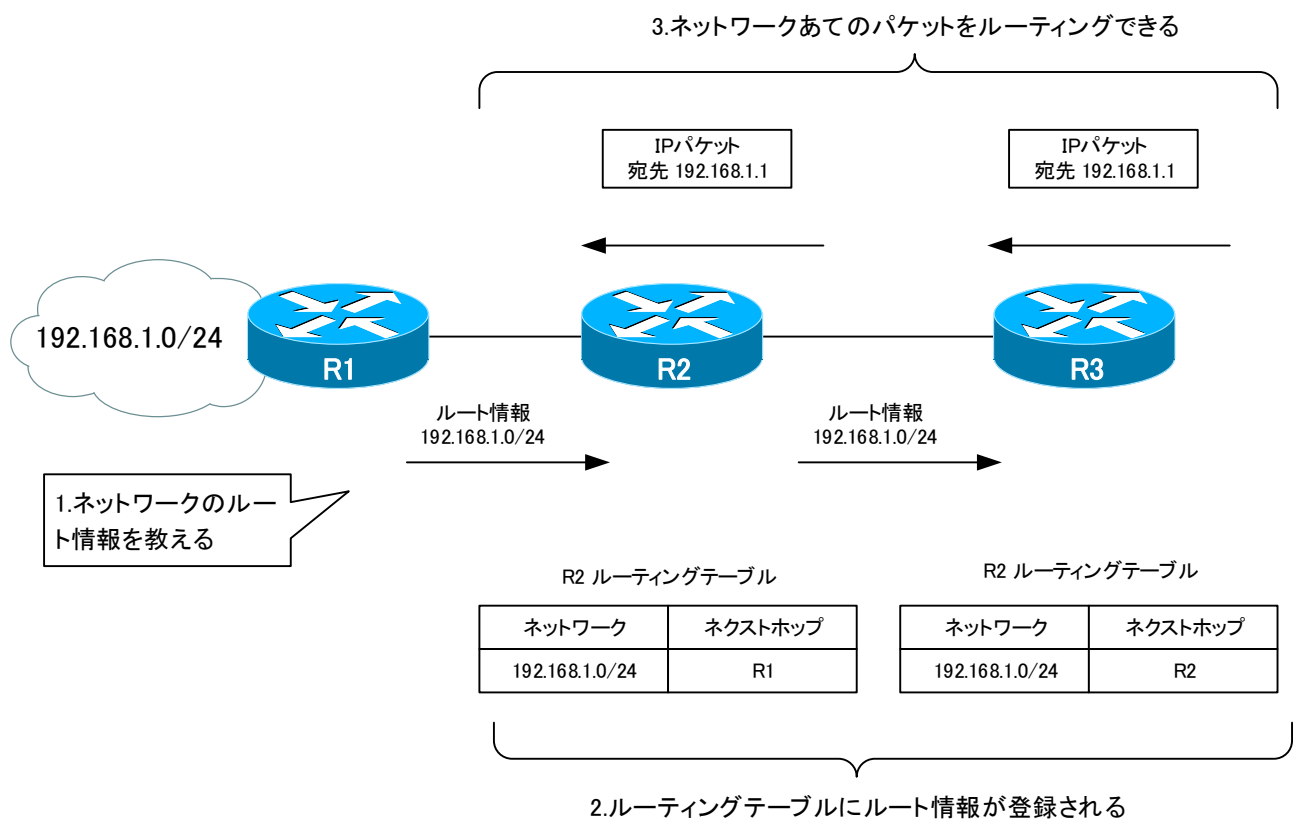


図 24 ルート情報の送信の動作

以上のように、ルーティングプロトコルで、あるネットワークのルート情報を送信すると、そのネットワークへの通信が可能です。すなわち、ネットワークへのアクセス許可を与えています。もし、特定のネットワークへのアクセスを許可したくないのであれば、そのネットワークのルート情報を送信しなければよいです。特定のネットワークのルート情報を送信しないようにすることがルートフィルタリングです。

※ CCNA 試験では、ルートフィルタリングの詳細は必要ありませんが、とてもよく利用しています。

## スタティックルートとルーティングプロトコルの選択

ここまで見てきたようにリモートネットワークのルート情報をルーティングテーブルに登録するためには、スタティックルートとルーティングプロトコルの 2 通りの方法があります。どちらかが一方よりも優れているというわけではありません。スタティックルートにはスタティックルートのメリット・デメリットがあり、ルーティングプロトコルにはルーティングプロトコルのメリット・デメリットがあります。

ネットワーク構成に応じて、スタティックルートとルーティングプロトコルを組み合わせ、必要なリモートネットワークのルート情報をルーティングテーブルに登録することがポイントです。また、1 台のルータで複数のルーティングプロトコルを利用することも可能です。

たとえば、次の図において R1 で 192.168.3.0/24 のルート情報をスタティックルートでルーティングテーブルに登録し、192.168.4.0/24 のルート情報を RIP というルーティングプロトコルでルーティングテーブルに登録することができます。

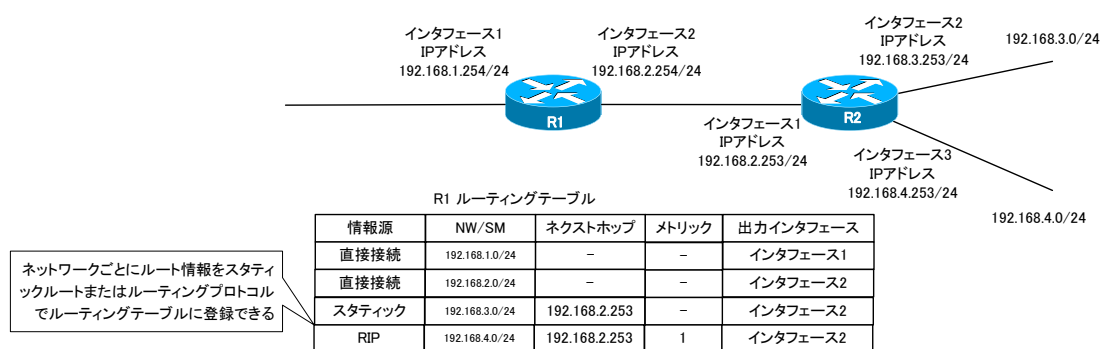


図 25 スタティックルートとルーティングプロトコルの組み合わせ

※ この図は、あくまでもスタティックルートとルーティングプロトコルを同時に利用できるという例を示しているだけです。この図のような設定をする何らかのメリットがあるわけではありません。

どのように組み合わせるかを知らするためには、スタティックルートとルーティングプロトコルのメリット・デメリットを把握しなければいけません。以下、スタティックルートとルーティングプロトコルのメリットとデメリットについてまとめます。

### スタティックルートのメリット・デメリット

スタティックルートのメリットとして、次の点が挙げられます。

- ・ ルーティングプロトコルの知識が不要  
スタティックルートの設定自体はシンプルで、特別な知識は必要ありません。
- ・ ルーティングテーブルが意図せず書き換わってしまう心配がほとんどない  
スタティックルートは管理者が明示的に設定するので、意図しないでルーティングテーブルが書き換わっ

てしまうことはほとんどありません。

- ・ ルートを厳密に決められる

目的のネットワークまでの複数のルートが存在している場合、スタティックルートを利用すれば管理者が意図したルートで IP パケットをルーティングすることができます。ルーティングプロトコルでも可能ですが、ルーティングプロトコルごとに追加の設定が必要です。

- ・ ルータやネットワークに負荷をかけない

スタティックルートを設定してもルータは、追加の処理を行いません。またルート情報をネットワークに送信しません。そのため、ネットワークやルータに余分な負荷をかけずに済みます。

一方、スタティックルートのデメリットは次の通りです。

- ・ 管理者の負荷が大きい

スタティックルートだけでルーティングテーブルにルート情報を登録するには、すべてのルータで、各ルータにとってのリモートネットワークのルート情報を設定しなければいけません。多くのルータで構成される大規模なネットワークでは、設定が煩雑になり管理者の負荷が非常に大きくなります。

- ・ ネットワーク構成の変更を自動的に反映できない

新しいネットワークが追加されたり、障害発生などでネットワークの構成が変更しても、スタティックルートではルーティングテーブルを自動的に変更することができません。ネットワークを冗長化していたとしても、スタティックルートだと、障害に応じて自動的にルーティングテーブルを書き換えて経路を切り替えることが困難です。

## ルーティングプロトコルのメリット・デメリット

ルーティングプロトコルのメリットは次の通りです。

- ・ ネットワーク構成の変更を自動的にルーティングテーブルに反映させられる

新しいネットワークの追加や障害発生などのネットワーク構成を反映して、ルーティングテーブルのルート情報を登録することができます。

- ・ 管理者の負荷が少ない

たくさんのリモートネットワークがあったとしても、各ルータではルータ全体とインタフェースでルーティングプロトコルを有効化するだけです。大規模なネットワークでもスタティックルートに比べると、設定の手間が少ないので、管理者の負荷も少なくなります。

一方、ルーティングプロトコルのデメリットは次の通りです。

- ・ 利用するルーティングプロトコルの知識が必要

効果的にルーティングプロトコルを利用するためには、利用するルーティングプロトコルの仕組みを理解しておかなければいけません。

- ・ 意図せずルーティングテーブルが書き換わってしまうことがある  
ネットワーク上に流れるルーティングプロトコルのルート情報が改ざんされてしまうと、不正なルーティングテーブルになり正しくルーティングできない可能性があります。また、ルート情報が盗聴されると、不正なユーザにネットワーク構成の情報を与えてしまうことになります。スタティックルートに比べると、セキュリティ上問題が発生する可能性が高くなります。
- ・ ルータやネットワークに負荷がかかる  
スタティックルートに比べると、ルーティングプロトコルの処理を行うためにルータに負荷がかかります。また、ネットワークにルート情報を送信するので、ネットワークの帯域幅を消費することになります。

このようなメリット・デメリットを踏まえて、スタティックルートとルーティングプロトコルを組み合わせ、ルーティングテーブルにリモートネットワークのルート情報を登録します。

スタティックルートを利用するのは、主に以下のような場合です。

- ・ 小規模なネットワークでルータやネットワークの数があまり多くない
- ・ 冗長化されていない
- ・ ネットワーク管理範囲の違いで共通したルーティングプロトコルを利用できない

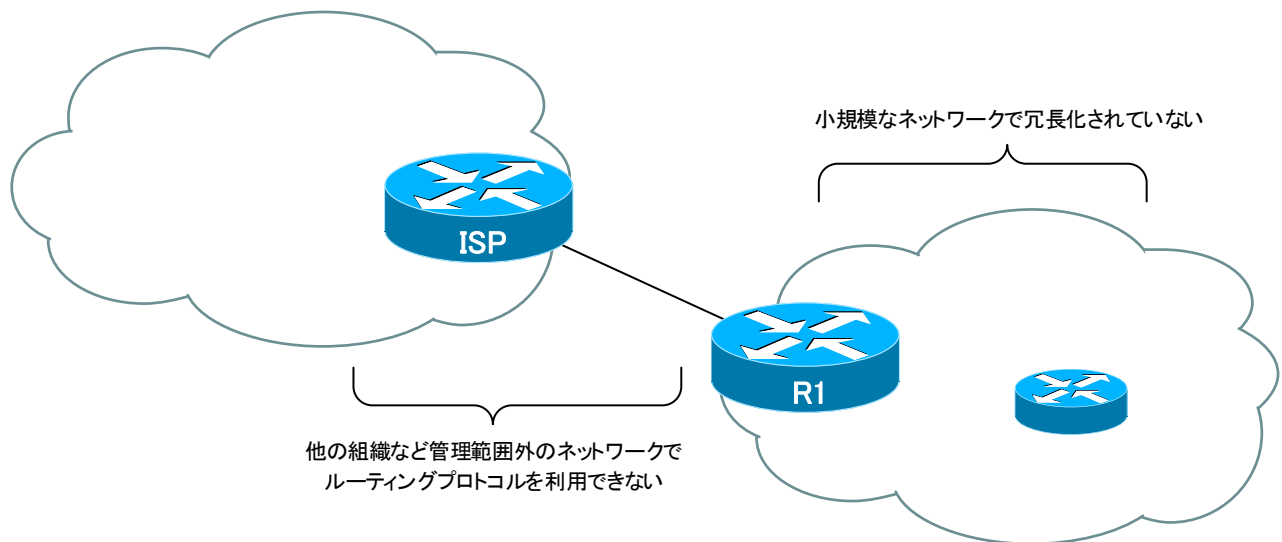


図 26 スタティックルートを利用する場合

そして、ルーティングプロトコルを利用するのは、主に以下のような場合です。

- ・ ルータやネットワークの数が多
- ・ 冗長化されている

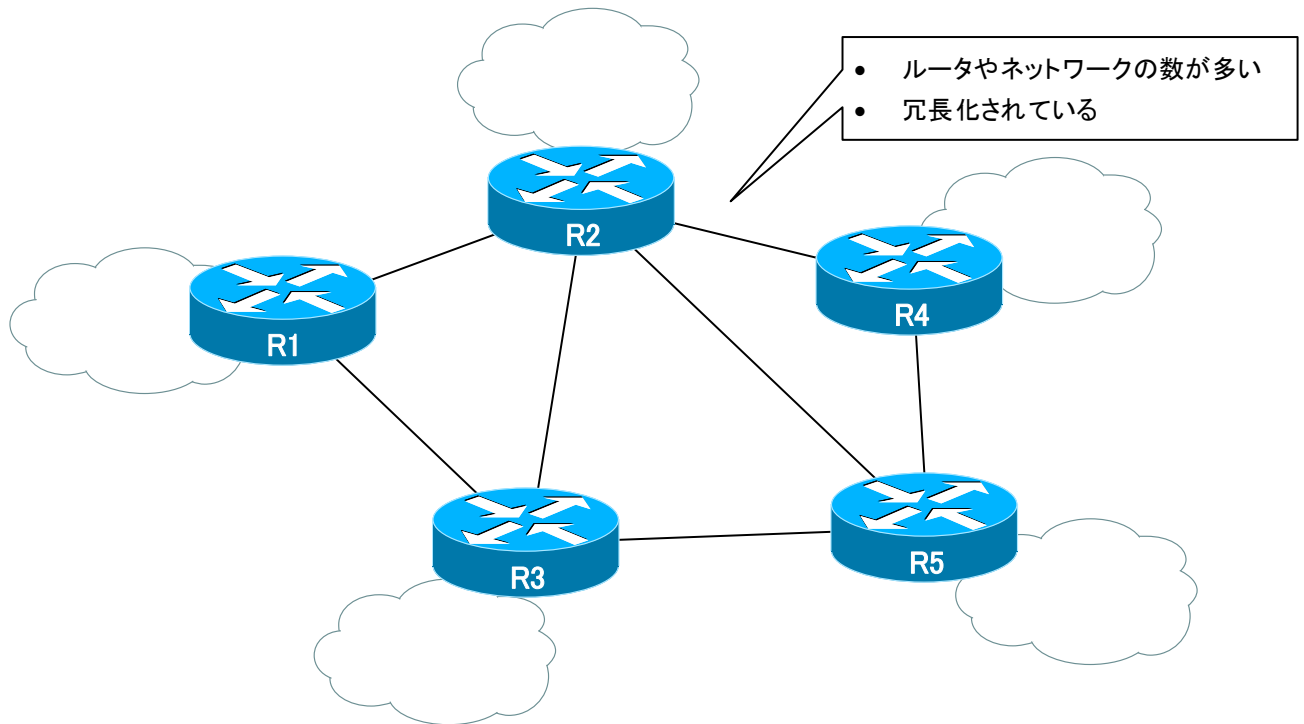


図 27 ルーティングプロトコルを利用する場合

## ルートの情報源の優先度(アドミニストレイティブディスタンス)

あるネットワークのルートをスタティックルートで設定しつつ、ルーティングプロトコルで学習することもできます。ルーティングプロトコルも 1 つだけでなく複数動作させて、あるネットワークのルート情報を複数のルーティングプロトコルで学習することもできます。すなわち、あるネットワークのルート情報を複数の情報源から学習することがあります。ルーティングテーブルには、原則として、最適ルートのみ登録します。そのため、複数の情報源からあるネットワークのルート情報を学習したときの最適ルートの決定について考えなければいけません。

以下の図のように、R1 で 192.168.10.0/24 のルート情報をスタティックルートで設定するだけではなく、RIP、OSPF でも学習した場合を考えます。

あるネットワークへの最適なルートを決定する基準としてメトリックが挙げられます。メトリックは宛先ネットワークまでの距離です。ただし、スタティックルートで設定したルート情報にはメトリックは意味がありません。Cisco ルータではスタティックルートのメトリックは「0」です。また、ルーティングプロトコルによってメトリックの考え方がまったく異なり、取りうる値の範囲も全く違ってしまっているので、単純にメトリックの数値を比較できません。メトリックの値を単純に比較することは、現実世界の距離で、「メートル」と「フィート」を単純に比較しようとするのと同じようなことです。ルーティングプロトコルごとのメトリックは以下の表の通りです。

表 5 ルーティングプロトコルのメトリック

ルーティングプロトコル	メトリック
RIP	ホップ数
OSPF	パスコスト
EIGRP	複合メトリック(帯域幅、遅延、負荷、信頼性、MTU)

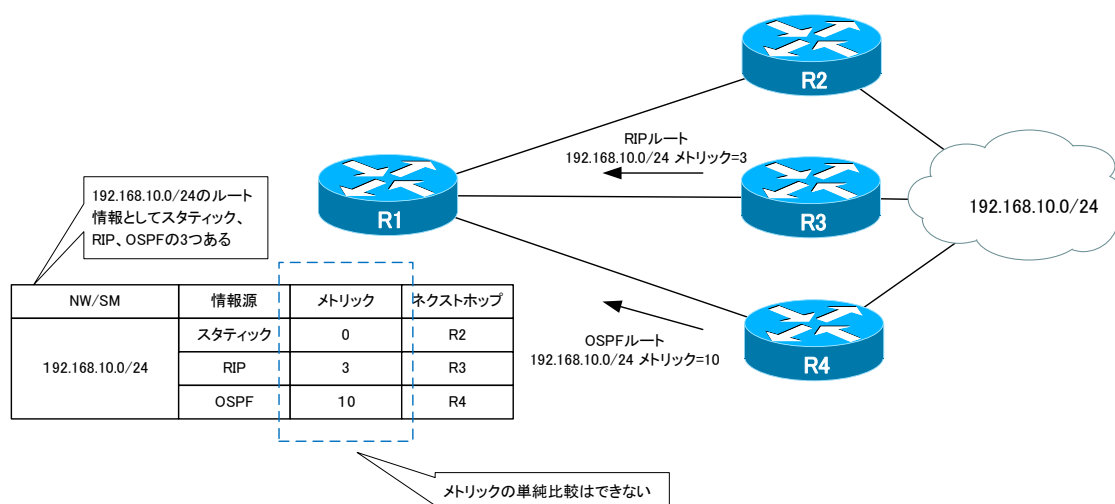


図 28 あるネットワークへのルートを複数の情報源で学習

※ 図ではわかりやすさを優先して、実際の動作とは異なる場合があります。OSPF ルート情報は、必

ずしも図のようなネットワークアドレス/サブネットマスク+メトリックになるわけではありません。また、R1 での OSPF ルートのメトリックは、受信したルート情報のメトリックから増加します。

現実世界の「メートル」と「フィート」のように単位の違う距離を比較するときには、単位を揃えなければいけません。メトリックを比較するときに単位を合わせるためのパラメータがアドミニストレイティブディスタンスです。アドミニストレイティブディスタンスとメトリックを組み合わせ、宛先ネットワークまでの距離とすることで、スタティックルート、RIP ルート、OSPF ルートといった情報源の異なるルートの距離を比較できるようにします。

宛先ネットワークへの距離 = アドミニストレイティブディスタンス/メトリック

距離は短いほうがよいので、アドミニストレイティブディスタンスもメトリックも値が小さいほうが優先されます。アドミニストレイティブディスタンスを前につけるため、アドミニストレイティブディスタンスの値が小さいほど距離が短いとみなされることになります。アドミニストレイティブディスタンスのデフォルトは、次の表のように決められています。

表 6 アドミニストレイティブディスタンスのデフォルト値

情報源	アドミニストレイティブディスタンス値
直接接続	0
スタティックルート	1
BGP	20
EIGRP	90
OSPF	110
RIP	120
外部 EIGRP	170
IBGP	200

前述の構成例で 192.168.10.0/24 のルート情報の距離を考えると、次のようになります。

192.168.10.0/24 への距離

スタティックルート:[1/0]

RIP ルート:[120/3]

OSPF ルート:[110/10]

スタティックルートが最も距離が短くなるので、192.168.10.0/24 の最適ルートとしてルーティングテーブルにはスタティックルートのルート情報が登録されます。

