FITELnet F310

機能説明書

古河電工

はじめに

このたびは、本装置をお買い上げいただき、まことにありがとうございます。
インターネットやLANをさらに活用するために、本装置をご利用ください。

目次

本書の使いかた

本書では、困ったときの原因・対処方法やご購入時の状態に戻す方法について説明しています。

本書の読者と前提知識

本書は、ネットワーク管理を行っている方を対象に記述しています。

本書を利用するにあたって、ネットワークおよびインターネットに関する基本的な知識が必要です。

ネットワーク設定を初めて行う方でも本書「機能説明書」に分かりやすく記載していますので、安心してお読みいただけます。

マークについて

本書で使用しているマーク類は、以下のような内容を表しています。

ヒント	本装置をお使いになる際に、役に立つ知識をコラム形式で説明しています。
こんな事に気をつけて	本装置をご使用になる際に、注意していただきたいことを説明しています。
補足	操作手順で説明しているもののほかに、補足情報を説明しています。
参照	操作方法など関連事項を説明している箇所を示します。
⚠警告	製造物責任法（PL）関連の警告事項を表しています。本装置をお使いの際は必ず守ってください。
⚠注意	製造物責任法（PL）関連の注意事項を表しています。本装置をお使いの際は必ず守ってください。

本書における商標の表記について

本書に記載されている会社名および製品名は、各社の商標または登録商標です。

本装置のマニュアルの構成

本装置の取扱説明書は、以下のとおり構成されています。使用する目的に応じて、お使いください。

マニュアル名称	内容
ご利用にあたって	設置方法やソフトウェアのインストール方法を説明しています。
コマンドリファレンス - 構成定義編 -	装置の機能の動作を設定するためのコマンドについて、パラメタの詳細な情報を説明しています。
コマンドリファレンス - 運用管理編 -	装置の再起動など運用に関わるコマンド、およびプロトコルセッションのクリアや統計情報のクリアなど装置を制御するためのコマンドについて、パラメタの詳細な情報を説明しています。
機能説明書（本書）	本装置の機能について説明しています。
トラブルシューティング	トラブルが起きたときの原因と対処方法を説明しています。
メッセージ集	システムログ情報などのメッセージの詳細な情報を説明しています。
仕様一覧	本装置のハード／ソフトウェア仕様と MIB/Trap 一覧を説明しています。
OSS 一覧	本装置が使用している Open Source Software のライセンス一覧です。

第1章
ネットワーク設計概念

この章では、一般的なネットワークの設計概念について説明します。

1.1　レイヤ 2 ネットワーク設計概念

1.1.1　VLAN

レイヤ 2 のネットワークは、MAC アドレスをもとに到達する先を制御します。レイヤ 2 のネットワークでは、VLAN と呼ばれる論理的なネットワークから構成されます。VLAN を使って複数の物理的な LAN から 1 つの論理的な LAN に構成したり、物理的に 1 つの LAN を複数の論理的な LAN に分けたりします。各 VLAN には VLAN ID（VID）を付けて管理します。

VLAN ID

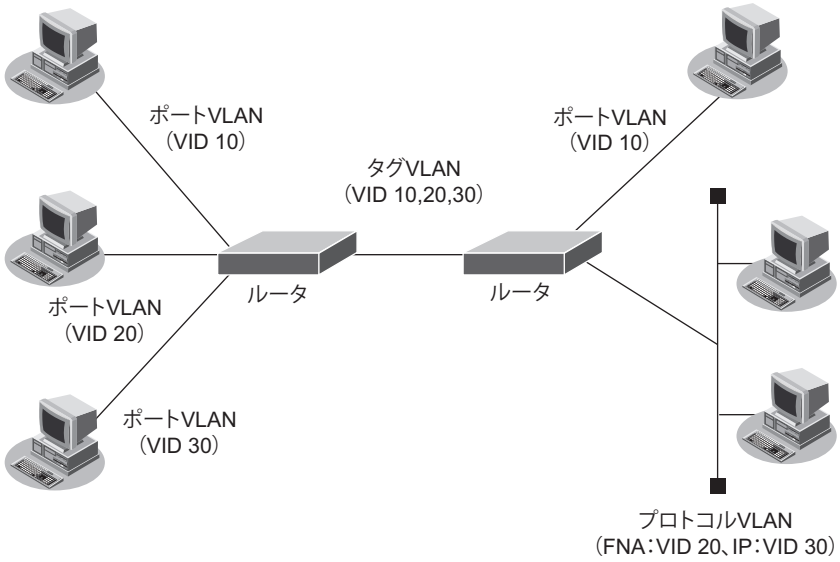
各 VLAN には 10 進数で 1 から 4094 までの番号を付けて管理します。これを VLAN ID と言います。同じ VLAN ID を持つ VLAN に属している装置間では通信可能ですが、異なる VLAN ID を持つ VLAN に属している装置間では通信はできません。

VLAN の種類

VLAN には以下の 3 つの種類があります。

- ポート VLAN
  ETHER ポートごとに「どの VLAN に所属するか」を設定するものです。
  その ETHER ポートのデータは、すべて指定された VLAN に属します。
- タグ VLAN
  1 つの物理回線上に複数の VLAN を設定する場合に使用します。IEEE802.1Q で標準化された方式で、VLAN ヘッダを Ethernet のフレームヘッダに挿入することによって、1 つの物理回線上に複数の VLAN を実現します。

この 3 つの種類は ETHER ポートごとに設定を変えることができます。つまり、VLAN ID が 10 の VLAN を、ETHER ポート 1 ではポート VLAN、ETHER ポート 2 ではタグ VLAN にするといったことができます。この場合、VLAN ID が 10 の VLAN のデータは、ETHER ポート 1 と ETHER ポート 2 で送受信され、ETHER ポート 1 ではタグのない通常のフレーム、ETHER ポート 2 ではタグ付きのフレームとして送受信されます。



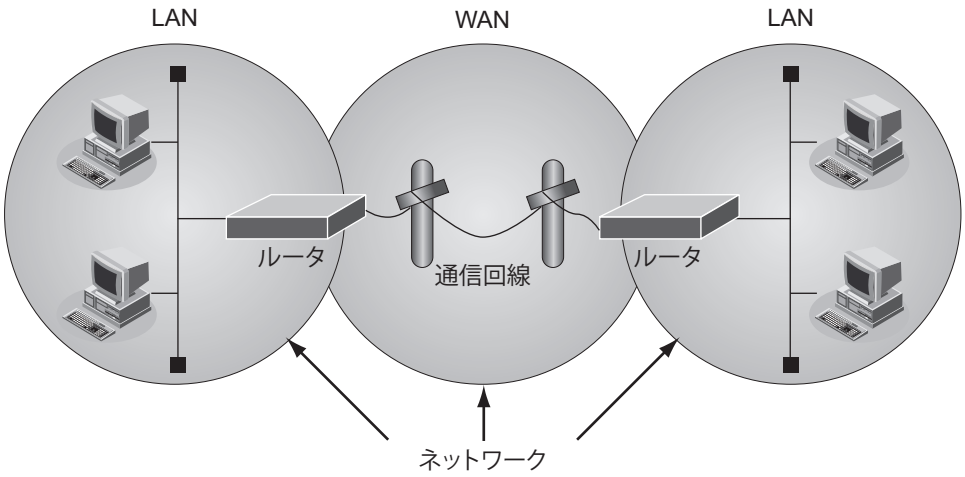
1.2 ネットワーク設計概念

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。

1.2.1 ネットワークの概念とルーティング

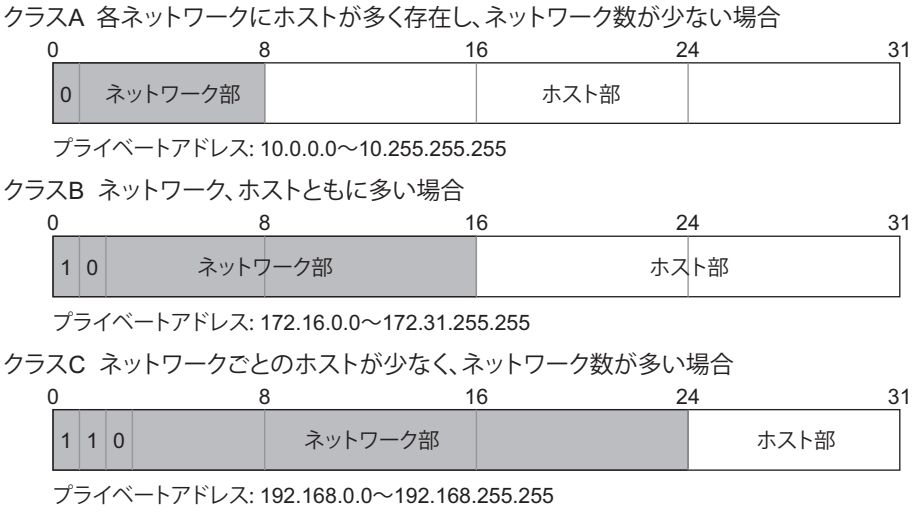
ネットワークの考え方

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なんらかの伝送媒体を介して接続した集合体のことです。たとえば、構築された 1 つの LAN は、HUB やスイッチなどの装置によって 1 つのネットワークとなります。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 1 つのネットワークとなります。また、広義の意味で、これら 1 つ 1 つのネットワークが接続された全体もネットワークとなります。

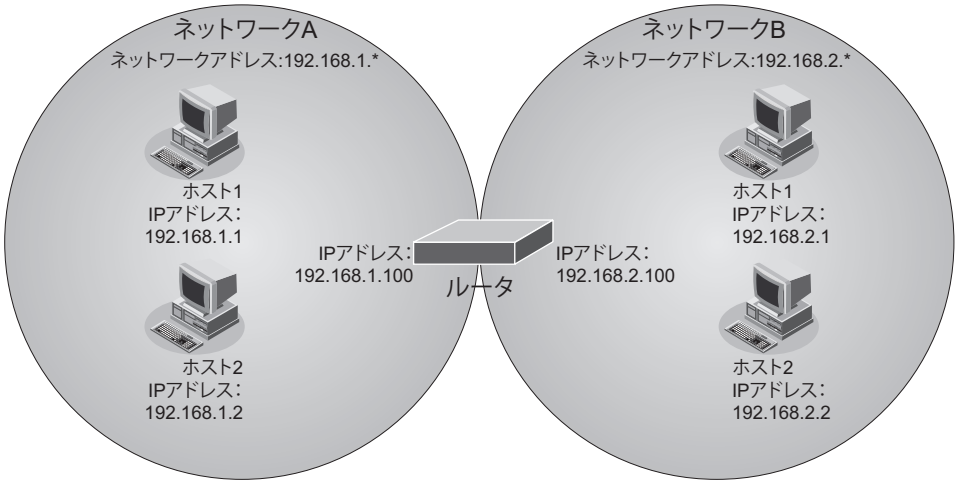


IP ネットワーク

IP ネットワークでは、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それぞれに唯一の 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。



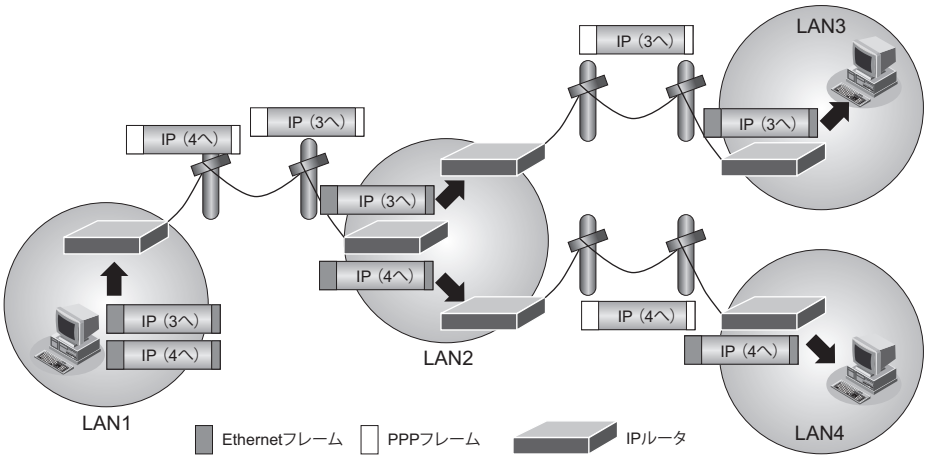
IP ネットワークでの 1 つのネットワークとは、IP アドレスのネットワーク部が同じアドレスを持つ機器の集まりです。つまり、同じデータリンクに接続される機器にはすべて同じネットワークアドレスを設定しなければなりません。さらに、ほかのデータリンクとネットワークアドレスが重ならないように割り当てる必要があります。



以降、本書では、IP の同じネットワーク群のことを「ネットワーク」と言います。また、広義のネットワークについては「ネットワーク全体」と言います。

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。ほかのネットワークあてのデータは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、このとき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を経路情報と言います。ルータはあらかじめ作成された経路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、2 種類の方法があります。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です。



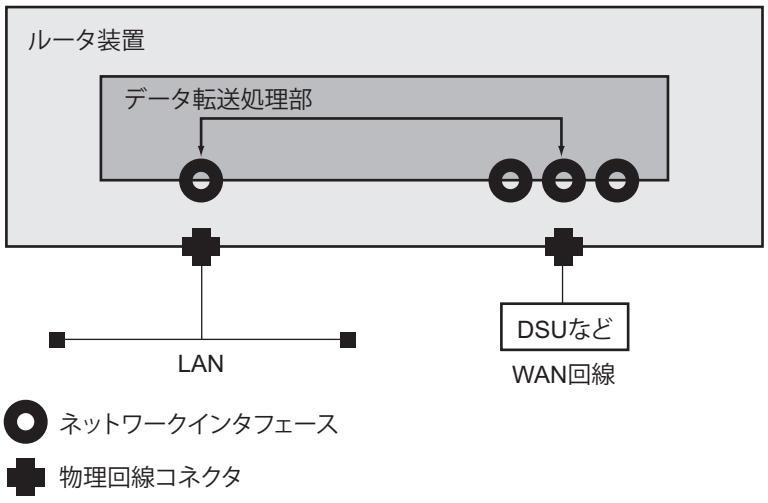
なお、本装置では IP 以外のパケットを転送する機能であるブリッジについてもサポートしています。IP アドレスを持たない IP 以外のパケットは、Ethernet フレームの情報に従って適切な相手にデータを転送することができます。

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 で対応しています。ただし、PPP 通信やトンネル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。



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。このとき、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は、個々のパケットに含まれる宛先 IP アドレスをもと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 あてのパケットを転送する場合

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	—	port-channel 1
192.168.2.0/24	192.168.1.2	port-channel 1
:	:	:

この経路情報から、192.168.2.1 に到達するために出口となるネットワークインタフェースは port-channel 1 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はなく、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。

ブリッジによる転送

もっとも簡単なブリッジによる転送の構造は、受信したデータをほか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。

1.2.2　ルータ設定の概要

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。

以下に、ネットワークインタフェースの種別について説明します。

- 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り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。
- port-channel 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。
- tunnel インタフェース
  PPPoE などの回線を利用して通信する場合、または IP トンネルや IPsec トンネルを利用して通信する場合に、定義された相手システムとの通信に利用されるネットワークインタフェースです。

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：loopback 1,port-channel 1,port-channel 2,tunnel 1,tunnel 2,...

経路情報の定義

経路情報は、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します。

高度な転送先選定定義（ポリシールーティング）

一般的な IP ルーティングでは、送信データ内の宛先 IP アドレスをもとにして、転送先インタフェースの選定を行います。

本装置では、それに加えて、送信データ内の宛先 IP アドレス以外の情報も利用して転送先を選定することができます（ポリシールーティング機能）。

本装置のポリシールーティング機能については、以下を参照してください。

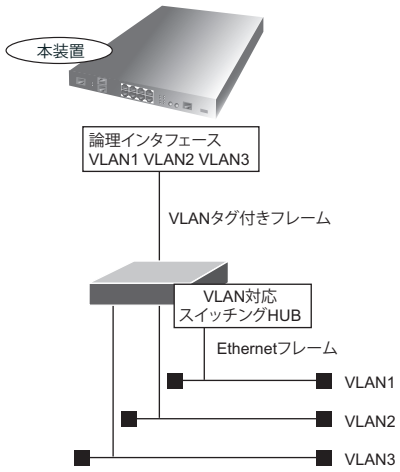
参照 「2.9 ポリシールーティング機能」（P.42）

第2章　機能概要

この章では、本装置の主な機能の概要を説明します。

2.1 VLAN 機能

VLAN 機能とは、物理的な LAN を仮想的な複数の LAN に分割し、ポート、MAC アドレス、プロトコルなどでグループ化を行う機能です。



装置内 VLAN

VLAN は、タギング方式と呼ばれる VLAN グループ識別方法を用いた通信方式を規定しています。タギング方式とは、フレームに VLAN タグを付与することで、そのフレームがどの VLAN に属するのかを識別する方法です。識別子として定義されたものを VLAN ID と言い、VLAN を 1 つ定義した場合、それに対応する VLAN ID も 1 つ割り当てます。

本装置でサポートする VLAN 機能は、IEEE802.1Q に準拠しています。

本装置は、各ポートを特定の VLAN のタグ付きまたはタグなしに設定を変更することができます。

VLAN とネットワークアドレス

VLAN 機能を使用した場合、ブリッジング通信はその VLAN 内に閉じたものになります。したがって、VLAN を定義するということは、MAC アドレスのレベルでブロードキャストフレームが届く範囲（ブロードキャストドメイン）を制限する、ということになります。

また、これをネットワーク層の位置から考えると、以下の 2 つのことができます。

- 各物理ポートに、VLAN タグを使用して複数のネットワークアドレスを対応させる。
- 複数の物理ポートを束ねたものに、1 つのネットワークアドレスを割り当てる。

VLAN 種別

本装置がサポートする VLAN 機能では、以下の単位で VLAN を分けることができます。

- ポート VLAN
  ポート単位でグループ化を行う機能です。すべてのネットワークプロトコルのアドレスを付与することができます。
- タグ VLAN
  フレームに付与される VLAN タグでグループ化を行う機能です。すべてのネットワークプロトコルのアドレスを付与することができます。

VLAN タグとポートの関係

VLAN 機能を使用する場合、あらかじめ VLAN 内のポートに、フレームを送信するときに VLAN タグを付与するか定義しておきます。付与するかどうかは、各ポートの先にあるノードが VLAN タグを識別できるかどうかによって決まります。

VLAN 機能を使用している場合、本装置の各ポートの先に接続されたセグメントは、以下の 3 つのどれかに属しています。

- アクセスリンク
  VLAN タグなしのフレームだけが流れる区間です。VLAN タグを理解できないエンドノードが接続されます。
- トランクリンク
  VLAN タグ付きフレームだけが流れる区間です。タグ付き VLAN 機能をサポートしている装置同士は、通常トランクリンクで接続します。VLAN タグを理解できないエンドノードは接続されません。
- ハイブリッドリンク
  VLAN タグ付きのフレームと VLAN タグなしのフレームの両方が流れる区間です。ここには、複数の VLAN が存在し、それぞれの VLAN にとってアクセスリンクまたはトランクリンクとなります。ただし、特定のプロトコルに注目した場合、ハイブリッドリンクをアクセスリンクとして運用できる VLAN は 1 つだけです。たとえば、1 つのハイブリッドリンク上に 2 つの VLAN がアクセスリンクとして運用している場合に、IP プロトコルに注目すると、そのうちの 1 つしか認識することができません。

同一ポート上での VLAN の混在

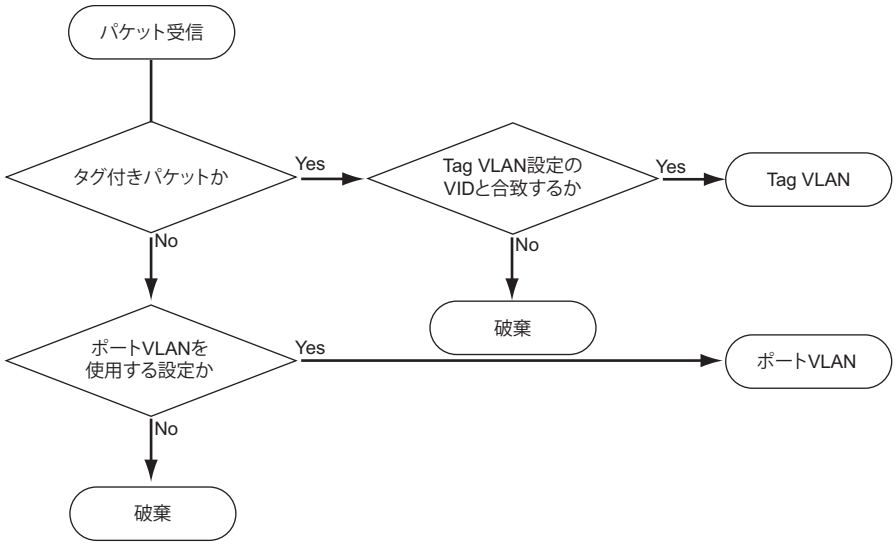
同一ポート上で使用できる VLAN の組み合わせを以下に示します。

○：混在できる、×：混在できない

VLAN 種別	ポート VLAN（untagged）	Tag VLAN（Tagged）
ポート VLAN（untagged）	×	○
Tag VLAN（Tagged）	○	○

パケット受信時の VLAN 判定

VLAN を設定したポートでパケットを受信した場合、受信したパケットの所属する VLAN の判定を以下の順序で行います。



受信したパケットを同一ブリッジグループに転送する時の VLAN タグ

受信したパケットを同一ブリッジグループに転送する時の VLAN タグの扱いは、受信するインタフェースの tagging 設定に従います。tagging transparent の場合は VLAN タグ有りで転送し、tagging terminate の場合は、VLAN タグを除去して転送します。

パケット送信時の VLAN タグ

パケット送信時の VLAN タグの扱いは、送信するポートの Tagged ／ Untagged 設定に従って、Tagged ポートの場合は VLAN タグを付与し、Untagged ポートの場合は VLAN タグを付与しないで送信します。

VLAN トランク機能

VLAN トランク機能とは、VLAN タグの付与および削除が可能なスイッチが VLAN 間の通信を行う際に使用する機能です。複数の VLAN に属するポートからルーティングするために、ほかのレイヤ 3 スイッチへ中継します。ポートでは、どの VLAN に属しているかを認識するために VLAN タグを付け、レイヤ 3 スイッチで VLAN タグ付きフレームを受け取り、ルーティングして中継します。

装置間 VLAN

VLAN が装置間をまたぐ場合、フレームに VLAN タグを付けてどの VLAN からきたフレームかを区別します。これによって、たとえば VLAN A 同士、VLAN B 同士は、それぞれ同じスイッチング HUB に接続されているように通信することができます。また、VLAN トランク機能を使用することによって、通常 2 本必要な伝送路が本装置間を 1 本で接続することができます。

参照 マニュアル「仕様一覧」

VLAN-ID 集約インタフェース機能（vlan-id any）

本装置はすべての VLAN-ID を 1 つのインタフェースで取り扱う VLAN-ID 集約インタフェース機能をサポートします。本機能は LAN ポート (GE1 ポート) のインタフェースの VLAN-ID を "any" 指定することにより動作します。

VLAN-ID 集約インタフェースが所属する bridge-group(VLAN-ID 集約ブリッジ) は装置に 1 つだけ設定可能です。

VLAN-ID 集約インタフェース／ブリッジには以下の制約があります。

- VLAN-ID に "any" を設定可能なのは LAN ポート (GE1 ポート) のインタフェースのみです（サブインタフェースには設定できません）。
- VLAN-ID"any" で取り扱うのは、LAN ポート (GE1 ポート) で使用中の VLAN-ID を除く、全 VLAN-ID のフレームです。
- "any" のインタフェースにて、Untagged フレームは L2 および L3 中継可能です。Tagged フレームは L2 中継のみ可能です。Tagged フレームの VLAN タグを透過します。
- コンフィグに "any" が設定されている場合、"any" のポート数に依存しますが、起動後もしくは refresh コマンド実行後、設定反映のために最大 10 分程度要する場合があります。グローバルモードの vlan-id any コマンドにて対象 VLAN-ID 値の範囲を限定すれば、設定反映時間を短縮することが可能です。

1bridge 複数 VLAN 機能

同一ブリッジグループに異なる複数の VLAN-ID をつけたインタフェースを設定することができます。ただし LAN ポート（GE1 ポート）内で、異なる VLAN-ID 間の折り返し通信はできません。

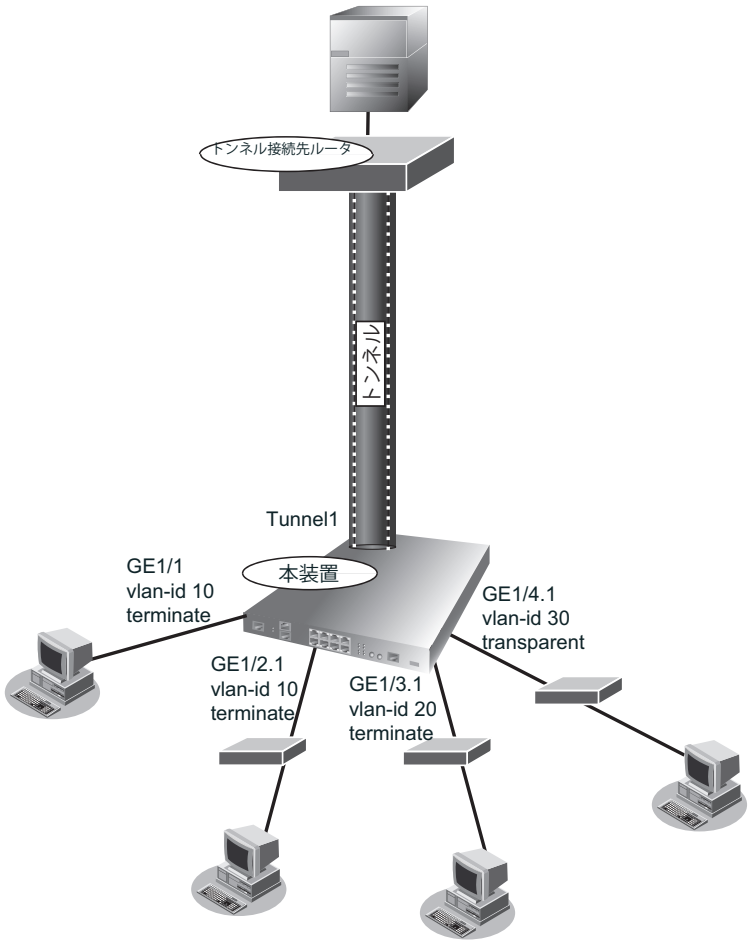
以下、設定例を用いて、動作を説明します。

こんな事に気をつけて

- LAN ポート（GE1 ポート）内で、異なる VLAN-ID 間の折り返し通信はできません。
- 同一ブリッジグループ内の同一 VLAN-ID 間では、tagging terminate と tagging transparent の混在はできません。
- vlan-id any を指定した場合は、tagging 設定は無効となります。Untagged フレームは Untagged のまま転送して、Tagged フレームは VLAN タグを透過して転送します。

（設定例 1）

```
!
interface GigaEthernet 1/1
 vlan-id 10
 bridge-group 10
 tagging terminate
exit
!
interface GigaEthernet 1/2.1
 vlan-id 10
 bridge-group 10
 tagging terminate
exit
!
interface GigaEthernet 1/3.1
 vlan-id 20
 bridge-group 10
 tagging terminate
exit
!
interface GigaEthernet 1/4.1
 vlan-id 30
 bridge-group 10
 tagging transparent
exit
!
interface Tunnel 1
 tunnel mode ether-ip tunnel-profile Bri10
 bridge-group 10
exit
!
```



各 LAN ポートから入力して、Tunnel 1 に出力する 4Flow の VLAN タグの処理は、それぞれ次の通りです。

Flow 番号	入力トラフィック			出力トラフィック		
	入力インタフェース	入力前の VLAN タグ	転送時の VLAN タグ処理	出力時の VLAN タグ処理	出力インタフェース	出力後の VLAN タグ
1	GE 1/1	Untag	-	-	Tunnel 1	Untag
2	GE 1/2.1	10	VLAN タグ除去	-	Tunnel 1	Untag
3	GE 1/3.1	20	VLAN タグ除去	-	Tunnel 1	Untag
4	GE 1/4.1	30	VLAN タグ透過	-	Tunnel 1	30

上記と逆向きの、Tunnel 1 から入力して、各 LAN ポートに出力する 4Flow の VLAN タグの処理は、それぞれ次の通りです。

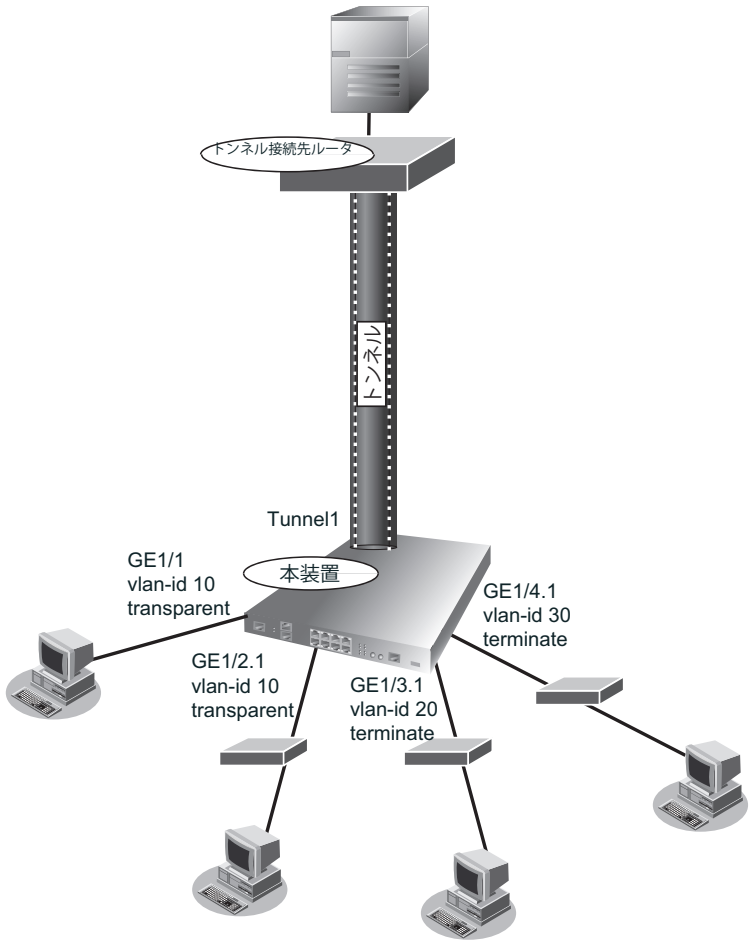
Flow 番号	入力トラフィック			出力トラフィック		
	入力インタフェース	入力前の VLAN タグ	転送時の VLAN タグ処理	出力時の VLAN タグ処理	出力インタフェース	出力後の VLAN タグ
1	Tunnel 1	Untag	-	-	GE 1/1	Untag
2	Tunnel 1	Untag	-	VLAN タグ付与	GE 1/2.1	10
3	Tunnel 1	Untag	-	VLAN タグ付与	GE 1/3.1	20
4	Tunnel 1	30	-	VLAN タグ透過	GE 1/4.1	30

