

All to brighten the world

FURUKAWA
ELECTRIC

FITELnet FH10 一般版

機能説明書

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。

本ドキュメントには「外国為替及び外国貿易管理法」に基づく特定技術が含まれています。
従って本ドキュメントを輸出または非居住者に提供するとき、同法に基づく許可が必要となります。
Microsoft Corporation のガイドラインに従って画面写真を使用しています。

©Furukawa Electric Co., Ltd

目次

はじめに	2
第 1 章 ネットワーク設計概念.....	5
1.1 レイヤ 2 ネットワーク設計概念	6
1.1.1 VLAN	6
1.2 ネットワーク設計概念	8
1.2.1 ネットワークの概念とルーティング	8
1.2.2 ルータ設定の概要	12
第 2 章 機能概要.....	13
2.1 VLAN 機能	15
2.2 バックアップポート機能	18
2.3 ポート間アクセス制御機能	19
2.4 ARP エージング機能	20
2.5 IPv6 機能	21
2.6 IP 経路制御機能	24
2.6.1 IP 経路情報の種類	24
2.6.2 IP 経路情報の管理	25
2.6.3 スタティックルーティング機能	26
2.6.4 ダイナミックルーティング機能	26
2.7 RIP 機能	28
2.8 BGP4 機能	30
2.9 OSPF 機能	33
2.10 IPv6 OSPF 機能	35
2.11 IP フィルタリング機能	36
2.11.1 動的フィルタリング (SPI)	37
2.12 ポリシールーティング機能	38
2.12.1 Ingress ポリシールーティング機能	38
2.13 IPsec 機能	40
2.14 NAT 機能	45
2.14.1 NAT 機能の選択基準	47
2.15 TOS/Traffic Class 値書き換え機能	48
2.16 シェーピング機能	49
2.17 帯域制御 (WFQ) 機能	50
2.17.1 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	51
2.18 DHCP 機能	53
2.18.1 IPv4 DHCP 機能	53
2.18.2 IPv6 DHCP 機能	55
2.19 DNS サーバ機能	58
2.19.1 DNS サーバ (スタティック) 機能	58
2.19.2 ProxyDNS (DNS 振り分け) 機能	58
2.20 SNMP 機能	60
2.20.1 ifIndex の割り当てと ifDescr	61
2.21 ECMP 機能	62
2.21.1 通信パス選択方法	63
2.21.2 通信バックアップ機能	64

2.22	VRRP 機能	65
2.22.1	簡易ホットスタンバイ機能	65
2.22.2	クラスタリング機能	67
2.23	ブリッジグループ機能	70
2.23.1	ブリッジグループピンギング機能	70
2.23.2	IP フレームの転送ポリシー	70
2.24	透過モード	71
2.24.1	VLAN モードと透過モード	71
2.24.2	透過モードとブリッジグループ機能	72
2.25	リンクアグリゲーション機能	73
2.25.1	LACP 機能	73
2.26	通信バックアップ機能	74
2.26.1	通信障害の検出機能	75
2.26.2	検出された通信障害に対する通信パス迂回機能	78
2.27	BFD 機能	81
2.28	ダイナミックセレクトタ機能	82
2.29	RADIUS 機能	83
2.29.1	RADIUS クライアント機能	83
2.30	SSH サーバ機能	84
2.31	アプリケーションフィルタ機能	86
2.32	PKI 機能	87
2.33	USB メモリ機能	88
2.33.1	構成定義の転送と保存	88
2.34	イベントアクション機能	89
索引	91

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.....	6
1.1.1	VLAN	6
1.2	ネットワーク設計概念.....	8
1.2.1	ネットワークの概念とルーティング.....	8
1.2.2	ルータ設定の概要.....	12

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

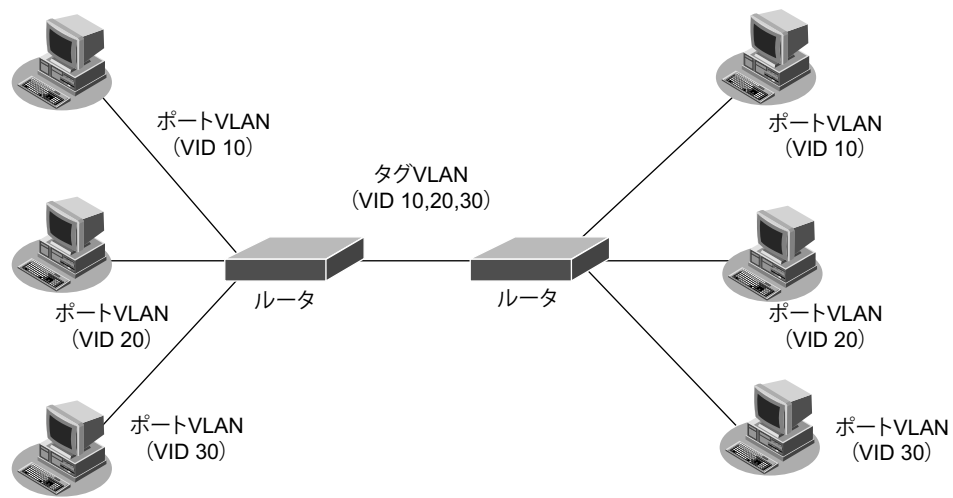
各VLANには10進数で1から4094までの番号を付けて管理します。これをVLAN IDと言います。同じVLAN IDを持つVLANに属している装置間では通信可能ですが、異なるVLAN IDを持つVLANに属している装置間では通信はできません。

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2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。



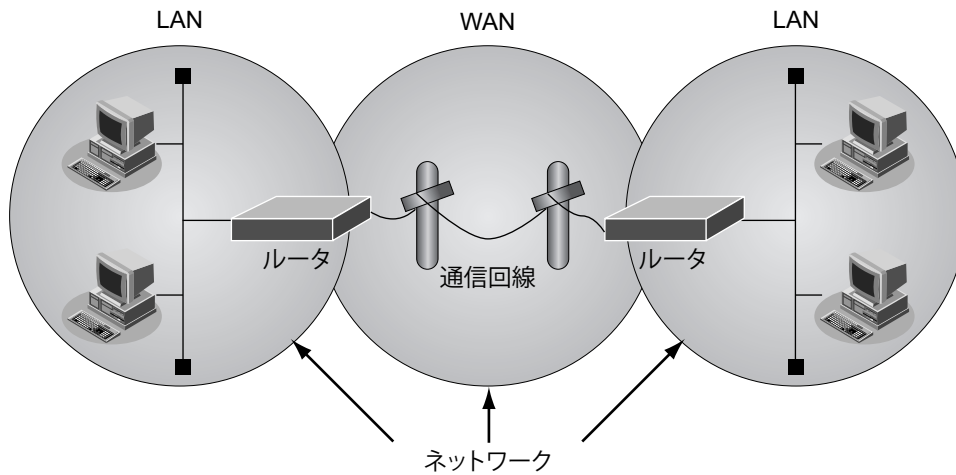
1.2 ネットワーク設計概念

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

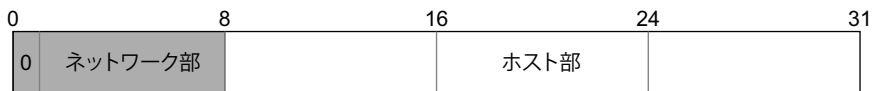
ネットワークとは、通信手段を備えたコンピュータ同士がなんらかの伝送媒体を介して接続した集合体のことです。たとえば、構築された1つのLANは、HUBやスイッチなどの装置によって1つのネットワークとなります。一般加入線や専用回線などを利用して遠隔地を接続しているWANと呼ばれる部分についても、同様に1つのネットワークとなります。また、広義の意味で、これら1つ1つのネットワークが接続された全体もネットワークとなります。



IP ネットワーク

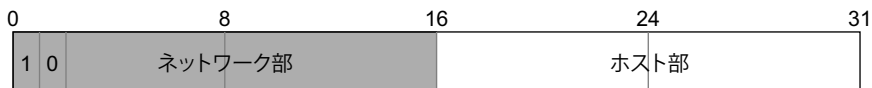
IP ネットワークでは、接続されるすべてのコンピュータ（ホスト）やルータなどのネットワーク機器それぞれに唯一のIPアドレスを割り当てる必要があります。このIPアドレスは「ネットワーク部」と「ホスト部」から構成されます。

クラスA 各ネットワークにホストが多く存在し、ネットワーク数が少ない場合



プライベートアドレス: 10.0.0.0~10.255.255.255

クラスB ネットワーク、ホストともに多い場合



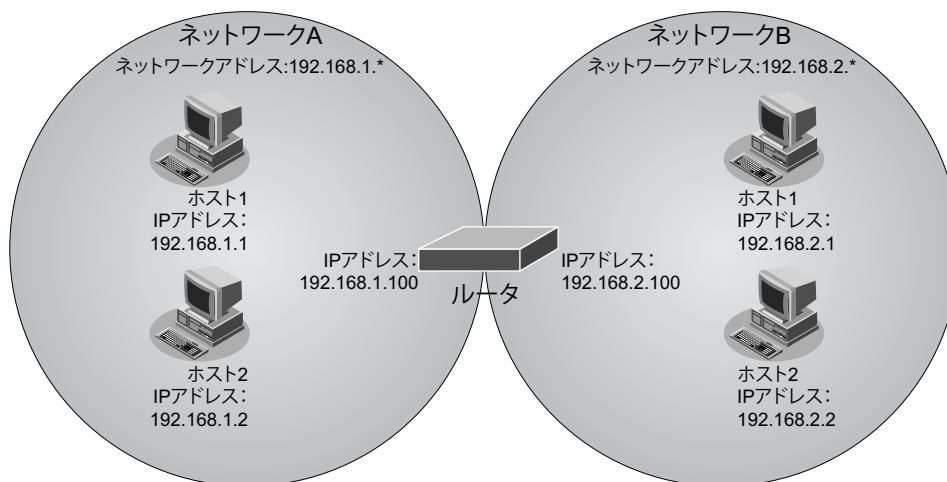
プライベートアドレス: 172.16.0.0~172.31.255.255

クラスC ネットワークごとのホストが少なく、ネットワーク数が多い場合



プライベートアドレス: 192.168.0.0~192.168.255.255

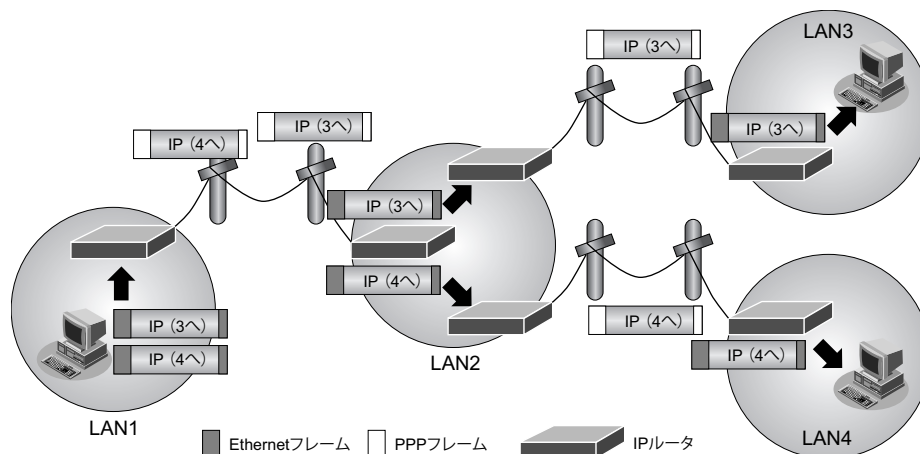
IP ネットワークでの1つのネットワークとは、IPアドレスのネットワーク部が同じアドレスを持つ機器の集まりです。つまり、同じデータリンクに接続される機器にはすべて同じネットワークアドレスを設定しなければなりません。さらに、ほかのデータリンクとネットワークアドレスが重ならないように割り当てる必要があります。



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。



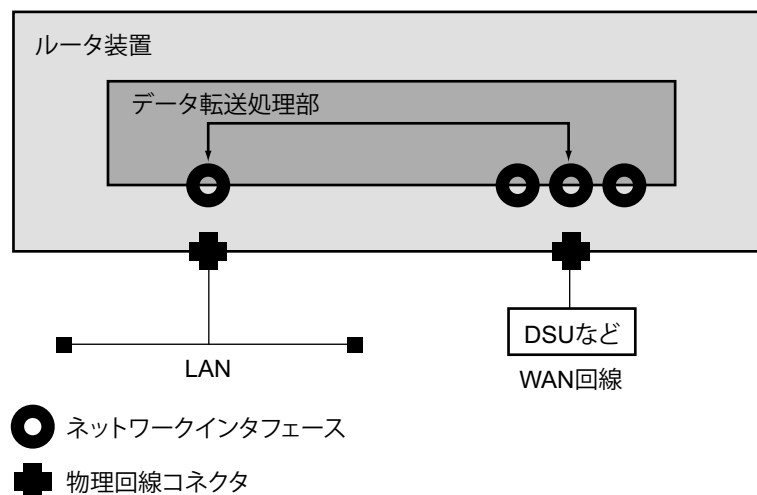
なお、本装置では IP 以外のパケットを転送する機能であるブリッジについてもサポートしています。IP アドレスを持たない IP 以外のパケットは、Ethernet フレームの情報に従って適切な相手にデータを転送することができます。

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 「2.12 ポリシールーティング機能」(P.38)