基礎からの CCNA(200-301)攻略テキスト  
第 10 章 IP ルーティング

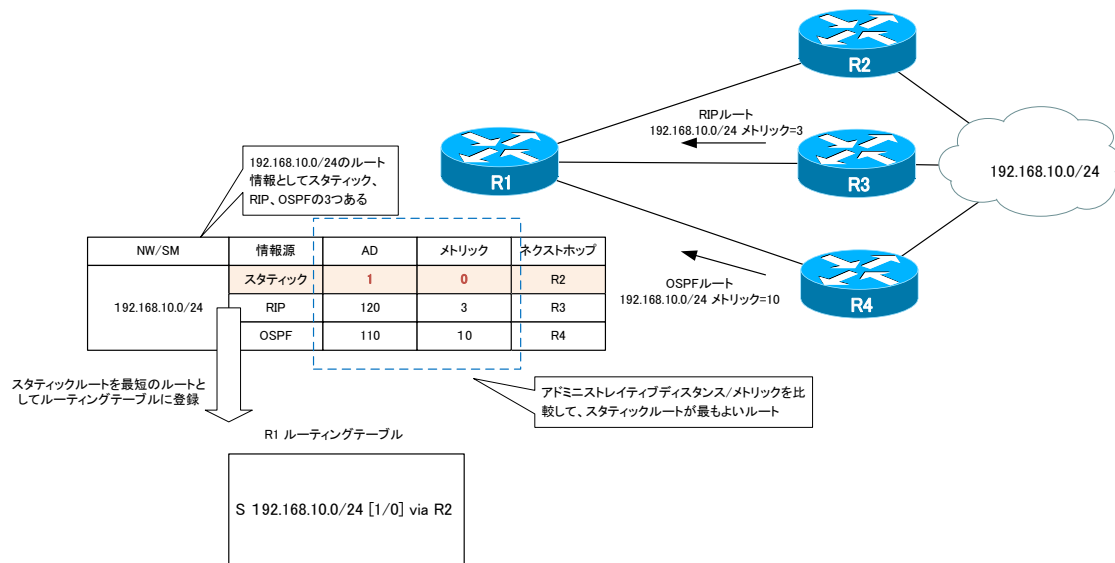


図 29 アドミニストレイティブディスタンス/メトリックによる最適ルートの選択

アドミニストレイティブディスタンスの値はデフォルトから変更することもできます。アドミニストレイティブディスタンスを変更すれば、あるネットワークのルート情報を複数の情報源で学習している場合、ルーティングテーブルにどの情報源のルート情報として登録するかを選択できます。

※ アドミニストレイティブディスタンスは、「ルートの情報源の信頼性」と解説されることが多くなっています。



## 等コストロードバランス

あるネットワークに対するルート情報は、原則として、最適ルートのみがルーティングテーブルに登録されます。最適なルート情報が複数ある場合、ルーティングの負荷分散を行うことができます。最適ルートが複数ある場合とは、メトリックが最小となるルート情報が複数のときです。このようなルーティングの負荷分散を等コストロードバランスと呼びます。

※ メトリックのことをコストとも表現するので、等「コスト」ロードバランスです。

※ EIGRP では、メトリックが同じでなくても可能です。メトリックが同じでない場合の負荷分散は不等コストロードバランスと呼びます。

以下は、等コストロードバランスの例です。

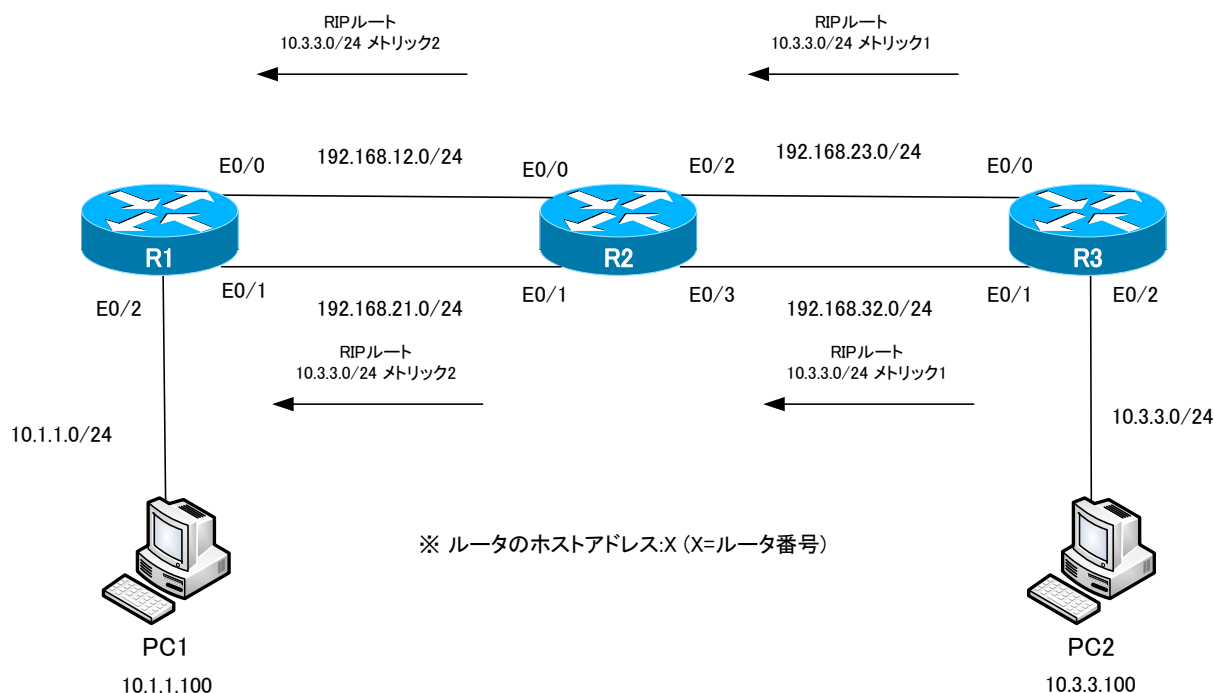


図 30 等コストロードバランスの例

R1 で 10.3.3.0/24 のネットワークについてのルート情報に注目します。この例では、ルーティングプロトコルに RIP を利用しています。R1-R2 間、R2-R3 間がそれぞれ 2 回線ずつ接続されています。

R3 から 10.3.3.0/24 のルート情報をそれぞれの回線から R2 へ送信します。そのメトリックは 1 です。そして、R2 からさらに R1 へと 10.3.3.0/24 のルート情報をメトリック 2 で送信します。

R1 では、10.3.3.0/24 のルート情報として同じメトリックの 2 つのルートを受信しているので、2 つともルーティングテーブルに登録します。R1 から 10.3.3.0/24 へパケットをルーティングするときには、ネクストホップ 192.168.12.2 と 192.168.21.2 に分散します。

RI のルーティングテーブルは、次のような表示となります。

RI

```
-----  
R1#show ip route rip  
    10.0.0.0/24 is subnetted, 2 subnets  
R    10.3.3.0 [120/2] via 192.168.21.2, 00:00:17, Ethernet0/1  
    [120/2] via 192.168.12.2, 00:00:24, Ethernet0/0  
R    192.168.23.0/24 [120/1] via 192.168.21.2, 00:00:17, Ethernet0/1  
    [120/1] via 192.168.12.2, 00:00:24, Ethernet0/0  
R    192.168.32.0/24 [120/1] via 192.168.21.2, 00:00:17, Ethernet0/1  
    [120/1] via 192.168.12.2, 00:00:24, Ethernet0/0  
-----
```

- ※ 等コストロードバランスで登録できる最大のルート数は、デフォルトで **4** です。その最大値をさらに設定で変更することができます。設定可能な等コストロードバランスの最大値は、**IOS** バージョンなどによって異なります。
- ※ ルーティングプロトコルのルート情報だけでなく、スタティックルートでも等コストロードバランスは可能です。

## ルート集約

ルート集約とは、複数のネットワークアドレスのルート情報を 1 つにまとめることです。まず、ルート集約がなぜ必要かについて考えましょう。ルーティングするためには、目的のネットワークのルート情報が必要です。ですが、すべてのネットワークのルート情報をルーティングテーブルに登録するのは大変です。たとえば、大規模な企業ネットワークであれば、数百～1000 以上の数のネットワークが存在することがあります。また、インターネット上には数え切れないほどの膨大な数のネットワークが存在します。

スタティックルートでこれほど膨大な数のルート情報を設定することは非常に難しいです。ルーティングプロトコルによってはそれほど多くの数のルート情報を扱うことができないので、膨大な数のルート情報をルーティングテーブルに登録することは現実的ではない場合があります。登録できたとしても、ルータに多大な負荷がかかり、処理性能が低いルータでは正常に動作できないことも考えられます。そして、膨大な数のルート情報をルーティングプロトコルで交換すると、ネットワークの帯域幅を消費してしまうことにもなります。

また、リモートネットワークへのルーティングの動作を考えると、膨大な数のルート情報をルーティングテーブルに一つずつ登録してもあまり意味がありません。たとえば、次の図のネットワーク構成を考えます。

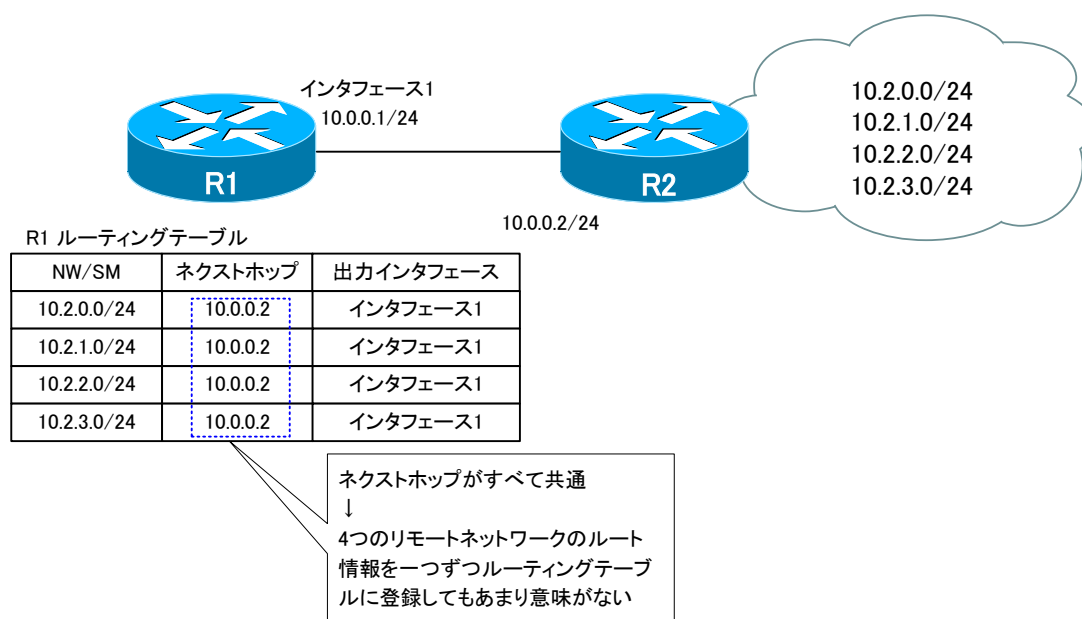


図 31 ネットワーク構成例

R1 にはリモートネットワークの 10.2.0.0/24～10.2.3.0/24 の 4 つのルート情報をルーティングテーブルに登録しています。リモートネットワークへパケットをルーティングするときには、ネクストホップへ転送します。この図では、4 つのリモートネットワークへルーティングするときのネクストホップはすべて 10.0.0.2 で共通です。10.2.0.0/24 へルーティングするときも、10.2.1.0/24 へルーティングするときも、10.2.2.0/24 へルーティングするときも、10.2.3.0/24 へルーティングするときも、結局はネクストホップの 10.0.0.2 へパケットを転送します。すると、4 つのリモートネットワークのルート情報を一つずつルーティングテーブルに登録することにはあまり意味がありません。

そこで、ルート集約を考えます。ネクストホップが共通しているリモートネットワークのルート情報を 1 つ

にまとめます。先ほどの構成例で考えると、4 つのリモートネットワークのルート情報を集約して、**10.2.0.0/16** でネクストホップ **10.0.0.2** というルート情報にまとめます。**R1** は、この **10.2.0.0/16** のルート情報で送信先 IP が **10.2.0.0/24** ~ **10.2.3.0/24** あてのパケットをネクストホップ **10.0.0.2** へ転送することができます。

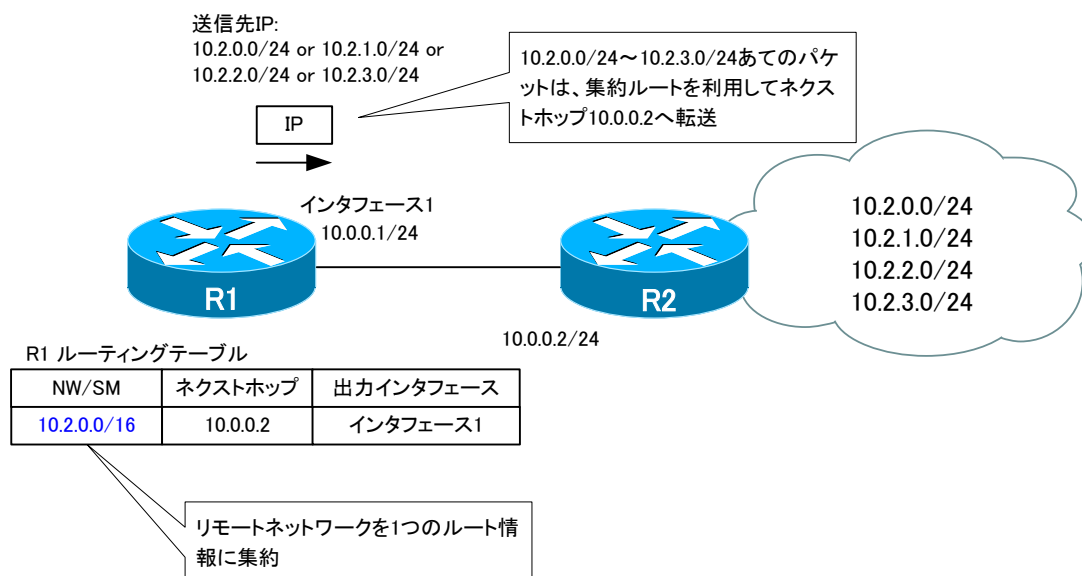


図 32 ルート集約の例

※ **10.2.0.0/16** というルート情報は、**10.2.0.0/24** ~ **10.2.255.0/24** の **256** 個のルート情報を 1 つにまとめていることになります。

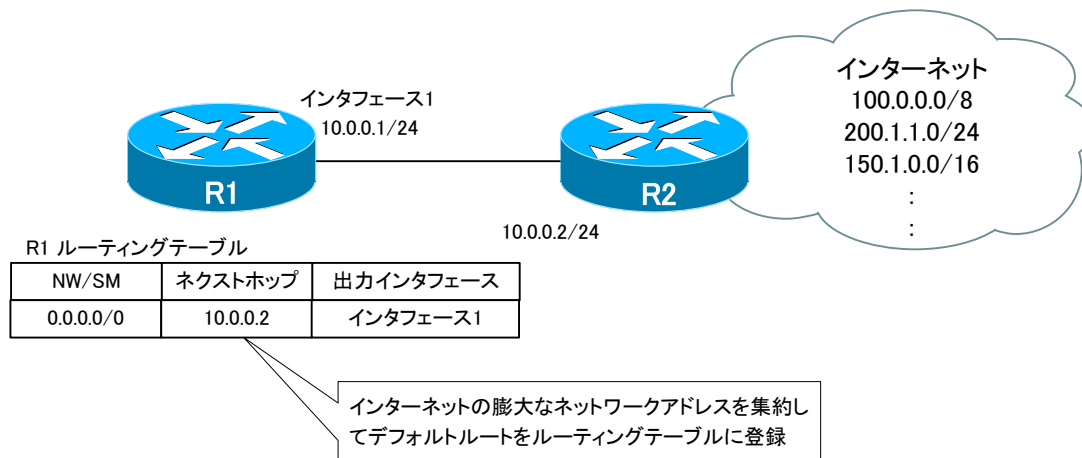
## デフォルトルート

ルート集約をもっとも極端にしたのがデフォルトルートです。デフォルトルートは「**0.0.0.0/0**」で表すルート情報で、すべてのネットワークを集約しています。つまり、デフォルトルートをルーティングテーブルに登録しておけば、すべてのネットワークのルート情報を登録していることになります。

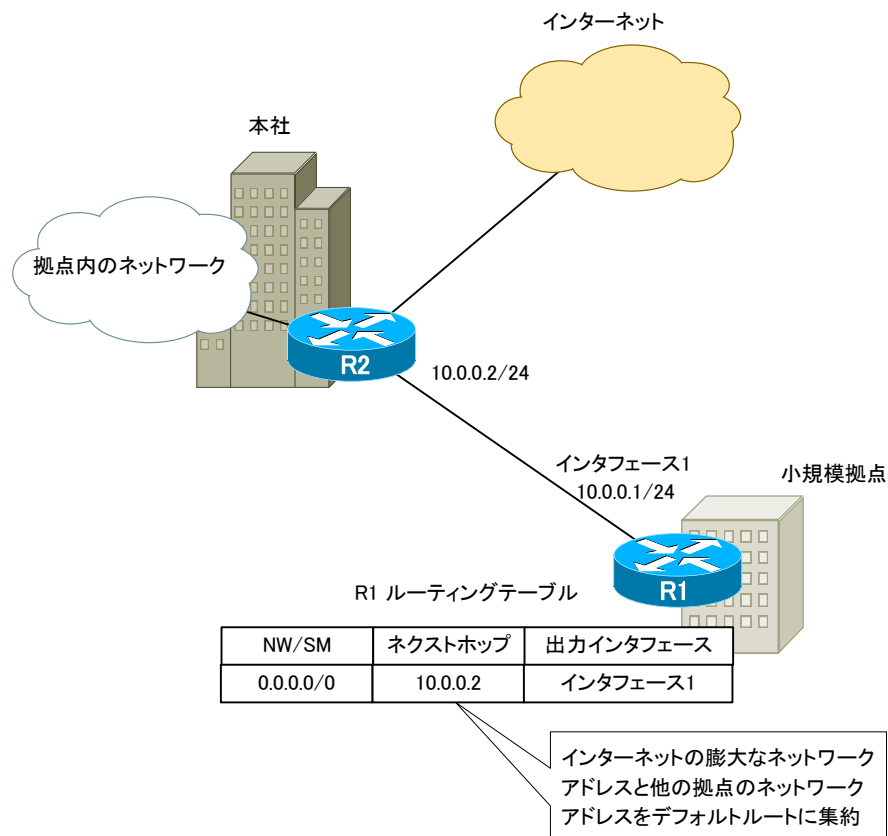
※ デフォルトルートは「未知のネットワークあてのパケットを転送するためのルート情報」という解説がよくされています。しかし、筆者個人としては、このような解説は不適切だと考えています。デフォルトルートはすべてのネットワークを表しています。デフォルトルートをルーティングテーブルに登録しているルータには、未知のネットワークはありません。ただ、非常に大雑把な形で登録しています。

デフォルトルートの利用例として、インターネットあてのパケットをルーティングするために、デフォルトルートをルーティングテーブルに登録することが多いです。インターネットには膨大な数のネットワークが存在しますが、パケットをルーティングするときにネクストホップが共通になっていることがほとんどです。そこで、インターネットの膨大な数のネットワークをデフォルトルートにすべて集約してルーティングテーブル

に登録します。



なお、デフォルトルートはインターネットあてのルーティングだけに使うわけではありません。企業ネットワークの小規模な拠点のルータには、インターネットと他の拠点のネットワークをすべてデフォルトルートに集約して、ルーティングテーブルに登録することもあります。たとえば、次の図のネットワーク構成では **R1** にとって、本社の拠点内のネットワークあてもインターネットあても、パケットをルーティングするためのネクストホップはすべて共通です。インターネットのネットワークだけでなく、本社内のネットワークもデフォルトルートに集約することができます。



「デフォルトルートはスタティックルートで設定する」と思いこんでいる方をときどきみかけますが、そんなことはありません。デフォルトルートの設定例で、スタティックルートとして設定していることが多いからでしょう。デフォルトルートも集約ルートのひとつです。ですから、スタティックルートの設定で、デフォルトルートをルーティングテーブルに登録することもできます。ルーティングプロトコルによって、ルータ間でデフォルトルートのルート情報を送受信してルーティングテーブルに登録することもできます。

## 最長一致検索(ロングストマッチ)

複数のネットワークアドレスを集約して集約ルートをルーティングテーブルに登録すると、実際のネットワークアドレス/サブネットマスクと集約ルートのネットワークアドレス/サブネットマスクが異なります。最長一致検索(ロングストマッチ)によって、パケットをルーティングするためのルート情報を検索するので、実際のネットワークアドレス/サブネットマスクとルーティングテーブル上のルート情報のネットワークアドレス/サブネットマスクが異なっても問題ありません。