LAN ポート内で折り返す 2Flow の VLAN タグの処理は、それぞれ次の通りです。次の 2Flow 以外の LAN ポートの組み合わせは、互いに VLAN-ID が異なるため、折り返し不可となります。

Flow 番号	入力トラフィック			出力トラフィック		
	入力インタフェース	入力前の VLAN タグ	転送時の VLAN タグ処理	出力時の VLAN タグ処理	出力インタフェース	出力後の VLAN タグ
1	GE 1/1	Untag	-	VLAN タグ付与	GE 1/2.1	10
2	GE 1/2.1	10	VLAN タグ除去	-	GE 1/1	Untag

（設定例 2）

```
!
interface GigaEthernet 1/1
 vlan-id 10
 bridge-group 10
 tagging transparent
exit
!
interface GigaEthernet 1/2.1
 vlan-id 10
 bridge-group 10
 tagging transparent
exit
!
interface GigaEthernet 1/3.1
 vlan-id 20
 bridge-group 10
 tagging terminate
exit
!
interface GigaEthernet 1/4.1
 vlan-id 30
 bridge-group 10
 tagging terminate
exit
!
interface Tunnel 1
 tunnel mode ether-ip tunnel-profile Bri10
 bridge-group 10
exit
!
```



各 LAN ポートから入力して、Tunnel 1 に出力する 4Flow の VLAN タグの処理は、それぞれ次の通りです。

Flow 番号	入力トラフィック			出力トラフィック		
	入力インタフェース	入力前の **VLAN** タグ	転送時の **VLAN** タグ処理	出力時の **VLAN** タグ処理	出力インタフェース	出力後の **VLAN** タグ
1	GE 1/1	Untag	VLAN タグ付与	-	Tunnel 1	10
2	GE 1/2.1	10	VLAN タグ透過	-	Tunnel 1	10
3	GE 1/3.1	20	VLAN タグ除去	-	Tunnel 1	Untag
4	GE 1/4.1	30	VLAN タグ除去	-	Tunnel 1	Untag

上記と逆向きの、Tunnel 1 から入力して、各 LAN ポートに出力する 4Flow の VLAN タグの処理は、それぞれ次の通りです。

Flow 番号	入力トラフィック			出力トラフィック		
	入力インタフェース	入力前の **VLAN** タグ	転送時の **VLAN** タグ処理	出力時の **VLAN** タグ処理	出力インタフェース	出力後の **VLAN** タグ
1	Tunnel 1	10	-	VLAN タグ除去	GE 1/1	Untag
2	Tunnel 1	10	-	VLAN タグ透過	GE 1/2.1	10
3	Tunnel 1	Untag	-	VLAN タグ付与	GE 1/3.1	20
4	Tunnel 1	Untag	-	VLAN タグ付与	GE 1/4.1	30

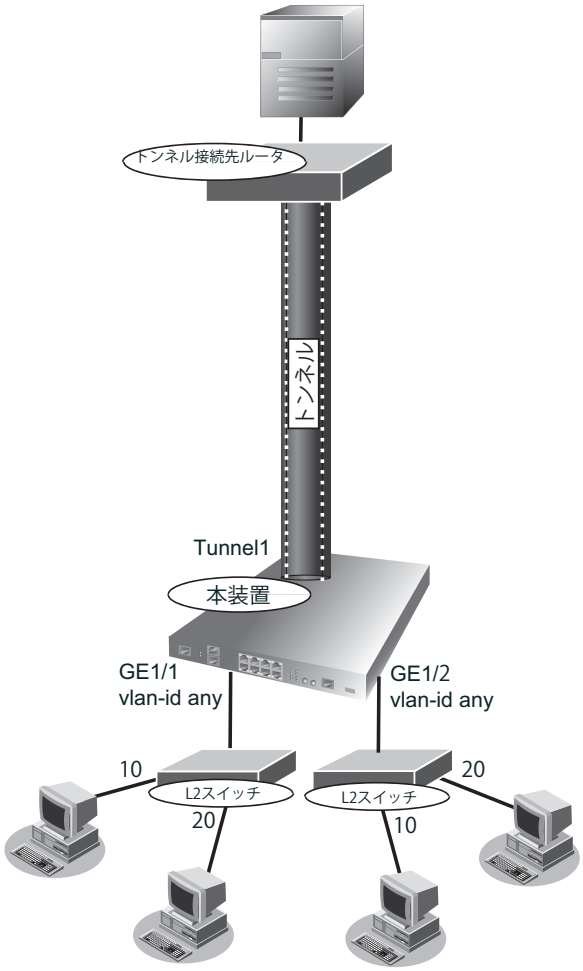
LAN ポート内で折り返す 2Flow の VLAN タグの処理は、それぞれ次の通りです。次の 2Flow 以外の LAN ポートの組み合わせは、互いに VLAN-ID が異なるため、折り返し不可となります。

Flow 番号	入力トラフィック			出力トラフィック		
	入力インタフェース	入力前の **VLAN** タグ	転送時の **VLAN** タグ処理	出力時の **VLAN** タグ処理	出力インタフェース	出力後の **VLAN** タグ
1	GE 1/1	Untag	VLAN タグ付与	VLAN タグ透過	GE 1/2.1	10
2	GE 1/2.1	10	VLAN タグ透過	VLAN タグ除去	GE 1/1	Untag

（設定例 3）

```
!
interface GigaEthernet 1/1
 vlan-id any
 bridge-group 10
exit
!
interface GigaEthernet 1/2
 vlan-id any
 bridge-group 10
exit
!
interface Tunnel 1
 tunnel mode ether-ip tunnel-profile Bri10
 bridge-group 10
exit
!
```

＊LAN側のL2スイッチは、VLAN10をUntaggedフレームとして本装置に、VLAN20をTaggedフレームとして本装置に、それぞれ転送するものとします。



各 LAN ポートから入力して、Tunnel 1 に出力する 4Flow の VLAN タグの処理は、それぞれ次の通りです。

Flow 番号	入力トラフィック			出力トラフィック		
	入力インタフェース	入力前の **VLAN** タグ	転送時の **VLAN** タグ処理	出力時の **VLAN** タグ処理	出力インタフェース	出力後の **VLAN** タグ
1	GE 1/1	Untag	-	-	Tunnel 1	Untag
2	GE 1/1	20	VLANタグ透過	-	Tunnel 1	20
3	GE 1/2	Untag	-	-	Tunnel 1	Untag
4	GE 1/2	20	VLANタグ透過	-	Tunnel 1	20

上記と逆向きの、Tunnel 1 から入力して、各 LAN ポートに出力する 4Flow の VLAN タグの処理は、それぞれ次の通りです。

Flow 番号	入力トラフィック			出力トラフィック		
	入力インタフェース	入力前の **VLAN**タグ	転送時の **VLAN**タグ処理	出力時の **VLAN**タグ処理	出力インタフェース	出力後の **VLAN**タグ
1	Tunnel 1	Untag	-	-	GE 1/1	Untag
2	Tunnel 1	20	-	VLANタグ透過	GE 1/1	20
3	Tunnel 1	Untag	-	-	GE 1/2	Untag
4	Tunnel 1	20	-	VLANタグ透過	GE 1/2	20

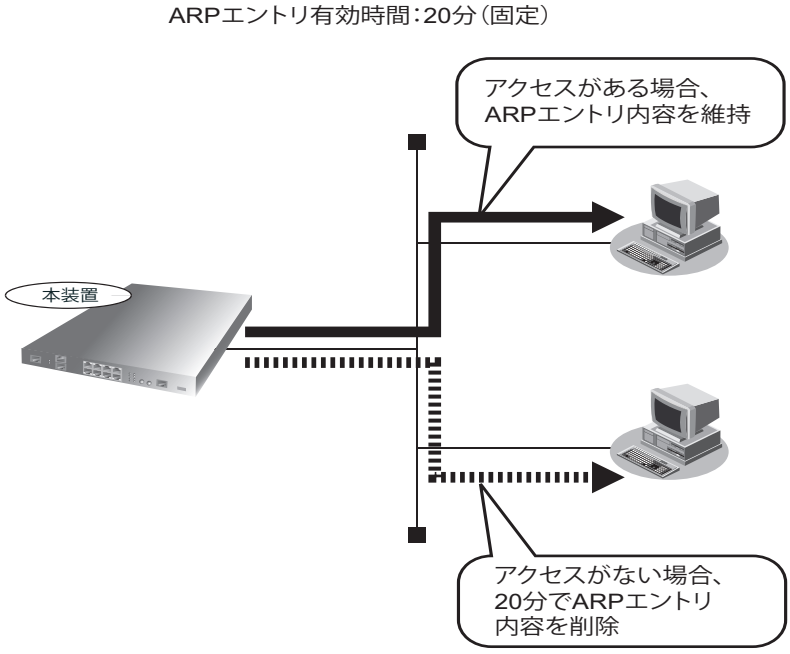
LAN ポート内で折り返す 4Flow の VLAN タグの処理は、それぞれ次の通りです。次の 4Flow 以外の LAN ポートの組み合わせは、互いに VLAN-ID が異なるため、折り返し不可となります。

Flow 番号	入力トラフィック			出力トラフィック		
	入力インタフェース	入力前の **VLAN**タグ	転送時の **VLAN**タグ処理	出力時の **VLAN**タグ処理	出力インタフェース	出力後の **VLAN**タグ
1	GE 1/1	Untag	-	-	GE 1/2	Untag
2	GE 1/1	20	VLANタグ透過	VLANタグ透過	GE 1/2	20
3	GE 1/2	Untag	-	-	GE 1/1	Untag
4	GE 1/2	20	VLANタグ透過	VLANタグ透過	GE 1/1	20

2.2 ARP エージング機能

ARP エージング機能とは、自動的に学習された ARP エントリ情報のうち、一定時間アクセスのない端末の ARP エントリを削除する機能です。

このほか、アクセスのある端末の ARP エントリについては削除前に ARP リクエストを発行し、学習している ARP エントリ内容を維持することができます。



こんな事に気をつけて

- スタティック ARP 機能で設定された ARP エントリは対象になりません。
- ARP エントリ削除前の ARP リクエスト発行は、登録後アクセスのあった端末を対象として行います。

2.3 IPv6 機能

IPv6 とは、現在、主に利用されている IP（IPv4）を置き換えるための次世代インターネットプロトコルです。本装置では、IPv4 パケットだけでなく IPv6 パケットも転送することができます。

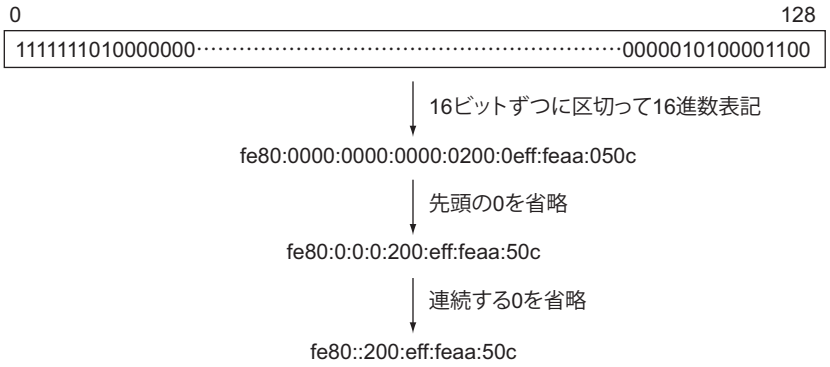
本装置がサポートしている IPv6 機能は、以下のとおりです。

- ルータ機能
  - 静的または動的な経路設定
  - Router Advertisement Message 送信によるホストのアドレスの自動設定
  - パケットフィルタリング
- ホスト機能
  - 静的な経路設定
  - Router Advertisement Message 受信によるアドレスの自動設定
  - Router Advertisement Message 受信によるデフォルト経路の自動設定
  - Router Advertisement Message 受信による ND 情報の自動設定
  - ソースアドレスの自動選択

IPv6 アドレスの表記方法

128 ビットの IPv6 アドレスを表記する場合は、そのアドレスを「:」（コロン）で 16 ビットずつに区切って、その内容を 16 進数で記述します。個々の 16 進数の値について先頭の 0 は省略することができます。連続して 0 が続く場合は、1 つの IPv6 アドレスの表記で 1 回限り「::」で省略することができます。

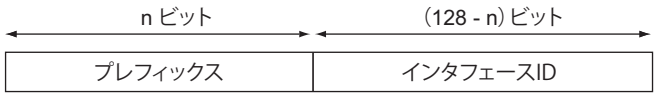
例を以下に示します。



IPv6 アドレス体系

IPv6 アドレスは、IPv4 アドレスがネットワーク部とホスト部に分離することができるように、プレフィックスとインタフェース ID に分離することができます。一般的には、プレフィックスのビット長（プレフィックス長）は 64 ビットで利用されます。

プレフィックス長を含めてアドレス表記をする場合は、プレフィックス長はアドレスの後ろに「/」で区切って付与します。



IPv6 で利用することができるアドレスは、IPv4 と同様に、先頭のビット数によって利用方法が決められています。本装置で利用できるアドレスは以下のようなものがあります。

- Global Unicast Addresses
  通常利用するアドレスです。一般的には、契約した ISP から割り当てられます。
  このアドレスは先頭の 7 ビットが 1111 110 で始まります。
- Link-Local Unicast Addresses（fe80::/64）
  link 内（ルータを介さないで通信できる範囲）だけで有効な特別なアドレスです。このアドレスは先頭の 10 ビットが 1111 1110 10 で始まります。通常は 11 ビット目から 64 ビット目まではすべて 0 となります。
- Multicast Addresses
  マルチキャストアドレスです。先頭の 8 ビットが 1111 1111 となります。

静的または動的な経路設定

IPv6 のネットワークとルーティングの概念は、IPv4 の場合とほぼ同じです。装置が持つ経路情報に従って転送先を決定します。この経路情報を装置に持たせる方法として、静的な経路設定（スタティックルーティング）と動的な経路設定（ダイナミックルーティング）があります。

スタティックルーティングとは、経路情報を構成定義として設定し、利用します。この経路情報は構成定義を変更しない限り変更されることはありません。

ダイナミックルーティングとは、ルーティングプロトコルを利用する通信によって、ネットワーク上のほかのノードから経路情報を学習して利用します。本装置では IPv6 ルーティングプロトコルとして BGP4、OSPF をサポートしています。

Router Advertisement Message 送信によるホストのアドレスの自動設定

本装置では、Router Advertisement Message の送信機能をサポートしています。

Router Advertisement Message には、そのネットワークで利用するプレフィックス情報とデフォルトルータ情報、隣接情報が含まれています。このメッセージを受信したホストは、その情報を利用して、自身の IPv6 グローバルアドレスとデフォルトルートを自動設定し、ネットワーク通信が可能となります。

パケットフィルタリング

本装置では、特定の IPv6 パケットの通過を許可／禁止するためのパケットフィルタリング機能があります。

Router Advertisement Message 受信によるアドレスの自動設定

本装置では、Router Advertisement Message の受信機能をサポートしています。

Router Advertisement Message には、そのネットワークで利用するプレフィックス情報が含まれています。プレフィックス情報を受信した場合、有効期限を管理するためのプレフィックスリストを生成し、インタフェース ID を付加した IPv6 アドレスを自動設定します。
受信したプレフィックス情報は、show ipv6 routers コマンドで参照できます。また、自動設定した IPv6 アドレスは、show ipv6 route または show interface コマンドで参照できます。

参照 マニュアル「コマンドリファレンス」の「show ipv6 routers」、「show ipv6 route」、「show interface」

こんな事に気をつけて

プレフィックス情報のオンリンクフラグと自動アドレス生成フラグが設定されている場合、IPv6 アドレスをインタフェースに設定します。

Router Advertisement Message 受信によるデフォルト経路の自動設定

Router Advertisement Message を受信した場合、送信ルータのリンクローカルアドレスを中継ゲートウェイとするデフォルト経路を設定します。

複数のルータより Router Advertisement Message を受信した場合、デフォルトルータとして利用できるデフォルトルータリストを生成し、この一覧の中でパケットが到達可能なルータをデフォルトルータとして設定します。
設定されたデフォルトルータは、show ipv6 route コマンドで参照できます。

参照 マニュアル「コマンドリファレンス」の「show ipv6 route」

こんな事に気をつけて

複数ルータから Router Advertisement Message を受信した場合、ルータプレファレンスに従って、デフォルトルータを選択します。

Router Advertisement Message 受信による ND 情報の自動設定

Router Advertisement Message には、通信時に使用する隣接情報（ND 情報）が含まれています。Router Advertisement Message を受信し、受信メッセージに含まれている ND 情報と本装置で保持している ND 情報が異なる場合は、ND 情報の更新が行われます。

以下に、本装置で保持している ND 情報とその初期値を示します。

- 隣接装置の到達性についての有効期間（初期値は 30 秒）
- 隣接装置の到達性確認を行う Neighbor Solicitation（NS）Message の送信間隔（初期値は 1 秒）
- 最大ホップ数（初期値は 64）
- 受信ネットワーク上で推奨する MTU 長（初期値は 1500 バイト）

2.4 IP 経路制御機能

IP 経路情報は、ルーティングテーブルで管理され、IP パケットの転送先の判断に使用します。

IP 経路情報は、以下の機能で制御します。

- インタフェースの障害検出による経路制御機能
- スタティックルーティング機能
- ダイナミックルーティング機能

ここでは、IP 経路情報の種類、管理方法および IP 経路情報を制御する機能について説明します。

2.4.1 IP 経路情報の種類

IP 経路情報は、以下に示す情報で分類されます。

- インタフェース経路（IPv4）
  ネットワークインタフェースに割り当てた IPv4 ネットワークまたは IPv4 アドレスを示します。ループバックインタフェースに割り当てた IPv4 アドレスは、ホストルート（32 ビットネットワークマスク）として管理されます。
- インタフェース経路（IPv6）
  ネットワークインタフェースに割り当てた IPv6 プレフィックスを示します。ループバックインタフェースに割り当てた IPv6 アドレスは、ホストルート（128 ビットネットワークマスク）として管理されます。
- RA 経路（IPv6）
  受信した Router Advertisement（RA）Message の情報に基づき、生成されるデフォルトルートを示します。
- スタティック経路（IPv4/IPv6）
  構成定義として設定し、装置に保持される経路情報を示します。
- RIP 経路（IPv4）
  RIP で受信した経路情報を示します。
- BGP4 経路（IPv4/IPv6）
  BGP4 で受信した経路情報を示します。
- OSPF 経路（IPv4/IPv6）
  OSPF で受信したリンク情報をもとに作成する最短経路（ショートパス）を示します。
- ISAKMP 経路（IPv4/IPv6）
  IPsec 機能による経路情報を示します。以下の 3 種類の経路情報があります。
  - SA-UP 経路（IPv4/IPv6）：SA-UP 機能による経路情報を示します。
  - tunnel-route 経路（IPv4/IPv6）：トンネルルート機能による VPN ピアへの経路情報を示します。
  - L2TPv2 経路（IPv4/IPv6）：L2TP/IPsec 機能による端末への経路情報を示します。
- DHCP クライアント経路（IPv4）
  DHCPv4 クライアント機能を使用し、DHCP サーバから受信した経路情報を示します。
- DHCP クライアント経路（IPv6）
  DHCPv6 クライアント機能を使用し、払い出されたプレフィックスに対する reject 経路情報を示します。
- DHCP サーバ経路（IPv6）
  DHCPv6 サーバ機能を使用し、払い出したプレフィックスへの経路情報を表示します。
- ローカルブレイクアウト経路 (IPv4/IPv6)
  ローカルブレイクアウト機能を使用し、ブレイクアウトする経路情報を示します。

各経路情報は、以下の優先度値が設定されています。

IP 経路情報	IP 版数	優先度値
インタフェース経路	IPv4/IPv6	0（固定）
スタティック経路	IPv4/IPv6	1（変更可）
RA 経路	IPv6	10（変更可）
RIP 経路	IPv4	120（変更可）
BGP4 経路（EBGP）	IPv4/IPv6	20（変更可）
BGP4 経路（IBGP）	IPv4/IPv6	200（変更可）
OSPF 経路	IPv4/IPv6	110（変更可）
ISAKMP SA-UP 経路	IPv4/IPv6	1（変更可）
ISAKMP tunnel-route 経路	IPv4/IPv6	2（固定）
ISAKMP L2TPv2 経路	IPv4/IPv6	1（固定）
DHCP クライアント経路	IPv4	1（変更可）
DHCP クライアント経路	IPv6	254（固定）
DHCP サーバ経路	IPv6	254（固定）
ローカルブレイクアウト経路	IPv4/IPv6	0（変更可）

2.4.2 IP 経路情報の管理

IP 経路情報は、ルーティングプロトコルの経路テーブルとルーティングテーブルで管理されます。

以下に、2 つのテーブルについて説明します。

ルーティングプロトコルの経路テーブル

ルーティングプロトコルでは、以下のテーブルで IP 経路情報を管理します。

参照 マニュアル「仕様一覧」

- RIP（IPv4）
  テーブル RIP で使用する経路テーブルを示し、以下のものを含みます。
  - RIP で受信した経路情報
  - RIP に再配布した経路情報

  インタフェース経路を除いた経路情報をエントリ数として管理します。
- BGP4（IPv4）テーブル
  BGP4 で使用する IPv4 経路テーブルを示し、以下のものを含みます。
  - EBGP/IBGP で受信した IPv4 経路情報
  - BGP に再配布した IPv4 経路情報

  BGP IPv4 ネットワーク経路、IPv4 集約機能で生成された経路情報を除いた経路情報をエントリ数として管理します。
- BGP4（IPv6）テーブル
  BGP4 で使用する IPv6 経路テーブルを示し、以下のものを含みます。
  - EBGP/IBGP で受信した IPv6 経路情報
  - BGP に再配布した IPv6 経路情報

BGP IPv6 ネットワーク経路、IPv6 集約機能で生成された経路情報をエントリ数として管理します。

- OSPF（IPv4）リンクステートデータベース（LSDB）
  OSPF で使用するリンク情報を保存するデータベースを示し、以下のものを含みます。
  - OSPF で受信した LSA 情報
  - OSPF に再配布した経路情報
- OSPF（IPv6）リンクステートデータベース（LSDB）
  OSPF で使用するリンク情報を保存するデータベースを示し、以下のものを含みます。
  - OSPF で受信した LSA 情報
  - OSPF に再配布した経路情報

ルーティングテーブル

ルーティングテーブルは、IP 経路情報の中から選択した優先経路（ベストパス）で構成されます。また、ルーティングテーブルで管理する IP 経路情報の中で、インタフェース経路を除いたものをルーティングエントリ数として管理します。

参照 マニュアル「仕様一覧」

2.4.3 スタティックルーティング機能

スタティック経路を使用し、以下の機能と組み合わせることにより、IP 経路情報を制御します。

また、優先度が同一値のスタティック経路を使用することにより、ECMP 機能で使用する IP 経路情報を作成できます。

参照 「2.17 ECMP 機能」（P.68）

- 優先経路制御機能
  同じ宛先の経路に対して、優先度（distance）によって、ルーティングテーブルに追加する IP 経路情報を選択することができます。優先度が小さいほど優先経路と扱われ、優先経路だけをルーティングテーブルに反映します。また、この優先経路が無効となった場合、次の優先経路に切り替えることができます。

2.4.4 ダイナミックルーティング機能

ルーティングプロトコルが経路情報の送受信を行うことにより、IP 経路情報を制御します。

本装置は、以下のルーティングプロトコルをサポートしています。

- RIP（IPv4）
- BGP（IPv4）
- BGP（IPv6）
- OSPF（IPv4）
- OSPF（IPv6）

なお、OSPF（IPv4）と BGP（IPv4）では、ECMP 機能で使用する IP 経路情報を作成できます。

参照 「2.5 RIP 機能」（P.33）、「2.6 BGP4 機能」（P.35）、「2.7 OSPF 機能」（P.38）、「2.8 IP フィルタリング機能」（P.40）、「2.17 ECMP 機能」（P.68）

また、以下の IP 経路制御機能をサポートしています。

- 経路再配布機能
  ルーティングテーブルに登録された IP 経路情報をルーティングプロトコルに取り込むことができます。本機能を使用することでルーティングプロトコルで受信した経路やスタティック経路などを異なるルーティングプロトコルで広報することができます。IPv4 経路情報から IPv6 経路情報、また、IPv6 経路情報から IPv4 経路情報への経路再配布はできません。
- インタフェースの障害検出による経路制御機能
  インタフェースの障害検出により、該当インタフェースを介して受信した経路情報をルーティングテーブルから削除できます。また、該当インタフェースを出口とする経路情報を再配布している場合、それらの経路情報が無効になったことを即座に広報することができます。
- 優先経路制御機能
  同じ宛先の経路に対して、優先度（distance）によって経路を選択することができます。優先度が小さいほど優先経路として扱われ、優先経路だけをルーティングテーブルに反映します。また、この優先経路が無効となった場合、次の優先経路に切り替えることができます。IPv4 経路情報と IPv6 経路情報との間で、優先経路制御はできません。
- 経路フィルタリング機能
  RIP（IPv4）と BGP4（IPv4/IPv6）では、送受信する IP 経路情報に対してフィルタリングすることができます。
- 再配布フィルタリング
  RIP（IPv4）、OSPF（IPv4/IPv6）および BGP4（IPv4/IPv6）に取り込む IP 経路情報に対してフィルタリングすることができます。このフィルタリングは、条件に一致した場合の動作として、“透過”または“遮断”を指定することができます。

こんな事に気をつけて

- IPv4 セカンダリアドレスが属するネットワーク上では、ルーティングプロトコルによる経路交換を行うことはできません。
- ダイナミックルーティングで利用するインタフェースは IP アドレスを設定する必要があります。

2.5 RIP 機能

RIP（Routing Information Protocol）は、ルータ間で使用するダイナミックルーティングプロトコルです。RIP プロトコルを使用するルータ間で経路情報の交換を行い、パケットを転送する経路を制御します。各ルータは、宛先のネットワークに到達するために、いくつのルータを経由するか（ホップ数）という情報を保持します。また、該当する宛先に対してホップ数が一番少ない経路を使用してパケットを転送します。

RIP 機能を使用した場合、直接接続しているネットワークの各ルータに対して、定期的に自装置が保持している経路情報を広報します。起動直後は直接接続しているインタフェースの経路情報だけを広報しますが、ほかのルータから経路情報の通知を受けると、以降はその経路情報も合わせて広報するようになります。

本装置では定期的に経路情報を広報する時間間隔にゆらぎを持たせています。ルータが一斉に立ち上がった場合に、同じ時間間隔で経路情報を広報するとタイミングが集中し、ネットワークのトラフィックが圧迫されるためです。ゆらぎがあると、このような事態を避けることができます。

定期広報タイマ設定値の 50 ～ 150% の範囲でゆらぎます。

RIP プロトコルを使用する場合は、ホップ数は 15 までに制限されます。ホップ数が 15 を超えるような大規模なネットワークは構築することができません。また、短い間隔（初期値では 30 秒）ですべての経路情報を再広報するため、ネットワークが大規模になるほど広報処理によってネットワークのトラフィックが圧迫されます。このため、RIP 機能は小規模なネットワークを構築する場合に使用してください。

本装置でサポートする RIP 機能は、「RFC2453：RIP Version 2」の RFC（Request For Comments）に準拠しています。

本装置でサポートする RIP 機能

項目	サポート内容
RIP バージョン	バージョン 2
トリガードアップデート	サポート
スプリットホライズン	サポート（シンプルのみ）
認証	テキスト認証、MD5 認証をサポート
RIP タイマ設定	以下のタイマ変更をサポート ・定期広報タイマ ・有効期限タイマ ・ガーベージタイマ
RIP への再配布	以下の経路情報の再配布をサポート ・インタフェース経路情報（ループバックインタフェースアドレスを含む） ・スタティック経路情報 ・BGP 経路情報 ・OSPF 経路情報 経路情報種別ごとに、再配布するかどうかを指定できます。
RIP 経路の他プロトコルへの広報	BGP、OSPF での広報をサポート
フィルタリング	経路情報単位での透過／遮断／メトリックの変更をサポート
再配布フィルタリング	経路情報単位での透過／遮断をサポート

⚠注意

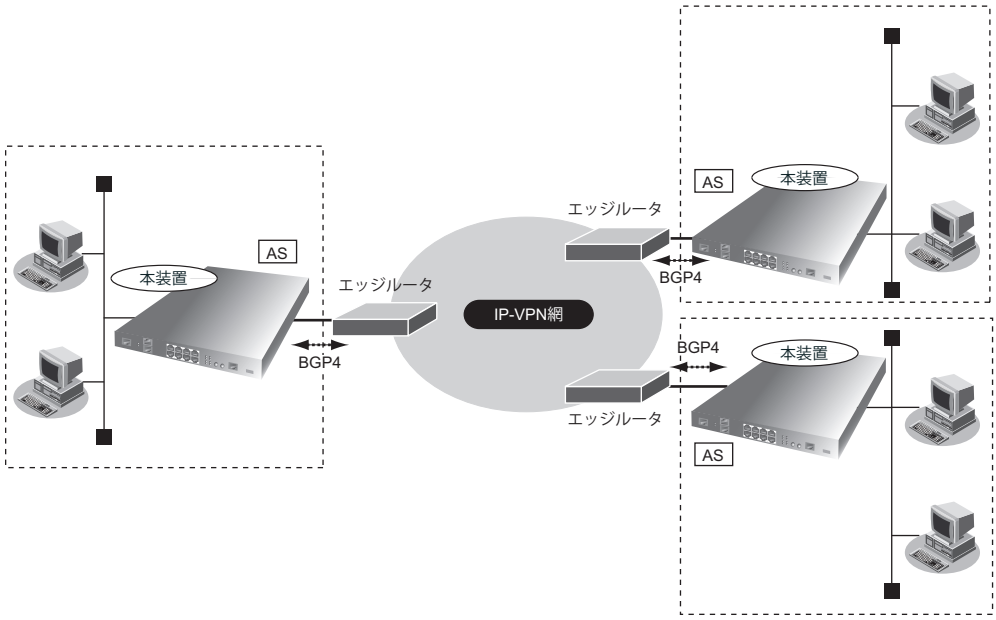
RIP 機能を使用する場合、定期的にパケットを送信します。このため、定額制でない回線を使用している場合は、超過課金の原因となることがあります。このような環境では **RIP** 機能は使用しないでください。