第2章 機能概要

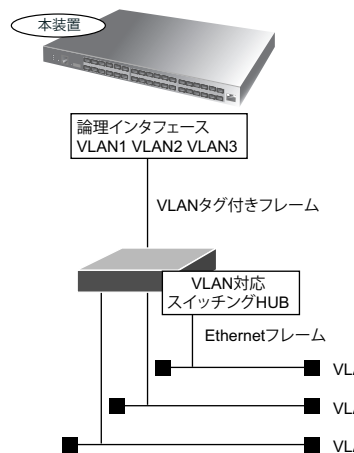
この章では、本装置の主な機能の概要を説明します。

2.1	VLAN 機能.....	15
2.2	バックアップポート機能.....	18
2.3	ポート間アクセス制御機能.....	19
2.4	ARP エージング機能.....	20
2.5	IPv6 機能.....	21
2.6	IP 経路制御機能.....	24
	2.6.1 IP 経路情報の種類.....	24
	2.6.2 IP 経路情報の管理.....	25
	2.6.3 スタティックルーティング機能.....	26
	2.6.4 ダイナミックルーティング機能.....	26
2.7	RIP 機能.....	28
2.8	BGP4 機能.....	30
2.9	OSPF 機能.....	33
2.10	IPv6 OSPF 機能.....	35
2.11	IP フィルタリング機能.....	36
	2.11.1 動的フィルタリング (SPI).....	37
2.12	ポリシーラーティング機能.....	38
	2.12.1 Ingress ポリシーラーティング機能.....	38
2.13	IPsec 機能.....	40
2.14	NAT 機能.....	45
	2.14.1 NAT 機能の選択基準.....	47
2.15	TOS/Traffic Class 値書き換え機能.....	48
2.16	シェーピング機能.....	49
2.17	帯域制御 (WFQ) 機能.....	50
	2.17.1 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.....	51

2.18	DHCP 機能	53
	2.18.1 IPv4 DHCP 機能.....	53
	2.18.2 IPv6 DHCP 機能.....	55
2.19	DNS サーバ機能	58
	2.19.1 DNS サーバ (スタティック) 機能.....	58
	2.19.2 ProxyDNS (DNS 振り分け) 機能.....	58
2.20	SNMP 機能	60
	2.20.1 ifIndex の割り当てと ifDescr.....	61
2.21	ECMP 機能	62
	2.21.1 通信パス選択方法.....	63
	2.21.2 通信バックアップ機能	64
2.22	VRRP 機能	65
	2.22.1 簡易ホットスタンバイ機能.....	65
	2.22.2 クラスタリング機能.....	67
2.23	ブリッジグループ機能.....	70
	2.23.1 ブリッジグループピング機能.....	70
	2.23.2 IP フレームの転送ポリシー	70
2.24	透過モード	71
	2.24.1 VLAN モードと透過モード.....	71
	2.24.2 透過モードとブリッジグループ機能.....	72
2.25	リンクアグリゲーション機能.....	73
	2.25.1 LACP 機能.....	73
2.26	通信バックアップ機能.....	74
	2.26.1 通信障害の検出機能.....	75
	2.26.2 検出された通信障害に対する通信パス迂回機能.....	78
2.27	BFD 機能.....	81
2.28	ダイナミックセレクト機能	82
2.29	RADIUS 機能.....	83
	2.29.1 RADIUS クライアント機能	83
2.30	SSH サーバ機能.....	84
2.31	アプリケーションフィルタ機能.....	86
2.32	PKI 機能	87
2.33	USB メモリ機能	88
	2.33.1 構成定義の転送と保存	88
2.34	イベントアクション機能	89

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を定義するという事は、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

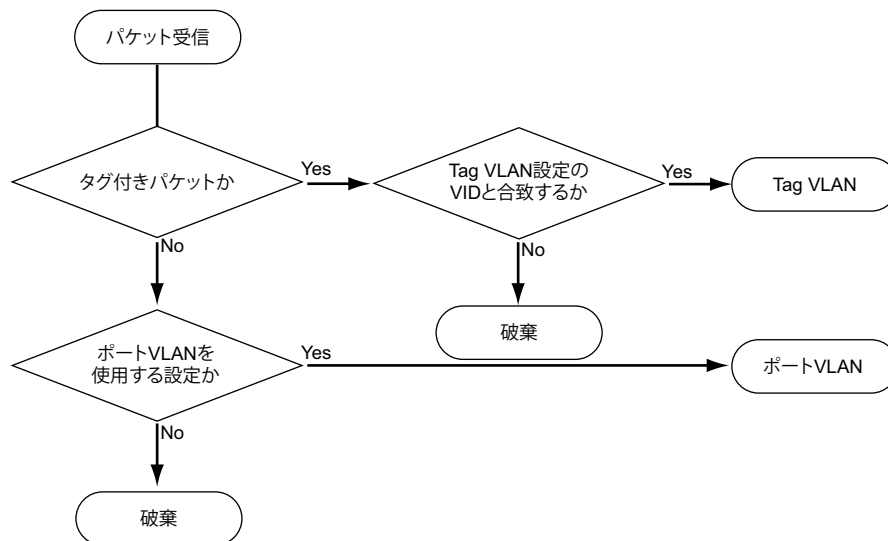
同一ポート上で使用できるVLANの組み合わせを以下に示します。

○：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。



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。

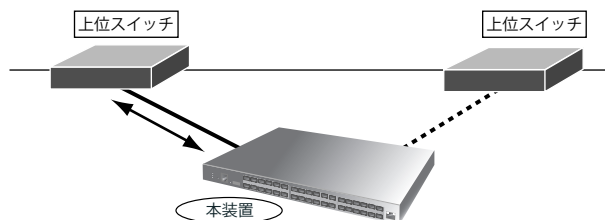
参照 マニュアル「仕様一覧」

2.2 バックアップポート機能

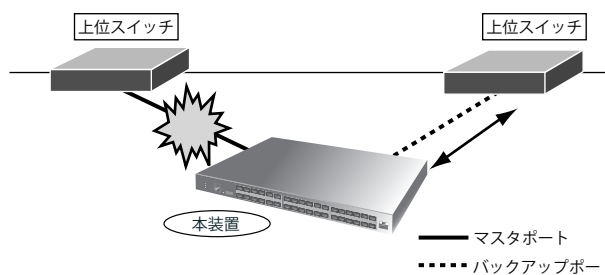
バックアップポート機能とは、リンクアグリゲーションで2つのポートをグループ化し、片方のポートをマスターポート（優先ポート）、もう一方のポートをバックアップポート（待機ポート）として管理し、常にどちらか一方のポートだけを稼働させる機能です。

稼働中のポートになんらかの障害が発生した場合に、もう一方の待機ポートを瞬時に稼働ポートに切り替えることで、ネットワーク障害の影響を最小限に抑えることが可能です。

- ・通常時は、マスターポートで通信



- ・マスターポートに障害が発生した場合は、瞬時にバックアップポートで通信

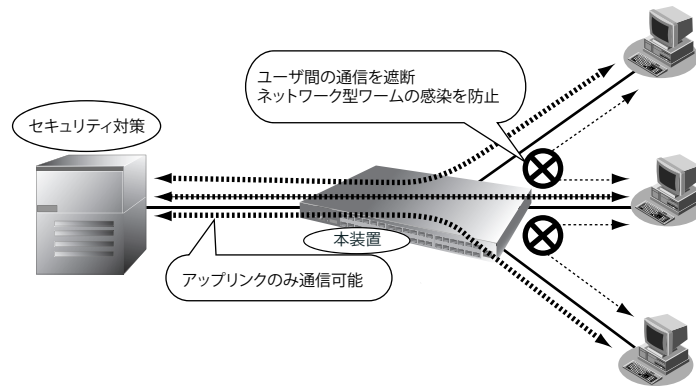


こんな事に気をつけて

バックアップポート機能では、障害発生時に稼働ポートを瞬時に切り替えることが可能ですが、各種プロトコルを使用した場合、通信が復旧するまでに各プロトコルでの復旧時間が必要となります。

2.3 ポート間アクセス制御機能

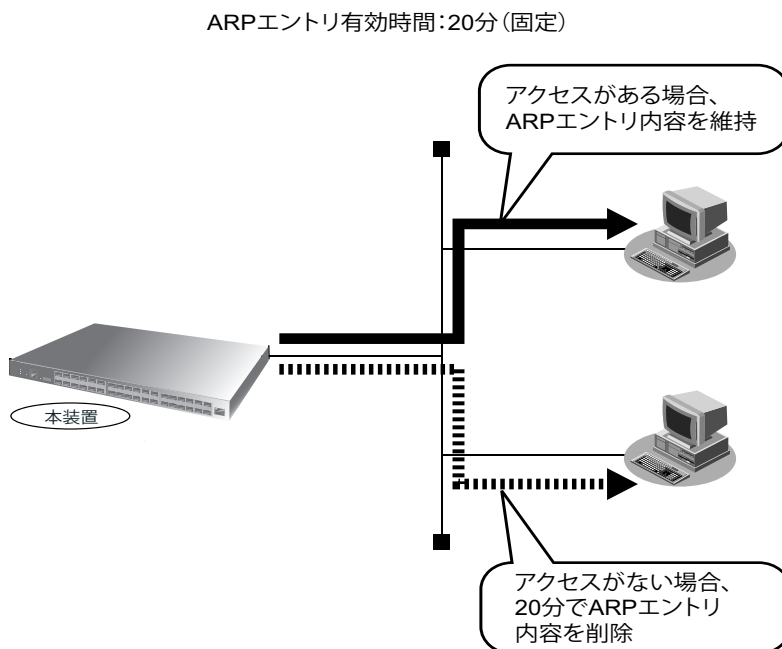
本装置配下に接続された端末（ユーザ）は、本装置の上位だけでアクセス可能とし、本装置配下の端末間での通信を防止する機能です。この機能により、ネットワーク型ワームの感染を防止でき、また、本装置配下の端末（ユーザ）が不正にほかの端末のデータを受信することも防止できます。



2.4 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。

2.5 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。

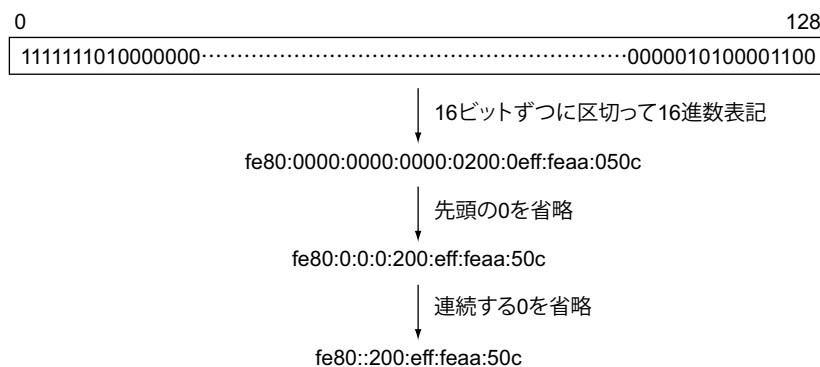
本装置がサポートしているIPv6機能は、以下のとおりです。

- 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。

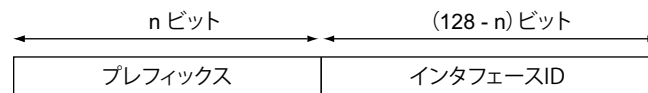
例を以下に示します。



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）

2.6 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。

2.6.1 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。
- IKE 経路 (IPv4/IPv6)
VPN 接続で情報交換された相手 IKE セッション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。

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)
IKE 経路	IPv4/IPv6	1 (変更可)
DHCP クライアント経路	IPv4	1 (固定)
DHCP クライアント経路	IPv6	254 (固定)
DHCP サーバ経路	IPv6	254 (固定)

2.6.2 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、以下のものを含まます。
 - 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、以下のものを含まます。
 - 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、以下のものを含まます。
 - 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、以下のものを含まみます。
 - 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、以下のものを含まみます。
 - 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」

2.6.3 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 「2.21 ECMP 機能」(P.62)

- 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。

2.6.4 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 「2.7 RIP 機能」(P.28)、 「2.8 BGP4 機能」(P.30)、 「2.9 OSPF 機能」(P.33)、 「2.10 IPv6 OSPF 機能」(P.35)、 「2.21 ECMP 機能」(P.62)

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。

2.7 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、いくつか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) に準拠していません。

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 1, 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 <ul style="list-style-type: none"> ・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 <ul style="list-style-type: none"> ・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

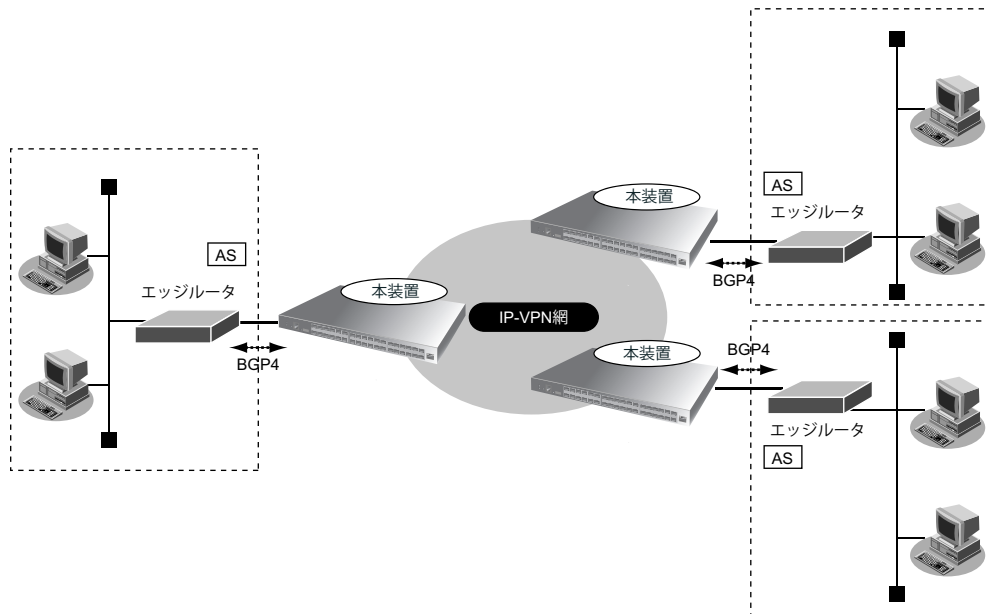
RIP 機能を使用する場合、定期的にパケットを送信します。このため、定額制でない回線を使用している場合は、超過課金の原因となることがあります。このような環境では RIP 機能は使用しないでください。