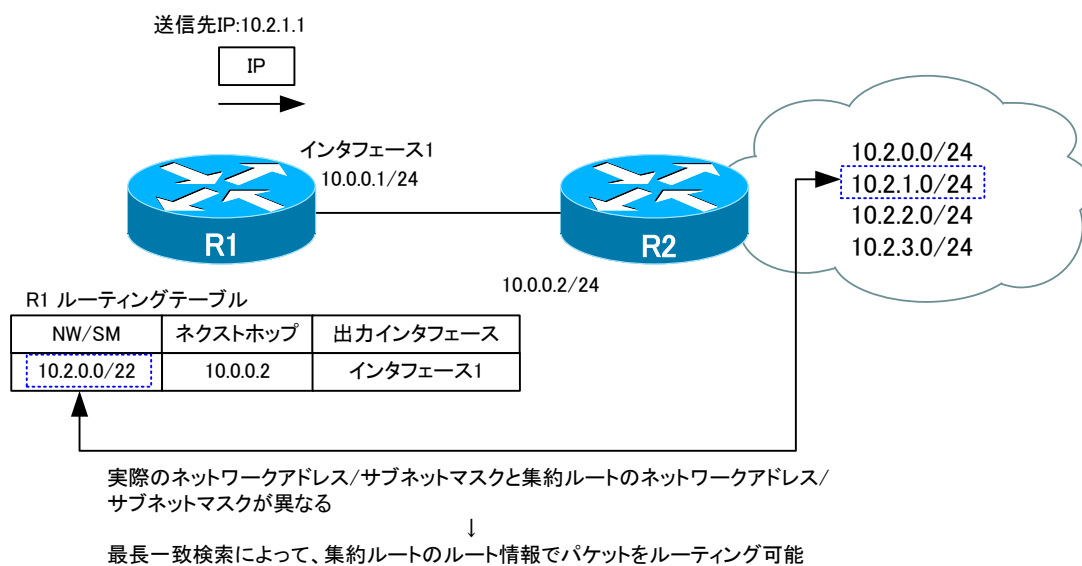


図 35 集約ルートによるルーティング

最長一致検索によるルート情報の検索は、宛先 IP アドレスとルート情報のネットワークアドレスについて、サブネットマスク分のビットが一致しているかをチェックしています。具体的には、パケットの宛先 IP アドレスとルート情報のサブネットマスクの論理積を計算します。その結果がルート情報のネットワークアドレスと同じであれば、そのルート情報をパケットのルーティングに利用することができます。つまり、宛先 IP アドレスがルート情報のネットワークアドレス/サブネットマスクの範囲に含まれているかどうかをチェックしています。

もし、該当するルート情報が複数ある場合、サブネットマスクのビット数が最も多いルート情報を利用して、パケットをルーティングします。

※ レイヤ 2 スイッチで宛先 MAC アドレスから MAC アドレステーブルのエントリを検索するときには、完全一致検索です。

具体的に次のようなルーティングテーブルで考えてみましょう。

表 7 ルーティングテーブルの例

ネットワークアドレス	サブネットマスク
10.2.0.0	/24
10.2.1.0	/24
10.2.2.0	/24
10.2.3.0	/24
10.2.0.0	/22
0.0.0.0	/0

※ このルーティングテーブルの例は、簡単にするためにネクストホップなどは省略して、ネットワークアドレスとサブネットマスクのみを抜き出しています。

このようなルーティングテーブルを持つルータに、送信先 IP アドレスとして 10.2.2.100 が指定されているパケットが届いたとします。各ルート情報のサブネットマスクと送信先 IP アドレスの論理積を計算し、ネットワークアドレスと比較します。

10.2.0.0/24

送信先IP 10.2.2.100 = 0000 1010 0000 0010 0000 0010 0110 0010  
サブネットマスク /24 = 1111 1111 1111 1111 1111 1111 0000 0000  
AND = 0000 1010 0000 0010 0000 0010 0000 0000

ネットワークアドレス 10.2.0.0 = 0000 1010 0000 0010 0000 0000 0000 0000

図 36 10.2.0.0/24 のルート情報との比較

10.2.1.0/24

送信先IP 10.2.2.100 = 0000 1010 0000 0010 0000 0010 0110 0010  
サブネットマスク /24 = 1111 1111 1111 1111 1111 1111 0000 0000  
AND = 0000 1010 0000 0010 0000 0010 0000 0000

ネットワークアドレス 10.2.1.0 = 0000 1010 0000 0010 0000 0001 0000 0000

図 37 10.2.1.0/24 のルート情報との比較



10.2.2.0/24

送信先IP 10.2.2.100 = 0000 1010 0000 0010 0000 0010 0110 0010  
サブネットマスク /24 = 1111 1111 1111 1111 1111 1111 0000 0000  
AND = 0000 1010 0000 0010 0000 0010 0000 0000

ネットワークアドレス 10.2.2.0 = 0000 1010 0000 0010 0000 0010 0000 0000

図 38 10.2.2.0/24 のルート情報との比較

10.2.3.0/24

送信先IP 10.2.2.100 = 0000 1010 0000 0010 0000 0010 0110 0010  
サブネットマスク /24 = 1111 1111 1111 1111 1111 1111 0000 0000  
AND = 0000 1010 0000 0010 0000 0010 0000 0000

ネットワークアドレス 10.2.3.0 = 0000 1010 0000 0010 0000 0011 0000 0000

図 39 10.2.3.0/24 のルート情報との比較

10.2.0.0/22

送信先IP 10.2.2.100 = 0000 1010 0000 0010 0000 0010 0110 0010  
サブネットマスク /22 = 1111 1111 1111 1111 1111 1100 0000 0000  
AND = 0000 1010 0000 0010 0000 0000 0000 0000

ネットワークアドレス 10.2.0.0 = 0000 1010 0000 0010 0000 0000 0000 0000

図 40 10.2.0.0/22 のルート情報との比較

0.0.0.0/0

送信先IP 10.2.2.100 = 0000 1010 0000 0010 0000 0010 0110 0010  
サブネットマスク /0 = 0000 0000 0000 0000 0000 0000 0000 0000  
AND = 0000 0000 0000 0000 0000 0000 0000 0000

ネットワークアドレス 0.0.0.0 = 0000 0000 0000 0000 0000 0000 0000 0000

図 41 0.0.0.0/0 のルート情報との比較

これを見ると、宛先 IP アドレス 10.2.2.100 のパケットをルーティングするために、次の 3 つのルート情報を利用できます。

- ・ 10.2.2.0/24(この範囲内に宛先 IP 10.2.2.100 が含まれている)
- ・ 10.2.0.0/22(この範囲内に宛先 IP 10.2.2.100 が含まれている)
- ・ 0.0.0.0/0(この範囲内に宛先 IP 10.2.2.100 が含まれている)

この中で実際にパケットをルーティングするために利用するのは、サブネットマスクが最も長い  
10.2.2.0/24 のルート情報です。

集約ルートは広い範囲のネットワークを示していますが、個別のネットワークを識別できないおおざっぱなルート情報です。最長一致検索を簡単に言えば、おおざっぱなルート情報と詳細なルート情報がある場合は、詳細なルート情報にしたがってパケットをルーティングするということです。

## ルート情報を地図にたとえると

ルート情報を地図にたとえると、集約ルートは縮尺が小さい地図です。縮尺が小さい地図は、広い範囲をカバーしていますが、建物や道など詳細がわかりません。縮尺が大きくなると、カバーする範囲は狭くなりますが、建物や道の詳細までわかります。最長一致検索は、目的地に行くために縮尺が小さい地図よりも縮尺が大きいより詳細な地図を使うのと同じようなことです。

たとえば、新宿駅から新宿御苑に行きたいときは、以下のどちらの地図を使いますか？当然、縮尺が大きい地図 I でしょう。

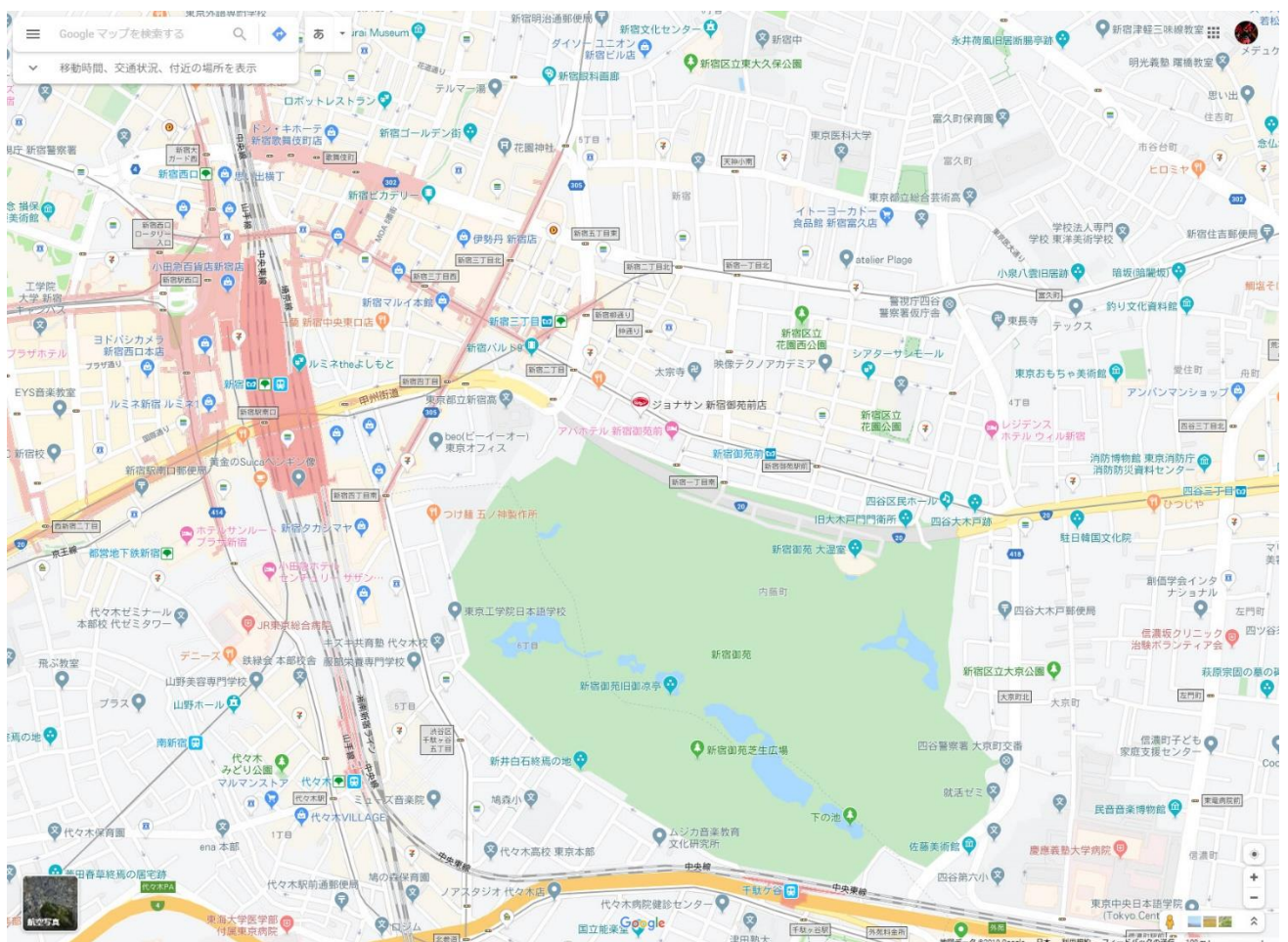


図 42 新宿御苑までの地図 I



# 基礎からの CCNA(200-301)攻略テキスト

## 第 10 章 IP ルーティング

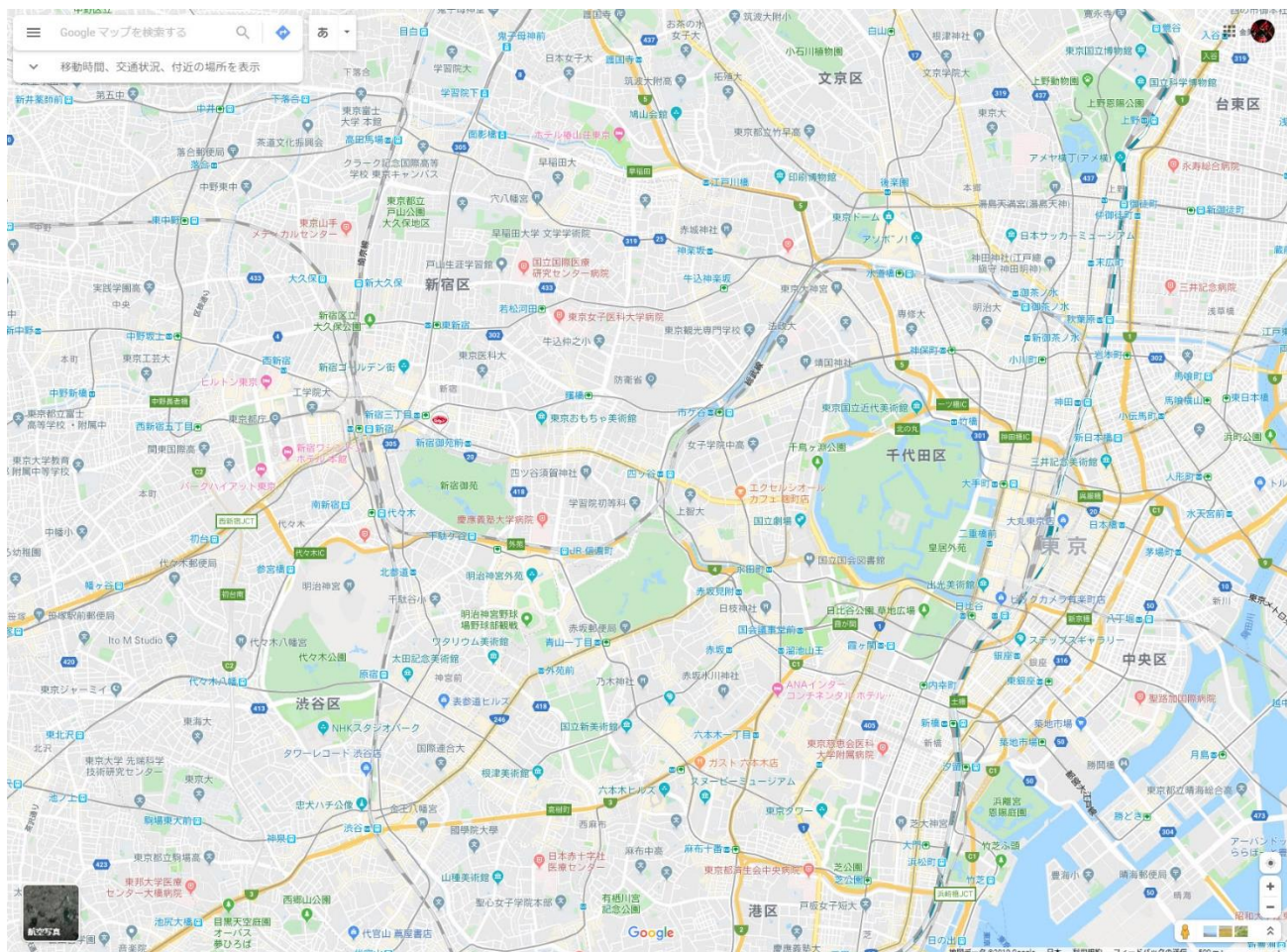


図 43 新宿御苑までの地図 2

どちらの地図にも、目的地となる新宿御苑は載っています。しかし、縮尺が小さい地図 2 では、新宿御苑までの細かな経路がわかりづらいです。縮尺が大きい地図 1 のほうが、より詳細な地図で建物や道の名前などが詳しく載せられているので目的地の新宿御苑へ到達しやすいでしょう。

ルーティングの場合も同じように考えてください。宛先 IP アドレスを含むルート情報が複数ある場合には、より詳細なサブネットマスクが長いルート情報を優先します。

### デフォルトルートは最後の手段

デフォルトルートは「**Last Resort(最後の手段)**」と呼ばれることがあります。デフォルトルートはあらゆるネットワークを集約している最も極端な集約ルートです。前述の例で考えたように、最長一致検索によって、デフォルトルートはどんな IP アドレスであっても一致するルート情報です。宛先 IP アドレスがどのようなアドレスであったとしてもサブネットマスク「**0.0.0.0**」との論理積をとると、「**0.0.0.0**」です。そのため、必ずデフォルトルートのネットワークアドレス「**0.0.0.0**」と一致することになります。

ただし、いつでもデフォルトルートを利用するわけではありません。他に利用できるルート情報がない場合だけの最後の手段としてデフォルトルートを利用することになります。なお、デフォルトルートを地図にたとえると、世界地図のようなイメージです。

# 基礎からの CCNA(200-301)攻略テキスト

## 第 10 章 IP ルーティング

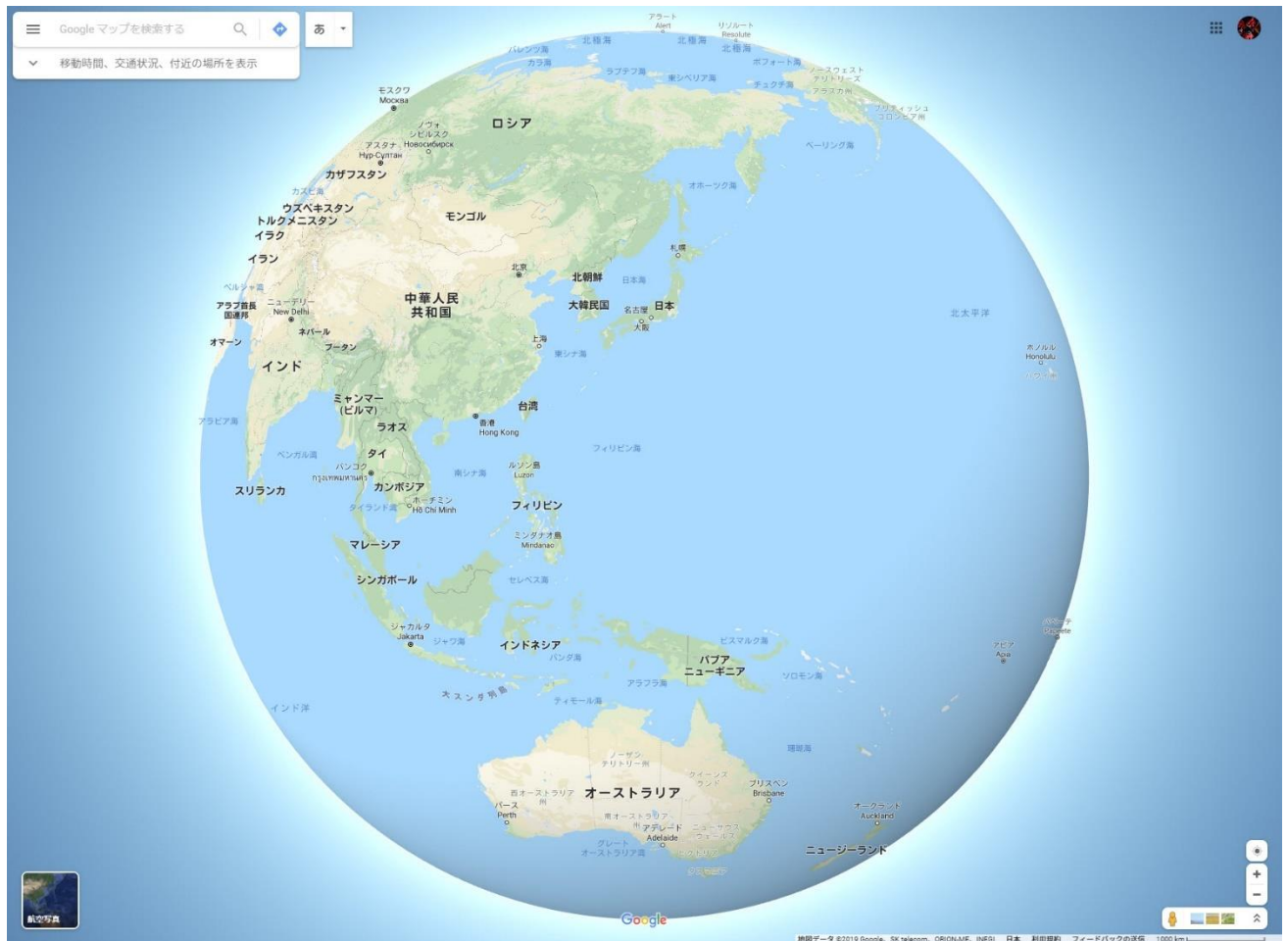


図 44 デフォルトルートのイメージ

## ルーティングプロトコルの分類

### ポイント

- ・ ルーティングプロトコルは、適用範囲、アルゴリズム、ネットワークアドレスの認識によって分類できます。

### ルーティングプロトコル分類の概要

RIP(Routing Information Protocol)、OSPF(Open Shortest Path First)、BGP(Border Gateway Protocol)などのルーティングプロトコルは、次の 3 つの観点から分類することができます。

- ・ ルーティングプロトコルの適用範囲による分類
- ・ ルーティングプロトコルのアルゴリズムによる分類
- ・ ネットワークアドレスの認識による分類

3 種類の分類の観点について順に解説します。

### ルーティングプロトコルの適用範囲

ルーティングプロトコルは、その適用範囲によって、「内部ゲートウェイプロトコル(Interior Gateway Protocol s: IGP s)」と「外部ゲートウェイプロトコル(Exterior Gateway Protocols : EGP s)」に分類することができます。