こんな事に気をつけて

- 本装置の初期設定では、インタフェース経路とスタティック経路の RIP 機能を使用して広報します。RIP 機能は定期的に保有するすべての経路情報を広報します。このため、大量のインタフェースが設定されていると、RIP は定期的に大量の RIP 広報パケットを送信し、通信トラフィックを圧迫する場合があります。インタフェース経路やスタティック経路が RIP で広報不要な場合は、インタフェース経路とスタティック経路の RIP への再配布を行わない設定に変更してください。なお、RIP 機能を使用するインタフェースに関しては、再配布の設定に関係なく必ず RIP で広報します。
- RIPv2 の経路集約は未サポートです。

2.6 BGP4 機能

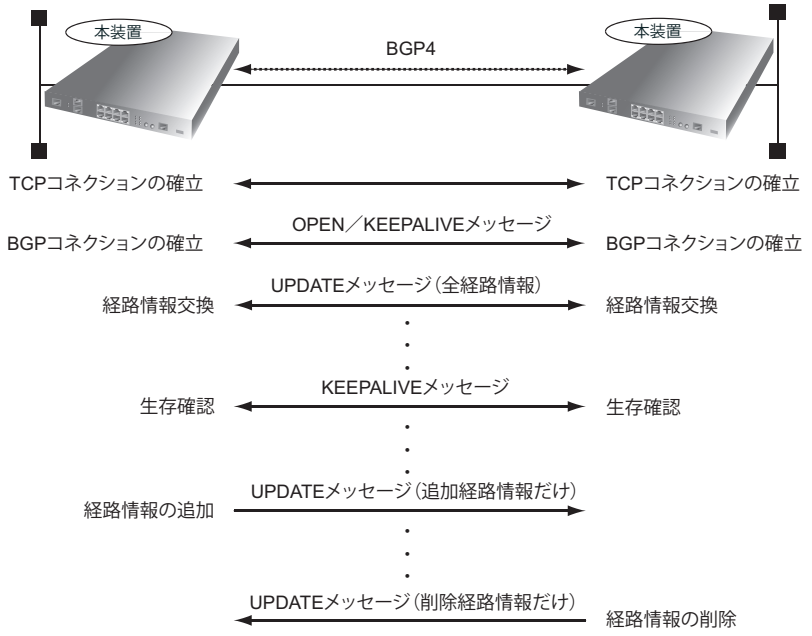
BGP4（Border Gateway Protocol version4）機能とは、AS（自律システム：同じポリシーに従って運用されているネットワークの単位）間で経路情報を交換するためのルーティングプロトコル機能です。BGP4 機能は、IP-VPN サービスで、信頼性の高いネットワーク構成を構築するために必要な機能です。



BGP4 のセッションには、EBGP（External BGP）と IBGP（Internal BGP）の 2 種類があります。

EBGP は AS 間で使用する BGP セッションで、IBGP は同じ AS 内で使用する BGP セッションです。

BGP4 は、TCP コネクションを確立し、TCP コネクション上に BGP コネクションを構築します。BGP コネクションは OPEN ／ KEEPALIVE メッセージを交換することにより確立します。BGP コネクションが確立すると、お互いの装置がすべての経路情報を UPDATE メッセージで交換しあいます。そのあとで、経路情報に変更がない場合は、定期的に KEEPALIVE パケットで生存確認を行います。経路情報に追加がある場合は、UPDATE パケットで追加された経路情報だけを広報します。経路情報の削除がある場合は、UPDATE パケットで削除された経路情報だけを広報します。



同じ宛先への経路情報が複数ある場合、以下の順番で優先経路を選択します。

（1） 設定された WEIGHT 値の大きい経路を選択します。

（2） LOCAL-PREF 値の大きい経路を選択します。

（3） 本装置で生成された BGP 経路について、次のコマンドで生成された順に選択します。
redistribute connected > redistribute static > network > aggregate-address

（4） AS-PATH 長が短い経路を選択します。

（5） ORIGIN 属性の値で、IGP(0) > EGP(1) > INCOMPLETE(2) の順に選択します。

（6） MED 値の小さい経路を選択します。

（7） 配布元が eBGP ピアと iBGP ピアである場合、eBGP ピアから学習した経路を選択します。

（8） NEXT-HOP 属性で指定された Next-hop へのメトリック値が小さい経路を選択します。

（9） ROUTER-ID 値が小さい経路を選択します。

（10）CLUSTER-LIST 属性に含まれる CLUSTER-ID 長の小さい経路を選択します。

（11）配布元の BGP ピアのアドレス値が小さい経路を選択します。

本装置でサポートしている BGP4 機能は、以下の RFC（Request For Comments）に準拠しています。

- RFC1771:A Border Gateway Protocol 4（BGP-4）
- RFC2385:Protection of BGP Sessions via the TCP MD5 Signature Option
- RFC2842:Capabilities Advertisement with BGP-4
- RFC4893:BGP Support for Four-octet AS Number Space
- RFC4724:Graceful Restart Mechanism for BGP

本装置でサポートする BGP 機能

項目	サポート内容
BGP バージョン	バージョン 4 をサポート
BGP セッション	IPv4 セッションと IPv6 セッションをサポート セッションごとに以下をサポート • EBGP 接続（マルチホップ接続を含む） • IBGP 接続
BGP4+（Multiprotocol Extensions for BGP-4）	IPv6 Unicast をサポート
アドレスファミリ	IPv4 セッションでは、以下のアドレスファミリをサポート • IPv4 Unicast IPv6 セッションでは、以下のアドレスファミリをサポート • IPv6 Unicast
認証	IPv4 セッションでの MD5 認証をサポート
ルートリフレッシュ	IPv4/IPv6 セッションごとに送信／受信が可能
グレースフルリスタート	IPv4 セッションで以下をサポート • レシーブルータ機能だけをサポート • stale タイマの設定が可能
BGP への再配布	以下の経路情報の再配布をサポート • インタフェース経路情報（IPv4/IPv6） • ループバックアドレス（IPv4/IPv6） • スタティック経路情報（IPv4/IPv6） • RIP 経路情報（IPv4） • OSPF 経路情報（IPv4/IPv6） 経路情報種別ごとに、再配布するかどうかを指定できます。
BGP 経路の他プロトコルへの広報	IPv4 BGP 経路は、RIP（IPv4）、OSPF（IPv4）での広報をサポート IPv6 BGP 経路は、OSPF（IPv6）での広報をサポート
フィルタリング	IPv4/IPv6 セッションごとに以下をサポート • 経路情報単位での透過／遮断 • 特定 AS からの経路情報の透過／遮断 • 経路情報単位での属性設定（MED メトリック値、AS パスプリペンド、 ローカル優先度）
再配布フィルタリング	IPv4/IPv6 経路ごとに以下をサポート • 経路情報単位での透過／遮断
経路集約	IPv4/IPv6 経路ごとの経路集約をサポート

⚠注意

BGP4 機能を使用する場合、定期的にパケットを送信します。このため、定額制でない回線を使用している場合は、超過課金の原因となることがあります。このような環境では、**BGP4** 機能を使用しないでください。

こんな事に気をつけて

- NAT 機能と併用することはできません。
- BGP4+ 機能での IPv6 プロトコルの利用を BGP（IPv6）と記載します。
- BGP を使用するインタフェースには、IP アドレスを設定する必要があります。

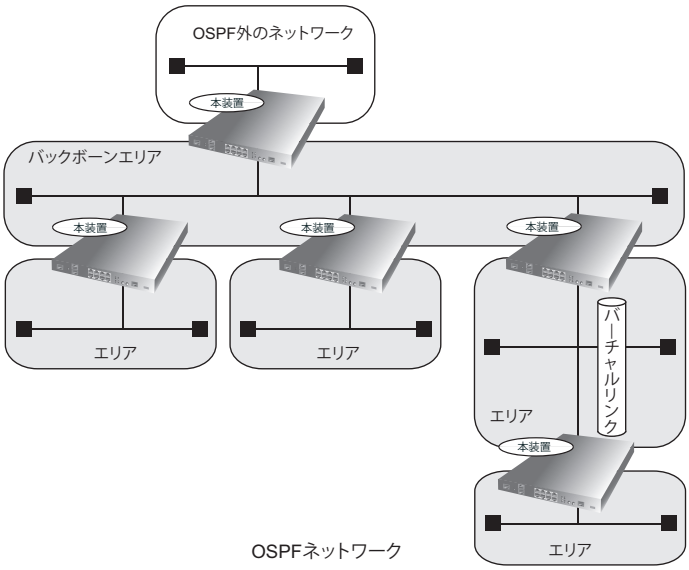
2.7 OSPF 機能

OSPF（Open Shortest Path First）は、大規模ネットワークに適したルーティングプロトコルです。

OSPF はリンクステート方式を使用して、各ルータが自装置に接続されているリンクの状態やコストなどの情報を LSA（Link State Advertisement）として広報します。また、各ルータは、受信した LSA でネットワーク構成の情報を持つ LSDB（Link State Data Base）を作成することにより最適な経路を決定します。

OSPF では、ネットワーク全体をエリアという単位で分割して管理します。OSPF ネットワークは、1 つのバックボーンエリアとその他のエリアから構成されます。バックボーンエリアにその他のエリアを接続し、各エリア間の LSA の交換は、バックボーンエリアを経由して行われます。

OSPF ネットワークは、OSPF 以外の経路情報を取り入れることができます。また、スタブエリア、準スタブエリアを設定して、OSPF 以外の経路情報数を削減することができます。



OSPF を使用するルータは、運用により以下のルータとして動作します。

- エリア境界ルータ（Area Border Router）
  エリア間に設置されたルータです。エリア間での LSA の交換を行います。エリア内の LSA は集約して広報することができます。
- AS 境界ルータ（AS Border Router）
  OSPF 以外の経路情報をエリア内に取り入れるルータです。OSPF 以外の経路情報を LSA に変換し、エリア内に広報します。OSPF 以外の経路情報を集約して広報することや、デフォルトルートを広報することができます。
- 内部ルータ（Internal Router）
  エリア内のルータです。自装置の OSPF を使用するインタフェースやコストの情報を広報します。
  マルチアクセスネットワーク（ポイント・ツー・ポイント以外のネットワーク）では、内部ルータを指定ルータ（Designated Router）として動作させる必要があります。指定ルータは、ほかのルータの代表として LSA の交換を行います。また、指定ルータのバックアップとして副指定ルータを動作させておくことができます。
- バックボーンルータ（Backbone Router）
  バックボーンエリアのルータです。機能は内部ルータと同じです。

本装置でサポートしている OSPF 機能は、以下の RFC（Request For Comments）に準拠しています。

- RFC1587:The OSPF NSSA Option
- RFC2328:OSPF Version 2

本装置でサポートする OSPF 機能

項目	サポート内容
OSPF バージョン	バージョン 2 をサポート
ルータ種別	バックボーンルータ、エリア境界ルータ、AS 境界ルータ、内部ルータをサポート
エリアタイプ	スタブエリア、準スタブエリアをサポート
エリア境界ルータでの経路集約	サポート
AS 境界ルータでの経路集約	サポート
AS 境界ルータでのデフォルトルート広報	サポート（NSSA 内部の AS 境界ルータを除く）
Passive-Interface	サポート
認証	テキスト認証、MD5 認証をサポート
OSPF への再配布	以下の経路情報の再配布をサポート • インタフェース経路情報（ループバックインタフェースアドレスを含む） • スタティック経路情報 • RIP 経路情報 • BGP 経路情報 経路情報種別ごとに、再配布するかどうかを指定できます。
OSPF 経路の他プロトコルへの広報	RIP、BGP での広報をサポート
ECMP 機能	サポート
再配布フィルタリング	以下のフィルタリングをサポート • AS 境界ルータでの AS 外部経路に対する経路情報単位の透過／遮断 • 透過経路のメトリック値／メトリックタイプの変更
サマリ LSA 入出力可否	エリア境界ルータで、サマリ LSA の入出力時の透過／破棄を指定可能

⚠注意

OSPF 機能を使用する場合、定期的にパケットを送信します。このため、定額制でない回線を使用している場合は、超過課金の原因となることがあります。このような環境では、**OSPF** 機能は使用しないでください。

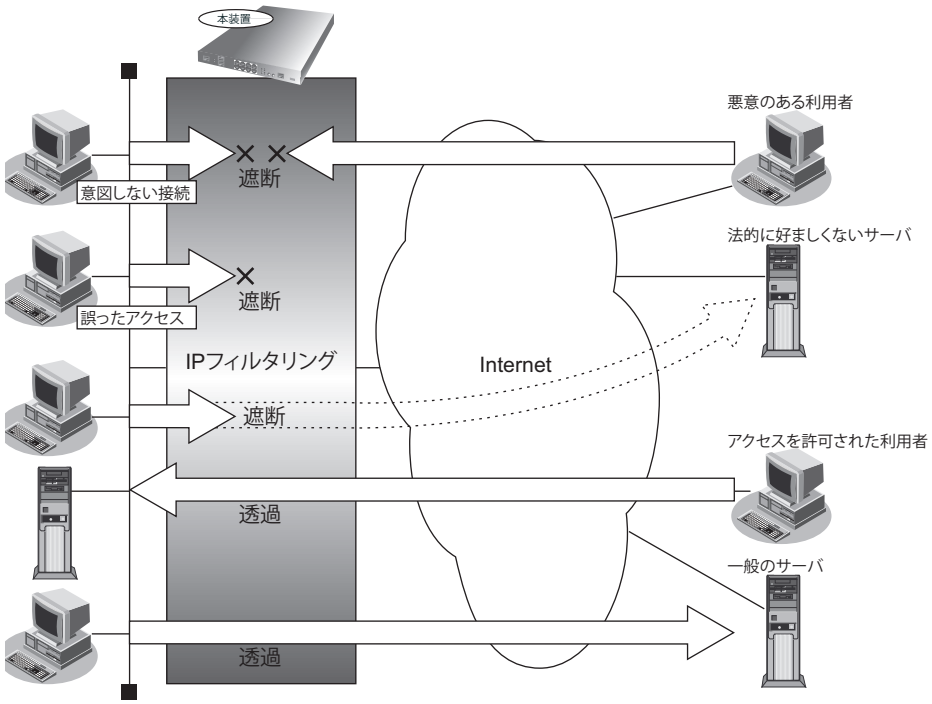
こんな事に気をつけて

- NAT 機能と併用することはできません。
- OSPF を使用できるインタフェースには上限があります。OSPF を使用するインタフェースの合計が本装置の上限を超えないように設定する必要があります。

2.8　IP フィルタリング機能

本装置は、IP フィルタリング機能やパスワードの設定などを使って、ネットワークのセキュリティを向上させることができます。

IP フィルタリング機能とは、本装置を経由してインターネットに送出されるパケット、またはインターネットから受信したパケットを IP アドレスとポート番号の組み合わせで制御することによって、ネットワークのセキュリティを向上させたり、回線への超過課金を防止することができます。



ネットワークのセキュリティを向上させるには、以下の要素について考える必要があります。

- ネットワークのセキュリティ方針
- ルータ以外の要素（ファイアーウォール、ユーザ認証など）

こんな事に気をつけて

本装置などのルータでは、コンピュータウィルスの感染を防ぐことはできません。パソコン側でウィルス対策ソフトを使用するなど、別の手段が必要です。

補足　NAT 機能にも、セキュリティを向上させる効果があります。

接続形態に応じてセキュリティ方針を決める

インターネットに接続する場合でも LAN 同士を接続する場合でも、データの流れには「外部から内部へ」、「内部から外部へ」という 2 つの方向があります。セキュリティ方針を決める場合は、2 つの方向について考慮する必要があります。

● 「外部から内部へ」流れるデータに対するセキュリティ方針の例

- インターネット（ネットワーク型接続）の場合
  特定のパケットを受け取らないようにする

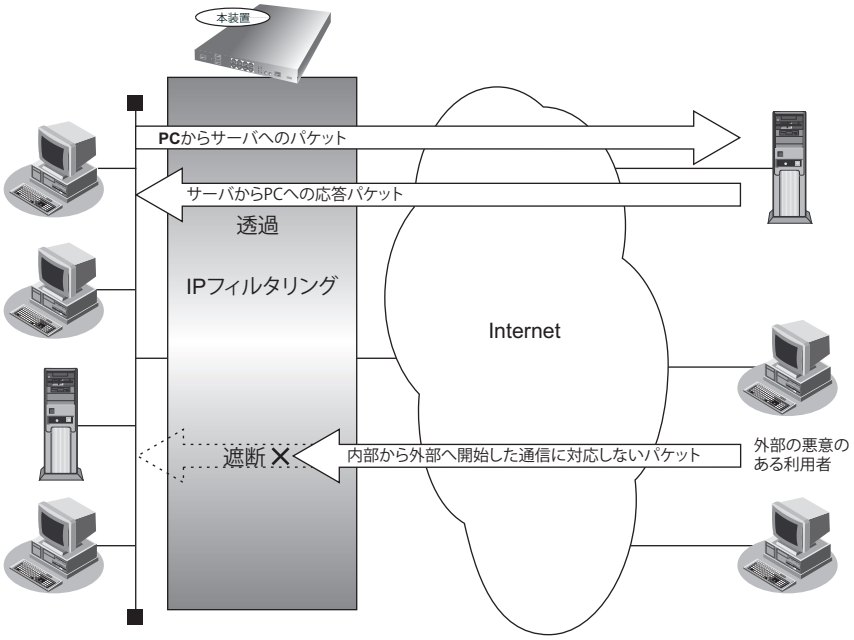
- インターネットの場合
  非公開ホストへのアクセスを拒否する
- LAN同士を接続する場合
  内部ユーザによる不要なアクセスを防ぐ

● 「内部から外部へ」流れるデータに対するセキュリティ方針の例

- インターネットの場合
  法的に問題のあるサイトなどへのアクセスを制限する
- LAN同士を接続する場合
  内部ユーザによる不要なアクセスを防ぐ

2.8.1 Stateful Packet Inspection（SPI）

SPIは内部から外部へ通信を開始すると、これに対応するフィルタリングルールを自動的に作成し、外部からの応答パケットを透過させます。また、フィルタリングルールに対応しない外部から内部への通信を開始したパケットを遮断することができます。



補足 ブロードキャストアドレスやマルチキャストアドレスあてにSPIでフィルタリングを行うことはできません。DHCP、RIPおよびRIPv2などブロードキャストアドレスを用いる通信をSPIと併用する場合は、これらの通信を透過させるフィルタリングルールを設定してください。

SPIによるフィルタリングは、構成定義で設定されたIPフィルタリングよりも先に行われます。

2.9 ポリシールーティング機能

ポリシールーティング機能とは、転送パケットの宛先 IP アドレスだけではなく、送信元 IP アドレスやポート番号などの情報（ポリシー）も利用して、転送先を選定する機能です。この機能を利用することによって、それぞれの通信内容に通信パスを分離することができます。

NAT の処理後にポリシールーティング処理が行われます。フィルター、Qos の設定がされている場合、フィルター、Qos の処理が優先されます。

パケットの処理の順番は、最初にフィルタ、次に QoS、最後に NAT の順で処理されます。

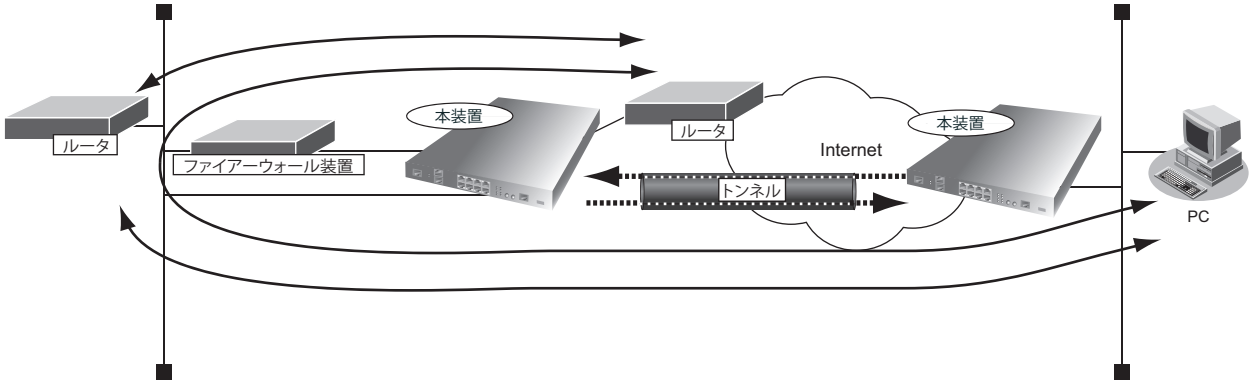
本装置では、IP ルーティングによる転送先選定の前にポリシーに応じた転送先選定を行う Ingress ポリシールーティングが利用できます。

2.9.1 Ingress ポリシールーティング機能

Ingress ポリシールーティング機能とは、ルーティングによる経路情報の参照前に、入力パケットの宛先 IP アドレスだけではなく、送信元 IP アドレスやポート番号などの情報も利用して、設定した送出先へパケットを転送する機能です。この機能を利用することによって、受信インタフェースごとに経路情報に従わないパケット転送を行うことができます。

例）インターネットから内部 LAN へのパケットはファイアーウォールを通し、VPN 接続先からのパケットはファイアーウォールを通さないで通信する

VPN 接続先からインターネット、インターネットから VPN 接続先へのパケットを内部 LAN のファイアーウォールを通して通信する



接続先監視

Ingress ポリシールーティングでは、ポリシーに指定した送出先ルータが回線切断や再起動などで通信不能状態になっていた場合、そのポリシーに一致したパケットは通信できなくなります。

接続先監視を設定することで、送出先ルータの通信状態を検出できます。通信できない場合は、そのポリシーを使用せずに、以降のポリシーや経路情報に従ったルーティングを行うことで、通信を復旧させることができます。

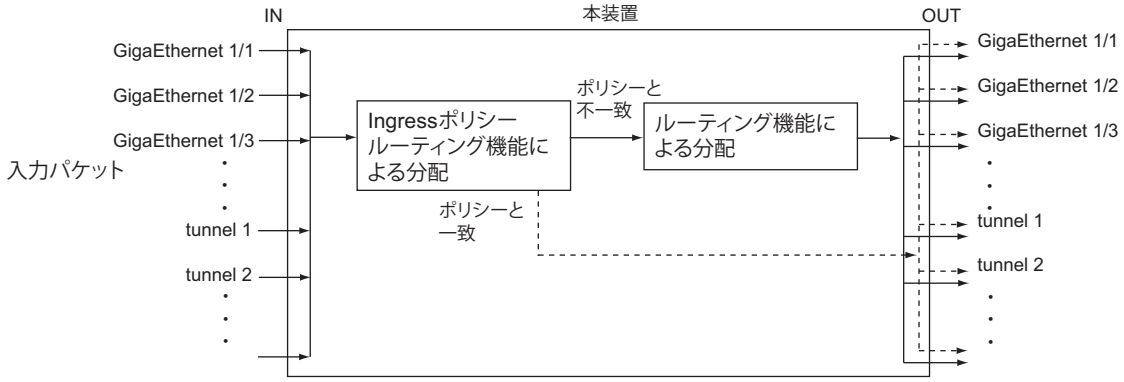
こんな事に気をつけて

接続先監視を使用すると、相手ノードに ICMP ECHO パケットを定期的に送信します。このため、定額制ではない回線を使用している場合は、超過課金の原因となることがあります。このような環境では、接続先監視を使用しないでください。

通常の IP ルーティングと Ingress ポリシールーティングの関係

IP ルーティングでの送信先選定では、経路情報に従って出力先インタフェースを選定します。

Ingress ポリシールーティング機能は、IP ルーティングによる送信先選定前に、入力パケットの IP アドレス・プロトコル番号などの情報をもとに出力先インタフェースを選定し、経路情報を無視してパケットを出力します。



利用する定義の選定方法

ここでは、それぞれの送信データに対して、利用する定義の選定方法を説明します。

ポリシールートマップ内の複数のクラス定義は、モード内で設定されるシーケンス番号の低いものから順に利用するかどうかを判断します。

同じシーケンス番号の場合は、名前順に利用するかどうかを判断します。

利用するクラス定義がない場合、経路情報に従います。

このクラスの定義に一致し、送出先に指定したインタフェースが有効な場合、そのインタフェースに転送します。

一致したクラス定義で指定したインタフェースが無効な場合や、接続先監視に通信不能が検出されていた場合、そのクラスは無視され、次の優先順位のクラスを検索します。

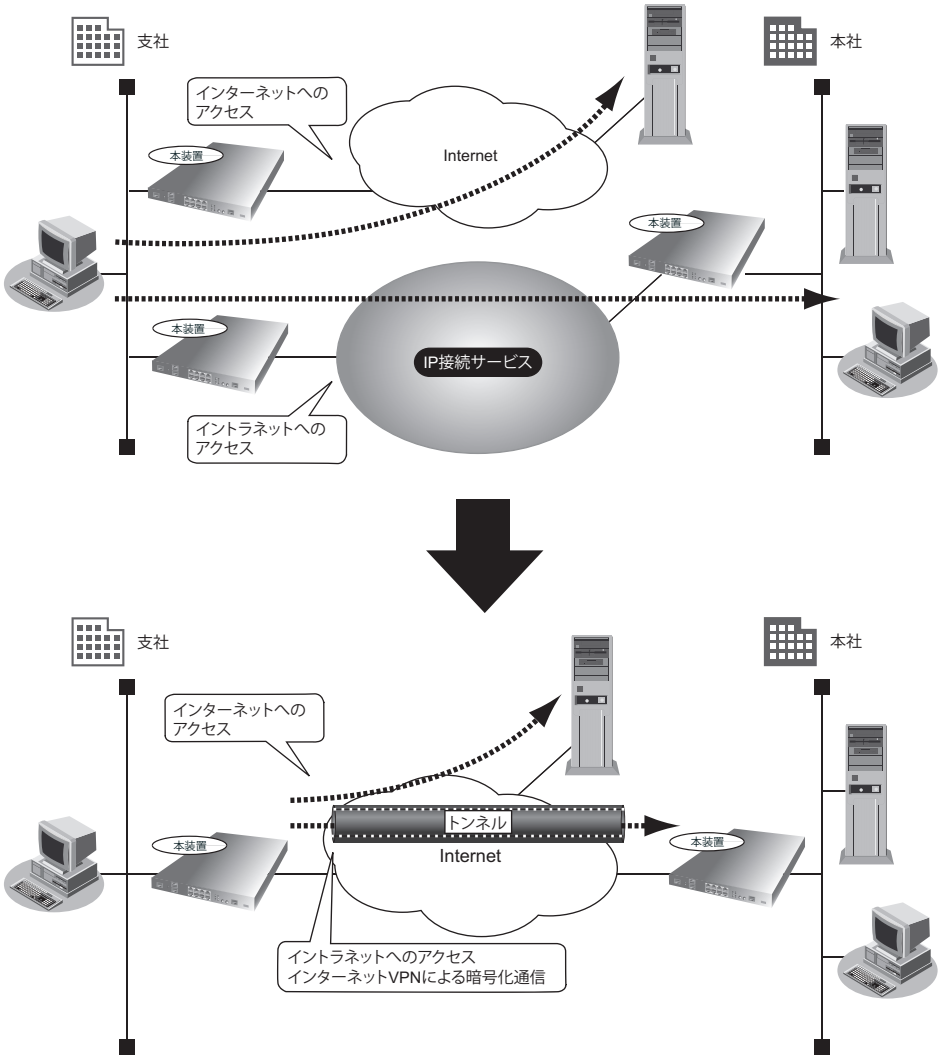
こんな事に気をつけて

Ingress ポリシールーティング機能は、パケット選択ルールに一致した場合、ブロードキャストパケットやマルチキャストパケット、自ルータあてパケットも転送します。

2.10 IPsec 機能

VPN（Virtual Private Network）とは、インターネットのように公衆で利用されているネットワークに、通信パスを仮想的に設定することによって専用線のように使用することができる技術です。最近ではインターネットを利用して VPN を構築する、インターネット VPN のこと自体を VPN ということもあります。

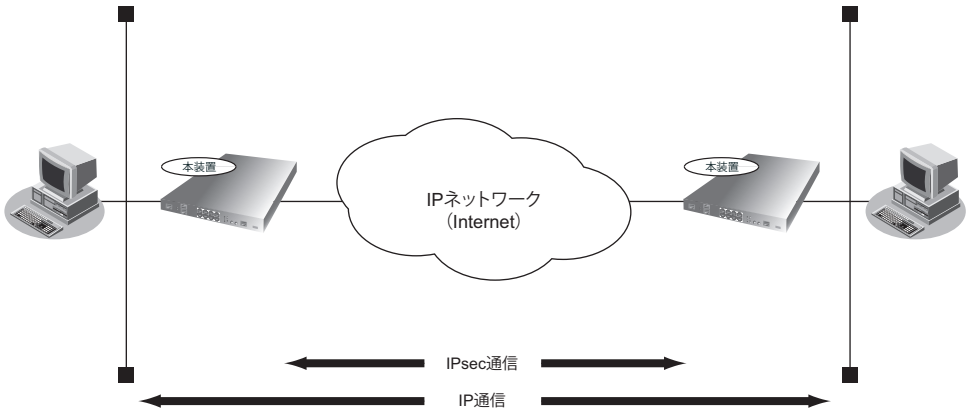
VPN では VPN 装置間でデータをカプセリングし、相手の VPN 装置に送信します。その際、データの盗聴、改ざんを防止するために、認証や暗号化などのセキュリティ機能によりデータを保護します。これにより、簡単に機密性の高いシステムが構築できます。



本装置ではVPNを実現するためにIPsecというプロトコルを使用します。

IPsecで使用できる機能は2つあります。IPパケットに認証用のヘッダを付けて認証する機能AHと、暗号化したあとに認証してカプセル化する機能ESPです。

IPsecには、IPヘッダを認証／暗号化しないトランスポートモードとIPヘッダを認証／暗号化するトンネルモードの2つのモードがあります。本装置はトンネルモードだけをサポートしているため、ここではトンネルモードだけを説明します。