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。
-

2.8 BGP4機能

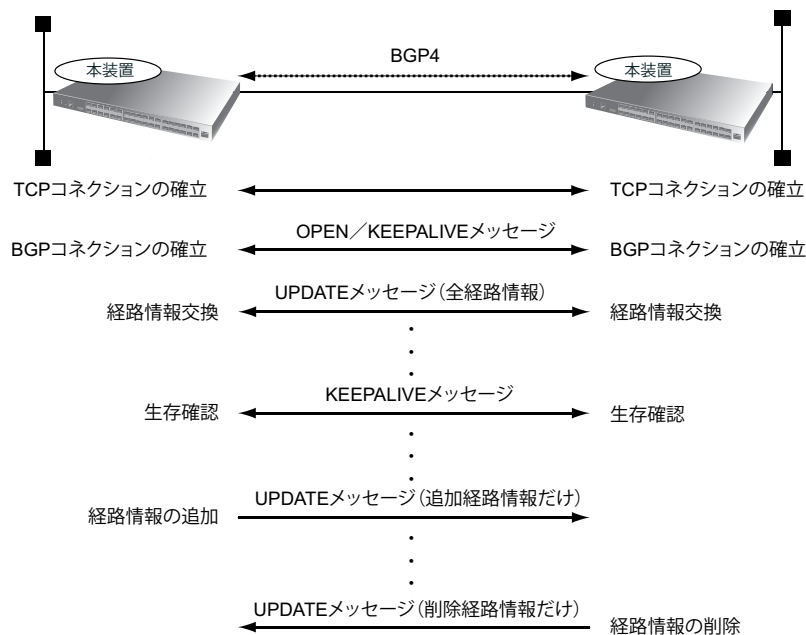
BGP4 (Border Gateway Protocol version4) 機能とは、AS (自律システム: 同じポリシーに従って運用されているネットワークの単位) 間で経路情報を交換するためのルーティングプロトコル機能です。BGP4機能は、IP-VPNサービスで、信頼性の高いネットワーク構成を構築するために必要な機能です。



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 <ul style="list-style-type: none"> • 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
アドレスファミリー	IPv4 セッションでは、以下のアドレスファミリーをサポート <ul style="list-style-type: none"> • IPv4 Unicast, VPNv4 IPv6 セッションでは、以下のアドレスファミリーをサポート <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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。

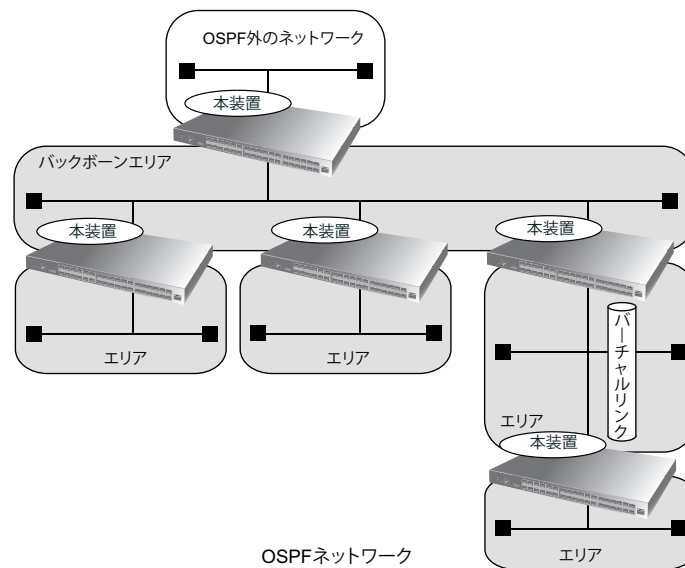
2.9 OSPF 機能

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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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。

2.10 IPv6 OSPF 機能

IPv6 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。

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

- RFC2740:OSPF for IPv6

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3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境界ルータでのデフォルトルート広報	サポート
Passive-Interface	サポート
OSPF への再配布	以下のIPv6経路情報の再配布をサポート <ul style="list-style-type: none"> • 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 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	BGP (IPv6) での広報をサポート
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 <ul style="list-style-type: none"> • 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
エリア間プレフィックスLSA入出力可否	エリア境界ルータでエリア間の入出力時の透過/破棄を指定可能

⚠注意

IPv6 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。

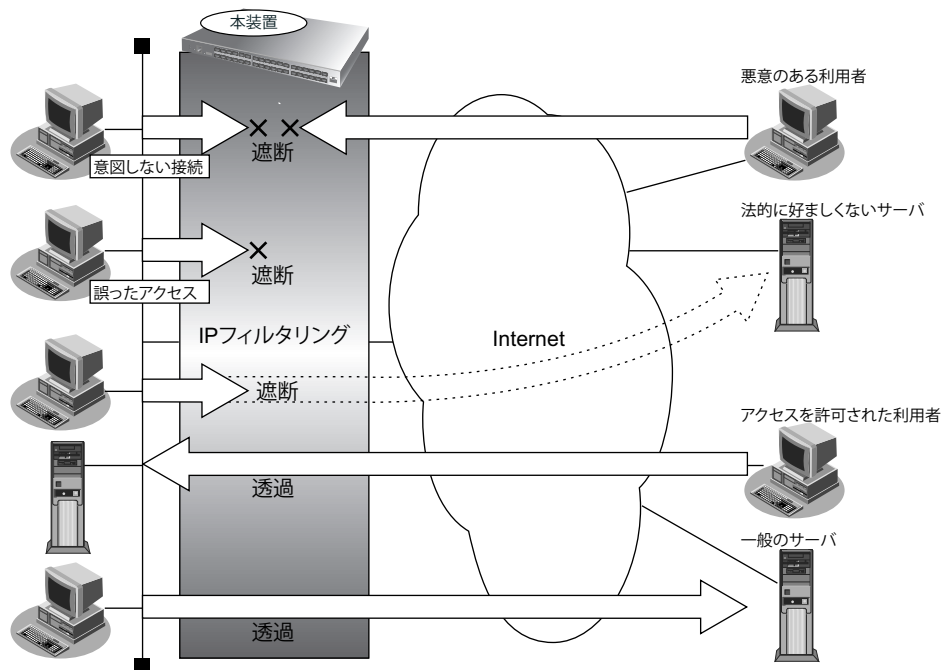
こんな事に気をつけて

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。

2.11 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。

接続形態に応じてセキュリティ方針を決める

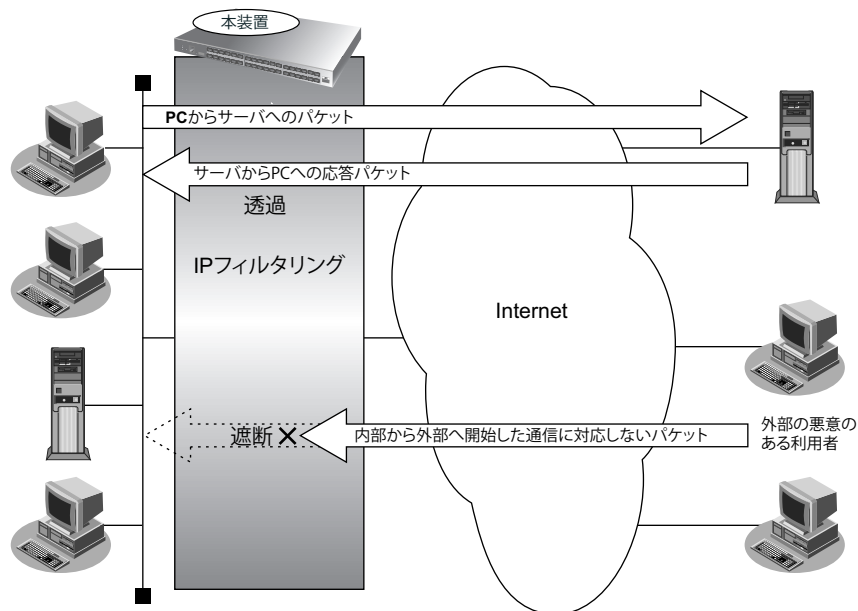
インターネットに接続する場合でもLAN同士を接続する場合でも、データの流れには「外部から内部へ」、「内部から外部へ」という2つの方向があります。セキュリティ方針を決める場合は、2つの方向について考慮する必要があります。

- 「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

2.11.1 動的フィルタリング (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。

2.12 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。

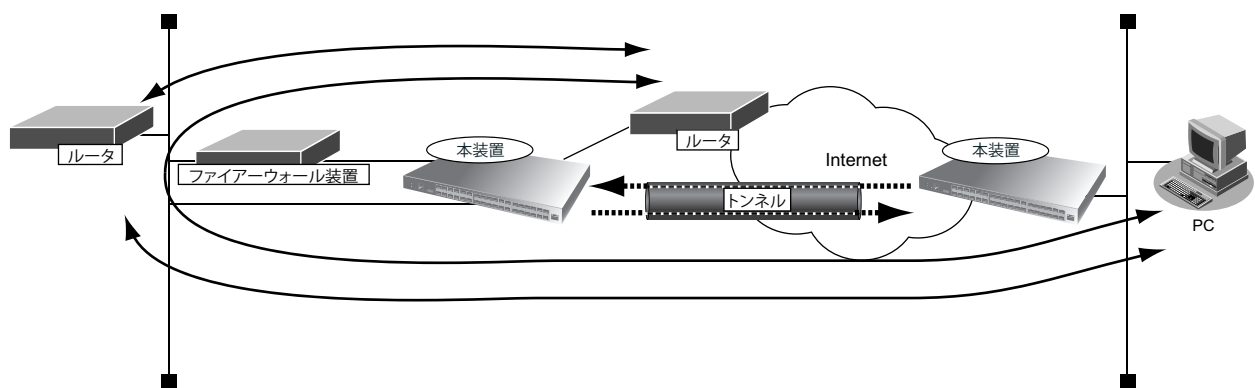
本装置では、IPルーティングによる転送先選定の前にポリシーに応じた転送先選定を行う **Ingress** ポリシールーティングが利用できます。