「内部」「外部」とありますが、これは「自律システム(Autonomous System : AS)」の外部か内部かということを示しています。自律システムとは、

「狭義：同一のルーティングプロトコルを採用しているネットワークの集合」

「広義：ある管理組織が同一の管理ポリシーに従って運用されているネットワークの集合」

です。

狭義の意味は、たとえば OSPF なら OSPF でルーティングの設定をしているネットワークの集合を指しています。OSPF では、ASBR(Autonomous System Boundary Router)という種類のルータがあります。OSPF の ASBR の「AS」は狭義の意味の AS です。

IGPs、EGPs の分類で考えている AS は、広義の「同一の管理ポリシーに従って運用されているネットワークの集合」です。簡単に言えば、ある組織のネットワーク全体が自律システムです。広義の AS のネットワークは、管理している組織がアドレスやルーティングのポリシーを決め、機器を導入して構築し、運用管理を行います。AS 内のネットワークのルート情報を扱うルーティングプロトコルが IGP s です。IGPs の分類の具体的なルーティングプロトコルには、RIP(Routing Information Protocol)、OSPF(Open Shortest



Path First)などがあります。

現在、広く普及しているインターネットは、世界規模で **AS** が相互に接続しているネットワークです。インターネットが「ネットワークのネットワーク」と呼ばれる所以です。

インターネット上で、各 **AS** を識別するために **AS** 番号を用いています。**AS** 間で相互に通信を行うためには、各 **AS** が管理しているネットワークのルート情報を交換します。そのために利用するルーティングプロトコルが **EGPs** です。**EGPs** の分類の具体的なルーティングプロトコルは **BGP(Border Gateway Protocol)** です。

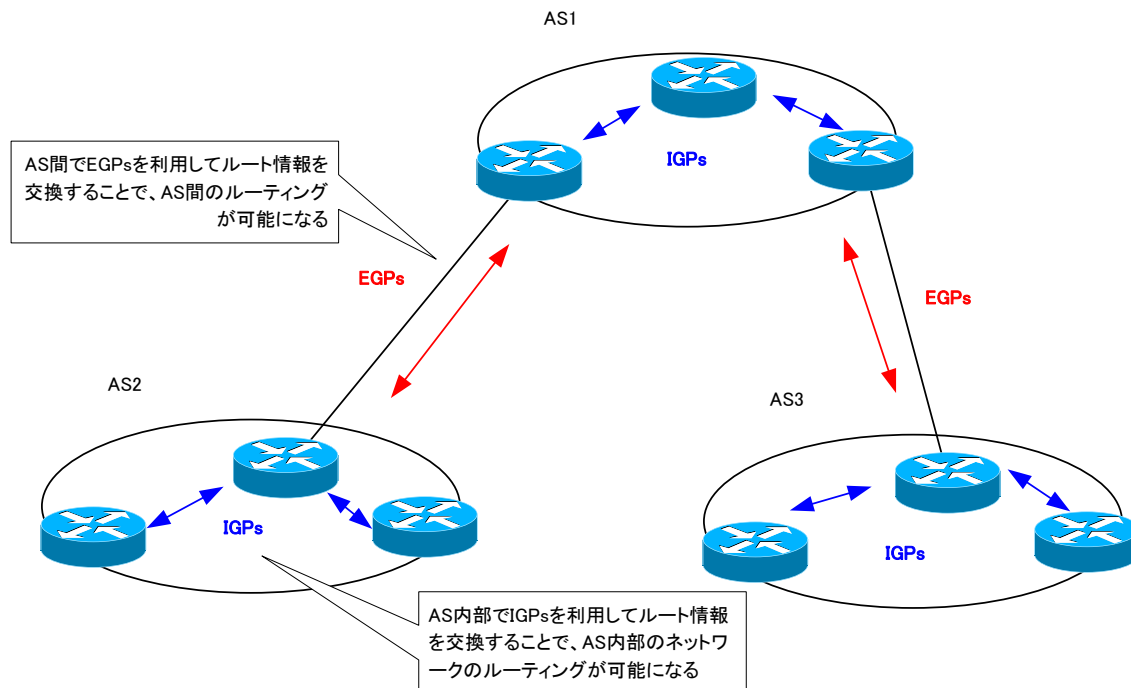


図 45 IGPs と EGPs

企業のネットワークは、ひとつの組織のネットワークです。つまり、企業ネットワーク内で利用するルーティングプロトコルは **RIP** や **OSPF** などの **AS** 内部で利用する **IGPs** です。ただし、**IP-VPN** サービスを利用して拠点間を接続しているときには、ある組織のネットワーク内で **BGP** を利用することもあります。以下の表に、**IGPs** と **EGPs** の特徴をまとめています。

表 8 IGPs と EGPs の特徴

特徴	IGPs	EGPs
適用範囲	AS 内部	AS 間
プロトコル例	RIPv1/v2 、 EIGRP 、 OSPF、 IS-IS	EGP、 BGP

## ルーティングアルゴリズムによる分類

ルーティングプロトコルのアルゴリズムとして、主に次の 3 つあります。

- ・ ディスタンスベクタ型
- ・ リンクステート型
- ・ ハイブリッド(拡張ディスタンスベクタ)型

そして、こうしたルーティングプロトコルのアルゴリズムのポイントは、次の 3 点です。

- ・ 「どのような情報」を交換するか
- ・ 「どのようなタイミング」で交換するか
- ・ 交換した情報から「どのように」最適ルートなルート情報を決定するか

以降、3 つのルーティングプロトコルのアルゴリズムについて、それぞれ 3 つのポイントを考えましょう。

### ディスタンスベクタ型

ディスタンスベクタ型ルーティングプロトコルでは、ルータ同士でネットワークアドレス/サブネットマスク+メトリックの情報を交換します。ディスタンスベクタ型のルーティングプロトコルは、「距離」と「方向」に基づいてルートを決めるといように説明されていることが多いです。具体的に、距離とはメトリックです。そして、方向はネクストホップとインタフェースです。ディスタンスベクタ型ルーティングプロトコルのルート情報の送信を簡単に示したものが次の図です。

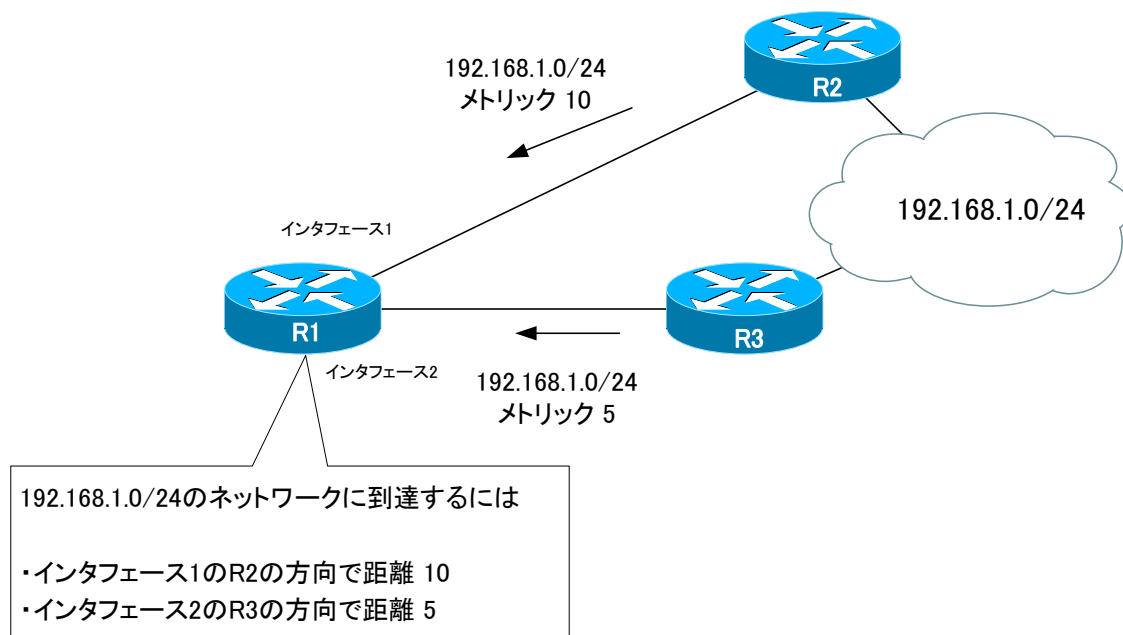


図 46 「距離」と「方向」

R1 は 192.168.1.0/24 のネットワークのルート情報を R2 と R3 から受信しています。R2 から送信されたルート情報にはメトリック 10 が含まれていて、R1 のインタフェース 1 で受信しています。R1 から見ると、192.168.1.0/24 のネットワークはインタフェース 1 の R2 の方向で距離 10 だけ離れていることになります。同様に R3 から送信された 192.168.1.0/24 のルート情報に含まれるメトリックは 5 で、R1 はインタフェース 2 で受信します。つまり、R1 から 192.168.1.0/24 のネットワークは、インタフェース 2 の R3 の方向で距離 5 だけ離れています。

また、ディスタンスベクタ型ルーティングプロトコルではネットワーク構成に何も変更がなくても定期的にルート情報を交換します。定期的にルート情報を交換することで、他のルータがきちんと動作していることやリモートネットワークがダウンしていないことを確認しています。

そして、交換したルート情報から最適ルートを決定するために、ベルマンフォードアルゴリズムを採用しています。簡単に言えば、メトリックが最小のルート情報が最適ルートとしてルーティングテーブルに登録されるようになります。

具体的なディスタンスベクタ型ルーティングプロトコルは、RIPv1 および RIPv2 です。

※ なお、RIPv1 は後述するクラスフルルーティングプロトコルなので、交換するルート情報にサブネットマスクを含みません。

## リンクステート型

リンクステート型ルーティングプロトコルでは、ルータは自分が持っているリンクステート情報(Link State Advertisement : LSA)を交換します。LSA の中には、そのルータがどのようなインタフェースを持っていて、どのようなタイプのネットワークに接続されていて、IP アドレスがいくつ、帯域幅がいくつなどという情報が入っています。なお、LSA の交換は何らかの変更があったタイミングで行います。この LSA を集めて、リンクステートデータベース(Link State Data Base : LSDB)を作成します。

LSDB には、ネットワーク上のルータの LSA がすべて含まれています。つまり、LSDB を見れば、ネットワーク上にルータが何台存在していて、各ルータがどんなインタフェースをいくつ持っていて、他のルータとどのように接続されているか、というネットワーク構成を再現することができます。

LSA を交換して作成した LSDB から、最適ルートを決定するために SPF(Shortest Path First)アルゴリズムを採用しています。LSDB 内のルータ自身を起点として、リモートネットワークへの最小コストとなるルートを最適ルートとしてルーティングテーブルに登録します。

具体的なリンクステート型ルーティングプロトコルは、OSPF と IS-IS です。次の図は、OSPF の動作を簡単に表したものです。



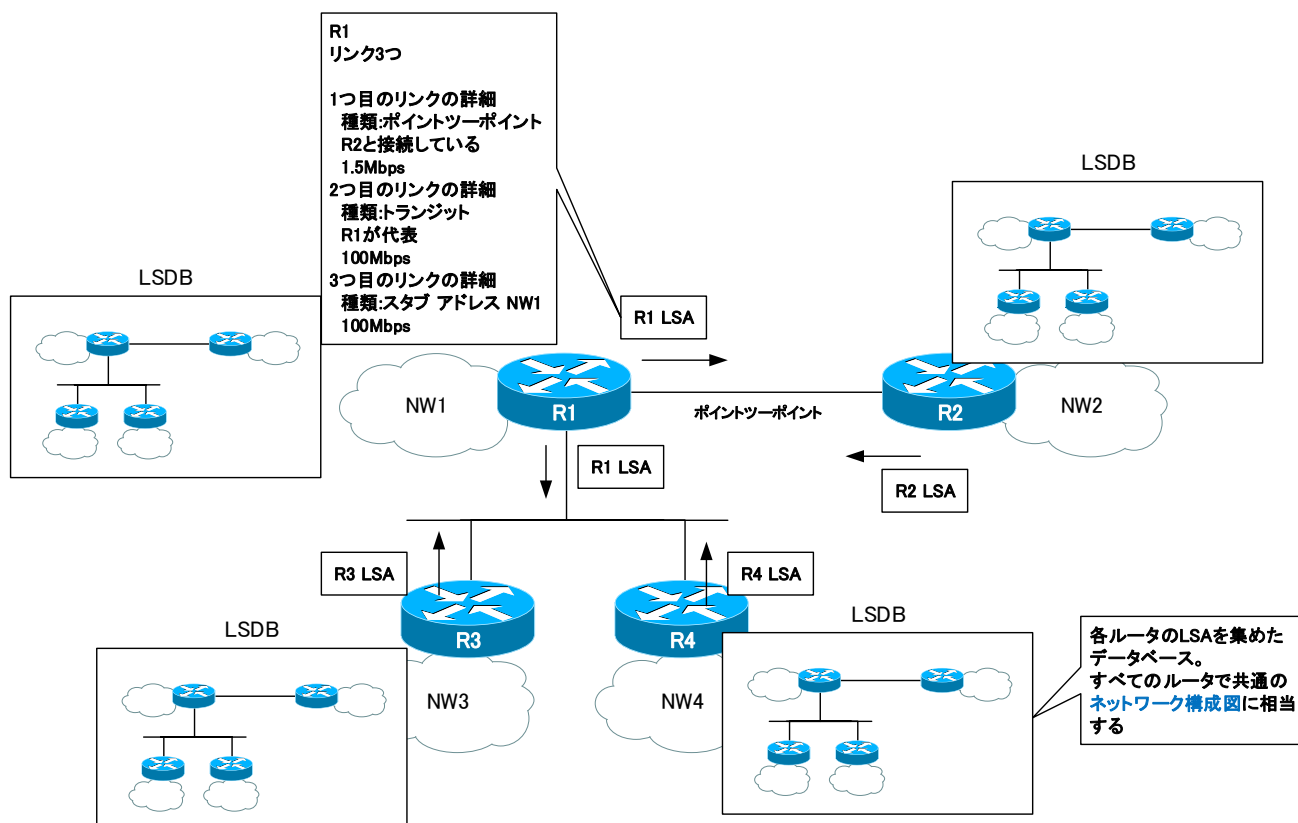


図 47 OSPF の動作の概要

## ハイブリッド(拡張ディスタンスベクタ)型

ハイブリッド(拡張ディスタンスベクタ)型は、Cisco が独自にディスタンスベクタ型を拡張したルーティングアルゴリズムです。ベースはディスタンスベクタなので、ルータ同士が交換する情報は、ネットワークアドレス/サブネットマスク+メトリックです。ただし、定期的ではなく、ネットワークに変更があったときのみ交換します。

交換したルート情報から **DUAL(Diffusing Update Algorithm)**によって、最適ルートを決定します。簡単に言えば、**DUAL**でもメトリックが最小のルート情報が最適ルートになり、ルーティングテーブルに登録されます。また **DUAL**では、最適ルートだけでなく利用可能なバックアップルートもあらかじめ決めておきます。利用可能なバックアップルートがあれば、障害発生時のコンバージェンスを非常に高速に行うことができます。

ハイブリッド型ルーティングプロトコルの具体的な例は、Cisco の **EIGRP** です。

次の表にルーティングアルゴリズムの特徴をまとめています。

表 9 ルーティングアルゴリズムの特徴

	ディスタンスベクタ	リンクステート	ハイブリッド
情報	ネットワークアドレス /サブネットマスク+メ トリック	リンクステート情報	ネットワークアドレス /サブネットマスク+メ トリック
タイミング	定期的	変更時	変更時
決定	ベルマンフォード	SPF	DUAL
プロトコル例	RIPv1 /v2	OSPF、IS-IS	EIGRP

## ネットワークアドレスの認識による分類

ルーティングプロトコルで、どのようにしてネットワークアドレスを認識するかによって次の 2 つに分類できます。

- ・ クラスフルルーティングプロトコル
- ・ クラスレスルーティングプロトコル

クラスフルルーティングプロトコルは、ネットワークアドレスを基本的にクラス単位で認識します。つまり、**32 ビットの IP アドレスのうちネットワークアドレスとして、クラス A なら先頭 8 ビット、クラス B なら先頭 16 ビット、クラス C なら 24 ビットとして認識します。**

クラス単位でネットワークアドレスを認識するので、ネットワークアドレスとホストアドレスの区切りを示すサブネットマスクは必要ありません。クラスフルルーティングプロトコルでは、ルータ同士で交換するルート情報の中にサブネットマスクが含まれていません。**RIPv1** はクラスフルルーティングプロトコルです。

※ 「基本的に」としているのは、必ずしもクラス単位でないことがあるからです。より厳密には、クラスとルート情報を受信したインタフェースのサブネットマスクによってネットワークアドレスを認識します。

現在の IP アドレスの考え方は、クラスにとらわれずに IP アドレスを考えるクラスレスアドレッシングが一般的です。そのため、クラスフルルーティングプロトコルでは、クラスレスアドレッシングを行っているネットワークのルート情報を正しく扱うことができません。クラスレスアドレッシングのネットワークのルート情報を正しく扱うためには、クラスレスルーティングプロトコルを利用します。

クラスレスアドレッシングでは、**32 ビットの IP アドレスのうち、ネットワークアドレスがどの部分かを表すためにサブネットマスクを利用します。**クラスレスルーティングプロトコルでは、クラスレスアドレッシングのネットワークアドレスを正しく扱うために、交換するルート情報にサブネットマスクの情報も含めています。

クラスレスルーティングプロトコルの例は、**RIPv2、OSPF、EIGRP、BGP** など一般的に利用するルーテ

イングプロトコルです。現在、アドレスの考え方はクラスレスアドレッシングなので、通常はルーティングプロトコルもクラスレスルーティングプロトコルを利用します。

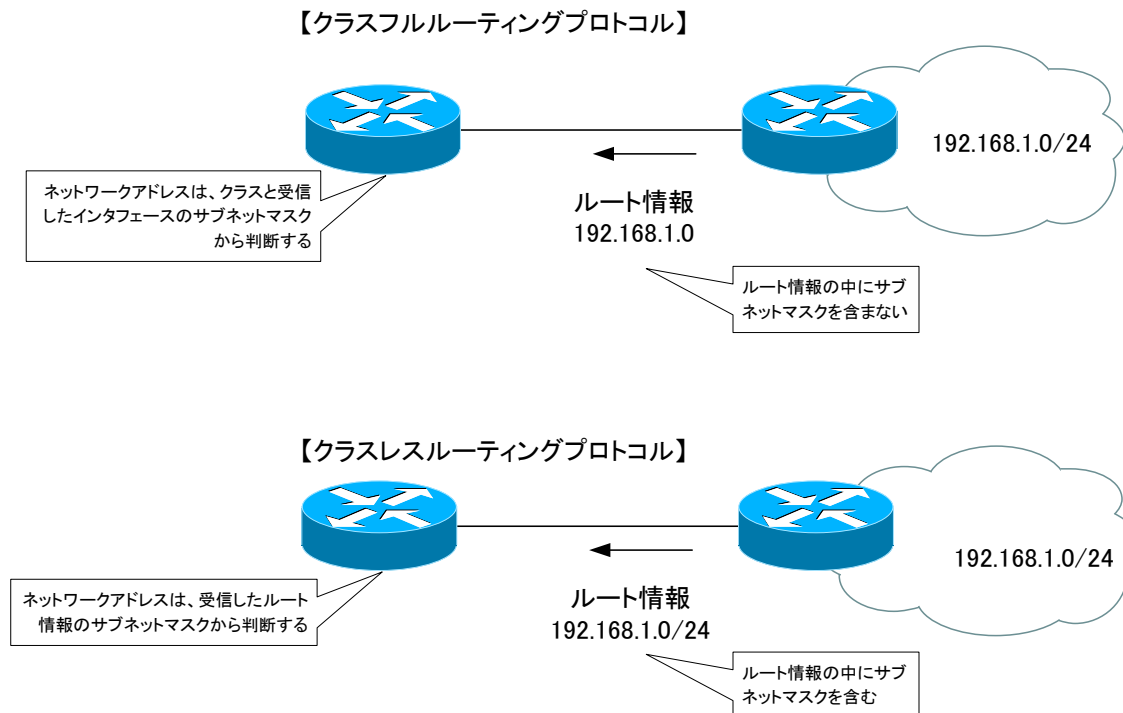


図 48 クラスフルルーティングプロトコルとクラスレスルーティングプロトコル

※ サブネット化されているアドレス構成でもクラスフルルーティングプロトコルを利用することは可能です。ただし、**FLSM** のアドレス構成のみで **VLSM** のアドレス構成では正しくルート情報を送信できません。また、不連続サブネットのアドレス構成も正常にルート情報を送信できません。

## スタティックルートの設定

### ポイント

- ・ スタティックルートの設定を行うにあたって、それぞれのルータにとってのリモートネットワークを明確にしておくことが重要です。
- ・ リモートネットワークのルート情報を **ip route** コマンドによってルーティングテーブルに登録します。

