AX8600R ソフトウェアマニュアル

コンフィグレーションガイド Vol.3

Ver. 12.8 対応 Rev.2

AX86R-S003-A0

■ 対象製品

このマニュアルは AX8600R を対象に記載しています。

■ 輸出時の注意

本製品を輸出される場合には，外国為替及び外国貿易法の規制ならびに米国の輸出管理規則など外国の輸出関連法規をご確認のうえ，必要な手続きをお取りください。なお，不明な場合は，弊社担当営業にお問い合わせください。

■ 商標一覧

Cisco は，米国 Cisco Systems, Inc. の米国および他の国々における登録商標です。
Ethernet は，富士ゼロックス株式会社の登録商標です。
IPX は，Novell,Inc.の商標です。
Python(R)は，Python Software Foundation の登録商標です。
RSA および RC4 は，米国およびその他の国における米国 EMC Corporation の登録商標です。
sFlow は，米国およびその他の国における米国 InMon Corp. の登録商標です。
ssh は，SSH Communications Security,Inc.の登録商標です。
UNIX は，The Open Group の米国ならびに他の国における登録商標です。
イーサネットは，富士ゼロックス株式会社の登録商標です。
そのほかの記載の会社名，製品名は，それぞれの会社の商標もしくは登録商標です。

■ マニュアルはよく読み，保管してください。

製品を使用する前に，安全上の説明をよく読み，十分理解してください。
このマニュアルは，いつでも参照できるよう，手近な所に保管してください。

■ ご注意

このマニュアルの内容については，改良のため，予告なく変更する場合があります。

■ 発行

２０２０年　３月 （第１１版） ＡＸ８６Ｒ－Ｓ００３－Ａ０

■ 著作権

All Rights Reserved, Copyright(C), 2012, 2020, ALAXALA Networks, Corp.

変更内容

【Ver. 12.8 対応 Rev.2 版】

表　変更内容

章・節・項・タイトル	追加・変更内容
1.1.2　サブネットマスク	• 31 ビット長のサブネットマスクを指定した IPv4 アドレスの設定について記述を追加しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver. 12.8 対応 Rev.1 版】

表　変更内容

項目	追加・変更内容
情報の配布	• RDNSS オプションおよび DNSSL オプションの記述を追加しました。

【Ver. 12.7 対応 Rev.1 版】

表　変更内容

項目	追加・変更内容
ARP	•「(4) ローカル ProxyARP」を追加しました。
サポート機能一覧	• マネージメントポートの VRF 対応に伴って記述を変更しました。

【Ver. 12.6 対応 Rev.1 版】

表　変更内容

項目	追加・変更内容
マルチホップの監視	• ループバックアドレスを変更または削除したときの BFD セッションの動作を追加しました。

【Ver. 12.6 対応版】

表　変更内容

項目	追加・変更内容
ループバックインタフェース	• 記述を追加しました。
複数のループバックインタフェースの設定	• 本項を追加しました。
ループバックインタフェース	• 記述を追加しました。
複数のループバックインタフェースの設定	• 本項を追加しました。
VRF の設定	• 記述を追加しました。
DHCP/BOOTP パケット転送時の設定内容	• DHCP のリレーエージェント情報オプション（Option82）のサポートに伴って記述を追加しました。
リレーエージェント情報オプション（Option82）	• 本項を追加しました。
リレーエージェント情報オプション（DHCP Option82）を付ける設定	• 本項を追加しました。

項目	追加・変更内容
DHCPv6 パケット転送時の設定内容	• VRF のサポートに伴って記述を追加しました。 • ループバックインタフェース関連の記述を変更しました。
VRF（経路交換によるエクストラネット）構成での設定	• 本項を追加しました。
ユニキャストルーティング高可用機能	• 本節を追加しました。
ノンストップルーティングの解説	• 本節を追加しました。
ノンストップルーティングのコンフィグレーション	• 本節を追加しました。
スタブルータの動作	• ノンストップルーティングのサポートに伴って「(2) 起動後にスタブルータとして動作する場合」の記述を変更しました。
ノンストップルーティングの確認	• 本項を追加しました。
ノンストップルーティングの解説	• 本節を追加しました。
ノンストップルーティングのコンフィグレーション	• 本節を追加しました。
スタブルータの動作	• ノンストップルーティングのサポートに伴って「(2) 起動後にスタブルータとして動作する場合」の記述を変更しました。
ノンストップルーティングの確認	• 本項を追加しました。
ノンストップルーティング	• 本項を追加しました。
ノンストップルーティングの設定	• 本項を追加しました。
ノンストップルーティングの設定	• 本項を追加しました。
ノンストップルーティングの確認	• 本項を追加しました。
IPv6 マルチキャスト拡張機能	• 本章を追加しました。
BFD とプロトコルの連携	•「(1) スタティックルーティングのゲートウェイ監視」を追加しました。
スタティックルーティングのゲートウェイ監視の設定	• 本項を追加しました。
プロトコルの確認	•「(1) スタティックルーティングの確認」を追加しました。

【Ver. 12.4 対応 Rev.1 版】

表　変更内容

項目	追加・変更内容
経路フィルタリングの運用への反映	• routing options auto-update-filter の記述を追加しました。
経路フィルタリングの運用への反映	• routing options auto-update-filter の記述を追加しました。
系切替時の無停止マルチキャスト中継機能	• 本項を追加しました。
BFD	• BFD と連携するプロトコルの追加（OSPFv3 および BGP4+）に伴い，記述を変更しました。

【Ver. 12.4 対応版】

表　変更内容

項目	追加・変更内容
ネクストホップ	• 指定できるインタフェース種別に VLAN インタフェースを追加しました。
DHCPv6 パケット転送時の設定内容	• VLAN インタフェースの記述を追加しました。
4 バイト AS 番号	• 本項を追加しました。
IPv4 PIM-SM	• PIM Bootstrap メッセージの広告範囲を制限する機能を追加しました。 • PIM Hello メッセージの DR-Priority オプションをサポートしました。
系切替時の無停止マルチキャスト中継機能	• 本項を追加しました。
マルチキャストロードバランス	• 本項を追加しました。
IPv6 PIM-SM	• PIM Hello メッセージの DR-Priority オプションをサポートしました。
BFD	• 本章を追加しました。

はじめに

■ 対象製品およびソフトウェアバージョン

このマニュアルは AX8600R のソフトウェア Ver. 12.8 の機能について記載しています。ソフトウェア機能のうち，オプションライセンスで提供する機能については次のマークで示します。

【OP-SHPS】

オプションライセンス OP-SHPS についての記述です。

【OP-SHPE】

オプションライセンス OP-SHPE についての記述です。

操作を行う前にこのマニュアルをよく読み，書かれている指示や注意を十分に理解してください。また，このマニュアルは必要なときにすぐ参照できるよう使いやすい場所に保管してください。

■ このマニュアルの訂正について

このマニュアルに記載の内容は，ソフトウェアと共に提供する「リリースノート」および「マニュアル訂正資料」で訂正する場合があります。

■ 対象読者

本装置を利用したネットワークシステムを構築し，運用するシステム管理者の方を対象としています。

また，次に示す知識を理解していることを前提としています。

- ネットワークシステム管理の基礎的な知識

■ このマニュアルの URL

このマニュアルの内容は下記 URL に掲載しております。

https://www.alaxala.com/

■ マニュアルの読書手順

本装置の導入，セットアップ，日常運用までの作業フローに従って，それぞれの場合に参照するマニュアルを次に示します。

●装置の開梱から，初期導入時の基本的な設定を知りたい

クイックスタートガイド (AX86R-Q001)

●ハードウェアの設備条件，取扱方法を調べる

ハードウェア取扱説明書 (AX86R-H001)

●ソフトウェアの機能，コンフィグレーションの設定，運用コマンドを知りたい

▽まず，ガイドで使用する機能や収容条件についてご確認ください。

- **収容条件**
- **ログインなどの基本操作**
- **イーサネット**

コンフィグレーションガイド Vol.1 (AX86R-S001)

- **フィルタ，QoS**
- **ネットワークの管理**

コンフィグレーションガイド Vol.2 (AX86R-S002)

- **IPパケット中継**
- **ユニキャストルーティング**
- **マルチキャストルーティング**

コンフィグレーションガイド Vol.3 (AX86R-S003)

▽必要に応じて，レファレンスをご確認ください。

・コマンドの入力シンタックス，パラメータ詳細について

コンフィグレーション コマンドレファレンス Vol.1 (AX86R-S004)

コンフィグレーション コマンドレファレンス Vol.2 (AX86R-S005)

コンフィグレーション コマンドレファレンス Vol.3 (AX86R-S006)

運用コマンドレファレンス Vol.1 (AX86R-S007)

運用コマンドレファレンス Vol.2 (AX86R-S008)

運用コマンドレファレンス Vol.3 (AX86R-S009)

・システムメッセージとログについて

メッセージ・ログレファレンス (AX86R-S010)

・MIBについて

MIBレファレンス (AX86R-S011)

●トラブル発生時の対処方法について知りたい

トラブルシューティングガイド (AX86R-T001)

■ このマニュアルでの表記

AC	Alternating Current
ACK	ACKnowledge
ARP	Address Resolution Protocol
AS	Autonomous System
AUX	Auxiliary
AXRP	Autonomous eXtensible Ring Protocol
BCU	Basic Control Unit
BEQ	Best Effort Queueing
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol - version 4
BGP4+	Multiprotocol Extensions for Border Gateway Protocol - version 4
bit/s	bits per second　*bpsと表記する場合もあります。
BOOTP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
C-Tag	Customer Tag

CA	Certificate Authority
CC	Continuity Check
CCM	Continuity Check Message
CFM	Connectivity Fault Management
CFP	C Form-factor Pluggable
CIDR	Classless Inter-Domain Routing
CLI	Command Line Interface
CoS	Class of Service
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DNS	Domain Name System
DNSSL	Domain Name System Search List
DR	Designated Router
DSA	Digital Signature Algorithm
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
E-mail	Electronic mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EFM	Ethernet in the First Mile
ETH-AIS	Ethernet Alarm Indicator Signal
ETH-LCK	Ethernet Locked Signal
FAN	Fan Unit
FCS	Frame Check Sequence
FE	Forwarding Engine
HDC	Hardware Dependent Code
HMAC	Keyed-Hashing for Message Authentication
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
ISP	Internet Service Provider
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LCD	Liquid Crystal Display
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLPQ	Low Latency Priority Queueing
LLQ	Low Latency Queueing
LLRLQ	Low Latency Rate Limited Queueing
LSA	Link State Advertisement
MA	Maintenance Association
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MEG	Maintenance Entity Group
MEP	Maintenance association End Point/Maintenance entity group End Point
MIB	Management Information Base
MIP	Maintenance domain Intermediate Point
MLD	Multicast Listener Discovery
MP	Maintenance Point
MRU	Maximum Receive Unit
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transfer Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NBMA	Non-Broadcast Multiple-Access

NDP	Neighbor Discovery Protocol
NIF	Network Interface
NSAP	Network Service Access Point
NSR	NonStop Routing
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OAM	Operations,Administration,and Maintenance
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
PA	Protocol Accelerator
packet/s	packets per second　　*ppsと表記する場合もあります。
PAD	PADding
PC	Personal Computer
PDU	Protocol Data Unit
PE-ME	Programmable Engine Micro Engine
PE-NIF	Programmable Engine Network Interface
PGP	Pretty Good Privacy
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PIM-SM	Protocol Independent Multicast-Sparse Mode
PIM-SSM	Protocol Independent Multicast-Source Specific Multicast
PQ	Priority Queueing
PRU	Packet Routing Unit
PS	Power Supply
PSINPUT	Power Supply Input
PSU	Packet Switching Unit
QoS	Quality of Service
QSFP+	Quad Small Form factor Pluggable Plus
QSFP28	28Gbps Quad Small Form factor Pluggable
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
RDNSS	Recursive Domain Name System Server
RFC	Request For Comments
RGQ	Rate Guaranteed Queueing
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RQ	ReQuest
RR	Round Robin
RSA	Rivest, Shamir, Adleman
S-Tag	Service Tag
SA	Source Address
SD	Secure Digital
SFD	Start Frame Delimiter
SFP	Small Form-factor Pluggable
SFP+	enhanced Small Form-factor Pluggable
SFU	Switch Fabric Unit
SHA1	Secure Hash Algorithm 1
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNPA	Subnetwork Point of Attachment
SNTP	Simple Network Time Protocol
SOP	System Operational Panel
SPF	Shortest Path First
SSAP	Source Service Access Point
SSH	Secure Shell
SSW	Sub-crossbar SWitch
STP	Spanning Tree Protocol
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLV	Type, Length, and Value
TOS	Type Of Service
TPID	Tag Protocol Identifier
TTL	Time To Live
UDLD	Uni-Directional Link Detection
UDP	User Datagram Protocol
URL	Uniform Resource Locator
uRPF	unicast Reverse Path Forwarding
VLAN	Virtual LAN
VPN	Virtual Private Network

VRF	Virtual Routing and Forwarding/Virtual Routing and Forwarding Instance
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WFQ	Weighted Fair Queueing
WWW	World-Wide Web

■ KB（キロバイト）などの単位表記について

1KB（キロバイト），1MB（メガバイト），1GB（ギガバイト），1TB（テラバイト）はそれぞれ 1024 バイト，1024^2 バイト，1024^3 バイト，1024^4 バイトです。

目次

第 1 編　IP パケット中継

1 IP・ARP・ICMP の解説 1

1.1 アドレッシング 2
1.1.1 IP アドレス 2
1.1.2 サブネットマスク 2
1.2 IP レイヤ機能 4
1.2.1 中継機能 4
1.2.2 IP アドレス付与単位 4
1.3 通信機能 5
1.3.1 インターネットプロトコル（IP） 5
1.3.2 ICMP 6
1.3.3 ARP 9
1.3.4 Address Conflict Detection 11
1.4 中継機能 12
1.4.1 IP パケットの中継方法 12
1.4.2 ブロードキャストパケットの中継方法 13
1.4.3 MTU とフラグメント 16
1.5 ループバックインタフェース 18
1.6 IPv4 使用時の注意事項 19

2 IP・ARP・ICMP の設定と運用 21

2.1 コンフィグレーション 22
2.1.1 コンフィグレーションコマンド一覧 22
2.1.2 インタフェースの設定 22
2.1.3 マルチホームの設定 23
2.1.4 ダイレクトブロードキャスト中継の設定 23
2.1.5 ループバックインタフェースの設定 23
2.1.6 複数のループバックインタフェースの設定 24
2.1.7 スタティック ARP の設定 24
2.2 オペレーション 25
2.2.1 運用コマンド一覧 25
2.2.2 IPv4 インタフェースの up/down 確認 25
2.2.3 宛先アドレスとの通信可否の確認 25
2.2.4 宛先アドレスまでの経路確認 26
2.2.5 ARP 情報の確認 26

3 IPv6・NDP・ICMPv6 の解説 27
3.1 アドレッシング 28
3.1.1 IPv6 アドレス 28
3.1.2 アドレス表記方法 30
3.1.3 アドレスフォーマットプレフィックス 30
3.1.4 ユニキャストアドレス 32
3.1.5 マルチキャストアドレス 36
3.1.6 本装置で使用する IPv6 アドレスの扱い 38
3.1.7 ステートレスアドレス自動設定機能 39
3.2 IPv6 レイヤ機能 40
3.2.1 中継機能 40
3.2.2 IPv6 アドレス付与単位 40
3.3 通信機能 41
3.3.1 インターネットプロトコル バージョン 6（IPv6） 41
3.3.2 ICMPv6 44
3.3.3 NDP 45
3.4 中継機能 47
3.4.1 ルーティングテーブルの内容 47
3.4.2 ルーティングテーブルの検索 47
3.5 ループバックインタフェース 48
3.6 IPv6 使用時の注意事項 49
4 IPv6・NDP・ICMPv6 の設定と運用 51
4.1 コンフィグレーション 52
4.1.1 コンフィグレーションコマンド一覧 52
4.1.2 インタフェースの設定 52
4.1.3 リンクローカルアドレスの手動設定 53
4.1.4 ループバックインタフェースの設定 53
4.1.5 複数のループバックインタフェースの設定 53
4.1.6 スタティック NDP の設定 54
4.2 オペレーション 55
4.2.1 運用コマンド一覧 55
4.2.2 IPv6 インタフェースの up/down 確認 55
4.2.3 宛先アドレスとの通信可否の確認 55
4.2.4 宛先アドレスまでの経路確認 56
4.2.5 NDP 情報の確認 56
5 VRF 57
5.1 解説 58

5.1.1 概要 58
5.1.2 サポート機能一覧 58
5.1.3 エクストラネット 63
5.2 コンフィグレーション 65
5.2.1 コンフィグレーションコマンド一覧 65
5.2.2 VRF の設定 65
5.3 オペレーション 67
5.3.1 運用コマンド一覧 67
5.3.2 VRF 情報の確認 67

6 Null インタフェース 69
6.1 解説 70
6.2 コンフィグレーション 72
6.2.1 コンフィグレーションコマンド一覧 72
6.2.2 Null インタフェースの設定 72
6.3 オペレーション 74
6.3.1 運用コマンド一覧 74
6.3.2 経路情報の確認 74
6.3.3 パケット廃棄数の確認 75

7 uRPF 77
7.1 解説 78
7.1.1 uRPF の概要 78
7.1.2 サポートモード 78
7.1.3 uRPF 使用時の注意事項 79
7.2 コンフィグレーション 81
7.2.1 コンフィグレーションコマンド一覧 81
7.2.2 装置全体での uRPF 設定 81
7.2.3 インタフェース単位での uRPF 設定 81
7.3 オペレーション 82
7.3.1 運用コマンド一覧 82
7.3.2 装置全体での uRPF 設定状態および廃棄パケット数確認 82
7.3.3 インタフェースごとの uRPF 設定状態および廃棄パケット数確認 82

8 ポリシーベースルーティング 85
8.1 解説 86
8.1.1 概要 86
8.1.2 対象パケット 88
8.1.3 ネクストホップ 88

8.1.4 ネクストホップの冗長化 89
8.1.5 対象パケットとネクストホップの指定方法 92
8.1.6 注意事項 92
8.2 コンフィグレーション 94
8.2.1 コンフィグレーションコマンド一覧 94
8.2.2 IPv4 パケットを対象としたポリシーベースルーティングの設定 95
8.2.3 IPv6 パケットを対象としたポリシーベースルーティングの設定 96
8.2.4 異なる VRF 間でのポリシーベースルーティングの設定 98
8.3 オペレーション 100
8.3.1 運用コマンド一覧 100
8.3.2 ポリシーベースルーティングの確認 100

9 RA 103
9.1 解説 104
9.1.1 概要 104
9.1.2 情報の配布 104
9.1.3 プレフィックス情報変更時の対処 108
9.2 コンフィグレーション 110
9.2.1 コンフィグレーションコマンド一覧 110
9.2.2 RA 送信抑止の設定 110
9.2.3 配布情報の設定 111
9.2.4 RA 送信間隔の調整 111
9.3 オペレーション 112
9.3.1 運用コマンド一覧 112
9.3.2 サマリー情報の確認 112
9.3.3 詳細情報の確認 112

10 DHCP/BOOTP リレーエージェント 113
10.1 解説 114
10.1.1 概要 114
10.1.2 サポート範囲 114
10.1.3 DHCP/BOOTP プロトコル 115
10.1.4 DHCP/BOOTP パケット転送時の設定内容 116
10.1.5 リレーエージェント情報オプション（Option82） 119
10.1.6 DHCP/BOOTP リレーエージェント使用時の注意事項 121
10.2 コンフィグレーション 122
10.2.1 コンフィグレーションコマンド一覧 122
10.2.2 DHCP/BOOTP パケットをサーバへ転送する設定（基本設定） 122
10.2.3 マルチホーム構成での設定 123

10.2.4 VRF 構成での設定 124
10.2.5 リレーエージェント情報オプション（DHCP Option82）を付ける設定 125
10.2.6 VRF（エクストラネット）構成での設定 126
10.3 オペレーション 128
10.3.1 運用コマンド一覧 128
10.3.2 DHCP/BOOTP リレーエージェントのインタフェース情報の確認 128

11 DHCPv6 リレーエージェント 129
11.1 解説 130
11.1.1 概要 130
11.1.2 サポート範囲 130
11.1.3 DHCPv6 パケット転送時の設定内容 132
11.1.4 プレフィックス委任情報の学習 134
11.1.5 プレフィックス委任に対する IPv6 スタティック経路自動生成 134
11.1.6 DHCPv6 リレーエージェント使用時の注意事項 135
11.2 コンフィグレーション 136
11.2.1 コンフィグレーションコマンド一覧 136
11.2.2 DHCPv6 パケットをサーバへ転送する設定（基本設定） 136
11.2.3 DHCPv6 パケットをネットワークセグメント内の全サーバへ転送する設定 137
11.2.4 DHCPv6 パケットを複数の DHCPv6 リレーエージェントを経由してサーバへ転送する設定 138
11.2.5 VRF（経路交換によるエクストラネット）構成での設定 139
11.3 オペレーション 141
11.3.1 運用コマンド一覧 141
11.3.2 プレフィックス委任の確認 141
11.3.3 IPv6 スタティック経路自動生成の確認 141

12 VRRP 143
12.1 解説 144
12.1.1 仮想ルータの MAC アドレスと IP アドレス 144
12.1.2 VRRP における障害検出の仕組み 146
12.1.3 マスタの選出方法 146
12.1.4 ADVERTISEMENT パケットの認証 147
12.1.5 アクセプトモード 148
12.1.6 VRRP のサポート規格 148
12.1.7 グループ切替機能 151
12.1.8 VRRP 使用時の注意事項 153
12.2 コンフィグレーション 155
12.2.1 コンフィグレーションコマンド一覧 155
12.2.2 VRRP のコンフィグレーションの流れ 155
12.2.3 仮想ルータへの IPv4 アドレス設定 156

12.2.4　仮想ルータへの IPv6 アドレス設定　157
12.2.5　優先度の設定　157
12.2.6　ADVERTISEMENT パケット送信間隔の設定　157
12.2.7　自動切り戻し抑止の設定　159
12.2.8　自動切り戻し抑止時間の設定　159
12.2.9　VRRP 動作モードの設定　159
12.2.10　仮想ルータのグループ化　160
12.2.11　グループ構成の変更　162
12.3　オペレーション　166
12.3.1　運用コマンド一覧　166
12.3.2　仮想ルータの設定確認　166
12.3.3　切り戻し処理の実行　167

第 2 編　ユニキャストルーティング

13 ユニキャストルーティング　169
13.1　ユニキャストルーティング共通の解説　170
13.1.1　ルーティング概要　170
13.1.2　スタティックルーティングとダイナミックルーティング　170
13.1.3　経路情報　171
13.1.4　ルーティングプロトコルごとの適用範囲　172
13.1.5　ルーティングプロトコルの同時動作　173
13.1.6　複数プロトコル同時動作時の注意事項　175
13.1.7　コンフィグレーション設定・変更時の留意事項　178
13.2　ユニキャストルーティング共通のオペレーション　179
13.2.1　運用コマンド一覧　179
13.2.2　宛先アドレスへの経路確認　180
13.3　ネットワーク設計の考え方　181
13.3.1　IPv4 ネットワークのアドレス設計　181
13.3.2　IPv4 ネットワークの直結経路の取り扱い　181
13.3.3　IPv4 ネットワークのアドレス境界の設計　181
13.3.4　IPv6 ネットワークのアドレス設計　181
13.3.5　IPv6 ネットワークの直結経路の取り扱い　182
13.4　ロードバランスの解説　183
13.4.1　ロードバランスの概要　183
13.4.2　ロードバランス仕様　184
13.4.3　出力インタフェースの決定　185
13.4.4　ロードバランス使用時の注意事項　185
13.5　ロードバランスのコンフィグレーション　187

13.6 ロードバランスのオペレーション 188
13.6.1 経路情報の確認 188
13.6.2 宛先アドレスとの通信可否の確認 188
13.7 経路集約の解説 189
13.7.1 概要 189
13.7.2 集約経路の転送方法 189
13.7.3 AS_PATH 属性の集約 189
13.7.4 集約元経路の広告抑止 190
13.8 経路集約のコンフィグレーション 192
13.8.1 コンフィグレーションコマンド一覧 192
13.8.2 IPv4 経路集約と集約経路広告の設定 192
13.8.3 IPv6 経路集約と集約経路広告の設定 193
13.9 経路集約のオペレーション 195
13.9.1 運用コマンド一覧 195
13.9.2 IPv4 集約経路の確認 195
13.9.3 IPv6 集約経路の確認 195
13.10 ユニキャストルーティング高可用機能 197
13.10.1 概要 197
13.10.2 ノンストップルーティング 198
13.10.3 グレースフル・リスタート 198
13.10.4 ユニキャストルーティング高可用機能使用時の注意事項 200
13.11 高速経路切替機能 202
13.11.1 概要 202
13.11.2 使用上の注意事項 203
13.12 VRF の解説 204
13.12.1 サポート範囲 204
13.12.2 経路数の制限 204
13.12.3 エクストラネット 206
13.13 VRF のコンフィグレーション 209
13.13.1 コンフィグレーションコマンド一覧 209
13.13.2 最大経路数の設定 209
13.13.3 エクストラネットの設定 210
13.14 VRF のオペレーション 211
13.14.1 運用コマンド一覧 211
13.14.2 最大経路数の確認 211
13.14.3 エクストラネットの確認 211

14 スタティックルーティング 213
14.1 解説 214
14.1.1 概要 214

14.1.2 経路選択基準 214
14.1.3 スタティック経路の中継経路指定 215
14.1.4 動的監視機能 215
14.2 コンフィグレーション 219
14.2.1 コンフィグレーションコマンド一覧 219
14.2.2 デフォルト経路の設定 219
14.2.3 シングルパス経路の設定 219
14.2.4 マルチパス経路の設定 220
14.2.5 動的監視機能の適用 221
14.2.6 VRF でのスタティック経路の設定 222
14.2.7 VRF 間にわたるスタティック経路の設定 222
14.2.8 IPv6 リンクローカルアドレスをネクストホップとした VRF 間にわたるスタティック経路の設定 223
14.3 オペレーション 224
14.3.1 運用コマンド一覧 224
14.3.2 経路情報の確認 224
14.3.3 ゲートウェイ情報の確認 225
15 RIP 227
15.1 解説 228
15.1.1 概要 228
15.1.2 経路選択基準 229
15.1.3 経路情報の広告 230
15.1.4 経路情報の学習 237
15.1.5 RIP-1 239
15.1.6 RIP-2 242
15.2 コンフィグレーション 245
15.2.1 コンフィグレーションコマンド一覧 245
15.2.2 RIP の適用 246
15.2.3 メトリックの設定 246
15.2.4 タイマの調整 247
15.2.5 RIP パケットの送信抑止 247
15.2.6 RIP パケット送信相手の限定 248
15.2.7 認証の適用 249
15.2.8 VRF での RIP の適用 249
15.3 オペレーション 251
15.3.1 運用コマンド一覧 251
15.3.2 RIP の動作状況の確認 251
15.3.3 送信先情報の確認 251
15.3.4 学習経路情報の確認 251
15.3.5 広告経路情報の確認 252

16 RIPng 253
16.1 解説 254
16.1.1 概要 254
16.1.2 経路選択基準 255
16.1.3 経路情報の広告 256
16.1.4 経路情報の学習 260
16.1.5 RIPng の諸機能 262
16.1.6 注意事項 263
16.2 コンフィグレーション 265
16.2.1 コンフィグレーションコマンド一覧 265
16.2.2 RIPng の適用 265
16.2.3 メトリックの設定 266
16.2.4 タイマの調整 267
16.2.5 VRF での RIPng の適用 267
16.3 オペレーション 269
16.3.1 運用コマンド一覧 269
16.3.2 RIPng の動作状況の確認 269
16.3.3 送信先情報の確認 269
16.3.4 学習経路情報の確認 269
16.3.5 広告経路情報の確認 270
17 OSPF 271
17.1 OSPF 基本機能の解説 272
17.1.1 OSPF の特長 272
17.1.2 OSPF の機能 272
17.1.3 経路選択アルゴリズム 273
17.1.4 LSA の広告 274
17.1.5 AS 外経路の導入例 275
17.1.6 経路選択の基準 276
17.1.7 イコールコストマルチパス 278
17.1.8 注意事項 278
17.2 OSPF 基本機能のコンフィグレーション 280
17.2.1 コンフィグレーションコマンド一覧 280
17.2.2 コンフィグレーションの流れ 280
17.2.3 OSPF 適用の設定 281
17.2.4 AS 外経路広告の設定 281
17.2.5 経路選択の設定 282
17.2.6 マルチパスの設定 282
17.2.7 VRF での OSPF の適用 283

17.3 インタフェースの解説 284
17.3.1 OSPF インタフェース種別 284
17.3.2 隣接ルータとの接続 284
17.3.3 ブロードキャスト型ネットワークと指定ルータ 285
17.3.4 LSA の送信 286
17.3.5 パッシブインタフェース 286
17.4 インタフェースのコンフィグレーション 287
17.4.1 コンフィグレーションコマンド一覧 287
17.4.2 コンフィグレーションの流れ 288
17.4.3 NBMA での隣接ルータの設定 288
17.4.4 インタフェースパラメータ変更の設定 289
17.5 OSPF のオペレーション 290
17.5.1 運用コマンド一覧 290
17.5.2 ドメインの確認 290
17.5.3 隣接ルータ情報の確認 290
17.5.4 インタフェース情報の確認 292
17.5.5 LSA の確認 292

18 OSPF 拡張機能 295
18.1 エリアとエリア分割機能の解説 296
18.1.1 エリアボーダ 296
18.1.2 エリア分割した場合の経路制御 297
18.1.3 スタブエリア 298
18.1.4 NSSA 298
18.1.5 仮想リンク 299
18.1.6 仮想リンクの動作 300
18.2 エリアのコンフィグレーション 302
18.2.1 コンフィグレーションコマンド一覧 302
18.2.2 コンフィグレーションの流れ 302
18.2.3 スタブエリアの設定 303
18.2.4 エリアボーダルータの設定 303
18.2.5 仮想リンクの設定 304
18.3 隣接ルータ認証の解説 305
18.3.1 認証手順 305
18.4 隣接ルータ認証のコンフィグレーション 306
18.4.1 コンフィグレーションコマンド一覧 306
18.4.2 MD5 認証キーの変更 306
18.4.3 平文パスワード認証の設定 306
18.4.4 MD5 認証の設定 307
18.5 ノンストップルーティングの解説 308

18.5.1 概要 308
18.5.2 注意事項 308
18.6 ノンストップルーティングのコンフィグレーション 309
18.6.1 コンフィグレーションコマンド一覧 309
18.6.2 ノンストップルーティングの設定 309
18.7 グレースフル・リスタートの解説 310
18.7.1 概要 310
18.7.2 ヘルパー機能 310
18.7.3 リスタート機能 310
18.8 グレースフル・リスタートのコンフィグレーション 313
18.8.1 コンフィグレーションコマンド一覧 313
18.8.2 リスタート機能の設定 313
18.8.3 ヘルパー機能の設定 313
18.9 スタブルータの解説 315
18.9.1 概要 315
18.9.2 スタブルータの動作 315
18.10 スタブルータのコンフィグレーション 317
18.10.1 コンフィグレーションコマンド一覧 317
18.10.2 スタブルータ機能の設定 317
18.11 OSPF 拡張機能のオペレーション 318
18.11.1 運用コマンド一覧 318
18.11.2 エリアボーダの確認 318
18.11.3 エリアの確認 318
18.11.4 ノンストップルーティングの確認 319
18.11.5 グレースフル・リスタートの確認 319

19 OSPFv3 321
19.1 OSPFv3 基本機能の解説 322
19.1.1 OSPFv3 の特長 322
19.1.2 OSPFv3 の機能 322
19.1.3 経路選択アルゴリズム 323
19.1.4 LSA の広告 324
19.1.5 AS 外経路の導入例 325
19.1.6 経路選択の基準 326
19.1.7 イコールコストマルチパス 327
19.1.8 注意事項 327
19.2 OSPFv3 基本機能のコンフィグレーション 329
19.2.1 コンフィグレーションコマンド一覧 329
19.2.2 コンフィグレーションの流れ 329
19.2.3 OSPFv3 適用の設定 330

19.2.4 AS 外経路広告の設定 330
19.2.5 経路選択の設定 330
19.2.6 マルチパスの設定 331
19.2.7 VRF での OSPFv3 の適用 332
19.3 インタフェースの解説 333
19.3.1 OSPFv3 インタフェース種別 333
19.3.2 隣接ルータとの接続 333
19.3.3 ブロードキャスト型ネットワークと指定ルータ 334
19.3.4 LSA の送信 334
19.3.5 パッシブインタフェース 335
19.4 インタフェースのコンフィグレーション 336
19.4.1 コンフィグレーションコマンド一覧 336
19.4.2 インタフェースパラメータ変更の設定 336
19.5 OSPFv3 のオペレーション 338
19.5.1 運用コマンド一覧 338
19.5.2 ドメインの確認 338
19.5.3 隣接ルータ情報の確認 338
19.5.4 インタフェース情報の確認 339
19.5.5 LSA の確認 340

20 OSPFv3 拡張機能 343
20.1 エリアとエリア分割機能の解説 344
20.1.1 エリアボーダ 344
20.1.2 エリア分割した場合の経路制御 345
20.1.3 スタブエリア 346
20.1.4 仮想リンク 346
20.1.5 仮想リンクの動作 347
20.2 エリアのコンフィグレーション 349
20.2.1 コンフィグレーションコマンド一覧 349
20.2.2 コンフィグレーションの流れ 349
20.2.3 スタブエリアの設定 350
20.2.4 エリアボーダルータの設定 350
20.2.5 仮想リンクの設定 351
20.3 ノンストップルーティングの解説 352
20.3.1 概要 352
20.3.2 注意事項 352
20.4 ノンストップルーティングのコンフィグレーション 353
20.4.1 コンフィグレーションコマンド一覧 353
20.4.2 ノンストップルーティングの設定 353
20.5 グレースフル・リスタートの解説 354

20.5.1 概要 354
20.5.2 ヘルパー機能 354
20.5.3 リスタート機能 354
20.6 グレースフル・リスタートのコンフィグレーション 358
20.6.1 コンフィグレーションコマンド一覧 358
20.6.2 リスタート機能の設定 358
20.6.3 ヘルパー機能の設定 358
20.7 スタブルータの解説 360
20.7.1 概要 360
20.7.2 スタブルータの動作 360
20.8 スタブルータのコンフィグレーション 362
20.8.1 コンフィグレーションコマンド一覧 362
20.8.2 スタブルータ機能の設定 362
20.9 OSPFv3 拡張機能のオペレーション 363
20.9.1 運用コマンド一覧 363
20.9.2 エリアボーダの確認 363
20.9.3 エリアの確認 363
20.9.4 ノンストップルーティングの確認 364
20.9.5 グレースフル・リスタートの確認 365

21 BGP4/BGP4+ 367
21.1 解説 368
21.1.1 概要 368
21.1.2 ピアの種別と接続形態 369
21.1.3 経路選択 370
21.1.4 VRF での BGP4 または BGP4+ 379
21.1.5 BGP4 または BGP4+使用時の注意事項 379
21.2 BGP4 のコンフィグレーション 383
21.2.1 コンフィグレーションコマンド一覧 383
21.2.2 コンフィグレーションの流れ 385
21.2.3 BGP4 ピアの設定 386
21.2.4 BGP4 経路の学習ポリシーの設定 386
21.2.5 BGP4 経路の広告ポリシーの設定 387
21.2.6 学習用経路フィルタの設定 387
21.2.7 広告用経路フィルタの設定 388
21.2.8 学習経路フィルタリングの条件の設定 388
21.2.9 広告経路フィルタリングの条件の設定 389
21.2.10 経路フィルタリングの運用への反映 389
21.2.11 VRF での BGP4 の設定 390
21.3 BGP4+のコンフィグレーション 391

21.3.1 コンフィグレーションコマンド一覧 391
21.3.2 コンフィグレーションの流れ 393
21.3.3 BGP4+ピアの設定 394
21.3.4 BGP4+経路の学習ポリシーの設定 395
21.3.5 BGP4+経路の広告ポリシーの設定 395
21.3.6 学習用経路フィルタの設定 395
21.3.7 広告用経路フィルタの設定 396
21.3.8 学習経路フィルタリングの条件の設定 397
21.3.9 広告経路フィルタリングの条件の設定 397
21.3.10 経路フィルタリングの運用への反映 398
21.3.11 VRF での BGP4+の設定 398
21.4 オペレーション 399
21.4.1 運用コマンド一覧 399
21.4.2 ピアの種別と接続形態の確認 399
21.4.3 経路選択結果の確認 400
21.4.4 経路の広告内容の確認 401

22 BGP4/BGP4+拡張機能 403
22.1 解説 404
22.1.1 ピアグループ 404
22.1.2 コミュニティ 404
22.1.3 マルチパス 406
22.1.4 サポート機能のネゴシエーション 408
22.1.5 ルート・リフレッシュ 409
22.1.6 TCP MD5 認証 410
22.1.7 広告用経路生成 410
22.1.8 ルート・フラップ・ダンプニング 412
22.1.9 ルート・リフレクション 412
22.1.10 コンフェデレーション 414
22.1.11 ノンストップルーティング 418
22.1.12 グレースフル・リスタート 419
22.1.13 学習経路数制限 423
22.1.14 インタフェースダウン時の外部ピア即時切断機能 423
22.1.15 4 バイト AS 番号 424
22.2 BGP4 拡張機能のコンフィグレーション 427
22.2.1 BGP4 ピアグループの設定 427
22.2.2 コミュニティの設定 428
22.2.3 BGP4 マルチパスの設定 430
22.2.4 TCP MD5 認証の設定 431
22.2.5 BGP4 広告用経路生成の設定 431