本装置でサポートする **IPsec** の範囲

本装置がサポートするIPsecの範囲は、以下のとおりです。

項目	**IPsec** の範囲
IPsec適用範囲	ESP、認証付ESP
自動鍵交換バージョン	IKE Version1、IKE Version2
鍵設定／鍵交換方式	自動鍵交換：IKE Version1（Main Mode、Aggressive Mode、Quick Mode） 自動鍵交換：IKE Version2（IKE SA INIT交換、IKE AUTH交換、CREATE CHILD SA交換）
自動鍵交換（IKE）認証方式	共有鍵認証（Pre-Shared Key）方式、デジタル署名認証方式（RSA、ECDSA）、 EAP認証方式
セキュリティパケット送信方法	トンネルモード（IPv4 over IPv4、IPv4 over IPv6、IPv6 over IPv4、IPv6 over IPv6） トランスポートモード（L2TP/IPsec、EtherIP over IPsec、IPinIP over IPsec、GRE over IPsecにて適用可）
暗号アルゴリズム	3DES-CBC、DES-CBC、AES-CBC、AES-GCM、NULL
認証アルゴリズム	HMAC-MD5、HMAC-SHA1、HMAC-SHA2（256,384,512）、認証なし 認証アルゴリズムと認証アルゴリズムモードの主な特徴 MD5 ：シンプルで認証が早い SHA1：セキュリティが強いが、認証が遅い SHA2：SHA1よりセキュリティが強化されている

本装置でサポートするIPsec機能は、以下の新プロトコルのRFCに準拠します。

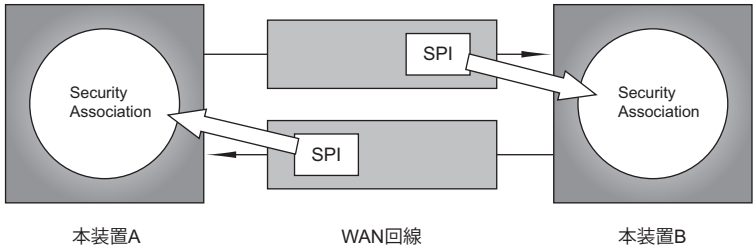
- RFC2104: "HMAC: Keyed-Hashing for Message Authentication"
- RFC2401: "Security Architecture for the Internet Protocol"
- RFC2402: "IP Authentication Header"
- RFC2403: "The Use of HMAC-MD5-96 within ESP and AH"
- RFC2404: "The Use of HMAC-SHA1-96 within ESP and AH"
- RFC2405: "The ESP DES-CBC Cipher Algorithm With Explicit IV"

- RFC2406: "IP Encapsulating Security Payload (ESP)"
- RFC2407: "The Internet IP Security Domain of Interpretation for ISAKMP"
- RFC2408: "Internet Security Association and Key Management Protocol(ISAKMP)"
- RFC2409: "The Internet Key Exchange (IKE)"
- RFC2411: "IPsecurity Document Roadmap"
- RFC3394: "Advanced Encryption Standard (AES) Key Wrap Algorithm"
- RFC3706: "A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers"
- RFC4301: "Security Architecture for the Internet Protocol"
- RFC4303: "IP Encapsulating Security Payload (ESP)"
- RFC4306: "Internet Key Exchange (IKEv2) Protocol"
- RFC4868: "Using HMAC-SHA256, HMAC-SHA384, and HMAC-SHA512 with IPsec"

Security Association と Security Parameters Index

IPsec の特徴は、認証・暗号化のアルゴリズムや鍵管理のしくみを IPsec のプロトコル自体から切り離したことです。IPsec で通信するホスト同士は、通信する前になんらかの方法で認証・暗号化のアルゴリズムや使用する鍵を決定して、その情報を共有する必要があります。この関係を SA（Security Association）と言います。

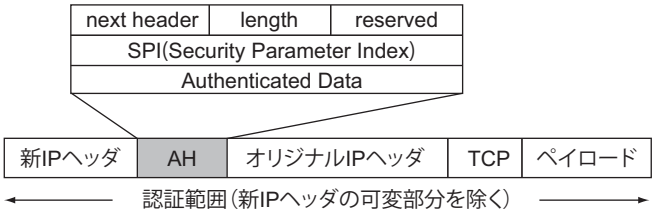
1 つのホストは複数の通信に対応するための複数の SA を持っています。このため、受け取った IPsec のパケットが、どの SA に対応するものなのかを識別する必要があります。識別するためのパラメタとして、あとに説明する AH や ESP のヘッダ中に含まれる SPI（Security Parameter Index）を使用します。



AH ヘッダと ESP ヘッダ

IPsec では、IP パケットのオプションヘッダに、認証には AH（Authentication Header）ヘッダを、暗号化および認証には ESP（Encapsulating Security Payload）ヘッダを使用しています。

IP パケット認証（AH:Authentication Header）



AH は IP パケットを認証するために IP ヘッダに拡張されるものです。元々ある IP パケットの前に IPsec ゲートウェイのアドレスと上記の構成からなる AH ヘッダを挿入します。

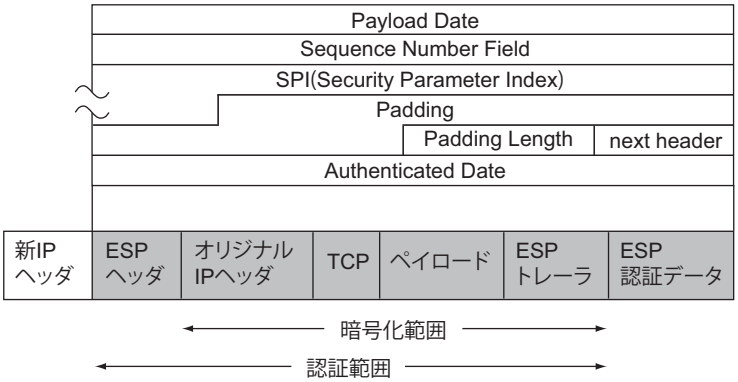
AH は認証アルゴリズム・認証キー・暗号アルゴリズム・暗号キー・キー寿命・キー配送方法などを決める SPI 値と、認証アルゴリズムで使用するデータ・フィールド Authenticated Data から成り立っています。

送信する側は、オリジナルの IP パケットと認証鍵からハッシュ関数を使って圧縮したものを Authenticated Data に書き込んで送信します。

受信する側は、SPI の情報で相手先を特定します。その相手先と同じ暗号鍵および認証アルゴリズムを使用して送信する側と同様の計算を行います。AH ヘッダ内の Authenticated Data と一致した場合に、相手を認証したと判断します。

認証に使用する認証鍵およびハッシュ関数などは、SA データベースにあらかじめ登録しておきます。SA とは、暗号に必要な認証方式や認証鍵などのデータが入っているデータ構造のことです。

IP パケット暗号化（ESP:Encapsulating Security Payload）



ESP は IP パケットを認証（IP パケットの改ざんチェック）だけではなく、IP パケットを暗号化します。

共有鍵認証（**Pre-Shared Key**）方式と **RSA** デジタル署名認証方式

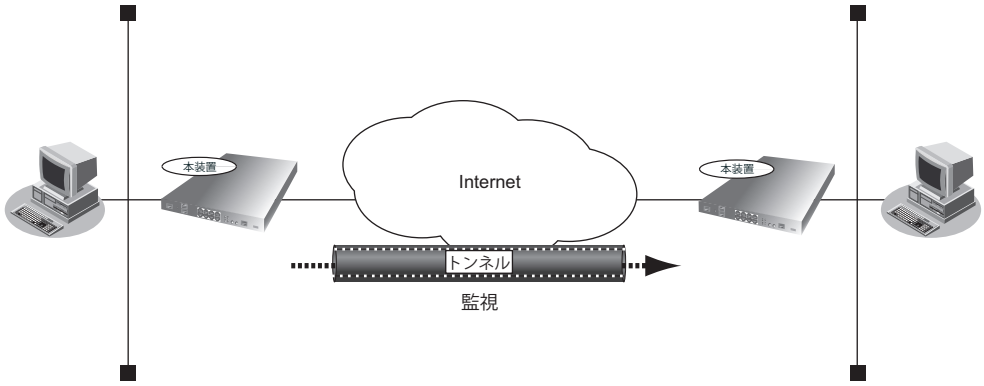
自動鍵交換（IKE）で、通信する相手の認証（本人性確認）を行います。本装置では、以下の 3 つの認証方式をサポートします。

- 共有鍵認証（Pre-Shared Key）方式
  パスワードによる認証方式です。双方の装置で決めたパスワードを設定し、IKE ネゴシエーション中にそのパスワードを使用して、通信する相手が正しいことを確認します。
- RSA デジタル署名認証方式
  IKE のネゴシエーションを行う双方の装置で、自身の秘密鍵を使用した署名データを作成し、IKE ネゴシエーション中に相手装置の公開鍵を使用して認証を行い、正しい相手であることを確認します。この認証のために使用する公開鍵は、第三者機関によって証明することにより、共有鍵認証方式よりも信頼性の高い相手認証が行えます。
- EAP 認証（Pre-Shared Key）
  IKE Version2 でのみ使用可能な認証方式です。
  ユーザ ID およびパスワードによる認証方式です。相手装置と同一のユーザ ID およびパスワードを設定し、IKE ネゴシエーション中にそのユーザ ID およびパスワードを使用して、通信する相手が正しいことを確認します。

接続先監視

IPsec 通信の場合、回線の切断や相手装置の再起動によって相手装置の SA が削除されることがあります。このとき、相手装置の SA が削除されたことを検出することができないため、通信できない状態になります。

接続先監視を使用することにより、IPsec トンネルを経由して相手装置の SA が削除されていることを検出します。IPsec 通信できない場合は、SA を再作成することによって、通信を復旧させることができます。



こんな事に気をつけて

- 接続先監視を使用すると、相手ノードに ICMP ECHO パケットを定期的に送信します。このため、定額制でない回線を使用している場合は、超過課金の原因となることがあります。このような環境では、接続先監視を使用しないでください。
- 接続先監視を使用する場合は、監視対象となる相手ノードおよび自装置のアドレスが IPsec 対象範囲に含まれる必要があります。IPsec 対象範囲に含まれない場合は、接続先監視のパケットが破棄され、IPsec 通信ができません。
- Dead Peer Detection（DPD）機能と併用する場合に接続先監視トラフィック（ICMP）は通信対象となります。

IKE の NAT トラバーサル

IPsec/IKE では、IPsec 装置または IPsec トンネル区間の装置に対して NAT を適用すると、IKE ネゴシエーションで失敗するなど通信ができません。

IPsec 通信を行うパケットのヘッダは、ポート番号を持たないため、NAT によるポート変換機能を使用できません。このため、IKE は送信元／宛先ポート番号を固定とする必要があります。

IKE の NAT トラバーサル機能を使用すると、これらが解消されて NAT を介しての IKE ネゴシエーションおよび IPsec 通信ができるようになります。

補足 ポート番号を変化させない NAT で、スタティックに ESP パケットを通過させるような場合は、NAT トラバーサルを使用しなくても IPsec 通信ができます。

本装置がサポートする IKE の NAT トラバーサル機能は、以下の RFC およびドラフトに準拠します。

- "Negotiation of NAT-Traversal in the IKE"
  RFC3947,
  draft-ietf-ipsec-nat-t-ike-03,
  draft-ietf-ipsec-nat-t-ike-00
- "UDP Encapsulation of IPsec ESP Packets"
  RFC3948
  draft-ietf-ipsec-udp-encaps-00.txt

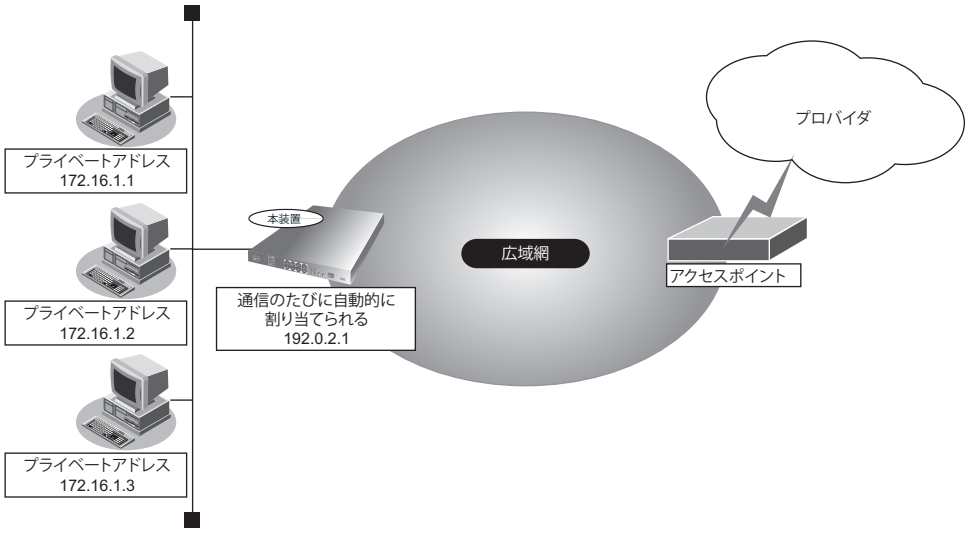
マルチポイント SA（MPSA）機能

センターを経由しない拠点間通信を 1 つの SA で行うための、マルチポイント SA 機能をサポートしています。下記ページの技術資料「マルチポイント SA についての機能概要」にまとめておりますので、ご参照ください。

URL: https://www.furukawa.co.jp/fitelnet/product/technical/index.html

2.11 NAT 機能

NAT 機能（アドレス変換機能）とは、LAN 内に接続された複数台のパソコンで使用するプライベートアドレスを、本装置に割り当てたグローバルアドレスに変換する機能です。NAT 機能を使用すると、限られた数のグローバルアドレスでそれ以上の数のパソコンを接続できます。たとえば、端末型接続でプロバイダから提供される 1 台分のグローバルアドレスを使って、複数台のパソコンからインターネットに接続できます。また、LAN 内に接続されたパソコンのプライベートアドレスは、外部から認識できないため、不正なアクセスを遮断できます。



補足
- プライベートアドレスとグローバルアドレスについて
  プライベートアドレスとは、ユーザが自由に割り当てることができる IP アドレスです。
  グローバルアドレスとは、インターネット上のホストを識別するために、InterNIC などのアドレス管理機構から割り当てられる世界で唯一の IP アドレスです。プロバイダ接続の場合はプロバイダから提供されます。
- LAN 同士を接続する場合（事業所間など）、両方プライベートアドレスとなることがあります。本装置では、WAN 側のアドレスをグローバルアドレス、LAN 側のアドレスをプライベートアドレスとしています。
- 「端末型接続」と「ネットワーク型接続」はインターネットに接続する際の IP アドレスの割り当て方が異なります。
  端末型接続は、接続先に接続するたびに、プロバイダからグローバルアドレスが動的に割り当てられます。
  ネットワーク型接続は、LAN を単位として接続する形態で、あらかじめプロバイダからグローバルアドレスが割り当てられます。プロバイダ接続の場合は契約時の申し込み台数に応じてグローバルアドレスが割り当てられます。

本装置の NAT 機能は、Port-channel インタフェースおよび Tunnel インタフェース（PPPoE, IPsec）で動作します。

本装置の NAT 機能は、以下の 3 つの機能で構成されます。

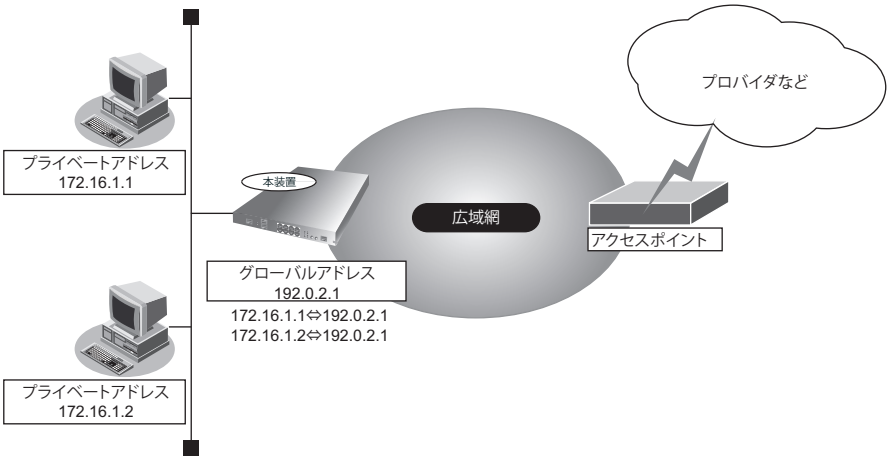
- 動的 NAT
- 静的 NAT
- NAT 宛先変換

こんな事に気をつけて

IP パケットのフラグメントが発生する環境の場合は、フラグメントされた先頭パケットより前に後続パケットを受信すると、そのフラグメントパケットは破棄され、正常に通信できない場合があります。

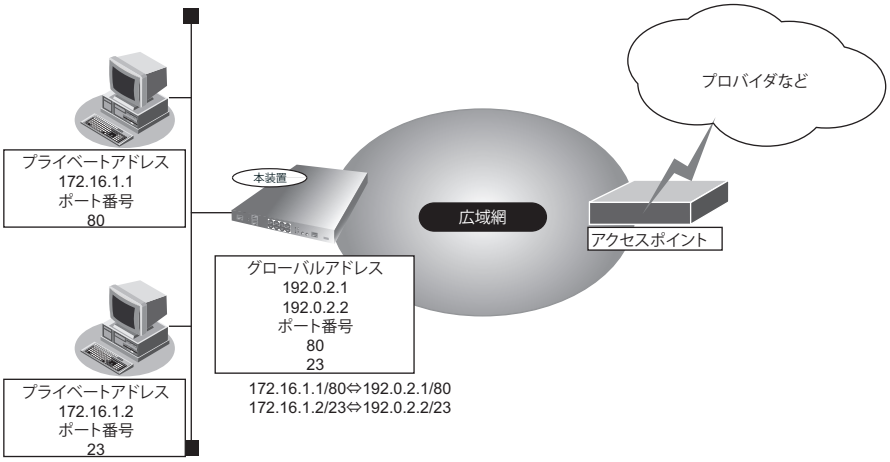
◆ 動的 **NAT** とは

「動的 NAT」を使用すると、使用可能なグローバルアドレスの個数以上のパソコンが同時に接続できます。



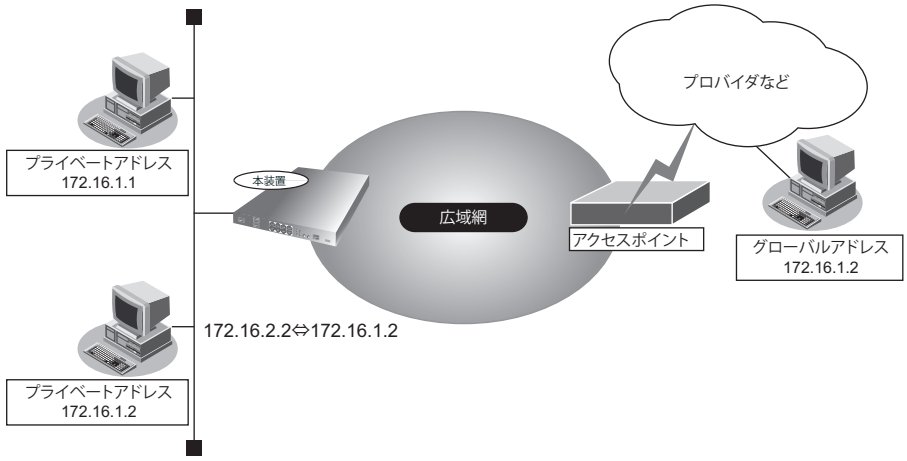
◆ 静的 **NAT** とは

LAN 上の Web サーバを公開するような場合、「静的 NAT」を使用すると、特定のパソコンやアプリケーションの IP アドレス、ポート番号に絞って公開可能です。



◆ **NAT** 宛先変換とは

通常の NAT では、外部と通信するために送信元のプライベートアドレスをグローバルアドレスに変換します。「宛先変換」では、外部のアドレスを変換することでグローバル側のホストにプライベートアドレスを割り当てます。そのため、外部の IP アドレスを隠蔽したり、プライベートアドレスとアドレスが重複するセグメントへ通信できます。



2.11.1 NAT 機能の選択基準

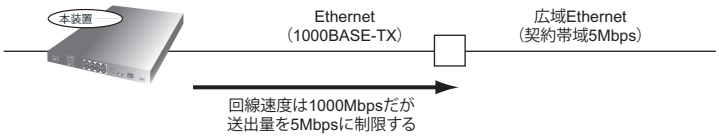
ネットワーク環境および使用目的によって、適切な NAT 機能を設定する必要があります。選択基準を以下に示します。

NAT 機能が必要な場合

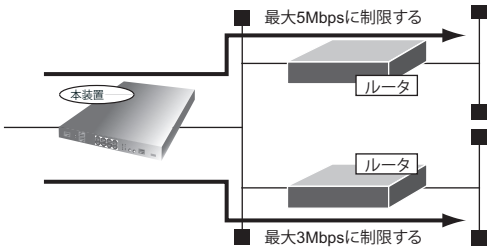
- プロバイダから割り当てられたグローバルアドレスより多くのパソコン（端末）を接続する場合（ここでいう端末には本装置も含まれます）
- 既存のネットワークのアドレスをそのまま使用する場合
- 自側のネットワークのアドレスを隠す場合
  - 動的 NAT が必要な場合
    - 同時に接続するパソコンの台数がグローバルアドレス数を超える場合
  - 静的 NAT が必要な場合
    - 外部にサービスを公開する場合（WWW サーバ、FTP サーバなど）
    - IP アドレスを意識して動作するアプリケーションを使用する場合

2.12 シェーピング機能

シェーピング機能とは、回線に送出するデータ量（帯域）を制限する機能です。この機能を利用することで、実際の回線の帯域ではなく、指定した帯域でデータ送信などができます。



また、シェーピング対象とするパケットの条件を指定することで、宛先ネットワークごとに送出帯域の制限などができます。



こんな事に気をつけて

シェーピング機能は、以下のインタフェース種別で動作します。

- ギガビットイーサネットインタフェース
- IPsec tunnelインタフェース
- PPPoE tunnel インタフェース
- IPinIP tunnelインタフェース

2.13 帯域制御（WFQ）機能

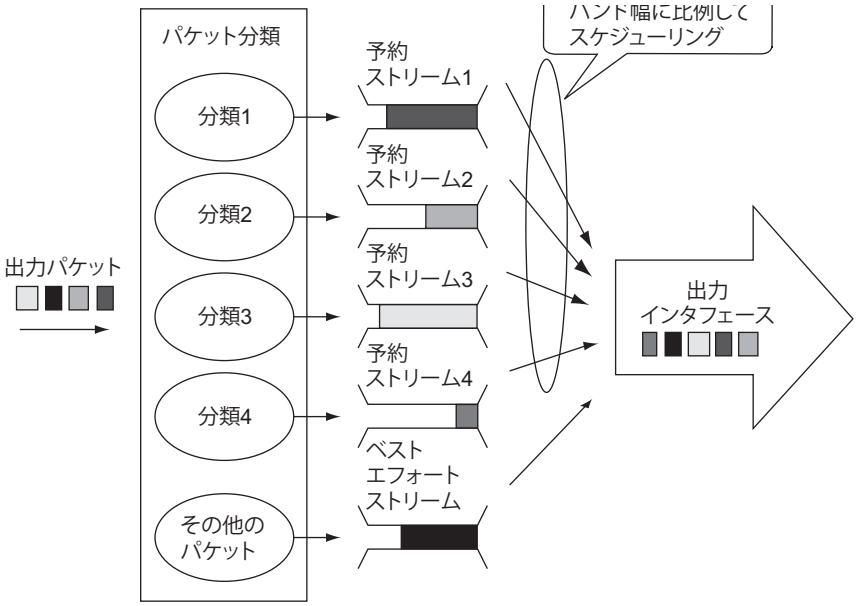
WFQ機能とは、回線上に流れる特定のデータの帯域を予約する機能です。

WFQ機能は予約したバンド幅の比率に応じて、出力パケットをスケジューリングします。

データストリームには、以下の3種類があります。

- エクスプレスストリーム
  常に最優先で送信するデータストリームをエクスプレスストリームと言います。
- 予約ストリーム
  帯域を予約したデータストリームを予約ストリームと言います。バンド幅（帯域幅）は、1Kbps単位または%で指定します。
- ベストエフォートストリーム
  エクスプレスストリームと予約ストリームが使用していないバンド幅を使用するデータフローをベストエフォートストリームと言います。

予約ストリームと予約フィルタ



出力パケットがどの予約ストリームに属するのかを判別する条件では、送信先IPアドレス、宛先ポート番号、送信元IPアドレス、送信元ポート番号、およびプロトコル番号などを指定できます。この条件に一致する出力パケットの属する予約ストリームを設定します。

2.13.1 トラフィックがあるストリーム数によるバンド幅の変動

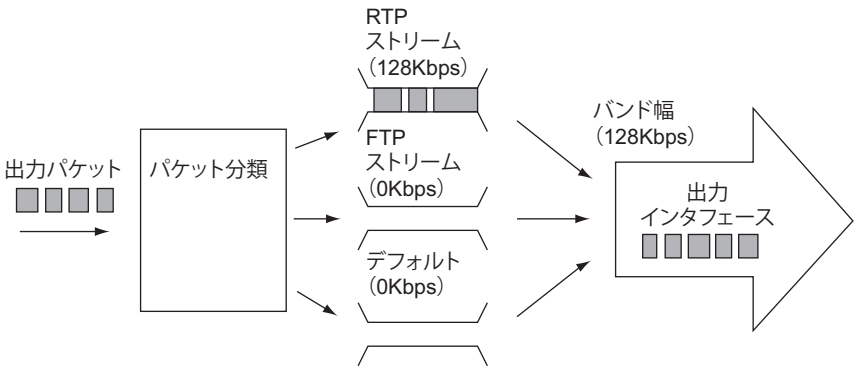
各ストリームが利用できるバンド幅は、トラフィックがあるストリーム数によって変動します。
以下の条件を設定している場合を例に説明します。

● **WFQ** の設定

- インタフェース：バンド幅＝ 128Kbps
- RTP ストリーム：バンド幅＝ 32Kbps
- FTP ストリーム：バンド幅＝ 16Kbps
- デフォルトストリーム：バンド幅＝ 80Kbps

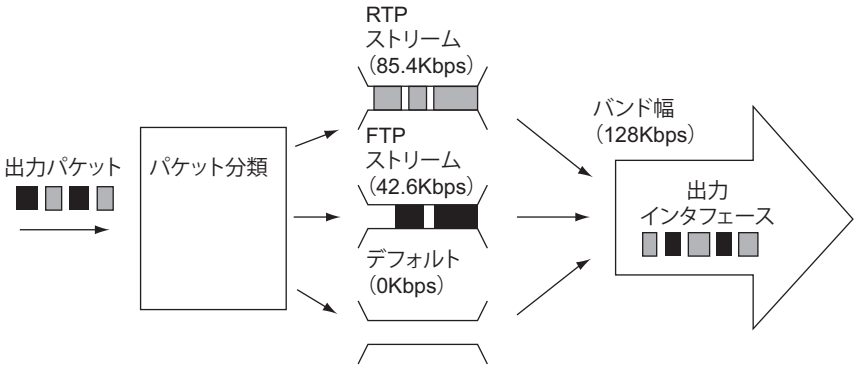
1 つのストリームにトラフィックがある場合

3 つのストリームのうち、1 つのストリームにだけトラフィックがある場合、その 1 つのストリームがインタフェースのすべての帯域を使用します。
以下のように RTP ストリームにだけトラフィックがある場合、128Kbps のすべて帯域を使用することができます。



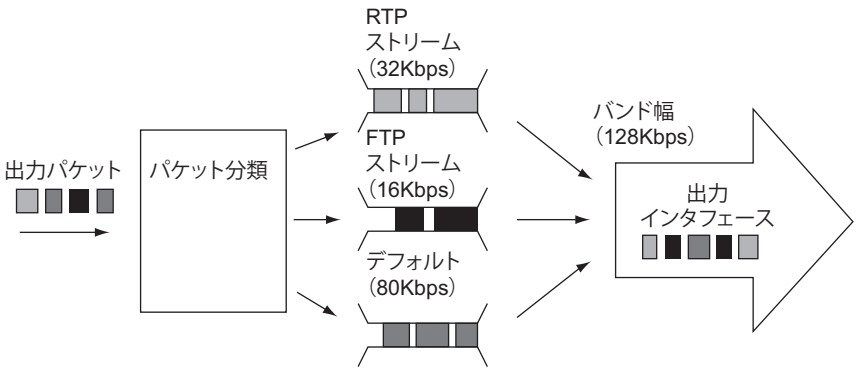
2 つのストリームにトラフィックがある場合

以下のように RTP ストリームと FTP ストリームにトラフィックがあります。デフォルトストリームにトラフィックがない場合、トラフィックがあるストリームの予約バンド幅の比率でパケットをスケジューリングします。
RTP ストリームと FTP ストリームの予約バンド幅の比率が 32：16 の場合、この比率で 128Kbps の帯域を分割します。RTP ストリームは 85.4Kbps、FTP ストリームは 42.6Kbps の帯域を使用することができます。



3つのストリームすべてにトラフィックがある場合

すべてのストリームにトラフィックがある場合は空いている帯域はありません。予約したバンド幅に従ってパケットをスケジューリングします。



こんな事に気をつけて

予約ストリームに設定するバンド幅は100%以上の負荷がかかったときの最大帯域であり、ほかのストリームが使用していない場合は空いている帯域を使って通信できます。

2.14 DHCP 機能

DHCP 機能は、IPv4 DHCP 機能と IPv6 DHCP 機能があります。

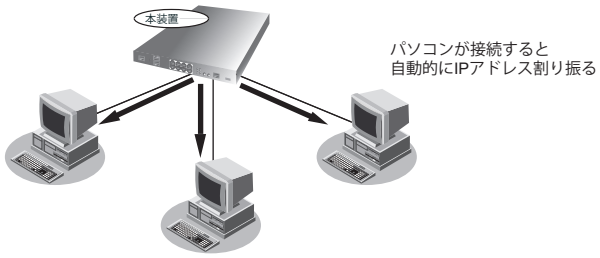
以下に、それぞれの機能について説明します。

2.14.1 IPv4 DHCP 機能

IPv4 DHCP 機能は、IP アドレスなどの情報を端末に割り振ったり（サーバ機能）、DHCP サーバから IP アドレスなどの情報を取得したり（クライアント機能）、DHCP サーバから配布される情報を遠隔地の DHCP クライアントに中継する（リレーエージェント機能）機能です。