### スタティックルートの設定

スタティックルートの設定の手順は、次のとおりです。

1. 各ルータにとってのリモートネットワークを明確にする
2. **ip route** コマンドでリモートネットワークのルート情報をもれなく登録する

スタティックルートの設定において重要なことは、各ルータにとってのリモートネットワークを明確にしておくことです。そして、1 台のルータだけでスタティックルートの設定をしても意味はありません。スタティックルートでルーティングの設定を行うときには、関係するすべてのルータでスタティックルートの設定をもれなく正しく行わなければいけません。

リモートネットワークを明確にしたうえで、次のコマンドでスタティックルートの設定を行います。

```
(config)#ip route <network> <subnetmask> <next-hop> [<interface>] [<AD>]
```

<network> : ネットワークアドレス

<subnetmask> : サブネットマスク

<next-hop> : ネクストホップアドレス

<interface> : 出力インタフェース

<AD> : アドミニストレイティブディスタンス

ネクストホップアドレスは、原則として同一ネットワークの次のルータの **IP** アドレスです。また、出力インタフェースを指定するのは、ポイントツーポイントインタフェースのときのみです。イーサネットのようなマルチアクセスインタフェースではアドレス解決ができないので、パケットを適切に出力できなくなってしまう。

アドミニストレイティブディスタンスは、省略するとデフォルトの 1 です。アドミニストレイティブディスタンスを大きくすることで、スタティックルートをバックアップルートとして設定することも可能です。

※ アドミニストレイティブディスタンスを大きく設定してバックアップルートとしたスタティックルートはフローティングスタティックルートと呼ばれます。

スタティックルートの確認は **show ip route** コマンドでルーティングテーブルを表示します。**show ip route static** とすれば、ルーティングテーブルの中からスタティックルートのみを表示できます。

なお、スタティックルートはネクストホップに到達できなければ、ルーティングテーブルから削除されます。以下の図で **R1 Fa0/0** がダウンすると、ネクストホップに到達できなくなるので、ルーティングテーブルからスタティックルートは削除されます。

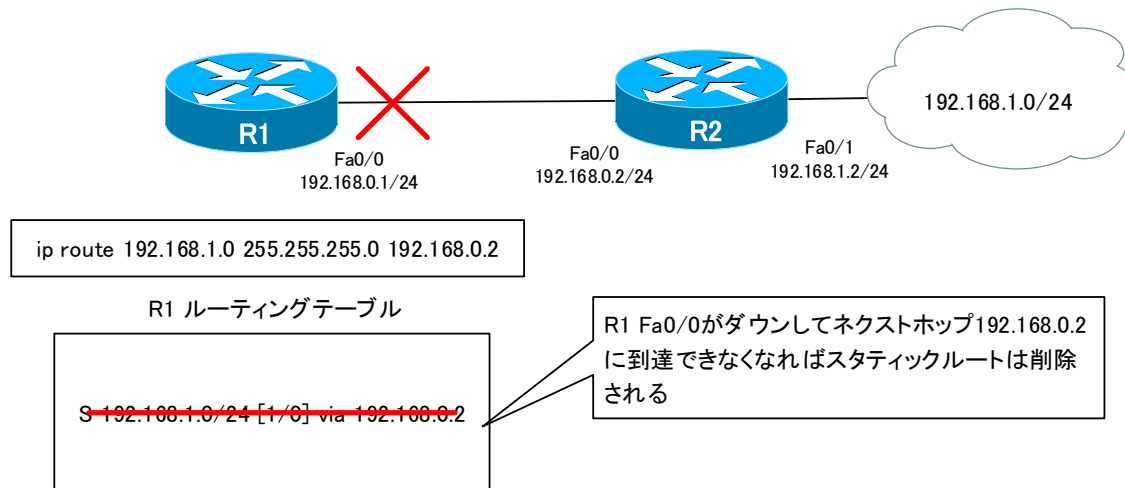


図 49 スタティックルートの削除 その 1

しかし、**R2 Fa0/1** がダウンして **192.168.1.0/24** のネットワークそのものに到達できなくなったとしても、**R1** のスタティックルートは残ったままです。

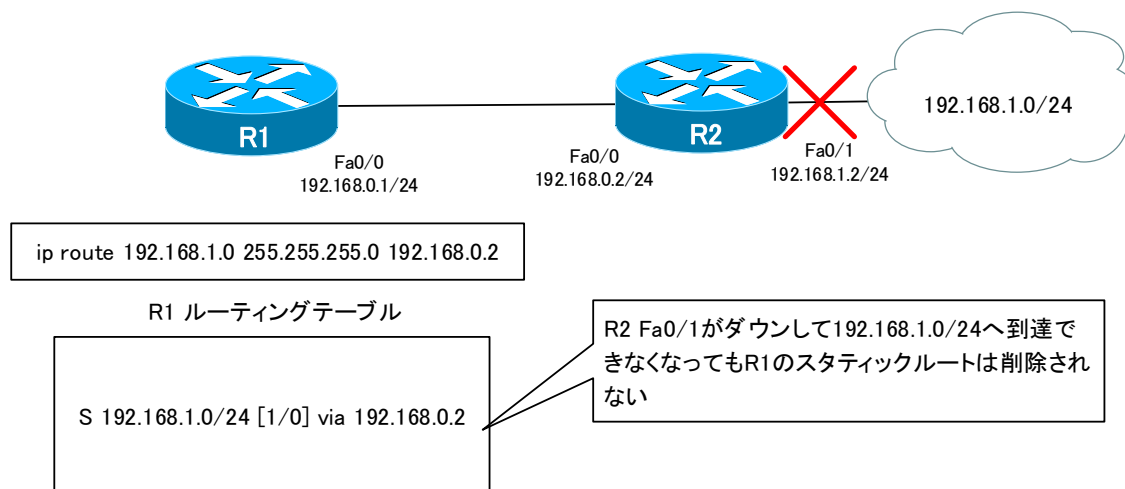


図 50 スタティックルートの削除 その 2

## ルーティングテーブル上のデフォルトルート

スタティックルートとしてデフォルトルートを登録する場合には、グローバルコンフィグレーションモードで以下のように設定します。

```
(config)#ip route 0.0.0.0 0.0.0.0 <next-hop>
```

通常のスタティックルートの設定コマンドでネットワークアドレスとサブネットマスクとともに「0.0.0.0」とすればよいだけです。

そして、Cisco ルータのルーティングテーブルにデフォルトルートを登録した場合、ルーティングテーブルは次のような例になります。

```
-----  
R2#show ip route  
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP  
        D - EIGRP, EX - EIGRP external, O - OSPF, 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  
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2  
        ia - IS-IS inter area, * - candidate default, U - per-user static route  
        o - ODR, P - periodic downloaded static route  
  
Gateway of last resort is 200.0.0.2 to network 0.0.0.0  
  
C    192.168.12.0/24 is directly connected, Ethernet0/0  
    200.0.0.0/24 is variably subnetted, 2 subnets, 2 masks  
C      200.0.0.0/30 is directly connected, Serial1/0  
C      200.0.0.2/32 is directly connected, Serial1/0  
C    192.168.21.0/24 is directly connected, Ethernet0/1  
    10.0.0.0/24 is subnetted, 2 subnets  
O IA   10.3.3.0 [110/11] via 192.168.32.3, 00:00:06, Ethernet0/3  
O IA   10.1.1.0 [110/20] via 192.168.21.1, 00:00:06, Ethernet0/1  
        [110/20] via 192.168.12.1, 00:00:08, Ethernet0/0  
C    192.168.23.0/24 is directly connected, Ethernet0/2  
C    192.168.32.0/24 is directly connected, Ethernet0/3  
S*    0.0.0.0/0 [1/0] via 200.0.0.2  
-----
```

ルーティングテーブルにデフォルトルートが登録されていると、ルート情報の個別のエントリの上部に「Gateway of last resort is 200.0.0.2 to network 0.0.0.0」と表示されます。これは、「ネットワークアドレス **0.0.0.0** でデフォルトルートが設定されていて、そのネクストホップが **200.0.0.2**」ということを意味しています。**last resort** とは、最後の手段という意味です。

そして、ルート情報の個別のエントリに、「S\* 0.0.0.0/0 [1/0] via 200.0.0.2」のように「\*」が付加されます。「\*」はデフォルトルートとして利用するルート情報であることを意味していて、「**0.0.0.0/0**」のルート情報には自動的に「\*」が付加されます。

## ip default-network コマンド

Cisco ルータでは、デフォルトルート「**0.0.0.0/0**」以外のルート情報に「\*」のフラグを付けてデフォルトルートのように扱うこともできます。そのための設定コマンドとして、**ip default network** コマンドがあります。

以下は、「**0.0.0.0/0**」以外のルート情報をデフォルトルートとして利用しているルーティングテーブルのサンプルです。R2 には、次のような設定をしています。

```
R2(config)#ip default-network 172.16.0.0
```

この設定により、**172.16.0.0/16** に「\*」のフラグを付けてデフォルトルートのように扱うものとしています。すると、ルーティングテーブルの上部に「Gateway of last resort is 192.168.23.3 to network 172.16.0.0」と表示されます。これは、「**172.16.0.0/16** のルート情報をデフォルトルート扱いとして、そのネクストホップは **192.168.23.3** である」ことを意味しています。「Gateway of last resort(ラストリゾートゲートウェイ)」とは、デフォルトルートのネクストホップのことを指しています。

-----  
R2#show ip route

～省略～

Gateway of last resort is 192.168.23.3 to network 172.16.0.0

C 192.168.12.0/24 is directly connected, Ethernet0/0

S\* 172.16.0.0/16 [1/0] via 192.168.23.3

C 192.168.21.0/24 is directly connected, Ethernet0/1

10.0.0.0/8 is variably subnetted, 4 subnets, 3 masks

S 10.3.3.0/24 [1/0] via 192.168.23.3

S 10.1.1.0/24 [1/0] via 192.168.12.1

S 10.0.0.0/8 [1/0] via 10.1.0.0

S 10.1.0.0/16 [1/0] via 192.168.21.1

C 192.168.23.0/24 is directly connected, Ethernet0/2

C 192.168.32.0/24 is directly connected, Ethernet0/3  
-----

※ あらためて確認ですが、デフォルトルートはスタティックルートの設定以外でもルーティングテーブルに登録することは可能です。



## フローティングスタティックルート

スタティックルートを障害発生時のバックアップルートとして自動的にルーティングテーブルに登録されるようにできます。そのようなスタティックルートをフローティングスタティックルートと呼びます。フローティングスタティックルートの設定自体はシンプルです。スタティックルートのアドミニストレイティブディスタンスはデフォルトで 1 ですが、その値を大きく設定すればよいだけです。設定する値は、利用しているルーティングプロトコルよりも大きい値とします。

フローティングスタティックルートは、主に拠点間を接続する WAN のバックアップとして、ISDN など従量課金の WAN サービスを利用しているケースで行う設定です。たとえば、以下のようなネットワーク構成です。

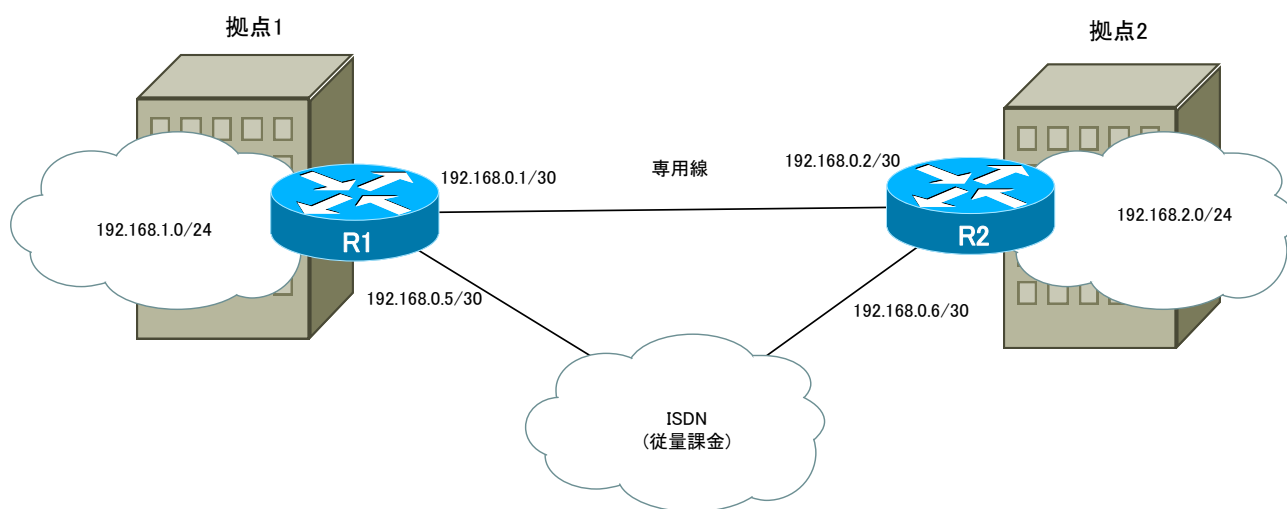


図 51 フローティングスタティックルート ネットワーク構成例

拠点 1 と拠点 2 を専用線で接続して、通常は専用線経由で拠点間の通信を行います。そして、そのバックアップとして ISDN を利用しているという例です。

専用線経由で通信するために、各拠点のルータでは専用線上でルーティングプロトコルを利用してルーティングテーブルにお互いの拠点のルートを登録します。ルーティングプロトコルは、定期的にルーティングプロトコルのパケットを送受信してしまいます。ISDN 上でルーティングプロトコルを利用すると、ISDN 回線を常時接続することになり通信料金が常にかかってしまいます。そのため、ISDN 上ではルーティングプロトコルを利用しません。専用線に障害発生したときのバックアップルートとしてフローティングスタティックルートの設定を行います。アドミニストレイティブディスタンスを専用線で利用しているルーティングプロトコルよりも大きい値で、お互いの拠点のルート情報を設定します。

利用しているルーティングプロトコルが RIP(アドミニストレイティブディスタンス 120)の場合、R1 と R2 でのフローティングスタティックルートの設定は、次のように行います。

## R1

```
ip route 192.168.2.0 255.255.255.0 192.168.0.6 125
```

## R2

```
ip route 192.168.1.0 255.255.255.0 192.168.0.5 125
```

お互いの拠点のルート情報のネクストホップを **ISDN** のインタフェースの **IP** アドレスとしています。そして、スタティックルートの設定の最後の「**125**」がアドミニストレイティブディスタンス値で **RIP** の **120** よりも大きい値にしています。

ルーティングテーブルには、専用線経由のルーティングプロトコルで学習したルートのみが登録されています。フローティングスタティックルートの設定は、ルーティングテーブル上には現れず、ルーティングプロトコルのルートの下に隠れています。

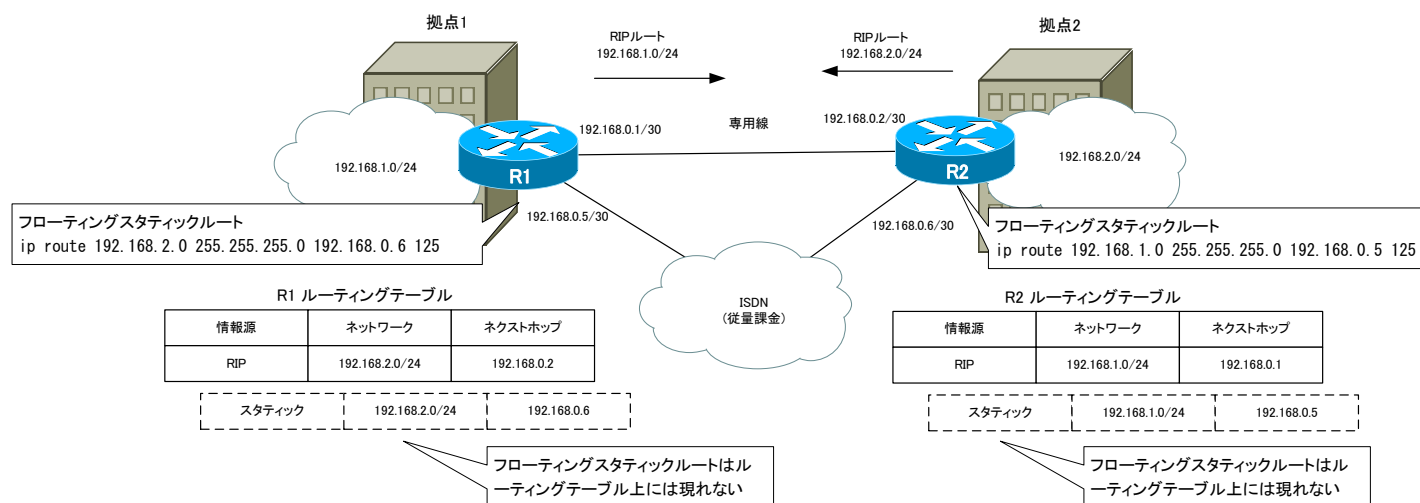


図 52 フローティングスタティックルート 正常時

専用線に障害が発生すると、専用線経由で学習している **RIP** のルート情報が削除されます。すると、隠れていたフローティングスタティックルートがルーティングテーブルに登録されて、**ISDN** 経由で通信を継続できます。障害時に隠れていたスタティックルートが浮かび上がってくるようなイメージなので「フローティング」スタティックルートと呼ばれています。

基礎からの CCNA(200-301)攻略テキスト  
第 10 章 IP ルーティング

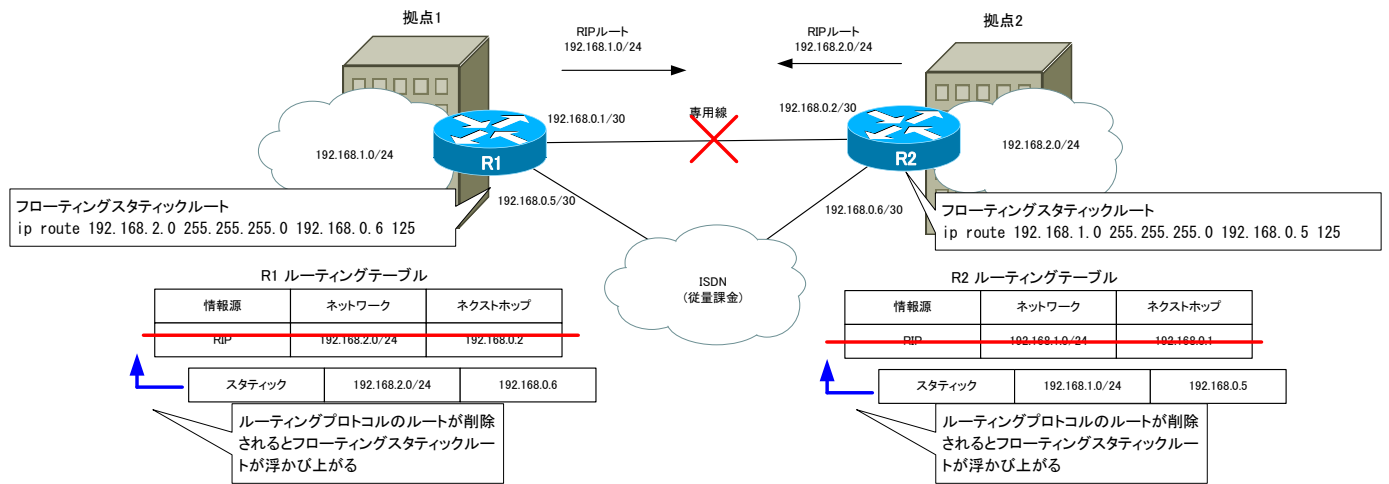
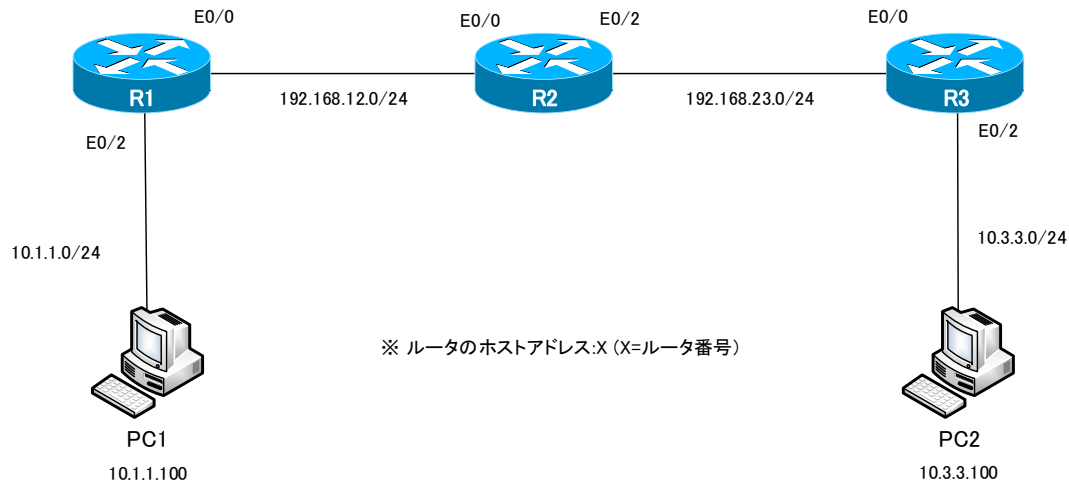