22.2.6 ルート・フラップ・ダンプニングの設定 434
22.2.7 ルート・リフレクションの設定 434
22.2.8 コンフェデレーションの設定 435
22.2.9 ノンストップルーティングの設定 437
22.2.10 グレースフル・リスタートの設定 438
22.2.11 BGP4 学習経路数制限の設定 439
22.2.12 インタフェースダウン時の外部ピア即時切断機能の設定 439
22.3 BGP4+拡張機能のコンフィグレーション 441
22.3.1 BGP4+ピアグループの設定 441
22.3.2 コミュニティの設定 442
22.3.3 BGP4+マルチパスの設定 444
22.3.4 TCP MD5 認証の設定 445
22.3.5 BGP4+広告用経路生成の設定 446
22.3.6 ルート・フラップ・ダンプニングの設定 448
22.3.7 ルート・リフレクションの設定 449
22.3.8 コンフェデレーションの設定 450
22.3.9 ノンストップルーティングの設定 452
22.3.10 グレースフル・リスタートの設定 453
22.3.11 BGP4+学習経路数制限の設定 454
22.3.12 インタフェースダウン時の外部ピア即時切断機能の設定 455
22.4 オペレーション 456
22.4.1 ピアグループの確認 456
22.4.2 コミュニティの確認 457
22.4.3 マルチパスの確認 458
22.4.4 サポート機能のネゴシエーションの確認 459
22.4.5 ルート・リフレッシュの確認 460
22.4.6 TCP MD5 認証の確認 462
22.4.7 広告用経路生成の確認 463
22.4.8 ルート・フラップ・ダンプニングの確認 464
22.4.9 ルート・リフレクションの確認 465
22.4.10 コンフェデレーションの確認 466
22.4.11 ノンストップルーティングの確認 467
22.4.12 グレースフル・リスタートの確認 468
22.4.13 学習経路数制限の確認 470
22.4.14 インタフェースダウン時の外部ピア即時切断機能の確認 471

23 経路フィルタリング 473
23.1 解説 474
23.1.1 経路フィルタリング概要 474
23.1.2 フィルタ方法 476

23.1.3 RIP および RIPng 483
23.1.4 OSPF および OSPFv3 487
23.1.5 BGP4 および BGP4+ 490
23.1.6 エクストラネット 494
23.2 コンフィグレーション（IPv4） 496
23.2.1 コンフィグレーションコマンド一覧 496
23.2.2 RIP 学習経路フィルタリング 498
23.2.3 RIP 広告経路フィルタリング 500
23.2.4 OSPF 学習経路フィルタリング 503
23.2.5 OSPF 広告経路フィルタリング 505
23.2.6 BGP4 学習経路フィルタリング 507
23.2.7 BGP4 広告経路フィルタリング 509
23.2.8 エクストラネット 511
23.3 コンフィグレーション（IPv6） 514
23.3.1 コンフィグレーションコマンド一覧 514
23.3.2 RIPng 学習経路フィルタリング 516
23.3.3 RIPng 広告経路フィルタリング 518
23.3.4 OSPFv3 学習経路フィルタリング 521
23.3.5 OSPFv3 広告経路フィルタリング 522
23.3.6 BGP4+学習経路フィルタリング 525
23.3.7 BGP4+広告経路フィルタリング 527
23.3.8 エクストラネット 529
23.4 オペレーション 532
23.4.1 運用コマンド一覧 532
23.4.2 学習経路フィルタリング前の確認 532
23.4.3 学習経路フィルタリング後の確認 534
23.4.4 広告経路フィルタリング前の確認 536
23.4.5 広告経路フィルタリング後の確認 537
23.4.6 エクストラネットの確認 539

第 3 編 マルチキャストルーティング

24 IPv4 マルチキャストの解説 541
24.1 IPv4 マルチキャスト概説 542
24.1.1 IPv4 マルチキャストアドレス 542
24.1.2 IPv4 マルチキャストルーティング機能 543
24.1.3 IPv4 マルチキャストパケットの受信 543
24.2 IPv4 マルチキャストグループマネージメント機能 544
24.2.1 IGMP の概要 544

24.2.2 IGMP メッセージサポート仕様 544
24.2.3 IGMP の動作 546
24.2.4 Querier の決定 548
24.2.5 IPv4 グループメンバの管理 549
24.2.6 IGMP タイマ値 550
24.2.7 IGMPv1/IGMPv2/IGMPv3 装置との接続 552
24.2.8 静的グループ参加機能 554
24.2.9 IGMP 使用時の注意事項 554
24.3 IPv4 マルチキャスト中継機能 555
24.3.1 IPv4 マルチキャスト中継対象外アドレス 555
24.3.2 IPv4 マルチキャストパケット中継処理 555
24.4 IPv4 経路制御機能 557
24.4.1 IPv4 マルチキャストルーティングプロトコル概説 557
24.4.2 IPv4 PIM-SM 557
24.4.3 IPv4 PIM-SSM 568
24.4.4 IGMPv3 使用時の IPv4 経路制御動作 571
24.4.5 系切替時の無停止マルチキャスト中継機能 573
24.4.6 マルチキャストロードバランス 575
24.4.7 VRF での IPv4 マルチキャスト 576
24.5 ネットワーク設計の考え方 580
24.5.1 IPv4 マルチキャスト中継 580
24.5.2 冗長経路（障害などによる経路切り替え） 581
24.5.3 適応ネットワーク構成例 582
24.5.4 ネットワーク構成での注意事項 584

25 IPv4 マルチキャストの設定と運用 589
25.1 コンフィグレーション 590
25.1.1 コンフィグレーションコマンド一覧 590
25.1.2 コンフィグレーションの流れ 591
25.1.3 IPv4 マルチキャストルーティング機能の設定 593
25.1.4 IPv4 PIM-SM/PIM-SSM 動作インタフェースの設定 593
25.1.5 IPv4 PIM-SM ランデブーポイント候補の設定 593
25.1.6 IPv4 PIM-SM ブートストラップルータ候補の設定 594
25.1.7 IPv4 PIM-SM 静的ランデブーポイント機能の設定 594
25.1.8 IPv4 PIM-SSM の設定 595
25.1.9 IGMP の設定 596
25.1.10 VRF での IPv4 マルチキャストルーティング機能の設定 596
25.1.11 VRF での IPv4 PIM-SM/PIM-SSM 動作インタフェースの設定 596
25.1.12 VRF での IPv4 PIM-SM ランデブーポイント候補の設定 597
25.1.13 VRF での IPv4 PIM-SM ブートストラップルータ候補の設定 598

25.1.14 VRF での IPv4 PIM-SM 静的ランデブーポイント機能の設定 598
25.1.15 VRF での IPv4 PIM-SSM の設定 599
25.1.16 VRF での IGMP の設定 600
25.1.17 IPv4 マルチキャストエクストラネットの設定 601
25.2 オペレーション 603
25.2.1 運用コマンド一覧 603
25.2.2 IPv4 PIM-SM 情報の確認 603
25.2.3 IGMP 情報の確認 607

26 IPv6 マルチキャストの解説 609
26.1 IPv6 マルチキャスト概説 610
26.1.1 IPv6 マルチキャストアドレス 610
26.1.2 IPv6 マルチキャストルーティング機能 610
26.1.3 IPv6 マルチキャストパケットの受信 610
26.2 IPv6 マルチキャストグループマネージメント機能 612
26.2.1 MLD の概要 612
26.2.2 MLD メッセージサポート仕様 612
26.2.3 MLD の動作 614
26.2.4 Querier の決定 616
26.2.5 IPv6 グループメンバの管理 617
26.2.6 MLD タイマ値 618
26.2.7 MLDv1/MLDv2 装置との接続 620
26.2.8 静的グループ参加機能 620
26.2.9 MLD 使用時の注意事項 621
26.3 IPv6 マルチキャスト中継機能 622
26.3.1 IPv6 マルチキャスト中継対象外アドレス 622
26.3.2 IPv6 マルチキャストパケット中継処理 622
26.4 IPv6 経路制御機能 624
26.4.1 IPv6 マルチキャストルーティングプロトコル概説 624
26.4.2 IPv6 PIM-SM 624
26.4.3 IPv6 PIM-SSM 636
26.4.4 MLDv2 使用時の IPv6 経路制御動作 639
26.4.5 系切替時の無停止マルチキャスト中継機能 640
26.4.6 VRF での IPv6 マルチキャスト 643
26.5 ネットワーク設計の考え方 646
26.5.1 IPv6 マルチキャスト中継 646
26.5.2 冗長経路（障害などによる経路切り替え） 647
26.5.3 適応ネットワーク構成例 649
26.5.4 ネットワーク構成での注意事項 650

27 IPv6 マルチキャストの設定と運用 657
27.1 コンフィグレーション 658
27.1.1 コンフィグレーションコマンド一覧 658
27.1.2 コンフィグレーションの流れ 659
27.1.3 IPv6 マルチキャストルーティング機能の設定 660
27.1.4 IPv6 PIM-SM/PIM-SSM 動作インタフェースの設定 660
27.1.5 IPv6 PIM-SM ランデブーポイント候補の設定 661
27.1.6 IPv6 PIM-SM ブートストラップルータ候補の設定 661
27.1.7 IPv6 PIM-SM 静的ランデブーポイント機能の設定 662
27.1.8 IPv6 PIM-SSM の設定 662
27.1.9 MLD の設定 663
27.1.10 VRF での IPv6 マルチキャストルーティング機能の設定 664
27.1.11 VRF での IPv6 PIM-SM/PIM-SSM 動作インタフェースの設定 664
27.1.12 VRF での IPv6 PIM-SM ランデブーポイント候補の設定 665
27.1.13 VRF での IPv6 PIM-SM ブートストラップルータ候補の設定 666
27.1.14 VRF での IPv6 PIM-SM 静的ランデブーポイント機能の設定 666
27.1.15 VRF での IPv6 PIM-SSM の設定 667
27.1.16 VRF での MLD の設定 668
27.1.17 IPv6 マルチキャストエクストラネットの設定 669
27.2 オペレーション 671
27.2.1 運用コマンド一覧 671
27.2.2 IPv6 PIM-SM 情報の確認 671
27.2.3 MLD 情報の確認 675

28 IPv6 マルチキャスト拡張機能 677
28.1 マルチキャストチャネル参加制限機能の解説 678
28.1.1 概要 678
28.1.2 マルチキャストチャネルリストでのフィルタリング 679
28.1.3 マルチキャストチャネルフィルタ機能 682
28.1.4 ソース数・マルチキャストグループ数制限機能 683
28.1.5 マルチキャストチャネル数制限機能 683
28.1.6 マルチキャストチャネル受信者数制限機能 684
28.1.7 帯域管理機能 685
28.1.8 マルチキャストチャネル参加制限機能の処理順序 686
28.1.9 系切替時の参加制限状態の維持 686
28.2 マルチキャストチャネル参加制限機能のコンフィグレーション 687
28.2.1 コンフィグレーションコマンド一覧 687
28.2.2 コンフィグレーションの流れ 687
28.2.3 マルチキャストチャネルリストの設定 688

28.2.4 マルチキャストチャネルへの帯域値の設定 688
28.2.5 マルチキャストチャネルフィルタ機能の設定 688
28.2.6 ソース数制限機能の設定 689
28.2.7 マルチキャストグループ数制限機能の設定 689
28.2.8 マルチキャストチャネル数制限機能の設定 689
28.2.9 マルチキャストチャネル受信者数制限機能の設定 690
28.2.10 帯域管理機能の設定 690
28.3 ホストトラッキング機能の解説 691
28.3.1 概要 691
28.3.2 注意事項 691
28.4 ホストトラッキング機能のコンフィグレーション 692
28.4.1 コンフィグレーションコマンド一覧 692
28.4.2 ホストトラッキング機能の設定 692
28.5 IPv6 マルチキャスト拡張機能のオペレーション 693
28.5.1 運用コマンド一覧 693
28.5.2 マルチキャストチャネルフィルタの統計情報の確認 693
28.5.3 帯域管理情報の確認 693
28.5.4 ホストトラッキング機能の受信者情報の確認 694

29 マルチキャスト経路フィルタリング 695
29.1 解説 696
29.1.1 マルチキャスト経路フィルタリング概説 696
29.1.2 マルチキャストフィルタ方法 697
29.1.3 マルチキャストエクストラネット 698
29.2 コンフィグレーション 700
29.2.1 コンフィグレーションコマンド一覧 700
29.2.2 IPv4 マルチキャストエクストラネットの設定 700
29.2.3 IPv6 マルチキャストエクストラネットの設定 703
29.3 オペレーション 707
29.3.1 運用コマンド一覧 707
29.3.2 マルチキャストエクストラネットの確認 707

第 4 編 ネットワーク経路監視機能

30 BFD 709
30.1 解説 710
30.1.1 概要 710
30.1.2 サポート機能一覧 710

30.1.3 BFD セッション 711
30.1.4 BFD による障害検出 713
30.1.5 マルチホップの監視 715
30.1.6 BFD とプロトコルの連携 716
30.1.7 BCU 二重化構成での動作 716
30.1.8 BFD 使用時の注意事項 717
30.2 コンフィグレーション 718
30.2.1 コンフィグレーションコマンド一覧 718
30.2.2 BFD の設定 718
30.2.3 スタティックルーティングのゲートウェイ監視の設定 719
30.2.4 OSPF および OSPFv3 の隣接ルータ監視の設定 719
30.2.5 BGP4 および BGP4+のピア監視の設定 719
30.3 オペレーション 721
30.3.1 運用コマンド一覧 721
30.3.2 BFD セッションの確認 721
30.3.3 プロトコルの確認 722

付録 725
付録 A 準拠規格 726
付録 A.1 IP・ARP・ICMP 726
付録 A.2 IPv6・NDP・ICMPv6 727
付録 A.3 uRPF 728
付録 A.4 RA 728
付録 A.5 DHCP/BOOTP リレーエージェント 728
付録 A.6 DHCPv6 リレーエージェント 729
付録 A.7 VRRP 729
付録 A.8 RIP 729
付録 A.9 RIPng 729
付録 A.10 OSPF 730
付録 A.11 OSPFv3 730
付録 A.12 BGP4 730
付録 A.13 BGP4+ 731
付録 A.14 IPv4 マルチキャスト 732
付録 A.15 IPv6 マルチキャスト 732
付録 A.16 BFD 733

索引 735

1 IP・ARP・ICMP の解説

IPv4 ネットワークには通信機能，IP パケット中継，経路制御機能があります。この章では，アドレッシングおよび IPv4 パケット中継について説明します。

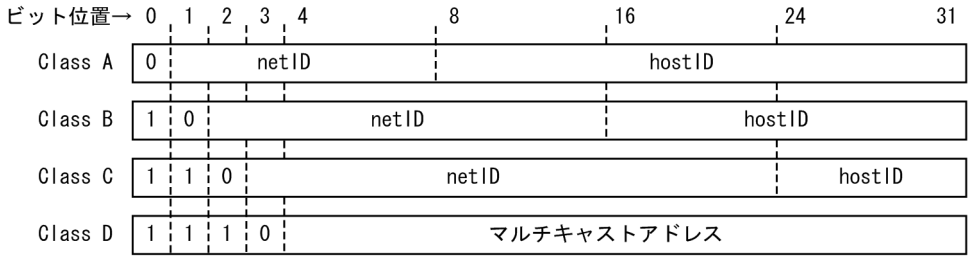
1.1　アドレッシング

本装置で使用する IP アドレスのアドレッシングについて概要を示します。

1.1.1　IP アドレス

本装置は IP アドレスの Class A，B，C，D をサポートします。Class D はルーティングプロトコルで使用します。使用するルーティングプロトコルによっては CIDR（Classless Inter-Domain Routing）で規定されているアドレスも使用できます。IP アドレスフォーマットを次の図に示します。

図 1-1　IP アドレスフォーマット



なお，ネットワークブロードキャストアドレスおよびサブネットワークブロードキャストアドレスは，host ID が 2 進数ですべて 1 またはすべて 0 の 2 種類をサポートしていて，その選択はインタフェース単位にコンフィグレーションで指定できます。インタフェースについては「1.2.2　IP アドレス付与単位」を参照してください。

本装置に付与する IP アドレスとして次に示す IP アドレスを使用できます。

- net ID
  net ID は次の範囲の値を使用できます。
  - Class A：1.x.x.x～126.x.x.x
  - Class B：128.1.x.x～191.254.x.x
  - Class C：192.0.1.x～223.255.254.x　（x = host ID）
- host ID
  host ID は次の範囲の値を使用できます。
  - Class A：y.0.0.1～y.255.255.254
  - Class B：y.y.0.1～y.y.255.254
  - Class C：y.y.y.1～y.y.y.254　（y = net ID）

1.1.2　サブネットマスク

「図 1-1　IP アドレスフォーマット」に示す Class A，B，C の net ID，host ID の境界位置に関係なく，サブネットマスクを使用して任意の境界位置に net ID と host ID の境界位置を指定できます。

例えば，Class B の net ID を一つ入手して，それを 256 個のサブネットに分割して使用する場合は，サブネットマスクを 255.255.255.0 とします。また，CIDR に対応した使い方として Class C の連続した二つの net ID（例えば，192.0.0.x と 192.0.1.x）を入手して，それを一つのサブネットワークとして使用する場合は，サブネットマスクを 255.255.254.0 とします。

サブネットマスクはインタフェースごとにコンフィグレーションで左詰め（2 進数表現で上位の桁から“1”が連続）で指定します。

例えば，サブネットマスクに 255.255.192.0 は設定できますが，255.255.96.0 は設定できません。

サブネットマスクに 255.255.255.254 を指定した IP アドレスを設定できます。その場合，hostID 部のビットをすべて 1 または 0 としたアドレスは，サブネットブロードキャストアドレスではなくホストの IP アドレスとして通信に使用できます。

1.2　IP レイヤ機能

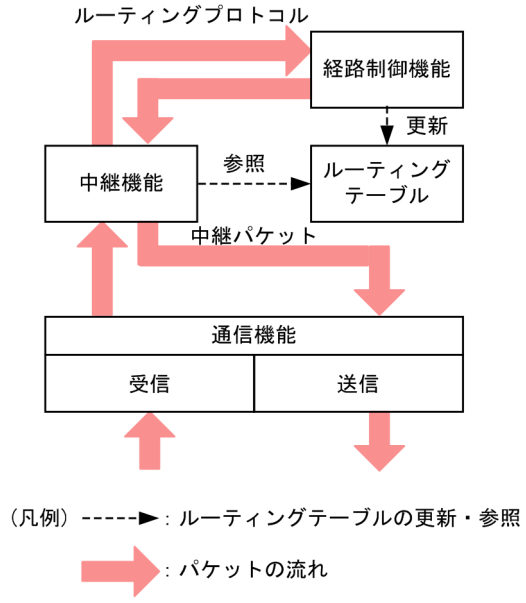
1.2.1　中継機能

本装置は受信した IP パケットをルーティングテーブルに従って中継します。この中継処理は大きく分けて次の三つの機能から構成されています。

- 通信機能
  IP レイヤの送信および受信処理をする機能です。
- 中継機能
  ルーティングテーブルに従って IP パケットを中継する機能です。
- 経路制御機能
  経路情報の送受信や，中継経路を決定してルーティングテーブルを作成する機能です。

IPv4 ルーティング機能の概要を次の図に示します。

図 1-2　IPv4 ルーティング機能の概要



1.2.2　IP アドレス付与単位

本装置ではインタフェースに対して IP アドレスを設定します。一つのインタフェースに複数の IP アドレスを設定するマルチホーム接続もできます。ネットワークへの接続形態は，ブロードキャスト型です。

1.3　通信機能

この節では，IPv4 で使用する通信プロトコルについて説明します。IPv4 で使用する通信プロトコルには次に示すものがあります。

- IP
- ICMP
- ARP

1.3.1　インターネットプロトコル（IP）

(1)　IP パケットフォーマット

本装置が送信する IP パケットのフォーマットおよび設定値は RFC791，RFC2474，RFC3168 に従います。

(2)　IP パケットヘッダ有効性チェック

IP パケット受信時に IP パケットヘッダの有効性をチェックします。IP パケットヘッダのチェック内容を次の表に示します。

表 1-1　IP パケットヘッダのチェック内容

IP パケット ヘッダフィールド	チェック内容	チェック異常時 パケット廃棄	パケット廃棄時 ICMP 送信
バージョン	バージョン＝４であること	○	×
ヘッダ長	ヘッダ長≧5 であること	○	×
TOS	チェックしない	－	－
全長	全長≧4×ヘッダ長であること パケット長（L3 ヘッダ先頭～FCS 直前までの長さ）≧全長であること	○	×
パケット識別子	チェックしない	－	－
フラグ	チェックしない	－	－
フラグメントオフセット	チェックしない	－	－
TTL	自装置宛てに受信したパケットの TTL： チェックしない	－	－
	中継するパケットの TTL： TTL－1 ＞ 0 であること	○	○※
プロトコル	チェックしない	－	－
ヘッダチェックサム	ヘッダチェックサムが正しいこと	○	×
送信元アドレス	次の条件をすべて満たすこと • クラス D アドレスではないこと	○	×

IP パケット ヘッダフィールド	チェック内容	チェック異常時 パケット廃棄	パケット廃棄時 ICMP 送信
	• クラス E アドレスではないこと • ネットワーク番号が 127（内部ループバックアドレス）ではないこと		
宛先アドレス	次の条件をすべて満たすこと • クラス A，クラス B，クラス C，クラス D アドレスであること • ネットワーク番号が 127（内部ループバックアドレス）ではないこと • ネットワーク番号が 0 ではないこと（ただし，0.0.0.0 を除く）	○	×

（凡例）　○：する　×：しない　－：該当しない

注※　ICMP Time Exceeded メッセージを送信します。

(3)　IP オプションサポート仕様

本装置がサポートする IP オプションを次の表に示します。

表 1-2　IP オプションサポート仕様

IP オプション	IP パケットの分類		
	本装置が発局のパケット	本装置が着局のパケット	本装置が中継するパケット
End of Option List	○	－	－
No Operation	○	－	－
Loose Source Routing	○	○	○
Strict Source Routing	×	○	○
Record Route	○	○	○
Internet Timestamp	×	○	○

（凡例）　○：サポートする　×：サポートしない　－：オプション処理なし

(4)　送信元アドレス選択

受信パケットに対する応答パケットを送信する場合は，受信パケットの宛先アドレスを送信元アドレスとして使用します。それ以外の送信パケットは，送信するインタフェースのプライマリアドレスに指定されたアドレスを送信元アドレスとして使用します。ただし，プロトコルやコンフィグレーションによって送信元アドレスが規定されているときは，その IPv4 アドレスを使用します。

1.3.2　ICMP

(1)　ICMP メッセージフォーマット

本装置が送信する ICMP メッセージのフォーマットおよび設定値は RFC792，RFC950，RFC1122 に従います。

(2)　ICMP メッセージサポート仕様

ICMP メッセージのサポート仕様を次の表に示します。

表 1-3　ICMP メッセージサポート仕様

ICMP メッセージ（値は 10 進数）				サポート
タイプ（種別）	値	コード（詳細種別）	値	
Echo Reply	0	−	0	○
Destination Unreachable	3	Net Unreachable	0	○
		Host Unreachable	1	○
		Protocol Unreachable	2	○
		Port Unreachable	3	○
		Fragmentation Needed and DF Set	4	○
		Source Route Failed	5	○
		Destination Network Unknown	6	×
		Destination Host Unknown	7	×
		Source host isolated error	8	×
		The destination network is administratively prohibited	9	×
		The destination host is administratively prohibited	10	×
		Network Unreachable for Type of Service	11	×
		Host Unreachable for Type of Service	12	×
		Communication Administratively Prohibited	13	○
		Host Precedence Violation	14	×
		Precedence Cutoff in Effect	15	×
Source Quench	4	−	0	×
Redirect	5	Redirect Datagrams for the Network	0	×
		Redirect Datagrams for the Host	1	○
		Redirect Datagrams for the Type of Service and Network	2	×
		Redirect Datagrams for the Type of Service and Host	3	×
Alternate Host Address	6	Alternate Address for Host	0	×
Echo Request	8	−	−	○

ICMP メッセージ（値は 10 進数）				サポート
タイプ（種別）	値	コード（詳細種別）	値	
Router Advertisement Message	9	Normal Router Advertisement	0	×
Router Solicitation Message	10	−	−	×
Time Exceeded	11	Time to Live Exceeded in Transit	0	○
		Fragment Reassembly Time Exceeded	1	×
Parameter Problem	12	Pointer Indicates the Error	0	○
		Missing a Required Option	1	×
		Bad Length	2	×
Timestamp Request	13	−	0	×
Timestamp Reply	14	−	0	○※
Information Request	15	−	0	×
Information Reply	16	−	0	×
Address Mask Request	17	−	0	×
Address Mask Reply	18	−	0	○※

（凡例）　○：サポートする　×：サポートしない　−：該当しない

注※　Request メッセージを受信した場合は，Reply メッセージを返します。

(3)　ICMP Redirect の送信仕様

受信インタフェースと送信インタフェースが同一の中継パケットは，ハードウェアによって ICMP Redirect 送信可否判定が必要であると判断され，ソフトウェアによって可否が判定されます。ソフトウェアでは，次の条件を満たすときに ICMP Redirect のパケットを送信します。

- パケット送信元とネクストホップのルータが同一セグメントにある（受信 IP パケットの送信元 IP アドレスのサブネットワークアドレスと中継先ネクストホップアドレスのサブネットワークアドレスが同一）

  ただし，デフォルト経路に一致した中継は除く
- 受信パケットが ICMP 以外の IP パケット
- コンフィグレーションの IP ルーティング情報で送信有効を指定している

(4)　ICMP Time Exceeded の送信仕様

次の条件を満たすときに ICMP Time Exceeded のパケットを送信します。

- 中継する受信 IP パケットの TTL が 1 以下
- 受信パケットが ICMP 以外の IP パケット（ただし，ICMP Echo パケットは除く）

1.3.3　ARP

(1)　ARP パケットフォーマット

本装置が送信する ARP パケットのフォーマットおよび設定値は RFC826，RFC5227 に従います。

(2)　ARP パケット有効性チェック

本装置は，受信した ARP パケットの有効性をチェックします。ARP パケットのチェック内容を次の表に示します。

表 1-4　ARP パケットのチェック内容

ARP パケットフィールド	チェック内容	チェック異常時パケット廃棄
ハードウェアタイプ	ハードウェアタイプ＝ 1（Ethernet）	○
プロトコルタイプ	プロトコル＝ 0800H（IP）であること 1000H（Trailer packet）であること※	○
ハードウェアアドレス長	6 であること	○
プロトコルアドレス長	4 であること	○
オペレーションコード	オペレーションコード＝ 1（REQUEST），1 以外は 2（REPLY）として扱う	－
送信元ハードウェアアドレス	以下の値ではないこと • 自装置ハードウェアアドレスと同じ	○
送信元プロトコルアドレス	以下のどちらかであること • ユニキャストアドレス • 0.0.0.0	○
宛先ハードウェアアドレス	チェックしない	－
宛先プロトコルアドレス	以下の値ではないこと • 0.0.0.0	○

（凡例）　○：廃棄する　－：該当しない

注※

Trailer packet の自発送信はしませんが，要求があった場合は応答を返して学習します。

(3)　ARP 受信時の動作

本装置は受信した ARP パケットに基づいて，新規 ARP エントリを学習したり，学習済み ARP エントリを更新したりします。また，必要に応じて ARP パケットを応答します。ARP 受信時の動作を次の表に示します。

表 1-5　ARP 受信時の動作

ARP 種別	宛先プロトコルアドレス	送信元プロトコルアドレス	ARP 応答	新規 ARP 学習	ARP 更新
ARP Request	自装置のアドレス	0.0.0.0 自装置のアドレス	○	－	－

ARP 種別	宛先プロトコルアドレス	送信元プロトコルアドレス	ARP 応答	新規 ARP 学習	ARP 更新
		その他	○	○	○
	その他	自装置のアドレス	○	−	−
		その他	−	−	−
ARP Reply	自装置のアドレス	自装置のアドレス	−	−	−
		その他	−	○	○
	その他	自装置のアドレス	−	−	−
		その他	−	−	○※

（凡例）　○：動作する　−：動作しない

注※　ARP Reply がブロードキャストまたはマルチキャストの場合

(4)　ProxyARP

ProxyARP 動作の有無はコンフィグレーションで設定します。本装置は次の条件をすべて満たす ARP 要求パケットを受信した場合に，宛先プロトコルアドレスの代理として ARP 応答パケットを送信します。

- ARP 要求パケットの宛先プロトコルアドレスがブロードキャストアドレスではない
- ARP 要求パケットの送信元プロトコルアドレスと宛先プロトコルアドレスのサブネットワーク番号が異なる
- ARP 要求パケットの宛先プロトコルアドレスがルーティングテーブルにあり到達できる

(5)　ローカル ProxyARP

ローカル ProxyARP 動作の有無はコンフィグレーションで設定します。ProxyARP とローカル ProxyARP の違いを次に示します。

- ProxyARP は，主にルーティングをサポートしていない端末のために，ARP 受信インタフェースとは異なるインタフェースのサブネットワーク宛ての ARP 要求に代理応答します。
- ローカル ProxyARP は，受信インタフェースのサブネットワーク宛ての ARP 要求に代理応答します。

本機能は，セキュリティ上の理由などで端末同士が直接通信できないサブネットワークや，ブロードキャストが禁止されているサブネットワークで使用します。本装置単体でローカル ProxyARP が動作する環境を実現するには，アイソレート VLAN を設定しておく必要があります。本機能を使用すると，同一サブネットワーク上の端末同士の通信も本装置で中継することになります。なお，本機能によって ICMP リダイレクトが多発するため，ICMP リダイレクト機能を無効にすることを推奨します。

本装置は，次の条件をすべて満たす ARP 要求パケットを受信した場合に，宛先プロトコルアドレスの代理として ARP 応答パケットを送信します。

- ARP 要求パケットの宛先プロトコルアドレスがブロードキャストアドレスではない
- ARP 要求パケットの宛先プロトコルアドレスのサブネットワークが, 受信インタフェースのサブネットワークと等しい
- 送信元プロトコルアドレスと宛先プロトコルアドレスが同一ではない

(6)　エージングタイマ

ARP 情報のエージング時間はインタフェースごとに分単位で指定できます。指定値は最小 1 分で最大 24 時間です。また，デフォルト値は 4 時間です。

(7)　ARP 情報の設定

ARP プロトコルを持たない製品を接続するために，MAC アドレスと IP アドレスの対応（ARP 情報）をコンフィグレーションコマンド arp で設定できます。

(8)　ARP 情報の参照

運用端末から運用コマンド show ip arp で ARP 情報が参照できます。ARP 情報から該当するインタフェースの IP アドレスと MAC アドレスの対応がわかります。

1.3.4　Address Conflict Detection

Address Conflict Detection は RFC5227 に従って，隣接ネットワーク上に競合する IPv4 アドレスを持つ装置が存在しないかどうかを確認する機能です。デフォルトでは本機能は無効です。本機能を有効にするには，コンフィグレーションコマンド ip conflict-detection を実行してください。

アドレスが重複すると，その IPv4 アドレスでは通信および中継できません。

1.4　中継機能

1.4.1　IP パケットの中継方法

中継機能は，受信したパケットをルーティングテーブルに従って次のルータまたはホストに転送する機能です。

(1)　ルーティングテーブルの内容

ルーティングテーブルは複数個のエントリから構成されていて，各エントリは次の内容を含んでいます。本装置のルーティングテーブルの内容は運用コマンド show ip route で表示できます。

Destination

宛先ネットワークアドレスと宛先ネットワークアドレスに対するサブネットマスクのビット長です。サブネットマスクは，ルーティングテーブル検索時，受信 IP パケットの宛先 IP アドレスに対するマスクになります。サブネットワークに分割されていない宛先ネットワークアドレスについては，そのネットワークアドレスのネットワーククラスに対応したマスクビット長（例えば，Class A なら 8）を表示します。なお，ホストアドレスによって中継する場合には 32 を表示します。

Next Hop

次に中継する必要のあるルータの IP アドレスです。マルチパス機能を使用すると，複数個の Next Hop が存在します。

Interface

Next Hop のあるインタフェース名です。

Metric

ルートのメトリックです。

Protocol

学習元プロトコルです。

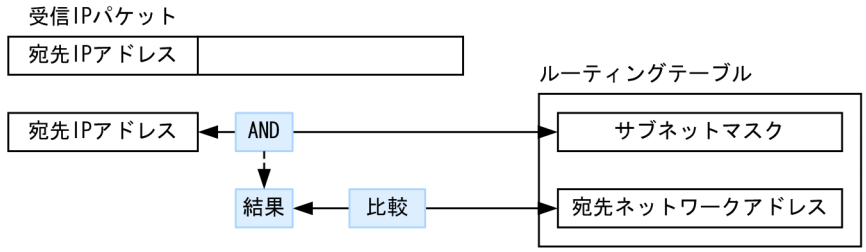
Age

ルートが確認，または変更されてからの時間（秒）です。

(2)　ルーティングテーブルの検索

受信した IP パケットの宛先 IP アドレスに該当するエントリをルーティングテーブルから検索します。該当するエントリとは，受信した IP パケットの宛先 IP アドレスをルーティングテーブルのサブネットマスクでマスク（AND）を取った結果が宛先ネットワークアドレスと同じ値になるものです。ルーティングテーブルの検索を次の図に示します。

図 1-3　ルーティングテーブルの検索

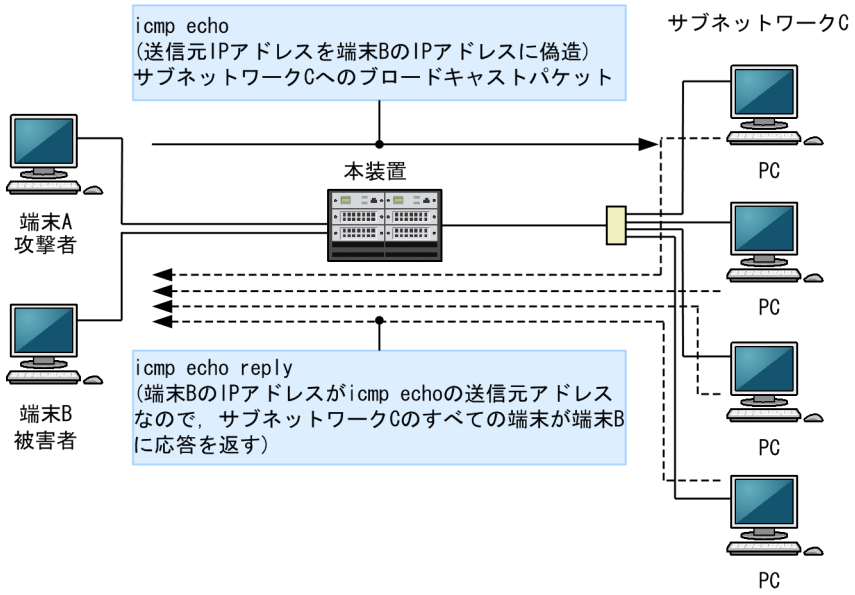


1.4.2　ブロードキャストパケットの中継方法

本装置では，IP 中継で直接接続するネットワークまたはサブネットワークのブロードキャスト（以降，ダイレクトブロードキャスト）パケットを中継するかどうかをコンフィグレーションで設定できます。コンフィグレーションコマンド ip subnet-broadcast で，受信側のインタフェースの動作を設定します。また，コンフィグレーションコマンド ip address の directed-broadcast パラメータで，送信側のインタフェースの動作をサブネットごとに設定します。

コンフィグレーションを設定しないデフォルトの状態では，ダイレクトブロードキャストを中継しませんが，中継を指定した場合は，次の図のような端末への攻撃が考えられるため注意が必要です。

図 1-4　サブネットワークへのブロードキャストパケットを使った攻撃例



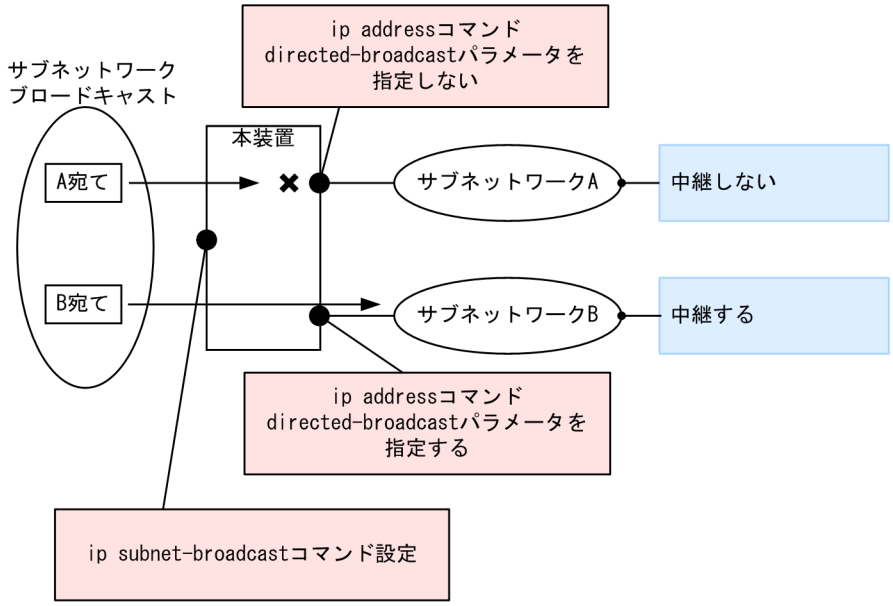
ip subnet-broadcast コマンドが設定され，かつ ip address コマンドの directed-broadcast パラメータが指定された場合に，ダイレクトブロードキャストパケットを中継します。これらのコマンドおよびパラメータの設定と動作の関係を次の表に示します。また，これらのコマンドの設定例を次の図に示します。

表 1-6　コマンド設定内容と動作

ip subnet-broadcast コマンド	ip address コマンド	
	directed-broadcast 指定	directed-broadcast 指定しない
デフォルトおよび ip subnet-broadcast 設定時	○	×
no ip subnet-broadcast 設定時	×	×

（凡例）　○：中継する　×：中継しない

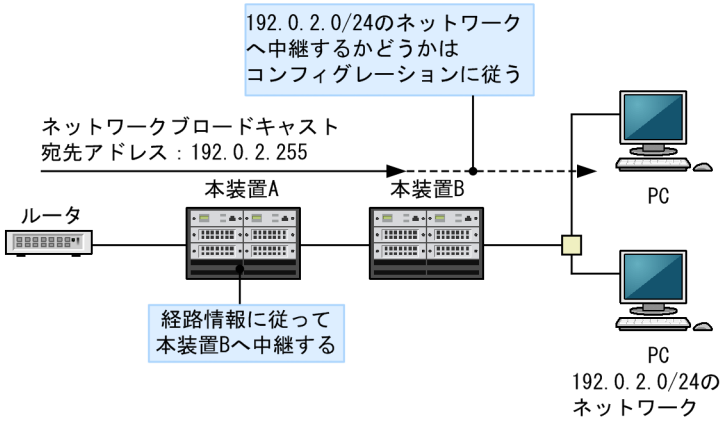
図 1-5　コマンド設定例



(1)　ネットワークブロードキャスト

ネットワークブロードキャストとは，サブネットワーク化されていないネットワークに対するブロードキャストです。例えば，192.0.2.0/24 のネットワークに対して 192.0.2.255 を宛先とするネットワークブロードキャストの IP パケットが送信された場合，本装置が 192.0.2.0/24 のネットワークと直接接続しているときはコンフィグレーションのブロードキャストを中継するかどうかの設定に従って，ネットワークブロードキャストの IP パケットを自装置配下へ中継するかどうかを判断します。ネットワークブロードキャストを次の図に示します。