2.12.1 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。

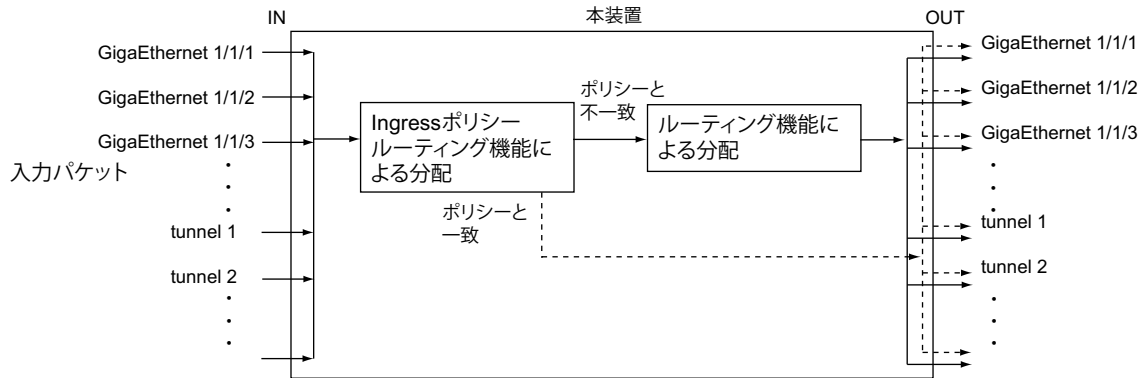
こんな事に気をつけて

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。

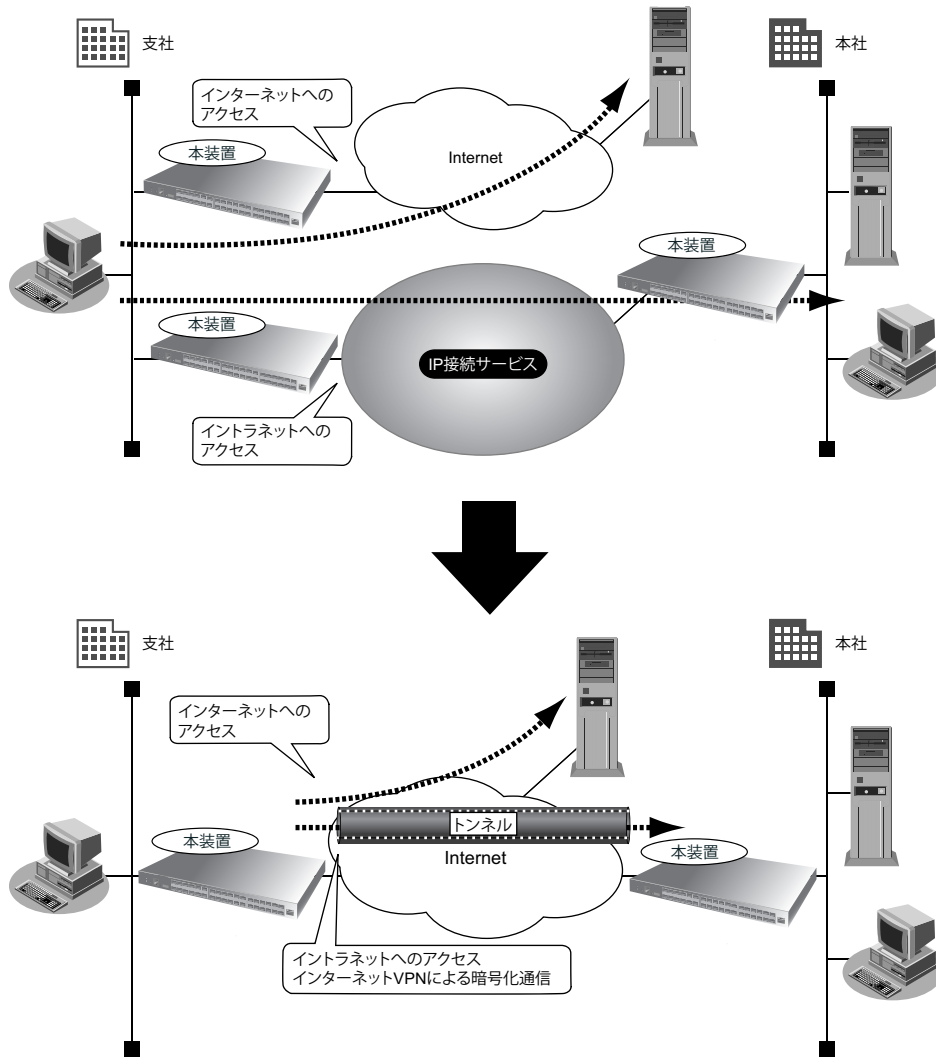
こんな事に気をつけて

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。

2.13 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。

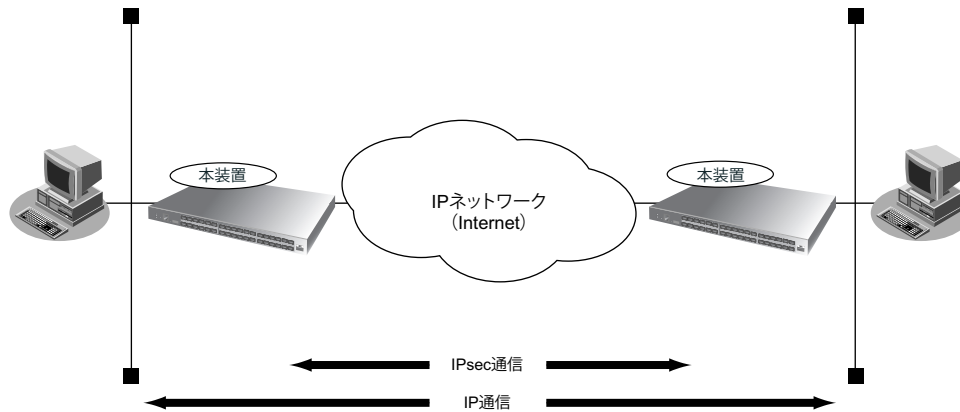
VPNではVPN装置間でデータをカプセル化し、相手のVPN装置に送信します。その際、データの盗聴、改ざんを防止するために、認証や暗号化などのセキュリティ機能によりデータを保護します。これにより、簡単に機密性の高いシステムが構築できます。



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、RSA デジタル署名認証方式、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)
暗号アルゴリズム	DES-CBC、3DES-CBC、AES-CBC
認証アルゴリズム	HMAC-MD5、HMAC-SHA1、HMAC-SHA2 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。

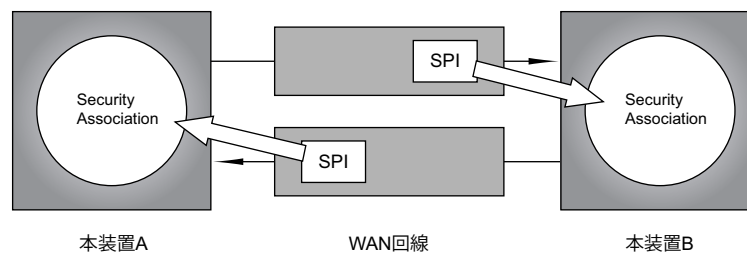
- RFC2104: "HMAC: Keyed-Hashing for Message Authentication"
- RFC2401: "Security Architecture for the Internet Protocol"
- RFC2402: "IP Authentication Header"
- RFC2403: "The Use of HMAC-MD5-96 within ESP and AH"
- RFC2404: "The Use of HMAC-SHA1-96 within ESP and AH"
- RFC2405: "The ESP DES-CBC Cipher 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)"
- RFC2410: "The NULL Encryption Algorithm and Its Use With IPsec"
- RFC2411: "IPsec 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。

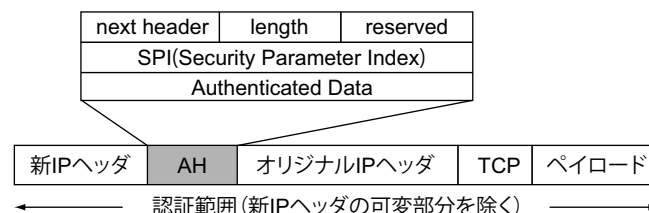
1つのホストは複数の通信に対応するための複数のSAを持っています。このため、受け取ったIPsecのパケットが、どのSAに対応するものなのかを識別する必要があります。識別するためのパラメータとして、あとに説明するAHやESPのヘッダに含まれるSPI（Security Parameter Index）を使用します。



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。

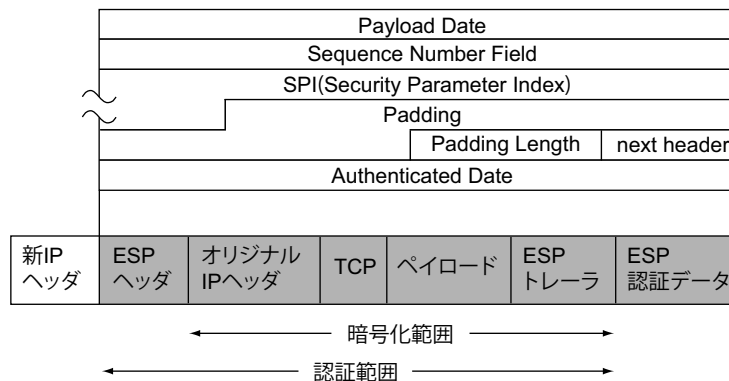
AHは認証アルゴリズム・認証キー・暗号アルゴリズム・暗号キー・キー寿命・キー配送方法などを決めるSPI値と、認証アルゴリズムで使用するデータ・フィールドAuthenticated Dataから成り立っています。

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

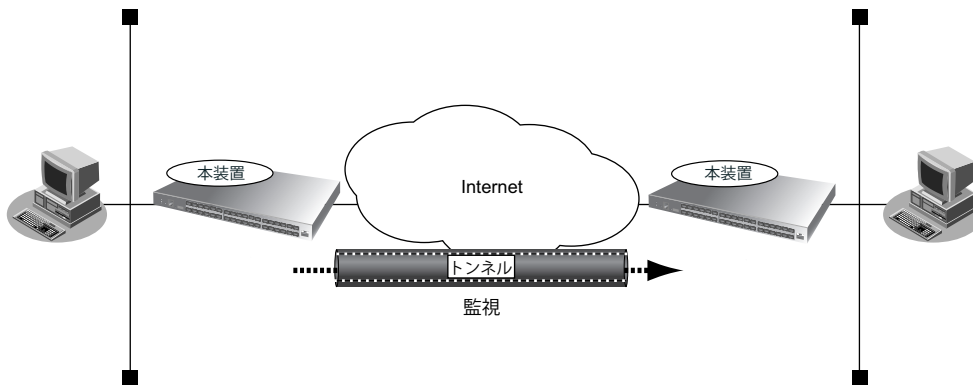
自動鍵交換（IKE）で、通信する相手の認証（本人性確認）を行います。本装置では、以下の3つの認証方式をサポートします。

- 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、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はトラフィック(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。

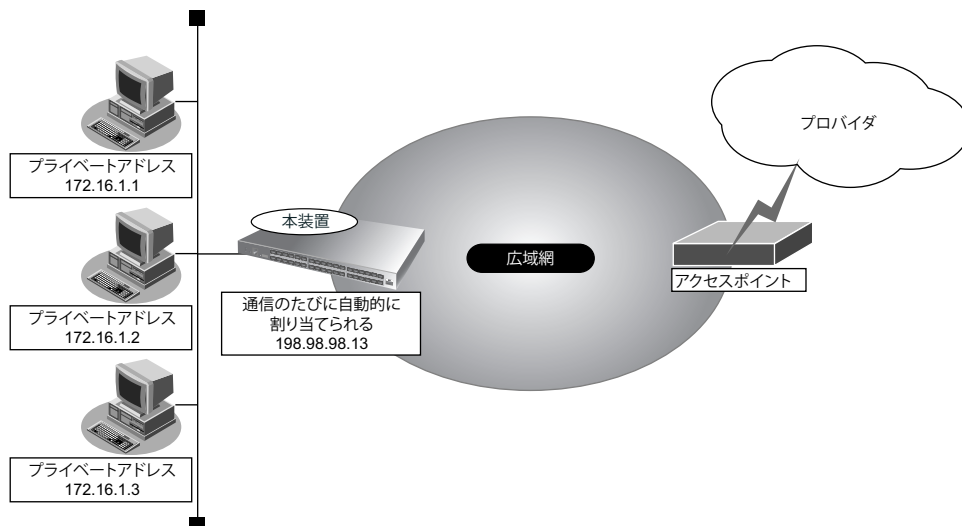
補足 ポート番号を変化させないNATで、スタティックにESPパケットを通過させるような場合は、NATトラバーサルを使用しなくてもIPsec通信ができます。

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

2.14 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）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。

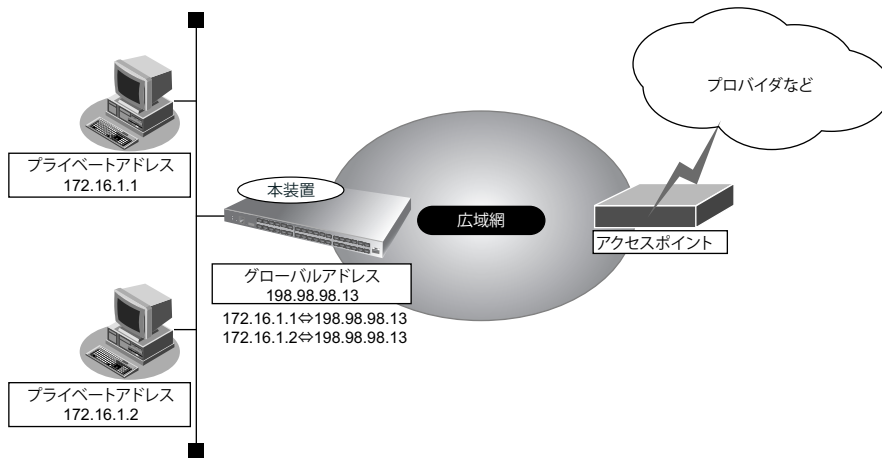
- 動的NAT
- 静的NAT
- NAT宛先変換

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。

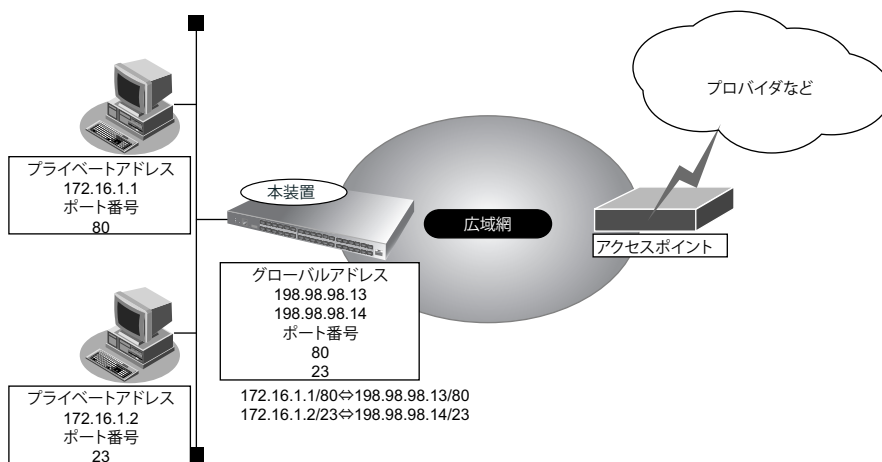
◆ 動的 NAT とは

「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。



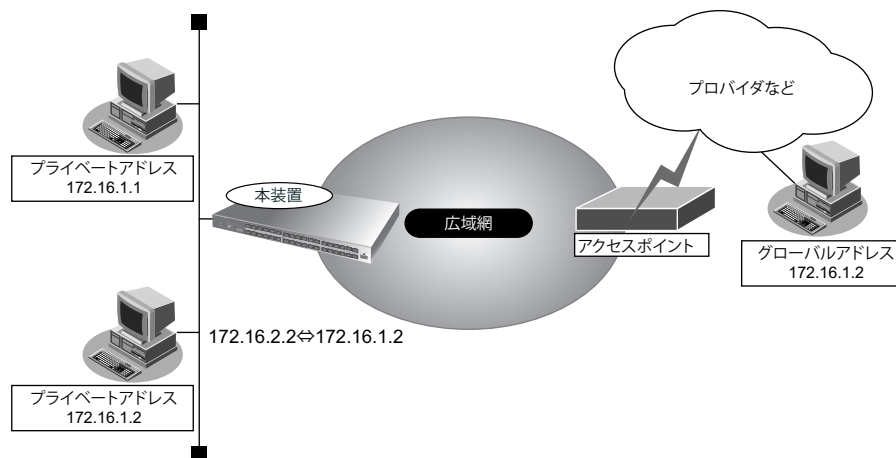
◆ 静的 NAT とは

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。



2.14.1 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

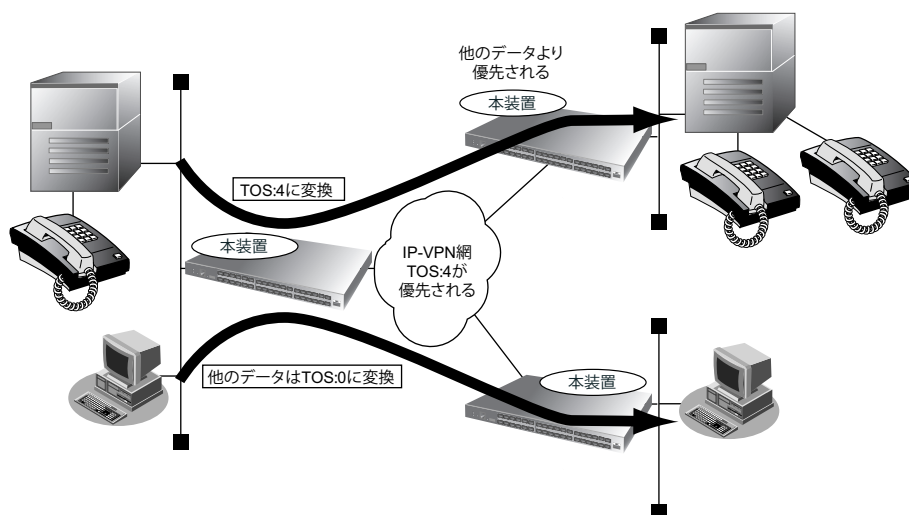
- プロバイダから割り当てられたグローバルアドレスより多くのパソコン（端末）を接続する場合（ここでいう端末には本装置も含まれます）
- 既存のネットワークのアドレスをそのまま使用する場合
- 自側のネットワークのアドレスを隠す場合
 - 動的NATが必要な場合
 - 同時に接続するパソコンの台数がグローバルアドレス数を超える場合
 - 静的NATが必要な場合
 - 外部にサービスを公開する場合（WWWサーバ、FTPサーバなど）
 - IPアドレスを意識して動作するアプリケーションを使用する場合