DHCP サーバ機能

DHCP サーバ機能とは、IP アドレスなどの情報を端末に動的に割り振る機能です。この機能を使用して、DHCP クライアント機能を持っている端末に IP アドレスを自動的に割り当てます。割り当てた IP アドレスは、クライアントの MAC アドレスと対応付けして管理します。したがって、本装置配下の LAN に DHCP クライアント機能を持つ端末を接続する場合は、端末側に IP アドレスを設定する必要はありません。Windows では DHCP クライアント機能をサポートしています。

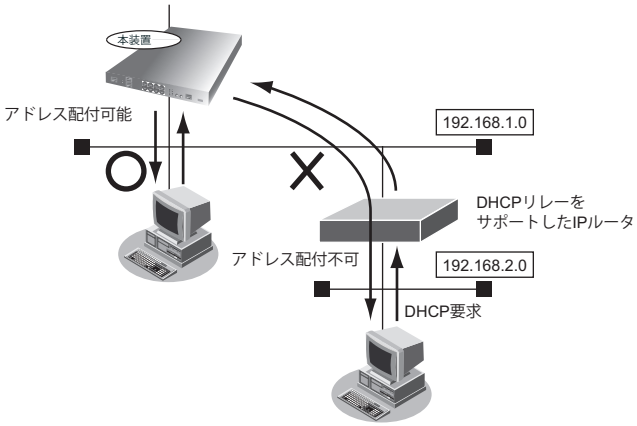


本装置はクライアントに IP アドレスを割り振る場合、ARP パケットにより、すでに特定の IP アドレスを割り当てられているホストが存在しないかどうかをチェックします。これにより、IP アドレスが重複する危険性を取り除くことができます。

実際の設定では、端末に割り当てる IP アドレスの範囲（最初の IP アドレスと最後の IP アドレス）を設定します。本装置の IP アドレスの割り当て個数は、マニュアル「仕様一覧」を参照してください。

こんな事に気をつけて

本装置の DHCP サーバ機能は、DHCP サーバ機能を有効にしたインタフェースのネットワークだけに IP アドレスを配布することができます。DHCP リレーをサポートした IP ルータを中継して、IP アドレスを配布することはできません。



以下に、本装置の DHCP サーバ機能の設定内容を示します。

オプション／設定	設定範囲	意味
Subnet Mask	本装置では設定不要	サブネットマスク 本機能が有効になっているインタフェースのサブネットマスクを使用するため、設定は不要です。
Router Option	IP アドレス（IPv4）	デフォルトゲートウェイ
Domain Name Server Option	IP アドレス（IPv4）	プライマリ DNS サーバアドレス セカンダリ DNS サーバアドレス
Network Time Protocol Servers Option	IP アドレス（IPv4）	NTP サーバアドレス
Time Server Option	IP アドレス（IPv4）	TIME サーバアドレス
WINS Server Option	IP アドレス（IPv4）	WINS サーバアドレス
SIP Server Option	IP アドレス（IPv4） または、 80 文字以内の英数字、"-"、"." （"." の間は、63 文字まで）	プライマリ SIP サーバアドレス セカンダリ SIP サーバアドレス または、 プライマリ SIP サーバドメイン名 セカンダリ SIP サーバドメイン名
Domain Name	80 文字以内の英数字、"-"、"." （"." の間は、63 文字まで）	ドメイン名
割り当てる IP アドレスの範囲 （割り当て開始アドレス／割り当て終了アドレス）	IP アドレス（IPv4）	割り当て開始アドレス（最初に割り当てを行うアドレス）と割り当て終了アドレス（割り当てるアドレスの範囲の最後のアドレス）を設定します（最大 2000 個）。 本装置のインタフェースのアドレスが範囲に含まれていても、除外されます（割り当てに使用されません）。
割り当て時間	1 ～ 31536000 秒 無限	リース期間 infinity と設定すると、リース期間が無限になります。
任意オプション	オプションコード（1 ～ 254）とデータ（127 バイト、16 進数表記）	オプションコードとオプション内容を設定することで、任意の DHCP 標準オプションをクライアントに配布することができます（最大 4 つ）。

DHCP クライアント機能

DHCP クライアント機能は、DHCP サーバから IP アドレスなどの情報を取得する機能です。使用する場合は、DHCP サーバが動作しているネットワークに接続する必要があります。利用者は、IP アドレスを意識することなくネットワークを利用できます。

本装置の DHCP クライアント機能は、以下の情報を受け取って動作します。

- IP アドレス
- ネットマスク
- リース期間
- デフォルトルータの IP アドレス
- SIP サーバ IP アドレス
- SIP ドメイン名
- NTP サーバの IP アドレス
- リース更新時間

本装置では、スタティック経路情報の設定を行うことで、デフォルトルータの IP アドレスを受け取り、その IP アドレスをデフォルトルートや任意の宛先にできます。

参照 スタティック経路情報の設定については、マニュアル「コマンドリファレンス」の「ip route」を参照してください。

DHCP リレーエージェント機能

DHCP クライアントは、同じネットワーク上にあるサーバから、IP アドレスなどの情報を獲得することができます。

DHCP リレーエージェントは、遠隔地にある DHCP クライアントの要求を DHCP サーバが配布する情報を中継する機能です。この機能を利用することで、遠隔地の別のネットワークに DHCP サーバが存在する場合も同様に情報を獲得することができます。

2.14.2 IPv6 DHCP 機能

IPv6 DHCP 機能は、IPv6 プレフィックスなどの情報を IPv6 DHCP クライアントに配布したり（サーバ機能）、プロバイダの IPv6 DHCP サーバから IPv6 プレフィックスなどの情報を取得したり（クライアント機能）、異なるネットワークにある IPv6 DHCP クライアントと IPv6 DHCP サーバ間を中継する（リレーエージェント機能）機能です。

IPv6 DHCP サーバ機能

本装置では、IPv6 DHCP サーバ機能を使用して、IPv6 アドレス、IPv6 プレフィックスとパラメタの配布をサポートしています。

以下に、IPv6 DHCP サーバ機能で配布できる項目および配布数を示します。

項目	配布数
動的に割り当てる IPv6 アドレス	2000
静的に割り当てる IPv6 アドレス	ホストデータベース定義数
IPv6 プレフィックス	1
DNS サーバアドレス	2
DNS ドメイン名	1
SIP サーバアドレス	2
SIP ドメイン名	2
SNTP サーバアドレス	2
任意オプション（オプションコードとオプション内容を設定）	4

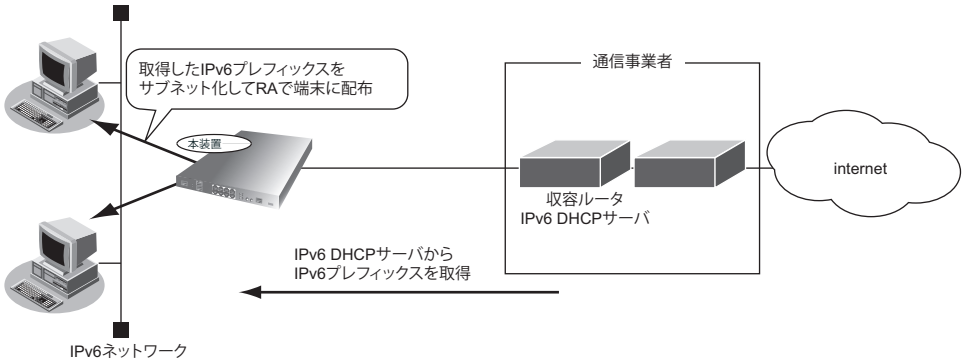
こんな事に気をつけて

本装置の IPv6 DHCP サーバ機能は、本装置に接続されたネットワークだけに配布することができます。
IPv6 DHCP リレーエージェントを中継して配布することはできません。

IPv6 DHCP クライアント機能

本装置では、IPv6 DHCP クライアント機能を使用して、IPv6 プレフィックスとパラメタの取得をサポートしています。

本機能を利用すると、プロバイダから取得した IPv6 プレフィックスをサブネット化して、Router Advertisement Message（RA）で下流ネットワークに 64 ビットの IPv6 プレフィックスを配布することができます。



本装置では、インタフェースごとに IPv6DHCP クライアントが機能し、最大 20 インタフェースまで可能です。

以下に、IPv6 DHCP クライアント機能で取得できる項目および取得数を示します。

項目	取得数（各 **DHCP Client** ごと）
IPv6 プレフィックス	1
SIP サーバアドレス	1
SIP ドメイン名	1
SNTP サーバアドレス	1

こんな事に気をつけて

SIP サーバアドレス、SIP ドメインは NGN 網に接続する場合のみに有効となります。

IPv6 DHCP リレーエージェント機能

IPv6 DHCP リレーエージェントは、異なるネットワークにある IPv6 DHCP クライアントと IPv6 DHCP サーバ間を中継する機能です。この機能を利用することで、遠隔地の別のネットワークに IPv6 DHCP サーバが存在する場合も情報を獲得することができます。

本装置でサポートする IPv6 DHCP 機能は、以下の RFC（Request For Comments）に準拠しています。

- RFC3315：Dynamic Host Configuration Protocol for IPv6（DHCPv6）
- RFC3319：Dynamic Host Configuration Protocol （DHCPv6）Options for Session Initiation Protocol （SIP） Servers
- RFC3633：IPv6 Prefix Options for Dynamic Host Configuration Protocol（DHCP）version 6
- RFC3646：DNS Configuration options for Dynamic Host Configuration Protocol for IPv6（DHCPv6）
- RFC3898：Network Information Service（NIS）Configuration Options for Dynamic Host Configuration Protocol for IPv6（DHCPv6）

- RFC4075：Simple Network Time Protocol（SNTP）Configuration Option for DHCPv6
- RFC4704：The Dynamic Host Configuration Protocol for IPv6（DHCPv6）Client Fully Qualified Domain Name（FQDN）Option

以下に、本機能でサポートする IPv6 DHCP メッセージを示します。

○：サポートする、×：サポートしない

IPv6 DHCP メッセージ	クライアント機能	サーバ機能
Solicit	○	○
Advertise	○	○
Request	○	○
Confirm	×	○
Renew	○	○
Rebind	○	○
Reply	○	○
Release	○	○
Decline	×	○
Information-Request	○	○

以下に、本機能でサポートする IPv6 DHCP オプションを示します。

○：サポートする、×：サポートしない

IPv6 DHCP オプション	クライアント機能	サーバ機能
OPTION_CLIENTID	○	○
OPTION_SERVERID	○	○
OPTION_IA_NA	×	○
OPTION_IA_ADDR	×	○
OPTION_ORO	○	○
OPTION_PREFERENCE	○	○
OPTION_ELAPSED_TIME	○	○
OPTION_STATUS_CODE	○	○
OPTION_SIP_SERVER_D	○	○
OPTION_SIP_SERVER_A	○	○
OPTION_DNS_SERVERS	○	○
OPTION_DOMAIN_LIST	○	○
OPTION_IA_PD	○	○
OPTION_IAPREFIX	○	○
OPTION_SNTP_SERVERS	○	○
OPTIONS_PREFIXDEL	×	×
OPTIONS_PREFIX_INFO	×	×

2.15 DNSサーバ機能

DNSサーバ機能とは、受信したDNS要求に対して、上位DNSサーバ（たとえば、プロバイダのDNSサーバ）への問い合わせを行わずに、本装置に設定したDNS情報（IPアドレス、ドメイン名）を返すことができる機能です。

DNSサーバ機能を使用する場合、端末にはDNSサーバアドレスとして本装置のインタフェースのIPアドレスを設定します。端末がDHCPクライアントの場合は、DHCPサーバは通知するDNSサーバアドレスとして本装置のインタフェースのIPアドレスを通知する必要があります。

本装置には、以下の2種類のDNSサーバ機能があります。

- DNSサーバ（スタティック）機能
- ProxyDNS（DNS振り分け）機能

補足
- 端末からのDNS問い合わせに対して、装置自身のDNS設定（ip name-serverに設定）のDNSサーバアドレスに問い合わせすることはありません。問い合わせ先を明示的に設定する必要があります。
- 本装置のDNSの解決（たとえばsshコマンド実行時の接続先ホスト名からアドレスを解決する処理）でも、本装置のDNSサーバ機能（DNS振り分け）を利用したい場合は、ip name-serverで127.0.0.1を設定します。

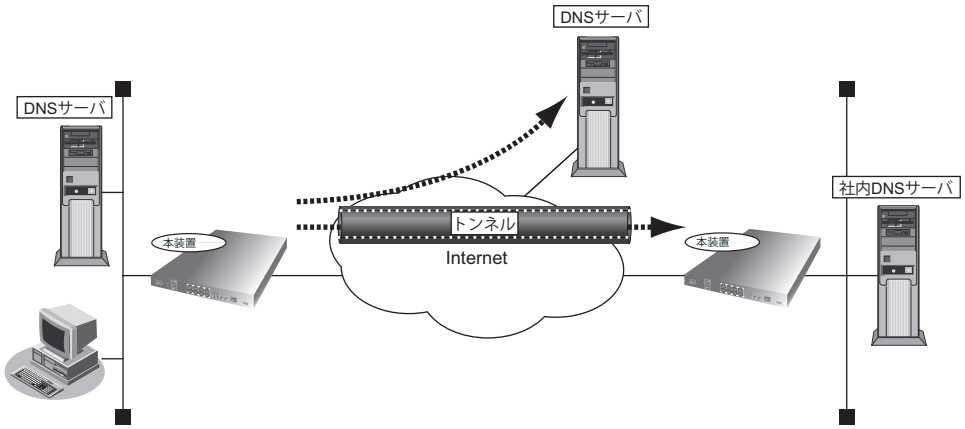
2.15.1 DNSサーバ（スタティック）機能

ドメイン名（FQDN：Fully Qualified Domain Name）とIPアドレスの組を静的に設定します。DNSクライアントからの問い合わせ（正引き、逆引き）に対し、設定したエントリを検索し、該当エントリが見つかった場合は応答します。見つからなかった場合は、上位DNSサーバに問い合わせます。逆引き（IPアドレスから名前を応答）する場合は、応答パケット内に含まれるTYPEとCLASSを、TYPE=A（1 a host address）、CLASS IN（1 the Internet）固定とします。

スタティックテーブルは最大で64エントリです。

2.15.2 ProxyDNS（DNS振り分け）機能

ProxyDNS（DNS振り分け）機能は、DNSサーバとして問い合わせられたドメイン名（正引き）またはIPアドレス（逆引き）により、本装置が問い合わせするDNSサーバを自動的に割り振ることができます。そのため、DNSサーバを使い分けることで、以下のような環境をリモートサイト側に実現できます。



本装置が端末からDNSのQueryメッセージを受信した場合、DNS振り分け設定内に、問い合わせ先のドメイン名と一致するエントリが存在するかどうかをチェックします。一致するエントリが存在する場合は、その一致したエントリのDNSアドレスにメッセージを転送します。一致するエントリが存在しない場合は、DNSのQueryメッセージは、廃棄されます。

DNS振り分け設定にはそれぞれ2つまでのDNSサーバを定義することができ、同時にメッセージを転送することで冗長化を行います。複数のサーバからの応答のうち、先に受信できたものが端末に転送されます。

問い合わせされたドメイン名と設定されたドメイン名を比較し、すべての文字列が一致している場合に、エントリと一致したと判断します。また、"＊"は、0文字以上の任意の文字列を表すものとして扱い（"＊"の箇所の比較を行わずに)、他の部分が一致すれば一致したと判断します。

設定例）

- ドメイン名 : DNSサーバアドレス
- www.example.co.jp : 1.1.1.1
- ftp.example.co.jp : 2.2.2.2
- *.is.fuku.example.co.jp : 3.3.3.3

IPCPまたはDHCPにより相手から通知されたDNSサーバアドレスを問い合わせ先にする設定も行うことができます。

DNS振り分けテーブルは最大32エントリです

2.16 SNMP機能

SNMP（Simple Network Management Protocol）とは、IP層およびTCP層レベルの情報を収集、管理するためのIP管理用のプロトコルです。

SNMP機能では、管理する装置をSNMPマネージャ、管理される装置をSNMPエージェントと言います。

SNMP機能でネットワークを管理する場合、管理する側はSNMPマネージャ機能を、管理される側はSNMPエージェント機能をサポートしている必要があります。

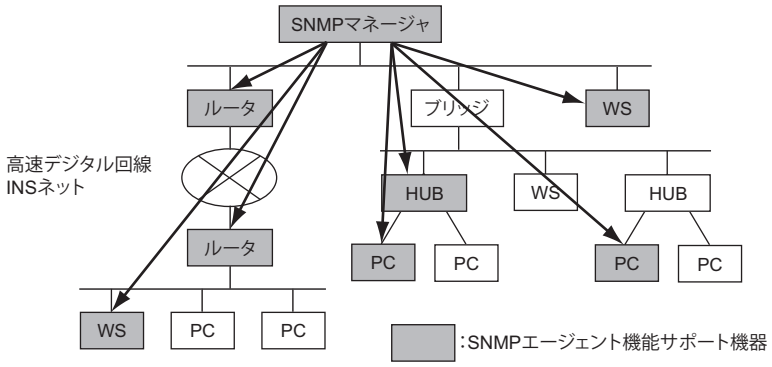
SNMPマネージャ機能は、ネットワーク上の端末の稼動状態や障害状態を一元管理します。SNMPエージェント機能は、SNMPマネージャの要求に対してMIB（Management Information Base：管理情報ベース）という管理情報を返します。

SNMP機能は、この2つの機能を使用して、SNMPマネージャとSNMPエージェントとの間でMIBに定義されたパラメタを送受信してネットワークを管理します。

本装置では、SNMPv1、SNMPv2cおよびSNMPv3をサポートします。また、標準MIBおよび古河拡張MIBをサポートしています。

参照 マニュアル「仕様一覧」

SNMP機能による管理



◆ **MIB**とは

MIBには、装置のベンダに関係ない標準MIBと装置ベンダ固有の拡張MIBがあります。RFC1213などで定義される標準MIBは、管理ノードのそれぞれの管理対象（オブジェクト）にアクセスするための仮想の情報領域です。RFCでは、SNMPエージェントが実装すべき管理情報を定義しています。管理情報には、SNMPノードとしてのシステム情報（システム名や管理者名など）やTCP/IPに関連する統計情報があります。しかし、RFCで定義されている項目では伝送路やHUBなどを十分に管理できません。このため、各種プロトコルの情報や各社の装置ごとのベンダ固有に合わせてMIBを拡張します。これを拡張MIBと言います。

MIBはASN.1（Abstract Syntax Notation 1）という形式で定義します。SNMPマネージャが拡張MIBを管理するためには、SNMPエージェント側でその拡張MIBを公開して、SNMPマネージャがその拡張MIBの情報を収集するように定義する必要があります。

2.16.1 ifIndex の割り当てと ifDescr

本装置での ifIndex の割り当て、および対応する ifDescr を以下に示します。

- 分類

ifIndex	定義／回線との対応
100000000	null インタフェース
200000000 ～	loopback インタフェース
300000000 ～	port-channel インタフェース
401010000 ～	gigaethernet インタフェース
501010000 ～	VLAN インタフェース
800010000 ～	trunk-channel インタフェース
900010000 ～	trunk VLAN インタフェース
1000000001 ～	tunnel インタフェース
1200000001 ～	bridge-group
1300000001 ～	usb-ethernet インタフェース

- 装置実回線との対応

ifIndex	ifDescr	回線との対応
401010000 ～	GigaEthernet X/Y	gigaethernet インタフェース (ifIndex=400000000+(1000000*X)+(10000*Y))

- 論理インタフェースとの対応

ifIndex	ifDescr	定義との対応
100000000	Null 0	null インタフェース
200000000 ～	Loopback X	loopback インタフェース (ifIndex=200000000+X)
300000000 ～	Port-channel X	port-channel インタフェース (ifIndex=300000000+X)
501010000 ～	GigaEthernet X/Y.Z (Z はサブインタフェースインデックス番号)	VLAN インタフェース (ifIndex=500000000+(1000000*X)+(10000*Y)+Z)
800010000 ～	Trunk-channel X	trunk-channel インタフェース (ifIndex=800000000+(10000*X))
900010000 ～	Trunk-channel X.Y (Y はサブインタフェースインデックス番号)	trunk VLAN インタフェース (ifIndex=900000000+(10000*X)+Y)
1000000001 ～	Tunnel X	tunnel インタフェース (ifIndex=1000000000+X)
1200000001 ～	Bridge-group X	bridge-group (ifIndex=1200000000+X)

2.16.2 imrscMonitorDataによるCP/NP/SP/App使用率の表示

本装置ではimrscMonitorData（infMgtResourceMonitorMIB グループ）により、CP/NP/SP/App各種使用率の情報を取得することが可能です。各オブジェクト識別子と表示内容の対応を以下に示します。

デフォルトの表示

- CP（コントロールプレーン）使用率

オブジェクト識別子	表示内容	対応する**show processes cpu**の情報
imrscMonitorData.101.7	最近5秒間のトータルCP（CPU0）使用率	CPU0 five seconds:
imrscMonitorData.101.8	最近1分間のトータルCP（CPU0）使用率	CPU0 one minute:
imrscMonitorData.101.9	最近5分間のトータルCP（CPU0）使用率	CPU0 five minutes:

- NP（ネットワークプロセッサ）使用率

オブジェクト識別子	表示内容	対応する**show processes cpu**の情報
imrscMonitorData.201.7	最近5秒間のトータルNP（CPU1）使用率	CPU1 five seconds:
imrscMonitorData.201.8	最近1分間のトータルNP（CPU1）使用率	CPU1 one minute:
imrscMonitorData.201.9	最近5分間のトータルNP（CPU1）使用率	CPU1 five minutes:
imrscMonitorData.201.10	最近5秒間のトータルNP（CPU2）使用率	CPU2 five seconds:
imrscMonitorData.201.11	最近1分間のトータルNP（CPU2）使用率	CPU2 one minute:
imrscMonitorData.201.12	最近5分間のトータルNP（CPU2）使用率	CPU2 five minutes:

- App（コンテナ）使用率

オブジェクト識別子	表示内容	対応する**show processes cpu**の情報
imrscMonitorData.601.7	最近5秒間のトータルApp（CPU3）使用率	CPU3 five seconds:
imrscMonitorData.601.8	最近1分間のトータルApp（CPU3）使用率	CPU3 one minute:
imrscMonitorData.601.9	最近5分間のトータルApp（CPU3）使用率	CPU3 five minutes:

dp coreコマンドでコアの割り当てを変更した時の表示

- CP（コントロールプレーン）使用率

オブジェクト識別子	表示内容	対応する**show processes cpu**の情報
imrscMonitorData.101.7	最近5秒間のトータルCP（CP1コア目のCPU）使用率	CPUx five seconds:
imrscMonitorData.101.8	最近1分間のトータルCP（CP1コア目のCPU）使用率	CPUx one minute:
imrscMonitorData.101.9	最近5分間のトータルCP（CP1コア目のCPU）使用率	CPUx five minutes:
imrscMonitorData.101.10	最近5秒間のトータルCP（CP2コア目のCPU）使用率	CPUy five seconds:
imrscMonitorData.101.11	最近1分間のトータルCP（CP2コア目のCPU）使用率	CPUy one minute:
imrscMonitorData.101.12	最近5分間のトータルCP（CP2コア目のCPU）使用率	CPUy five minutes:
imrscMonitorData.101.13	最近5秒間のトータルCP（CP3コア目のCPU）使用率	CPUz five seconds:
imrscMonitorData.101.14	最近1分間のトータルCP（CP3コア目のCPU）使用率	CPUz one minute:
imrscMonitorData.101.15	最近5分間のトータルCP（CP3コア目のCPU）使用率	CPUz five minutes:

- NP（ネットワークプロセッサ）使用率

オブジェクト識別子	表示内容	対応する**show processes cpu**の情報
imrscMonitorData.201.7	最近5秒間のトータルNP（NP1コア目のCPU）使用率	CPUx five seconds:
imrscMonitorData.201.8	最近1分間のトータルNP（NP1コア目のCPU）使用率	CPUx one minute:
imrscMonitorData.201.9	最近5分間のトータルNP（NP1コア目のCPU）使用率	CPUx five minutes:
imrscMonitorData.201.10	最近5秒間のトータルNP（NP2コア目のCPU）使用率	CPUy five seconds:
imrscMonitorData.201.11	最近1分間のトータルNP（NP2コア目のCPU）使用率	CPUy one minute:
imrscMonitorData.201.12	最近5分間のトータルNP（NP2コア目のCPU）使用率	CPUy five minutes:

- SP（セキュリティプロセッサ）使用率

オブジェクト識別子	表示内容	対応する**show processes cpu**の情報
imrscMonitorData.301.7	最近5秒間のトータルSP（SP1コア目のCPU）使用率	CPUx five seconds:
imrscMonitorData.301.8	最近1分間のトータルSP（SP1コア目のCPU）使用率	CPUx one minute:
imrscMonitorData.301.9	最近5分間のトータルSP（SP1コア目のCPU）使用率	CPUx five minutes:

- App（コンテナ）使用率

オブジェクト識別子	表示内容	対応する**show processes cpu**の情報
imrscMonitorData.601.7	最近5秒間のトータルApp（App1コア目のCPU）使用率	CPUx five seconds:
imrscMonitorData.601.8	最近1分間のトータルApp（App1コア目のCPU）使用率	CPUx one minute:
imrscMonitorData.601.9	最近5分間のトータルApp（App1コア目のCPU）使用率	CPUx five minutes:
imrscMonitorData.601.10	最近5秒間のトータルApp（App2コア目のCPU）使用率	CPUy five seconds:
imrscMonitorData.601.11	最近1分間のトータルApp（App2コア目のCPU）使用率	CPUy one minute:
imrscMonitorData.601.12	最近5分間のトータルApp（App2コア目のCPU）使用率	CPUy five minutes:

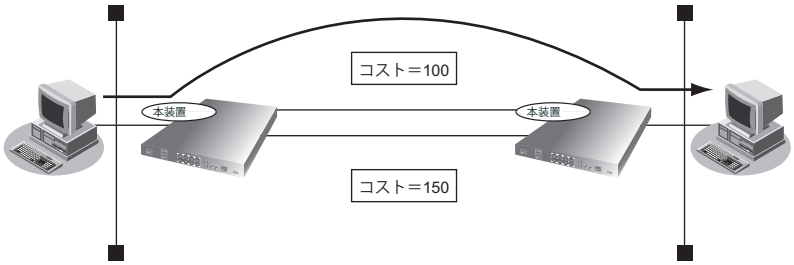
2.17 ECMP 機能

経路として設定された 1 つのネットワークに対して到達可能な通信パスが複数ある場合、ルーティングによる転送先は、一般的にその通信コストを考慮して、もっとも通信コストの小さい通信パスを決定します。

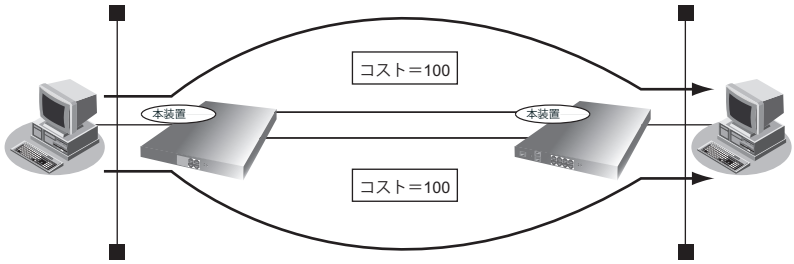
ECMP(Equal Cost Multi Path) 機能は、同じ通信コストのパスを複数同時に利用できる機能です。この機能によって、同じ宛先ネットワークにパケットを送信する場合に、同じ通信コストのパスを併用して、通信パスの負荷を分散できます。

通信パスは、最大 8 つまで同時に利用できます。

- 一般的なルーティング（通信コストが最小の通信パスだけを利用する場合）



- ECMP 機能によるルーティング（同じ通信コストの通信パスを同時利用する場合）



ECMP 機能では、スタティックルーティングによる経路設定、または OSPF/BGP を利用した経路学習を行った場合に、複数の通信パスを同時に利用することができます。

スタティックルートと OSPF, BGP を併用した複数パスは構成できません。以下は、独立して設定されます。

- スタティックルートの範囲で構成される複数の通信パス
- OSPF の範囲で構成される複数の通信パス
- BGP の範囲で構成される複数の通信パス

同じ経路に対してスタティックルートと OSPF, BGP の複数の通信パスが存在した場合は、「2.4.1 IP 経路情報の種類」（P.29）で示した優先度設定に基づいて、いずれかの通信パスが決定されます。また、ECMP として扱われる条件は、それぞれ下記の通りです。

- スタティックルーティングの場合
  経路優先度およびメトリック値が同じスタティックルートは ECMP として同時に利用されます。
- OSPF を利用する場合
  通信パスの経路計算によって同じ通信コストとなった場合に、ECMP として同時利用されます。
- BGP を利用する場合
  コマンドリファレンス構成定義編の「bgp multi-path」コマンドをご参照ください。

参照 マニュアル「コマンドリファレンス」の「bgp multi-path」

本装置では、再帰的な経路検索で複数回の経路検索を行う場合に、経路検索ごとにECMP機能を使って通信パスを振り分けることが可能です。このようなケースでは最大8×8の64パスまで通信パスを増やすことが可能です。

こんな事に気をつけて

- 特定の通信セッションを特定の通信パスに意図的に通すことはできません。利用する通信パスは、パケット転送時に決定されます。また、通信パス数が変化すると、利用される通信パスが変更されることがあります。
- NAT機能とECMP機能を併用することはできません。また、ECMP機能によって負荷を分散した通信パスの途中経路で、NAT機能によってアドレス変換を動作させることはできません。NAT機能を利用する場合は、それぞれの通信セッションが同じ通信パスを利用し続けることが必要です。ただし、ECMP機能を利用して負荷を分散した場合、同じ通信パスを利用し続けることができなくなることがあります。
- PPPoE通信、IPトンネル通信で常時接続機能を利用しない接続先との通信パスは、認証失敗などの理由で通信できない場合でも通信パスの異常が検出できません。このため、ECMP機能の通信パスに利用しないでください。正常に通信できなくなる場合があります。

2.17.1 通信パス選択方法

ECMP機能では、どの複数の通信パスでパケットを転送するのかを決定するのにハッシュ方式を用います。

ハッシュ方式は、送出パケットの内容によって、利用する通信パスを選択します。この方法を利用した場合、同じホスト間の通信は同じ通信パスを利用します。このため、パケットの転送順は保証されますが、通信パスの負荷は偏る場合があります。