図 1-6　ネットワークブロードキャスト



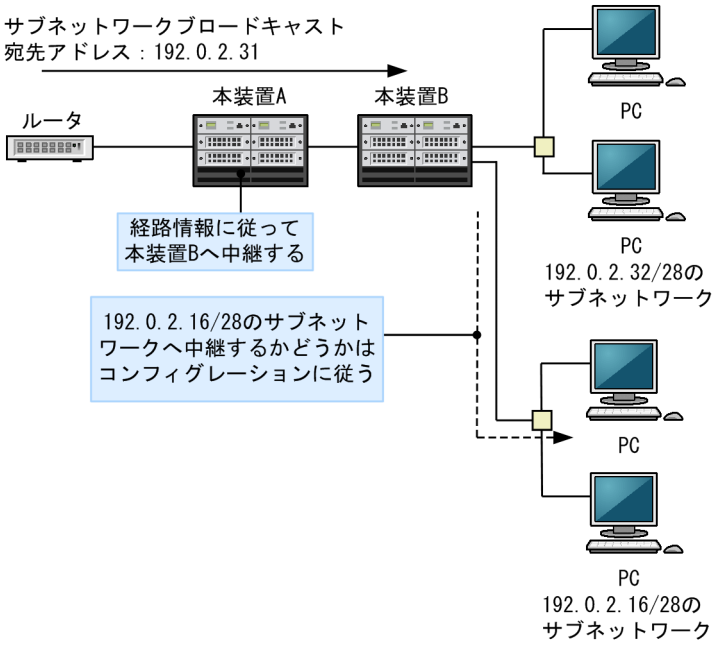
(2)　サブネットワークブロードキャスト

サブネットワークブロードキャストとは，サブネットワーク化されたネットワークに対するブロードキャストです。

例えば，192.0.2.0/24 のネットワークをサブネットワーク化して，192.0.2.16/28，192.0.2.32/28 の二つのサブネットワークに分割して使用している場合に，192.0.2.31 を宛先とするサブネットワークブロードキャスト（サブネットワーク 192.0.2.16/28 へのブロードキャスト）の IP パケットが送信された場合，

本装置が 192.0.2.16/28 のサブネットワークと直接接続しているときはコンフィグレーションのブロードキャストを中継するかどうかの設定に従って，サブネットワークブロードキャストの IP パケットを自装置配下へ中継するかどうかを判断します。サブネットワークブロードキャストを次の図に示します。

図 1-7　サブネットワークブロードキャスト

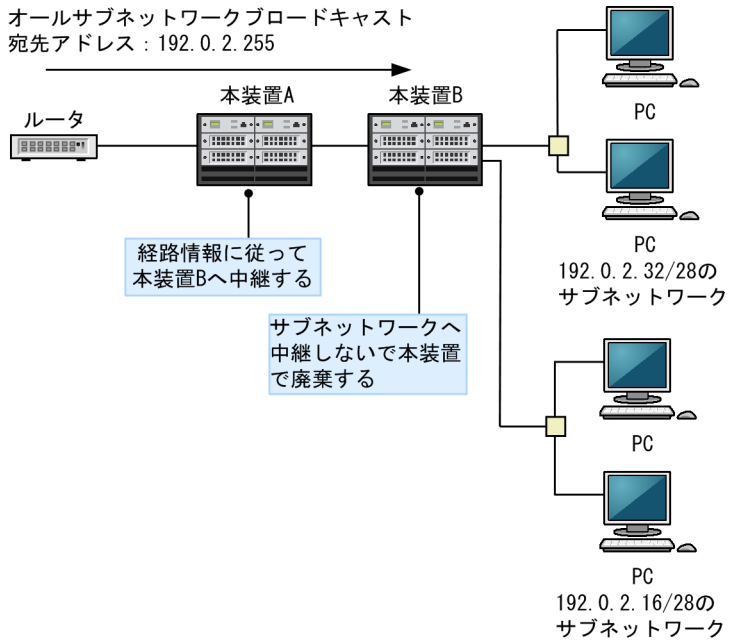


(3)　オールサブネットワークブロードキャスト

オールサブネットワークブロードキャストとは，サブネットワーク化されたすべてのネットワークに対するブロードキャストです。本装置では，オールサブネットワークブロードキャストを通常の経路として扱います。

例えば，192.0.2.0/24 のネットワークをサブネットワーク化して，192.0.2.16/28 と 192.0.2.32/28 の二つのサブネットワークに分割して使用している場合に，192.0.2.255 を宛先とするオールサブネットワークブロードキャストの IP パケットが送信された場合，192.0.2.16/28 と 192.0.2.32/28 のサブネットワークを直接接続する本装置までは該当パケットが届きますが，本装置配下の 192.0.2.16/28 と 192.0.2.32/28 のサブネットワークへは中継しないで本装置で該当パケットを廃棄します。なお，デフォルト経路などほかに一致する経路がある場合，その経路を使用して IP パケットが送信されます。オールサブネットワークブロードキャストを次の図に示します。

図 1-8　オールサブネットワークブロードキャスト



1.4.3　MTU とフラグメント

IP パケットを中継するとき，最大転送単位（MTU：Maximum Transfer Unit）に従って，それ以上大きなパケットは分割して送信します。これを**フラグメント化**といいます。MTU のサイズに収まるパケットはハードウェア処理で中継しますが，分割して送信する場合はソフトウェア処理で中継するため中継パフォーマンスが低下しますので注意が必要です。

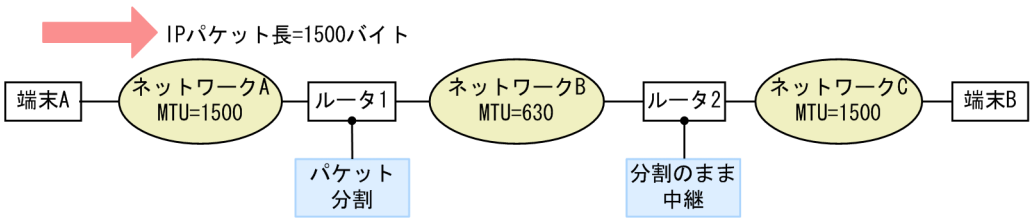
IP インタフェースで使用する MTU については，「コンフィグレーションガイド Vol.1　20.1.4 IP インタフェース動作仕様」を参照してください。

(1)　MTU とフラグメント

ネットワークの中には異なる MTU のサブネットワークがある可能性があります。サイズの大きな IP パケットが小さな MTU を持つネットワークを経由する場合，IP パケットを分割して中継します。

フラグメント化モデルを次の図に示します。ネットワーク A から送信したパケットをネットワーク B へ中継するとき，MTU が 1500 から 630 に小さくなるためフラグメント化します。

図 1-9　フラグメント化モデル

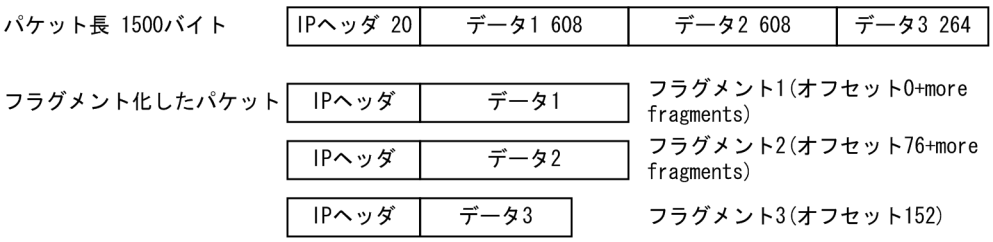


(2)　フラグメントの生成

MTU を超える IP パケットは，IP ヘッダを除くデータ部分を 8 の倍数長でフラグメント化します。

ネットワーク B は MTU が 630 なため，IP ヘッダ長を除くと 610 となります。610 での 8 の倍数長は 608 なため，608 バイトずつフラグメント化します。フラグメント化したパケットにはそれぞれ IP ヘッダを付けます。パケットのフラグメント化を次の図に示します。

図 1-10　パケットのフラグメント化



MTU に収まるようにフラグメント化した IP パケットは，フラグメント化したことを IP ヘッダ内のフラグメントオフセットと more fragments フラグに書き込みます。また，同一のパケット識別子を設定して checksum を再計算します。フラグメントオフセットには，先頭からのデータ長を 8 で割った値を設定します。

(3)　フラグメントの再構成

フラグメント化された IP パケットは，終端で IP ヘッダ内のパケット識別子，フラグメントオフセット，および more fragments フラグを基に再構成します。途中のルータでは再構成しません。それは，終端までの中継で各フラグメントを独立して経路制御させることを前提としているため，仮に途中のルータがフラグメントを蓄積して再構成しようとした場合，そのルータを通過しなかったフラグメントがあると，蓄積していたフラグメントを破棄することになるためです。

1.5　ループバックインタフェース

ループバックインタフェースは物理回線に依存しない仮想的なインタフェースで，IPv4 アドレスを設定できます。ループバックインタフェースに設定した IPv4 アドレスは，各運用機能の送信元アドレスやルーティングプロトコルで使用します。

グローバルネットワークおよび任意の VRF には，複数のループバックインタフェースを設定できます。装置の送信元アドレスとして自動選択するループバックインタフェースの IPv4 アドレスは一つだけですが，コンフィグレーションによって特定の運用機能の送信元アドレスなどに設定できます。

1.6　IPv4 使用時の注意事項

(1)　マルチホーム構成時の注意事項

インタフェースに複数の IPv4 アドレスを設定する場合，該当インタフェースと同一のブロードキャストドメインに接続された端末間で異なるサブネットアドレスを使用して通信すると，本装置を経由した IPv4 中継が発生することがあります。

この際，ICMP Redirect の送信可否判定をするため，ハードウェアによってパケットがソフトウェアに中継されて，本装置の CPU が高負荷となるおそれがあります。そのため，次の点に注意してください。

- 同一ブロードキャストドメイン内で端末同士が直接通信してもよい場合は，すべての端末のサブネットをそろえてください。
- セキュリティ上の理由などで，同一ブロードキャストドメイン内の端末のサブネットを分ける場合は，CPU の高負荷を防止するため，コンフィグレーションコマンドでハードウェアによる ICMP Redirect の送信可否判定を停止することをお勧めします。

2 IP・ARP・ICMP の設定と運用

この章では，IPv4 ネットワークのコンフィグレーションの設定方法および状態の確認方法について説明します。

2.1　コンフィグレーション

2.1.1　コンフィグレーションコマンド一覧

IPv4 コンフィグレーションコマンド一覧を次の表に示します。

表 2-1　コンフィグレーションコマンド一覧

コマンド名	説明
arp	スタティック ARP テーブルを作成します。
arp dynamic-limit	インタフェースで学習できる ARP エントリ数を指定します。
arp max-send-count	ARP 要求パケットの最大送信回数を指定します。
arp send-interval	ARP 要求パケットの送信リトライ間隔を指定します。
arp timeout	ARP キャッシュテーブルエージング時間を指定します。
ip address	インタフェースの IPv4 アドレスを指定します。
ip conflict-detection	インタフェースの IPv4 アドレスの重複を検出する Address Conflict Detection の使用可否を指定します。
ip icmp rate-limit unreachable	ICMP エラーの送信間隔を指定します。
ip local-proxy-arp	ローカル Proxy ARP 応答可否を指定します。
ip mtu	インタフェースでの送信 IP MTU 長を指定します。
ip proxy-arp	ARP 代理応答可否を指定します。
ip redirects	ICMP リダイレクトメッセージの送信可否を指定します。
ip source-route	ソースルートオプション付き IPv4 パケット中継可否を指定します。
ip subnet-broadcast	サブネットブロードキャストの IPv4 パケット中継可否を指定します。ブロードキャストパケットの中継については，ip address コマンドの directed-broadcast パラメータと合わせて設定する必要があります。
system-source-address※	ループバックインタフェースのアドレスを装置の送信元アドレスとして自動選択しないように指定します。

注※

「コンフィグレーションコマンドレファレンス Vol.3　4. ループバックインタフェース」を参照してください。

2.1.2　インタフェースの設定

[設定のポイント]

インタフェースに IPv4 アドレスを設定します。IPv4 アドレスを設定するには，インタフェースのコンフィグレーションモードに移行する必要があります。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**

ポート 1/1 のコンフィグレーションモードに移行します。

2. **(config-if)# ip address 192.0.2.1 255.255.255.0**

   ポート 1/1 のインタフェースに IPv4 アドレス 192.0.2.1，サブネットマスク 255.255.255.0 を設定します。

2.1.3　マルチホームの設定

[設定のポイント]

インタフェースに複数の IPv4 アドレスを設定します。二つ目以降の IPv4 アドレスには secondary パラメータを指定する必要があります。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**

   ポート 1/1 のコンフィグレーションモードに移行します。

2. **(config-if)# ip address 192.0.2.1 255.255.255.0**

   ポート 1/1 のインタフェースにプライマリ IPv4 アドレス 192.0.2.1，サブネットマスク 255.255.255.0 を設定します。

3. **(config-if)# ip address 198.51.100.1 255.255.255.0 secondary**

   ポート 1/1 のインタフェースにセカンダリ IPv4 アドレス 198.51.100.1，サブネットマスク 255.255.255.0 を設定します。

2.1.4　ダイレクトブロードキャスト中継の設定

[設定のポイント]

ダイレクトブロードキャスト中継を有効にする場合，ip address コマンドの directed-broadcast パラメータを有効にする必要があります。no ip subnet-broadcast コマンドでサブネットブロードキャストパケット中継を抑止している場合は，ip subnet-broadcast コマンドを実行して有効にしてください。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**

   ポート 1/1 のコンフィグレーションモードに移行します。

2. **(config-if)# ip subnet-broadcast**

   サブネットブロードキャストパケット中継オプションを有効にします（本設定は，no ip subnet-broadcast を以前に実行した場合だけ必要です）。

3. **(config-if)# ip address 192.0.2.1 255.255.255.0 directed-broadcast**

   ポート 1/1 のインタフェースにプライマリ IPv4 アドレス 192.0.2.1，サブネットマスク 255.255.255.0，ダイレクトブロードキャストの IPv4 パケット中継を設定します。

2.1.5　ループバックインタフェースの設定

[設定のポイント]

装置を識別するための IPv4 アドレスを設定します。インタフェース番号 0 はグローバルネットワーク専用です。設定できるアドレスは一つだけです。

[コマンドによる設定]

1. **(config)# interface loopback 0**

ループバックインタフェースのコンフィグレーションモードに移行します。

2. **(config-if)# ip address 192.0.2.1**
ループバックインタフェースに IPv4 アドレス 192.0.2.1 を設定します。

2.1.6　複数のループバックインタフェースの設定

[設定のポイント]

ループバックインタフェースを複数設定するには，装置の送信元アドレスとして自動選択されないように設定したあと，IP アドレスを設定します。

[コマンドによる設定]

1. **(config)# interface loopback 0**
ループバックインタフェースのコンフィグレーションモードに移行します。
2. **(config-if)# ip address 192.0.2.1**
ループバックインタフェースに IPv4 アドレス 192.0.2.1 を設定します。
3. **(config)# interface loopback 1**
ループバックインタフェース 1 のコンフィグレーションモードに移行します。
4. **(config-if)# no system-source-address**
装置の送信元アドレスとして自動選択しない設定をします。
5. **(config-if)# ip address 192.0.2.2**
ループバックインタフェース 1 に IPv4 アドレス 192.0.2.2 を設定します。

2.1.7　スタティック ARP の設定

[設定のポイント]

本装置にスタティック ARP を設定します。インタフェースを指定する必要があります。

[コマンドによる設定]

1. **(config)# arp 192.0.2.2 interface gigabitethernet 1/1 0012.e240.0a00**
ポート 1/1 のインタフェースにネクストホップ IPv4 アドレス 192.0.2.2，接続先 MAC アドレス 0012.e240.0a00 でスタティック ARP を設定します。

2.2　オペレーション

2.2.1　運用コマンド一覧

IP・ARP・ICMP の運用コマンド一覧を次の表に示します。

表 2-2　運用コマンド一覧

コマンド名	説明
show ip-dual interface	IPv4 および IPv6 インタフェースの状態を表示します。
show ip interface	IPv4 インタフェースの状態を表示します。
clear ip interface statistics	IP インタフェースの IPv4 統計情報を 0 クリアします。
show ip arp	ARP エントリ情報を表示します。
clear arp-cache	ダイナミック ARP 情報を削除します。
clear ip duplicate-address	Address Conflict Detection によって重複が検出されたアドレスの通信の抑止状態を解除します。
show netstat (netstat)	ネットワークのステータスを表示します。
clear netstat	ネットワーク統計情報カウンタをクリアします。
show tcpdump (tcpdump)	BCU-CPU で送受信されるパケットをモニタします。
show tcp ha connections	TCP 高可用対象コネクションの状態を表示します。
clear tcp	TCP コネクションを切断します。
ping	エコーテストを行います。
traceroute	経由ルートを表示します。

2.2.2　IPv4 インタフェースの up/down 確認

IPv4 ネットワークに接続する本装置の回線や回線内のポートに IPv4 アドレスを設定したあとに，show ip interface コマンドを実行して，IPv4 インタフェースの up/down 状態が「UP」であることを確認してください。

図 2-1　show ip interface コマンドの実行結果

```
> show ip interface summary
Date 20XX/03/25 12:00:00 UTC
Eth1/1: UP 192.0.2.1/24
Eth1/2: UP 198.51.100.1/24
>
```

2.2.3　宛先アドレスとの通信可否の確認

IPv4 ネットワークに接続している本装置のインタフェースについて，ping コマンドを実行して通信相手となる装置に対して通信できることを確認してください。

図 2-2　ping コマンドの実行結果（通信可の場合）

```
> ping 198.51.100.51
Date 20XX/03/25 12:00:00 UTC
```

```
PING 198.51.100.51 (198.51.100.51): 56 data bytes
64 bytes from 198.51.100.51: icmp_seq=0 ttl=255 time=0.286 ms
64 bytes from 198.51.100.51: icmp_seq=1 ttl=255 time=0.271 ms
64 bytes from 198.51.100.51: icmp_seq=2 ttl=255 time=0.266 ms
^C
--- 198.51.100.51 PING Statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max = 0.266/0.274/0.286 ms
>
```

図 2-3　ping コマンドの実行結果（通信不可の場合）

```
> ping 192.0.2.2
Date 20XX/03/25 12:00:00 UTC
PING 192.0.2.2 (192.0.2.2): 56 data bytes
^C
--- 192.0.2.2 PING Statistics ---
3 packets transmitted, 0 packets received, 100.0% packet loss
>
```

2.2.4　宛先アドレスまでの経路確認

traceroute コマンドを実行して，IPv4 ネットワークに接続している本装置のインタフェースから通信相手となる装置までの中継装置を確認してください。

図 2-4　traceroute コマンドの実行結果

```
> traceroute 203.0.113.101 numeric
Date 20XX/03/25 12:00:00 UTC
traceroute to 203.0.113.101 (203.0.113.101), 30 hops max, 40 byte packets
1  192.0.2.2  0.612 ms  0.541 ms  0.532 ms
2  198.51.100.55  0.905 ms  0.816 ms  0.807 ms
3  203.0.113.101  1.325 ms  1.236 ms  1.227 ms
>
```

2.2.5　ARP 情報の確認

IPv4 ネットワークに接続する本装置の回線や回線内のポートに IPv4 アドレスを設定したあとに，show ip arp コマンドを実行して，本装置と隣接装置間のアドレス解決をしている（ARP エントリ情報がある）ことを確認してください。

図 2-5　show ip arp コマンドの実行結果

```
> show ip arp interface gigabitethernet 1/1
Date 20XX/03/25 12:00:00 UTC
Total: 3 entries
 IP Address    Linklayer Address  Netif      Expire    Type
 192.0.2.2     0012.e240.0a00     Eth1/1     Static    arpa
 192.0.2.3     0012.e240.0a01     Eth1/1     Static    arpa
 192.0.2.4     0012.e240.0a02     Eth1/1     3h30m0s   arpa
```

3 IPv6・NDP・ICMPv6 の解説

IPv6 ネットワークには通信機能，IP パケット中継，フィルタリング，ロードバランスなどいろいろな機能があります。この章では IPv6 パケット中継について説明します。

3.1　アドレッシング

IPv6 は IPv4 と比較して次のような特長があります。

- **アドレス構造を拡張している**
  アドレス長が 32 ビットから 128 ビットに拡張されています。そのため，ノードへ割り当てができるアドレス数がほぼ無限となり，IPv4 で問題となっていたアドレス枯渇問題が解消されます。また，アドレス構造階層のレベル数が増加したため，新しいアドレスを定義できるようになります。
- **ヘッダ形式を単純化している**
  IPv4 と比較してヘッダフィールドが簡略化され，プロトコル処理のオーバーヘッドが減少しています。
- **拡張ヘッダとオプションヘッダを強化している**
  転送効率の向上，オプションの長さ制限の緩和，また，オプション拡張が容易です。
- **フローラベルを設定できる**
  特定のトラフィックフローを識別するためのラベル付けができます。

本装置で使用する IPv6 ネットワークのアドレッシングについて概要を示します。

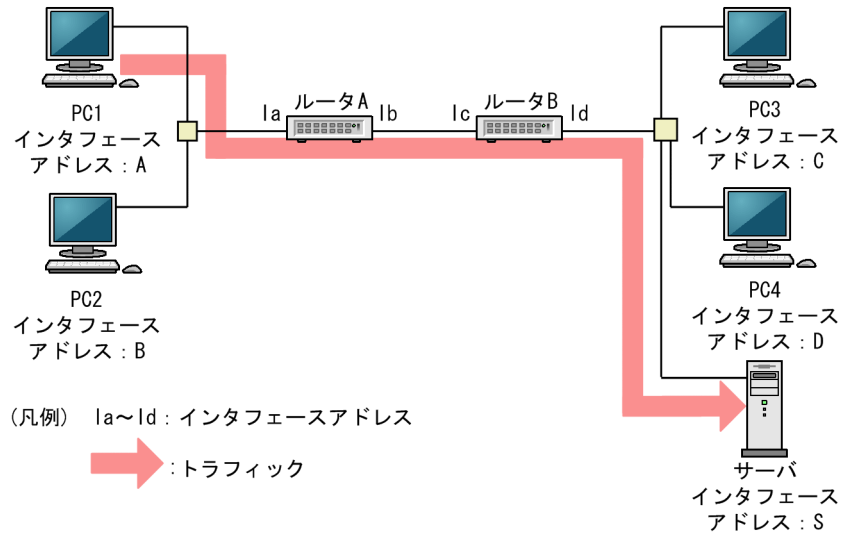
3.1.1　IPv6 アドレス

IPv6 アドレスにはユニキャスト，エニキャスト，マルチキャストの 3 種類のアドレス形式が定義されています。

(1)　ユニキャストアドレス

単一のインタフェースを示すアドレスです。終点アドレスがユニキャストアドレスのパケットは，そのアドレスが示すインタフェースに配送されます。ユニキャストアドレス通信を次の図に示します。

図 3-1　ユニキャストアドレス通信

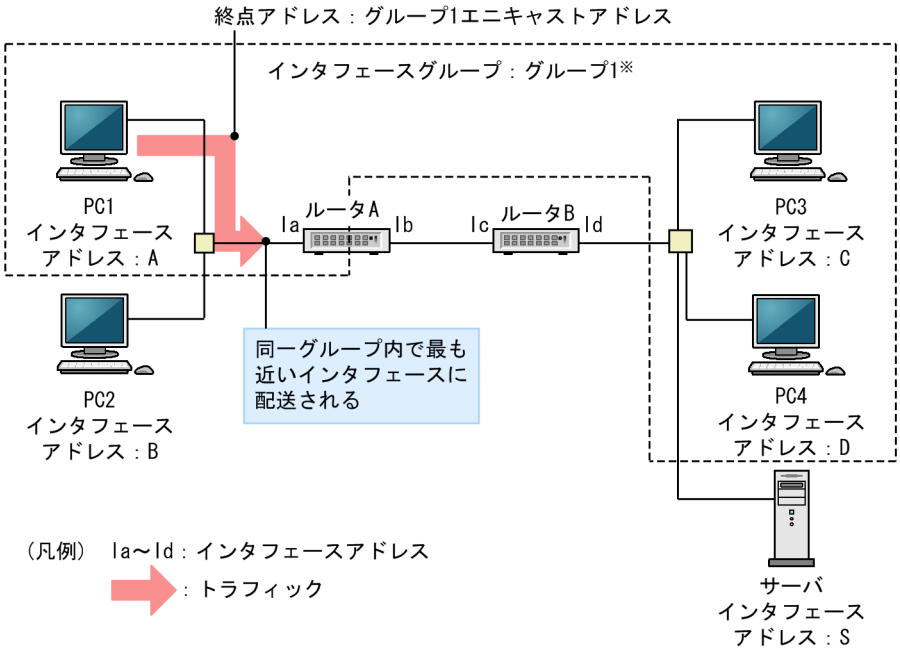


(2)　エニキャストアドレス

インタフェースの集合を示すアドレスです。終点アドレスがエニキャストアドレスのパケットは，インタフェースグループのうち，経路制御プロトコルによって測定された距離の最も近いインタフェースに配送さ

れます。なお，本装置ではエニキャストアドレスは未サポートです。エニキャストアドレス通信を次の図に示します。

図 3-2　エニキャストアドレス通信

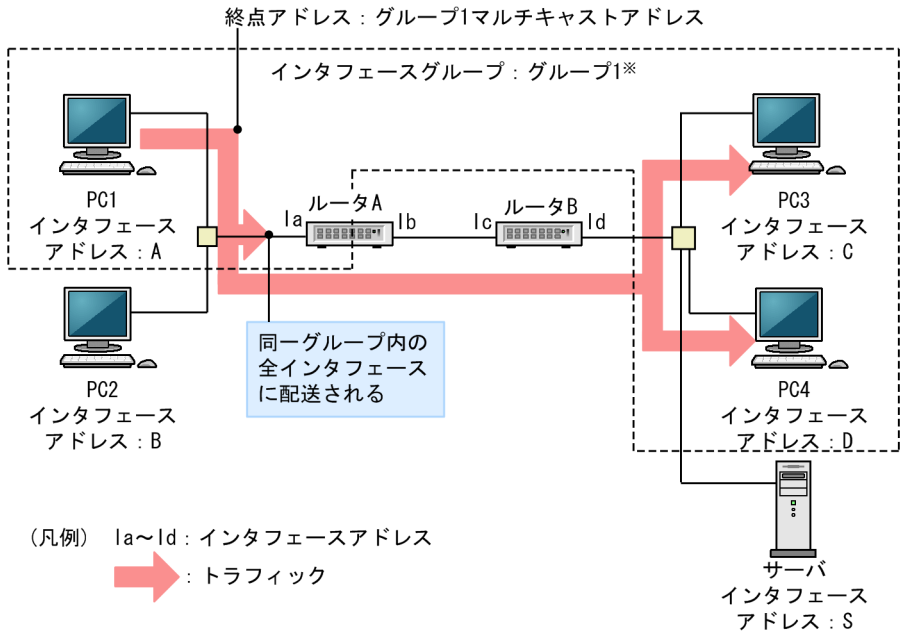


注※　グループ 1 にはインタフェースアドレス A，C，D，Ia が所属します。

(3)　マルチキャストアドレス

インタフェースの集合を示すアドレスです。終点アドレスがマルチキャストアドレスのパケットは，そのアドレスが示すインタフェースグループのすべてのインタフェースに配送されます。マルチキャストアドレス通信を次の図に示します。

図 3-3　マルチキャストアドレス通信



注※　グループ 1 にはインタフェースアドレス A，C，D，Ia が所属します。

3.1.2　アドレス表記方法

IPv6 のアドレスは 128 ビット長です。実際に表記するときの方法を次に示します。

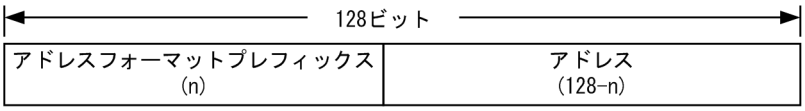
- 16 進数で 16 ビットごとにコロン（:）で区切った形式で表記します。
  （例）　2001:db8:0811:ff02:0000:08ff:fe8b:3090
- 16 進数の先頭にくる“0”は省略できます。
  （例）　2001:db8:811:ff02:0:8ff:fe8b:3090
- 連続する“0”は二つのコロン“::”に置換できます。ただし，“::”に置換できるのは一つのアドレス表記に 1 か所までと定義されています。
  （例）　次に示す IPv6 アドレスのときの置換方法
  fe80:0000:0000:0000:0000:0000:0000:3090　→　fe80::3090
  （例）　2 か所以上の“::”は禁止
  fe80:0000:0000:0000:0000:0000:0000:3090　→　fe80::0::3090
- 次に示す形式でアドレスとプレフィックス長を指定できます。
  - IPv6 アドレス/プレフィックス長
  - IPv6 アドレス prefixlen プレフィックス長

  プレフィックス長はアドレス左端から何ビットまでがプレフィックスかを 10 進数で指定します。

3.1.3　アドレスフォーマットプレフィックス

128 ビット長の IPv6 アドレスが複数のサブフィールドに分割されています。先頭ビットは IPv6 アドレスのタイプを識別する役割があり，アドレスフォーマットプレフィックスと呼ばれます。アドレスフォーマットプレフィックスを次の図に示します。

図 3-4　アドレスフォーマットプレフィックス



（　）内の数字はビット数を示す。

また，アドレスフォーマットプレフィックスの種類を次の表に示します。

表 3-1　アドレスフォーマットプレフィックスの種類

プレフィックス（2 進数）	割り当て
0000 0000	未割り当て
0000 0001	未割り当て
0000 001	未割り当て
0000 010	未割り当て
0000 011	未割り当て
0000 1	未割り当て
0001	未割り当て
001	集約可能グローバルユニキャストアドレス
010	未割り当て
011	未割り当て
100	未割り当て
101	未割り当て
110	未割り当て
1110	未割り当て
1111 0	未割り当て
1111 10	未割り当て
1111 110	ユニークローカルユニキャストアドレス
1111 1110 0	未割り当て
1111 1110 10	リンクローカルユニキャストアドレス
1111 1110 11	未割り当て
1111 1111	マルチキャストアドレス

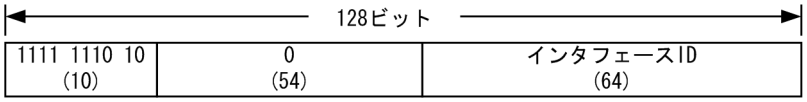
3.1.4　ユニキャストアドレス

(1)　リンクローカルアドレス

アドレスプレフィックスの上位 64 ビットが fe80::で，64 ビットのインタフェース ID 部を含むアドレスを**IPv6 リンクローカルアドレス**と呼びます。IPv6 リンクローカルアドレスは同一リンク内だけで有効なアドレスで，自動アドレス設定，近隣探索，またはルータが存在しないときに使用されます。パケットの始点または終点アドレスが IPv6 リンクローカルアドレスの場合，本装置はパケットをほかのリンクに転送しません。

本装置で IPv6 を使用するインタフェースには，IPv6 リンクローカルアドレスが必ず一つ設定されます。二つ以上は設定できません。IPv6 リンクローカルアドレスを次の図に示します。

図 3-5　IPv6 リンクローカルアドレス

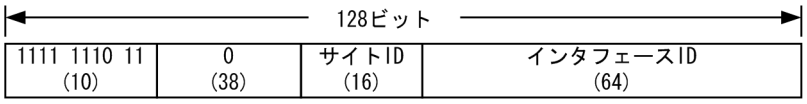


（　）内の数字はビット数を示す。

(2)　サイトローカルアドレス

アドレスプレフィックスの上位 10 ビットが 1111 1110 11 で，64 ビットのインタフェース ID 部を含むアドレスを**IPv6 サイトローカルアドレス**と呼びます。本装置は IPv6 サイトローカルアドレスを「(3)　グローバルアドレス」の IPv6 グローバルアドレスとして扱います。そのため，IPv6 サイトローカルアドレスをインタフェースに設定した場合は，IPv6 サイトローカルアドレス情報がサイト外に出ないようにルーティングやフィルタリングを設定してください。IPv6 サイトローカルアドレスを次の図に示します。なお，サイトローカルアドレスは RFC3879 で廃止されました。

図 3-6　IPv6 サイトローカルアドレス

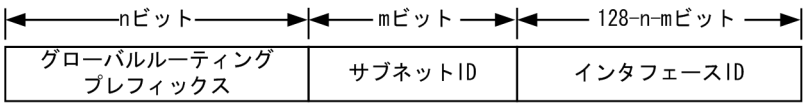


（　）内の数字はビット数を示す。

(3)　グローバルアドレス

アドレスプレフィックスの上位 3 ビットが 001 で始まるアドレスを**IPv6 グローバルアドレス**と呼びます。IPv6 グローバルアドレスは世界で一意なアドレスで，インターネットを経由して通信する場合に使用されます。パケットの始点アドレスが IPv6 グローバルアドレスの場合，経路情報に従ってパケットが転送されます。IPv6 グローバルアドレスを次の図に示します。

図 3-7　IPv6 グローバルアドレス

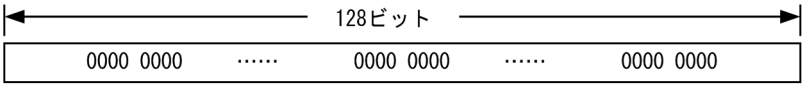


(4)　未指定アドレス

すべてのビットが 0 のアドレス 0:0:0:0:0:0:0:0（0::0，または::）は，**未指定アドレス**と定義されています。未指定アドレスはインタフェースにアドレスが存在しないことを表しています。これは，アドレスの割

り当てを受けていないノードの接続開始時などに使用されます。未指定アドレスはノードに対して意図的に割り当てられません。未指定アドレスを次の図に示します。

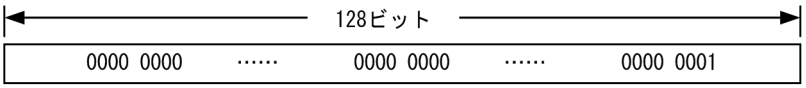
図 3-8　未指定アドレス



(5)　ループバックアドレス

アドレス 0:0:0:0:0:0:0:1（0::1，または::1）は，**ループバックアドレス**と定義されています。ループバックアドレスは自ノード宛てに通信するときにパケットの宛先アドレスとして使用されます。ループバックアドレスはインタフェースに対して割り当てられません。また，終点アドレスがループバックアドレスの IPv6 パケットは, そのノード外に送信することや, ルータによって転送することは禁止されています。ループバックアドレスを次の図に示します。

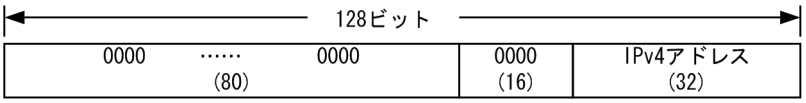
図 3-9　ループバックアドレス



(6)　IPv4 互換アドレス

IPv4 互換 IPv6 アドレスは，二つの IPv6 ノードが IPv4 で経路制御されたネットワークで通信するためのアドレスです。下位 32 ビットに IPv4 アドレスを含む特殊なユニキャストアドレスで, IPv4 ネットワークに接続している機器同士が通信する場合に使用します。プレフィックスは 96 ビット長ですべて 0 です。IPv4 互換アドレスを次の図に示します。なお，IPv4 互換 IPv6 アドレスは RFC4291 で廃止されました。

図 3-10　IPv4 互換アドレス

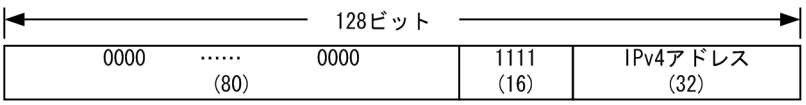


（ ）内の数字はビット数を示す。

(7)　IPv4 射影アドレス

IPv4 射影 IPv6 アドレスは，IPv6 をサポートしていない IPv4 専用ノードで使用されます。IPv4 しかサポートしないホストと IPv6 ホストが通信する場合に IPv6 ホストは IPv4 射影 IPv4 アドレスを使用します。プレフィックスは 96 ビット長で上位 80 ビットの 0 に続き 16 ビットの 1 が設定されます。IPv4 射影アドレスを次の図に示します。

図 3-11　IPv4 射影アドレス

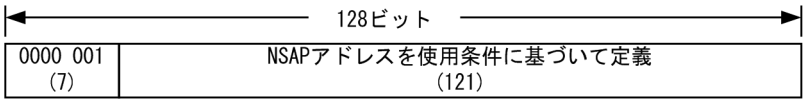


（ ）内の数字はビット数を示す。

(8)　NSAP 互換アドレス

IPv6 で NSAP アドレスを変換して使用するためのアドレス形式です。NSAP をサポートするアドレスフォーマットプレフィックスとして上位 7 ビットに 0000 001 が定義されています。NSAP 互換アドレスを次の図に示します。なお，NSAP 互換アドレスは RFC4048 で廃止されました。

図 3-12　NSAP 互換アドレス

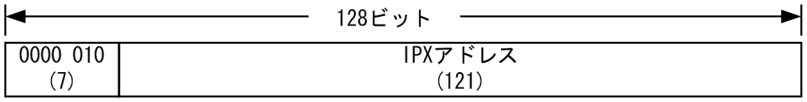


（　）内の数字はビット数を示す。

(9)　IPX 互換アドレス

IPv6 で IPX アドレスを変換して使用するためのアドレス形式です。IPX をサポートするアドレスフォーマットプレフィックスとして上位 7 ビットに 0000 010 が定義されています。IPX 互換アドレスを次の図に示します。なお，IPX 互換アドレスは RFC3513 で廃止されました。