2.15 TOS/Traffic Class 値書き換え機能

TOS/Traffic Class 値書き換え機能とは、指定する IP パケットの TOS 値または IPv6 パケットの Traffic Class 値を書き換える機能です。IP-VPN 網を使って音声やレスポンスが要求されるデータの TOS/Traffic Class 値を変更して送信することで、IP-VPN 網内の遅延を減らすことができます。TOS/Traffic Class 値でパケット優先制御を行うキャリア VPN サービス（スーパー VPN など）と接続する場合に有効な機能です。

本装置でサポートしている TOS/Traffic Class 値書き換え機能は、以下の RFC（Request For Comments）に準拠しています。

- RFC2474:Definition of the Differentiated Services Field（DS Field） in the IPv4 and IPv6 Headers



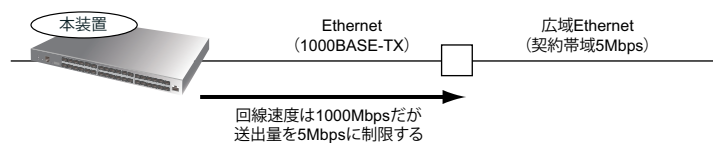
TOS 値書き換え機能は、IPv4[RFC791]で定義された IP パケットヘッダにある 8 ビットの Type Of Service（TOS）フィールドを制御することができます。

書き換え条件では、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パケットの TOS/Traffic Class 値を書き換えて送信します。

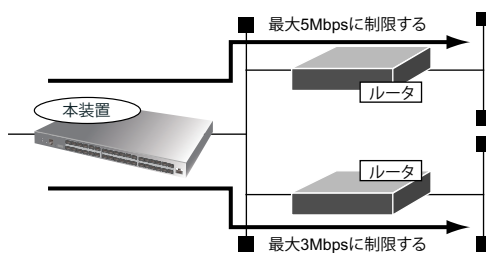
書き換えの対象とならなかったパケットの TOS/Traffic Class 値は書き換えられません。

2.16 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
- Ether-IP tunnel インタフェース
- L2TPv3 tunnel インタフェース
- トランクインタフェース

2.17 帯域制御 (WFQ) 機能

WFQ機能はソフトスケジューラのシェーパ配下のキューに対して適用される機能です。

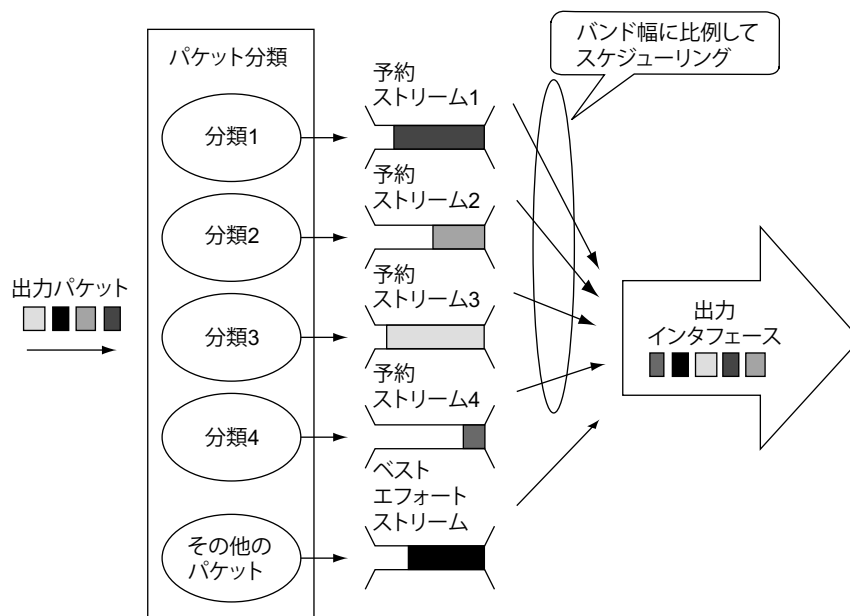
WFQ機能とは、回線上に流れる特定のデータの帯域を予約する機能です。

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単位または重さで指定します。
- 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。

2.17.1 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。

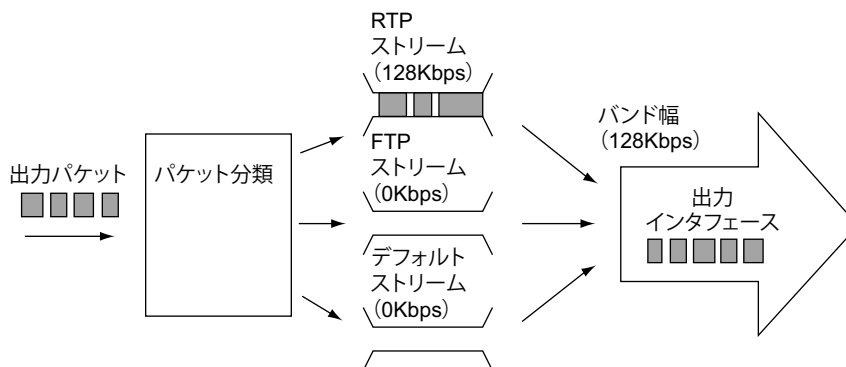
● WFQの設定

- ・ 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。

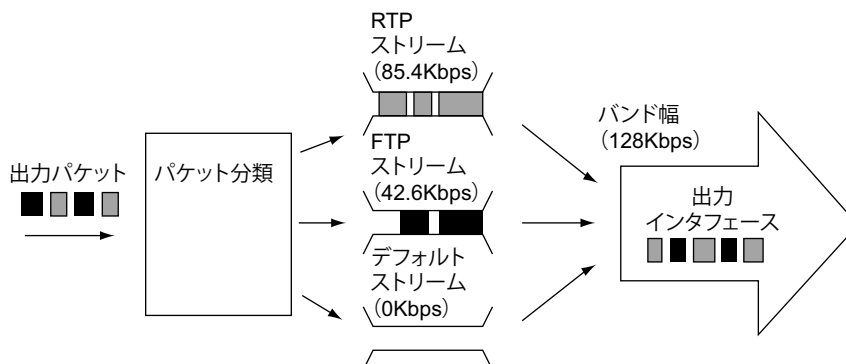
以下のようにRTPストリームにだけトラフィックがある場合、128Kbpsのすべて帯域を使用することができます。



2つのストリームにトラフィックがある場合

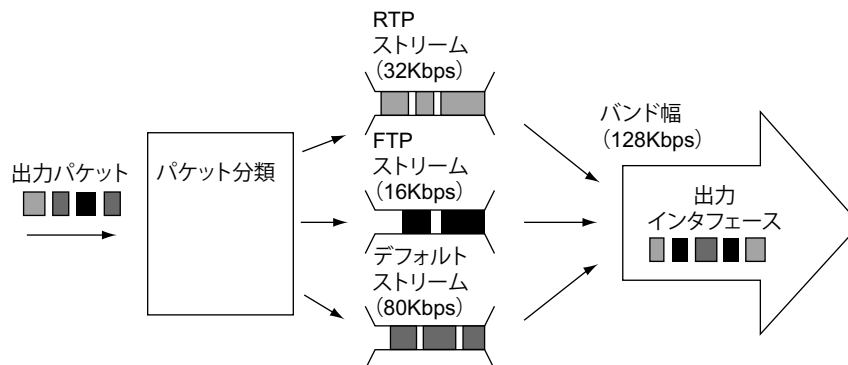
以下のようにRTPストリームとFTPストリームにトラフィックがあります。デフォルトストリームにトラフィックがない場合、トラフィックがあるストリームの予約バンド幅の比率でパケットをスケジューリングします。

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。

2.18 DHCP機能

DHCP機能は、IPv4 DHCP機能とIPv6 DHCP機能があります。

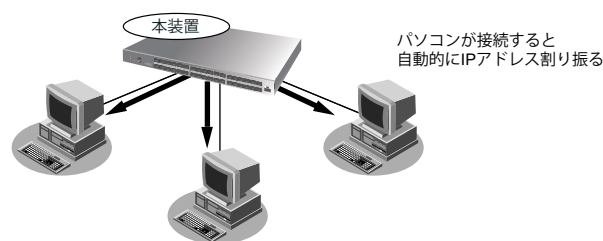
以下に、それぞれの機能について説明します。

2.18.1 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。

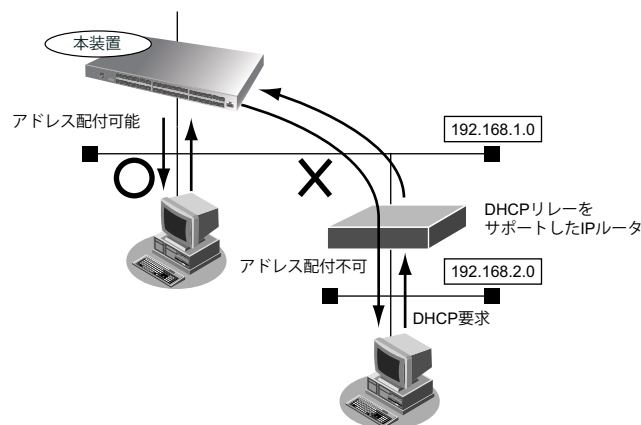


本装置はクライアントにIPアドレスを割り振る場合、ARPパケットにより、すでに特定のIPアドレスを割り当てられているホストが存在しないかどうかをチェックします。これにより、IPアドレスが重複する危険性を取り除くことができます。

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
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10の範囲)。 割り当て終了アドレスから順に、より小さいアドレスを順に 割り当てます。 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。

2.18.2 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	253
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

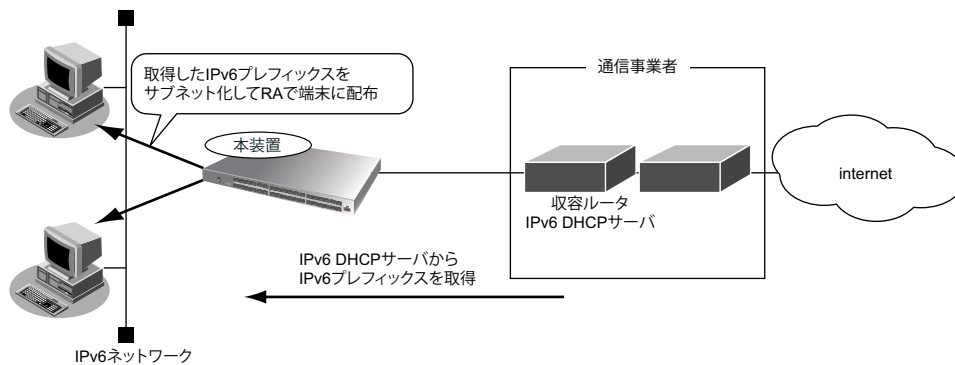
こんな事に気をつけて

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	×	×

2.19 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。

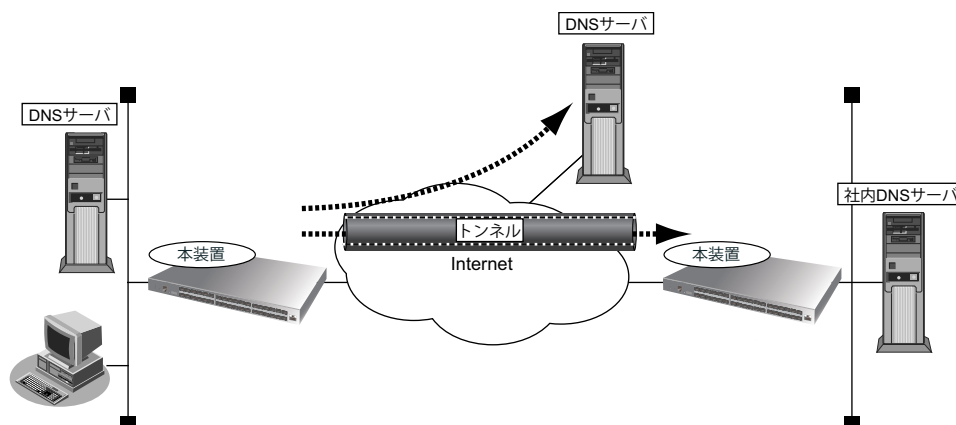
2.19.1 DNSサーバ（スタティック）機能

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。

2.19.2 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

2.20 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。

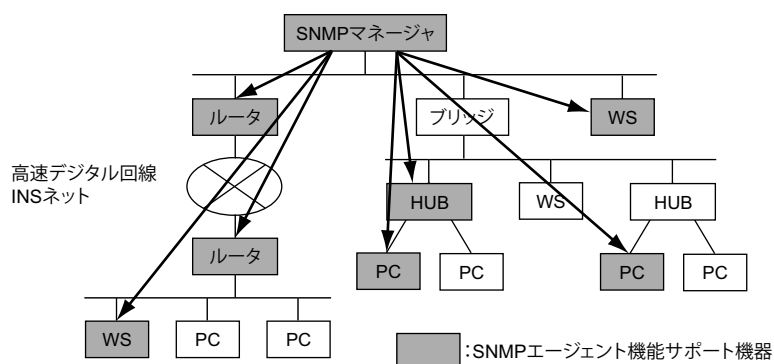
SNMPマネージャ機能は、ネットワーク上の端末の移動状態や障害状態を一元管理します。SNMPエージェント機能は、SNMPマネージャの要求に対してMIB（Management Information Base：管理情報ベース）という管理情報を返します。