また、本装置では再帰的な経路検索で複数回の経路検索を行う場合に、経路検索ごとにECMP機能を使って通信パスを振り分けることが可能です。このような多段のECMP機能を使った場合により多くの通信パスを利用できるよう、2つのハッシュ値を生成して通信パスを選択します。

本装置では、以下の順序で通信パスを選択します。

(1) 転送パケットの送信元IPアドレスと宛先IPアドレスを、32ビットの値として加算します。

(2) (1) の結果の上位16ビットの値と下位16ビットの値を加算し、桁上がりを無視して16ビットの値を算出します。

(3) (2)の結果の上位8ビットの値と下位8ビットの値を加算し､桁上がりを無視して8ビットの値を算出します。

(4) (3) の結果のビット0～2（ハッシュ値1）およびビット4～6（ハッシュ値2）をハッシュ値として抽出します。

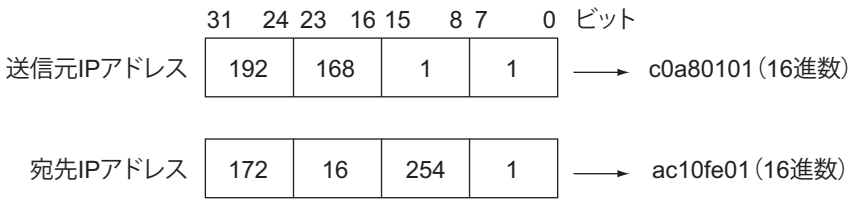
(5) 経路検索の回数に応じて使用するハッシュ値を選択します。
・奇数回の経路検索時：ハッシュ値1を使用する。
・偶数回の経路検索時：ハッシュ値2を使用する。

(6) (5) の結果を利用可能な通信パス数で割った余りを求めます。

(7) (6) の余りを、以下にあてはめて、通信パスを決定します。
・余りが0の場合：通信パス1を利用
・余りが1の場合：通信パス2を利用
・余りが2の場合：通信パス3を利用
・余りが3の場合：通信パス4を利用
・余りが4の場合：通信パス5を利用
・余りが5の場合：通信パス6を利用
・余りが6の場合：通信パス7を利用
・余りが7の場合：通信パス8を利用

例）送信元 IP アドレスが 192.168.1.1、宛先 IP アドレスが 172.16.254.1 であるパケットについて、192.168.2.0/24 に到達する通信パス 1、通信パス 2、通信パス 3、通信パス 4 が存在する場合

（1）



それぞれを加算します。
c0a80101 + ac10fe01 = 16cb8ff02（16 進数）
桁上がりを無視して 32 ビットの値にすると 6cb8ff02（16 進数）となります。

（2） （1）の結果の上位 16 ビットと下位 16 ビットを加算します。
6cb8 + ff02 = 16bba（16 進数）
桁上がりを無視して 16 ビットの値にすると 6bba（16 進数）となります。

（3） （2）の結果の上位 8 ビットと下位 8 ビットを加算します。
6b + ba = 125（16 進数）
桁上がりを無視して 8 ビットの値にすると 25（16 進数）となります。

（4） 初回の経路検索であるため、ハッシュ値 1 を使用します。（3）の結果の 25（16 進数）から 5 となります。

（5） （4）の結果の 5 を 4 で割った余りを求めると 1 となります。

（6） （5）の結果により、通信パス 2 の利用が決定されます。

2.17.2 通信バックアップ機能

通信バックアップ機能と併用することによって、通信パスの一部に障害が発生した場合、正常な通信パスを利用して通信を継続することができます。これによって、正常時には複数通信パスを利用して負荷を分散し、通信障害発生時には利用可能な通信パスを利用して通信を継続することができます。

2.18 VRRP機能

VRRP機能とは、動的に経路制御できない端末から、別のネットワークへの通信に使用しているルータがなんらかの理由で中継できなくなった場合、自動でほかのルータが通信をバックアップする機能（簡易ホットスタンバイ機能）です。また、VRRPのグループを複数設定することで、通信の負荷分散と冗長構成を実現する機能（クラスタリング機能）もサポートしています。

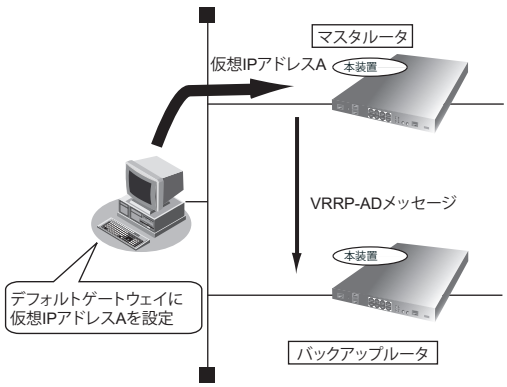
VRRP機能は2つ以上のルータがグループを形成し、1台のルータ（仮想ルータ）のように動作します。グループ内の各ルータには優先度が設定されており、その優先度に従ってマスタルータ（実際にルーティングを行う装置）とバックアップルータ（マスタルータで異常を検出したときにルーティング処理を引き継ぐ装置）を決定します。また、グループごとに仮想IPアドレスを設定し、マスタルータがグループあてのパケットを処理します。動的な経路制御をサポートしていない端末では、静的経路のデフォルトルータとして仮想IPアドレスを設定することで、仮想ルータを使用した信頼性の高い通信を実現できます。

さらに、2つ以上のルータで複数のグループをマスタルータが分散するように設定し、端末ごとにデフォルトルートの仮想ルータを分けて設定することで、負荷分散と冗長構成のクラスタリング機能も実現できます。

VRRP機能を使用するときのルータの動作を以下に説明します。

2.18.1 簡易ホットスタンバイ機能

- 通常時の動作
  VRRP機能を使用している場合、マスタルータは、定期的にバックアップルータにVRRP-ADメッセージ（VRRP Advertisement message:VRRP広報メッセージ）を送信します。バックアップルータは、マスタルータからのVRRP-ADメッセージを受信することで、マスタルータが正常に動作していると判断します。
  マスタルータでは、仮想IP／MACアドレスあてのパケットは処理されますが、バックアップルータではすべて破棄されます。

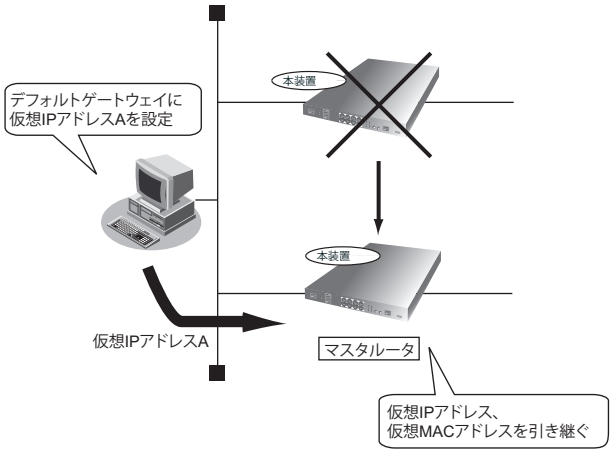


- 障害発生時の動作
  マスタルータがダウンすると、VRRP-AD メッセージは送信されません。よって、バックアップルータでは、最後に VRRP-AD メッセージを受信してからマスタルータのダウン検出時間までに次の VRRP-AD メッセージが受信できなかった場合、マスタルータがダウンしたと判断します。バックアップルータは、仮想 IP アドレスと仮想 MAC アドレスを引き継いで、マスタルータとして動作します。マスタルータのダウン時間は、以下の計算式で計算されます。

  VRRP-AD メッセージ送信間隔 × 3 ＋ Skew_Time［秒］

  Skew_Time　：マスタルータがダウンした際に、より優先度の高いバックアップルータがスムーズに切り替われるようにするための誤差であり、以下の計算式で計算されます。

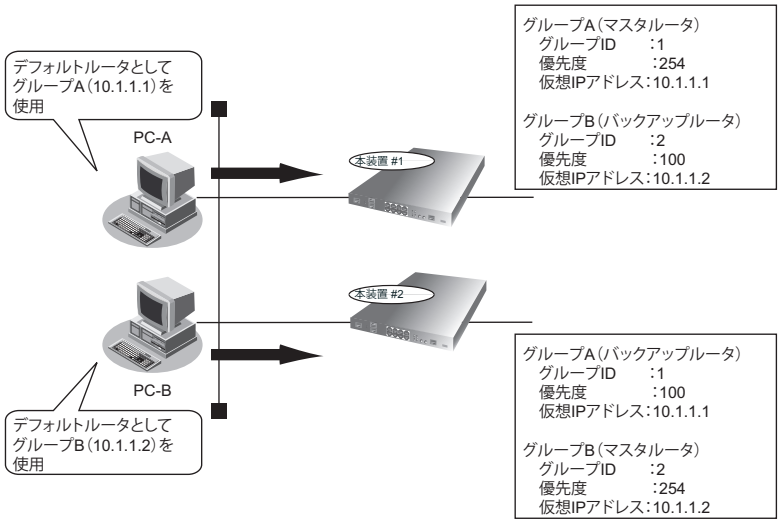
  Skew_Time =　（(256 - VRRP 優先度）x VRRP-AD メッセージ送信間隔) / 256［秒］



- トラッキング
  トラッキング対象の状態がダウンとなった場合、VRRP グループの現在の優先度から指定した値を減算した優先度の VRRP ルータとして動作します。
  - インタフェース
    指定したインタフェースがトラッキング対象となります。
  - 経路
    指定した宛先への経路情報がトラッキング対象となります。
    指定した宛先への経路情報がない場合にダウンとなります。到達性がない場合にダウンとなります。
  - 端末接続監視
    端末接続監視機能により指定した監視先装置への到達性がトラッキング対象となります。
- 障害復旧時の動作
  グループ内でもっとも優先度の高いルータが復旧した場合、同じグループ内のマスタルータはマスタルータを放棄し、バックアップルータとなります。
  自動復旧を望まない環境ではプリエンプトモードを off にすることで、自動復旧を禁止することができます。その場合は、保守作業完了後にマスタルータで clear vrrp status コマンドを実行することでマスタルータの切り替え（切り戻し）ができます。

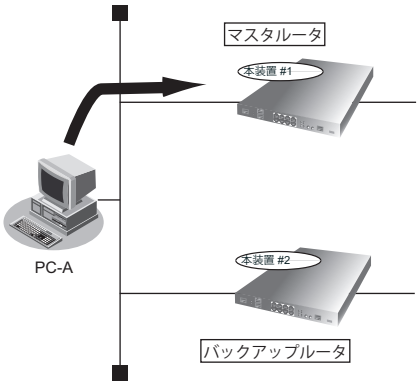
2.18.2 クラスタリング機能

- 通常時の動作
  PC-A グループは VRRP グループ A を、PC-B グループは VRRP グループ B をデフォルトルータとして設定することで、負荷分散を実現できます。また、グループごとにバックアップルータが存在して、ルータを相互にバックアップしているので、グループ A のマスタルータがダウンした場合でもバックアップルータが処理を引き継ぐことができます。

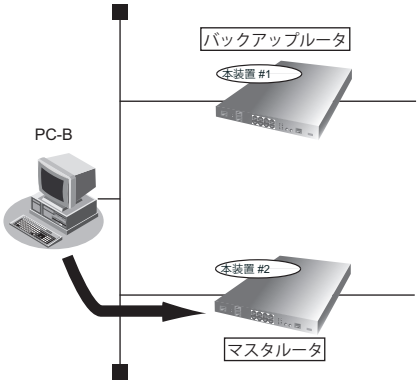


上の図を PC-A グループ、PC-B グループから見たときの構成は以下のようになります。

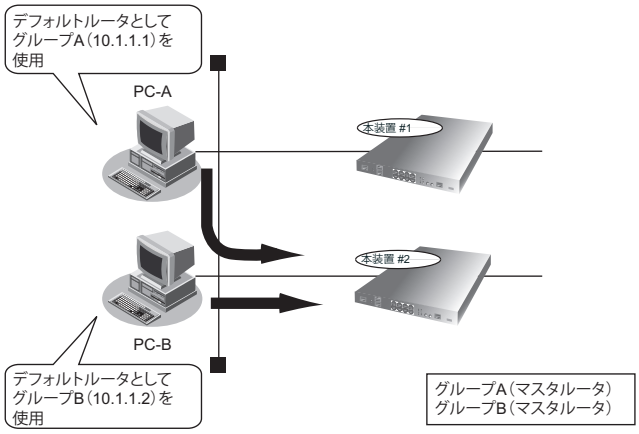
PC-A グループから見たときの構成



PC-B グループから見たときの構成



- 障害発生時の動作
  本装置#1 がダウンしたとき、グループ A に対するマスタルータは本装置#2 に引き継がれます。切り替え動作については、「2.18.1 簡易ホットスタンバイ機能」（P.71）を参照してください。



- トラッキング
  トラッキングを使用した場合、VRRP グループの現在の優先度から指定した値を減算した優先度の VRRP ルータとして動作します。
  トラッキングの種類については、「2.18.1 簡易ホットスタンバイ機能」（P.71）を参照してください。
- 障害復旧時の動作
  「2.18.1 簡易ホットスタンバイ機能」（P.71）と同様の手順で切り替えが発生します。

こんな事に気をつけて

- 同一のインタフェースに定義可能な VRRP グループは最大 4 つまでです。
- VRRP グループに割り当てる仮想 IP アドレスと実 IP アドレスは、必ず同じサブネットになるよう設定することをお勧めします。
- 本装置の電源の投入、マスタルータでの設定反映、または装置リセットを実行した場合、バックアップルータがマスタルータとなることがあります。
- VRRP 機能を使用している場合、マスタルータは、VRRP-AD（VRRP Advertisement message:VRRP 広報メッセージ）をバックアップルータに定期的に送信します。バックアップルータは、マスタルータからの VRRP-AD メッセージを受信することで、マスタルータが正常に動作していると判断します。バックアップルータは VRRP-AD メッセージを最後に受信してから一定時間内に次の VRRP-AD メッセージを受信できなかった場合、マスタルータがダウンしたと判断し、新たなマスタルータとして動作します。
- VRRP 構成における代表アドレスの使用は、下記の機能にてサポートしています。
  - ARP、Proxy ARP
  - IPv6 Neighbor
  - RA 送信、RA 受信
  - DHCPv4 サーバ
  - NAT
  - フィルタリング
  - ポリシールーティング
  - QoS
  - NTP サーバ
  - VPN（IPsec／次項の注意点をご確認ください）
  - SSH クライアント（SCP、SFTP 含む／デフォルトは実アドレス使用）
  - TELNET クライアント（デフォルトは実アドレス使用）
  - FTP クライアント（デフォルトは実アドレス使用）
  - ping（デフォルトは実アドレス使用）
  - traceroute（デフォルトは実アドレス使用）
  - SNMP MIB 取得（Trap 送信は未サポート）
- VRRP 機能と併用して、以下の機能を使用する場合は注意が必要です。
  - 課金制御機能：切り替え発生時に課金情報は引き継がれません。課金情報の累計は 0 から再スタートとなります。

- VPN（IPsec）：IPsec の終端アドレスとして仮想 IP アドレスを指定した場合、VRRP が Master 状態の場合のみ SA を確立・維持し、Master 以外の状態に遷移した際に SA を削除します。また、下記の動作においては、代表アドレスの使用をサポートしていません。
  - ・VPN ピアのドメイン解決時の DNS クライアント動作
  - ・CRL 取得動作 (HTTP クライアント動作)
  - ・RADIUS 認証 /Accounting
  - ・ICMP-Keepalive
  - ・自動鍵交換

• VRRP 機能は、DNS サーバ機能、タイムサーバ機能といった本装置上で動作する各種サーバ機能の冗長化を目的として利用することはできません。

2.19 ブリッジグループ機能

本装置では、ブリッジグループ機能に対応しています。

ブリッジ機能とは、異なる LAN を接続し、MAC フレームを中継する機能です。

本装置では、本装置ポート間のブリッジ中継と、Ethernet over IP トンネルの技術を使用してブリッジ中継することができます。

Ethernet over IP トンネルの方式としては、EtherIP および L2TPv3 をサポートしています。

本装置では、以下の 2 つの機能をサポートしています。

- ブリッジドメインを分割するためのブリッジグルーピング機能
- IP フレームの転送機能

2.19.1 ブリッジグルーピング機能

ブリッジグルーピング機能とは、各インタフェースにグループ識別子を設定し、それぞれのインタフェースにグループを割り当てることによって、ブリッジ転送が、そのグループ内に閉じた形で行われるようにする機能です。グループを分けることで、ブリッジ通信を各グループに分離することができます。

こんな事に気をつけて

- ブリッジ学習テーブル生存時間は、mac-address-table aging-time に設定した値がすべてのグループで使用されます。
- グループメンバとして指定可能なインタフェースは、物理（サブを含む）インタフェースとトランクインタフェース、および tunnel インタフェースです。
- IP フレームをルーティングする場合、そのブリッジグループに属するすべてのインタフェース上に IP 中継のための設定を行う必要があります。本設定を行うことで、以下の機能を利用することができます。ただし、tunnel インタフェースでは、IP フレームをルーティングすることはできません。tunnel インタフェースでは IP に関する設定は定義しないでください。
  - FTP（ファームアップデートなど）
  - telnet
  - システムログの送信
  - SNMP エージェント、Trap 送信
  - ダイナミックルーティング

2.19.2 IP フレームの転送ポリシ転送方式

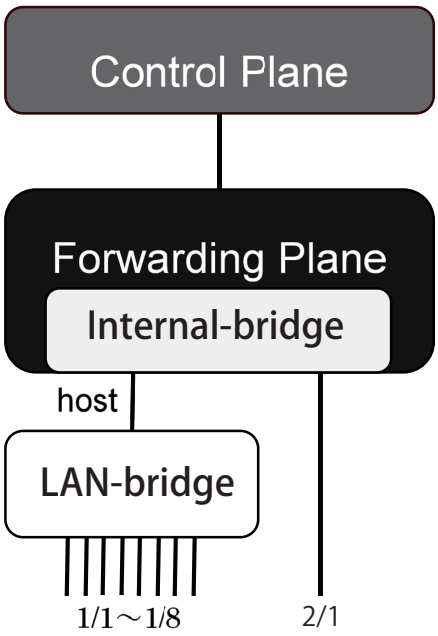
IPv4 または IPv6 のフレームをブリッジで処理する場合、受信した IP フレームの宛先 MAC アドレスが本装置あてでないとき、その IP フレームはそのままブリッジで転送されます。

ルーティング設定のあるインタフェースで受信した IP フレームの宛先 MAC アドレスが受信インタフェースあてで、宛先 IP アドレスも受信インタフェースあての場合は、本装置あての IP フレームとして処理します（これによって Ping の応答やソフトウェアの更新などが IP フレームをブリッジで転送するインタフェース上でも可能になります）。

また、宛先 MAC アドレスが受信インタフェースあてで、宛先 IP アドレスが受信インタフェースあてではない場合は、ルーティングして転送します。ルーティング設定のないインタフェースで受信した IP フレームの宛先 MAC アドレスが受信インタフェースあてである場合、IP フレームは廃棄されます。

2.19.3 ブリッジグループの装置内部構成

本装置は、下記の図のように 2 つの独立したブリッジ (LAN-bridge/Internal-bridge) で構成されています。LAN-bridge には slot 1 のポート (LAN ポート) が、Internal-bridge には slot 2,3 のポート (WAN ポート) が直接接続されています。2 つのブリッジは、host インタフェースで接続されています。2 つのブリッジを跨いでブリッジグループを構成することが可能ですが、それぞれの bridge の特性により、設定できる内容にいくつかの差異があります。



Internal-bridge のみ実施可能な機能例：

・MAC-address 学習テーブルの ageout 時間の設定

・MAC-address 学習テーブルの静的登録設定

・MAC-address 学習テーブルのクリア機能

・同一 VLAN-ID のインタフェースを異なるブリッジグループに設定可能

例) bridge-group 1:

GigaEthernet 1/1.100 vlan-id 100

bridge-group 2

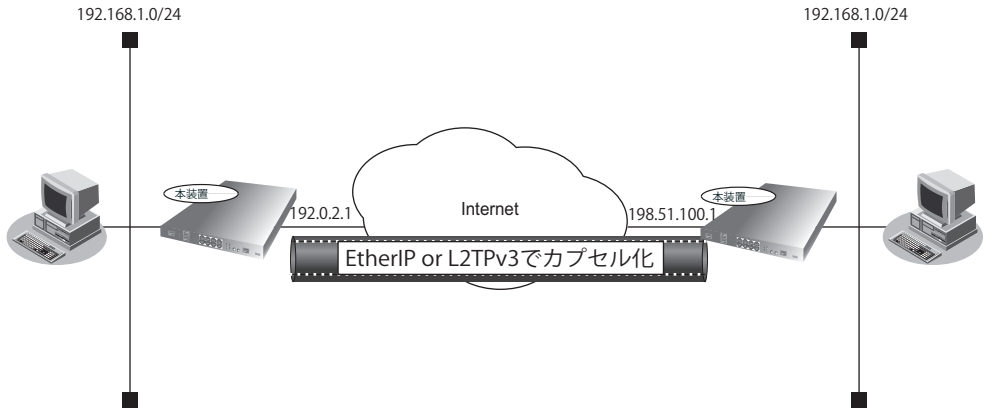
GigaEthernet 2/1.100 vlan-id 100

2.19.4　Ethernet over IP トンネル（EtherIP/L2TPv3）

Ethernet over IP トンネル（EtherIP/L2TPv3）とは、Ether フレームをカプセル化し、IP 網を介して Ether フレームを中継する L2VPN 機能です。

本機能を用いることで、下図のように離れた拠点間で同一セグメントでのネットワーク構築が可能となります。

EtherIP/L2TPv3 機能では Ether フレームの暗号化は行えません。IPsec 機能との併用を推奨いたします。



EtherIP と L2TPv3 の違いは主に以下となります。

・通信相手の認証機能の有無 (EtherIP 無 / L2TPv3 有)

・UDP ヘッダの付与機能の有無 (EtherIP 無 / L2TPv3 有)

・1 つの接続先アドレスで、複数のネットワークセグメントをカプセル化する機能の有無 (EtherIP 無 / L2TPv3 有)

L2VPN の用途に応じて EtherIP、L2TPv3 のどちらかを選択ください。

以下に、本装置でサポートする L2TPv3 機能を示します。

機能	詳細
制御プレーン	RFC3931 対応
	Control Connection 確立、切断
	セッション確立、切断
	Tie Breaker 機能
	Keepalive 機能
	1Control Connection N セッション対応
	Cisco 独自拡張機能
	Tunnel protection
データプレーン	Cookie 機能
	L2TPv3 over IP
	L2TPv3 over UDP
	L2TPv3 over IP over IPsec
	L2TPv3 over UDP over IPsec
	Tunnel protection

2.20 リンクアグリゲーション機能

リンクアグリゲーション機能とは、複数のポートを多重化し、1 本の高速リンク（トランク・グループ）として扱うための機能です。この機能を使用すると、多重化されたリンク（メンバポート）の 1 本が故障した場合に、そのトラフィックをほかのメンバポートに分散することによって、リンクの冗長性を高めることができます。リンクアグリゲーション機能は、マルチリンクイーサまたはポート・トランキングとも呼ばれます。

- トランク・グループへのトラフィックは、送信先 MAC アドレスと送信元 MAC アドレスを元に負荷分散されます。
- F310 では Giga インタフェース 1/2 ～ 1/5 の最大 4 ポートを同一トランク・グループとして使用可能です。
- Giga インタフェース 1/1, 2/1 はトランク・グループとして使用できません。
- F310 では最大 2 つのトランク・グループを使用可能です。
- スタティック LAG をサポートしています。
- トランク・グループにて QoS 機能は未サポートです（interface Trunk-channel モードにて service-policy コマンドはお使いになれません）。

こんな事に気をつけて

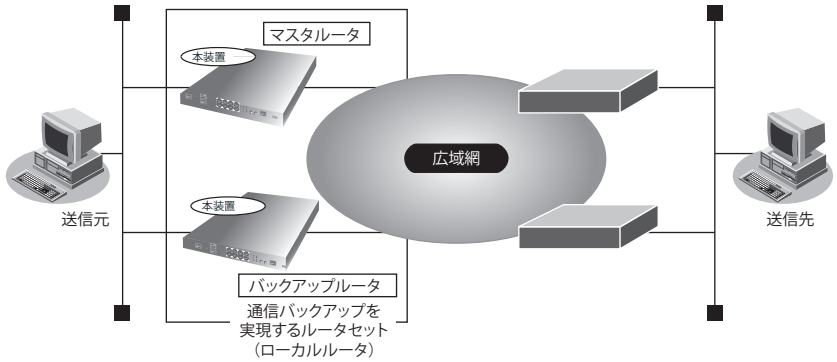
多重化されたポートは、論理的な 1 本のポートとして扱われます。VLAN 機能を併用した場合も同じです。

2.21 通信バックアップ機能

通信バックアップ機能とは、通信障害が発生した通信パスを検出した場合に、迂回通信パスを利用することで、エンドツーエンドの通信を維持する機能です。通信バックアップ機能は、以下の 2 つの機能を組み合わせることで実現できます。

- 通信障害の検出機能
- 検出された通信障害に対する通信パス迂回機能

ここでは、以下の図のネットワーク例に基づいて説明します。



こんな事に気をつけて

ここでは片方向通信について説明していますが、一般的なクライアントーサーバモデルの通信は、「クライアントからサーバへの通信（主に要求）」と「サーバからクライアントへの通信（主に応答）」が成立して初めて成立します。このため、実際に利用する場合は、本書を参考にして、双方向の通信が成立するようにネットワーク設計を行ってください。

2.21.1 通信障害の検出機能

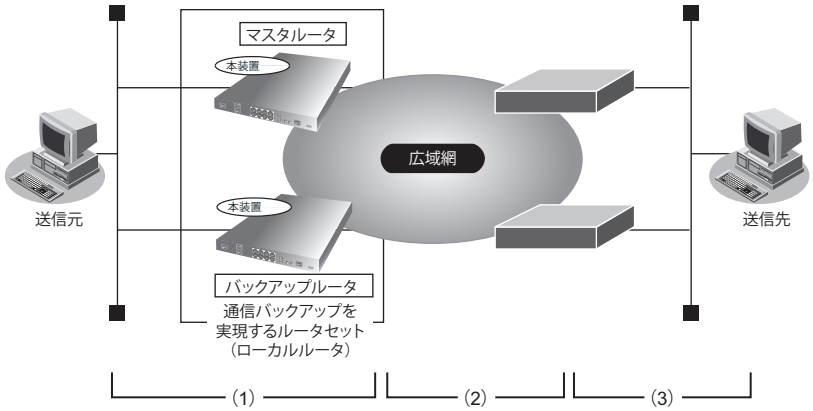
通信障害はさまざまな要因で発生します。その要因は、主に、以下の3つに分類することができます。

(1) 送信元とローカルルータとの間の到達性喪失を要因とする通信障害

(2) ローカルルータと隣接ルータとの間の到達性喪失を要因とする通信障害

(3) 隣接ルータと送信先との間の到達性喪失を要因とする通信障害

それぞれ障害が発生する箇所について、以下に示します。



ここでは、要因ごとに本装置の障害検出機能について説明します。

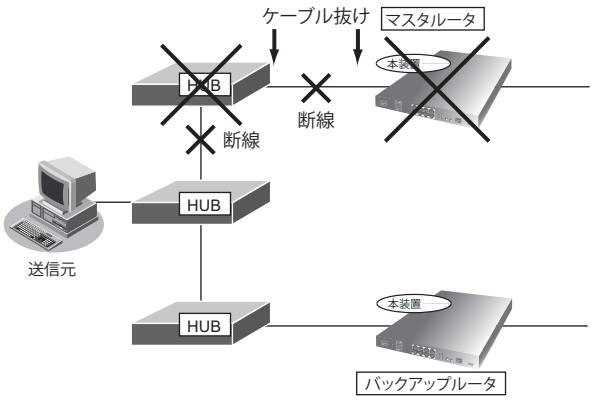
(1) 送信元とローカルルータとの間の通信障害

送信元とローカルルータとの間の通信障害には、以下の要因が考えられます。

- マスタルータとローカルネットワークとの間の障害（ケーブル断線、ケーブル抜け、HUB の故障など）
- マスタルータの故障

これらの障害に対する本装置の検出方法と障害検出可能な箇所は、以下のとおりです。

- VRRP 機能を利用した障害検出（IPv4）
- ダイナミックルーティング機能を利用した障害検出



以下に、それぞれの検出方法について説明します。

VRRP 機能を利用した障害検出（IPv4）

本装置では、VRRP（Virtual Router Redundancy Protocol）をサポートしています。この障害検出方法は、送信元でダイナミックルーティングプロトコルが利用できない（しない）場合に利用します。

マスタルータとバックアップルータ間で VRRP を利用する場合、ローカルネットワーク上では 1 台のルータ（仮想ルータ）だけ動作しているように見えます。このため、マスタルータが故障した場合も、Ethernet 上のほかのノードはその故障を検出する必要はありません。

マスタルータは、定期的にバックアップルータに VRRP-AD パケットを送信します。バックアップルータは、VRRP-AD パケットを一定時間受信できなかった場合に、VRRP でマスタルータの障害を検出します。障害復旧は、バックアップルータが VRRP-AD パケットを受信することによって検出されます。

ダイナミックルーティング機能を利用した障害検出

本装置では、いくつかのダイナミックルーティングプロトコルをサポートしています。この障害検出方法は、送信元でダイナミックルーティングプロトコルを使用する場合に利用します。

どのダイナミックルーティングプロトコルも、定期的に制御データが送信されています。制御データを一定時間受信できなかった場合に、バックアップルータは経路喪失としてマスタルータの障害を検出します。障害復旧は、バックアップルータが制御データを受信することによって検出されます。

(2) ローカルルータと隣接ルータとの間の通信障害

ローカルルータと隣接ルータとの間の通信障害には、以下の要因が考えられます。

- ローカルルータと隣接ルータとの間の障害（ケーブル断線、ケーブル抜け、広域網障害など）
- 隣接ルータの故障

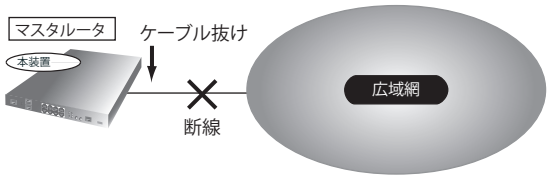
これらの障害に対する本装置の検出方法と障害検出可能な箇所は、以下のとおりです。

- ハードウェアによる障害検出
- データリンクプロトコルを利用した障害検出
- 端末接続監視機能を利用した障害検出
- ダイナミックルーティング機能を利用した障害検出