図 3-13　IPX 互換アドレス

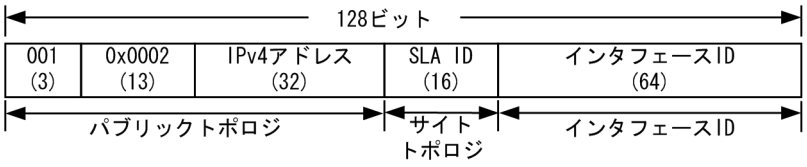


（　）内の数字はビット数を示す。

(10)　6to4 アドレス

6to4 トンネルで使用するアドレス形式です。プレフィックスとして 2002::/16 が割り当てられていて，17 ビット目から 48 ビット目にトンネルを使用するサイトの IPv4 アドレスを設定します。6to4 アドレスを次の図に示します。

図 3-14　6to4 アドレス



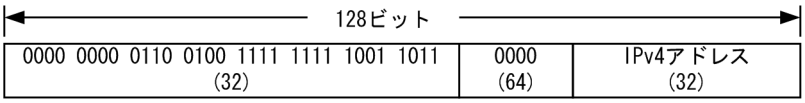
（　）内の数字はビット数を示す。

(11)　IPv4 埋め込み IPv6 アドレス

IPv4 アドレスと IPv6 アドレスの変換に使用されるアドレス形式です。プレフィックスとしてウェルノウン・プレフィックスを使用する形式と，任意のプレフィックスを使用する形式があります。本装置では通常のグローバルアドレスとして扱います。

ウェルノウン・プレフィックス（64:ff9b::/96）を使用する形式では，下位 32 ビットに IPv4 アドレスが格納されます。ウェルノウン・プレフィックスを使用した IPv4 埋め込み IPv6 アドレスを次の図に示します。

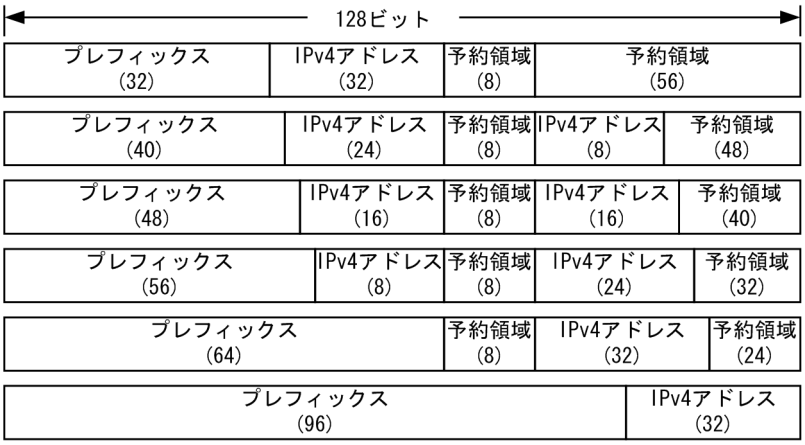
図 3-15　IPv4 埋め込み IPv6 アドレス（ウェルノウン・プレフィックスを使用）



（　）内の数字はビット数を示す。

任意のプレフィックスを使用する形式では，プレフィックス長は 32，40，48，56，64，96 のどれかになります。プレフィックス長が 32，40，48，56，64 の形式には，8 ビットの予約領域と末尾の予約領域があります。このうちプレフィックス長が 40，48，56 の形式では，IPv4 アドレスが 8 ビットの予約領域によって分割されます。任意のプレフィックスを使用した IPv4 埋め込み IPv6 アドレスを次の図に示します。

図 3-16　IPv4 埋め込み IPv6 アドレス（任意のプレフィックスを使用）

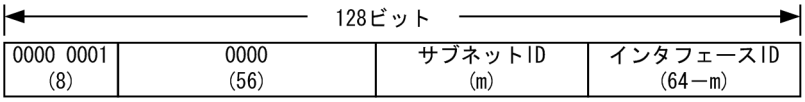


（　）内の数字はビット数を示す。

(12)　廃棄プレフィックスアドレス

特定の送信元または宛先アドレスのパケットを廃棄するために使用されるアドレス形式です。プレフィックスとして 100::/64 が割り当てられています。本装置では通常のグローバルアドレスとして扱います。廃棄プレフィックスアドレスを次の図に示します。

図 3-17　廃棄プレフィックスアドレス

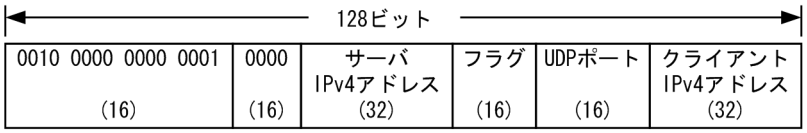


（　）内の数字はビット数を示す。

(13)　Teredo IPv6 アドレス

UDP による IPv6 トンネリングを実現する Teredo で使用されるアドレス形式です。プレフィックスとして 2001::/32 が割り当てられています。本装置では通常のグローバルアドレスとして扱います。Teredo IPv6 アドレスを次の図に示します。

図 3-18　Teredo IPv6 アドレス

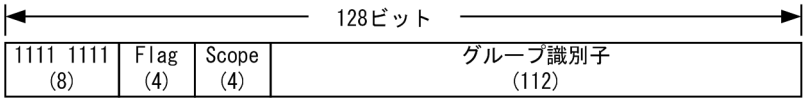


（　）内の数字はビット数を示す。

3.1.5　マルチキャストアドレス

マルチキャストアドレスは複数のノードの集合体を示すアドレスです。アドレスフォーマットプレフィックスの上位 8 ビットが ff であるアドレスが定義されています。ノードは複数のマルチキャストグループに所属できます。マルチキャストアドレスは，パケットの始点アドレスとして使用できません。マルチキャストアドレスには，アドレスフォーマットプレフィックスに続いて，フラグフィールド（4 ビット），スコープフィールド（4 ビット）およびグループ識別子フィールド（112 ビット）が含まれます。IPv6 マルチキャストアドレスを次の図に示します。

図 3-19　IPv6 マルチキャストアドレス



（　）内の数字はビット数を示す。

フラグフィールドの 4 ビットは，1 ビットずつフラグとして次のように定義されています。

1 ビット目

予約されていて，0 に初期化されます。

2 ビット目

R フラグビットと定義されていて，次の値を取ります。

- R フラグビットが 0
  ランデブーポイントのアドレスが埋め込まれていないマルチキャストアドレス
- R フラグビットが 1
  ランデブーポイントのアドレスが埋め込まれているマルチキャストアドレス

3 ビット目

P フラグビットと定義されていて，次の値を取ります。

- P フラグビットが 0
  ネットワークプレフィックスに基づかないで割り当てられたマルチキャストアドレス
- P フラグビットが 1
  ネットワークプレフィックスに基づいて割り当てられたマルチキャストアドレス

4 ビット目

T フラグビットと定義されていて，次の値を取ります。

- T フラグビットが 0
  IANA によって永続的に割り当てられた既知のマルチキャストアドレス
- T フラグビットが 1
  一時的に使用される（非永続的な）マルチキャストアドレス

スコープフィールドは４ビットのフラグでマルチキャストグループのスコープを限定するために使用します。マルチキャストアドレスのスコープフィールド値を次の表に示します。

表 3-2　マルチキャストアドレスのスコープフィールド値

値	スコープの範囲
0	予約
1	インタフェースローカルスコープ
2	リンクローカルスコープ
3	予約
4	アドミンローカルスコープ
5	サイトローカルスコープ
6	未割り当て
7	未割り当て
8	組織ローカルスコープ
9	未割り当て
A	未割り当て
B	未割り当て
C	未割り当て
D	未割り当て
E	グローバルスコープ
F	予約

(1)　全ノードアドレス

全ノードアドレスは，指定されたスコープ内すべての IPv6 ノードの集合体を示すアドレスです。このアドレスを終点アドレスに持つパケットは，指定スコープ内すべてのノードで受信されます。全ノードアドレスの種類を次に示します。

- ff01:0:0:0:0:0:0:1　インタフェースローカル・全ノードアドレス
- ff02:0:0:0:0:0:0:1　リンクローカル・全ノードアドレス

(2)　全ルータアドレス

全ルータアドレスは，指定されたスコープ内すべての IPv6 ルータの集合体を示すアドレスです。このアドレスを終点アドレスに持つパケットは，指定スコープ内すべてのルータで受信されます。全ルータアドレスの種類を次に示します。

- ff01:0:0:0:0:0:0:2　インタフェースローカル・全ルータアドレス
- ff02:0:0:0:0:0:0:2　リンクローカル・全ルータアドレス
- ff05:0:0:0:0:0:0:2　サイトローカル・全ルータアドレス

(3)　要請ノードアドレス

要請ノードアドレスは，ノードのユニキャストアドレスとエニキャストアドレスから変換され，要請ノードのアドレス（ユニキャストまたはエニキャスト）の下位 24 ビットを 104 ビットのプレフィックス ff02:0:0:0:0:1:ff00::/104 に加えたものです。要請ノードアドレスの範囲を次に示します。

ff02:0:0:0:0:1:ff00:0000　～　ff02:0:0:0:0:1:ffff:ffff

集約プロバイダごとに上位プレフィックスが異なるなどの理由で上位の数ビットだけが異なる IPv6 アドレスが生成された場合，これらのアドレスは同じ要請ノードアドレスとなります。これによってノードが加入しなくてはならないマルチキャストアドレスの数を少なくできます。

3.1.6　本装置で使用する IPv6 アドレスの扱い

(1)　設定できるアドレス

本装置のインタフェースに設定する IPv6 アドレスとして次のアドレスを使用できます。

- グローバルユニキャストアドレス
- リンクローカルユニキャストアドレス

また，次に示す IPv6 アドレスは設定できますが，グローバルユニキャストアドレスと同等として扱われます。

- サイトローカルユニキャストアドレス
- エニキャストアドレス
- アドレスフォーマットプレフィックスが未割り当てのアドレス
- NSAP 互換アドレス
- IPX 互換アドレス

(2)　設定できないアドレス

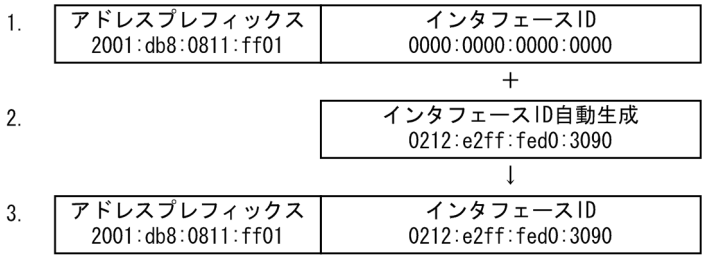
次に示す形式の IPv6 アドレスはインタフェースに設定できません。

- マルチキャストアドレス
- 未指定アドレス
- ループバックアドレス
- IPv4 互換アドレス
- IPv4 射影アドレス
- 上位 10 ビットが 1111 1110 10 で始まり，11 ビットから 64 ビットまでがすべて 0 ではないアドレス
- アドレスを自動生成しない場合にインタフェース ID がすべて 0 となるアドレス

(3)　インタフェース ID 省略時のアドレス自動生成

本装置では，インタフェースへの IPv6 アドレス設定時に，インタフェース ID を省略したプレフィックス形式を指定できます。プレフィックス形式指定の場合，プレフィックス長が 64，または省略した形式で指定すると，インタフェース ID を装置側で MAC アドレスから自動生成できます。アドレス自動生成例を次の図に示します。

図 3-20　アドレス自動生成例



1. アドレスプレフィックス形式を指定します（例　2001:db8:0811:ff01::）。
2. インタフェース ID をメディア種別によって自動生成します（例　0212:e2ff:fed0:3090）。
3. 生成されたインタフェース ID と指定されたアドレスプレフィックスを合成してアドレスとします。

また，インタフェースにリンクローカルアドレス以外の IPv6 アドレスが指定されたときに該当するインタフェースにリンクローカルアドレスが存在しなかった場合は，リンクローカルユニキャストアドレスを EUI64 方式で自動生成して設定します。さらに，インタフェースに対してリンクローカルユニキャストアドレスだけを自動生成で設定することもできます。

(4)　プレフィックス長で設定できる具体例

プレフィックス長で設定できる具体例を次の表に示します。

表 3-3　プレフィックス長で設定できる具体例

アドレス指定形式	設定許可	説明
2001:db8::/1～2001:db8::/28	○	プレフィックス長の指定がプレフィックスより短いため，インタフェース ID 部がすべて 0 にはならないので設定できます。
2001:db8::/29～2001:db8::/63	×	プレフィックス長の指定がプレフィックスより長いため，インタフェース ID 部がすべて 0 になるので設定できません。
2001:db8::/64 or 2001:db8::	○	プレフィックス長が 64 または未指定でインタフェース ID 部が省略されている場合はインタフェース ID を装置で自動生成するため設定できます。
2001:db8::/65～2001:db8::/127	×	プレフィックス長の指定がプレフィックスより長いため，インタフェース ID 部がすべて 0 になるので設定できません。
2001:db8::/128	○	すべてアドレスプレフィックスのため設定できます。

（凡例）　○：設定できる　×：設定できない

3.1.7　ステートレスアドレス自動設定機能

IPv6 リンクローカルアドレスを装置内で自動生成する機能，およびホストが IPv6 アドレスを自動生成する場合に必要な情報をルータから通知する機能です。本装置では IPv6 ステートレスアドレス自動設定（RFC4862 準拠）をサポートしています。

3.2　IPv6 レイヤ機能

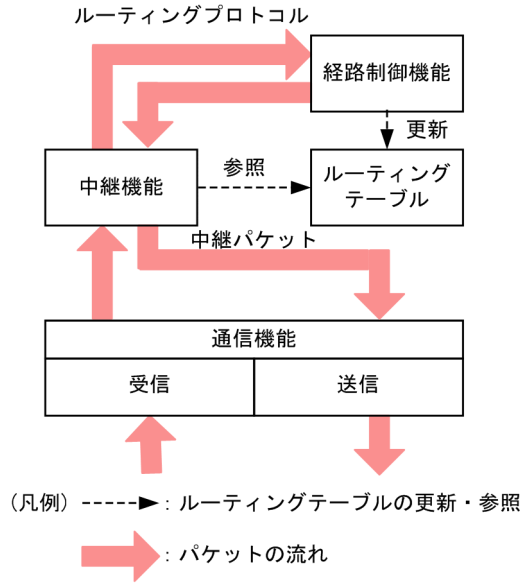
3.2.1　中継機能

本装置は受信した IPv6 パケットをルーティングテーブルに従って中継します。この中継処理は大きく分けて次の三つの機能から構成されています。

- 通信機能
  IPv6 レイヤの送信および受信処理をする機能です。
- 中継機能
  ルーティングテーブルに従って IPv6 パケットを中継する機能です。
- 経路制御機能
  経路情報の送受信や，中継経路を決定してルーティングテーブルを作成する機能です。

IPv6 ルーティング機能の概要を次の図に示します。

図 3-21　IPv6 ルーティング機能の概要



3.2.2　IPv6 アドレス付与単位

本装置ではインタフェースに対して IPv6 アドレスを設定します。IPv6 では一つのインタフェースに複数の IPv6 アドレスを設定でき，IPv6 アドレスを設定したインタフェースには自動的に IPv6 リンクローカルアドレスが付与されます。ただし，リンクローカルアドレスをコンフィグレーションで設定した場合を除きます。

3.3　通信機能

この節では, IPv6 で使用する通信プロトコルについて説明します。IPv6 で使用する通信プロトコルには次に示すものがあります。

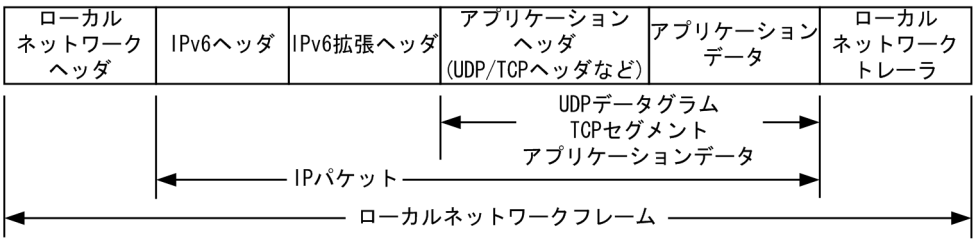
- IPv6
- ICMPv6
- NDP

3.3.1　インターネットプロトコル　バージョン 6（IPv6）

(1)　IPv6 パケットフォーマット

本装置が送信する IPv6 パケットのフォーマットおよび設定値は RFC2460 に従います。IPv6 パケットフォーマットを次の図に示します。

図 3-22　IPv6 パケットフォーマット



(2)　IPv6 パケットヘッダ有効性チェック

IPv6 では 40 オクテット長のヘッダに，8 個のフィールドと 2 個のアドレスが含まれます。IPv6 ヘッダ形式を次の図に示します。

図 3-23　IPv6 ヘッダ形式



・バージョン(4ビット)　IPバージョンを示す領域
・トラフィッククラス(8ビット)　クラス，優先度の特定および識別
・フローラベル(20ビット)　パケットの属するフローの番号
・ペイロード長(16ビット)　オクテット単位で示したペイロード長
・次ヘッダ(8ビット)　IPv6ヘッダ直後に続くヘッダの種別
・ホップリミット(8ビット)　中継限界数
・始点アドレス(128ビット)　パケットの送信元アドレス
・終点アドレス(128ビット)　パケットの宛先アドレス

IPv6 パケット受信時に IPv6 パケットヘッダの有効性をチェックします。IPv6 パケットヘッダのチェック内容を次の表に示します。

表 3-4　IPv6 パケットヘッダのチェック内容

IPv6 パケット ヘッダフィールド	チェック内容	チェック異常時 パケット廃棄	パケット廃棄時 ICMPv6 送信
バージョン	バージョン＝ 6 であること	○	×
トラフィッククラス	チェックしない	−	−
フローラベル	チェックしない	−	−
ペイロード長	リンクレイヤデータ長＜ 3 層データ長（Payload Length ＋ 40Byte（L3 ヘッダ分））ではないこと	○	×
次ヘッダ	チェックしない	−	−
ホップリミット	自装置宛てアドレスの受信パケットのホップリミット： チェックしない	−	−
	中継するパケットのホップリミット： ホップリミット−1≧0 であること	○	○※
送信元アドレス	次の条件をすべて満たすこと • マルチキャストアドレスではないこと • IPv4 射影アドレスではないこと • 未指定アドレスではないこと（中継時） • グローバルスコープであること(中継時)	○	×

IPv6 パケット ヘッダフィールド	チェック内容	チェック異常時 パケット廃棄	パケット廃棄時 ICMPv6 送信
宛先アドレス	次の条件をすべて満たすこと • ループバックアドレスではないこと • IPv4 射影アドレスではないこと • 未指定アドレスではないこと	○	×

（凡例）　○：する　×：しない　－：該当しない

注※　ICMPv6 Time Exceeded メッセージを送信します。

(3)　IPv6 拡張ヘッダサポート仕様

本装置がサポートする IPv6 拡張ヘッダの項目を次の表に示します。

表 3-5　IPv6 拡張ヘッダの項目

IPv6 拡張ヘッダ	IPv6 パケットの分類		
	本装置が発局となるパケット	本装置が着局となるパケット※1	本装置が中継するパケット
Hop-by-Hop Options Header	○	○	○※2
Routing Header※3	○	○	－
Fragment Header	○	○	－
Authentication Header	×	×	－
Encapsulating Security Payload Header	×	×	－
Destination Options Header	○	○	－

（凡例）　○：サポートする　×：サポートしない　－：ヘッダ処理なし

注※1

本装置が受信するパケットが次の条件に該当する場合，パケットを廃棄します。

・拡張ヘッダが 9 個以上設定されたパケット

・一つの拡張ヘッダ内に 9 個以上のオプションが設定されたパケット

注※2

本装置が中継するパケットが次の条件に該当する場合，パケットを廃棄します。

・Hop-by-Hop Options ヘッダ内に 9 個以上のオプションが設定されたパケット

注※3

RFC5095 に従って Routing Header Type0 の付いたパケットは廃棄します。

(4)　送信元アドレス選択

送信インタフェースに設定された IPv6 アドレスの中で宛先アドレスに最も近いアドレスを，送信元アドレスとして使用します。ただし，プロトコルやコンフィグレーションによって送信元アドレスが規定されているときは，その IPv6 アドレスを使用します。

3.3.2　ICMPv6

本装置が送信する ICMPv6 メッセージのフォーマットおよび設定値は RFC4443 に従います。ICMPv6 メッセージのサポート仕様を次の表に示します。

表 3-6　ICMPv6 メッセージサポート仕様

ICMPv6 メッセージ（値は 10 進数）				サポート
タイプ（種別）	値	コード（詳細種別）	値	
Destination Unreachable	1	no route to destination	0	○
		communication with destination administratively prohibited	1	○
		beyond scope of source address	2	○
		address unreachable	3	○
		port unreachable	4	○
Packet Too Big	2	−	0	○
Time Exceeded	3	hop limit exceeded in transit	0	○
		fragment reassembly time exceeded	1	○
Parameter Problem	4	erroneous header field encountered	0	○
		unrecognized Next Header type encountered	1	○
		unrecognized IPv6 option encountered	2	○
Echo Request	128	−	0	○
Echo Reply	129	−	0	○
Multicast Listener Query	130	−	0	○
Multicast Listener Report	131	−	0	○
Multicast Listener Done	132	−	0	○
Router Solicitation	133	−	0	○
Router Advertisement	134	−	0	○
Neighbor Solicitation	135	−	0	○
Neighbor Advertisement	136	−	0	○
Redirect	137	−	0	○
ICMP Node Information Response	140	A successful reply. The Reply Data field may or may not be empty.	0	○

（凡例）　○：サポートする　−：該当しない

(1)　ICMPv6 Redirect の送信仕様

受信インタフェースと送信インタフェースが同一の中継パケットは，ハードウェアによって ICMPv6 Redirect 送信可否判定が必要であると判断され，ソフトウェアによって可否が判定されます。ソフトウェアでは，次の条件を満たすときに ICMPv6 Redirect のパケットを送信します。

- パケット送信元とネクストホップのルータが同一リンク内にある
- 受信パケットが ICMPv6 以外の IPv6 パケット

(2)　ICMPv6 Time Exceeded の送信仕様

次の条件を満たすときに ICMPv6 Time Exceeded のパケットを送信します。

- 中継する受信 IPv6 パケットのホップリミットが 1 以下
- 受信パケットが ICMPv6 以外の IPv6 パケット

3.3.3　NDP

本装置が送信する NDP パケットのフォーマットおよび設定値は RFC4861 に従います。

(1)　ProxyNDP

本装置は，イーサネットに接続するすべてのインタフェースで ProxyNDP を動作させられます。本装置は次の条件をすべて満たす NDP 近隣要求メッセージを受信した場合に，宛先プロトコルアドレスの代理として NDP 近隣広告メッセージを送信します。

- NDP 近隣要求メッセージの宛先プロトコルアドレスがマルチキャストアドレス，エニキャストアドレスではない
- NDP 近隣要求メッセージの送信元プロトコルアドレスと宛先プロトコルアドレスのネットワーク番号が等しい
- NDP 近隣要求メッセージの宛先プロトコルアドレスがルーティングテーブルにあり到達できる

(2)　NDP エントリの削除条件

次の条件のどれかを満たす場合，該当する NDP エントリを削除します。ただし，コンフィグレーションで設定されたスタティック NDP エントリは削除しません。

- NDP エントリに対応する IPv6 アドレスとの通信が停止したあと，10 分が経過した場合
- ステータス状態が stale の NDP エントリに対応する IPv6 アドレスへ通信が再開されたときに到達性がなかった場合
- インタフェース状態が Down となった場合の該当するインタフェースに存在する全 NDP エントリ

(3)　スタティック NDP 情報の設定

NDP プロトコルを持たない製品を接続するために，イーサネットの MAC アドレスと IPv6 アドレスの対応（スタティック NDP 情報）をコンフィグレーションコマンド ipv6 neighbor で設定できます。

(4)　NDP 情報の参照

運用端末から運用コマンド show ipv6 neighbors で NDP 情報が参照できます。NDP 情報から該当するインタフェースの IPv6 アドレスと MAC アドレスの対応がわかります。

(5)　IPv6 アドレス重複

IPv6 には，隣接ネットワーク上に競合する IPv6 アドレスを持つ装置が存在しないかどうかを確認する Duplicate Address Detection があります。アドレスが重複すると，その IPv6 アドレスでは通信できません。

3.4　中継機能

中継機能は, 受信したパケットをルーティングテーブルに従って次のルータまたはホストに転送する機能です。

3.4.1　ルーティングテーブルの内容

ルーティングテーブルは複数個のエントリから構成されていて, 各エントリは次の内容を含んでいます。本装置のルーティングテーブルの内容は運用コマンド show ipv6 route で表示できます。

Destination

宛先ネットワークプレフィックス，アドレスとそのプレフィックス長です。プレフィックス長は，ルーティングテーブル検索時，受信 IPv6 パケットの宛先アドレスに対するマスクとなります。なお，ホストアドレスによって中継する場合には 128 を表示します。

Next Hop

次に中継するルータの IPv6 アドレスです。

Interface

Next Hop のあるインタフェース名です。

Metric

ルートのメトリックです。

Protocol

学習元プロトコルです。

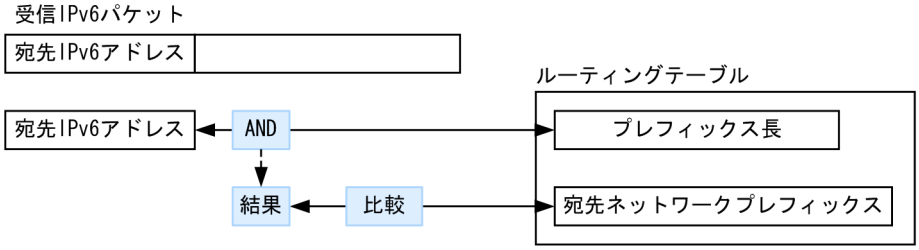
Age

ルートが確認，または変更されてからの時間（秒）です。

3.4.2　ルーティングテーブルの検索

受信した IPv6 パケットの宛先アドレスに該当するエントリをルーティングテーブルから検索します。該当するエントリとは，受信した IPv6 パケットの宛先アドレスを各エントリのプレフィックス長で上位ビットからマスク（AND）を取って，その結果が宛先ネットワークプレフィックスと同じ値になるものです。ルーティングテーブルの検索を次の図に示します。

図 3-24　ルーティングテーブルの検索



3.5　ループバックインタフェース

ループバックインタフェースは物理回線に依存しない仮想的なインタフェースで，IPv6 アドレスを設定できます。ループバックインタフェースに設定した IPv6 アドレスは，各運用機能の送信元アドレスやルーティングプロトコルで使用します。

グローバルネットワークおよび任意の VRF には，複数のループバックインタフェースを設定できます。装置の送信元アドレスとして自動選択するループバックインタフェースの IPv6 アドレスは一つだけですが，コンフィグレーションによって特定の運用機能の送信元アドレスなどに設定できます。

3.6　IPv6 使用時の注意事項

(1)　IPv6 中継回線の MTU 長の変更

IPv6 の最小パケット長は 1280 バイト以上と RFC2460 で規定されています。そのため, MTU 長を 1280 バイト未満に設定すると, IPv6 通信ができません。IPv6 通信をするインタフェースの MTU 長は 1280 バイト以上で使用してください。

(2)　インタフェースへの複数グローバルアドレスの設定

インタフェースに複数のグローバルアドレスを設定する場合, 該当インタフェースと同一のリンクに接続された端末間で異なるグローバルアドレスを使用して通信すると，本装置を経由した IPv6 中継が発生することがあります。

この際，ICMPv6 Redirect の送信可否判定をするため，ハードウェアによってパケットがソフトウェアに中継されて，本装置の CPU が高負荷となるおそれがあります。そのため，次の点に注意してください。

- 同一リンクに接続された端末は，RA による IPv6 アドレス自動設定を使用するなどして，すべてのプレフィックスを一致させてください。
- セキュリティ上の理由などで，同一リンクに接続された端末のプレフィックスを分ける場合は，CPU の高負荷を防止するため，コンフィグレーションコマンドでハードウェアによる ICMPv6 Redirect の送信可否判定を停止することをお勧めします。

(3)　スタティック NDP についての注意事項

本装置のインタフェースに設定された IPv6 アドレスと重複するスタティック NDP を設定すると，通信ができなくなるなど，装置の挙動が不安定になります。このため，本装置では，コンフィグレーション入力時にインタフェースの IPv6 アドレスとスタティック NDP の重複チェックを実行しますが，次に示す IPv6 アドレスについては重複チェックをしません。

- リンクローカルアドレス（自動生成および手動設定）
- インタフェース ID 省略時に自動生成されるグローバルアドレス

したがって，インタフェースに設定されたこれらの IPv6 アドレスと同じスタティック NDP を設定しないようにしてください。誤って設定した場合は，該当スタティック NDP を削除して，該当インタフェースを再起動してください。

(4)　IPv6 拡張オプション付きパケットのレイヤ 3 中継

- Hop-by-Hop Options Header 付きパケットをレイヤ 3 中継する場合，ソフトウェア中継になります。
- 受信側の QoS 制御機能を使用している場合，経路制御オプションまたは終点オプションを付けている TCP パケットのレイヤ 3 中継は，ソフトウェア中継になります。

4 IPv6・NDP・ICMPv6 の設定と運用

この章では，IPv6 ネットワークのコンフィグレーションの設定方法および状態の確認方法について説明します。

4.1　コンフィグレーション

4.1.1　コンフィグレーションコマンド一覧

IPv6 コンフィグレーションコマンド一覧を次の表に示します。

表 4-1　コンフィグレーションコマンド一覧

コマンド名	説明
ipv6 address	IPv6 アドレスを設定します。
ipv6 enable	インタフェースの IPv6 機能を有効にします。このコマンドによって，リンクローカルアドレスが自動生成されます。
ipv6 icmp error-interval	ICMPv6 エラーの送信間隔を指定します。
ipv6 icmp nodeinfo-query	端末の問い合わせ情報に対して応答します。
ipv6 nd dynamic-limit	インタフェースで学習できる NDP エントリ数を指定します。
ipv6 nd onlink-check	NDP 近隣探索パケット受信時の受信インタフェースとパケットの送信元アドレスのプレフィックスの一致確認実施有無を指定します。
ipv6 nd stale-time	近隣ノードの到達性についての情報の有効期間が経過したあと，情報が破棄されるまでの無通信時間を指定します。
ipv6 nd warning-threshold	インタフェースごとに NDP エントリ数の超過および回復を知らせるシステムメッセージを出力する閾値を指定します。
ipv6 neighbor	スタティック NDP テーブルを作成します。
ipv6 redirects	ICMPv6 リダイレクトメッセージの送信可否を指定します。
ipv6 source-route	IPv6 のルーティングヘッダタイプ 0 パケット処理を有効にします。
system-source-address※	ループバックインタフェースのアドレスを装置の送信元アドレスとして自動選択しないように指定します。

注※

「コンフィグレーションコマンドレファレンス Vol.3　4. ループバックインタフェース」を参照してください。

4.1.2　インタフェースの設定

[設定のポイント]

インタフェースに IPv6 アドレスを設定します。1 インタフェース当たり七つまでのアドレスが指定できます。ipv6 enable コマンドを設定して，IPv6 機能を有効にする必要があります。ipv6 enable コマンドの設定がない場合，IPv6 設定は無効になります。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**

   ポート 1/1 のコンフィグレーションモードに移行します。

2. **(config-if)# ipv6 enable**

   ポート 1/1 のインタフェースに IPv6 アドレス使用可を設定します。

3. **(config-if)# ipv6 address 2001:db8:100::1/64**

ポート 1/1 のインタフェースに IPv6 アドレス 2001:db8:100::1, プレフィックス長 64 を設定します。

4. **(config-if)# ipv6 address 2001:db8:200::1/64**

   ポート 1/1 のインタフェースに IPv6 アドレス 2001:db8:200::1, プレフィックス長 64 を追加します。

4.1.3　リンクローカルアドレスの手動設定

[設定のポイント]

本装置では ipv6 enable コマンドの実行時に，リンクローカルアドレスを自動生成します。リンクローカルアドレスは，1 インタフェース当たり一つだけ使用でき，手動で設定することもできます。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**

   ポート 1/1 のコンフィグレーションモードに移行します。

2. **(config-if)# ipv6 enable**

   ポート 1/1 のインタフェースに IPv6 アドレスの使用可を設定します。このとき，リンクローカルアドレスが自動生成されます。

3. **(config-if)# ipv6 address fe80::1 link-local**

   ポート 1/1 のインタフェースに自動生成されたリンクローカルアドレスを fe80::1 に変更します。

4.1.4　ループバックインタフェースの設定

[設定のポイント]

装置を識別するための IPv6 アドレスを設定します。インタフェース番号 0 はグローバルネットワーク専用です。設定できるアドレスは一つだけです。

[コマンドによる設定]

1. **(config)# interface loopback 0**

   ループバックインタフェースのコンフィグレーションモードに移行します。

2. **(config-if)# ipv6 address 2001:db8::1**

   装置に IPv6 アドレス 2001:db8::1 を設定します。

4.1.5　複数のループバックインタフェースの設定

[設定のポイント]

ループバックインタフェースを複数設定するには，装置の送信元アドレスとして自動選択されないように設定したあと，IP アドレスを設定します。

[コマンドによる設定]

1. **(config)# interface loopback 0**

   ループバックインタフェースのコンフィグレーションモードに移行します。

2. **(config-if)# ipv6 address 2001:db8::1**

   ループバックインタフェースに IPv6 アドレス 2001:db8::1 を設定します。

3. **(config)# interface loopback 1**

   ループバックインタフェース 1 のコンフィグレーションモードに移行します。

4. **(config-if)# no system-source-address**
   装置の送信元アドレスとして自動選択しない設定をします。
5. **(config-if)# ipv6 address 2001:db8::2**
   ループバックインタフェース 1 に IPv6 アドレス 2001:db8::2 を設定します。

4.1.6　スタティック NDP の設定

[設定のポイント]

本装置にスタティック NDP を設定します。

[コマンドによる設定]

1. **(config)# ipv6 neighbor 2001:db8:100::2 interface gigabitethernet 1/1 0012.e240.0a00**
   ポート 1/1 のインタフェースにネクストホップ IPv6 アドレス 2001:db8:100::2, 接続先 MAC アドレス 0012.e240.0a00 でスタティック NDP を設定します。

4.2　オペレーション

4.2.1　運用コマンド一覧

IPv6・NDP・ICMPv6 の運用コマンド一覧を次の表に示します。

表 4-2　運用コマンド一覧

コマンド名	説明
show ip-dual interface	IPv4 および IPv6 インタフェースの状態を表示します。
show ipv6 interface	IPv6 インタフェースの状態を表示します。
clear ipv6 interface statistics	IP インタフェースの IPv6 統計情報を 0 クリアします。
show ipv6 neighbors	NDP 情報を表示します。
clear ipv6 neighbors	ダイナミック NDP 情報をクリアします。
clear ipv6 duplicate-address	Duplicate Address Detection によって重複が検出されたアドレスの通信の抑止状態を解除します。
show netstat (netstat)	ネットワークのステータスを表示します。
clear netstat	ネットワーク統計情報カウンタをクリアします。
show tcpdump (tcpdump)	BCU-CPU で送受信されるパケットをモニタします。
show tcp ha connections	TCP 高可用対象コネクションの状態を表示します。
clear tcp	TCP コネクションを切断します。
ping ipv6	ICMP6 エコーテストを行います。
traceroute ipv6	IPv6 経由ルートを表示します。

4.2.2　IPv6 インタフェースの up/down 確認

IPv6 ネットワークに接続する本装置の回線や回線内のポートに IPv6 アドレスを設定したあとに，show ipv6 interface コマンドを実行して，IPv6 インタフェースの up/down 状態が「UP」であることを確認してください。

図 4-1　show ipv6 interface コマンドの実行結果

```
> show ipv6 interface summary
Date 20XX/03/25 12:00:00 UTC
Eth1/1: UP  2001:db8:1::1/64
Eth1/2: UP  2001:db8:2::1/64
>
```

4.2.3　宛先アドレスとの通信可否の確認

IPv6 ネットワークに接続している本装置のインタフェースについて，ping ipv6 コマンドを実行して通信相手となる装置に対して通信できることを確認してください。

図 4-2　ping ipv6 コマンドの実行結果（通信可の場合）

```
> ping ipv6 2001:db8::2
Date 20XX/03/25 12:00:00 UTC
```

```
PING6 (56=40+8+8 Bytes) 2001:db8::1 -->2001:db8::2
16 bytes from 2001:db8::2, icmp_seq=0 ttl=255 time=0.286 ms
16 bytes from 2001:db8::2, icmp_seq=1 ttl=255 time=0.271 ms
16 bytes from 2001:db8::2, icmp_seq=2 ttl=255 time=0.266 ms
^C
--- 2001:db8::2 ping6 statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.266/0.274/0.286 ms
>
```

図 4-3　ping ipv6 コマンドの実行結果（通信不可の場合）

```
> ping ipv6 2001:db8::2
Date 20XX/03/25 12:00:00 UTC
PING6 (56=40+8+8 bytes) 2001:db8::1 --> 2001:db8::2
^C
--- 2001:db8::2 ping6 statistics ---
12 packets transmitted, 0 packets received, 100% packet loss
>
```

4.2.4　宛先アドレスまでの経路確認

traceroute ipv6 コマンドを実行して，IPv6 ネットワークに接続している本装置のインタフェースから通信相手となる装置までの中継装置を確認してください。

図 4-4　traceroute ipv6 コマンドの実行結果

```
> traceroute ipv6 2001:db8:3::1 numeric
Date 20XX/03/25 12:00:00 UTC
traceroute6 to 2001:db8:3::1 (2001:db8:3::1), 30 hops max, 40 byte packets
1  2001:db8:1::1  0.612 ms  0.541 ms  0.532 ms
2  2001:db8:2::1  0.905 ms  0.816 ms  0.807 ms
3  2001:db8:3::1  1.325 ms  1.236 ms  1.227 ms
>
```

4.2.5　NDP 情報の確認

IPv6 ネットワークに接続する本装置の回線や回線内のポートに IPv6 アドレスを設定したあとに，show ipv6 neighbors コマンドを実行して，本装置と隣接装置間のアドレス解決をしている（NDP エントリ情報がある）ことを確認してください。

図 4-5　show ipv6 neighbors コマンドの実行結果

```
> show ipv6 neighbors interface gigabitethernet 1/1
Date 20XX/03/25 12:00:00 UTC
Total: 3 entries
Neighbor             Linklayer Address Netif      Expire    S Flgs P
2001:db8:1::1        0012.e222.f298    Eth1/1     7s        R
2001:db8:2::1        0012.e26b.8e1b    Eth1/1     24s       R
fe80::1%Eth1/1       0012.e240.3f90    Eth1/1     2s        R R
```