図 53 フローティングスタティックルート 障害発生時

## スタティックルートの設定例

### ネットワーク構成

以下のとてもシンプルなネットワーク構成で、スタティックルートの設定について考えます。



### IP アドレスのみを設定しているときのルーティングテーブル

R1～R3 で IP アドレスのみを設定していると、それぞれのルータの直接接続のネットワークについてのルート情報のみがルーティングテーブルに登録されています。

R1

-----

R1#show ip route

～省略～

Gateway of last resort is not set

C 192.168.12.0/24 is directly connected, Ethernet0/0

10.0.0.0/24 is subnetted, 1 subnets

C 10.1.1.0 is directly connected, Ethernet0/2

-----

## R2

-----

R2#show ip route

～省略～

Gateway of last resort is not set

C 192.168.12.0/24 is directly connected, Ethernet0/0

C 192.168.23.0/24 is directly connected, Ethernet0/2

-----

## R3

-----

R3#show ip route

～省略～

Gateway of last resort is not set

10.0.0.0/24 is subnetted, 1 subnets

C 10.3.3.0 is directly connected, Ethernet0/2

C 192.168.23.0/24 is directly connected, Ethernet0/0

-----

ルーティングテーブルから **R1～R3** によって、以下の **4** つのネットワークが相互接続されていることがわかります。

ネットワークアドレス	接続しているルータ
<b>10.1.1.0/24</b>	<b>R1</b>
<b>192.168.12.0/24</b>	<b>R1/R2</b>
<b>192.168.23.0/24</b>	<b>R2/R3</b>
<b>10.3.3.0/24</b>	<b>R3</b>

ただ、IP アドレスを設定して直接接続のネットワークのルート情報だけしかルーティングテーブルになければ、すべてのネットワーク間でデータを転送できません。たとえば、PC1(10.1.1.100)から PC2(10.3.3.3)へ Ping を実行しても応答は返ってきません。

## PC1

```
PC1> ping 10.3.3.100
```

```
*10.1.1.1 icmp_seq=1 ttl=255 time=8.114 ms (ICMP type:3, code:1, Destination host unreachable)
*10.1.1.1 icmp_seq=2 ttl=255 time=8.081 ms (ICMP type:3, code:1, Destination host unreachable)
*10.1.1.1 icmp_seq=3 ttl=255 time=11.207 ms (ICMP type:3, code:1, Destination host unreachable)
*10.1.1.1 icmp_seq=4 ttl=255 time=4.270 ms (ICMP type:3, code:1, Destination host unreachable)
*10.1.1.1 icmp_seq=5 ttl=255 time=9.841 ms (ICMP type:3, code:1, Destination host unreachable)
```

PC1 から PC2 への Ping の ICMP エコーリクエストは R1 で破棄されます。R1 には 10.3.3.3 へ転送するためのルート情報がないからです。

R1 ルーティングテーブル

ネットワーク	ネクストホップ
10.1.1.0/24	Directly connected
192.168.12.0/24	Directly connected

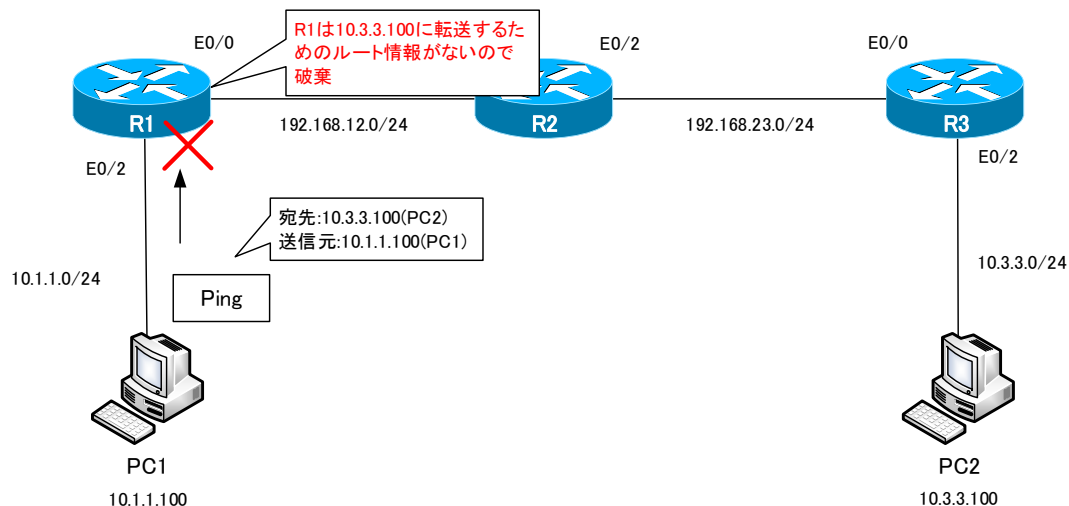


図 54 PC1 から PC2 への Ping その 1

## PC1-PC2 間の通信を行うためのスタティックルートの設定

### R1 に 10.3.3.0/24 のスタティックルートを設定

PC1-PC2 間で通信を行うためにスタティックルートの設定を行います。R1 で、以下のコマンドで 10.3.3.0/24 のルート情報を設定します。ネクストホップは R2、すなわち 192.168.12.2 です。

R1

-----

```
ip route 10.3.3.0 255.255.255.0 192.168.12.2
```

-----

10.3.3.0/24 のスタティックルートを設定すると、R1 のルーティングテーブルは以下のようになります。

R1

-----

```
R1#show ip route
```

～省略～

```
Gateway of last resort is not set
```

```
C    192.168.12.0/24 is directly connected, Ethernet0/0
```

```
    10.0.0.0/24 is subnetted, 2 subnets
```

```
S    10.3.3.0 [1/0] via 192.168.12.2
```

```
C    10.1.1.0 is directly connected, Ethernet0/2
```

-----

R1 にだけ 10.3.3.0/24 のスタティックルートを設定しても PC1 から PC2 の Ping の応答は返ってきません。

PC1

-----

```
PC1> ping 10.3.3.100
```

```
10.3.3.100 icmp_seq=1 timeout
```

```
10.3.3.100 icmp_seq=2 timeout
```

```
10.3.3.100 icmp_seq=3 timeout
```

```
10.3.3.100 icmp_seq=4 timeout
```

```
10.3.3.100 icmp_seq=5 timeout
```

-----

R1 は PC1 から PC2 への Ping を R2 に転送しています。でも、R2 に宛先 IP アドレス 10.3.3.100 に一致するルート情報がないので、R2 で PC1 から PC2 への Ping パケットが破棄されています。

R1 ルーティングテーブル

ネットワーク	ネクストホップ
10.1.1.0/24	Directly connected
192.168.12.0/24	Directly connected
10.3.3.0/24	192.168.12.2(R2)

R2 ルーティングテーブル

ネットワーク	ネクストホップ
192.168.12.0/24	Directly connected
192.168.23.0/24	Directly connected

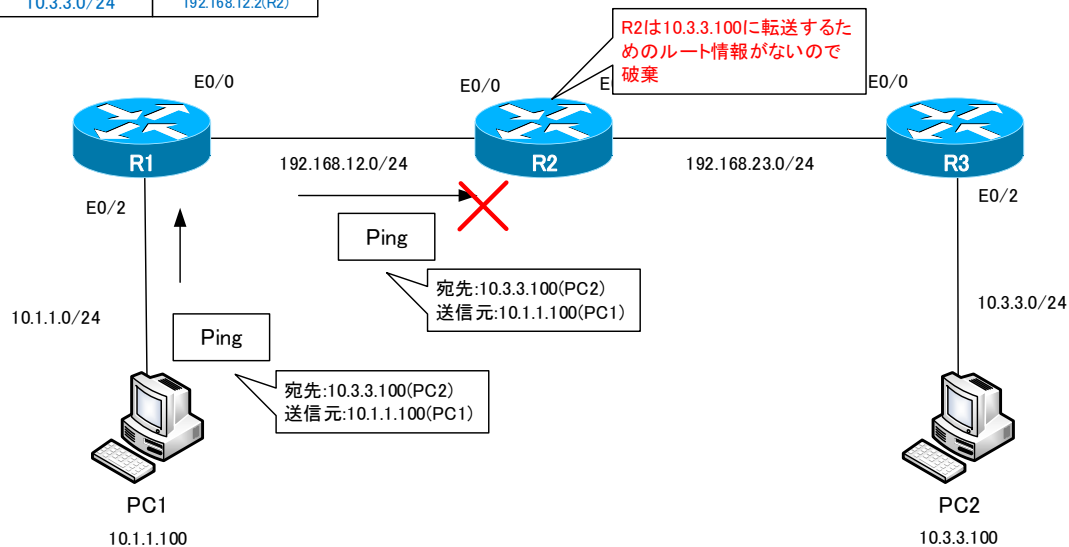


図 55 PC1 から PC2 への Ping その 2

### R2 に 10.3.3.0/24 のスタティックルートを設定

R1 だけでなく R2 にも 10.3.3.0/24 のスタティックルートを設定しなければいけません。R2 ではネクストホップは R3、すなわち 192.168.23.3 です。

R2

```
-----  
ip route 10.3.3.0 255.255.255.0 192.168.23.3  
-----
```

R2 でルーティングテーブルを確認すると、10.3.3.0/24 のスタティックルートが追加されます。

R2

```
-----  
R2#show ip route
```

～省略～

Gateway of last resort is not set



```
C 192.168.12.0/24 is directly connected, Ethernet0/0
  10.0.0.0/24 is subnetted, 1 subnets
S 10.3.3.0 [1/0] via 192.168.23.3
C 192.168.23.0/24 is directly connected, Ethernet0/2
```

R2 に 10.3.3.0/24 のスタティックルートを設定しても、PC1 から PC2 への Ping は成功しません。

PC1

```
PC1> ping 10.3.3.100
10.3.3.100 icmp_seq=1 timeout
10.3.3.100 icmp_seq=2 timeout
10.3.3.100 icmp_seq=3 timeout
10.3.3.100 icmp_seq=4 timeout
10.3.3.100 icmp_seq=5 timeout
```

R1 と R2 に 10.3.3.0/24 のスタティックルートを設定すると、PC1 から PC2 への Ping を実行した ICMP エコーリクエストは PC2 まで届いています。

R1 ルーティングテーブル

ネットワーク	ネクストホップ
10.1.1.0/24	Directly connected
192.168.12.0/24	Directly connected
10.3.3.0/24	192.168.12.2(R2)

R2 ルーティングテーブル

ネットワーク	ネクストホップ
192.168.12.0/24	Directly connected
192.168.23.0/24	Directly connected
10.3.3.0/24	192.168.23.3(R3)

R3 ルーティングテーブル

ネットワーク	ネクストホップ
10.3.3.0/24	Directly connected
192.168.23.0/24	Directly connected

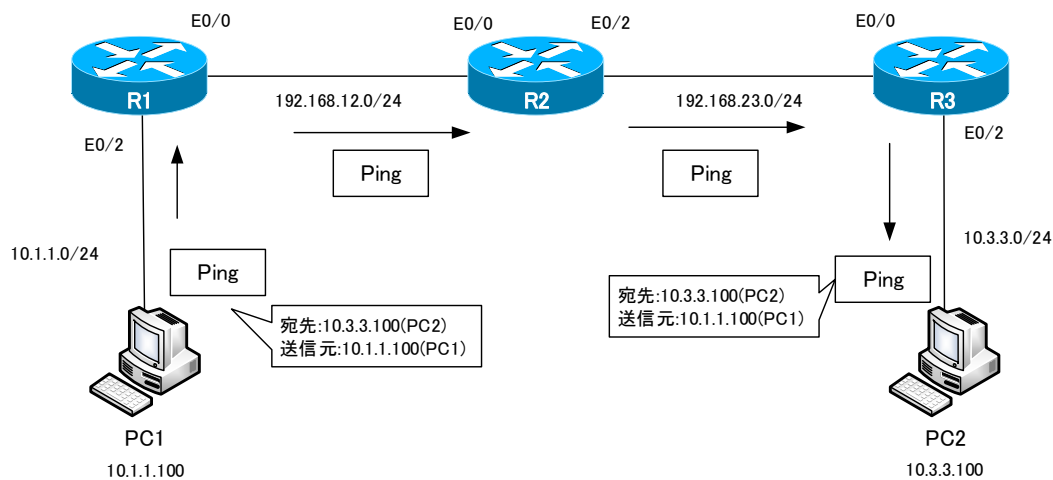


図 56 PC1 から PC2 への Ping その 3

基礎からの CCNA(200-301)攻略テキスト  
第 10 章 IP ルーティング

ここで忘れてはいけないことが、「通信は双方向」ということです。PC1 から PC2 へ Ping して ICMP エコーリクエストが PC2 まで届くと、その返事として ICMP エコーリプライを返します。ICMP エコーリプライは、ICMP エコーリクエストの宛先 IP アドレスと送信元 IP アドレスが入れ替わったものになります。宛先は 10.1.1.100(PC1)で送信元は 10.3.3.100(PC2)です。R3 には、宛先 10.1.1.100 に一致するルート情報が無いので破棄します。

R1 ルーティングテーブル

ネットワーク	ネクストホップ
10.1.1.0/24	Directly connected
192.168.12.0/24	Directly connected
10.3.3.0/24	192.168.12.2(R2)

R2 ルーティングテーブル

ネットワーク	ネクストホップ
192.168.12.0/24	Directly connected
192.168.23.0/24	Directly connected
10.3.3.0/24	192.168.23.3(R3)

R3 ルーティングテーブル

ネットワーク	ネクストホップ
10.3.3.0/24	Directly connected
192.168.23.0/24	Directly connected

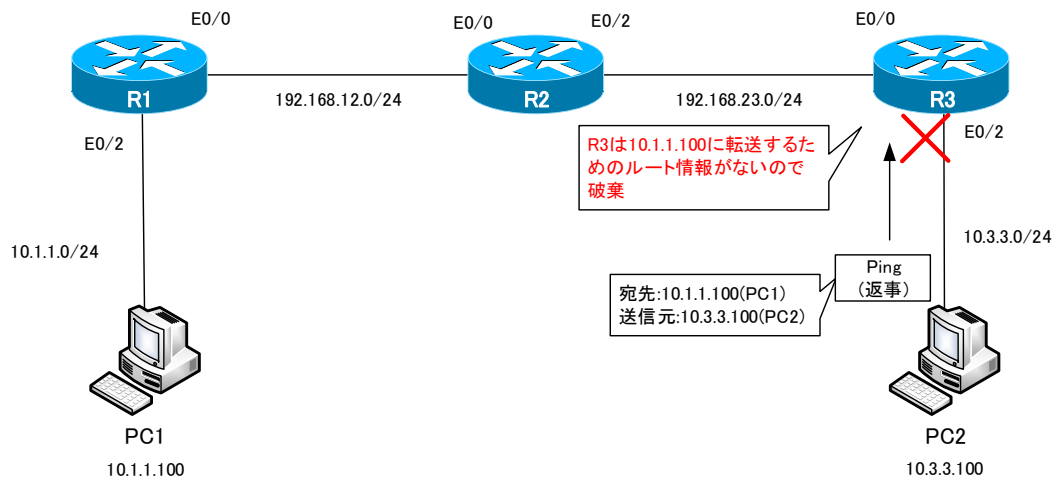


図 57 PC1 から PC2 への Ping その 4

### R3 に 10.1.1.0/24 のスタティックルートを設定

PC2 から PC1 へ Ping の返事を返せるようにするためには、R3 に宛先 10.1.1.100 に一致するルート情報として 10.1.1.0/24 のスタティックルートを設定します。

R3

```
-----  
ip route 10.1.1.0 255.255.255.0 192.168.23.2  
-----
```

この設定により、R3 のルーティングテーブルには、次のように 10.1.1.0/24 のスタティックルートが登録されます。

R3

```
-----
```

```
R3#show ip route
```

～省略～

```
Gateway of last resort is not set
```

```
10.0.0.0/24 is subnetted, 2 subnets
C    10.3.3.0 is directly connected, Ethernet0/2
S    10.1.1.0 [1/0] via 192.168.23.2
C    192.168.23.0/24 is directly connected, Ethernet0/0
-----
```

しかし、**PC1** から **PC2** への **Ping** はまだ成功しません。

**PC1**

```
-----
PC1> ping 10.3.3.100
10.3.3.100 icmp_seq=1 timeout
10.3.3.100 icmp_seq=2 timeout
10.3.3.100 icmp_seq=3 timeout
10.3.3.100 icmp_seq=4 timeout
10.3.3.100 icmp_seq=5 timeout
-----
```

**PC1** から **PC2** へ **Ping** を実行すると、**ICMP** エコーリクエストは **PC2** まで転送されています。そして、**PC2** から **PC1** へ返事として **ICMP** エコーリプライを送っています。エコーリプライは **R3** から **R2** へ転送されているのですが、**R2** には宛先 **10.1.1.100** に一致するルート情報がありません。**ICMP** エコーリプライを **R2** が破棄してしまうので、**Ping** は成功しません。

R1 ルーティングテーブル

ネットワーク	ネクストホップ
10.1.1.0/24	Directly connected
192.168.12.0/24	Directly connected
10.3.3.0/24	192.168.12.2(R2)

R2 ルーティングテーブル

ネットワーク	ネクストホップ
192.168.12.0/24	Directly connected
192.168.23.0/24	Directly connected
10.3.3.0/24	192.168.23.3(R3)

R3 ルーティングテーブル

ネットワーク	ネクストホップ
10.3.3.0/24	Directly connected
192.168.23.0/24	Directly connected
10.1.1.0/24	192.168.23.2(R2)

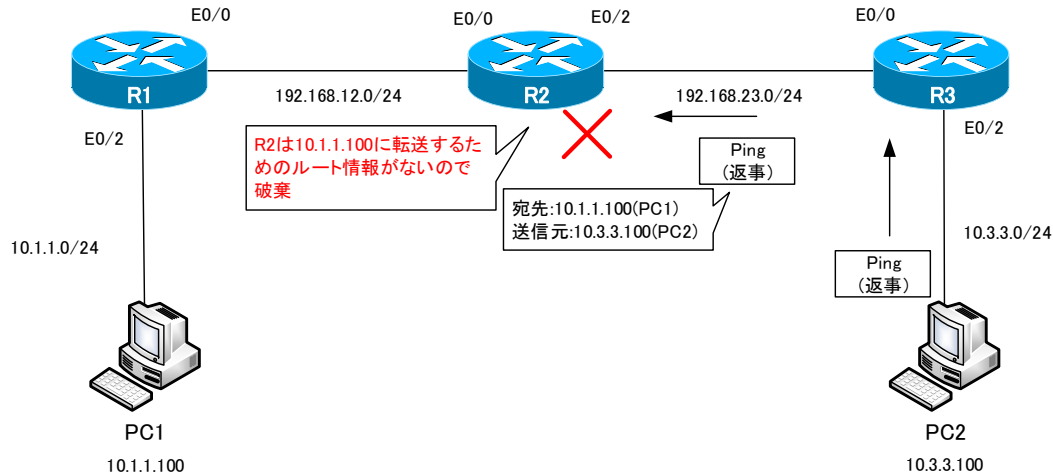


図 58 PC1 から PC2 への Ping その 5

### R2 に 10.1.1.0/24 のスタティックルートを設定

PC1 から PC2 への Ping の ICMP エコーリクエストに対する返事の ICMP エコーリプライを返せるように R2 に 10.1.1.0/24 についてのスタティックルートを設定します。

R2

```
ip route 10.1.1.0 255.255.255.0 192.168.12.1
```

R2 のルーティングテーブルには、以下のように 10.1.1.0/24 のスタティックルートが登録されます。

R2

```
R2#show ip route
```

～省略～

```
Gateway of last resort is not set
```

```
C 192.168.12.0/24 is directly connected, Ethernet0/0
```

```
10.0.0.0/24 is subnetted, 2 subnets
```

```
S 10.3.3.0 [1/0] via 192.168.23.3
```

```
S 10.1.1.0 [1/0] via 192.168.12.1
C 192.168.23.0/24 is directly connected, Ethernet0/2
-----
```

これでようやく PC1 から PC2 への Ping が成功します。

## PC1

```
PC1> ping 10.3.3.100
84 bytes from 10.3.3.100 icmp_seq=1 ttl=61 time=55.660 ms
84 bytes from 10.3.3.100 icmp_seq=2 ttl=61 time=63.150 ms
84 bytes from 10.3.3.100 icmp_seq=3 ttl=61 time=66.075 ms
84 bytes from 10.3.3.100 icmp_seq=4 ttl=61 time=57.319 ms
84 bytes from 10.3.3.100 icmp_seq=5 ttl=61 time=61.142 ms
-----
```

R1 ルーティングテーブル

ネットワーク	ネクストホップ
10.1.1.0/24	Directly connected
192.168.12.0/24	Directly connected
10.3.3.0/24	192.168.12.2(R2)

R2 ルーティングテーブル

ネットワーク	ネクストホップ
192.168.12.0/24	Directly connected
192.168.23.0/24	Directly connected
10.3.3.0/24	192.168.23.3(R3)
10.1.1.0/24	192.168.12.1(R1)