以下に、それぞれの検出方法について説明します。

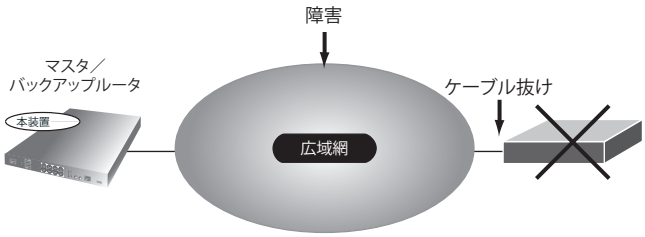
ハードウェアによる障害検出

この障害検出は、物理回線を直接利用して隣接ルータと通信する場合に利用できます。IPsec および IP トンネルでは利用できません。この方法で検出された障害は、物理回線を直接利用して通信できない障害と判断されます。



データリンクプロトコルを利用した障害検出

この障害検出方法は、ローカルルータと隣接ルータとの間で以下の接続先種別を利用している場合に利用できます。この方法で検出された障害は、この接続先が利用できないと判断されます。



- PPPoE を利用する場合（常時接続機能利用時のみ）
  PPPoE で常時接続機能を利用した場合は、PPPoE セッション切断の発生が通信障害として検出されます。また、障害復旧は PPPoE セッション接続によって検出されます。

端末接続監視機能を利用した障害検出

本装置は、確認先装置に対して定期的に ICMP echo request を送信して、その応答を受信することによって到達性を確認する L3 監視機能をサポートしています。

応答がない場合、到達性なしとして障害を検出します。

また、障害復旧は応答である ICMP echo reply の受信によって検出します。

ダイナミックルーティングを利用した障害検出

「送信元とローカルルータとの間の通信障害」（P.81）の方法と同様です。

(3) 隣接ルータと送信先との間の通信障害

隣接ルータと送信先との間の通信障害には、以下の要因が考えられます。

- 隣接ルータから送信先までの経路制御障害

この障害に対する本装置の検出方法は、以下のとおりです。

- 端末接続監視機能を利用した障害検出
- ダイナミックルーティング機能を利用した障害検出

以下に、それぞれの検出方法について説明します。

端末接続監視機能を利用した障害検出

「ローカルルータと隣接ルータとの間の通信障害」（P.82）の方法と同様です。

監視先を送信先に設定することによって、隣接ルータの先の通信障害まで検出できます。

こんな事に気をつけて

- L3 監視機能を利用して双方向通信の相互監視を行う場合は、互いに隣接ルータを監視するように設定してください。隣接ルータより先の装置を監視した場合、ICMP echo reply は、迂回経路を利用して監視元に転送されます。迂回経路でも通信障害が発生した場合、障害が復旧しても ICMP echo reply が監視元に到達できなくなるため、復旧検出が行うことができなくなります。
- Tunnel 以外で ICMP echo request を受信した場合は、Tunnel 以外でしか ICMP echo reply 送信できません（たとえば物理で ICMP echo request を受信した場合、Tunnel で ICMP echo reply 送信はできません。逆に、Tunnel で ICMP echo request を受信した場合、物理でも ICMP echo reply 送信できます）。

ダイナミックルーティングを利用した障害検出

ダイナミックルーティングを利用した場合、隣接ルータからの経路喪失の通知によって検出されます。障害復旧は、隣接ルータからの経路通知により検出されます。

2.21.2 検出された通信障害に対する通信パス迂回機能

通信障害の検出方法によって、本装置での通信パス迂回機能による利用方法が異なります。

ここでは、それぞれの検出方法による利用方法と本装置での通信パス迂回機能について説明します。

検出された通信障害の利用

「2.21.1 通信障害の検出機能」（P.81）によって検出された通信障害は、以下のように利用されます。

- VRRP機能を利用した障害検出
  VRRP機能で、マスタルータ切り替え要因として利用されます。
- ダイナミックルーティング機能を利用した障害検出
  経路制御機能で、経路切り替え要因として利用されます。
- ハードウェアによる障害検出
  Ethernet回線で、VLANおよびlanインタフェースのダウン要因として利用されます。
- データリンクプロトコルを利用した障害検出
  該当するtunnelインタフェースのダウン要因として利用されます。
- 端末接続監視機能を利用した障害検出
  確認先装置の到達性と連携させた機能について利用不能状態への遷移要因として利用されます。

通信パス迂回機能

本装置の通信パス迂回機能は、以下のとおりです。

- VRRP機能を利用した迂回機能
- 経路制御機能を利用した迂回機能
- マルチルーティング機能を利用した迂回機能

以下に、それぞれの通信パス迂回機能の詳細を説明します。

VRRP機能を利用した迂回機能

VRRP機能を利用した場合、VRRPルータは、自身より優先度の高い装置が存在すると判断されているときは、仮想ルータのMACアドレスあてに送信されたパケットを受信しません。LAN内のもっとも優先度が高いVRRPルータ（マスタルータ）がパケットを受信し、転送します。ほかのVRRPルータ（バックアップルータ）は転送しません。

マスタルータは、障害検出を契機に自身の優先度の変更をLAN上に広報します。マスタルータが優先度を下げる契機として、以下の契機があります。

- インタフェーストラッキング
  インタフェーストラッキングは、インタフェースのダウンを契機として利用します。この機能はtrack port-channelコマンドによって設定されます。
- 経路トラッキング
  経路トラッキングは、設定された経路が装置から喪失したことを契機として利用します。この機能はtrack ipコマンドによって設定されます。

- 端末接続監視トラッキング
  端末接続監視トラッキングは、端末接続監視機能を利用して監視先装置への到達性がなくなったことを契機として利用します。この機能はtrack surveyコマンドによって設定されます。

経路制御機能を利用した迂回機能

本装置は、受信したパケットをどのインタフェースから転送するかを、自身が持つ経路情報によって判断します。経路制御機能を利用することにより、障害検出時に経路情報を迂回経路側に変更し、通信パスが迂回されます。また、ダイナミックルーティング機能を利用している場合は、経路情報の変更を、ダイナミックルーティングプロトコルを利用して隣接ルータに通知することによって、本装置に到達する前に、迂回するように指示することもできます。これら経路制御機能は、利用するプロトコルによって異なります。

IPv4を利用する場合

ダイナミックルーティング機能を利用して障害検出された場合、まず、そのダイナミックルーティングプロトコルの範囲で経路変更が行われます。RIPv2、OSPFおよびBGP4の場合、代替経路を学習しているときは、代替経路に変更されます。代替経路がないときは、削除されます。

インタフェースダウンによって障害検出された場合は、以下の動作となります。

- スタティックルート（distanceが1以上に設定されたもの）
  経路情報が削除されます。
- ダイナミックルーティングによって学習された経路
  ダウンしたインタフェースを利用する経路に対して、ダイナミックルーティングを利用した障害検出時の処理と同じです。

これらの処理を行ったあと、スタティックルートおよびそれぞれのダイナミックルーティングの中で最適な経路が選択され、最終的な新経路が決定されます。また、ダイナミックルーティング機能を利用している場合は、最終的な新経路の決定結果を隣接ルータに対して通知します。異なるダイナミックルーティングプロトコル間の経路通知は、redistribute定義によって決定されます。

IPv6を利用する場合

IPv6 OSPFを利用して障害検出された場合、代替経路を学習しているときは、代替経路に変更されます。代替経路がないときは、削除されます。

インタフェースダウンによって障害検出された場合は、以下の動作となります。

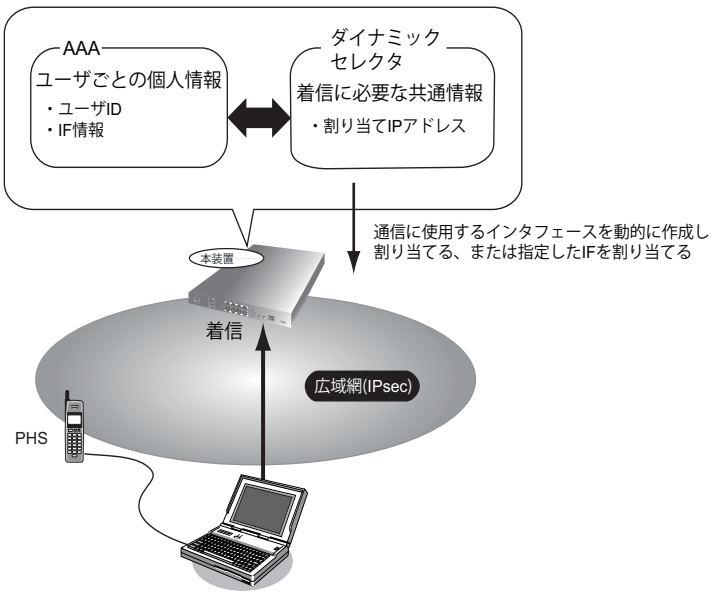
- スタティックルート（distanceが1以上に設定されたもの）
  経路情報が削除されます。
- IPv6 OSPFによって学習された経路
  ダウンしたインタフェースを利用する経路に対して、ダイナミックルーティングを利用した障害検出時の処理と同じです。

2.22 ダイナミックセレクタ機能

ダイナミックセレクタ機能とは、あらかじめ着信接続時に共通する情報をテンプレートに定義しておき、そのテンプレートを使って着信を行う機能です。ダイナミックセレクタへの着信は、接続するたびに、設定したプール情報の中から使用していない情報を接続相手に動的に割り当てるため、不特定相手着信を実現できます。

また、同一の相手には、AAA（Authentication、Authorization、Accounting）情報から個別情報を取得することで、同一の情報を静的に割り当てることができます。さらに、AAA 情報から通信情報を取得することで、接続先を相手ネットワーク情報に設定したときに比べて、より多くの接続相手を登録できます。AAA 情報は、本装置に設定された AAA 情報または RADIUS サーバから取得できます。

本装置の AAA 情報では、ダイナミックセレクタへの着信で接続するユーザの認証情報など通信接続に関する情報を登録しておくことができます。



ダイナミックセレクタへの着信時に使用するインタフェースは、インタフェースを動的に作成するか、指定したインタフェースで通信します。

また、着信時の認証は、AAA 情報に登録されたユーザ情報で行われます。

接続相手の登録を追加する場合は、AAA 情報に接続相手のユーザ情報を登録するだけで追加できます。

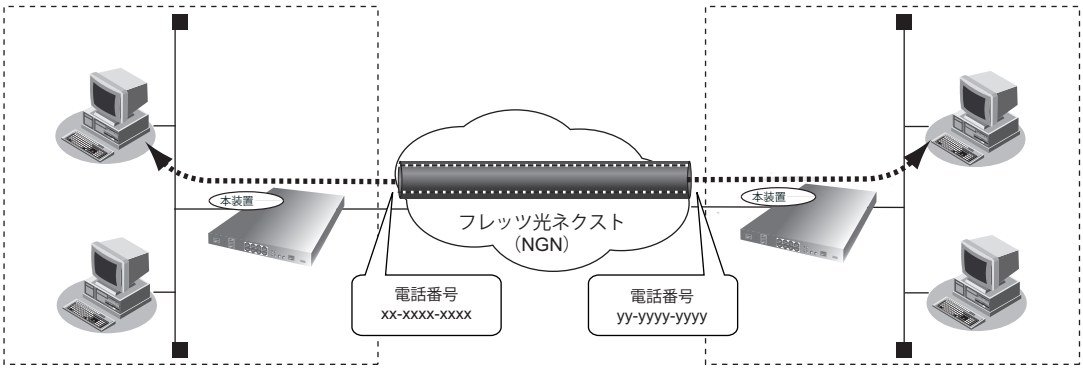
こんな事に気をつけて

- ダイナミックセレクタ機能をサポートする接続形態は IPsec です。
- インタフェースを動的に作成する場合はインタフェース単位での情報を見ることはできません。IPsec SA 情報を参照してください。
- ダイナミックセレクタとスタティックセレクタで使用可能なインタフェースの最大数は 128 です。

2.23 データコネクト機能

データコネクトは、フレッツ光ネクストの「ひかり電話」を利用した、帯域確保型データ通信サービスです。電話サービスを利用するため、接続相手の指定は電話番号で行います。

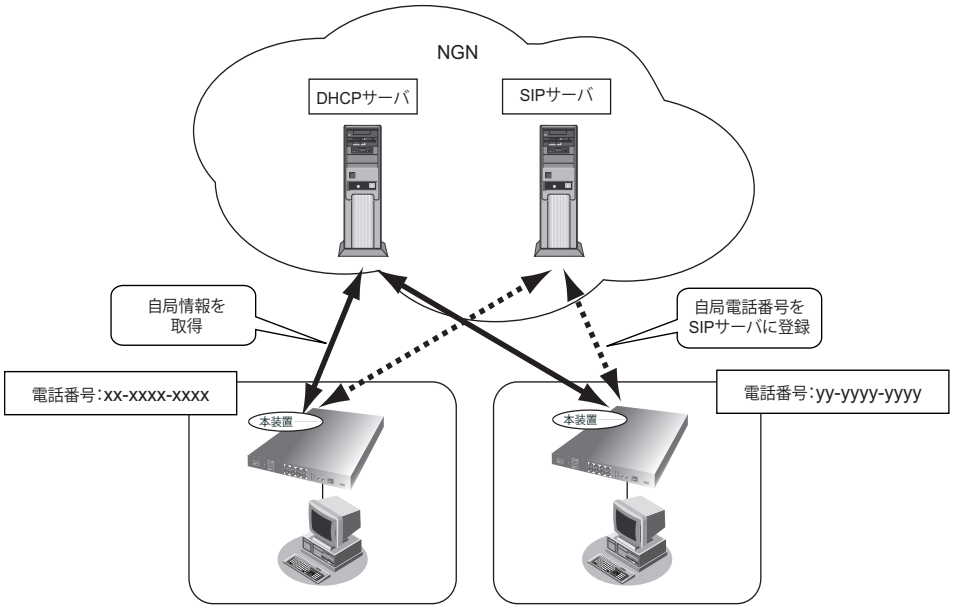
帯域保障型の通信サービスであるデータコネクトを利用して VPN 通信パスを構築することで、安定した通信ができます。



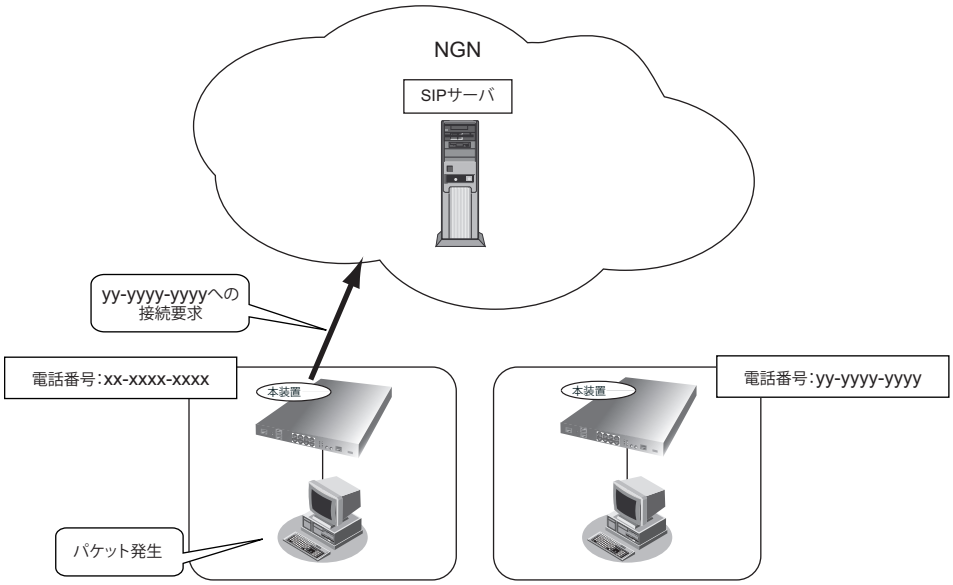
データコネクトを利用した VPN 接続の動作を以下に示します。

(1) ひかり電話への接続

NGN 回線を接続して本装置を起動すると、NGN 網の DHCP サーバから IP アドレスや SIP サーバのアドレス、電話番号などの自局情報を取得します。取得した自局情報をもとに、NGN 網の SIP サーバに登録処理を行います。登録完了後は、定期的に登録パケットを送出します。

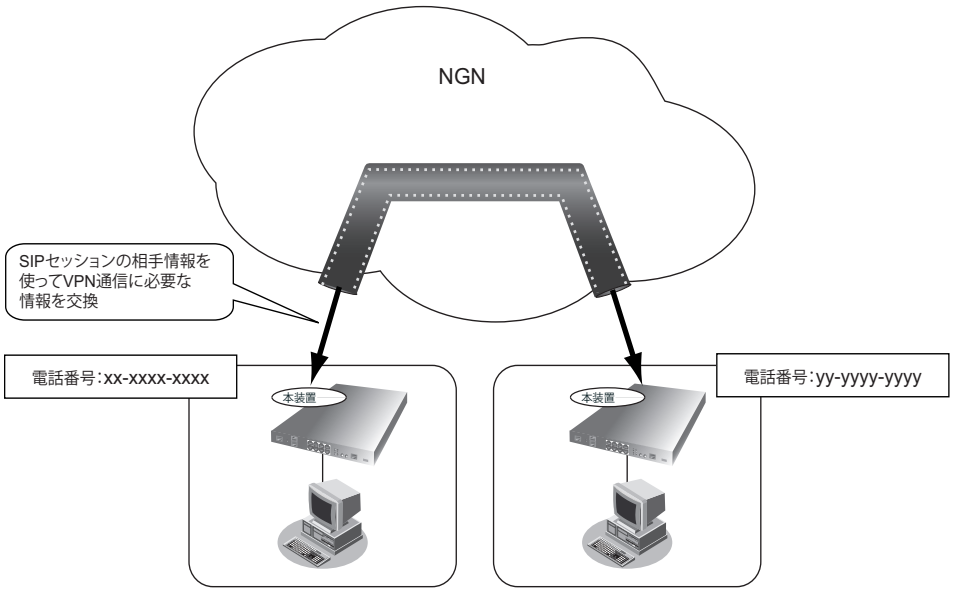


(2) 他拠点へのパケット発生
データコネクトを利用する対象となっている他拠点に、通信パケットが発生したとき、SIP サーバに対し他拠点の電話番号に向けた接続要求を送信します。



(3) データ通信用 SIP セッションの確立
自装置 IP やメディア種別、利用帯域の情報を設定した接続要求は SIP サーバを経由して相手装置に送信されます。相手装置は受信したメディア種別や帯域などの情報をチェックし、問題がなければ接続応答が SIP サーバを経由して返信されます。

(4) VPN 通信パスの構築
SIP セッション確立時に交換した相手装置の情報をもとに、VPN 通信パスを構築します。



(5) VPN 通信パスおよび SIP セッションの切断
通信パケットがなくなり、一定時間が経過すると VPN 通信パス、SIP セッションともに自動的に切断されます。

こんな事に気をつけて

- データコネクト機能を使用する場合、DHCP クライアント機能の設定を IPv4 と IPv6 両方で有効にしてください。
- データコネクトは従量課金制のため、長時間通信を行うと超過課金の原因となります。ご使用する際は、通信料金に十分ご注意ください。
- データコネクトは、利用する帯域により通信料金が異なりますので、ご注意ください。
- データコネクト機能を使用する場合は、NAT トラバーサル機能を使用する必要があります。
- データコネクト接続は、IPv4 および IPv6 の IPsec 通信をサポートしています。

2.24 RADIUS 機能

RADIUS 機能は、AAA（Authentication, Authorization, Accounting）情報の管理を外部サーバ（RADIUS サーバ）を利用して行う機能です。複数の装置で同じ AAA 情報が必要な場合や、大量のユーザ情報を管理する場合など、ユーザの認証情報や設定情報、ユーザごとの接続時間や回線の利用情報を集約して管理できます。

本装置には、RADIUS クライアント機能があります。

以下に、機能について説明します。

2.24.1 RADIUS クライアント機能

RADIUS クライアント機能は、以下の RADIUS サポート機能から AAA を経由して利用されます。

以下に、それぞれの機能で利用可能な AAA 情報を示します。

RADIUS サポート機能	認証方式（**authentication**）	ユーザ情報（**authorization**）	アカウンティング（**accounting**）
ログインユーザ認証機能	• PAP 認証 • CHAP 認証	使用しません	使用しません
拡張認証機能 （IPsec ／ IKE 接続）	• PAP 認証 • CHAP 認証 • EAP 認証	• IPv4 スタティック経路情報 • IPv6 スタティック経路情報	• 送受信オクテット数 • 送受信パケット数 • 接続時間
データコネクト電話番号 認証機能	• PAP 認証 • CHAP 認証	• IKE セッション確立時の共有鍵（Pre-Shared key） • IPsec の IPv4 スタティック経路情報	• 接続時間

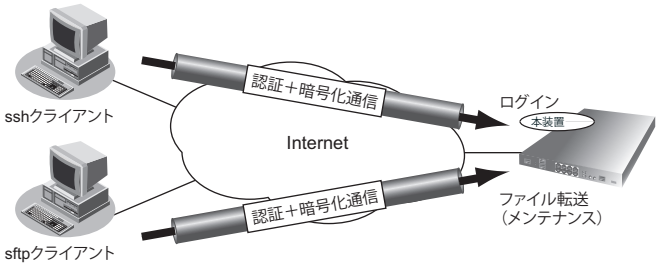
本装置の RADIUS クライアント機能は、複数台の RADIUS サーバを使用したバックアップ構成または負荷分散構成が可能です。

拡張認証機能とデータコネクト電話番号認証機能は共通の設定方法であり、ログインユーザ認証機能は別設定になります。

2.25 SSH サーバ機能

SSH サーバ機能とは、TELNET サーバ機能と同じリモートログイン機能（ssh サーバ）と FTP サーバ機能と同じリモートファイル転送機能（scp サーバ、sftp サーバ）をサポートしています。

TELNET サーバ機能および FTP サーバ機能では、平文テキストデータのまま通信するため、通信内容を傍受されたり、改ざんされる危険性があります。SSH サーバ機能では、ホスト認証および暗号化通信により、安全で信頼できるログイン機能およびファイル転送機能を利用することができます。



crypto key generate コマンド実行時に本装置の SSH ホスト認証鍵が生成されます。

SSH クライアントソフトウェアにあらかじめ接続相手の SSH ホスト認証鍵を設定しておく必要がある場合は、本装置で show crypto key コマンドを実行して表示される SSH ホスト認証鍵を設定します。

本装置に SSH 接続した際に、本装置の SSH ホスト認証鍵が SSH クライアント側に送信されて、設定または保存されている鍵と異なる場合は、SSH 接続が拒否されます。したがって、装置交換などにより、SSH ホスト認証鍵が変更された場合は、SSH クライアントソフトウェアに設定または保存されている SSH ホスト認証鍵を再設定するか削除してから SSH 接続します。

その後、パスワード入力プロンプトが表示されますが、SSH ホスト認証などの処理により、表示されるまで多少時間がかかります。

本装置では出荷状態から SSH ホスト認証鍵(RSA/DSA)が生成されています。ssh-seraver shutdown 設定または、crypto key zeroize コマンドで認証鍵をすべて削除することによって、SSH サーバ機能を完全に停止できます。

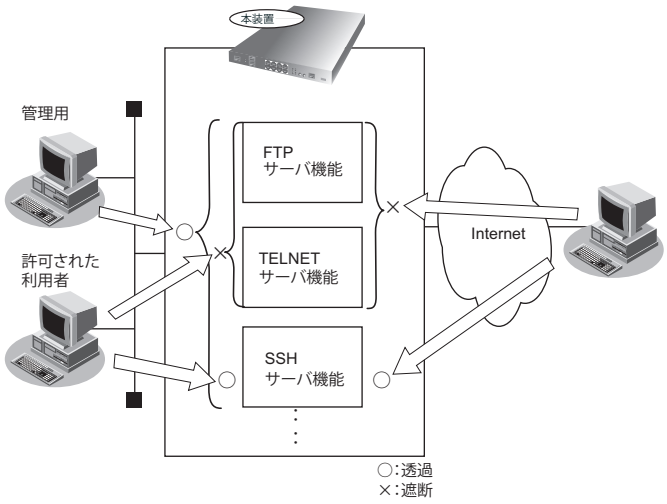
本装置でサポートする SSH サーバ機能

項目	サポート内容
SSH プロトコルバージョン	SSH プロトコルバージョン V1/V2 をサポート
SSH ポート番号／プロトコル	22 ／ TCP（設定により変更可）
IP プロトコルバージョン	IPv4 および IPv6 をサポート
ホスト認証プロトコル	RSA/DSA、RSA1
ホスト認証アルゴリズムの種類	ssh-rsa、ssh-dss
暗号方式の種類	SSHv1: des, 3des, blowfish SSHv2: 3des-cbc, blowfish-cbc, cast128-cbc, arcfour, aes128-cbc, aes192-cbc, aes256-cbc, rijndael-cbc@lysator.liu.se, aes128-ctr, aes192-ctr, aes256-ctr
メッセージ認証コードの種類	hmac-md5, hmac-sha1, hmac-ripemd160, hmac-ripemd160@openssh.com, hmac-sha1-96, hmac-md5-96
同時接続数	16（SSH によるログインセッションの数、SFTP での接続は含みません）

2.26 アプリケーションフィルタ機能

アプリケーションフィルタ機能では、本装置で動作する各サーバ機能に対してアクセスを制限できます。

これにより、本装置のメンテナンスまたは本装置のサーバ機能を使用する端末を限定し、セキュリティを向上できます。



2.27 PKI 機能

PKI 機能とは、デジタル証明書の作成、登録、削除を行う機能です。

証明書とは、ITU-T 勧告の X.509 に定義されており、本人情報、公開鍵、有効期限、シリアル番号、シグネチャなどが含まれています。

PKI 機能を使用するアプリケーションは、以下のとおりです。

- IPsec 機能（RSA/ECDSA デジタル署名認証方式）

こんな事に気をつけて

- RSA/ECDSA 鍵ペアおよび自装置証明書がない場合は、RSA/ECDSA デジタル署名認証は使用できません。
- 認証局証明書は証明書の検証に利用されるため、設定した認証局証明書から発行されていない証明書の場合、検証に失敗することがあります。
  詳細は、各アプリケーションの説明を参照してください。

2.28 USB メモリ機能

USB メモリ機能とは、USB メモリに構成定義情報を保存したり、USB メモリから構成定義情報を転送するための機能です。

本装置では以下のファイルシステムをサポートしています。

- FAT16（VFAT）
- FAT32（VFAT）

また、本装置では以下の作業を行うことができます。

- USB メモリからの構成定義の転送
- USB メモリへの構成定義の保存
- USB メモリからのソフトウェアの更新
- USB メモリへのソフトウェアの保存
- USB メモリへの tech-support・report-all の保存
- ファイル操作（ファイル一覧の表示、ファイルの削除、ファイルのコピー、ファイル名変更）

こんな事に気をつけて

- 本装置は VFAT をサポートしているため、ロングファイル名を指定できます。ただし、日本語のファイル名は指定できません。
- USB メモリは、複数のパーティションに分割されたものを利用できます。ただし、利用できるのは、先頭のパーティションのみです。
- ショートカットは利用できません。

2.28.1 構成定義の転送と保存

構成定義の転送および保存は、以下の方法で行います。

copy コマンドで行う場合

USB1 メモリのファイルは“/usb1/<filename>“、USB2 メモリのファイルは“/usb2/<filename>“ でアクセスできます。たとえば、USB メモリ 1 に格納されている“config.txt” というファイルは、copy コマンドで“/usb1/config.txt“ のように指定します。USB メモリが複数パーティションに分割されている場合は、先頭のパーティションが利用されます。ディレクトリの区切り記号は/ です。たとえば、USB メモリ 1 の“dir” というディレクトリに格納されている“config.txt” というファイルは、“/usb1/dir/config.txt“ のように指定します。

同様にしてソフトウェアの更新および保存ができます。

こんな事に気をつけて

- Windows で編集した末尾 <CR><LF> のコンフィグは読み込みができません。
- 末尾に end が無いコンフィグは、起動時に読み込み失敗します（load では読み込み失敗しません）

2.29 マルチキャスト機能

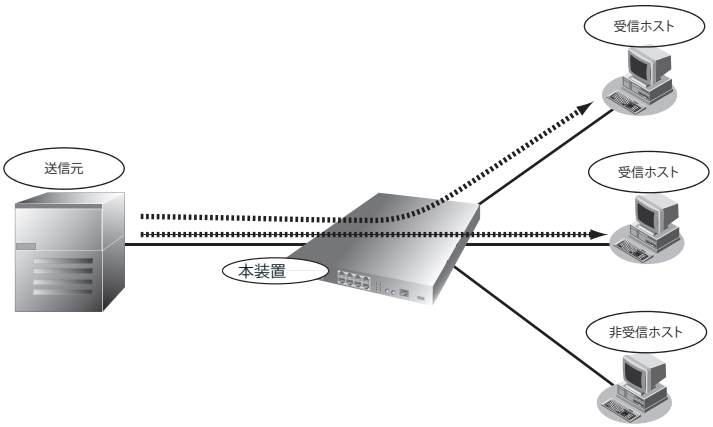
マルチキャスト機能とは、ネットワーク上で複数のノードに対してデータを一斉に送信できる機能です。

同一データを複数のノードに送信する場合、1 対 1 のユニキャスト送信では、送信者は受信するノードの数だけパケットを生成して送信します。一方 1 対多のマルチキャスト送信では、送信者は一つのデータを送信し、経路上のルータがパケットを複製して受信ノードがいるインタフェースへ送信します。

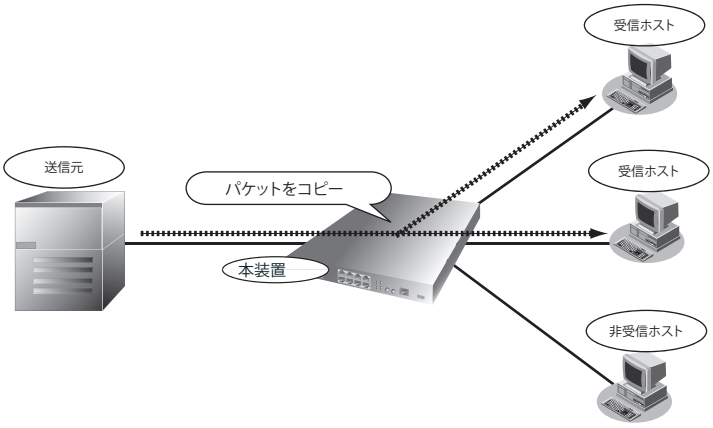
ユニキャスト送信と比べてネットーワーク上の負荷を軽減することができ、特定ユーザ向けのリアルタイム動画配信や情報配信サービス等で、効率的にデータ送信を行うことができます。