5 VRF

この章では，VRF の解説と操作方法について説明します。

5.1 解説

5.1.1 概要

VRF は，装置内に論理的に分離された複数のルーティングテーブルを保持して，各ルーティングテーブルに従ってパケットを転送する機能です。この異なるルーティング空間のことを **VRF インスタンス**と呼びます。VRF インスタンスが異なれば，同じ IP アドレスを重複して使用できます。また，ルーティングプロトコルを VRF インスタンスごとに独立して動作させられます。VRF によってネットワークを論理的に分離することで，トラフィックを分離して，セキュリティを確保できます。

すべての IP インタフェースは，VRF インスタンスまたはグローバルネットワークのどちらかに所属します。グローバルネットワークとは，VRF 設定されていない状態のネットワークを指します。グローバルネットワークは，VRF 設定されていないインスタンスであり，ほかの VRF インスタンスとは分離されています。

5.1.2 サポート機能一覧

各機能の VRF のサポート状況を次の表に示します。

表 5-1 VRF サポート状況

項目		サポート状況	備考
IP パケット中継	IPv4 ユニキャスト中継	○	詳細は次を参照してください。 • 13.12 VRF の解説 • 13.13 VRF のコンフィグレーション • 13.14 VRF のオペレーション
	IPv4 ユニキャスト VRF 間中継	○	詳細は次を参照してください。 • 13.12.3 エクストラネット • 14.2.7 VRF 間にわたるスタティック経路の設定 • 23.1.6 エクストラネット • 23.2.8 エクストラネット • 23.4.6 エクストラネットの確認
	IPv4 マルチキャスト中継	○	詳細は次を参照してください。 • 24.4.7 VRF での IPv4 マルチキャスト • 25.1 コンフィグレーション • 29 マルチキャスト経路フィルタリング
	IPv4 マルチキャスト VRF 間中継	○	
	IPv6 ユニキャスト中継	○	詳細は次を参照してください。 • 13.12 VRF の解説 • 13.13 VRF のコンフィグレーション

項目		サポート状況	備考
			• 13.14 VRF のオペレーション
	IPv6 ユニキャスト VRF 間中継	○	詳細は次を参照してください。 • 13.12.3 エクストラネット • 14.2.7 VRF 間にわたるスタティック経路の設定 • 23.1.6 エクストラネット • 23.3.8 エクストラネット • 23.4.6 エクストラネットの確認
	IPv6 マルチキャスト中継	○	詳細は次を参照してください。 • 26.4.6 VRF での IPv6 マルチキャスト • 27.1 コンフィグレーション • 29 マルチキャスト経路フィルタリング
	IPv6 マルチキャスト VRF 間中継	○	
IP インタフェース	イーサネットインタフェース	○	なし
	イーサネットサブインタフェース	○	
	ポートチャネルインタフェース	○	
	ポートチャネルサブインタフェース	○	
	マネージメントポート	○	
	ループバックインタフェース	○	
	Null インタフェース	○	グローバルネットワークと VRF で一つの Null インタフェースを共用します。
uRPF		○	なし
ポリシーベースルーティング		○	VRF 間ルーティングもできます。 VRF 間ポリシーベースルーティングのコンフィグレーションについては，次を参照してください。 • 8.2.4 異なる VRF 間でのポリシーベースルーティングの設定
RA		○	なし
DHCP/BOOTP リレーエージェント		○	VRF 上でのリレーエージェントのコンフィグレーションについては，次を参照してください。 • 10.2.4 VRF 構成での設定

項目		サポート状況	備考
			• 10.2.6 VRF（エクストラネット）構成での設定
DHCPv6 リレーエージェント		○	コンフィグレーションについては，次を参照してください。 • 11.2.5 VRF（経路交換によるエクストラネット）構成での設定
VRRP		○	なし
IPv4 スタティックルーティング		○	VRF 間ルーティングもできます。 コンフィグレーションについては，次を参照してください。 • 14.2.6 VRF でのスタティック経路の設定 • 14.2.7 VRF 間にわたるスタティック経路の設定
IPv6 スタティックルーティング		○	VRF 間ルーティングもできます。 コンフィグレーションについては，次を参照してください。 • 14.2.6 VRF でのスタティック経路の設定 • 14.2.7 VRF 間にわたるスタティック経路の設定 • 14.2.8 IPv6 リンクローカルアドレスをネクストホップとした VRF 間にわたるスタティック経路の設定
IPv4 ユニキャストルーティングプロトコル	RIP	○	コンフィグレーションについては，次を参照してください。 • 15.2.8 VRF での RIP の適用 • 17.2.7 VRF での OSPF の適用
	OSPF	○	
	BGP4	○	詳細は次を参照してください。 • 21.1.4 VRF での BGP4 または BGP4+ • 21.2.11 VRF での BGP4 の設定
	経路フィルタリング	○	なし
IPv6 ユニキャストルーティングプロトコル	RIPng	○	コンフィグレーションについては，次を参照してください。 • 16.2.5 VRF での RIPng の適用 • 19.2.7 VRF での OSPFv3 の適用
	OSPFv3	○	
	BGP4+	○	詳細は次を参照してください。

項目		サポート状況	備考
			• 21.1.4 VRF での BGP4 または BGP4+ • 21.3.11 VRF での BGP4+の設定
	経路フィルタリング	○	なし
IPv4 マルチキャストルーティングプロトコル	IGMP	○	詳細は次を参照してください。 • 24.4.7 VRF での IPv4 マルチキャスト • 25.1 コンフィグレーション • 29 マルチキャスト経路フィルタリング
	PIM-SM	△※	
	PIM-SSM	○	
IPv6 マルチキャストルーティングプロトコル	MLD	○	詳細は次を参照してください。 • 26.4.6 VRF での IPv6 マルチキャスト • 27.1 コンフィグレーション • 29 マルチキャスト経路フィルタリング
	PIM-SM	△※	
	PIM-SSM	○	
BFD		○	なし
フィルタ		○	なし
QoS		○	なし
トラッキング機能		○	なし
ネットワーク管理機能	ポートミラーリング	○	なし
	sFlow 統計	△	VRF も統計対象に含みます。ただし，VRF を設定したインタフェースで収集する情報では，ルータ型拡張データ形式およびゲートウェイ型拡張データ形式は無効となります。 また，コレクタはグローバルネットワークに設置してください。
	CFM	○	なし
	LLDP	△	Draft6.0 の Organizationally Specific TLVs はグローバルネットワークだけが対応します。詳細は次を参照してください。 • コンフィグレーションガイド Vol.2 28.1.4 LLDP 使用時の注意事項
運用管理	SNMP	○	VRF 上での SNMP のコンフィグレーションについては，次を参照してください。

項目		サポート状況	備考
			• コンフィグレーションガイド Vol.1　16.2 コンフィグレーション
	MIB	△	一部の MIB はグローバルネットワークだけが対象です。詳細は次を参照してください。 • MIB レファレンス　2. 標準 MIB（RFC 準拠および IETF ドラフト MIB） • MIB レファレンス　3. プライベート MIB
	SNMP 通知	△	一部の SNMP 通知はグローバルネットワークだけが対象です。詳細は次を参照してください。 • MIB レファレンス　4. SNMP 通知
	syslog 出力	○	VRF への syslog 出力のコンフィグレーションについては，次を参照してください。 • コンフィグレーションガイド Vol.1　15.2.3 syslog 出力の設定
	E-mail 出力	－	グローバルネットワークだけが対象
運用・保守	ping	○	なし
	traceroute	○	
	telnet	○	
	ftp	○	
	tftp	○	
	telnet によるログイン	○	詳細は次を参照してください。 • コンフィグレーションガイド Vol.1　8.1.10 VRF でのリモート運用端末からのログインの許可 • コンフィグレーションガイド Vol.1　8.1.11 VRF でのリモート運用端末からのログインを許可する IP アドレスの設定
	ftp によるログイン	○	
	SSH	○	詳細は次を参照してください。 • コンフィグレーションガイド Vol.1　9.2.8 VRF での SSH によるログインを許可する
	運用情報のバックアップ・リストア	○	なし

項目		サポート状況	備考
	DNS リゾルバ	－	グローバルネットワークだけが対象
	NTP/SNTP	○	コンフィグレーションについては，次を参照してください。 • コンフィグレーションガイド Vol.1　10.3.5 VRF での NTP による時刻同期の設定 • コンフィグレーションガイド Vol.1　10.4.4 VRF での SNTP による時刻同期の設定

（凡例）○：サポート　△：一部サポート　－：未サポート

注※

IPv4 マルチキャストエクストラネットおよび IPv6 マルチキャストエクストラネットは未サポートです。

5.1.3　エクストラネット

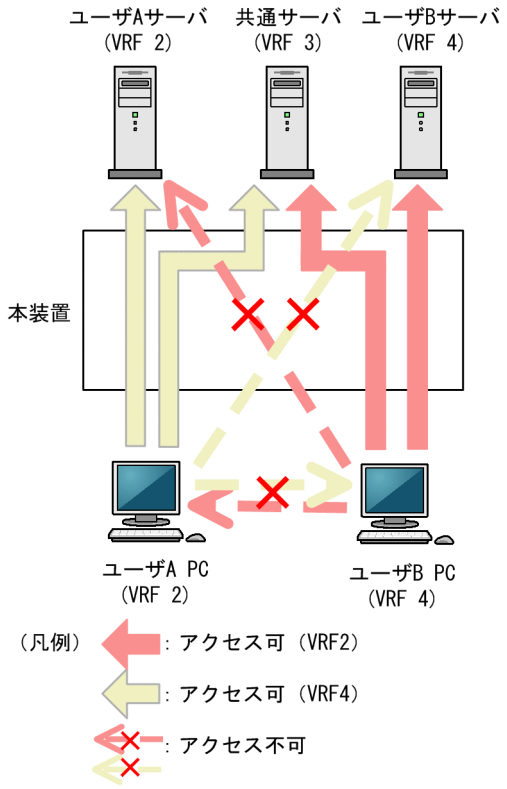
VRF によってトラフィックを分離しながら，特定の VRF 間だけ通信できるようにすることを**エクストラネット**と呼びます。これによって，VRF 間のセキュリティを確保した状態で共通サーバを設置するような共有ネットワークが構築できます。

エクストラネットの実現には，次に示す VRF 間中継技術のどれかを使用します。

- VRF 間の経路交換
- VRF 間にわたるスタティックルーティング
- ポリシーベースルーティング

エクストラネットの構築例を次の図に示します。

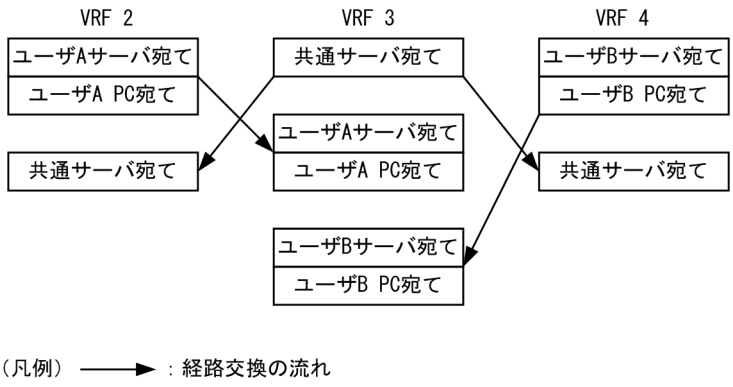
図 5-1 経路交換によるエクストラネット



- ユーザ A（VRF2）とユーザ B（VRF 4）は経路情報が分離されているため通信できません。
- ユーザ A（VRF 2）と共通サーバ（VRF 3），およびユーザ B（VRF 4）と共通サーバ（VRF 3）はそれぞれ経路交換しているため通信できます。

このとき，本装置で持つ経路情報と情報交換の流れについて，次の図に示します。

図 5-2 本装置の経路情報



エクストラネットを実現する各機能の詳細は，ポリシーベースルーティング，ユニキャストルーティング，マルチキャストルーティングおよび各機能の章を参照してください。

5.2 コンフィグレーション

5.2.1 コンフィグレーションコマンド一覧

VRF のコンフィグレーションコマンド一覧を次の表に示します。

表 5-2 コンフィグレーションコマンド一覧

コマンド名	説明
ipv6 maximum routes	該当 VRF で収容する IPv6 の最大経路数を指定します。
maximum routes	該当 VRF で収容する IPv4 の最大経路数を指定します。
vrf definition	VRF を設定します。
arp-limit※1	VRF の ARP エントリ上限数を設定します。
vrf forwarding※1	インタフェースに VRF を指定します。
nd-limit※2	VRF の NDP エントリ上限数を設定します。

注※1

「コンフィグレーションコマンドレファレンス Vol.3　2. IPv4・ARP・ICMP」を参照してください。

注※2

「コンフィグレーションコマンドレファレンス Vol.3　3. IPv6・NDP・ICMPv6」を参照してください。

5.2.2 VRF の設定

本装置で VRF 機能を動作させるには，VRF の設定，インタフェースの VRF 設定，および各機能の VRF 設定が必要です。ここでは，VRF の設定とインタフェースの VRF 設定を示します。各機能の VRF 設定については，各機能のコンフィグレーションの節を参照してください。

[設定のポイント]

VRF を使用するには, vrf definition コマンドで VRF を設定します。そのあと, インタフェースに VRF を指定します。

[コマンドによる設定]

1. **(config)# vrf definition 1**
   (config-vrf)# maximum routes 500 70
   (config-vrf)# arp-limit 50
   (config-vrf)# ipv6 maximum routes 400 70
   (config-vrf)# nd-limit 50
   (config-vrf)# exit
   VRF 1 を設定します。IPv4 最大経路数を 500，警告のシステムメッセージを出力する閾値を 70%に設定します。ARP エントリの上限を 50 に設定します。IPv6 最大経路数を 400，警告のシステムメッセージを出力する閾値を 70%に設定します。NDP エントリの上限を 50 に設定します。
2. **(config)# interface loopback 1**
   (config-if)# vrf forwarding 1
   (config-if)# ip address 192.168.0.1

```
(config-if)# ipv6 address 2001:db8::1
(config-if)# exit
```

ループバックインタフェースに VRF を指定します。ループバックインタフェース 1 に VRF 1 を指定して，IPv4 アドレスとして 192.168.0.1，IPv6 アドレスとして 2001:db8::1 を設定します。

3.
```
(config)# interface loopback 2
(config-if)# no system-source-address
(config-if)# vrf forwarding 1
(config-if)# ip address 192.168.0.2
(config-if)# ipv6 address 2001:db8::2
(config-if)# exit
```

ループバックインタフェース 1 のほかに，ループバックインタフェース 2 を設定します。ループバックインタフェース 2 に送信元アドレスとして自動選択しない設定をしたあとに，VRF 1 を指定して，IPv4 アドレスとして 192.168.0.2，IPv6 アドレスとして 2001:db8::2 を設定します。

4.
```
(config)# interface gigabitethernet 1/1
(config-if)# vrf forwarding 1
(config-if)# ip address 192.168.10.1 255.255.255.0
(config-if)# ipv6 enable
(config-if)# ipv6 address 2001:db8:10::1/64
```

イーサネットインタフェースに VRF を指定します。イーサネットインタフェース 1/1 に VRF 1 を指定して，IPv4 アドレスとして 192.168.10.1，サブネットマスク 255.255.255.0 を設定します。IPv6 を有効にして，IPv6 アドレスとして 2001:db8:10::1，プレフィックス長 64 を設定します。

5.3 オペレーション

5.3.1 運用コマンド一覧

VRF の運用コマンド一覧を次の表に示します。

表 5-3 運用コマンド一覧

コマンド名	説明
show ip vrf※1	VRF の IPv4 情報を表示します。
show ipv6 vrf※2	VRF の IPv6 情報を表示します。

注※1

「運用コマンドレファレンス Vol.3 10. IPv4 ルーティングプロトコル」を参照してください。

注※2

「運用コマンドレファレンス Vol.3 11. IPv6 ルーティングプロトコル」を参照してください。

5.3.2 VRF 情報の確認

(1) IPv4 情報の確認

show ip vrf コマンドで，VRF の IPv4 経路情報や VRF に所属する IPv4 インタフェースの状態を確認できます。コマンドの実行結果を次に示します。

図 5-3 show ip vrf コマンドの実行結果

```
> show ip vrf all
Date 20XX/12/20 12:00:00 UTC
VRF              Routes        ARP
global           12/100        12/100
100              7/30          7/50
```

図 5-4 show ip vrf コマンド（detail パラメータ指定）の実行結果

```
>show ip vrf all detail
Date 20XX/12/20 12:00:00 UTC
VRF: global
  Maximum routes: 100, Warn threshold: 70%, Current routes: 12
  Maximum ARP entries: 100, Current ARP entries: 12
  Import inter-vrf: Match_Ext
Interface
Name           Local              Remote          Status
Eth1/9         192.168.1.1/24     192.168.1.255   Up
localhost      127.0.0.1/8        127.0.0.1       Up

VRF: 10
  Maximum routes: 50, Warn threshold: 70%, Current routes: 10
  Maximum ARP entries: 30, Current ARP entries: 10
  Import inter-vrf: FLT_SET
Interface
Name           Local              Remote          Status
Eth1/1         192.168.10.1/24    192.168.10.255  Up
localhost      127.0.0.1/8        127.0.0.1       Up

VRF: 20
  Maximum routes: 10, Warning only, Current routes: 5
  Maximum ARP entries: 10, Current ARP entries: 5
  Import inter-vrf: FLT_EXT1
Interface
Name           Local              Remote          Status
Eth1/5         172.16.1.100/16    172.16.255.255  Up
```

```
localhost       127.0.0.1/8         127.0.0.1       Up
>
```

(2) IPv6 情報の確認

show ipv6 vrf コマンドで，VRF の IPv6 経路情報や VRF に所属する IPv6 インタフェースの状態を確認できます。コマンドの実行結果を次に示します。

図 5-5 show ipv6 vrf コマンドの実行結果

```
>show ipv6 vrf all
Date 20XX/10/08 12:00:00 UTC
VRF              Routes          Neighbor
global           12/100          12/100
100              7/30            7/50
```

図 5-6 show ipv6 vrf コマンド（detail パラメータ指定）の実行結果

```
>show ipv6 vrf all detail
Date 20XX/10/08 12:00:00 UTC
VRF: global
  Maximum routes: 100, Warn threshold: 70%, Current routes: 12
  Maximum Neighbor entries: 100, Current Neighbor entries: 12
  Import inter-vrf: Match_Ext
Interface
Name            Address                                     Status
Eth1/9          2001:db8:3:3::3/64                          Up
Eth1/9          fe80::212:e2ff:fe86:5300%Eth1/9/64          Up
localhost       fe80::1%localhost/64                        Up

VRF: 10
  Maximum routes: 50, Warn threshold: 70%, Current routes: 10
  Maximum Neighbor entries: 30, Current Neighbor entries: 10
  Import inter-vrf: FLT_SET
Interface
Name            Address                                     Status
Eth1/1          2001:db8:1:1::1/64                          Up
Eth1/1          fe80::212:e2ff:fe86:5300%Eth1/1/64          Up
localhost       ::1/128                                     Up
localhost       fe80::1%localhost/64                        Up

VRF: 20
  Maximum routes: 10, Warning only, Current routes: 5
  Maximum Neighbor entries: 10, Current Neighbor entries: 5
  Import inter-vrf: FLT_EXT1
Interface
Name            Address                                     Status
Eth1/2          2001:db8:2:2::2/64                          Up
Eth1/2          fe80::212:e2ff:fe86:5300%Eth1/2/64          Up
localhost       ::1/128                                     Up
localhost       fe80::1%localhost/64                        Up
>
```

6 Null インタフェース

この章では，IPv4 ネットワークおよび IPv6 ネットワークを対象とする Null インタフェースの解説および操作方法について説明します。

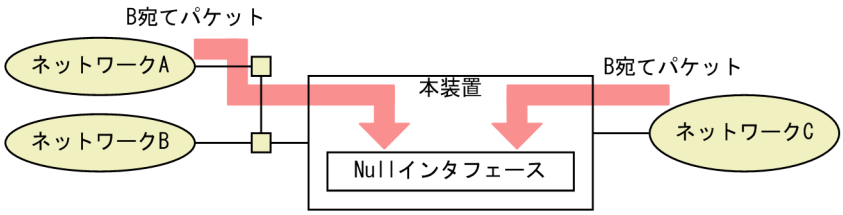
6.1　解説

Null インタフェースは，物理回線に依存しないパケット廃棄用の仮想的なインタフェースで，特定フローの出力先を Null インタフェースに向けることでパケットを廃棄する機能を提供します。

Null インタフェースは常に UP 状態にあり，トラフィックを中継または受信しません。廃棄したパケットに対して，送信元に ICMP（Unreachable）によるパケット廃棄の通知もしません。また，マルチキャストパケットについては Null インタフェース上で廃棄しません。

Null インタフェースを使用して，本装置を経由する特定のネットワーク宛て，または特定の端末宛ての通信を制限できます。次の図では，本装置を経由するネットワーク B 宛ての通信をすべて Null インタフェースに向けて，ネットワーク B 宛てのパケットを廃棄することを示しています。

図 6-1　Null インタフェースネットワーク構成



この機能はスタティックルーティングの一部として位置づけられます。このため，Null インタフェースでパケットを廃棄する場合，出力先が Null インタフェースになるスタティック経路情報を設定する必要があります。

経路検索時，Null インタフェース宛てと判断された（Null 宛てのスタティック経路情報に基づいてルーティングする）パケットは中継しないで本装置内で廃棄します。

スタティックルーティングおよび経路制御については「14　スタティックルーティング」～「22　BGP4/BGP4+拡張機能」を参照してください。

本装置では，インタフェース単位に複数の条件設定によってパケット廃棄ができるようにするフィルタリング機能も提供していますが，Null インタフェースは特定の宛先フローだけをスタティック経路として設定するだけで，装置で一括してパケットを廃棄できるメリットがあります。

Null インタフェースとフィルタリング機能使用時のパケットの廃棄部位を次の表に示します。

表 6-1　Null インタフェースとフィルタリング機能使用時のパケットの廃棄部位

経路情報	フィルタリング設定		動作	廃棄部位
	入力側	出力側		
Null 宛て	中継	中継	廃棄	Null インタフェース
		廃棄	廃棄	
	廃棄	中継	廃棄	フィルタリング（入力側）
		廃棄	廃棄	
他経路宛て（Null 以外）	中継	中継	中継	－
		廃棄	廃棄	フィルタリング（出力側）

経路情報	フィルタリング設定		動作	廃棄部位
	入力側	出力側		
	廃棄	中継	廃棄	フィルタリング（入力側）
		廃棄	廃棄	

（凡例）　－：該当しない

なお，Null インタフェースによるフィルタ・QoS フローへの影響については，「コンフィグレーションガイド Vol.2　9. フィルタ」または「コンフィグレーションガイド Vol.2　12. QoS フロー」を参照してください。

6.2　コンフィグレーション

6.2.1　コンフィグレーションコマンド一覧

Null インタフェースのコンフィグレーションコマンド一覧を次の表に示します。

表 6-2　コンフィグレーションコマンド一覧

コマンド名	説明
interface null	Null インタフェースを使用する場合に指定します。
ip route※1	IPv4 スタティック経路を生成します。
ipv6 route※2	IPv6 スタティック経路を生成します。

注※1
「コンフィグレーションコマンドレファレンス Vol.3　15. スタティックルーティング（IPv4)」を参照してください。

注※2
「コンフィグレーションコマンドレファレンス Vol.3　16. スタティックルーティング（IPv6)」を参照してください。

6.2.2　Null インタフェースの設定

(1)　IPv4 の場合

[設定のポイント]

Null インタフェースを設定して，本装置を経由する特定のネットワーク宛て，または特定の端末宛てのパケットを廃棄します。

[コマンドによる設定]

1. **(config)# interface null 0**
   Null インタフェースを設定します。
2. **(config)# ip route 203.0.113.0 255.255.255.0 null 0**
   スタティック経路 203.0.113.0/24 のネクストホップとして Null インタフェースを指定します。これらのネットワーク宛てパケットが本装置を通過するとき，パケットは中継されないですべて Null インタフェースに送信され，廃棄されます。

(2)　IPv6 の場合

[設定のポイント]

Null インタフェースを設定して，本装置を経由する特定のネットワーク宛て，または特定の端末宛てのパケットを廃棄します。

[コマンドによる設定]

1. **(config)# interface null 0**
   Null インタフェースを設定します。
2. **(config)# ipv6 route 2001:db8:ffff:1::/64 null 0**

スタティック経路 2001:db8:ffff:1::/64 のネクストホップとして Null インタフェースを指定します。これらのネットワーク宛てパケットが本装置を通過するとき，パケットは中継されないですべて Null インタフェースに送信され，廃棄されます。

6.3　オペレーション

6.3.1　運用コマンド一覧

Null インタフェースの運用コマンド一覧を次の表に示します。

表 6-3　運用コマンド一覧

コマンド名	説明
show ip-dual interface※1	IPv4 および IPv6 インタフェースの状態と統計情報を表示します。
show ip interface※1	IPv4 インタフェースの状態と統計情報を表示します。
clear ip interface statistics※1	IP インタフェースの IPv4 統計情報を 0 クリアします。
show ipv6 interface※2	IPv6 インタフェースの状態と統計情報を表示します。
clear ipv6 interface statistics※2	IP インタフェースの IPv6 統計情報を 0 クリアします。
show ip route※3	ルーティングテーブルで保持する経路情報を表示します。
show ipv6 route※4	ルーティングテーブルで保持する経路情報を表示します。

注※1
「運用コマンドレファレンス Vol.3　2. IPv4・ARP・ICMP」を参照してください。

注※2
「運用コマンドレファレンス Vol.3　3. IPv6・NDP・ICMPv6」を参照してください。

注※3
「運用コマンドレファレンス Vol.3　10. IPv4 ルーティングプロトコル」を参照してください。

注※4
「運用コマンドレファレンス Vol.3　11. IPv6 ルーティングプロトコル」を参照してください。

6.3.2　経路情報の確認

(1)　IPv4 の場合

show ip route コマンドを実行して, コンフィグレーションコマンド static で設定した経路情報の設定内容が正しく反映されていることを確認してください。

図 6-2　Null インタフェース経路情報表示

```
> show ip route static
Date 20XX/03/25 12:00:00 UTC
Total: 1 routes
Destination        Next Hop        Interface     Metric  Protocol  Age
203.0.113.0/24     ----            null0         0/0     Static     1m  9s
>
```

(2)　IPv6 の場合

show ipv6 route コマンドを実行して，コンフィグレーションコマンド static で設定した経路情報の設定内容が正しく反映されていることを確認してください。

図 6-3　Null インタフェース経路情報表示

```
> show ipv6 route static
Date 20XX/03/25 12:00:00 UTC
Total: 1 routes
Destination             Next Hop   Interface      Metric   Protocol  Age
2001:db8:ffff:1::/64    ----       null0          0/0      Static    16s
>
```

6.3.3　パケット廃棄数の確認

(1)　IPv4 の場合

show ip interface コマンドを実行して, Null インタフェースでパケットが廃棄されていることを確認してください。

図 6-4　Null インタフェースパケット廃棄数表示例

```
> show ip interface null 0 statistics
Date 20XX/03/25 12:00:00 UTC
Interface Name               : null
Status                       : UP
IPv4 Discard Packets         :                    92
IPv4 Discard(BCU-CPU) Packets:                    56
>
```

(2)　IPv6 の場合

show ipv6 interface コマンドを実行して，Null インタフェースでパケットが廃棄されていることを確認してください。

図 6-5　Null インタフェースパケット廃棄数表示例

```
> show ipv6 interface null 0 statistics
Date 20XX/03/25 12:00:00 UTC
Interface Name               : null
Status                       : UP
IPv6 Discard Packets         :                    92
IPv6 Discard(BCU-CPU) Packets:                    56
>
```

7 uRPF

uRPF はフィルタ機能の一種で，パケットの送信元アドレスとルーティングテーブルとの整合性を自動で確認する機能です。設定が容易で, 動的な経路変更にも対応できます。この章では, uRPF 機能の解説と操作方法について説明します。

7.1　解説

uRPF（Unicast Reverse Path Forwarding）はフィルタ機能の一種です。通常のフィルタ機能が遮断したいトラフィックの種別をリスト形式で記述しなければならないのに対して，uRPF ではフィルタを実施したいインタフェースを指定するだけなので，設定が簡易であるという特長があります。

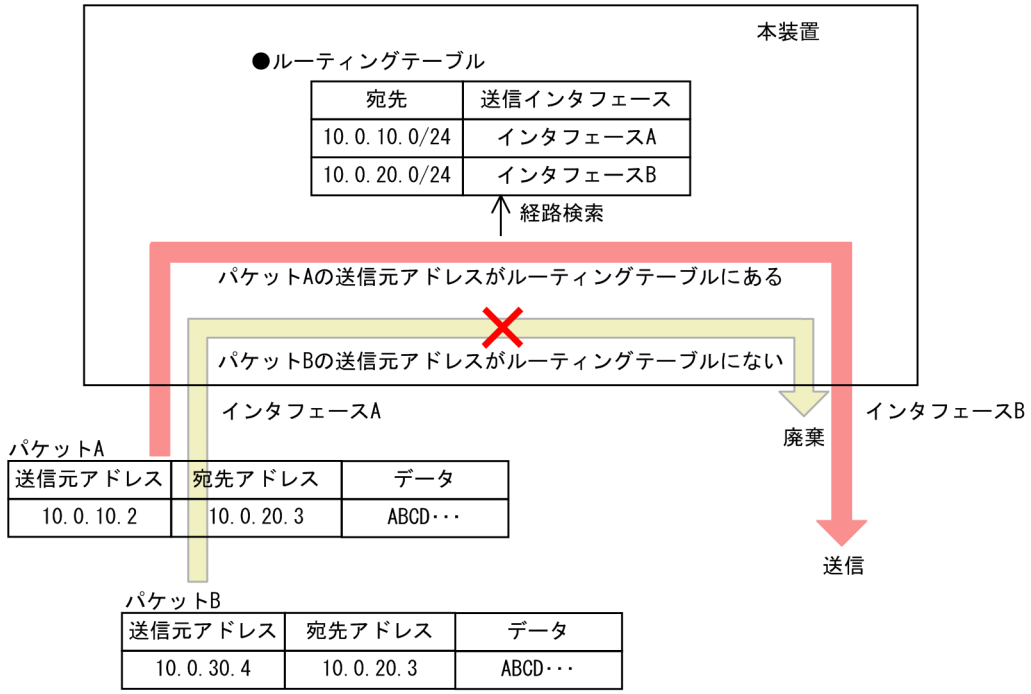
受信パケットの廃棄判定は，パケットの送信元アドレスが妥当かどうかを検証することで行われ，主に DoS 攻撃でよく見られる成りすましパケットの防御手段となります。

uRPF の廃棄対象となるパケットは IPv4 パケットおよび IPv6 パケットです。

7.1.1　uRPF の概要

uRPF は，受信パケットの送信元アドレスを装置のルーティングテーブルから検索して，ルーティングテーブルと不整合であればパケットを廃棄します。uRPF の動作概要を次の図に示します。

図 7-1　uRPF の動作概要



この図では，パケット A 受信時に uRPF が有効であれば，本装置はパケット A の送信元アドレス 10.0.10.2 をルーティングテーブルから検索します。ルーティングテーブルに 10.0.10.2 に一致する経路が存在するため，本装置はパケット A を正当なパケットと見なし，通常の経路検索によって中継します。次項で説明している Strict モードではさらにインタフェースの妥当性も検証します。

パケット B 受信時は，パケット B の送信元アドレス 10.0.30.4 をルーティングテーブルから検索しますが，一致する経路が存在しないため，パケット B は廃棄されます。

7.1.2　サポートモード

本装置の uRPF でサポートしているモードを次に示します。本装置では，インタフェース単位にモードを指定でき，さらに IPv4／IPv6 プロトコルごとに有効または無効を指定できます。

1. Strict モード

   受信パケットの送信元アドレスがルーティングテーブルに存在して，かつ該当する経路で指定されている送信インタフェースが受信インタフェースと一致した場合だけ，パケットを受信可能とします。

2. Loose モード

   受信パケットの送信元アドレスがルーティングテーブルに存在するかどうかだけで受信可・不可を判定して，インタフェースの妥当性は検証しません。

各モードで送信元アドレスの経路検索のときに，デフォルト経路を検索対象にするかどうかを設定できます。さらに，送信元アドレスが未指定アドレス（IPv4 では「0.0.0.0」，IPv6 では「::」）の受信パケットを uRPF の対象外にするかどうかを設定できます。

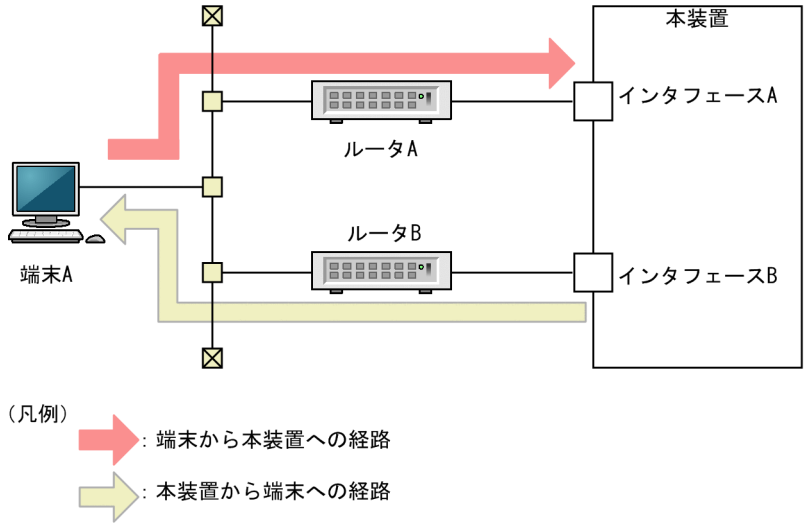
なお，デフォルト経路検索対象設定および未指定アドレス対象外設定は装置全体で有効となります。

7.1.3　uRPF 使用時の注意事項

(1)　Strict モード使用時の注意

Strict モード使用時は，受信インタフェースと送信元アドレスの経路で指定した送信インタフェースが一致するかどうかも検証されます。したがって，次の図に示すように，本装置と隣接ルータ A および B 間で経路が非対称になるような場合，廃棄対象にしてはならないパケットも廃棄されることがあります。

図 7-2　非対称経路の例



この図では，本装置のルーティングテーブルに，端末 A 宛ての経路として送信インタフェースはインタフェース B であることが登録されているため，ルータ B を経由して中継されます。端末側では，本装置宛てまたは本装置を経由する宛先の経路がルータ A を経由するように設定されているため，端末 A からのパケットは本装置のインタフェース A で受信されます。

本装置のインタフェース A で uRPF の Strict モードを設定した場合，ルーティングテーブルの検索結果であるインタフェース B 以外から受信するため，端末 A からのパケットは廃棄されます。

ただし，ロードバランスのためのマルチパスによって受信インタフェースと送信インタフェースが異なる場合は，出力対象のパスをすべて検証するため問題ありません。

(2)　ロードバランス機能との併用について

本装置では uRPF とロードバランス機能を併用する場合，マルチパス最大数が 8 に制限されます。uRPF を設定するとき，各種ルーティングプロトコルで 9 以上のマルチパス設定が存在すると設定できないため，マルチパス設定を 8 以下に設定し直す必要があります。

マルチパス数の設定変更直後は，経路数が多い場合など，本装置のハードウェアルーティングテーブルにマルチパス経路が再設定されるのに時間が掛かることがあり，uRPF が誤動作するおそれがあります。マルチパス数を変更する必要がある場合は，装置を再起動することをお勧めします。

(3)　フィルタ，QoS フロー，ポリシーベースルーティングとの同時使用について

本装置では，uRPF とフィルタ，QoS フロー，ポリシーベースルーティングは同時に動作できます。パケットがフィルタ，QoS フロー，ポリシーベースルーティングと，uRPF の両方で評価される場合，廃棄のアクションが優先されます。したがって，フィルタ，QoS フロー，ポリシーベースルーティングの検索結果が廃棄以外のアクションであっても，uRPF で廃棄となった場合，そのパケットは廃棄されます。

uRPF とフィルタ，QoS フロー，ポリシーベースルーティングを同時に使用した場合の統計情報を次の表に示します。

表 7-1　uRPF とフィルタ，QoS フロー，ポリシーベースルーティングを同時に使用した場合の統計情報

フロー検出条件による パケット検索結果	uRPF によるパケット検索結果			
	通過		廃棄	
一致	uRPF の廃棄統計情報	×	uRPF の廃棄統計情報	○
	フロー検出条件に一致したフレームの統計情報	○	フロー検出条件に一致したフレームの統計情報	×
不一致	uRPF の廃棄統計情報	×	uRPF の廃棄統計情報	○
	フロー検出条件に一致したフレームの統計情報	×	フロー検出条件に一致したフレームの統計情報	×

（凡例）○：カウントされる　×：カウントされない

なお，uRPF によるフィルタ，QoS フロー，ポリシーベースルーティングへの影響については，「コンフィグレーションガイド Vol.2　9. フィルタ」，「コンフィグレーションガイド Vol.2　12. QoS フロー」，または「8　ポリシーベースルーティング」を参照してください。

7.2 コンフィグレーション

7.2.1 コンフィグレーションコマンド一覧

uRPF のコンフィグレーションコマンド一覧を次の表に示します。

表 7-2 コンフィグレーションコマンド一覧

コマンド名	説明
ip urpf	装置全体で uRPF を使用可能にします。
ip verify unicast source reachable-via	インタフェースで IPv4 の uRPF を使用します。
ipv6 verify unicast source reachable-via	インタフェースで IPv6 の uRPF を使用します。

7.2.2 装置全体での uRPF 設定

装置全体で uRPF を有効にするための設定例を次に示します。

[設定のポイント]

uRPF はインタフェース単位で設定しますが, その前に装置全体で uRPF を有効にする必要があります。装置全体で uRPF が有効になっていない場合, インタフェースで uRPF を設定しても無効になり装置には反映されません。また, 本設定時には, 各ルーティングプロトコルでマルチパス数が 8 以下に設定されている必要があります。

[コマンドによる設定]

1. **(config)# ip urpf**
   装置全体で uRPF を有効にします。

7.2.3 インタフェース単位での uRPF 設定

各インタフェースで uRPF を有効にするための設定例を次に示します。

[設定のポイント]