R3 ルーティングテーブル

ネットワーク	ネクストホップ
10.3.3.0/24	Directly connected
192.168.23.0/24	Directly connected
10.1.1.0/24	192.168.23.2(R2)

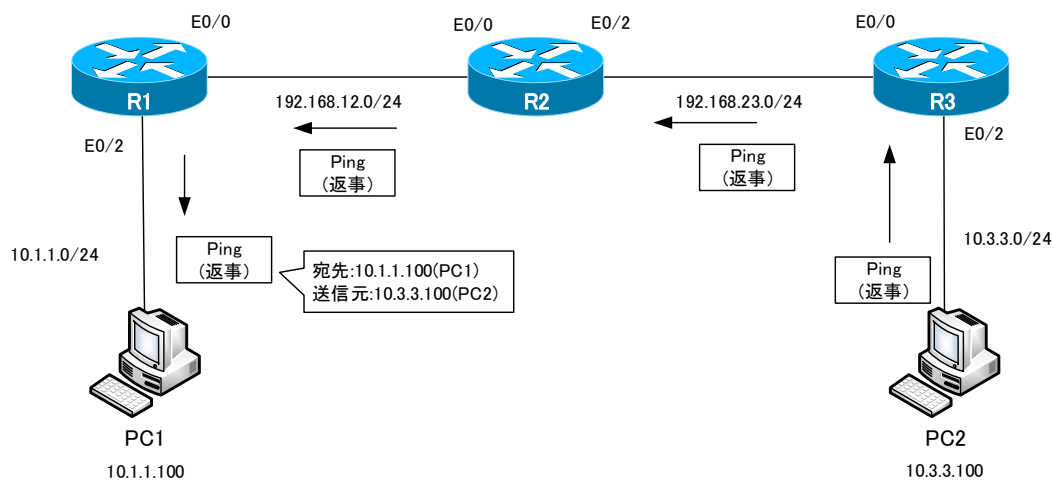


図 59 PC1 から PC2 への Ping その 6

## RI-R3 間の通信を行うためのスタティックルートの設定

### RI から R3 に Ping できない・・・

ここまでのスタティックルートの設定によって PC1-PC2 間は通信できるのですが、RI から R3 に Ping を実行すると失敗します。

RI

-----

R1#ping 192.168.23.3

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.23.3, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

-----

PC1-PC2 間は Ping の応答がきちんと返ってくるようになったのに、その経路上にある RI-R3 間で Ping の応答が返ってきません。「それは当然」とすんなりと思える方は、ルーティングの大原則がしっかりと頭に入っています。RI から R3 の 192.168.23.3 へ Ping を実行すると、宛先/送信元 IP アドレスは以下のようになっています。

宛先 IP アドレス : 192.168.23.3

送信元 IP アドレス : 192.168.12.2

RI のルーティングテーブルに宛先 IP アドレス 192.168.23.3 に一致するルート情報が存在しないので、Ping の ICMP エコーリクエストを送信できません。

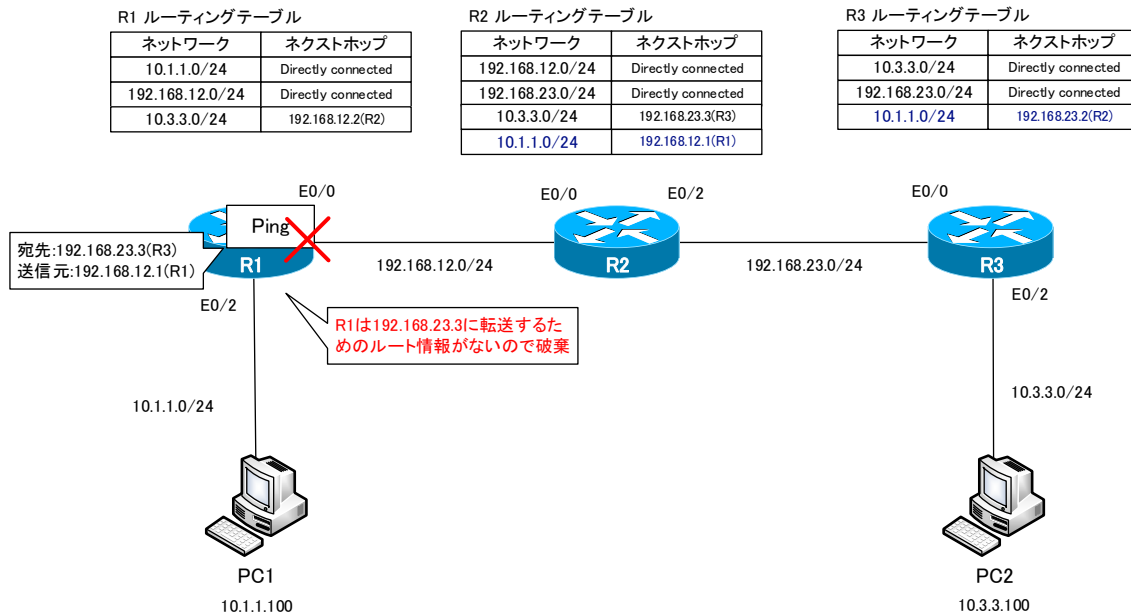


図 60 R1 から R3 への Ping その 1

### R1 に 192.168.23.0/24 のスタティックルートを設定

R1 から R3(192.168.23.3)への Ping の ICMP エコーリクエストを送信するためには、R1 のルーティングテーブルに 192.168.23.0/24 のルート情報を登録します。

R1

```

-----
ip route 192.168.23.0 255.255.255.0 192.168.12.2
-----

```

この設定により、R1 のルーティングテーブルには、192.168.23.0/24 のスタティックルートが登録されます。

R1

```

-----
R1#show ip route
~省略~

```

Gateway of last resort is not set

```

C    192.168.12.0/24 is directly connected, Ethernet0/0
      10.0.0.0/24 is subnetted, 2 subnets
S    10.3.3.0 [1/0] via 192.168.12.2
C    10.1.1.0 is directly connected, Ethernet0/2

```

```
S 192.168.23.0/24 [1/0] via 192.168.12.2
```

R1 に 192.168.23.0/24 のスタティックルートを設定するだけでは、R1 から R3 への Ping はまだ失敗します。

R1

```
R1#ping 192.168.23.3
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.23.3, timeout is 2 seconds:
```

```
.....
```

```
Success rate is 0 percent (0/5)
```

R1 に 192.168.23.0/24 のスタティックルートを設定することで、R1 から R3 への Ping の ICMP エコーリクエストは転送されるようになっています。

R1 ルーティングテーブル

ネットワーク	ネクストホップ
10.1.1.0/24	Directly connected
192.168.12.0/24	Directly connected
10.3.3.0/24	192.168.12.2(R2)
192.168.23.0/24	192.168.12.2(R2)

R2 ルーティングテーブル

ネットワーク	ネクストホップ
192.168.12.0/24	Directly connected
192.168.23.0/24	Directly connected
10.3.3.0/24	192.168.23.3(R3)
10.1.1.0/24	192.168.12.1(R1)

R3 ルーティングテーブル

ネットワーク	ネクストホップ
10.3.3.0/24	Directly connected
192.168.23.0/24	Directly connected
10.1.1.0/24	192.168.23.2(R2)

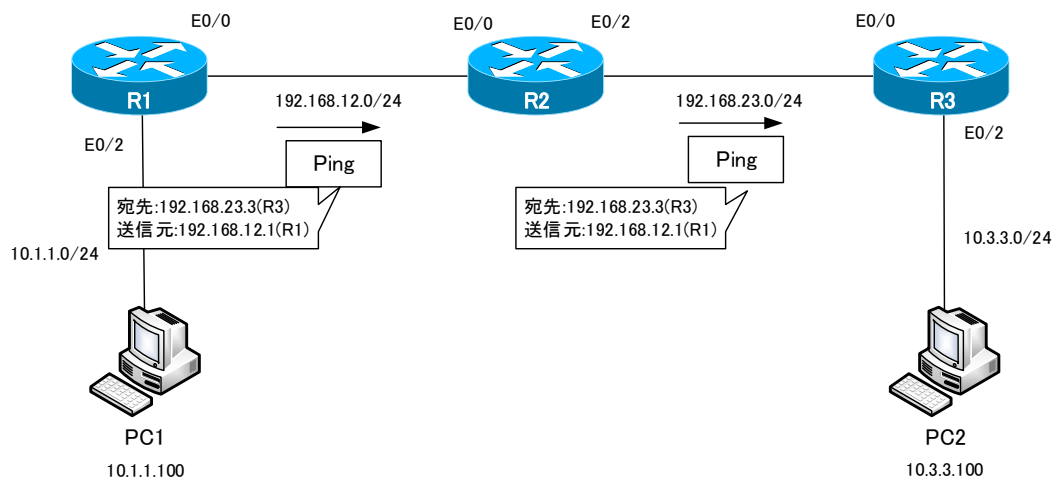


図 61 R1 から R3 への Ping その 2

やはり、忘れてはいけないことが、「通信は双方向」ということです。**R3** から **R1** へ Ping の返事の ICMP エコーリプライを返します。その宛先/送信元 IP アドレスは次のようになります。



基礎からの CCNA(200-301)攻略テキスト  
第 10 章 IP ルーティング

宛先 IP アドレス : 192.168.12.1

送信元 IP アドレス : 192.168.23.3

R3 のルーティングテーブルには 192.168.12.1 宛ての IP パケットを転送するためのルート情報がないために破棄します。

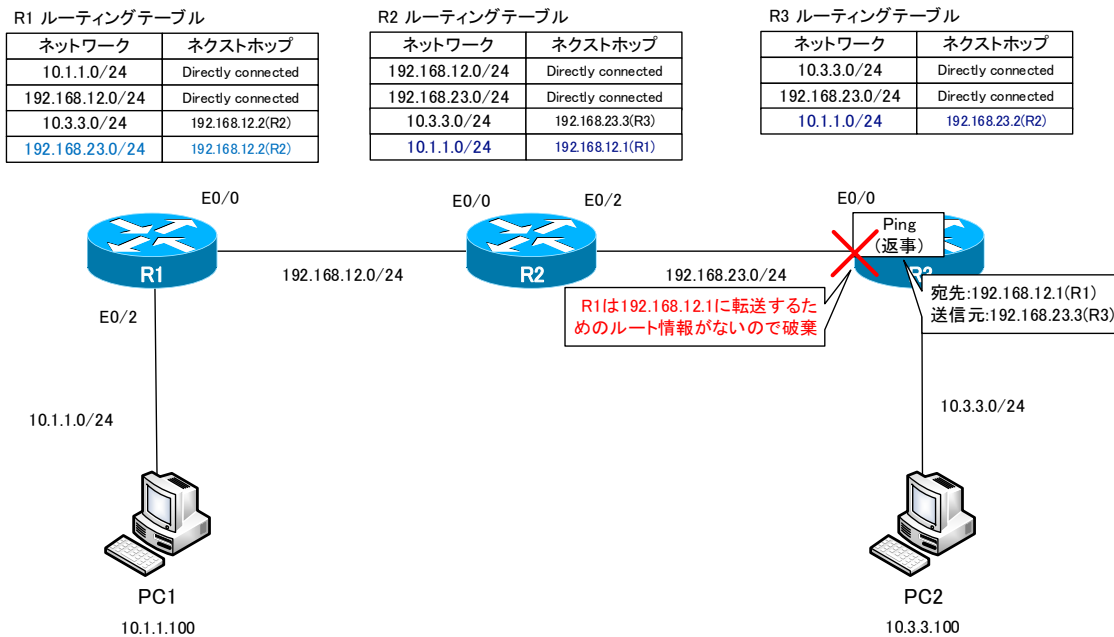


図 62 R1 から R3 への Ping その 3

### R3 に 192.168.12.0/24 のスタティックルートを設定

R1 から R3 の Ping の返事を返せるように、R3 に 192.168.12.0/24 のスタティックルートを設定します。

R3

```
-----  
ip route 192.168.12.0 255.255.255.0 192.168.23.2  
-----
```

R3 のルーティングテーブルを確認すると、以下のようになります。

R3

```
-----  
R3#show ip route  
～省略～
```

Gateway of last resort is not set

```
S 192.168.12.0/24 [1/0] via 192.168.23.2
    10.0.0.0/24 is subnetted, 2 subnets
C    10.3.3.0 is directly connected, Ethernet0/2
S    10.1.1.0 [1/0] via 192.168.23.2
C    192.168.23.0/24 is directly connected, Ethernet0/0
-----
```

これでようやく R1 から R3 への Ping が成功するようになります。

R1

R1#ping 192.168.23.3

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.23.3, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 60/67/92 ms

R1 ルーティングテーブル

ネットワーク	ネクストホップ
10.1.1.0/24	Directly connected
192.168.12.0/24	Directly connected
10.3.3.0/24	192.168.12.2(R2)
192.168.23.0/24	192.168.12.2(R2)

R2 ルーティングテーブル

ネットワーク	ネクストホップ
192.168.12.0/24	Directly connected
192.168.23.0/24	Directly connected
10.3.3.0/24	192.168.23.3(R3)
10.1.1.0/24	192.168.12.1(R1)

R3 ルーティングテーブル

ネットワーク	ネクストホップ
10.3.3.0/24	Directly connected
192.168.23.0/24	Directly connected
10.1.1.0/24	192.168.23.2(R2)
192.168.12.0/24	192.168.23.2(R2)

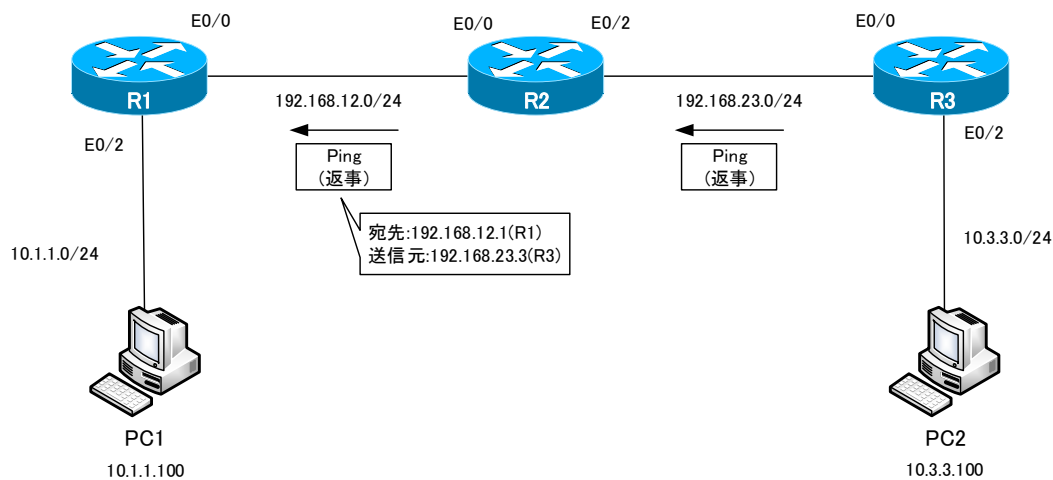


図 63 R1 から R3 への Ping その 4

## 最終的なルーティングテーブル

R1～R3 の最終的なルーティングテーブルは以下のようになります。

### R1

-----

R1#show ip route

～省略～

Gateway of last resort is not set

C 192.168.12.0/24 is directly connected, Ethernet0/0

10.0.0.0/24 is subnetted, 2 subnets

S 10.3.3.0 [1/0] via 192.168.12.2

C 10.1.1.0 is directly connected, Ethernet0/2

S 192.168.23.0/24 [1/0] via 192.168.12.2

-----

### R2

-----

R2#show ip route

～省略～

Gateway of last resort is not set

C 192.168.12.0/24 is directly connected, Ethernet0/0

10.0.0.0/24 is subnetted, 2 subnets

S 10.3.3.0 [1/0] via 192.168.23.3

S 10.1.1.0 [1/0] via 192.168.12.1

C 192.168.23.0/24 is directly connected, Ethernet0/2

-----

### R3

-----

R3#show ip route

～省略～

Gateway of last resort is not set

```
S 192.168.12.0/24 [1/0] via 192.168.23.2
    10.0.0.0/24 is subnetted, 2 subnets
C    10.3.3.0 is directly connected, Ethernet0/2
S    10.1.1.0 [1/0] via 192.168.23.2
C    192.168.23.0/24 is directly connected, Ethernet0/0
-----
```

R1～R3 のルーティングテーブルに以下の 4 つのネットワークのルート情報がすべて登録されている状態になってはじめて、これら 4 つのネットワーク間の通信ができるようになります。

- ・ 10.1.1.0/24
- ・ 10.3.3.0/24
- ・ 192.168.12.0/24
- ・ 192.168.23.0/24

実際にスタティックルートの設定を行うときには、1 つずつ登録する必要はもちろんありません。ただ、ネットワークの規模が大きくなってきて、ルータや相互接続しているネットワークの数が増えてくると、設定すべきスタティックルートの数が増えすぎていってしまうことになります。

## 転送経路を決定する方法

### ポイント

- 宛先ネットワークまでの転送経路を明確にしておくことは、ネットワークを管理するうえでとても重要です。
- 宛先ネットワークまでの転送経路が複数ある場合、2 つの方法で転送経路を決められます。
  - ルート情報の距離を近くする
  - ルート情報を詳しく登録する

### 宛先ネットワークまでの転送経路をきちんと把握しよう

ルーティングテーブルは、宛先ネットワークまでの最適なルート情報が登録されています。宛先ネットワークまでのパケットの転送経路は、ルーティングテーブルでわかります。宛先ネットワークまでの転送経路が複数存在する場合、どの経路でパケットが転送されるかをしっかりと把握しておくことが重要です。たとえば、転送経路がよくわかっていないと、何か問題が発生したときに原因の切り分けに時間を要することになります。

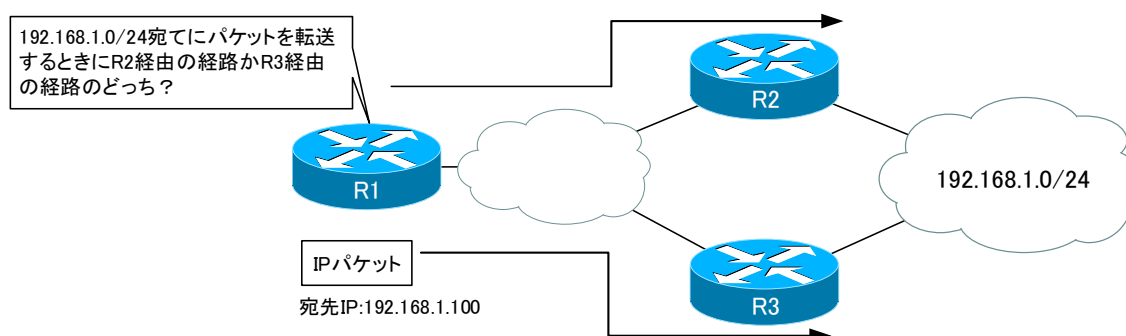


図 64 転送経路が複数ある場合

※ 1 台のルータだけのルーティングテーブルでは、宛先ネットワークまでの完全なパケットの転送経路はわかりません。経路上のルータそれぞれのルーティングテーブルを見ていく必要があります。

### 転送経路の決め方の方法

宛先ネットワークまでパケットを転送するときにどの経路を利用するかを決めるために、次の 2 つの方法があります。

- ルート情報の距離を近くする  
利用したい経路のルート情報の距離を近くして、最適ルートとしてルーティングテーブルに登録されるようにする

- ・ ルート情報を詳しく登録する

利用したい経路のルート情報を詳しくルーティングテーブルに登録してパケットを転送するときに優先して利用されるようにする

## ルート情報の距離を近くする

ルーティングテーブルには最適なルート情報のみが登録されます。最適なルート情報であるかは、距離に基づいて決めています。Cisco では、ルート情報の距離は[アドミニストレイティブディスタンス/メトリック]で表しています。

利用したい転送経路のルート情報の距離が近くなるようにして、最適ルートとしてルーティングテーブルに登録されるようにします。そのためには、利用したい転送経路のルート情報のアドミニストレイティブディスタンスやメトリックを小さくすれば OK です。あるいは、利用したくないルート情報のアドミニストレイティブディスタンスやメトリックを大きくします。どちらの設定を行うかは好みで決めるとよいでしょう。

RIP を利用している簡単な例を考えます。R1 から 192.168.1.0/24 宛ての IP パケットの転送経路を R2 経由にするとします。R2 と R3 は RIP で 192.168.1.0/24 のルート情報を R1 へアドバタイズします。このとき、R3 からアドバタイズするルート情報のメトリックを大きくします。すると、R2 からアドバタイズされたルート情報が最適ルートとなり、ルーティングテーブルに登録されます。RIP のルート情報のメトリックを大きくするにはオフセットリストの設定を行います。