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ー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。

2.20.1 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
1	管理ポート
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

- 装置実回線との対応

FX2

ifIndex	ifDescr	回線との対応
1	Management 1	管理ポート
401010000 ~	GigaEthernet 1/1/X	gigaethernet インタフェース X:1 ~ 12 の場合 (ifIndex=401000000+10000*X) X:101 ~ 104 の場合 (ifIndex=401000000+10000*(X-100+12))

- 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 1/1/X.Y (Y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 X:1 ~ 12 の場合 (ifIndex=501000000+10000*X+Y) X:101 ~ 104 の場合 (ifIndex=501000000+10000*(X-100+12)+Y)
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)

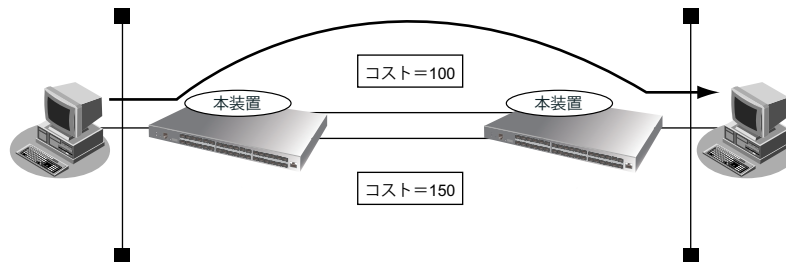
2.21 ECMP 機能

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。

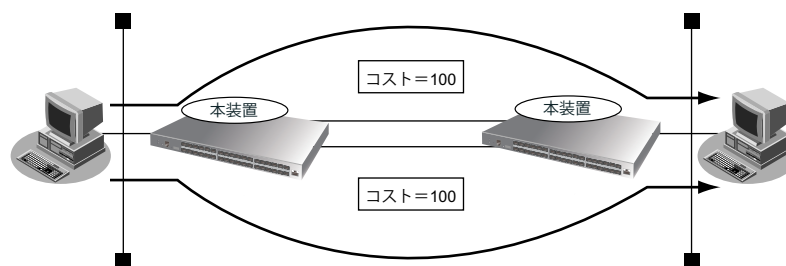
ECMP(Equal Cost Multi Path)機能は、同じ通信コストのパスを複数同時に利用できる機能です。この機能によって、同じ宛先ネットワークにパケットを送信する場合に、同じ通信コストのパスを併用して、通信パスの負荷を分散できます。

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の両方の通信パスが存在した場合は、「[2.6.1 IP経路情報の種類](#) (P.24)」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。

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。

2.21.1 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、桁上りを見捨て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、桁上りを見捨て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)
- | | | | | | | | | | | |
|-----------|-----|-----|----|----|----|---|---|---|-----|-------------------|
| | 31 | 24 | 23 | 16 | 15 | 8 | 7 | 0 | ビット | |
| 送信元IPアドレス | 192 | 168 | 1 | 1 | | | | | | → c0a80101 (16進数) |
-
- | | | | | | | | | | | |
|----------|-----|----|-----|---|--|--|--|--|--|-------------------|
| 宛先IPアドレス | 172 | 16 | 254 | 1 | | | | | | → ac10fe01 (16進数) |
|----------|-----|----|-----|---|--|--|--|--|--|-------------------|

それぞれを加算します。

$c0a80101 + ac10fe01 = 16cb8ff02$ (16進数)

桁上りを無視して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。

2.21.2 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。

2.22 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ールータ（実際にルーティングを行う装置）とバックアップルータ（マスター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、マスタールータがグループあての packets 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。

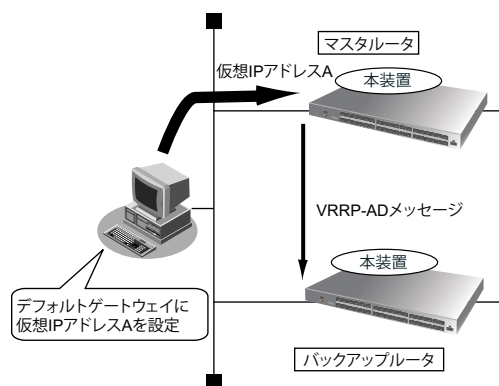
さらに、2つ以上のルータで複数のグループをマスタールータが分散するように設定し、端末ごとにデフォルトルータの仮想ルータを分けて設定することで、負荷分散と冗長構成のクラスタリング機能も実現できます。

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。

2.22.1 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、マスタールータは、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、マスタールータからの VRRP-AD メッセージを受信することで、マスタールータが正常に動作していると判断します。マスタールータでは、仮想 IP / MAC アドレスあての packets 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。

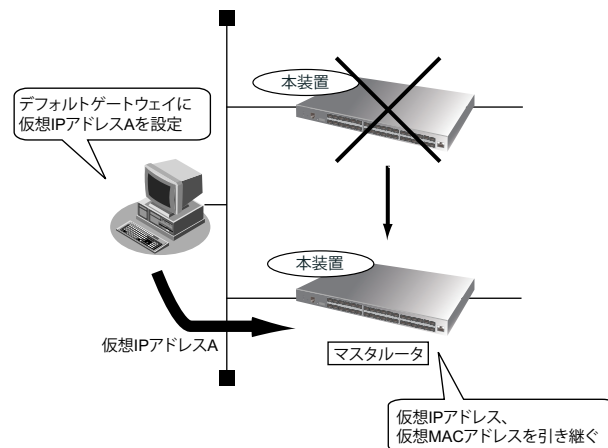


- 障害発生時の動作
 マスタルータがダウンすると、VRRP-ADメッセージは送信されません。よって、バックアップルータでは、最後にVRRP-ADメッセージを受信してからマスタルータのダウン検出時間までに次のVRRP-ADメッセージを受信できなかった場合、マスタルータがダウンしたと判断します。バックアップルータは、仮想IPアドレスと仮想MACアドレスを引き継いで、マスタルータとして動作します。マスタルータのダウン時間は、以下の計算式で計算されます。

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) × VRRP-ADメッセージ送信間隔) / 256 [秒]

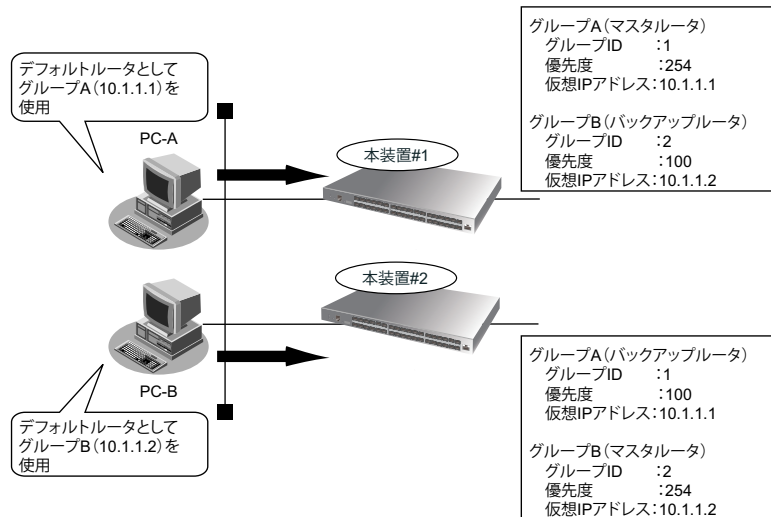


- トラッキング
 トラッキング対象の状態がダウンとなった場合、VRRPグループの現在の優先度から指定した値を減算した優先度のVRRPルータとして動作します。
 - インタフェース
指定したインタフェースがトラッキング対象となります。
 - 経路
指定した宛先への経路情報がトラッキング対象となります。
指定した宛先への経路情報がない場合にダウンとなります。到達性がない場合にダウンとなります。
 - 端末接続監視
端末接続監視機能により指定した監視先装置への到達性がトラッキング対象となります。
- 障害復旧時の動作
 グループ内でもっとも優先度の高いルータが復旧した場合、同じグループ内のマスタル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。

2.22.2 クラスタリング機能

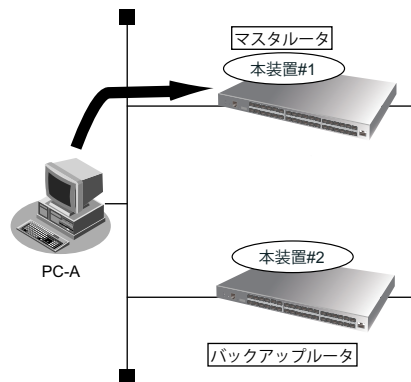
- 通常時の動作

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ため、グループ A のマスター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。

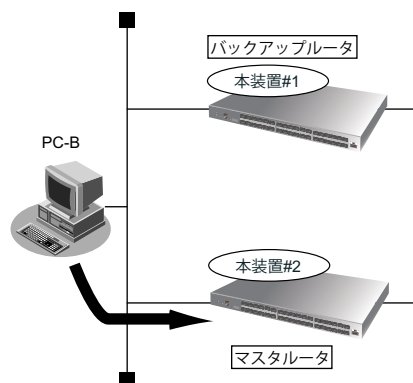


上の図をPC-A グループ、PC-B グループから見たときの構成は以下のようになります。

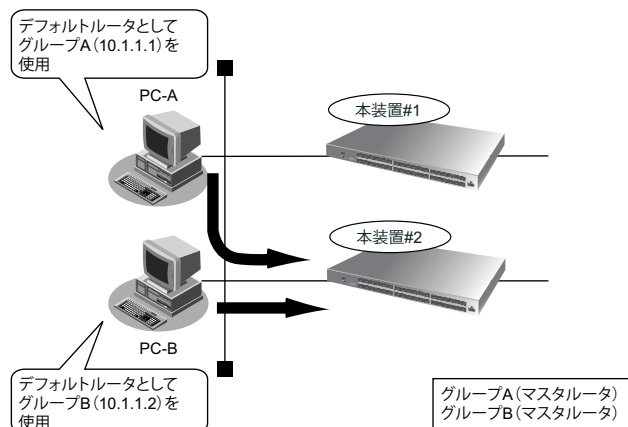
PC-A グループから見たときの構成



PC-B グループから見たときの構成



- ・ 障害発生時の動作
FX2#1 がダウンしたとき、グループ A に対するマスタールータは FX2#2 に引き継がれます。切り替え動作については、「2.22.1 簡易ホットスタンバイ機能」(P.65) 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、「2.22.1 簡易ホットスタンバイ機能」(P.65) を参照してください。
- ・ 障害復旧時の動作
「2.22.1 簡易ホットスタンバイ機能」(P.65) 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、マスター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ー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、マスタールータは、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送信します。バックアップルータは、マスタールータからの VRRP-AD メッセージを受信することで、マスター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、マスタールータがダウンしたと判断し、新たなマスター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。

- 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。
-

2.23 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 L2TPv2/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プピング機能
- IP フレームの転送機能

2.23.1 ブリッジグループピング機能

ブリッジグループピング機能とは、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ンネルインタフェース、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

2.23.2 IP フレームの転送ポリシー

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。

2.24 透過モード

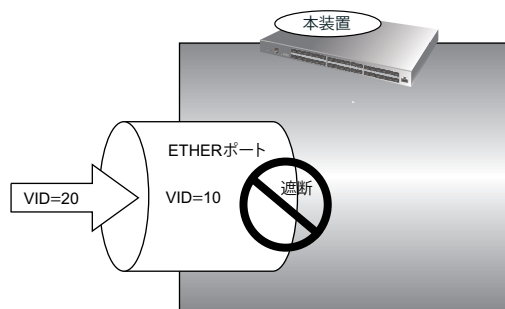
透過モードとは、タグ付き VLAN フレームおよびタグなしフレームを VLAN 設定なしに転送可能とするモードです。本装置では、VLAN 設定を行い、設定に従った転送と、VLAN 設定なしに全フレームを透過するモードをサポートします。

2.24.1 VLAN モードと透過モード

本装置では、VLAN 設定に従って転送する「VLAN モード」と、VLAN 設定なしに全フレームを透過される「透過モード」を切り替えることができます。

VLAN モード

VLAN モードでは、受信ポートに設定されていない VID のフレームを受信した場合、そのフレームは破棄されます。また、送信先ポートからは、設定した VID で送出されます。