インタフェース単位で uRPF を有効にします。本設定の前に, 装置全体で uRPF が有効になっている必要があります。また, IPv4 と IPv6 の両方で uRPF を有効にする場合, インタフェースごとにモードを合わせる必要があります。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   ポート 1/1 のコンフィグレーションモードに移行します。
2. **(config-if)# ip verify unicast source reachable-via rx**
   ポート 1/1 に Strict モードで IPv4 の uRPF を設定します。
3. **(config-if)# ipv6 verify unicast source reachable-via rx**
   ポート 1/1 に Strict モードで IPv6 の uRPF を設定します。

7.3 オペレーション

7.3.1 運用コマンド一覧

uRPF の運用コマンド一覧を次の表に示します。

表 7-3 運用コマンド一覧

コマンド名	説明
show ip urpf statistics	uRPF（IPv4）の設定状態および廃棄統計情報を表示します。
show ipv6 urpf statistics	uRPF（IPv6）の設定状態および廃棄統計情報を表示します。
clear ip urpf statistics	uRPF（IPv4）の廃棄統計情報のカウンタをクリアします。
clear ipv6 urpf statistics	uRPF（IPv6）の廃棄統計情報のカウンタをクリアします。

7.3.2 装置全体での uRPF 設定状態および廃棄パケット数確認

show ip urpf statistics コマンドまたは show ipv6 urpf statistics コマンドで，装置全体での uRPF 設定状態および廃棄パケット数を確認できます。コマンドの実行結果を次に示します。

図 7-3 装置全体での uRPF 設定状態および廃棄パケット数確認（IPv4）

```
> show ip urpf statistics
Date 20XX/06/14 12:00:00 UTC
uRPF: enable
Allowing default route (IPv4)         : on
Ignoring unspecified address(0.0.0.0) : on
Statistics
  Discarded IPv4 packets (strict mode):                  222
  Discarded IPv4 packets (loose mode) :                    0
```

図 7-4 装置全体での uRPF 設定状態および廃棄パケット数確認（IPv6）

```
> show ipv6 urpf statistics
Date 20XX/06/14 12:00:00 UTC
uRPF: enable
Allowing default route (IPv6)         : on
Ignoring unspecified address(::)      : off
Statistics
  Discarded IPv6 packets (strict mode):                    0
  Discarded IPv6 packets (loose mode) :                13902
```

7.3.3 インタフェースごとの uRPF 設定状態および廃棄パケット数確認

show ip urpf statistics コマンドまたは show ipv6 urpf statistics コマンドで interface パラメータを指定すると，インタフェースごとの uRPF 設定状態および廃棄パケット数を確認できます。コマンドの実行結果を次に示します。

図 7-5 インタフェースごとの uRPF 設定状態および廃棄パケット数確認（IPv4）

```
> show ip urpf statistics interface gigabitethernet 1/1
Date 20XX/07/07 19:31:00 UTC
Interface Name: Eth1/1
  uRPF(IPv4)  : enable
  Mode        : strict
  Statistics
    Discarded IPv4 packets:                1615
```

図 7-6 インタフェースごとの uRPF 設定状態および廃棄パケット数確認（IPv6）

```
> show ipv6 urpf statistics interface gigabitethernet 1/1
Date 20XX/07/06 09:16:00 UTC
Interface Name: Eth1/1
  uRPF(IPv6)  : enable
  Mode        : loose
  Statistics
    Discarded IPv6 packets:                 268
```

8 ポリシーベースルーティング

この章では，IPv4 パケットおよび IPv6 パケットを対象とするポリシーベースルーティングの解説と操作方法について説明します。

8.1　解説

8.1.1　概要

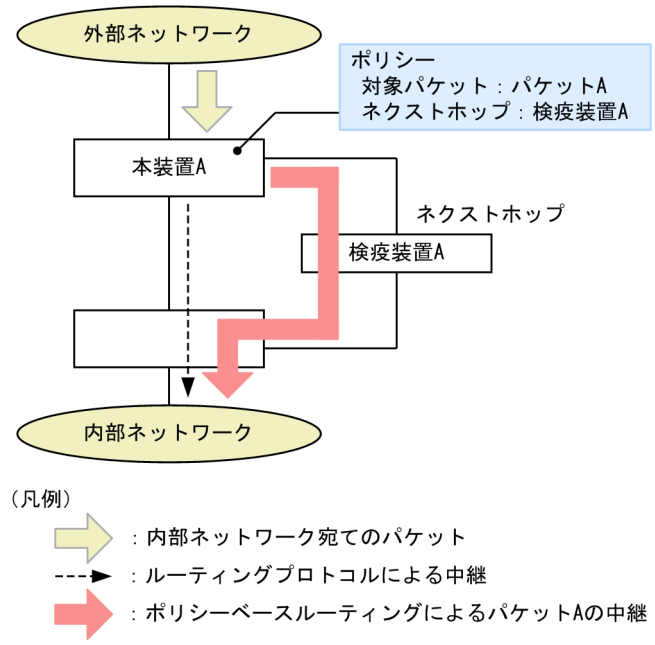
本装置のポリシーベースルーティングは，フィルタの機能を使用して，ユーザの任意のポリシーに従ってパケットを中継する機能です。ユーザの任意のポリシーとして，対象パケットとネクストホップをコンフィグレーションで指定できます。

ポリシーベースルーティングはルーティングプロトコルよりも優先して動作します。また，本機能では異なる VRF 間でパケットを中継できます。

(1)　ポリシーベースルーティングの基本動作

ポリシーベースルーティングの基本動作を次の図に示します。

図 8-1　ポリシーベースルーティングの基本動作



本装置 A は，外部ネットワークからのパケットをルーティングプロトコルによって内部ネットワークに中継します。

内部ネットワークのセキュリティを確保するために外部ネットワークからのパケット A を検疫する場合，対象パケットをパケット A，ネクストホップを検疫装置 A とするポリシーを設定します。このポリシーに従ったポリシーベースルーティングによって，検疫装置 A を経由してパケット A を内部ネットワークに中継できます。

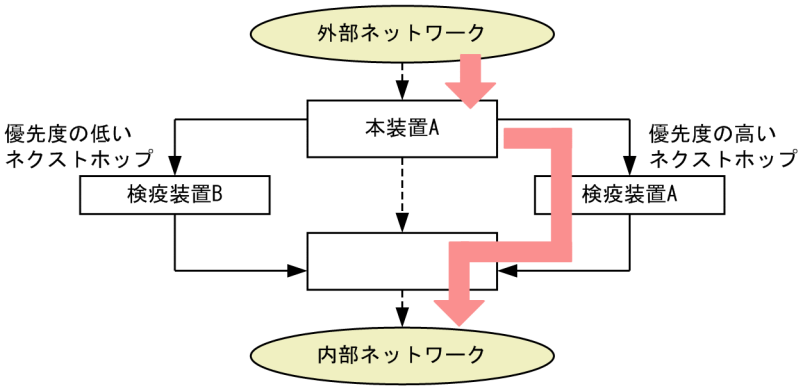
このようにポリシーベースルーティングでは，ユーザの任意のポリシーに従ってパケット種別ごとに任意の経路を経由させられます。そのため，セキュリティの確保，負荷分散，認証などに適用できます。

(2)　ポリシーベースルーティングの冗長化

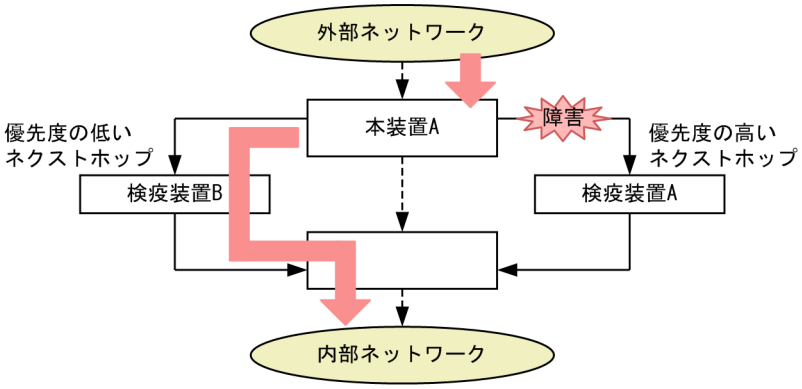
ポリシーベースルーティングでは，ネクストホップを冗長化できます。中継先となるネクストホップは，冗長化したネクストホップの中から送信先インタフェースの状態と優先度によって自動で選択されます。ネクストホップを冗長化したポリシーベースルーティングの動作を次の図に示します。

図 8-2　ネクストホップを冗長化したポリシーベースルーティングの動作

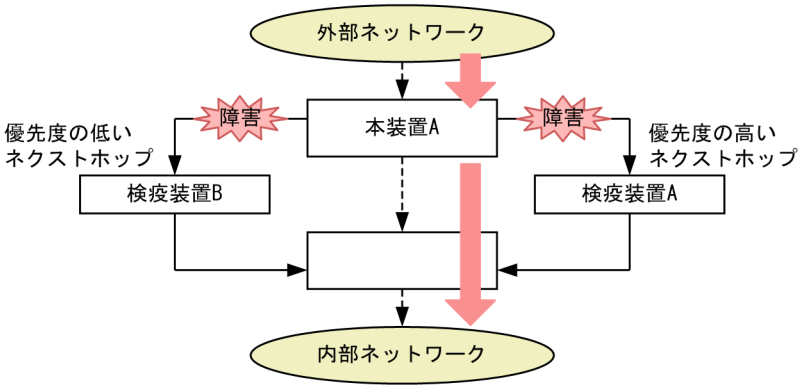
1. 通常時



2. 優先度の高いネクストホップで障害が発生した場合



3. 優先度の低いネクストホップでも障害が発生した場合



（凡例）
：ポリシーベースルーティングによる経路
：ルーティングプロトコルによる経路
：ポリシーベースルーティングの対象パケット

1. 本装置 A は，外部ネットワークからのパケットを冗長化したネクストホップのうち優先度の高いネクストホップ（検疫装置 A 宛て）へ中継します。
2. 優先度の高いネクストホップ（検疫装置 A 宛て）が障害によって中継できなくなった場合，冗長化している優先度の低いネクストホップ（検疫装置 B 宛て）に切り替えて中継します。

3. 優先度の高いネクストホップ（検疫装置 A 宛て）に加えて，優先度の低いネクストホップ（検疫装置 B 宛て）も障害によって中継できなくなった場合，コンフィグレーションで指定したデフォルト動作に従います（ルーティングプロトコルに従った中継，または廃棄）。

このようにネクストホップを冗長化すると，障害発生時などでも運用を継続できます。

8.1.2　対象パケット

ポリシーベースルーティングでは，対象パケットをフィルタのフロー検出条件で検出します。ポリシーベースルーティングの対象パケットを次の表に示します。

表 8-1　ポリシーベースルーティングの対象パケット

パケット種別	対象パケット		サポート対象
IPv4 パケット	ユニキャスト	中継	○
		自宛※1	―※2
		自発	―
	マルチキャスト		―※2
	制限付きブロードキャスト		―※2
	ダイレクトブロードキャスト		○
IPv6 パケット	ユニキャスト	中継	○
		自宛※3	―※2
		自発	―
	マルチキャスト		―※2
上記以外のパケット			―

（凡例）○：対象　―：対象外

注※1

マネージメントポートを経由するパケット，および受信側インタフェースへのサブネットブロードキャスト宛てパケットも含みます。

注※2

フロー検出条件のコンフィグレーションで指定できますが，ポリシーベースルーティングの対象パケットとして検出しません。

注※3

マネージメントポートを経由するパケット，およびリンクローカルアドレス宛てパケットも含みます。

8.1.3　ネクストホップ

ポリシーベースルーティングのネクストホップは，送信先インタフェースおよびネクストホップアドレスで指定します。

(1)　送信先インタフェース

送信先インタフェースとは，対象パケットを送信するインタフェースです。送信先インタフェースに指定できるインタフェース種別を次の表に示します。

表 8-2　送信先インタフェースに指定できるインタフェース種別

インタフェース種別	指定可否
イーサネットインタフェース	○
イーサネットサブインタフェース	○
ポートチャネルインタフェース	○
ポートチャネルサブインタフェース	○
VLAN インタフェース	○※
ループバックインタフェース	－
Null インタフェース	－
マネージメントポート	－
AUX ポート	－

（凡例）○：指定できる　－：指定できない

注※

MAC アドレスを学習していない場合，VLAN に所属する全ポートへ中継します。

(2)　ネクストホップアドレス

ネクストホップアドレスとは，対象パケットの中継先となる宛先装置のアドレスです。ネクストホップアドレスに指定できるアドレス種別を次の表に示します。

表 8-3　ネクストホップアドレスに指定できるアドレス種別

パケット種別	アドレス種別	指定可否
IPv4 パケット	ユニキャスト	○※
	マルチキャスト	－
	制限付きブロードキャスト	－
	送信先インタフェースに接続するネットワークへのダイレクトブロードキャスト	－
IPv6 パケット	ユニキャスト（非リンクローカル）	○※
	ユニキャスト（リンクローカル）	○
	マルチキャスト	－

（凡例）○：指定できる　－：指定できない

注※

送信先インタフェースに指定しているアドレスと同一ネットワークのホストアドレスだけ指定できます。

8.1.4　ネクストホップの冗長化

ポリシーベースルーティングは，複数のネクストホップを指定することで冗長化できます。

冗長化したネクストホップの中から，ネクストホップの選択動作によって中継先となるネクストホップを決定します。ネクストホップがすべて中継できない，またはネクストホップが指定されていない場合は，デフォルト動作に従います。なお，ネクストホップの選択動作は抑止できます。

(1)　ネクストホップの選択動作

冗長化したネクストホップの中から，次の情報を基に中継先となるネクストホップを決定します。

- 本装置の送信先インタフェースの状態による中継可否
- ネクストホップの優先度

中継できるネクストホップが複数ある場合，常に最も優先度の高いネクストホップを中継先として選択します。

● 送信先インタフェースの状態による中継可否

送信先インタフェースの状態による中継可否を次の表に示します。

表 8-4　送信先インタフェースの状態による中継可否

送信先インタフェースの状態	中継可否
Up	中継できる
Down	中継できない

● ネクストホップの優先度

ネクストホップの優先度は，優先して使用するネクストホップを決定するために使用します。

(2)　デフォルト動作

ネクストホップがすべて中継できない，またはネクストホップが指定されていない場合の動作をデフォルト動作といいます。デフォルト動作はコンフィグレーションで指定できます。デフォルト動作指定について次の表に示します。

表 8-5　デフォルト動作指定

コンフィグレーションでの指定	動作説明
permit 指定	対象パケットをルーティングプロトコルに従って中継します
deny 指定	対象パケットを廃棄します
未指定	対象パケットをルーティングプロトコルに従って中継します

(3)　ネクストホップの選択抑止

系切替後，ネクストホップの選択動作を一定時間抑止します。これは，系切替後，送信先インタフェースの状態を中継不可と判断することがあるためです。

系切替してからネクストホップの選択を再開するまでの状態を選択抑止中といいます。選択抑止中は，系切替前に選択していたネクストホップで動作します。なお，ネクストホップの選択を抑止する時間は，コンフィグレーションで変更できます。

(a)　選択抑止中の動作

系切替を検知すると，ネクストホップの選択抑止を開始します。選択抑止中の装置の状態変化に対する動作を次の表に示します。

表 8-6　選択抑止中の装置の状態変化に対する動作

装置の状態変化	動作説明
対象パケットに関するコンフィグレーションの設定および変更	次のどれかの動作になります。 • 対象パケットを検出する条件を変更した場合，ルーティングプロトコルに従って中継します。 • 系切替後に設定したネクストホップを指定した場合，ルーティングプロトコルに従って中継します。 • 系切替前に動作していたネクストホップを指定した場合，系切替前に動作していたネクストホップに中継します。
ネクストホップに関するコンフィグレーションの設定および変更	選択抑止前に選択していたネクストホップに従います。次に示すコマンドでコンフィグレーションを設定および変更しても，ネクストホップを選択しません。 • default • ip policy-list • ipv6 policy-list • policy-interface
送信先インタフェースの状態変化	選択抑止前に選択していたネクストホップに従います。送信先インタフェースの状態が変化しても，ネクストホップを選択しません。
対象パケットを受信する PRU の再起動	再起動後の PRU で受信する対象パケットは，すべてルーティングプロトコルに従って中継します。
選択抑止中の終了	選択抑止中の終了時の装置状態に合わせて，ネクストホップを再選択します。

(b)　選択抑止中の終了と延長

系切替後の選択抑止中の状態遷移と遷移条件について次の表に示します。

表 8-7　選択抑止中の状態遷移と遷移条件

状態遷移	遷移条件
選択抑止中の終了	次の場合に選択抑止中を終了します。 • ネクストホップの選択抑止時間の経過 • ネクストホップの選択抑止時間を現在の経過時間よりも短く変更 • ポリシーベースルーティング制御プログラムの再起動
選択抑止中の延長	ネクストホップの選択抑止時間をより長く変更すると選択抑止中を延長します。この場合，変更後の時間から現在の経過時間を差し引いた時間が経過すると，選択抑止中を終了します。 また，系切替が再度発生すると選択抑止時間をカウントし直すため，選択抑止中を継続します。

(c)　選択抑止時間

ネクストホップの選択抑止に必要な時間は，ネットワーク構成によって異なります。コンフィグレーションでネットワーク構成に合わせて調整してください。

8.1.5　対象パケットとネクストホップの指定方法

(1)　対象パケットの指定方法

ポリシーベースルーティングの対象パケットは，アクセスリストで指定します。アクセスリストとポリシーベースルーティングの関係を次の表に示します。

表 8-8　アクセスリストとポリシーベースルーティングの関係

アクセスリスト		ポリシーベースルーティングの指定可否
MAC 条件	受信側	－
	送信側	－
IPv4 条件	受信側	○※
	送信側	－
IPv6 条件	受信側	○
	送信側	－
Advance 条件	受信側	○
	送信側	－

（凡例）○：指定できる　－：指定できない

注※

IPv4 パケットフィルタだけ指定できます。

(2)　ネクストホップの指定方法

ポリシーベースルーティングのネクストホップは，ポリシーベースルーティングリストで指定します。
IPv4 パケットを対象パケットとする場合は IPv4 ポリシーベースルーティングリスト，IPv6 パケットを対象パケットとする場合は IPv6 ポリシーベースルーティングリストで指定します。

8.1.6　注意事項

(1)　ポリシーベースルーティングリストとアクセスリストの設定順序

ポリシーベースルーティングリストと，そのポリシーベースルーティングリストを動作に指定しているアクセスリストを設定する場合は，手動コミットモードで同時に設定したり，逐次コミットモードで連続して設定したりしないでください。

ポリシーベースルーティングリストを設定したあと，しばらくしてからアクセスリストを設定してください。

(2)　デフォルト動作で対象パケットを廃棄している場合の統計について

ネクストホップにデフォルト動作が選択されていて，かつデフォルト動作に deny を指定している場合の廃棄パケット数は，IPv4 パケットを対象としたポリシーベースルーティングでは運用コマンド show ip interface，IPv6 パケットを対象としたポリシーベースルーティングでは運用コマンド show ipv6 interface で確認できます。

(3)　ネクストホップの選択抑止中の終了時について

系切替後，選択抑止中を終了するとネクストホップを再選択しますが，ネクストホップの選択によるシステムメッセージを出力しません。なお，ネクストホップの選択抑止の終了時刻は，運用コマンド show ip cache policy または show ipv6 cache policy で確認できます。

(4)　uRPF との併用について

uRPF で廃棄対象となるパケットがポリシーベースルーティングの対象となる場合，該当パケットを uRPF によって廃棄します。このとき，ポリシーベースルーティングは動作しません。

(5)　ポリサーとの併用について

ポリシーベースルーティングの対象パケットがポリサーによる監視結果で違反フレームとなった場合，ポリシーベースルーティングの統計情報にはカウントしないで，違反フレームをポリサーによって廃棄します。

(6)　sFlow 統計との併用について

sFlow 統計のフローサンプル収集の対象パケットがポリシーベースルーティングの対象となる場合，ポリシーベースルーティングの中継動作に従いますが，sFlow 統計で採取する情報のうち，次の情報はルーティングプロトコルに従った中継先の経路情報となります。

- ルータ型のフォーマットのうち，nexthop および dst_mask
- ゲートウェイ型のフォーマットのうち，dst_peer_as および dst_as

8.2　コンフィグレーション

8.2.1　コンフィグレーションコマンド一覧

ポリシーベースルーティングのコンフィグレーションコマンド一覧を次の表に示します。

表 8-9　コンフィグレーションコマンド一覧

コマンド名	説明
default	ポリシーベースルーティングリスト内のすべてのネクストホップが中継できない場合，またはポリシーベースルーティングリストにネクストホップが設定されていない場合のデフォルト動作を指定します。
ip policy-list	IPv4 ポリシーベースルーティングリストを設定します。
ip policy-list rearrange	IPv4 ポリシーベースルーティングリスト内に設定しているネクストホップの優先度の値を等間隔に再設定します。
ipv6 policy-list	IPv6 ポリシーベースルーティングリストを設定します。
ipv6 policy-list rearrange	IPv6 ポリシーベースルーティングリスト内に設定しているネクストホップの優先度の値を等間隔に再設定します。
policy-based-routing suspend-update	ポリシーベースルーティングでネクストホップの選択を抑止する時間を設定します。
policy-interface	ポリシーベースルーティングリストにネクストホップを設定します。
advance access-group※	ポリシーベースルーティングの対象パケットを Advance フィルタで検出するインタフェースを指定します。
advance access-list※	ポリシーベースルーティングの対象パケットを Advance フィルタで検出するアクセスリストを設定します。
ip access-group※	ポリシーベースルーティングの対象パケットを IPv4 パケットフィルタで検出するインタフェースを指定します。
ip access-list extended※	ポリシーベースルーティングの対象パケットを IPv4 パケットフィルタで検出するアクセスリストを設定します。
ipv6 access-list※	ポリシーベースルーティングの対象パケットを IPv6 フィルタで検出するアクセスリストを設定します。
ipv6 traffic-filter※	ポリシーベースルーティングの対象パケットを IPv6 フィルタで検出するインタフェースを指定します。
permit※	対象パケットを検出するフロー検出条件と，対象パケットの中継先となるポリシーベースルーティングリストを，アクセスリストに指定します。

注※

「コンフィグレーションコマンドレファレンス Vol.2　7. アクセスリスト」を参照してください。

8.2.2　IPv4 パケットを対象としたポリシーベースルーティングの設定

ポリシーベースルーティングの対象パケット，および対象パケットの中継先となるポリシーベースルーティングリストは，IPv4 パケットを対象パケットとしたアクセスリストで指定します。ネクストホップおよびネクストホップの冗長化は，IPv4 ポリシーベースルーティングリストで設定します。

(1)　基本設定

IPv4 パケットを対象としたポリシーベースルーティングの基本設定例を次に示します。

[設定のポイント]

IPv4 ポリシーベースルーティングリストにネクストホップを設定します。次に，IPv4 パケットを対象パケットとしたアクセスリストを設定します。

[コマンドによる設定]

1. **(config)# ip policy-list POLICY_LIST_IPv4_A**
   IPv4 ポリシーベースルーティングリスト（POLICY_LIST_IPv4_A）を作成します。本リストを作成すると，IPv4 ポリシーベースルーティングリストのモードに移行します。
2. **(config-ip-pbr)# policy-interface gigabitethernet 2/1 next-hop 192.168.10.10**
   IPv4 ポリシーベースルーティングリストにネクストホップとしてイーサネットインタフェース 2/1，ネクストホップアドレス 192.168.10.10 を設定します。
3. **(config-ip-pbr)# exit**
   IPv4 ポリシーベースルーティングリストのモードからグローバルコンフィグレーションモードに戻ります。
4. **(config)# ip access-list extended IPv4_POLICY_A**
   IPv4 アクセスリスト（IPv4_POLICY_A）を作成します。本リストを作成すると，IPv4 パケットフィルタの動作モードに移行します。
5. **(config-ext-nacl)# permit tcp any any action policy-list POLICY_LIST_IPv4_A**
   IPv4 パケットに対して IPv4 ポリシーベースルーティングリスト（POLICY_LIST_IPv4_A）を設定します。
6. **(config-ext-nacl)# permit ip any any**
   すべてのパケットを中継する IPv4 パケットフィルタを設定します。
7. **(config-ext-nacl)# exit**
   IPv4 パケットフィルタの動作モードからグローバルコンフィグレーションモードに戻ります。
8. **(config)# interface gigabitethernet 1/1**
   (config-if)# ip access-group IPv4_POLICY_A in
   イーサネットインタフェース 1/1 の受信側に IPv4 アクセスリスト（IPv4_POLICY_A）を適用します。

(2)　冗長化設定

IPv4 パケットを対象としたポリシーベースルーティングの冗長化設定例を次に示します。

[設定のポイント]

IPv4 ポリシーベースルーティングリストに複数のネクストホップを設定します。次に，IPv4 パケットを対象パケットとしたアクセスリストを設定します。なお，ネクストホップの優先度指定を省略した場合は，優先度を自動で割り当てます。

[コマンドによる設定]

1. **(config)# ip policy-list POLICY_LIST_IPv4_B**
   IPv4 ポリシーベースルーティングリスト（POLICY_LIST_IPv4_B）を作成します。本リストを作成すると，IPv4 ポリシーベースルーティングリストのモードに移行します。
2. **(config-ip-pbr)# 10 policy-interface port-channel 100 next-hop 192.168.100.10**
   IPv4 ポリシーベースルーティングリストに優先度の高いネクストホップ（優先度の値 10）としてポートチャネルインタフェース 100，ネクストホップアドレス 192.168.100.10 を設定します。
3. **(config-ip-pbr)# 20 policy-interface port-channel 200 next-hop 192.168.200.10**
   IPv4 ポリシーベースルーティングリストに冗長用のネクストホップ(優先度の値 20)としてポートチャネルインタフェース 200，ネクストホップアドレス 192.168.200.10 を設定します。
4. **(config-ip-pbr)# default deny**
   IPv4 ポリシーベースルーティングリストのデフォルト動作に deny（廃棄）を設定します。
5. **(config-ip-pbr)# exit**
   IPv4 ポリシーベースルーティングリストのモードからグローバルコンフィグレーションモードに戻ります。
6. **(config)# ip access-list extended IPv4_POLICY_B**
   IPv4 アクセスリスト（IPv4_POLICY_B）を作成します。本リストを作成すると，IPv4 パケットフィルタの動作モードに移行します。
7. **(config-ext-nacl)# permit ip any 192.168.1.10 0.0.0.255 action policy-list POLICY_LIST_IPv4_B**
   宛先 IPv4 アドレス 192.168.1.10 へのパケットに対して IPv4 ポリシーベースルーティングリスト（POLICY_LIST_IPv4_B）を設定します。
8. **(config-ext-nacl)# permit ip any any**
   すべてのパケットを中継する IPv4 パケットフィルタを設定します。
9. **(config-ext-nacl)# exit**
   IPv4 パケットフィルタの動作モードからグローバルコンフィグレーションモードに戻ります。
10. **(config)# interface port-channel 10.1**
    (config-subif)# ip access-group IPv4_POLICY_B in
    ポートチャネルサブインタフェース 10.1 の受信側に IPv4 アクセスリスト（IPv4_POLICY_B）を適用します。

8.2.3　IPv6 パケットを対象としたポリシーベースルーティングの設定

ポリシーベースルーティングの対象パケット，および対象パケットの中継先となるポリシーベースルーティングリストは，IPv6 パケットを対象パケットとしたアクセスリストで指定します。ネクストホップおよびネクストホップの冗長化は，IPv6 ポリシーベースルーティングリストで設定します。

(1)　基本設定

IPv6 パケットを対象としたポリシーベースルーティングの基本設定例を次に示します。

[設定のポイント]

IPv6 ポリシーベースルーティングリストにネクストホップを設定します。次に，IPv6 パケットを対象パケットとしたアクセスリストを設定します。

[コマンドによる設定]

1. **(config)# ipv6 policy-list POLICY_LIST_IPv6_A**
   IPv6 ポリシーベースルーティングリスト（POLICY_LIST_IPv6_A）を作成します。本リストを作成すると，IPv6 ポリシーベースルーティングリストのモードに移行します。
2. **(config-ipv6-pbr)# policy-interface gigabitethernet 2/2 next-hop 2001:db8:10::100**
   IPv6 ポリシーベースルーティングリストにネクストホップとしてイーサネットインタフェース 2/2, ネクストホップアドレス 2001:db8:10::100 を設定します。
3. **(config-ipv6-pbr)# exit**
   IPv6 ポリシーベースルーティングリストのモードからグローバルコンフィグレーションモードに戻ります。
4. **(config)# ipv6 access-list IPv6_POLICY_A**
   IPv6 アクセスリスト（IPv6_POLICY_A）を作成します。本リストを作成すると，IPv6 フィルタの動作モードに移行します。
5. **(config-ipv6-acl)# permit udp any any action policy-list POLICY_LIST_IPv6_A**
   IPv6 パケットに対して IPv6 ポリシーベースルーティングリスト（POLICY_LIST_IPv6_A）を設定します。
6. **(config-ipv6-acl)# permit ipv6 any any**
   すべてのパケットを中継する IPv6 フィルタを設定します。
7. **(config-ipv6-acl)# exit**
   IPv6 フィルタの動作モードからグローバルコンフィグレーションモードに戻ります。
8. **(config)# interface gigabitethernet 1/2**
   (config-if)# ipv6 traffic-filter IPv6_POLICY_A in
   イーサネットインタフェース 1/2 の受信側に IPv6 アクセスリスト（IPv6_POLICY_A）を適用します。

(2)　冗長化設定

IPv6 パケットを対象としたポリシーベースルーティングの冗長化設定例を次に示します。

[設定のポイント]

IPv6 ポリシーベースルーティングリストに複数のネクストホップを設定します。次に，IPv6 パケットを対象パケットとしたアクセスリストを設定します。なお，ネクストホップの優先度指定を省略した場合は，優先度を自動で割り当てます。

[コマンドによる設定]

1. **(config)# ipv6 policy-list POLICY_LIST_IPv6_B**
   IPv6 ポリシーベースルーティングリスト（POLICY_LIST_IPv6_B）を作成します。本リストを作成すると，IPv6 ポリシーベースルーティングリストのモードに移行します。
2. **(config-ipv6-pbr)# 10 policy-interface port-channel 100 next-hop 2001:db8:100::100**
   IPv6 ポリシーベースルーティングリストに優先度の高いネクストホップ（優先度の値 10）としてポートチャネルインタフェース 100，ネクストホップアドレス 2001:db8:100::100 を設定します。
3. **(config-ipv6-pbr)# 20 policy-interface port-channel 200 next-hop 2001:db8:200::100**
   IPv6 ポリシーベースルーティングリストに冗長用のネクストホップ(優先度の値 20)としてポートチャネルインタフェース 200，ネクストホップアドレス 2001:db8:200::100 を設定します。
4. **(config-ipv6-pbr)# default deny**

IPv6 ポリシーベースルーティングリストのデフォルト動作に deny（廃棄）を設定します。

5. **(config-ipv6-pbr)# exit**

   IPv6 ポリシーベースルーティングリストのモードからグローバルコンフィグレーションモードに戻ります。

6. **(config)# ipv6 access-list IPv6_POLICY_B**

   IPv6 アクセスリスト（IPv6_POLICY_B）を作成します。本リストを作成すると，IPv6 フィルタの動作モードに移行します。

7. **(config-ipv6-acl)# permit ipv6 any 2001:db8:1::/64 action policy-list POLICY_LIST_IPv6_B**

   宛先 IPv6 アドレス 2001:db8:1::/64 へのパケットに対して IPv6 ポリシーベースルーティングリスト（POLICY_LIST_IPv6_B）を設定します。

8. **(config-ipv6-acl)# permit ipv6 any any**

   すべてのパケットを中継する IPv6 フィルタを設定します。

9. **(config-ipv6-acl)# exit**

   IPv6 フィルタの動作モードからグローバルコンフィグレーションモードに戻ります。

10. **(config)# interface port-channel 10.1**

    (config-subif)# ipv6 traffic-filter IPv6_POLICY_B in

    ポートチャネルサブインタフェース 10.1 の受信側に IPv6 アクセスリスト（IPv6_POLICY_B）を適用します。

8.2.4　異なる VRF 間でのポリシーベースルーティングの設定

異なる VRF 間でのポリシーベースルーティングの設定例を次に示します。

[設定のポイント]

対象パケットを受信するインタフェースと送信先インタフェースを異なる VRF にすると，複数の VRF にわたるポリシーベースルーティングができます。

[コマンドによる設定]

1. **(config)# vrf definition 2**
   (config-vrf)# exit
   (config)# interface gigabitethernet 1/2
   (config-if)# vrf forwarding 2
   (config-if)# ip address 192.168.20.1 255.255.255.0
   (config-if)# exit

   イーサネットインタフェース 1/2 に VRF2 と IPv4 アドレスを設定します。

2. **(config)# vrf definition 3**
   (config-vrf)# exit
   (config)# interface gigabitethernet 1/3
   (config-if)# vrf forwarding 3
   (config-if)# ip address 192.168.30.1 255.255.255.0
   (config-if)# exit

   イーサネットインタフェース 1/3 に VRF3 と IPv4 アドレスを設定します。

3. **(config)# ip policy-list EX_POLICY_TO_VRF3**

```
(config-ip-pbr)# policy-interface gigabitethernet 1/3 next-hop 192.168.30.10
(config-ip-pbr)# default deny
(config-ip-pbr)# exit
```

IPv4 ポリシーベースルーティングリスト（EX_POLICY_TO_VRF3）を作成して，ネクストホップとして VRF3 のインタフェースを設定します。

4.
```
(config)# ip access-list extended EXTRA_NET_POLICY_VRF_2_TO_3
(config-ext-nacl)# permit ip any 192.168.30.0 0.0.0.255 action policy-list
EX_POLICY_TO_VRF3
(config-ext-nacl)# exit
```

IPv4 アクセスリスト（EXTRA_NET_POLICY_VRF_2_TO_3）を作成して，宛先 IPv4 アドレス 192.168.30.0/24 の IPv4 パケットに対して IPv4 ポリシーベースルーティングリスト（EX_POLICY_TO_VRF3）を設定します。

5.
```
(config)# interface gigabitethernet 1/2
(config-if)# ip access-group EXTRA_NET_POLICY_VRF_2_TO_3 in
(config-if)# exit
```

イーサネットインタフェース 1/2 の受信側に IPv4 アクセスリスト（EXTRA_NET_POLICY_VRF_2_TO_3）を適用します。

8.3　オペレーション

8.3.1　運用コマンド一覧

ポリシーベースルーティングの運用コマンド一覧を次の表に示します。

表 8-10　運用コマンド一覧

コマンド名	説明
show ip cache policy	IPv4 ポリシーベースルーティングリストのネクストホップの情報と状態を表示します。
show ipv6 cache policy	IPv6 ポリシーベースルーティングリストのネクストホップの情報と状態を表示します。
restart policy-based-routing	ポリシーベースルーティング制御プログラムを再起動します。
dump policy-based-routing	ポリシーベースルーティング制御プログラムで採取している制御情報をファイルへ出力します。
show access-filter※	ポリシーベースルーティングを動作に指定したアクセスリストの設定内容と統計情報を表示します。
clear access-filter※	ポリシーベースルーティングを動作に指定したアクセスリストの統計情報を 0 クリアします。

注※

「運用コマンドレファレンス Vol.2　7. フィルタ」を参照してください。

8.3.2　ポリシーベースルーティングの確認

(1)　アクセスリストの確認

show access-filter コマンドで, ポリシーベースルーティングリストを動作に指定したアクセスリストを確認できます。

図 8-3　show access-filter コマンドの実行結果

```
> show access-filter interface port-channel 10.1
Date 20XX/01/01 12:00:00 UTC
Using interface : port-channel 10.1 in
Extended IP access-list : IPv4_POLICY_B
      10 permit ip any 192.168.1.10 0.0.0.255 action policy-list POLICY_LIST_IPv4_B
                        Matched packets        Matched bytes
         Total  :              11032378           2966258332
         PRU 1  :              11000255           2965612120
         PRU 3  :                 32123               646212
      20 permit ip any any
                        Matched packets        Matched bytes
         Total  :                 54778             70197700
         PRU 1  :                 54555             70182240
         PRU 3  :                   223                15460
      Implicit-deny
                        Matched packets        Matched bytes
         Total  :                     0                    0
         PRU 1  :                     0                    0
         PRU 3  :                     0                    0
>
```

指定したインタフェースのフィルタに「Extended IP access-list」とアクセスリスト名（IPv4_POLICY_B）が表示されることを確認します。また，アクセスリストに「action policy-list」とポリシーベースルーティングリスト名（POLICY_LIST_IPv4_B）が表示されて，Matched packets および Matched bytes がカウントされていることを確認します。

(2)　ポリシーベースルーティングリストの確認

show ip cache policy コマンドで，IPv4 ポリシーベースルーティングリスト内で選択しているネクストホップを確認できます。また，show ipv6 cache policy コマンドで IPv6 ポリシーベースルーティングリストを確認できます。

図 8-4　show ip cache policy コマンドの実行結果

```
> show ip cache policy POLICY_LIST_IPv4_B
Date 20XX/01/01 12:00:00 UTC
IPv4 policy-based routing suspend-update switch-over : 200
    Start time : 20XX/01/01 15:00:00 UTC
    End time   : 20XX/01/01 15:03:20 UTC
IPv4 policy-based routing list : POLICY_LIST_IPv4_B
    Priority    Status  Interface       Next Hop
 *> 10          Up      ChGr100         192.168.100.10
    20          Up      ChGr200         192.168.200.10
    Default   : Deny
>
```

指定した IPv4 ポリシーベースルーティングリストに設定しているネクストホップがすべて表示されること，また，選択しているネクストホップを示す「*>」が表示されることを確認します。

9 RA

この章では，RA（Router Advertisement）について説明します。

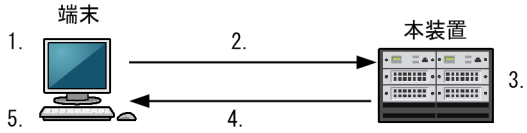
9.1 解説

9.1.1 概要

RA（Router Advertisement）は，ルータが端末群に IPv6 アドレス生成に必要な情報やデフォルトルートを配布する機能です。

ルータはアドレスのプレフィックス部だけを一定間隔で配布して，受信した各端末は，端末固有のインタフェース ID 部と RA のプレフィックス情報からアドレスを生成します。こうした特徴によって，RA はサーバレスで端末数に依存しない簡便な Plug & Play を実現します。なお, RA によるアドレス自動設定はルータ以外の端末だけで設定でき，ルータは RA を受信してもアドレスを自動設定しません。