本装置では、IPv4 でのマルチキャスト機能をサポートしています。IPv6 でのマルチキャスト機能は未サポートです。

本装置では、マルチキャスト機能を動作させるマルチキャストルーティングプロトコルとして、IGMPv2、IGMP proxy をサポートしています。



ユニキャスト送信



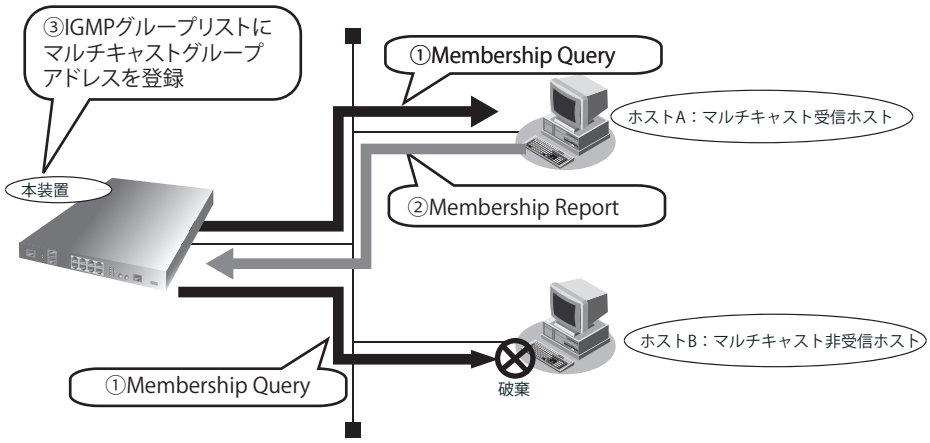
マルチキャスト送信

2.29.1 IGMPv2

マルチキャストルータは受信ノードの情報を得るために Membership Query メッセージを定期的に送信します。宛先は全マルチキャストホスト (224.0.0.1) になります。

マルチキャストを受信するノードは、マルチキャストグループに参加するため、Membership Report を送信します。マルキャストグループから離脱する場合は Leave Group メッセージを送信します。

マルチキャストルータは、Membership Report を受信すると、IGMP グループリストに登録し、受信インタフェースからマルチキャストパケットを送信します。

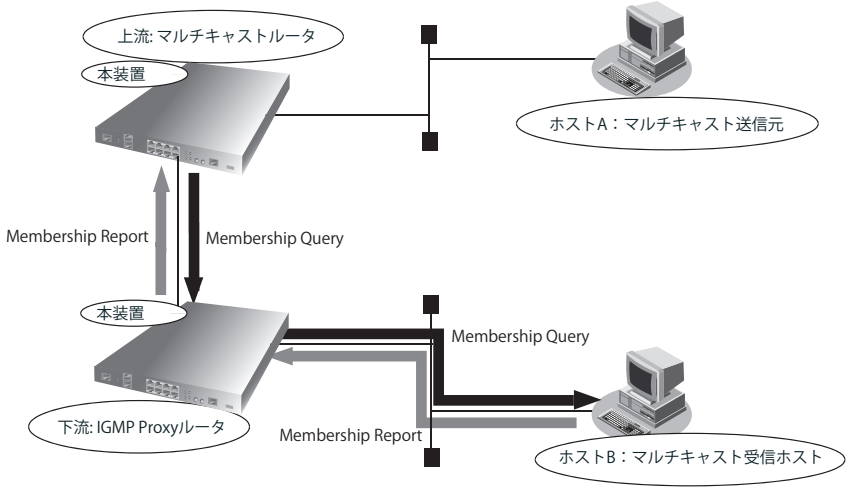


2.29.2 IGMP Proxy

IGMP Proxy は、マルチキャスト受信ノードからの IGMP パケットを上位のルータに転送する機能です。

下流インタフェースにおいては、IGMP グループリストを管理し、上流インタフェースにおいては、マルチキャスト受信ノードとして振舞います。

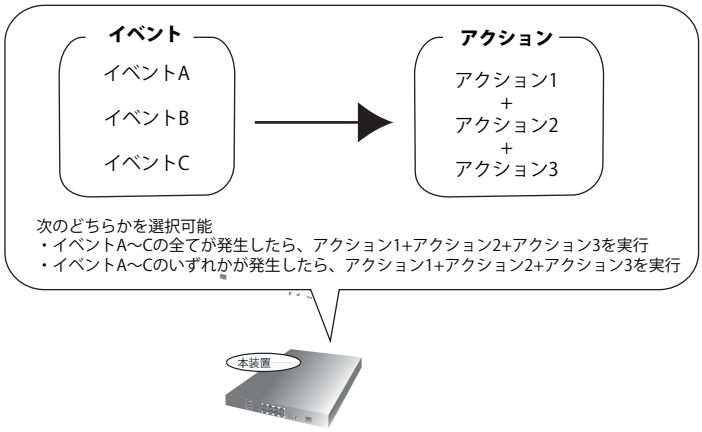
本機能により、上流のマルチキャストルータは受信ノードが存在すると認識してマルチキャストパケットを送信し、IGMP Proxy ルータは上流インタフェースから受信したマルチキャストパケットを下流インタフェースへ中継します。



2.30 イベントアクション機能

イベントアクション機能は，装置障害・ネットワーク障害が発生した際に"～だったら(～が発生したら)…する"というロジックをネットワーク管理者に設定していただき、従来管理者の手動オペレーションにより行なわれていたことを、設定により装置が自動で対応できるようにすることで、ネットワーク管理者の負担の軽減・装置運用の幅を広げることを目的としています。

イベントアクション機能は，ユーザの設定により特定のイベントを検知して，そのイベントに対するアクションを実行する機能です。
イベント検知において、複数のイベントが設定された場合，設定により"全てのイベントが発生した場合にアクションを行う"，"いずれかのイベントが発生したらアクションを行う"の2つのパターンを選択可能としています。
1つのイベントに対して、最大50件のアクションを実行可能です。イベント発生からアクション実行までの待ち時間を指定することも可能です。



監視イベントと実行アクションについて

【監視イベント】

イベント	備考
interface のカウンタを監視する	監視可能な interface は 10 件まで
interface の up/down を監視する	
syslog を監視する	
時刻・タイマを監視する	
ping による疎通監視	監視先は 10 件まで
survey のステータスを監視する	

【アクション】

アクション	備考
CLI コマンドを実行する	対話式コマンドは不可
SNMP Trap を通知する	
syslog メッセージを通知する	
interface の up/down を実行する	
シェルスクリプトを実行する	ユーザ作成のシェルスクリプト実行は未サポート
経路登録を行う	event-track を設定

こんな事に気をつけて

イベントアクション機能では、イベントとアクションの組み合わせにより様々な対応が可能となりますが、組み合わせやパラメータの指定によっては、不安定な状態を継続することも考えられます。本機能を使用される場合には十分な検討をお願いします。

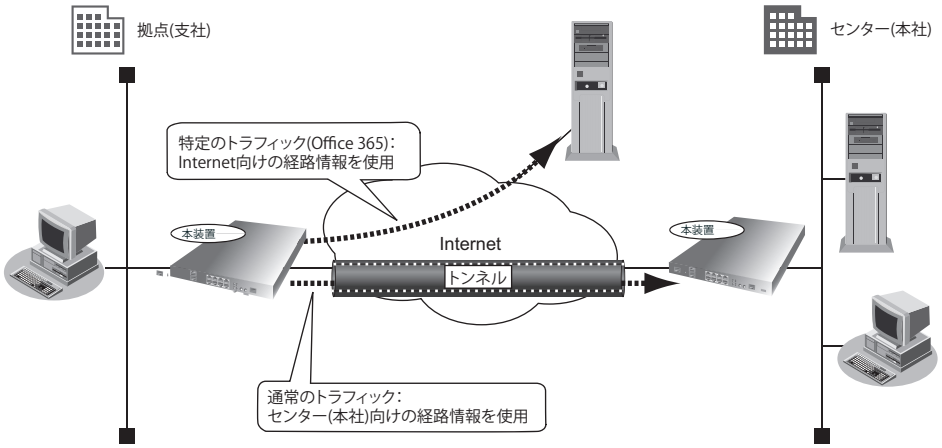
2.31 ローカルブレイクアウト機能

ローカルブレイクアウト機能は、SaaS へのアクセスなど特定のトラフィックを直接インターネットに通すことにより、企業ネットワークのセンターと各拠点を結ぶ WAN 回線の圧迫を防ぐことができる機能です。

通常のトラフィックはセンター向けの経路情報を使用し、特定のトラフィックに対してはインターネット向けとなるように経路情報を登録します。

本装置では、ローカルブレイクアウトの対象として、Microsoft 365（旧 Office365）のトラフィック等をサポートしています。

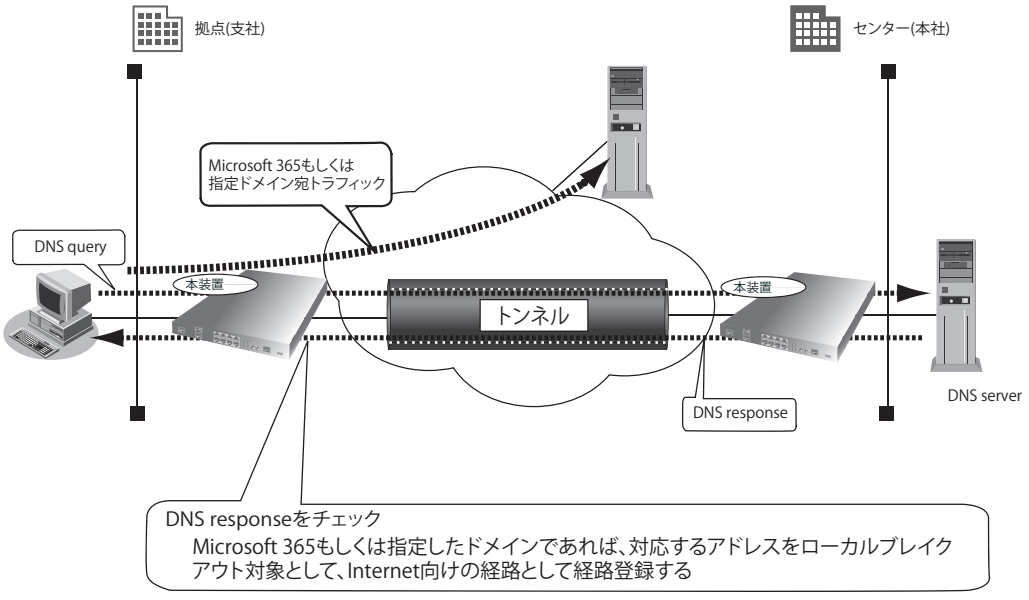
Microsoft が公開している Microsoft 365 エンドポイント情報に Microsoft 365 と通信する際に使用される IPv4, IPv6, FQDN の情報が記載されているので、この情報を基に経路登録を行います。



2.31.1 DNS パケット覗きによる経路情報登録

DNS response パケットを中継する際、パケットの中身をチェックし、Microsoft 365 エンドポイント情報に記載の FQDN の場合は、対応するアドレスをローカルブレイクアウト対象として経路登録します。

Microsoft 365 以外のトラフィックについても、ドメインを指定することにより、当該ドメインに含まれる FQDN の場合に、対応するアドレスをローカルブレイクアウト対象経路として登録可能です。



2.31.2　HTTP パケット覗きによる経路情報登録

プロキシ環境下にて、DNS パケット覗きができない環境を考慮して、HTTP パケット覗きによるローカルブレイクアウトをサポートしました。

下記ページの技術資料「ローカルブレイクアウト機能説明資料」にまとめておりますので、ご参照ください。

URL: https://www.furukawa.co.jp/fitelnet/product/technical/index.html

2.32 ポートミラーリング機能

ポートミラーリング機能とはコマンドにより指定した mirroed port で流れるトラフィックをコピーし、同じくコマンドにより指定した monitor port から出力することでトラフィックを監視する機能です。

monitor port で指定したポートの先に、トラフィックを監視可能な装置を設置してください。

mirrored port の指定では監視対象を受信、送信、送受信から選択できます。

また、mirrored port は複数のポートを指定することも可能です。

こんな事に気をつけて

- ポートミラーリング機能を有効にするとルータの中継処理に影響を及ぼす場合があります。
- mirrored port と monitor port は同一ポートを指定することはできません。
- GigaEthernet 2/1 はポートミラーリング機能で使用できません。
- リンクアグリゲーションしているポート（interface Trunk-channel）のミラーリング中に、トランク・グループへのメンバポートの追加や削除は行わないようにしてください。ミラーリングが正常に行われない場合があります。

2.33 SELECT/ENTER ボタン操作および情報表示ランプ（INFO ランプ）表示機能

「SELECT/ENTER ボタン操作機能」は、装置フロントパネルの SELECT ボタンと ENTER ボタンを操作して、次の処理を行う機能です。

・INFO ランプ表示（通常表示）

・装置電源 OFF 前のコンテナ機能停止

・report-all の取得（実行モード A）

・コンテナ機能の停止（実行モード B）

・イベントアクション連携（実行モード C/D/E）

操作方法の詳細を、「2.33.1 SELECT/ENTER ボタン操作機能」（P.103）で説明します。

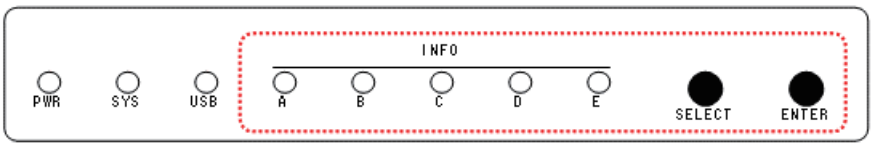
「情報表示ランプ（INFO ランプ）表示機能」は、装置フロントパネルの INFO ランプで以下の情報を表示する機能です。表示の切り替えは設定コマンド（led display-mode）により行います。

・led info-led コマンドによる点灯／点滅／消灯（デフォルト）

・コンテナ機能の動作状態表示

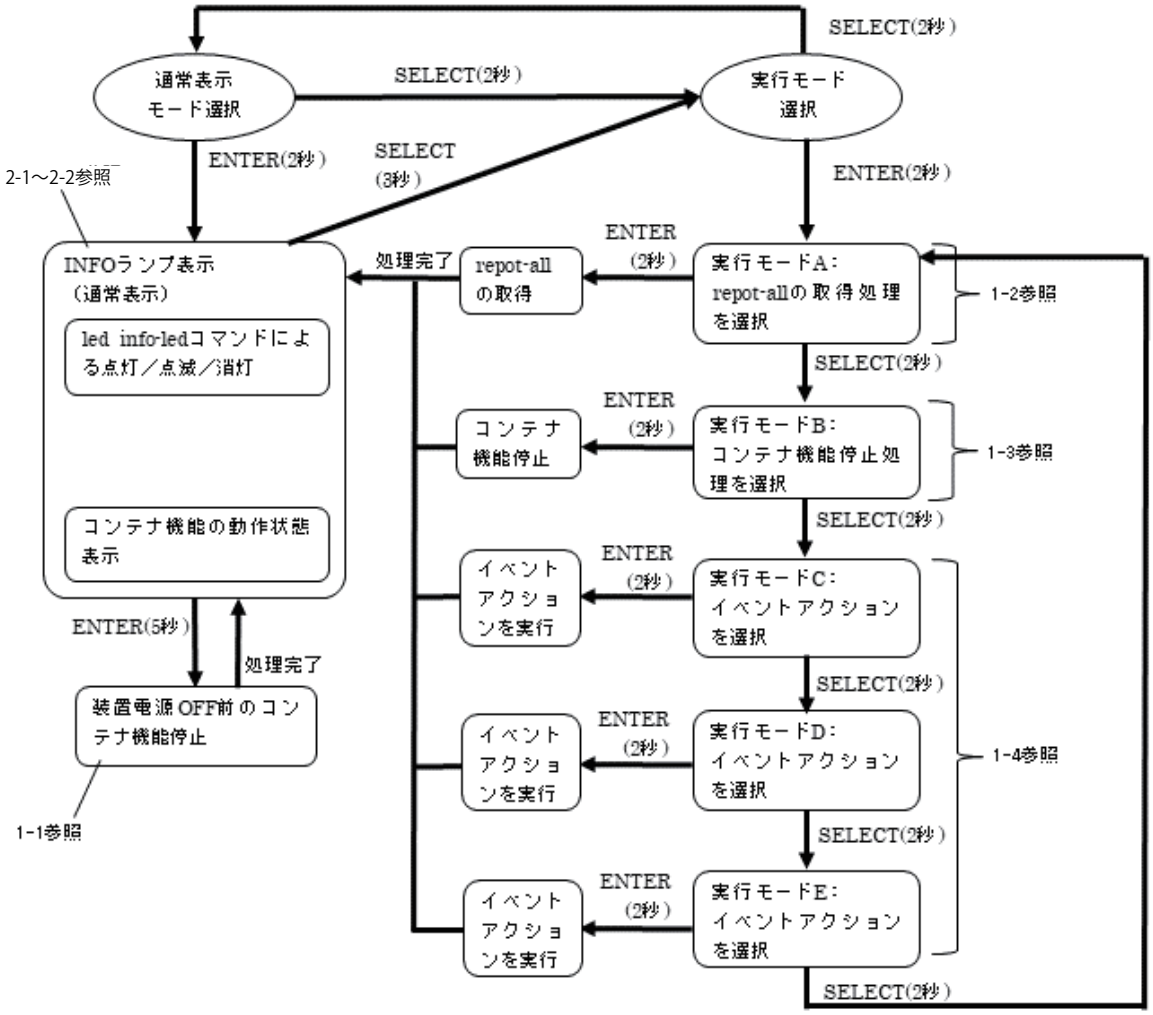
表示の詳細を、「2.33.2 情報表示ランプ（INFO ランプ）表示機能」（P.106）で説明します。

F310 の SELECT/ENTER ボタンと INFO ランプを以下に示します。



F310フロントパネル

本機能の処理フローを以下の図に示します。() 内の秒数は SELECT もしくは ENTER ボタンを長押しする秒数です。装置起動後、ボタン操作の終了、ボタン操作のタイムアウト時は INFO ランプ表示（通常表示）となります。



2.33.1 SELECT/ENTER ボタン操作機能

1-1 装置電源 OFF 前のコンテナ機能停止

装置電源を OFF にする前に ENTER ボタンを 5 秒間長押しする事で、コンテナ機能を停止して、安全に装置電源 OFF できるようにします。操作手順を以下に示します。

手順	操作	実行される処理 （処理フロー図の該当処理を記載）	**INFO** ランプの状態
0	操作前	INFO ランプ表示（通常表示）	通常表示
1	ENTER ボタンを 5 秒間長押し	装置電源 OFF 前のコンテナ機能停止	INFO ランプ (A) を 0.25 秒間隔で緑点滅
2	処理完了まで待機	INFO ランプ表示（通常表示）	正常終了時：INFO ランプ (A) を 10 秒間緑点灯した後、消灯 異常終了時：INFO ランプ (A) を 10 秒間橙点灯した後、消灯

こんな事に気をつけて

- コンテナ機能を使っている場合に、安全に電源 OFF する為に本操作を実行する必要があります。
- コンテナ機能を使用していない場合は、本操作は実行不要です。
- 本操作を実行した後、装置電源 OFF 又は装置再起動を行ってください。

1-2　report-all の取得

report-all を取得する場合に、SELECT ボタンと ENTER ボタンで実行モード A を選択して実行します。操作手順を以下に示します。

手順	操作	実行される処理 （処理フロー図の該当処理を記載）	**INFO** ランプの状態
0	操作前	INFO ランプ表示（通常表示）	通常表示
1	SELECT ボタンを 3 秒間長押し	実行モード選択	全 INFO ランプを 1 秒間隔で緑点滅
2	ENTER ボタンを 3 秒間長押し	実行モード A：report-all の取得処理を選択	INFO ランプ (A) を 1 秒間隔で緑点滅
3	ENTER ボタンを 2 秒間長押し	report-all の取得	INFO ランプ (A) を 0.25 秒間隔で緑点滅
4	処理完了まで待機	INFO ランプ表示（通常表示）	正常終了時：INFO ランプ (A) を 10 秒間緑点灯した後、通常表示 異常終了時：INFO ランプ (A) を 10 秒間橙点灯した後、通常表示

こんな事に気をつけて

report-all の取得ログを /drive/ ディレクトリに report-all_YYYYMMDD_hhmmss.gz というファイル名で保存します（YYYYMMDD_hhmmss は取得日時）。/drive の空き容量を確保した状態で実行してください。

1-3　コンテナ機能の停止

コンテナ機能を停止する場合に、SELECT ボタンと ENTER ボタンで実行モード B を選択して実行します。操作手順を以下に示します。

手順	操作	実行される処理 （処理フロー図の該当処理を記載）	**INFO** ランプの状態
0	操作前	INFO ランプ表示（通常表示）	通常表示
1	SELECT ボタンを 3 秒間長押し	実行モード選択	全 INFO ランプを 1 秒間隔で緑点滅
2	ENTER ボタンを 3 秒間長押し	実行モード A：report-all の取得処理を選択	INFO ランプ (A) を 1 秒間隔で緑点滅
3	SELECT ボタンを 2 秒間長押し	実行モード B：コンテナ機能停止処理を選択	INFO ランプ (B) を 1 秒間隔で緑点滅
4	ENTER ボタンを 2 秒間長押し	コンテナ機能停止	INFO ランプ (B) を 0.25 秒間隔で緑点滅
5	処理完了まで待機	INFO ランプ表示（通常表示）	正常終了時：INFO ランプ (B) を 10 秒間緑点灯した後、通常表示 異常終了時：INFO ランプ (B) を 10 秒間橙点灯した後、通常表示

こんな事に気をつけて

本操作により停止したコンテナ機能を再起動する場合、container enable の設定を削除し refresh した後で、container enable の設定を追加し refresh する必要があります。

1-4 イベントアクション連携

ENTER ボタン押下をイベントとしたイベントアクションを定義して、実行することが可能です。

事前に、ENTER ボタン押下により出力される SYSLOG をイベントアクションと連携する様 に設定します。

設定例：イベント（SYSLOG メッセージ「Button execution mode c」）を監視して、同イベントが確認されたらアクション（INFO ランプ (C) を緑点滅→構成定義 :/drive/default.cfg を refresh →INFO ランプ (C) を消灯）を実行する。

```
!
led display-mode exec-command
!
syslog filter btn-c
 message Button execution mode c
exit
!
logging filter 1 btn-c event-action
!
event-action 1
 event syslog filter btn-c
 action 1.0 cli exec command led info-led c green blink fast
 action 1.1 cli exec command refresh /drive/default.cfg load moff
 action 1.2 cli exec command no led info-led c
exit
!
```

上記イベントアクションを実行する場合には、SELECT ボタンと ENTER ボタンで実行モード C を選択して実行します。操作手順を以下に示します。

手順	操作	実行される処理 （処理フロー図の該当処理を記載）	**INFO** ランプの状態
0	操作前	INFO ランプ表示（通常表示）	通常表示
1	SELECT ボタンを 3 秒間長押し	実行モード選択	全 INFO ランプを 1 秒間隔で緑点滅
2	ENTER ボタンを 3 秒間長押し	実行モード A：report-all の取得処理を選択	INFO ランプ (A) を 1 秒間隔で緑点滅
3	SELECT ボタンを 2 秒間長押し	実行モード B：コンテナ機能停止処理を選択	INFO ランプ (B) を 1 秒間隔で緑点滅
4	SELECT ボタンを 2 秒間長押し	実行モード C：イベントアクションを選択	INFO ランプ (C) を 1 秒間隔で緑点滅

手順	操作	実行される処理 （処理フロー図の該当処理を記載）	**INFO** ランプの状態
5	ENTER ボタンを 2 秒間長押し	イベントアクションを実行	INFO ランプ (C) を 0.25 秒間隔で緑点滅 （構成定義にて定義を行う）
6	処理完了まで待機	INFO ランプ表示（通常表示）	INFO ランプ (C) を消灯後、通常表示 （構成定義にて定義を行う）

実行モード D もしくは E のイベントアクションを実行する場合には、手順 4 を繰り返して実行モード D もしくは E のイベントアクションを選択します。

参照 「2.30 イベントアクション機能」（P.97）

2.33.2 情報表示ランプ（INFO ランプ）表示機能

設定コマンド（led display-mode）により、次の 3 つのうちのいずれかを選択します。

1 led info-led コマンドによる点灯／点滅／消灯（デフォルト）

2 コンテナ機能の動作状態表示

参照 マニュアル「コマンドリファレンス－構成定義編」の「led display-mode」

2-1 led info-led コマンドによる点灯／点滅／消灯

デフォルトもしくは led display-mode exec-command 設定時に、led info-led コマンドによる INFO ランプの点灯／点滅／消灯の制御が行われます。

参照 マニュアル「コマンドリファレンス－運用管理編」の「led display-mode exec-command 」、「led info-led」

実行例
★INFOランプ(A)を緑点灯
FITELnet#led info-led a green

% Command succeeded.
★INFOランプ(A)を1秒間隔で橙点滅
FITELnet#led info-led a amber blink

% Command succeeded.
★INFOランプ(A)を消灯
FITELnet#no info-led a

% Command succeeded.

補足 イベントアクション機能のアクションとして、led info-ledコマンドを実行する事で、イベントの状態をINFOランプに反映する事ができます。「2.30 イベントアクション機能」（P.97）をご参照ください。

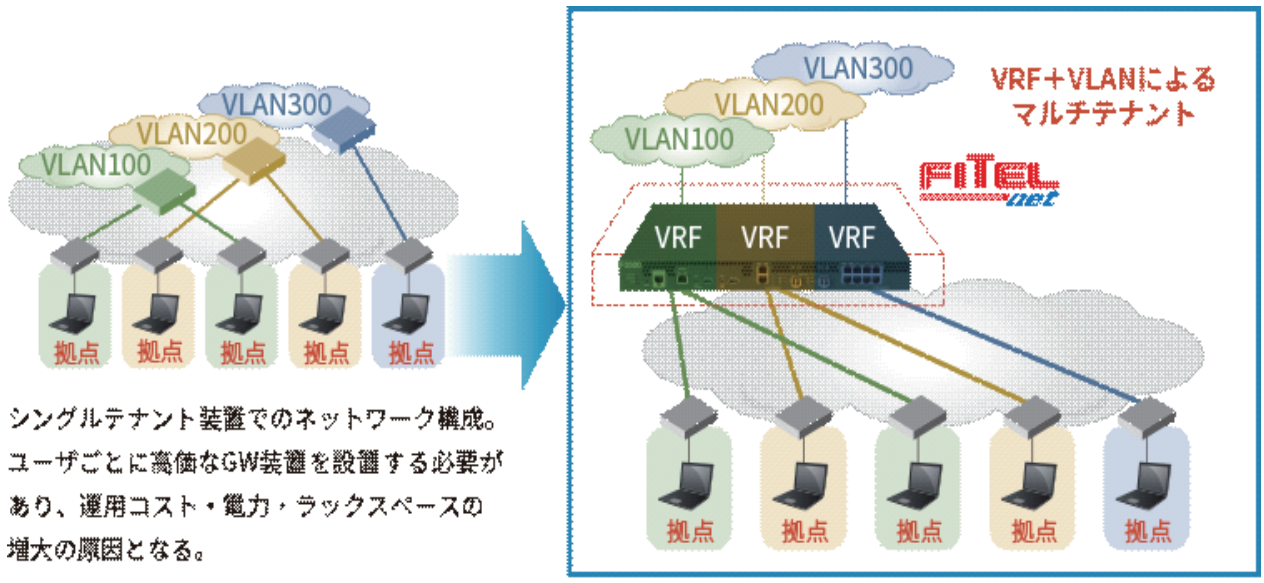
2-2　コンテナ機能の動作状態表示

led display-mode container-status 設定時に、コンテナ機能の動作状態を INFO ランプ (A) で表示します。

コンテナ機能の動作状態	**INFO** ランプの状態
コンテナ機能動作中	INFO ランプ (A) を緑点灯
コンテナ機能停止中	INFO ランプ (A) を消灯

2.34 VRF 機能

本装置では、VRF 機能をサポートしています。VRF 機能を使用することにより、複数のテナントユーザを独立した VRF に収容することが可能です。テナントユーザ毎にそれぞれ異なる IPsec トンネルを利用した通信が可能です。
1 台で複数のテナントを収容できるため、テナント毎にセンター機を用意する必要がなく、運用コストや電力、ラックスペースを軽減することが出来ます。



参照　本装置のVRF対応機能は、マニュアル「仕様一覧　2.4 VRF対応機能一覧」をご参照ください。

VRFの設定方法については、マニュアル「コマンドリファレンス　- 構成定義編-」付録（VRF設定の関連付け動作について）を参照してください。

2.35 コンテナ機能

本装置では、コンテナ型仮想環境を作成することができます。ルータ OS から隔離された、仮想マシンのような独立した環境で様々なアプリケーションを実行することが可能です。

また、ルータ OS とコンテナ環境は内部のインタフェースを経由して通信することができます。コンテナ環境でネットワーク解析用アプリケーションを動作させることで、ルータ装置の中継データ等を解析することも可能です。

コンテナ機能の使用を希望される場合は、別途手順書等を提供させていただきますので、弊社までお問い合わせください。

こんな事に気をつけて

- 電源 OFF を行う際には、コンテナ機能を停止してから電源 OFF するようにしてください。コンテナ機能は、container stop コマンドを実行するか、もしくは装置本体の ENTER ボタンを 5 秒間長押しすることにより停止します。
- コンテナ機能を停止せずに電源 OFF を行った場合には、コンテナで使用しているファイルが破損する可能性があります。
- 急な停電等に備えて、コンテナで使用しているファイルのバックアップを行うようにしてください。container backup コマンドによりコンテナをイメージファイルとして保存すること、container restore コマンドによりコンテナをイメージファイルから復元して起動することが、それぞれ可能です。

参照 container backupコマンドとcontainer restoreコマンドについては、マニュアル「コマンドリファレンス - 運用管理編-」を参照してください。

索引

記号

A

B

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W

あ

い

え

か

き

く

け

こ

さ

し

す

せ

た

つ

て

と

な

に

ね

は

ひ

ふ

へ

ほ

ま

ゆ

よ

り

る

ろ

FITELnet F310　機能説明書

130-B0501-BS01

発行日　　2024年2月

発行責任　　古河電気工業株式会社