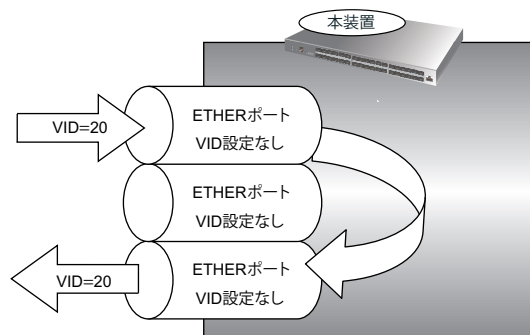
透過モード

透過モードでは、ポートに VID を設定することなく、タグ付きフレーム・タグなしフレームを扱うことができます。

透過モードで、ポートに VID を設定した場合でも、設定した VID を無効とし、透過モード優先で動作します。

透過モードのポートルーティング設定を行った場合、タグなしフレームのみルーティングを行うことができます。タグありフレームはルーティング対象外です。

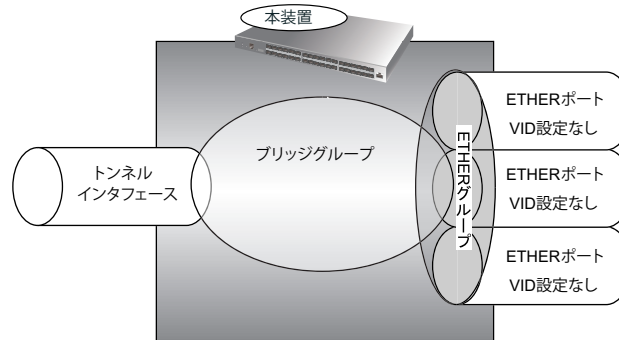
透過モードでは、ほかのポートで学習されていない宛先フレームを受信した場合、ブリッジグループ内の全ポートへの転送を行います。



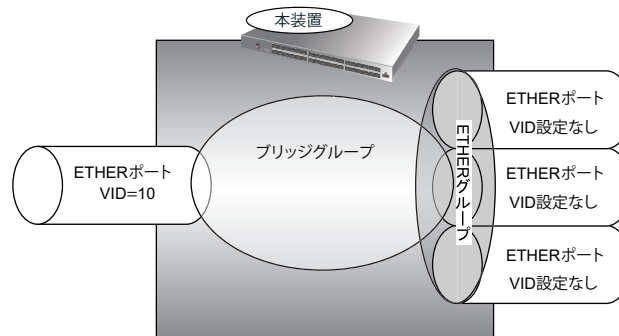
2.24.2 透過モードとブリッジグループ機能

透過モードでブリッジグループ機能を使用することができます。グループメンバとして指定可能なインターフェースは以下のとおりです。

- tunnel インタフェース
VLAN モードと同様、複数の tunnel インタフェースとグループを構成することができます。



- VLAN インタフェース
VLAN モードの各ポートに設定された VLAN とグループを構成することができます。
透過モードのポートから VLAN インタフェースへの転送では受信したタグの上に VLAN インタフェースのタグが挿入され QinQ の形で転送されます。逆に VLAN インタフェースから透過モードへの転送では受信した先頭のタグが一段削除されて転送されます。



2.25 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、送信パケットのMACアドレスまたは、IPアドレスで判断し、負荷分散されます。

以下の方式から選択して指定することができます。

- 送信先MACアドレスと送信元MACアドレスを元にした負荷分散
- 送信先IPアドレスと送信元IPアドレスを元にした負荷分散

トランク・グループを通信可能とさせるまでの最小メンバポート数を指定することができます。

トランク・グループのメンバポートが指定した数だけ有効となるまでトランク・グループの通信を抑止します。

たとえば、リンクダウンしたメンバポートなどは有効なポートに含まれません。

冗長構成などでトランク・グループを必要な帯域が確保できるまで通信させたくない場合に使用します。

なお、この機能はLACPと併用することができます。

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。

2.25.1 LACP機能

LACP機能とは、IEEE802.3 準拠のLACPを利用したリンクアグリゲーションです。LACPを取り付けたシステム間で実現可能な最大レベルのリンクアグリゲーションを継続的に提供します。

LACPの利用によってリンクアグリゲーションの整合性確認や、リンクの正常性確認、障害検知の確度を向上できます。

導入のメリット

- 隣接装置と整合性を確認するので、たとえばポートを差し間違えていたといったようなミスがあった場合でも、プロトコルレベルで一本一本正しいリンク先に接続されていることを確認しながら通信を開始します。そのため誤った接続先へ通信してしまいうことがありません。
- 隣接装置からのLACPパケットが一定時間受信されない場合は、リンク異常と判断するので、装置ポートの異常検出範囲を超えたリンクの障害検知が可能です。
- ポートがオートネゴシエーションに設定された場合、接続が半二重であるリンクをリンクアグリゲーションのトランク・グループに含めません。

こんな事に気をつけて

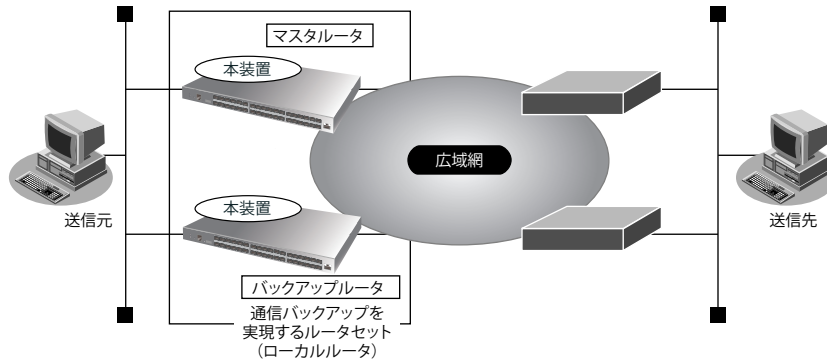
- LACPを利用したリンクアグリゲーションは、接続先もLACPを有効にする必要があります。リンクアグリゲーション動作モードにstaticを指定したなどのLACP以外のリンクアグリゲーションとは接続できません。
- リンクアグリゲーション動作モードにpassiveを指定して、接続先も同様にpassiveとするとリンクアグリゲーションは構成されません。どちらか一方はactiveと指定してください。双方をactiveと指定してもかまいません。

2.26 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

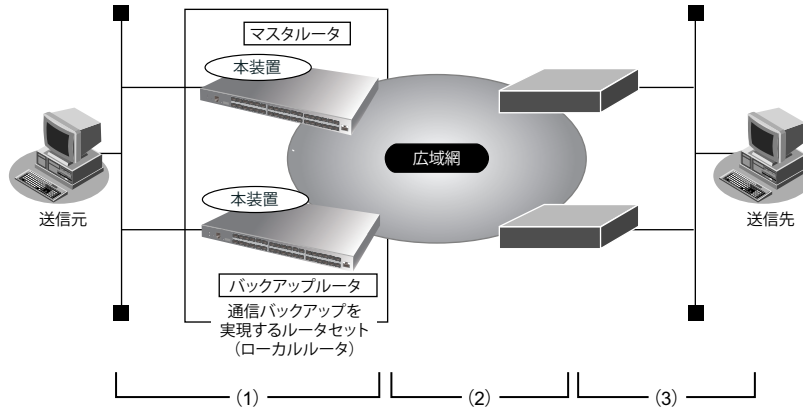
ここでは片方向通信について説明していますが、一般的なクライアント-サーバモデルの通信は、「クライアントからサーバへの通信（主に要求）」と「サーバからクライアントへの通信（主に応答）」が成立して初めて成立します。このため、実際に利用する場合は、本書を参考にして、双方向の通信が成立するようにネットワーク設計を行ってください。

2.26.1 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。

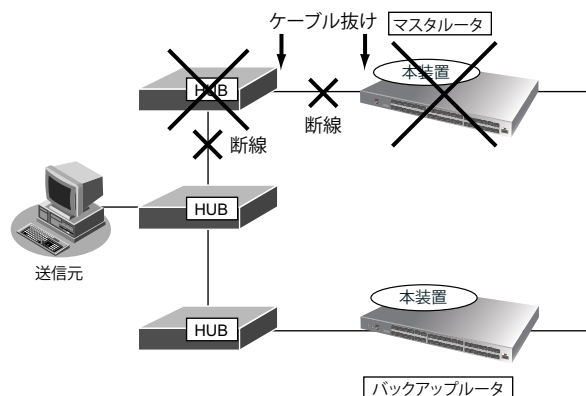
(1) 送信元とローカルルータとの間の通信障害

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。

- マスター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）
- マスタールータの故障

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。

マスター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、マスター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。

マスタールータは、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でマスター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ー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

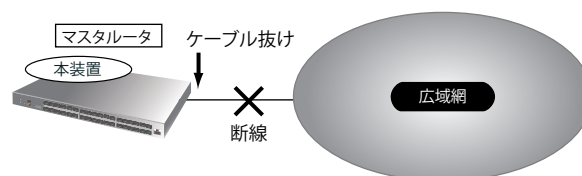
これらの障害に対する本装置の検出方法と障害検出可能な箇所は、以下のとおりです。

- 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。

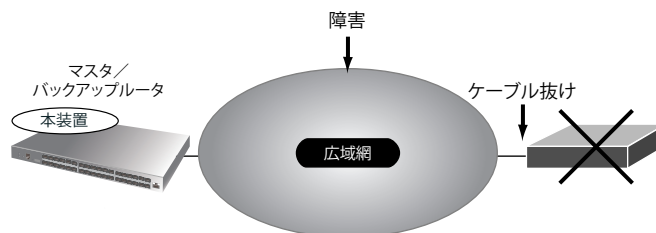
ハードウェアによる障害検出

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.75) 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.76) 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ず、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。

2.26.2 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

「2.26.1 通信障害の検出機能」(P.75) 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
- バックアップポート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。

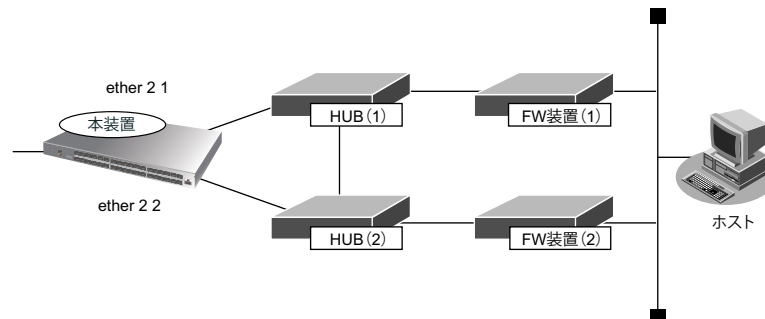
インタフェースダウンによって障害検出された場合は、以下の動作となります。

- 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。

バックアップポート機能を利用した迂回機能

バックアップポート機能を利用した場合、同じセグメントに対して2つの EHTERNET ポートを接続できます。これによって、一方の EHTERNET ポートで障害が発生したときも、他方の障害の発生していない EHTERNET ポートを利用して通信を継続できます。

以下に、バックアップポート機能を利用する場合の構成例を示します。



● 運用前提

- 本装置は、trunk グループポート 1 を通信ポート、trunk グループ 2 ポート 2 をバックアップとして定義されている
- FW 装置 (1) と FW 装置 (2) は、お互いをバックアップする構成となっている (HUB と FW 装置との間の通信障害を検出し、系切り替えを行うことができる)

● 通信動作

通常状態

本装置は、trunk グループ 2 ポート 1 を通信ポート、trunk グループ 2 ポート 2 をバックアップとして定義され、trunk グループ 2 ポート 1 で通信しています。

この状態の通信経路を、以下に示します。

本装置 [trunk-group 2 1] ↔ HUB (1) ↔ FW 装置 (1) ↔ ホスト

「通常状態」の [trunk-group 2 ポート 1] でケーブル抜け、断線などが発生した場合

本装置は、trunk グループ 2 ポート 1 の通信障害を検出し、通信ポートを trunk グループ 2 ポート 2 に切り替えます。この場合、FW 装置は障害に気付くことはありません。この状態の通信経路を、以下に示します。

本装置 [trunk-group 2 2] ↔ HUB (2) ↔ HUB (1) ↔ FW 装置 (1) ↔ ホスト

「通常状態」の HUB (1) の故障が発生した場合

本装置は、trunk グループ 2 ポート 1 の通信障害を検出し、通信ポートを trunk グループ 2 ポート 2 に切り替えます。この場合、FW 装置 (1) も障害を検出し、FW 装置 (2) を経由した通信に切り替わったことを前提とします。この状態の通信経路を、以下に示します。

本装置 [trunk-group 2 2] ↔ HUB (2) ↔ FW 装置 (2) ↔ ホスト

こんな事に気をつけて

- バックアップポート機能を利用する際に、trunk-channel or port-channe の LinkUp trap および LinkDown trap は、以下の場合に送出されます。
 - LinkUp trap は、両 ETHERNET ポートが利用できない状態から、どちらか一方が利用できる状態になった場合に送出されます。
 - LinkDown trap は、両 ETHERNET ポートが利用できない状態になった場合に送出されます。
- それぞれの ETHERNET ポートの状態の変化では、trunk-channel or port-channe の LinkUp trap および LinkDown trap は送出されません。

2.27 BFD機能

BFD (Bidirectional Forwarding Detection) は、隣接ノード間での経路の生存状況 (隣接ノードへの到達性) を監視し、障害を高速に検知する機能です。