図 9-1　RA による端末のアドレス設定



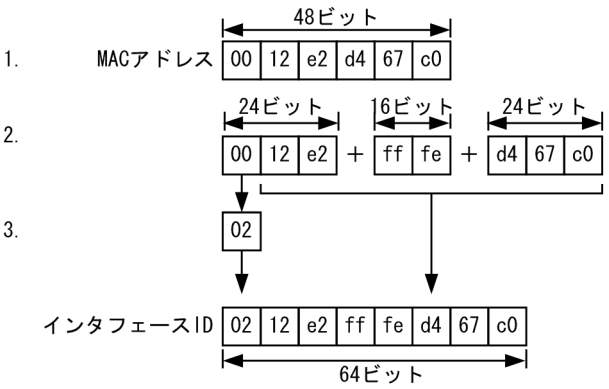
1. インタフェース ID を生成します。
2. プレフィックスを要求します。
3. RA で配布するプレフィックスを設定します。
4. プレフィックスを通知します。
5. 通知されたプレフィックスとインタフェース ID を組み合わせてアドレスを生成して，設定します。

9.1.2 情報の配布

RA によるアドレス配布には，ルータからの定期的な配布と，端末からのリクエストに対するルータの応答の二種類があります。両者は配布の契機が異なるだけで，どちらの場合も，ルータからのアドレス配布は ICMPv6 パケット Type134 で規定された RA によって行われます。また，端末からのリクエストは ICMPv6 パケット Type133 の RS（Router Solicitation）によって行われます。

RA を受信した端末は，与えられたプレフィックスと各端末で固有である 64 ビットのインタフェース ID（通常は 48 ビットの MAC アドレスを基に生成）を組み合わせたグローバルアドレスを生成して，RA を受信したインタフェースに設定します。同時に RA 送信元アドレス（=RA を送信したルータのインタフェースリンクローカルアドレス）を端末のデフォルトゲートウェイとして設定します。MAC アドレスからのインタフェース ID 生成を次の図に示します。

図 9-2 MAC アドレスからのインタフェース ID 生成



1. MAC アドレスを 24 ビットで二つに分割します。
2. 中間に固定値“ff fe”を挿入します。
3. 最初の 8 ビットの下位 2 ビット目の値を反転します。

ルータから端末に伝えられるプレフィックスは，通常は RA を広告するインタフェースに設定されたアドレスプレフィックスのうち，リンクローカルを除いたものです。ただし，それに加えてそのほかのプレフィックスを広告することもできます。また，ルータからの RA 送出時間間隔の最大値，最小値をインタフェース単位で設定できます。RA で配布される情報を次の表に示します。

表 9-1 RA で配布される情報

配布情報	説明	設定できる範囲	省略時の初期値
アドレス自動管理設定フラグ（ManagedFlag）	RA 受信を契機に，DHCPv6 によって IPv6 アドレスを端末に自動で設定させるかどうか指定するフラグ。 DHCPv6 で IPv6 アドレスを設定する場合は，ON にしてください。	ON/OFF	OFF
アドレス以外情報設定フラグ（OtherConfigFlag）	RA 受信を契機に，DHCPv6 によって IPv6 アドレス以外の情報（DNS サーバなど）を端末に自動で設定させるかどうか指定するフラグ。 DHCPv6 で IPv6 アドレス以外の情報（DNS サーバなど）を設定する場合は，ON にしてください。	ON/OFF	OFF
リンク MTU（LinkMTU）	端末が実際の通信に使用する MTU 値を指定します。通常使用される MTU 値は RA を受信したインタフェースの MTU 値ですが，インタフェースの MTU いっぱいのパケットを端末に使わせたくない場合に，このパラメータを MTU 値よりも小さい値に設定します。インタ	0（配布しない），または 1280～インタフェースの MTU	インタフェースの MTU

配布情報	説明	設定できる範囲	省略時の初期値
	フェースの MTU よりも大きい値は通知できません。		
可到達時間（ReachableTime）	IPv6 では ICMPv6 によって隣接ノードの到達性を確認しますが，その確認結果の有効期間を端末に指定します。未指定または 0 を指定した場合は，端末ごとに定められたデフォルト値が到達性確認結果の有効期間になります。なお，0 以外の値を指定した場合は，本装置の該当インタフェースで学習する NDP エントリの Reachable 状態遷移時間のベース値にも適用されます。	0～4294967295（ミリ秒）	0
再送時間（RetransTimer）	IPv6 では ICMPv6 によって隣接ノードの到達性を確認しますが，そのとき送信する ICMPv6 パケットの送信間隔を端末に指定します。未指定または 0 を指定した場合は，端末ごとに決められたデフォルト値が再送間隔として使用されます。なお，0 以外の値を指定した場合は，本装置の該当インタフェースで学習する NDP エントリの解決処理時および近隣到達不能検出時の再送間隔にも適用されます。	0，または 1000～4294967295（ミリ秒）	0
端末ホップリミット（CurHopLimit）	端末がパケットを送信するときに，何ホップ先まで中継できるかを示す IPv6 ヘッダ内のホップリミット領域に設定する値を指定します。	0～255	64
ルータ生存時間（DefaultLifetime）	端末が RA によって確定したデフォルトルータの有効期間。0 を指定すると，端末は，受信した RA の送信元アドレスをデフォルトゲートウェイと見なしません。	0，または RA 送出間隔の最大値～9000（秒）	1800（秒）
リンク層オプション（SourceLink-layerAddressOption）	RA 送信元の IPv6 アドレスに対応するリンク層アドレス。本装置の場合は，RA 広告インタフェースがイーサネットおよびギガビット・イーサネットの場合だけ，そのポートの MAC アドレスが入ります。リンク層アドレスによる負荷分散などを行う場合に，このオプションを OFF にして，各端末でデフォル	ON/OFF	ON

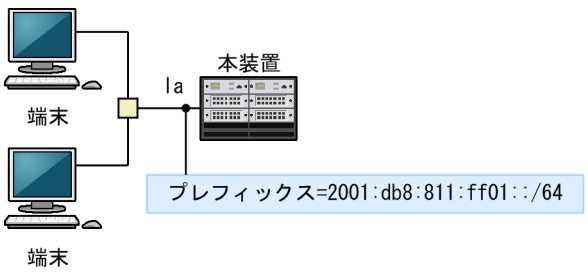
配布情報	説明	設定できる範囲	省略時の初期値
	トゲートウェイのリンク層アドレス解決を行います。		
ルータ優先度（DefaultRouterPreference）	端末が複数ルータから RA を受信した場合に，どの RA の情報を優先して使用するか指定します。	high，medium，low	medium
プレフィックス（PrefixList）	RA で広告するプレフィックス。指定していないときは，広告するインタフェースに付いているグローバルプレフィックスを広告します。それ以外に，さらにプレフィックスを広告したい場合や，インタフェースに付いているプレフィックスに対して有効期間を設定する場合に使用します。	グローバルプレフィックス	インタフェースに付いているグローバルプレフィックス
自律設定有効フラグ（AutonomousFlag）	このオプションが ON の場合，端末は IPv6 アドレス生成にそのプレフィックスを使用します。 このオプションが OFF の場合，端末は IPv6 アドレス生成にそのプレフィックスを使用しません。DHCPv6 だけを使用して IPv6 アドレスを設定するときは，OFF にしてください。	ON/OFF	ON
オンリンクフラグ（OnLinkFlag）	このオプションが ON のプレフィックスは，RA を受信したインタフェースと同じリンク上に存在することを示します。 このオプションが OFF のプレフィックスは，RA を受信したインタフェースと異なるリンク上に存在して，ルータを経由する必要があることを示します。	ON/OFF	ON
推奨有効期間（PreferredLifetime）	RA によって通知されたプレフィックスを，端末が通信時のソースアドレスに使用することを許可する時間。推奨する有効期間を過ぎても RA を受信しないと，該当するプレフィックス以外のアドレスを通信のソースアドレスとして使用することを試行します。ただし，ほかに適切なプレフィックスを持たない場合は，端末は推奨する有効期間を過ぎたプレフィックスを通信に使用します。	0，または RA 送出間隔の最大値～4294967295（秒）	604800（秒）

配布情報	説明	設定できる範囲	省略時の初期値
最終有効期間（ValidLifetime）	RA によって通知されたプレフィックスが消滅するまでの時間。最終有効期間を過ぎても RA を受信しないと，端末は該当するプレフィックスのアドレスを削除します。	0，または RA 送出間隔の最大値～4294967295（秒）	2592000（秒）
DNS サーバ情報（RDNSS）	端末が DNS 解決で使用する DNS サーバの IPv6 アドレスを指定します。	グローバルアドレスまたはリンクローカルアドレス	配布しない
DNS サーバ情報の使用期限（Lifetime）	RA によって通知された DNS サーバを使用できる最大時間です。	0～4294967295（秒）	RA 送出間隔の最大値の 3 倍
DNS サーチリスト（DNSSL）	端末が DNS 解決を実行するときに使用するドメイン名を指定します。	253 文字以内のドメイン名	配布しない
DNS サーチリストの使用期限（Lifetime）	RA によって通知されたドメイン名を使用できる最大時間です。	0～4294967295（秒）	RA 送出間隔の最大値の 3 倍

9.1.3 プレフィックス情報変更時の対処

RA で端末にプレフィックスを配布している構成では，プレフィックスの値を変更すると，急なアドレス変更によって疎通できなくなることがあります。それを防ぐために，標準設定では古いプレフィックスが 604800 秒（7 日間）残るようになっています。古いプレフィックスを削除するには，変更対象のプレフィックスと同時に新しいプレフィックスを広告して，有効時間を徐々に変更することで古いプレフィックスを削除してください。RA の使用例を次の図に示します。

図 9-3 RA の使用例



1. イーサネットのインタフェース Ia から RA をネットワークに広告する設定をします。
   - Ia のプレフィックス＝ 2001:db8:811:ff01::/64
2. Ia のプレフィックスを 2001:db8:811:ff01::/64 から 2001:db8:811:ff22::/64 に変更する設定をします。
   - Ia で新しく広告するプレフィックス 2001:db8:811:ff22::/64 の広告間隔を短く設定して，広告を開始します。
   - Ia で利用を停止するプレフィックス 2001:db8:811:ff01::/64 の推奨有効期間，最終有効期間を短く設定して，広告をします。

- Ia での 2001:db8:811:ff22::/64 の広告間隔をデフォルト値に戻します。
- 広告を終了するプレフィックス 2001:db8:811:ff01::/64 の広告を停止します。

9.2 コンフィグレーション

コンフィグレーションコマンド ipv6 address または ipv6 enable を設定し，IPv6 が有効になっているインタフェースでは自動的に RA が送信されます。

RA 送信の抑止や RA の各種属性の変更は，インタフェース単位で設定します。

9.2.1 コンフィグレーションコマンド一覧

RA のコンフィグレーションコマンド一覧を次の表に示します。

表 9-2 コンフィグレーションコマンド一覧

コマンド名	説明
ipv6 hop-limit	RA を受信した端末が送信時に使用するホップリミットの初期値を指定します。
ipv6 nd dns-search-list	RA で配布する DNS サーチリストを指定します。
ipv6 nd dns-server	RA で配布する IPv6 DNS サーバ情報を指定します。
ipv6 nd link-mtu	RA で送信する link-mtu 情報の MTU 値を指定します。
ipv6 nd managed-config-flag	RA によるアドレス自動設定とは別に，DHCPv6 による自動アドレス設定を端末に行わせるフラグを設定します。
ipv6 nd no-advertise-link-address	ルータの IP アドレスに対応するリンク層アドレスを RA に含ませないことを指定します。
ipv6 nd ns-interval	RA を受信した端末が通信時に相手の到達可能性を確認するための制御パケットの送出間隔を設定します。
ipv6 nd other-config-flag	DHCPv6 によって IPv6 アドレス以外の情報を端末に自動的に取得させるフラグを設定します。
ipv6 nd prefix	RA で送信する IPv6 プレフィックス情報，またプレフィックスに関連する情報を指定します。
ipv6 nd ra-interval	RA を送信する最小間隔時間と最大間隔時間を指定します。
ipv6 nd ra-lifetime	RA によって設定される端末のデフォルトルートの有効期間を指定します。
ipv6 nd reachable-time	RA を受信した端末が送信時に確認できた隣接ノードの到達性についての情報の有効期間を指定します。
ipv6 nd router-preference	複数の RA を受信した端末が，どのルータ広告の情報を優先して使用するかを指定します。
ipv6 nd suppress-ra	RA 送信を抑止します。

9.2.2 RA 送信抑止の設定

インタフェースに対して RA 送信を抑止する設定をします。

[設定のポイント]

RA の送信抑止は，ipv6 nd suppress-ra コマンドを使用します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   (config-if)# ipv6 nd suppress-ra
   ポート 1/1 で RA 送信を抑止する設定をします。
2. **(config-if)# ipv6 address 2001:db8:1:1::1/64**
   ポート 1/1 に IPv6 アドレス 2001:db8:1:1::1/64 を設定します。

9.2.3 配布情報の設定

RA によって配布する情報を設定します。

[設定のポイント]

RA の配布情報はインタフェースモードで設定します。ここでは例として，ipv6 nd other-config-flag コマンドによるアドレス以外の情報を DHCPv6 で設定するフラグ（OtherConfigFlag）と，ipv6 nd router-preference コマンドによるルータ優先度（DefaultRouterPreference）を設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   (config-if)# ipv6 nd other-config-flag
   ポート 1/1 から送信する RA に，アドレス以外の情報を DHCPv6 で設定するフラグ（OtherConfigFlag）を設定します。端末は RA 受信を契機に，DHCPv6 によって，アドレス以外の情報を取得します。
2. **(config-if)# ipv6 nd router-preference high**
   ポート 1/1 から送信する RA のルータ優先度（DefaultRouterPreference）に，high（最も高い）を設定します。

9.2.4 RA 送信間隔の調整

RA の送信間隔を設定します。

[設定のポイント]

RA の送信間隔の設定には，ipv6 nd ra-interval コマンドを使用します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   (config-if)# ipv6 nd ra-interval 600 1200
   RA を 10 分～20 分の間のランダムな間隔で送信する設定をします。

9.3 オペレーション

9.3.1 運用コマンド一覧

RA の運用コマンド一覧を次の表に示します。

表 9-3 運用コマンド一覧

コマンド名	説明
show ipv6 routers	RA 情報を表示します。
show netstat (netstat)※1	ネットワークの状態・統計を表示します。
show ipv6 interface※2	IPv6 インタフェースの状態を表示します。

注※1

「運用コマンドレファレンス Vol.3 2. IPv4・ARP・ICMP」を参照してください。

注※2

「運用コマンドレファレンス Vol.3 3. IPv6・NDP・ICMPv6」を参照してください。

9.3.2 サマリー情報の確認

RA を送信しているインタフェースの一覧を表示します。

図 9-4 RA を送信しているインタフェースの一覧

```
> show ipv6 routers global
Date 20XX/03/14 12:00:00 UTC
#Index Name            Prefix
#2     Eth1/1          2001:db8:1:1::/64
#3     Eth2/1          2001:db8:1:2::/64
#4     Eth3/1          2001:db8:1:3::/64
```

9.3.3 詳細情報の確認

RA を送信しているインタフェースの詳細情報を表示します。

図 9-5 RA を送信しているインタフェースの詳細情報

```
> show ipv6 routers interface gigabitethernet 1/1
Date 20XX/03/14 12:00:00 UTC
Index: 3, Name: Eth1/1, VRF: global
Statistics:
  RSin(wait): 5(0), RAout: 10, RAin(invalid): 0(0)
Intervals:
  RA Interval: 600-1200s (next=219s later), RA Lifetime: 1800s
  Reachable Time: ---, NS Interval: ---
Managed Config Flag: off, Other Config Flag: on, Hop Limit: 64
No Advertised Link Address: off, Link MTU: 1500
DNS Server Address(lifetime):
  2001:db8:2::1(3600s)

Prefix                          ValidLife[s] PrefLife[s] OnLink Autoconfig
2001:db8:1:1::/64               2592000      604800      on     on
```

10 DHCP/BOOTP リレーエージェント

この章では，DHCP/BOOTP リレーエージェントの解説および操作方法について説明します。

10.1　解説

10.1.1　概要

DHCP/BOOTP リレーエージェントは，DHCP/BOOTP クライアント（以降，クライアント）と DHCP/BOOTP サーバ（以降，サーバ）が異なるネットワークセグメントにあるネットワーク構成のときに，DHCP/BOOTP パケットを異なるネットワークセグメントへレイヤ 7 転送します。DHCP/BOOTP リレーエージェントのネットワーク構成例を次に示します。

図 10-1　DHCP/BOOTP リレーエージェントのネットワーク構成例（1 段）

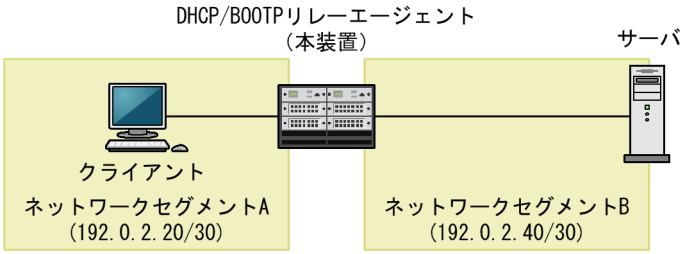
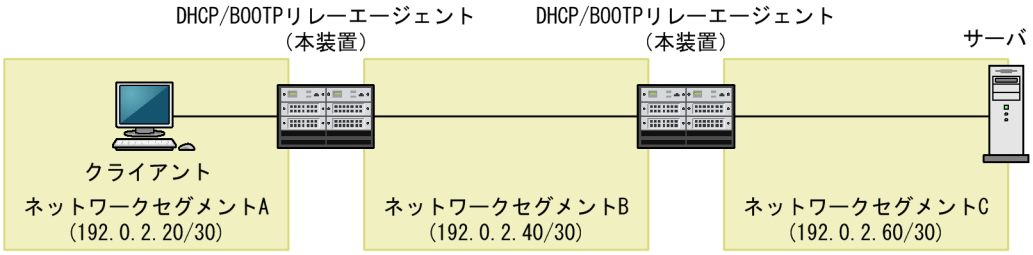


図 10-2　DHCP/BOOTP リレーエージェントのネットワーク構成例（多段）



10.1.2　サポート範囲

DHCP/BOOTP リレーエージェントでサポートする機能を次の表に示します。

表 10-1　DHCP/BOOTP リレーエージェントでサポートする機能

項目	仕様	サポート
接続形態（クライアント側）	クライアント直接	○
	DHCP/BOOTP リレーエージェント経由	○
接続形態（サーバ側）	サーバ直接	○
	DHCP/BOOTP リレーエージェント経由	○
転送	サーバまたは DHCP/BOOTP リレーエージェント宛て	○
	クライアント宛て	○
	ネットワークセグメント内の全サーバ宛て	×
	ネットワークセグメント内の全サーバおよび全 DHCP/BOOTP リレーエージェント宛て	○※1

項目	仕様	サポート
	BOOTP	○
	送信元インタフェース変更	×
インタフェース	イーサネットインタフェース	○
	イーサネットサブインタフェース	○
	ポートチャネルインタフェース	○
	ポートチャネルサブインタフェース	○
	VLAN インタフェース	○
	ループバックインタフェース	×
	Null インタフェース	×
	マネージメントポート	×
	シリアル接続ポート（AUX）	×
バインディングデータベース		×
IP	フラグメント送信（サーバ側）	○
	フラグメント受信（サーバ側）	○
	フラグメント送信（クライアント側）	×
	フラグメント受信（クライアント側）	○
UDP	最大 UDP 長（ヘッダ+ペイロード）	2048byte※2

（凡例）　○：サポートする　×：サポートしない

注※1

DHCP/BOOTP サーバの IP アドレスにダイレクトブロードキャストアドレスを設定してください。

注※2

フラグメント化する前の長さです。

10.1.3　DHCP/BOOTP プロトコル

ここでは，DHCP/BOOTP パケット転送で使用する通信プロトコルの DHCP/BOOTP について説明します。

(1)　DHCP/BOOTP パケットフォーマット

本装置が送信する DHCP/BOOTP パケットのフォーマットおよび設定値は RFC2131 および RFC3046 に従います。

(2)　DHCP/BOOTP パケット有効性チェック

DHCP/BOOTP パケット受信時にパケットの有効性をチェックします。DHCP/BOOTP パケットのチェック内容を次に示します。

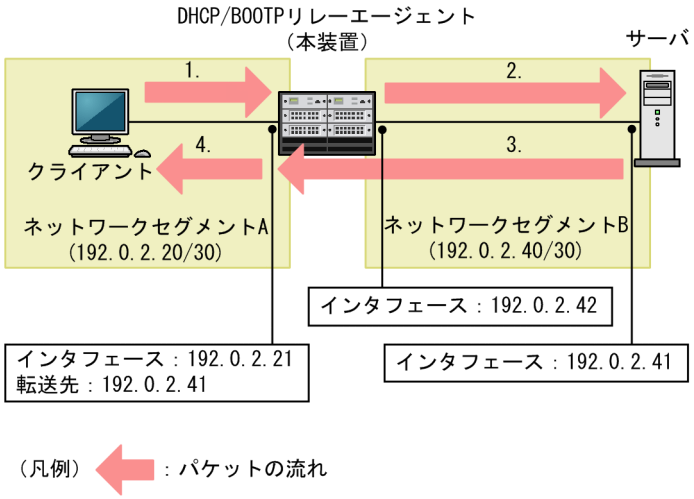
表 10-2　DHCP/BOOTP パケットのチェック内容

パケットフィールド	チェック内容（サーバ宛て）	チェック内容（クライアント宛て）	チェック異常時
メッセージ op コード／メッセージタイプ	BOOTREQUEST（1）であること	BOOTREPLY（2）であること	パケット廃棄
ホップ数	最大ホップ数未満であること	チェックしない	パケット廃棄
リレーエージェントアドレス	チェックしない	本装置宛てであること	パケット廃棄

10.1.4　DHCP/BOOTP パケット転送時の設定内容

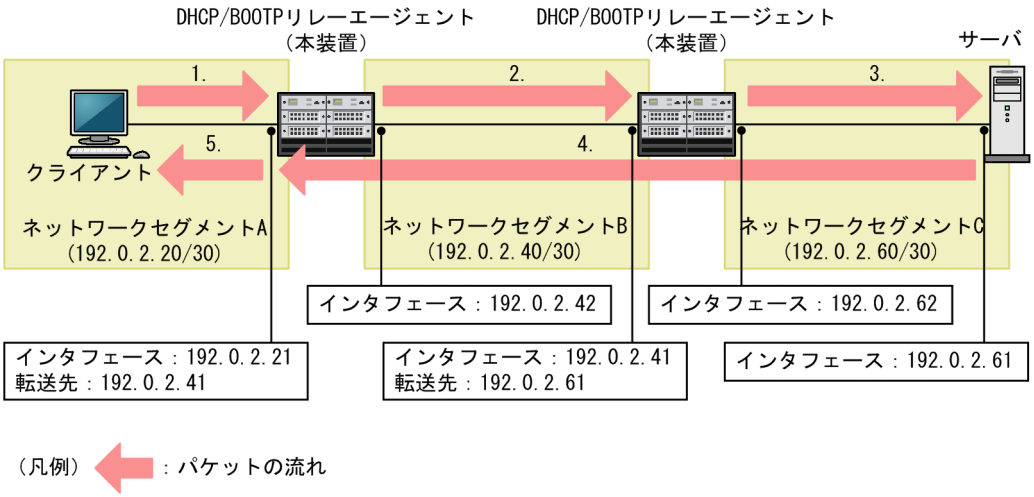
DHCP/BOOTP リレーエージェントが DHCP/BOOTP パケットを転送するときの設定内容を次に示します。

図 10-3　DHCP/BOOTP パケットの設定内容（1 段）



パケット（図中の番号）	パケット内の値			
	宛先 IP アドレス	送信元 IP アドレス	宛先 UDP ポート番号	送信元 UDP ポート番号
1.	255.255.255.255	0.0.0.0	67	任意
2.	192.0.2.41	192.0.2.42	67	68
3.	192.0.2.21	192.0.2.41	67	任意
4.	割り当て DHCP アドレス	192.0.2.21	68	67

図 10-4　DHCP/BOOTP パケットの設定内容（多段）



パケット（図中の番号）	パケット内の値			
	宛先 IP アドレス	送信元 IP アドレス	宛先 UDP ポート番号	送信元 UDP ポート番号
1.	255.255.255.255	0.0.0.0	67	任意
2.	192.0.2.41	192.0.2.42	67	68
3.	192.0.2.61	192.0.2.62	67	68
4.	192.0.2.21	192.0.2.61	67	任意
5.	割り当て DHCP アドレス	192.0.2.21	68	67

表 10-3　DHCP/BOOTP パケット転送時の設定内容

パケットフィールド		設定条件		設定する内容	
				サーバ宛て	クライアント宛て
DHCP/BOOTP	リレーエージェントアドレス	リレーエージェントアドレスが 0.0.0.0 で，リンクセレクションを付けないで転送する	DHCP/BOOTP リレーエージェント IP アドレスが設定されていない	受信インタフェースのプライマリ IP アドレスを設定します	設定しません
			DHCP/BOOTP リレーエージェント IP アドレスが設定されている	DHCP/BOOTP リレーエージェント IP アドレスを設定します	設定しません
		リレーエージェントアドレスが 0.0.0.0 で，リンクセレクションを付けて転送する※1		ループバックインタフェースの IP アドレスを設定します※1	−
		リレーエージェントアドレスが 0.0.0.0 以外		変更しません	リンクセレクションサブオプションが含まれる場合，リンクセレク

パケット フィールド		設定条件	設定する内容	
			サーバ宛て	クライアント宛て
				ションの値を設定します
	ホップ数	なし	1 増加させます	変更しません
	リレーエージェント情報オプション（Option82）	リレーエージェントアドレスが 0.0.0.0 で，Option82 が付いていない	サーキット ID とリモート ID の二つのサブオプションを含む情報（Option82）を付けます※2	－
		リレーエージェントアドレスが本装置のアドレス	受信した内容を変更しません	Option82 を削除します※2
		上記以外	受信した内容を変更しません	－
	その他のオプション	なし	受信した内容を変更しません	受信した内容を変更しません
IP	送信元 IP アドレス	なし	送信元インタフェースまたはループバックインタフェースの IP アドレスを設定します※1	リレーエージェントアドレスフィールドの値を設定します
	宛先 IP アドレス	ブロードキャストフラグが OFF	DHCP/BOOTP パケットの転送先を設定します	割り当てアドレスを設定します
		ブロードキャストフラグが ON	DHCP/BOOTP パケットの転送先を設定します	制限付きブロードキャストアドレスを設定します

（凡例）　－：該当しない

注※1

Option82 にリンクセレクションを含める場合，コンフィグレーションコマンド ip dhcp relay source-interface による送信元インタフェースの指定が必須となります。詳細は「表 10–4　サーバへ送信する DHCP/BOOTP パケットの設定内容」を参照してください。

注※2

コンフィグレーションコマンド ip dhcp relay information option-insert を設定していない場合，受信した内容を変更しません。

表 10–4　サーバへ送信する DHCP/BOOTP パケットの設定内容

サーバへの送信条件		パケットフィールド	
リンクセレクションとサーバ ID オーバライドの付加	送信元インタフェース指定	送信元アドレス	リレーエージェントアドレス
両方付ける	あり	指定されたインタフェース	指定されたインタフェース
サーバ ID オーバライドだけを付ける	なし	パケットの送信元（サーバ側）インタフェース	クライアント側のインタフェース

サーバへの送信条件		パケットフィールド	
リンクセレクションとサーバ ID オーバライドの付加	送信元インタフェース指定	送信元アドレス	リレーエージェントアドレス
付けない	あり	指定されたインタフェース	クライアント側のインタフェース
	なし	パケットの送信元（サーバ側）インタフェース	クライアント側のインタフェース

10.1.5　リレーエージェント情報オプション（Option82）

リレーエージェント情報オプション（DHCP Option82）は，DHCP/BOOTP リレーエージェントでパケットを中継するときに，リレーエージェント固有の情報を付けてからサーバに転送するためのオプションです。

コンフィグレーションコマンド ip dhcp relay information option-insert を設定すると，DHCP/BOOTP パケットのオプションの最後に，次の四つのサブオプションを含む情報を付けます。

- サーキット ID
- リモート ID
- リンクセレクション
- サーバ ID オーバライド

このうち，サーキット ID およびリモート ID は常に付きますが，リンクセレクションおよびサーバ ID オーバライドを付けるかどうかは任意です。また，リモート ID の形式は，コンフィグレーションで指定できます。

サーキット ID には，ポートを識別するための情報として，VLAN ID とポート情報を設定します。また，リモート ID には，装置を識別するための情報として，装置 MAC アドレスを設定します。リモート ID の形式として port-unique を指定した場合，サーキット ID と同様に VLAN ID とポート情報をリモート ID に含めます。

なお，クライアントが接続されているポートによって，Option82 フィールドに設定される内容は異なります。Option82 フィールドに設定される VLAN ID とポート情報を次の表に示します。

表 10-5　Option82 フィールドに設定される VLAN ID とポート情報

クライアントが接続されているポート		サーキット ID およびリモート ID の設定内容		
		VLAN ID	Mode 値	ポート情報
イーサネットインタフェースまたはイーサネットサブインタフェース		VLAN Tag の VLAN ID※	0x00	NIF 番号とポート番号
ポートチャネルインタフェースまたはポートチャネルサブインタフェース		VLAN Tag の VLAN ID※	0x01	チャネルグループ番号
VLAN インタフェース	スイッチポートがチャネルグループに所属しない	VLAN ID	0x80	NIF 番号とポート番号
	スイッチポートがチャネルグループに所属する	VLAN ID	0x81	チャネルグループ番号

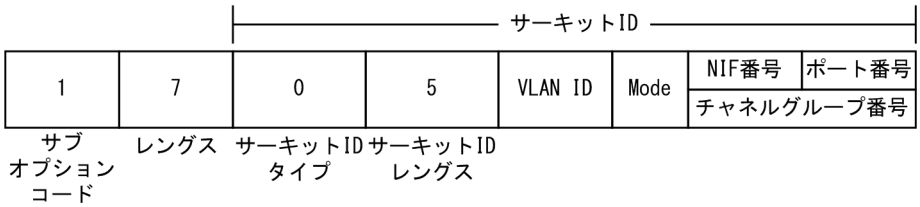
注※ VLAN Tag を使用しない場合，0 を設定します。

クライアントに DHCP/BOOTP パケットを転送する場合，リレーエージェント情報オプションを削除してから転送します。

(1) サーキット ID

サーキット ID は，クライアントが接続されているポートを識別するための ID です。サーキット ID には，VLAN ID およびポート情報（NIF 番号とポート番号，またはチャネルグループ番号）を設定します。サーキット ID の形式を次の図に示します。

図 10-5 サーキット ID の形式



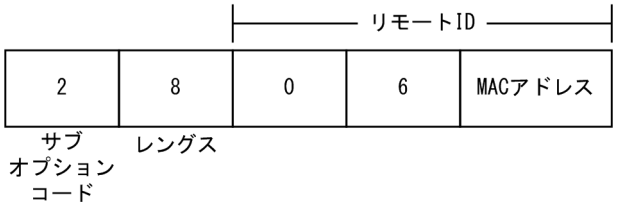
(2) リモート ID

リモート ID は，装置を識別するための ID です。リモート ID の形式は，コンフィグレーションで指定できます。

コンフィグレーションコマンド ip dhcp relay information option-insert でパラメータ指定なし

リモート ID の MAC アドレス（6 バイト）には，本装置の装置 MAC アドレスを設定します。リモート ID の形式（パラメータ指定なし）を次の図に示します。なお，この形式では，クライアントが接続されているポートごとの制御をする場合に，サーバ側でサーキット ID と組み合わせる必要があります。

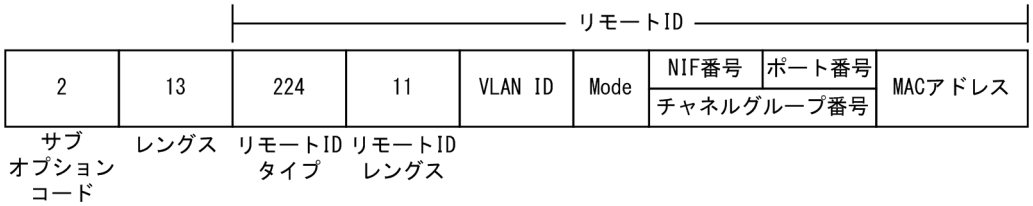
図 10-6 リモート ID の形式（パラメータ指定なし）



コンフィグレーションコマンド ip dhcp relay information option-insert で remote-id port-unique パラメータ指定あり

リモート ID には，サーキット ID と同様の VLAN ID およびポート情報（NIF 番号とポート番号，またはチャネルグループ番号）と，MAC アドレスを設定します。MAC アドレス（6 バイト）には，本装置の装置 MAC アドレスを設定します。リモート ID の形式（port-unique 指定）を次の図に示します。

図 10-7 リモート ID の形式（port-unique 指定）



(3)　リンクセレクションおよびサーバ ID オーバライド

リンクセレクションは，プライベートネットワークとグローバルネットワークの異なるネットワーク間で，サーバから DHCP/BOOTP パケットを受信できるようにするサブオプションです。リンクセレクションサブオプションは RFC3527 に従います。

サーバ ID オーバライドは，クライアントからのアドレス再割り当て要求時やアドレス返却時でも，必ず DHCP/BOOTP リレーエージェント（本装置）を中継させるためのサブオプションです。サーバ ID オーバライドサブオプションは RFC5107 に従います。

リンクセレクションおよびサーバ ID オーバライドに設定する IP アドレスを次の表に示します。

表 10-6　リンクセレクションおよびサーバ ID オーバライドに設定する IP アドレス

設定条件	リンクセレクションおよびサーバ ID オーバライドに設定する IP アドレス
DHCP/BOOTP リレーエージェント IP アドレスが設定されていない	受信インタフェースのプライマリ IP アドレス
DHCP/BOOTP リレーエージェント IP アドレスが設定されている	DHCP/BOOTP リレーエージェント IP アドレス

10.1.6　DHCP/BOOTP リレーエージェント使用時の注意事項

- DHCP/BOOTP リレーエージェントと VRRP を同一インタフェースに設定する場合，VRRP によって別装置に切り替わってもクライアントからサーバへのゲートウェイが同じになるようにしてください。例えば，サーバでは，仮想ルータアドレスをデフォルトルータ（ルータオプション）としてクライアントに割り当てられるように設定してください。
- クライアントと接続するインタフェースにコンフィグレーションコマンド ip dhcp relay source-interface を指定する場合，サーバが所属する VRF，またはクライアントが接続する VRF と同じ VRF のインタフェースを指定してください。

  エクストラネット構成でクライアント側の VRF がプライベートネットワークの場合，送信元インタフェースをクライアント側の VRF にすると，サーバから本装置宛ての DHCP/BOOTP パケットが適切に送信されないおそれがあります。

  このため，送信元インタフェースには，サーバ側の VRF（またはグローバルネットワーク）のインタフェースを使用することが望ましいです。クライアント側の VRF のループバックインタフェースを使用する場合は，VRF 間で重複しないアドレスを設定して，その経路をサーバ側の VRF にエクストラネット経路として導入してください。

10.2　コンフィグレーション

10.2.1　コンフィグレーションコマンド一覧

DHCP/BOOTP リレーエージェントのコンフィグレーションコマンド一覧を次の表に示します。

表 10-7　コンフィグレーションコマンド一覧

コマンド名	説明
ip dhcp relay gateway	DHCP/BOOTP リレーエージェント IP アドレス（giaddr）を設定します。
ip dhcp relay information no-check	リレーエージェント情報オプション（DHCP Option82）の有効性チェックを抑止します。
ip dhcp relay information option server-id-override	サーバ ID オーバライドを設定します。
ip dhcp relay information option-insert	リレーエージェント情報オプション（DHCP Option82）の付加を有効にします。
ip dhcp relay maximum-hop-count	DHCP/BOOTP パケットの最大ホップ数を設定します。
ip dhcp relay source-interface	送信元インタフェースを指定します。
ip helper-address	DHCP/BOOTP パケットの転送先を設定します。

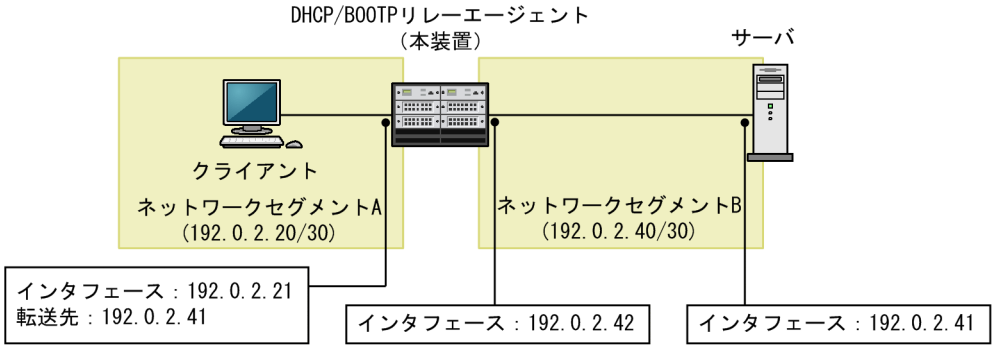
10.2.2　DHCP/BOOTP パケットをサーバへ転送する設定（基本設定）

[設定のポイント]

DHCP/BOOTP リレーエージェントで，サーバ宛て DHCP/BOOTP パケットの転送先を設定します。

DHCP アドレスが割り当てられたあと，クライアントとサーバは DHCP/BOOTP リレーエージェントを経由しないでユニキャストで通信します。そのため，クライアントとサーバがユニキャスト通信できるようなネットワーク構成としてください。次の図に示す構成では，サーバにネットワークセグメント A の経路情報を設定してください。

図 10-8　DHCP/BOOTP パケットをサーバへ転送する構成（基本構成）



[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/5**
   (config-if)# ip address 192.0.2.21 255.255.255.252

```
(config-if)# exit
```