そして、宛先 IP アドレスが 192.168.1.100 の IP パケットが R1 へやってくると、R1 は R2 へと転送することになります。

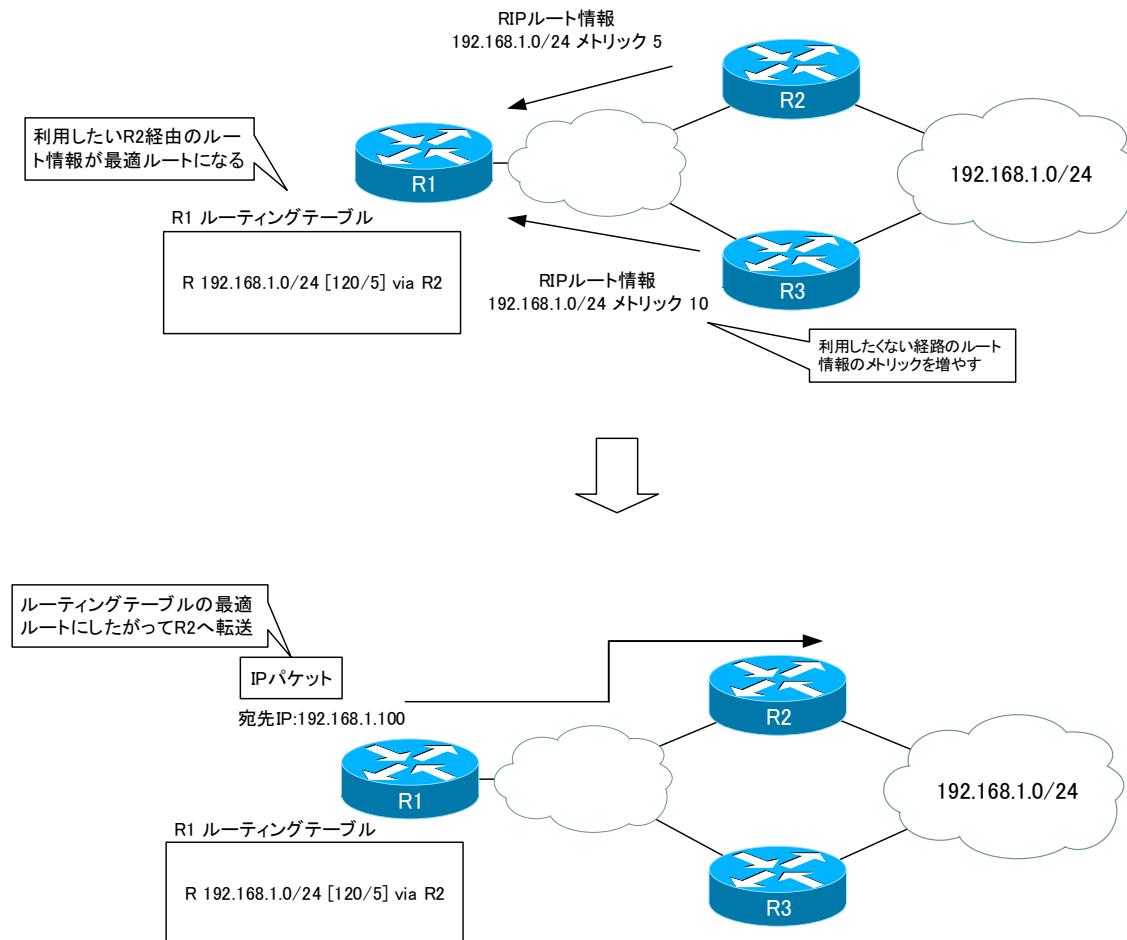


図 65 ルート情報の距離を近くする例(RIP)

- ※ アドミニストレイティブディスタンスは **Cisco** 独自のパラメータです。他のベンダでも同様のパラメータがあります。
- ※ スタティックルートでこのような制御をしたいときには、アドミニストレイティブディスタンスを変更します。
- ※ メトリックはルート情報に付随して他のルータへとアドバタイズされていきますが、アドミニストレイティブディスタンスはルータローカルのパラメータです。メトリックを変更すれば、他のルータの最適ルートの決定にも影響することがあります。一方、アドミニストレイティブディスタンスの変更はそのルータのみの最適ルート決定に影響します。

## ルート情報を詳しく登録する

IP パケットをルーティングするとき、宛先 IP アドレスに一致するルーティングテーブル上のルート情報を検索します。このとき、最長一致検索で一致するルート情報を検索します。一致するルート情報はひとつだけでなく、複数存在することもあります。その場合は、よりサブネットマスクが長いルート情報を優先してパケットの転送先を判断します。サブネットマスクが長いルート情報は、詳細なルート情報です。

そこで、**利用したい経路のルート情報をより詳細にルーティングテーブルに登録すれば、その経路を優先して利用することになります。**あるいは、利用したくない経路のルート情報は集約しても OK です。

先ほどと同様に RIP を利用している簡単な例で考えます。R1 から 192.168.1.0/24 へ IP パケットをルーティングするとき R2 経由にするとします。利用したくない経路である R3 から RIP のルート情報をアドバタイズするときに 192.168.0.0/16 に集約します。R1 のルーティングテーブルには、R2 経由の 192.168.1.0/24 のルート情報と R3 経由の 192.168.0.0/16 のルート情報が両方とも登録されます。

そして、宛先 IP アドレス 192.168.1.100 の IP パケットが R1 にやってくると、最長一致検索により 192.168.1.0/24 のルート情報にも 192.168.0.0/16 のルート情報にも一致します。サブネットマスクがより長い 192.168.1.0/24 のルート情報に基づいて、パケットは R2 へ転送されることになります。

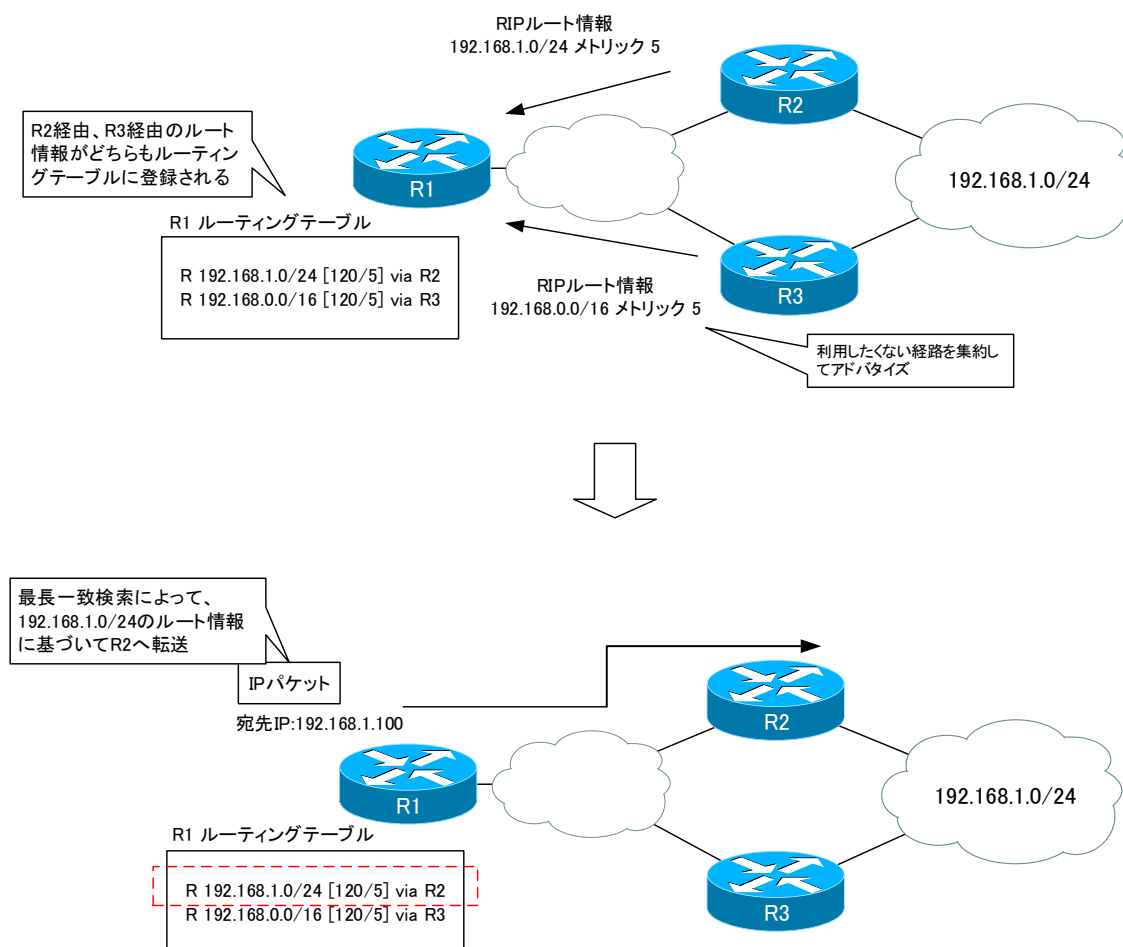


図 66 ルート情報を詳しく登録する例(RIP)



以上のように転送経路を決める方法が 2 通りあります。どちらを利用しても最終的に同じことを実現できます。それぞれの方法で、転送経路を決める仕組みが違います。この 2 つの方法で IP パケットが転送される経路が決まるプロセスをしっかりと理解することで、より深くルーティングの仕組みを理解できるようになるでしょう。

## CEF の概要

### ポイント

- ・ 主なパケットの転送方式には、次の 3 通りあります。
  - プロセススイッチング
  - ファストスイッチング
  - CEF
- ・ CEF はデータプレーンのみで高速なパケットの転送を行います。
- ・ CEF でパケットを転送するためには、次の 2 つのテーブルを利用します。
  - FIB テーブル
  - 隣接テーブル

### パケットの転送方式

パケットを転送する主な方式として以下の 3 つが挙げられます。

- ・ プロセススイッチング
- ・ ファストスイッチング
- ・ CEF(Cisco Express Forwarding)

プロセススイッチングがパケットの転送性能が最も低く、CEF が最も高速なパケットの転送処理が可能です。

### パケットの転送を制御するハードウェア構造

パケットの転送方式を理解するうえで、ルータやレイヤ 2/レイヤ 3 スイッチの内部のハードウェア構造を知っておく必要があります。以下の 4 つから構成されています。

- ・ コントロールプレーン  
汎用 CPU とメモリ、IOS で構成されてネットワーク機器全体を制御しています。また、パケットを転送するためのルーティングテーブルなどの情報を管理しています。
- ・ データプレーン  
ASIC と TCAM によって構成され、パケット転送処理を行っています。
- ・ バックプレーン  
ネットワーク機器内部でパケットを転送するための仕組みです。スイッチングファブリックとも呼ばれます。
- ・ インタフェース

伝送媒体を接続してネットワークに接続します。最もよく利用されているインタフェースはイーサネットインタフェースです。

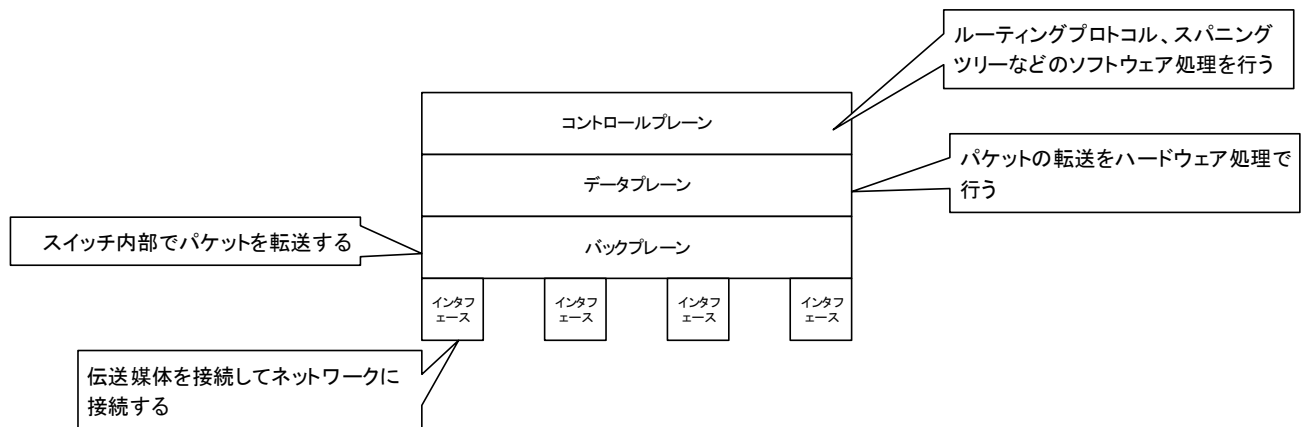


図 67 ハードウェア構造

パケットの転送方式の違いは、パケットを転送する際にコントロールプレーンとデータプレーンでどのように処理されるかの違いです。プロセススイッチングは、パケットを転送する際にコントロールプレーンとデータプレーンでひとつずつ処理されます。ファストスイッチングはフローの最初のパケットのみコントロールプレーンとデータプレーンで処理されます。フローの 2 番目以降はデータプレーンのみで転送処理を行います。そして、CEF はパケットの転送をデータプレーンのみで行います。

## プロセススイッチングとファストスイッチングによるパケット転送

プロセススイッチングは最も初期のパケット転送方式です。パケットをひとつひとつコントロールプレーンで転送先を判断して、データプレーンで転送処理を行います。コントロールプレーンの処理は、CPU プロセスを消費し、時間あたりにパケットを処理することができる数も少なくなるため、あまり高速な転送を行うことができません。

ファストスイッチングは、プロセススイッチよりも高速にパケットを転送するために開発された転送方式です。ネットワーク上を流れるパケットは、「フロー」を形成することに注目します。フローとは、同じアドレス情報を持つ一連のパケットを意味します。たとえば、HTTP や FTP などのプロトコルでファイル転送を行うとき、連続して複数のパケットが送信されます。これらの複数のパケットは同じアドレス情報を持っています。同じアドレス情報を持っているので、フローを形成するパケットをルーティングするとどれも同じ結果になります。

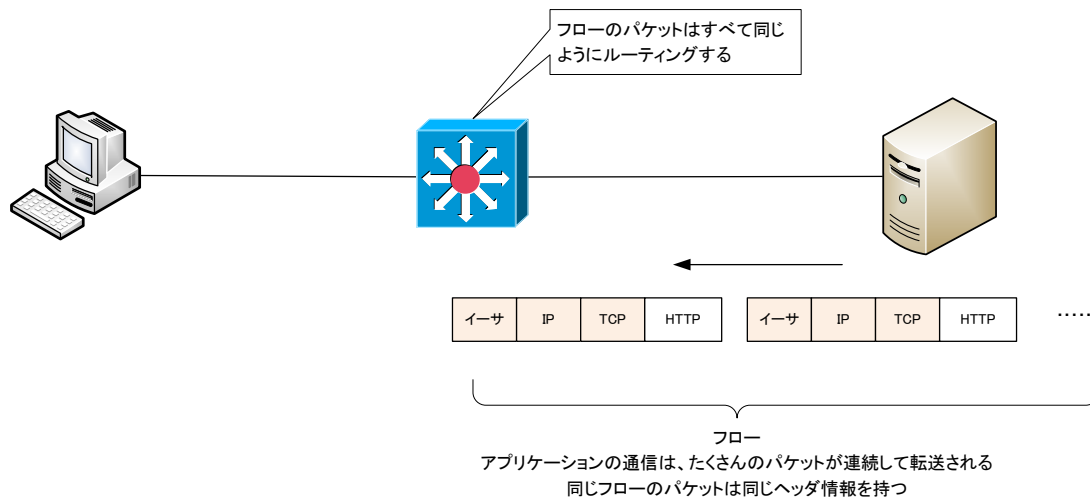


図 68 フローの例

そこで、ファストスイッチングでは、**フローの先頭のパケットをプロセススイッチングによって処理し、その結果をキャッシュします。2 番目以降のパケットは、キャッシュを参照し、データプレーンでの高速なパケット転送を行います。**ファストスイッチングはトラフィックドリブン型の転送方式と呼ばれることもあります。フローの発生(トラフィック)が引き金となって(ドリブン)キャッシュが作成されることから、こういう呼び方があります。

ただし、現在のネットワークでは非常に多くのフローが発生します。キャッシュの容量は有限なので、たくさんのフローが発生すると、キャッシュの書き換えが頻発し、プロセススイッチングされるパケットが多くなります。その結果、パケット転送のパフォーマンスが低下します。

## CEF によるパケット転送

CEF では、次の 2 つのテーブルを利用してパケットの転送を行います。

- ・ FIB(Forwarding Information Base)テーブル
- ・ 隣接テーブル

**CEF では、あらかじめコントロールプレーンのルーティングテーブルからデータプレーン上に FIB(Forwarding Information Base)テーブルを作成し、ARP テーブルから隣接テーブルを作成します。**データを転送する際、FIB テーブルでパケットの転送先を判断し、隣接テーブルでレイヤ 2 ヘッダの書き換えを行います。CEF はトポロジベーススイッチングとも呼ばれ、パケットの転送をデータプレーンのみで完結させて、非常に高速にパケットを転送することができます。

FIB テーブルには、ルーティングテーブルのネットワークアドレスのエントリはすべて含まれています。そのため、送信先 IP アドレスが FIB テーブルのエントリに一致しないパケットは破棄されます。ネットワークのトポロジを表しているルーティングテーブルからあらかじめ FIB テーブルを作成してパケットを転送することからトポロジドリブン型の転送方式とも呼ばれます。CEF では、フローが多発してもキャッシュの書

き換えは発生しないので、パケット転送のパフォーマンス低下はありません。

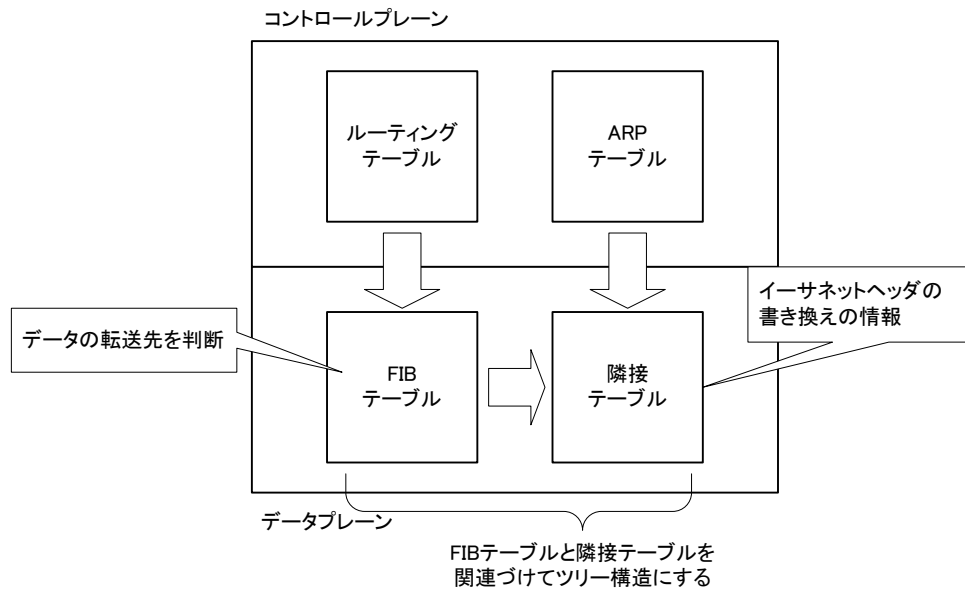


図 69 CEF のテーブル

なお、次のようなパケットはデータプレーンのみではなく、コントロールプレーンで処理されることになります。

- ・ トンネルインタフェースから転送される、もしくはトンネルインタフェースに転送されるパケット
- ・ 分割する必要があるパケット
- ・ IP ヘッダのオプションが付加されているパケット
- ・ **ARPA** 以外のイーサネットカプセル化のパケット

## まとめ

- ・ ルータはネットワークを相互接続し、ネットワーク間のデータの転送を行います。
- ・ ルータがデータを転送するには、**IP** パケットの宛先 **IP** アドレスとルーティングテーブルを参照します。
- ・ ルータがルーティングするにしたがって、レイヤ **2** ヘッダは書き換わっていきます。
- ・ ルーティングするときのレイヤ **2** ヘッダの書き換えの仕組みは **CCNA** 試験でとても重要です。
- ・ ルータがルーティングするための大前提は、ルーティングテーブルにデータを転送したい宛先ネットワークのルート情報が登録されていることです。
- ・ ルーティングテーブルに登録されていない未知のネットワーク宛てのデータは破棄します。
- ・ ルーティングプロトコルは、適用範囲、アルゴリズム、ネットワークアドレスの認識によって分類できます。
- ・ スタティックルートの設定を行うにあたって、それぞれのルータにとってのリモートネットワークを明確にしておくことが重要です。
- ・ リモートネットワークのルート情報を **ip route** コマンドによってルーティングテーブルに登録します。
- ・ 宛先ネットワークまでの転送経路を明確にしておくことは、ネットワークを管理するうえでとても重要です。
- ・ 宛先ネットワークまでの転送経路が複数ある場合、**2** つの方法で転送経路を決められます。
  - ルート情報の距離を近くする
  - ルート情報を詳しく登録する
- ・ 主なパケットの転送方式には、次の **3** 通りあります。
  - プロセススイッチング
  - ファストスイッチング
  - **CEF**
- ・ **CEF** はデータプレーンのみで高速なパケットの転送を行います。
- ・ **CEF** でパケットを転送するためには、次の **2** つのテーブルを利用します。
  - **FIB** テーブル
  - 隣接テーブル