本装置のBFD機能の動作は以下のとおりです。

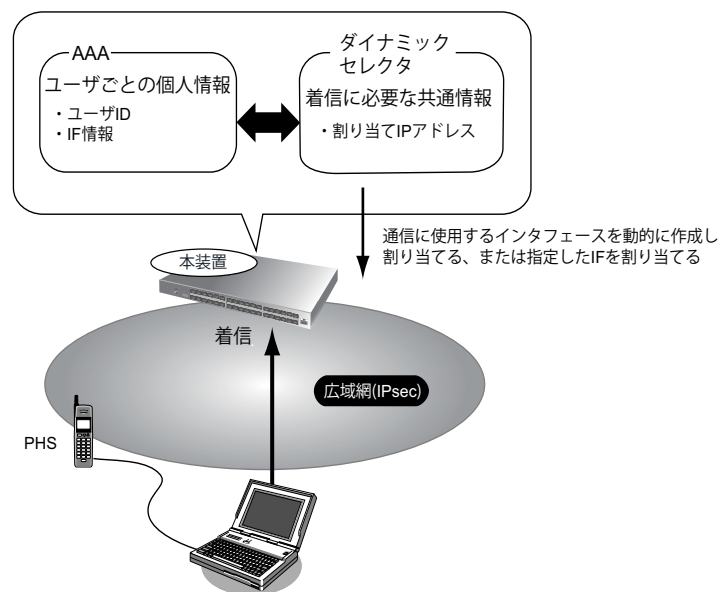
- 隣接ノード間のリンクやパスの障害を高速に検知します。
- UDPパケット (ポート番号: 3784/4784/6784) を使った生存確認を行い、障害発生時には経路制御プロトコル等へすばやく障害を通知します。
- 障害の通知を行うプロトコルや機能は以下のとおりです。
 - IPv4スタティック経路 / IPv6スタティック経路
BFD session ダウン時の経路の登録 (迂回経路の登録) を行います。
 - OSPFv2 / OSPFv3
OSPF ネイバーを監視対象とし、Hello プロトコルよりも早く DOWN を検知して冗長経路への切り替えを行います。
 - リンクアグリゲーション (micro BFD)
リンク状態の確認と変化を検出するために使用します。
- OSPFv2、OSPFv3の連携時は、ネイバーステータスが Full になってから BFD 監視を開始します。
- BFD のパケットの送信間隔を設定できます (異常を検知するまでの時間を調整することができます)。

2.28 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 20000 です。

2.29 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。

2.29.1 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)	アカウントिंग (accounting)
ログインユーザ認証機能	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> IPv4 スタティック経路情報 IPv6 スタティック経路情報 	<ul style="list-style-type: none"> 送受信オクテット数 送受信パケット数 接続時間

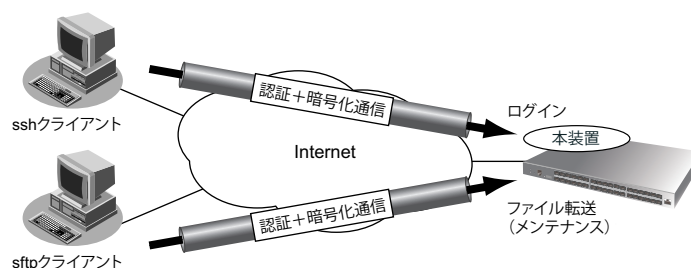
本装置の RADIUS クライアント機能は、複数台の RADIUS サーバを使用したバックアップ構成または負荷分散構成が可能です。

拡張認証機能とログインユーザ認証機能は別設定になります。

2.30 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（sftp サーバ、scp 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) が生成されています。ssh-server 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

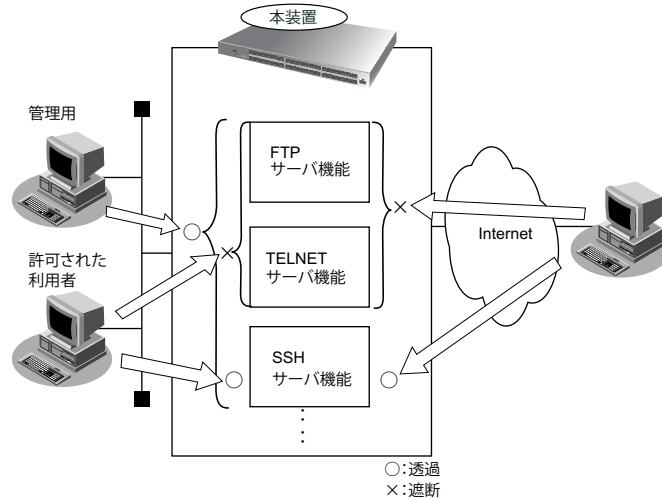
項目	サポート内容
SSH プロトコルバージョン	SSH プロトコルバージョン V2 をサポート
SSH ポート番号/プロトコル	22 / TCP (設定により変更可)
IP プロトコルバージョン	IPv4 および IPv6 をサポート
ホスト認証プロトコル	RSA/DSA、ECDSA、ED25519

項目	サポート内容
ホスト認証アルゴリズムの種類	ssh-dss ssh-ed25519-cert-v01@openssh.com ecdsa-sha2-nistp256-cert-v01@openssh.com ecdsa-sha2-nistp384-cert-v01@openssh.com ecdsa-sha2-nistp521-cert-v01@openssh.com sk-ssh-ed25519-cert-v01@openssh.com sk-ecdsa-sha2-nistp256-cert-v01@openssh.com rsa-sha2-512-cert-v01@openssh.com rsa-sha2-256-cert-v01@openssh.com ssh-ed25519 ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 ecdsa-sha2-nistp521 sk-ssh-ed25519@openssh.com sk-ecdsa-sha2-nistp256@openssh.com rsa-sha2-512 rsa-sha2-256 ssh-rsa
暗号方式の種類	3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com chacha20-poly1305@openssh.com
メッセージ認証コードの種類	hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1
鍵交換アルゴリズム	curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256
認証方式	パスワード認証 (login 認証 / local-username 認証) RADIUS 認証 TACACS+ 認証 公開鍵認証
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)

2.31 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。



2.32 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 デジタル署名認証方式）

こんな事に気をつけて

- RSA 鍵ペアおよび自装置証明書がない場合は、RSA 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。
-

2.33 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。

2.33.1 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

USB メモリのファイルは、“/usb1/<filename>“でアクセスできます。たとえば、USB メモリに格納されている“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）

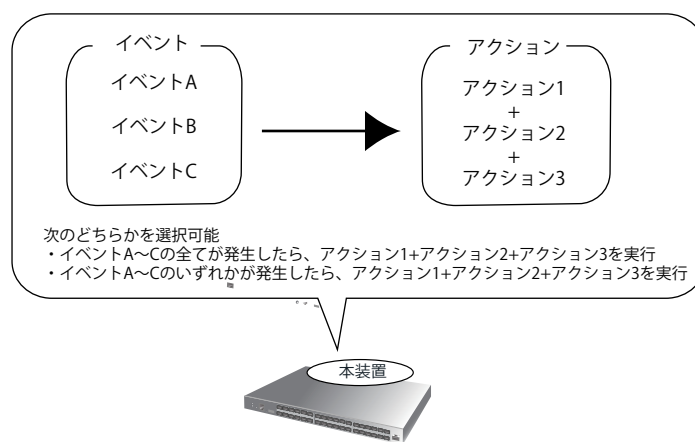
2.34 イベントアクション機能

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"というロジックを設定し、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。



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

【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	
指定時間アクション実行待ち	
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

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。

索引

A

AAA 情報	83
AH ヘッダ	42
ARP エージング機能	20
ARP パケット	53
AS	30
AS 境界ルータ	33

B

BFD 機能	81
BGP	62
BGP4 機能	30
BGP4 経路	24

D

DHCP 機能	53
DHCP クライアント機能	53, 54
DHCP クライアント経路 (IPv4)	24
DHCP クライアント経路 (IPv6)	24
DHCP サーバ機能	53
DHCP サーバ経路 (IPv6)	24
DHCP リレーエージェント機能	55
DNS サーバ機能	58
DNS 振り分け機能	58

E

EAP 認証	43
ECMP 機能	62
ESP ヘッダ	42
External BGP	30

F

FTP ストリーム	51
-----------	----

G

Global Unicast Addresses	22
--------------------------	----

I

ICMP ECHO パケット	44
IKE 経路	24
Ingress ポリシールーティング機能	38
Internal BGP	30
IPsec 機能	40
IPsec の範囲	41
IPv4 DHCP 機能	53

IPv6 DHCP 機能	55
IPv6 DHCP クライアント機能	56
IPv6 DHCP サーバ機能	55
IPv6 DHCP リレーエージェント機能	56
IPv6 OSPF 機能	35
IPv6 アドレス体系	22
IPv6 アドレスの表記方法	21
IPv6 機能	21
IP 経路情報の管理	25
IP 経路情報の種類	24
IP 経路制御機能	24
IP パケット	10
IP パケット暗号化	43
IP パケット認証	42
IP フィルタリング機能	36
IP フレームの転送方式	70
IP ルーティング	39

L

Link-Local Unicast Addresses	22
LSA	33

M

MIB	60
Multicast Addresses	22

N

NAT あて先変換	47
NAT 機能	45
NAT 機能の選択基準	47
NAT トラバース	44

O

OSPF	62
OSPF 機能	33
OSPF 経路	24

P

PKI 機能	87
port-channel インタフェース	12
PPPoE	77
ProxyDNS 機能	58

R

RADIUS 機能	83
RADIUS クライアント機能	83
RA 経路	24

RFC	48
RIP 機能	28
Router Advertisement Message 受信	23
Router Advertisement Message 送信	22
RSA デジタル署名認証	43
RTP ストリーム	51

S

Security Association	42
Security Parameters Index	42
Skew_Time	66
SNMP エージェント	60
SNMP 機能	60
SNMP マネージャ	60
SPI	37
SSH サーバ機能	84

T

TELNET サーバ機能	84
TOS/Traffic Class 値書き換え機能	48
tunnel インタフェース	12

U

UPDATE パケット	30
USB メモリ機能	88

V

VLAN	6
VLAN ID	6
VLAN 機能	15
VLAN 種別	15
VLAN トランク機能	17
VLAN の種類	6
VLAN モード	71
VPN	40
VRRP	78
VRRP-AD メッセージ	65
VRRP 機能	65, 76

W

WFQ 機能	50
--------------	----

あ

アクセスリンク	16
アプリケーションフィルタ機能	86
暗号化	40

い

イベントアクション機能	89
インタフェース	12, 51
インタフェース経路 (IPv4)	24
インタフェース経路 (IPv6)	24

え

エクспレスストリーム	50
エリア境界ルータ	33
エンドツーエンド	74
エントリ	59

か

簡易ホットスタンバイ機能	65
--------------------	----

き

共有鍵認証	43
-------------	----

く

クラスタリング機能	65, 67
グローバルアドレス	45

け

経路再配布機能	27
経路制御機能	27, 79
経路フィルタリング機能	27

こ

コネクション	30
--------------	----

さ

再配布フィルタリング	27
------------------	----

し

シェーピング機能	49
自律システム	30

す

スタティック機能	58
スタティック経路	24
スタティックルーティング	10, 22, 62
スタティックルーティング機能	26
スタブエリア	33
ストリーム数	51

せ

静的 NAT	46, 47
セキュリティ	36
セキュリティ方針	36
接続先監視	44

た

帯域制御機能	50
ダイナミックセレクト機能	82
ダイナミックルーティング	10, 22
ダイナミックルーティング機能	26, 76
タグ VLAN	6
端末型接続	45
端末接続監視機能	77

つ

通信障害の検出機能	75
通信パス迂回機能	78
通信パス選択方法	63
通信バックアップ機能	64, 73

て

データリンクプロトコル	77
デフォルトルータ	67
転送先	38
転送先選定定義	12

と

透過モード	71
動的 NAT	46, 47
動的フィルタリング	37
ドメイン名	59
トラッキング	66
トラフィック	51
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	51
トランクリンク	16
トランスポートモード	41
トンネルモード	41

な

内部ルータ	33
-------------	----

に

認証	40
----------	----

ね

ネットワーク	8
ネットワークインタフェース	10
ネットワーク型接続	45
ネットワーク設計概念	8
ネットワーク全体	9
ネットワーク部	9

は

ハードウェア	76
ハイブリッドリンク	16
パケットフィルタリング	22
バックアップポート	18
バックアップポート機能	18, 80
バックアップルータ	65
バックボーンエリア	33
バックボーンルータ	33
ハッシュ方式	63
バンド幅	50
バンド幅の変動	51

ふ

ファイアーウォール	36
フィルタリングルール	37
プライベートアドレス	45
フラグメント	45
ブリッジグループピンギング機能	70
ブリッジグループ機能	70
ブリッジ転送	11
プレフィックス長	22

へ

ベストエフォートストリーム	50, 51
---------------------	--------

ほ

ポート VLAN	6, 15
ポート間アクセス制御機能	19
ホスト部	9
ホップ数	28
ポリシールーティング機能	38

ま

マスタポート	18
マスタルータ	65

ゆ

ユーザ認証	36
優先経路制御機能	26, 27

ゆらぎ 28

よ

予約ストリーム 50

り

リモートログイン機能 84

リンクアグリゲーション機能 73

リンクステート方式 33

る

ルータ 10

ルータ設定 12

ルーティング 8, 62

ルーティングテーブル 10, 26

ルーティング転送 11

ルーティングプロトコルの経路テーブル 25

ループバックインタフェース 12

ろ

ローカルルータ 75

FITELnet FH10 一般版 機能説明書

初版

発行日 2026年6月

発行責任 古河電気工業株式会社

- 本書の一部または全部を無断で他に転載しないよう、お願いいたします。
- 本書は、改善のために予告なしに変更することがあります。
- 本書に記載されたデータの使用に起因する第三者の特許権、その他の権利、損害については、弊社はその責を負いません。