クライアントと接続するインタフェースにあらかじめ IP アドレスを設定しておきます。

2.
```
(config)# interface gigabitethernet 1/7
(config-if)# ip address 192.0.2.42 255.255.255.252
(config-if)# exit
```

項番 1 と同様に，サーバへ転送するインタフェースにもあらかじめ IP アドレスを設定しておきます。

3.
```
(config)# interface gigabitethernet 1/5
(config-if)# ip helper-address 192.0.2.41
(config-if)# exit
```

クライアントと接続するインタフェースに，サーバ宛て DHCP/BOOTP パケットの転送先としてサーバの IP アドレスを設定します。

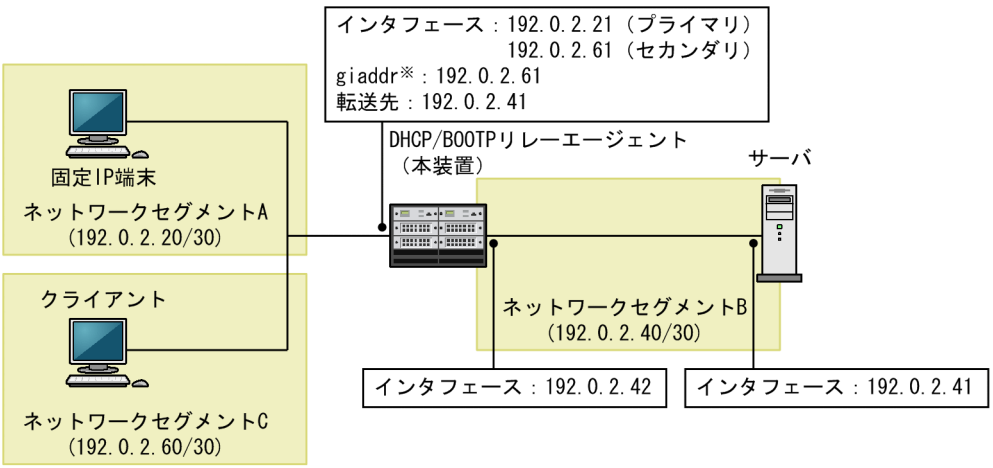
10.2.3　マルチホーム構成での設定

[設定のポイント]

マルチホーム構成の場合，デフォルトではプライマリ IP アドレスが DHCP/BOOTP リレーエージェント IP アドレスとなります。

ip dhcp relay gateway コマンドで DHCP/BOOTP リレーエージェント IP アドレスを別に設定すると，セカンダリ IP アドレスを DHCP/BOOTP リレーエージェント IP アドレスとして使用できます。次の図では，セカンダリ IP アドレスのネットワークセグメント C にだけ DHCP/BOOTP を適用するネットワーク構成としています。

図 10-9　マルチホーム構成



注※　DHCP/BOOTP リレーエージェント IP アドレス

[コマンドによる設定]

1.
```
(config)# interface gigabitethernet 1/5
(config-if)# ip address 192.0.2.21 255.255.255.252
```

クライアントと接続するインタフェースに，あらかじめネットワークセグメント A の IP アドレスをプライマリとして設定しておきます。

2.
```
(config-if)# ip address 192.0.2.61 255.255.255.252 secondary
(config-if)# exit
```

さらに，クライアントと接続するインタフェースにネットワークセグメント C の IP アドレスをセカンダリとして設定します。

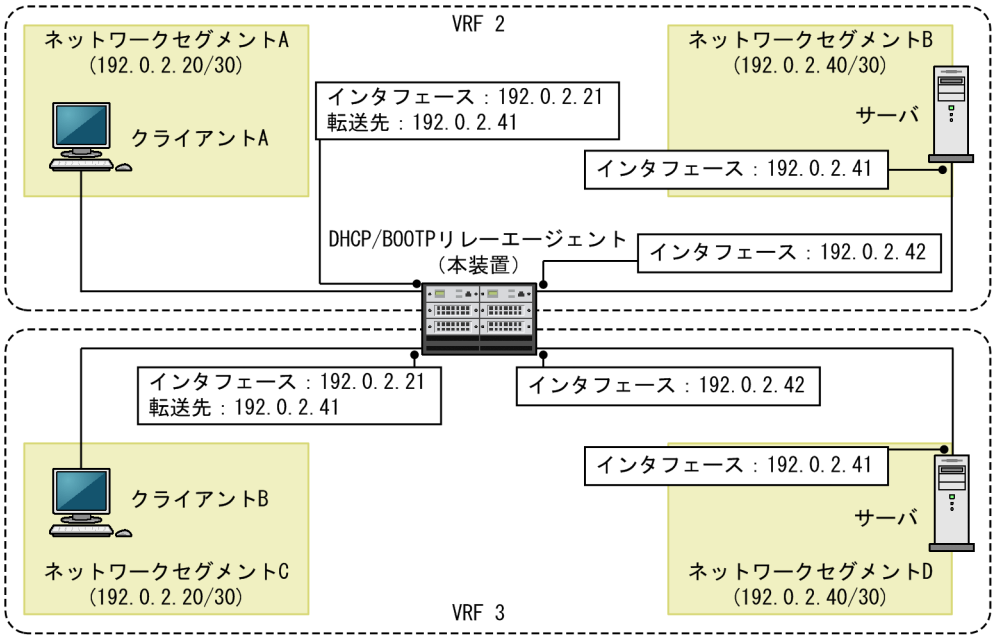
3. **(config)# interface gigabitethernet 1/7**
   (config-if)# ip address 192.0.2.42 255.255.255.252
   (config-if)# exit
   項番 1 と同様に，サーバへ転送するインタフェースにもあらかじめ IP アドレスを設定しておきます。
4. **(config)# interface gigabitethernet 1/5**
   (config-if)# ip helper-address 192.0.2.41
   クライアントと接続するインタフェースに，サーバ宛て DHCP/BOOTP パケットの転送先としてサーバの IP アドレスを設定します。
5. **(config-if)# ip dhcp relay gateway 192.0.2.61**
   (config-if)# exit
   さらに，セカンダリ IP アドレス（ネットワークセグメント C）を DHCP/BOOTP リレーエージェント IP アドレスとして設定します。

10.2.4　VRF 構成での設定

[設定のポイント]

VRF 構成では，VRF ごとにサーバを用意します。VRF ID が異なる場合，サーバの IP アドレスが同じでも別のサーバとして扱われます。

図 10-10　VRF 構成



[コマンドによる設定]

1. **(config)# vrf definition 2**
   (config-vrf)# exit
   (config)# interface gigabitethernet 1/5
   (config-if)# vrf forwarding 2

```
(config-if)# ip address 192.0.2.21 255.255.255.252
(config-if)# exit
```

あらかじめ，VRF とクライアント側インタフェース（VRF 2）の VRF ID，IP アドレスを設定しておきます。

2.
```
(config)# interface gigabitethernet 1/7
(config-if)# vrf forwarding 2
(config-if)# ip address 192.0.2.42 255.255.255.252
(config-if)# exit
```

項番 1 と同様に，サーバへ転送するインタフェース（VRF 2）にもあらかじめ VRF ID，IP アドレスを設定しておきます。

3.
```
(config)# vrf definition 3
(config-vrf)# exit
(config)# interface gigabitethernet 1/9
(config-if)# vrf forwarding 3
(config-if)# ip address 192.0.2.21 255.255.255.252
(config-if)# exit
```

項番 1 と同様に，VRF とクライアント側インタフェース（VRF 3）にもあらかじめ VRF ID，IP アドレスを設定しておきます。

4.
```
(config)# interface gigabitethernet 1/11
(config-if)# vrf forwarding 3
(config-if)# ip address 192.0.2.42 255.255.255.252
(config-if)# exit
```

項番 3 と同様に，サーバへ転送するインタフェース（VRF 3）にもあらかじめ VRF ID，IP アドレスを設定しておきます。

5.
```
(config)# interface gigabitethernet 1/5
(config-if)# ip helper-address 192.0.2.41
(config-if)# exit
```

クライアントと接続するインタフェース（VRF 2）に，サーバ宛て DHCP/BOOTP パケットの転送先として VRF 2 側のサーバの IP アドレスを設定します。

6.
```
(config)# interface gigabitethernet 1/9
(config-if)# ip helper-address 192.0.2.41
(config-if)# exit
```

クライアントと接続するインタフェース（VRF 3）に，サーバ宛て DHCP/BOOTP パケットの転送先として VRF 3 側のサーバの IP アドレスを設定します。

10.2.5 リレーエージェント情報オプション（DHCP Option82）を付ける設定

[設定のポイント]

クライアントと接続するインタフェースで，DHCP/BOOTP パケットにリレーエージェント情報オプション（DHCP Option82）を付けて，サーバへ転送します。

[コマンドによる設定]

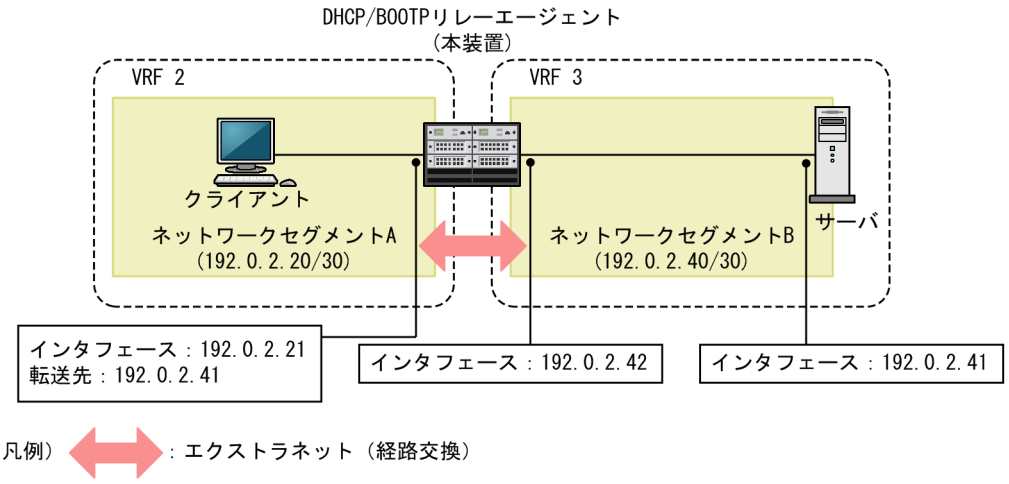
1. (config)# interface gigabitethernet 1/5
   (config-if)# ip address 192.0.2.21 255.255.255.252
   (config-if)# exit
   クライアントと接続するインタフェースにあらかじめ IP アドレスを設定しておきます。
2. (config)# interface gigabitethernet 1/7
   (config-if)# ip address 192.0.2.42 255.255.255.252
   (config-if)# exit
   項番 1 と同様に，サーバへ転送するインタフェースにもあらかじめ IP アドレスを設定しておきます。
3. (config)# interface gigabitethernet 1/5
   (config-if)# ip helper-address 192.0.2.41
   (config-if)# ip dhcp relay information option-insert
   (config-if)# exit
   リレーエージェント情報オプション（DHCP Option82）を付ける設定をします。

10.2.6　VRF（エクストラネット）構成での設定

[設定のポイント]

VRF（エクストラネット）構成では，VRF 間の経路交換を設定します。DHCP/BOOTP パケットの転送先を設定するときに，vrf パラメータを指定します。

図 10-11　VRF（エクストラネット）構成



[コマンドによる設定]

1. (config)# vrf definition 2
   (config-vrf)# exit
   (config)# interface gigabitethernet 1/5
   (config-if)# vrf forwarding 2
   (config-if)# ip address 192.0.2.21 255.255.255.252
   (config-if)# exit
   あらかじめ，VRF とクライアント側インタフェース（VRF 2）の VRF ID，IP アドレスを設定しておきます。
2. (config)# vrf definition 3

```
(config-vrf)# exit
(config)# interface gigabitethernet 1/7
(config-if)# vrf forwarding 3
(config-if)# ip address 192.0.2.42 255.255.255.252
(config-if)# exit
```

項番 1 と同様に，サーバへ転送するインタフェース（VRF 3）にもあらかじめ VRF ID，IP アドレスを設定しておきます。

3.
```
(config)# route-map VRF3PERMIT permit
(config-route-map)# match vrf 3
(config-route-map)# exit
(config)# vrf definition 2
(config-vrf)# import inter-vrf VRF3PERMIT
(config-vrf)# exit
```

VRF 3 の経路へのアクセスを許可して，VRF 3 の経路を VRF 2 に導入するように設定します。

4.
```
(config)# route-map VRF2PERMIT permit
(config-route-map)# match vrf 2
(config-route-map)# exit
(config)# vrf definition 3
(config-vrf)# import inter-vrf VRF2PERMIT
(config-vrf)# exit
```

VRF 2 の経路へのアクセスを許可して，VRF 2 の経路を VRF 3 に導入するように設定します。

5.
```
(config)# interface gigabitethernet 1/5
(config-if)# ip helper-address vrf 3 192.0.2.41
```

クライアントと接続するインタフェース（VRF 2）に，サーバ宛て DHCP/BOOTP パケットの転送先として VRF 3 側のサーバの IP アドレスを設定します。

10.3　オペレーション

10.3.1　運用コマンド一覧

DHCP/BOOTP リレーエージェントの運用コマンド一覧を次の表に示します。

表 10-8　運用コマンド一覧

コマンド名	説明
show ip dhcp relay statistics	DHCP/BOOTP リレーエージェントの統計情報を表示します。
clear ip dhcp relay statistics	DHCP/BOOTP リレーエージェントの統計情報を 0 クリアします。
show ip dhcp relay interface	DHCP/BOOTP リレーエージェントのインタフェース情報を表示します。

10.3.2　DHCP/BOOTP リレーエージェントのインタフェース情報の確認

show ip dhcp relay interface コマンドを実行して, DHCP/BOOTP リレーエージェントのインタフェース情報がネットワーク構成と一致していることを確認してください。

図 10-12　show ip dhcp relay interface コマンドの実行結果

```
>show ip dhcp relay interface
Date 20XX/10/15 12:00:00 UTC
Interface:Eth1/1            Gateway:192.0.2.61
Interface:Eth1/2            Gateway:192.0.2.21      VRF:2
Interface:Eth1/4            Gateway:192.0.2.61      VRF:2
Interface:Eth1/3            Gateway:192.0.2.21      VRF:3
>
```

11 DHCPv6 リレーエージェント

この章では，DHCPv6 リレーエージェントの解説および操作方法について説明します。

11.1　解説

11.1.1　概要

DHCPv6 リレーエージェントは，DHCPv6 クライアント（以降，クライアント）と DHCPv6 サーバ（以降，サーバ）が異なるネットワークセグメントにあるネットワーク構成のときに，DHCPv6 パケットを異なるネットワークセグメントへレイヤ 7 転送します。

クライアントはサーバが提供するサービスを利用するために，リンクローカルマルチキャストで通信します。このとき，異なるネットワークセグメントにあるクライアントとサーバ間では通信できないため，クライアントとサーバは同一ネットワークセグメントに設置されている必要があります。しかし，DHCPv6 リレーエージェントを使用すると，DHCPv6 リレーエージェントが DHCPv6 パケットを異なるネットワークセグメントに転送するため，異なるネットワークセグメントにあるクライアントとサーバ間で通信できます。DHCPv6 リレーエージェントのネットワーク構成例を次に示します。

図 11-1　DHCPv6 リレーエージェントのネットワーク構成例（1 段）

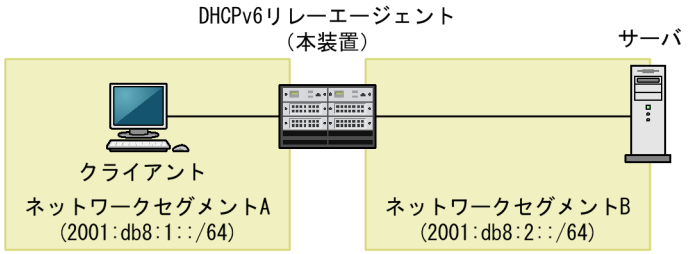
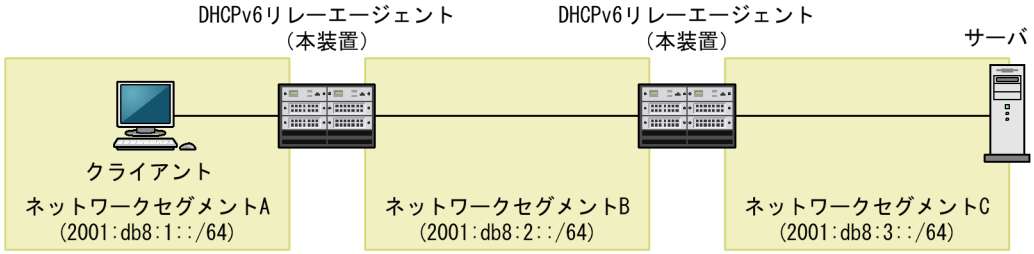


図 11-2　DHCPv6 リレーエージェントのネットワーク構成例（多段）



11.1.2　サポート範囲

DHCPv6 リレーエージェントでサポートする機能を次の表に示します。

表 11-1　DHCPv6 リレーエージェントでサポートする機能

項目	仕様	サポート
接続形態（クライアント側）	クライアント直接	○
	DHCPv6 リレーエージェント経由	○
接続形態（サーバ側）	サーバ直接	○
	DHCPv6 リレーエージェント経由	○
転送	サーバまたは DHCPv6 リレーエージェント宛て	○

項目	仕様	サポート
	クライアント宛て	○
	ネットワークセグメント内の全サーバ宛て※1	○
	ネットワークセグメント内の全サーバおよび全 DHCPv6 リレーエージェント宛て※2	×
	非一時的アドレス（IA_NA）	○
	一時的アドレス（IA_TA）	○
	プレフィックス（IA_PD）	○
	送信元インタフェース変更	○※3
インタフェース	イーサネットインタフェース	○
	イーサネットサブインタフェース	○
	ポートチャネルインタフェース	○
	ポートチャネルサブインタフェース	○
	VLAN インタフェース	○
	ループバックインタフェース	×※3
	Null インタフェース	×
	マネージメントポート	×
	シリアル接続ポート（AUX）	×
バインディングデータベース	非一時的アドレス（IA_NA）	×
	一時的アドレス（IA_TA）	×
	プレフィックス（IA_PD）	○※4
IPv6 スタティック経路自動生成	非一時的アドレス（IA_NA）	×
	一時的アドレス（IA_TA）	×
	プレフィックス（IA_PD）	○※4
IPv6	フラグメント送信（サーバ側）	○
	フラグメント受信（サーバ側）	○
	フラグメント送信（クライアント側）	○
	フラグメント受信（クライアント側）	○

（凡例）　○：サポートする　×：サポートしない

注※1

IPv6 サイトローカルマルチキャストアドレス宛て（ff05::1:3）に転送します。

注※2

IPv6 リンクローカルマルチキャストアドレス宛て（ff02::1:2）に転送します。

注※3

サーバまたは DHCPv6 リレーエージェント宛てに転送する場合，送信元インタフェースをループバックインタフェースに変更できます。

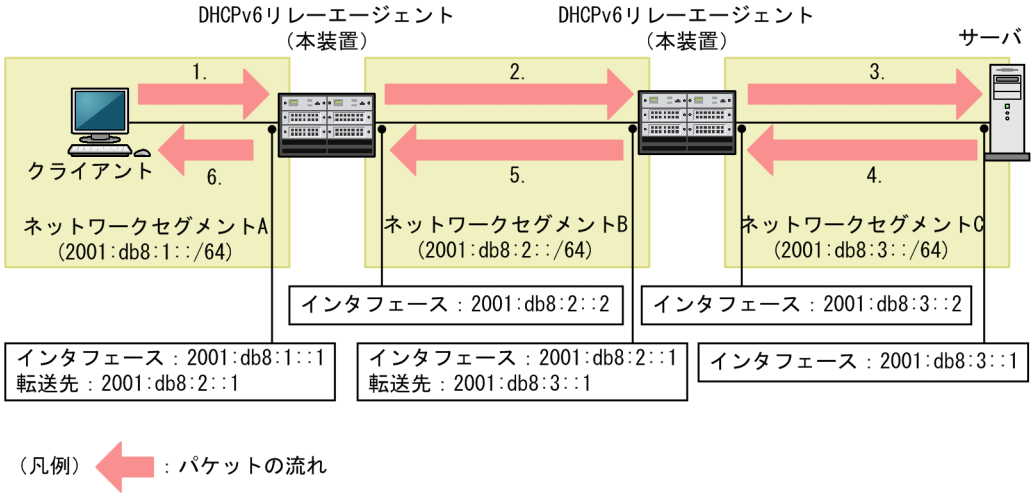
注※4

クライアントと直接接続している場合だけです。

11.1.3　DHCPv6 パケット転送時の設定内容

DHCPv6 リレーエージェントが DHCPv6 パケットを転送するときの設定内容を次に示します。

図 11-3　DHCPv6 パケットの設定内容



パケット（図中の番号）	パケット内の値			
	宛先 IPv6 アドレス	送信元 IPv6 アドレス	宛先 UDP ポート番号	送信元 UDP ポート番号
1.	ff02::1:2	クライアントリンクローカルアドレス	547	任意
2.	2001:db8:2::1	2001:db8:2::2	547	547
3.	2001:db8:3::1	2001:db8:3::2	547	547
4.	2001:db8:3::2	2001:db8:3::1	547	任意
5.	2001:db8:2::2	2001:db8:2::1	547	547
6.	クライアントリンクローカルアドレス	DHCPv6 リレーエージェントリンクローカルアドレス	546	547

(1)　インタフェース ID オプション

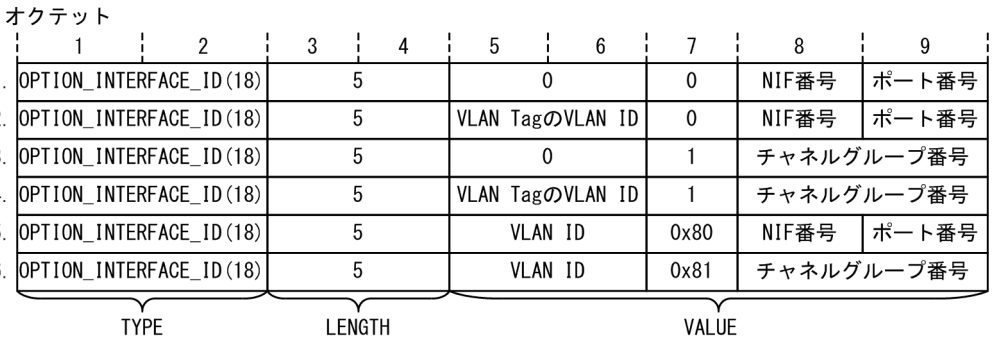
DHCPv6 リレーエージェントはクライアントから受信した DHCPv6 パケットにインタフェース ID オプションを付けて，サーバへ転送します。

インタフェース ID オプションには，クライアントから DHCPv6 パケットを受信したインタフェースの情報が含まれています。このため，サーバから受信した DHCPv6 パケットをクライアントに送信するとき，

DHCPv6 リレーエージェントは受信した DHCPv6 パケットに付いているインタフェース ID オプションを基にクライアントへの転送先インタフェースを判断します。

DHCPv6 パケットに付けるインタフェース ID オプションは，クライアント側のインタフェース設定によって異なります。インタフェース ID オプションのフォーマットを次の図に示します。

図 11-4　インタフェース ID オプションのフォーマット



図中の番号に対応するクライアント側のインタフェース設定は次のとおりです。

1. イーサネットインタフェース，またはイーサネットサブインタフェース（VLAN Tag なし）
2. イーサネットサブインタフェース（VLAN Tag あり）
3. ポートチャネルインタフェース，またはポートチャネルサブインタフェース（VLAN Tag なし）
4. ポートチャネルサブインタフェース（VLAN Tag あり）
5. VLAN インタフェースのスイッチポート（チャネルグループに所属しない）
6. VLAN インタフェースのスイッチポート（チャネルグループに所属する）

(2)　送信元インタフェースの自動選択

コンフィグレーションコマンド ipv6 dhcp relay source-interface で送信元アドレスとして使用するインタフェースを指定していない場合，DHCPv6 リレーエージェントがサーバに DHCPv6 パケットを転送するときに送信元 IPv6 アドレスを自動で選択します。

(a)　ループバックインタフェースを選択する場合の動作

DHCPv6 パケットの送信元となるグローバルネットワークまたは VRF で，ループバックインタフェースに IPv6 アドレスが設定されている場合，コンフィグレーションコマンド no system-source-address が設定されていないループバックインタフェースの IPv6 アドレスを使用します。DHCPv6 パケットの送信元として使用するループバックインタフェースは，転送先アドレスによって決定します。

転送先がマルチキャスト（コンフィグレーションコマンド ipv6 dhcp relay destination で，all-servers パラメータを指定）

指定した転送先インタフェースが所属するグローバルネットワークまたは VRF のループバックインタフェースを使用します。

転送先がユニキャスト

クライアント側インタフェースが所属するグローバルネットワークまたは VRF のループバックインタフェースを使用します。

なお，ループバックインタフェースに IPv6 アドレスが設定されている場合，サーバは DHCPv6 パケットをインタフェースに依存しない装置固有のアドレスに対して送信します。そのため，優先経路のインタフェースに障害が発生した場合でも，冗長経路のインタフェースで DHCPv6 パケットを受信できます。

(b)　ループバックインタフェースを選択しない場合の動作

サーバ側の送信元インタフェースのアドレスを送信元 IPv6 アドレスとして使用します。そのため，サーバと DHCPv6 リレーエージェント間に冗長経路のある構成であっても，優先経路のインタフェースに障害が発生すると，障害が発生する前に DHCPv6 リレーエージェントが中継した DHCPv6 パケットの応答を受信できません。

11.1.4　プレフィックス委任情報の学習

プレフィックス委任の管理情報（以降，バインディング（IA_PD）と呼びます）は DHCPv6 リレーエージェントで保持して，IPv6 スタティック経路自動生成の情報として使用します。なお，IPv6 ユニキャストアドレスの割り当て（IA_NA または IA_TA）は学習対象外となります。

バインディング（IA_PD）を更新する契機を次の表に示します。

表 11-2　バインディング（IA_PD）を更新する契機

変更内容	契機
追加	DHCPv6 REPLY メッセージの転送
更新	DHCPv6 REPLY メッセージの転送
削除	バインディング（IA_PD）に対応する DHCPv6 RELEASE メッセージの転送
	バインディング（IA_PD）のエージングアウト
	DHCPv6 パケットの転送先の削除（コンフィグレーションコマンド no ipv6 dhcp relay destination）※
	手動によるバインディング（IA_PD）の削除（運用コマンド clear ipv6 dhcp relay binding）

注※
実行したインタフェース内のすべてのバインディング（IA_PD）を削除します。

11.1.5　プレフィックス委任に対する IPv6 スタティック経路自動生成

クライアントに経路情報の広告機能がない場合，コンフィグレーションコマンド ipv6 dhcp relay static-route-setting で IPv6 スタティック経路自動生成を有効にすると，本装置でプレフィックス委任に対する IPv6 スタティック経路を自動で生成します。

本装置で自動生成する IPv6 スタティック経路のパラメータを次の表に示します。

表 11-3　自動生成する IPv6 スタティック経路のパラメータ

パラメータ	設定値
経路の VRF（対象が VRF 向き経路の場合だけ）	クライアント側の VRF ID
宛先 IPv6 プレフィックス	IA_PD の IPv6 プレフィックス
プレフィックス長	IA_PD のプレフィックス長

パラメータ	設定値
IPv6 ネクストホップアドレス	クライアントリンクローカルアドレス
ディスタンス値	250
上記以外	デフォルト値

11.1.6　DHCPv6 リレーエージェント使用時の注意事項

(1)　IPv6 マルチキャストとの共存について

本装置で IPv6 マルチキャストと DHCPv6 リレーエージェントを同時に使用する場合，DHCPv6 リレーエージェントの転送先として各サーバを個別に指定することを推奨します。

本装置の DHCPv6 パケットの転送先として全サーバ宛てを指定して，かつ IPv6 マルチキャストを同時に使用する場合は，次の点に注意してください。

- 本装置の対向ルータ側で，本装置と接続するインタフェースのリンクローカルアドレスをインタフェース内の最大値に設定して，IPv6 マルチキャストでの中継代表ルータ（DR）になるようにしてください。なお，詳細な設定方法は対向ルータのマニュアルを参照してください。
- 対向ルータがランデブーポイントとなるように，本装置および対向ルータの IPv6 マルチキャストを設定してください。
- 本装置とサーバの間のルータで DHCPv6 パケットを IPv6 マルチキャスト中継するネットワーク構成で，かつ送信元インタフェースを変更している場合，本装置の対向ルータ側で本装置のループバックインタフェースの IPv6 アドレスを設定して，マルチキャストサーバ仮想接続機能の送信者となるようにしてください。なお，詳細な設定方法は対向ルータのマニュアルを参照してください。

11.2　コンフィグレーション

11.2.1　コンフィグレーションコマンド一覧

DHCPv6 リレーエージェントのコンフィグレーションコマンド一覧を次の表に示します。

表 11-4　コンフィグレーションコマンド一覧

コマンド名	説明
ipv6 dhcp relay destination	DHCPv6 パケットの転送先を設定します。
ipv6 dhcp relay maximum-hop-count	DHCPv6 パケットの最大ホップ数を設定します。
ipv6 dhcp relay source-interface	送信元インタフェースを指定します。
ipv6 dhcp relay static-route-setting	DHCPv6 リレーエージェントを経由して委任したプレフィックスから IPv6 スタティック経路を自動で生成します。

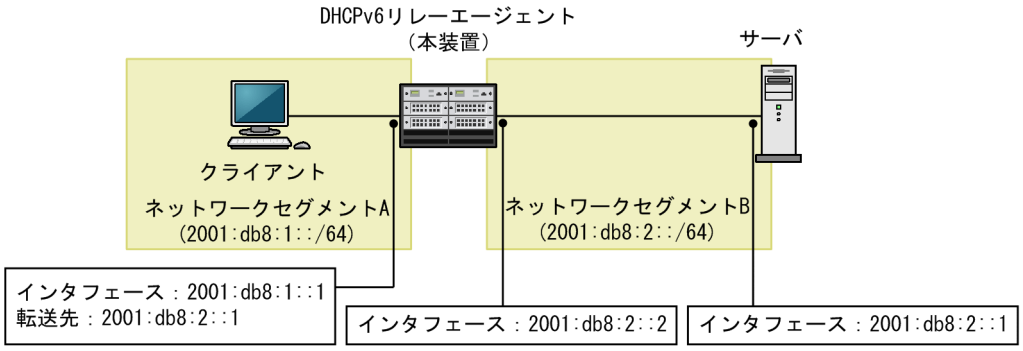
11.2.2　DHCPv6 パケットをサーバへ転送する設定（基本設定）

[設定のポイント]

DHCPv6 リレーエージェントで，サーバ宛て DHCPv6 パケットの転送先としてサーバの IPv6 アドレスを設定します。

DHCPv6 リレーエージェントとサーバはユニキャストで通信します。そのため，DHCPv6 リレーエージェントとサーバがユニキャスト通信できるようなネットワーク構成としてください。特に，DHCPv6 リレーエージェントの送信元インタフェースを変更している場合，直接接続でも経路情報を設定してください。

図 11-5　DHCPv6 パケットをサーバへ転送する構成（基本構成）



[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/5**
   (config-if)# ipv6 enable
   (config-if)# ipv6 address 2001:db8:1::1/64
   (config-if)# exit
   クライアントと接続するインタフェースにあらかじめ IPv6 アドレスを設定しておきます。
2. **(config)# interface gigabitethernet 1/7**
   (config-if)# ipv6 enable

```
(config-if)# ipv6 address 2001:db8:2::2/64
(config-if)# exit
```

項番 1 と同様に，サーバへ転送するインタフェースにもあらかじめ IPv6 アドレスを設定しておきます。

3.
```
(config)# interface gigabitethernet 1/5
(config-if)# ipv6 dhcp relay destination 2001:db8:2::1
(config-if)# exit
```

クライアントと接続するインタフェースに，サーバ宛て DHCPv6 パケットの転送先としてサーバの IPv6 アドレスを設定します。

4.
```
(config)# ipv6 dhcp relay static-route-setting
```

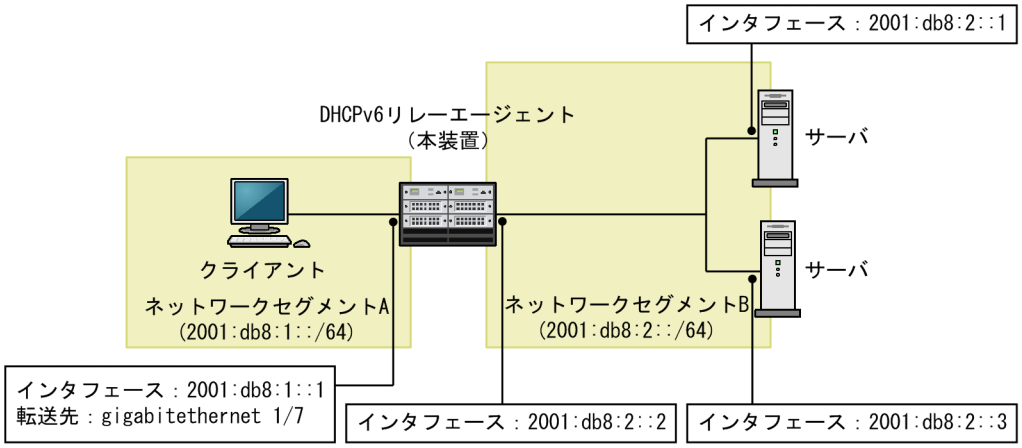
委任したプレフィックスから IPv6 スタティック経路を自動で生成する設定をします。

11.2.3　DHCPv6 パケットをネットワークセグメント内の全サーバへ転送する設定

[設定のポイント]

DHCPv6 リレーエージェントで，サーバ宛て DHCPv6 パケットの転送先としてサーバに接続するインタフェースを設定します。

図 11-6　DHCPv6 パケットをネットワークセグメント内の全サーバへ転送する構成



[コマンドによる設定]

1.
```
(config)# interface gigabitethernet 1/5
(config-if)# ipv6 enable
(config-if)# ipv6 address 2001:db8:1::1/64
(config-if)# exit
```

クライアントと接続するインタフェースにあらかじめ IPv6 アドレスを設定しておきます。

2.
```
(config)# interface gigabitethernet 1/7
(config-if)# ipv6 enable
(config-if)# ipv6 address 2001:db8:2::2/64
(config-if)# exit
```

項番 1 と同様に，サーバへ転送するインタフェースにもあらかじめ IPv6 アドレスを設定しておきます。

3.
```
(config)# interface gigabitethernet 1/5
```

```
(config-if)# ipv6 dhcp relay destination all-servers interface gigabitethernet 1/7
(config-if)# exit
```

クライアントと接続するインタフェースに，DHCPv6 パケットの転送先としてサーバに接続するインタフェースを設定します。

4. `(config)# ipv6 dhcp relay static-route-setting`

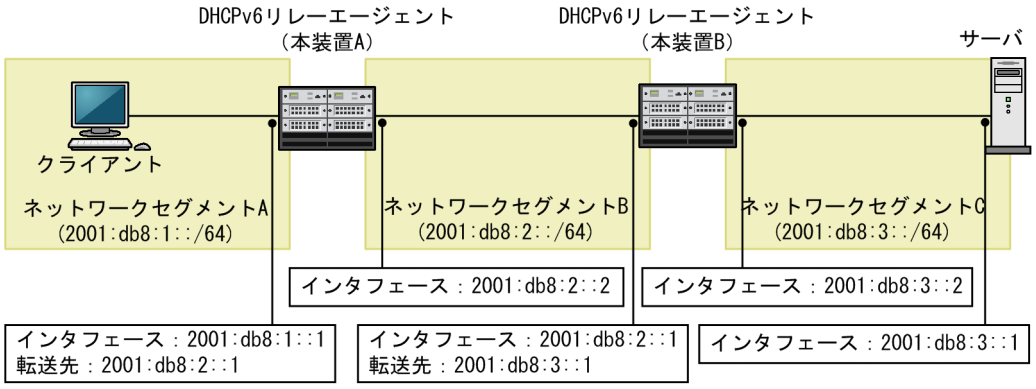
委任したプレフィックスから IPv6 スタティック経路を自動で生成する設定をします。

11.2.4　DHCPv6 パケットを複数の DHCPv6 リレーエージェントを経由してサーバへ転送する設定

[設定のポイント]

一段目の DHCPv6 リレーエージェント（本装置 A）で，サーバ宛て DHCPv6 パケットの転送先として二段目の DHCPv6 リレーエージェント（本装置 B）の IPv6 アドレスを設定します。

図 11-7　複数の DHCPv6 リレーエージェントを経由する構成



[コマンドによる設定]

- 本装置 A の設定

1.
```
(config)# interface gigabitethernet 1/5
(config-if)# ipv6 enable
(config-if)# ipv6 address 2001:db8:1::1/64
(config-if)# exit
```

クライアントと接続するインタフェースにあらかじめ IPv6 アドレスを設定しておきます。

2.
```
(config)# interface gigabitethernet 1/7
(config-if)# ipv6 enable
(config-if)# ipv6 address 2001:db8:2::2/64
(config-if)# exit
```

項番 1 と同様に，サーバへ転送するインタフェースにもあらかじめ IPv6 アドレスを設定しておきます。

3.
```
(config)# interface gigabitethernet 1/5
(config-if)# ipv6 dhcp relay destination 2001:db8:2::1
(config-if)# exit
```

クライアントと接続するインタフェースに，サーバ宛て DHCPv6 パケットの転送先として二段目の DHCPv6 リレーエージェントでクライアントと接続するインタフェースの IPv6 アドレスを設定します。

4. (config)# ipv6 dhcp relay static-route-setting

   委任したプレフィックスから IPv6 スタティック経路を自動で生成する設定をします。

- 本装置 B の設定

1. (config)# interface gigabitethernet 1/5
   (config-if)# ipv6 enable
   (config-if)# ipv6 address 2001:db8:2::1/64
   (config-if)# exit

   クライアントと接続するインタフェースにあらかじめ IPv6 アドレスを設定しておきます。

2. (config)# interface gigabitethernet 1/7
   (config-if)# ipv6 enable
   (config-if)# ipv6 address 2001:db8:3::2/64
   (config-if)# exit

   項番 1 と同様に，サーバへ転送するインタフェースにもあらかじめ IPv6 アドレスを設定しておきます。

3. (config)# interface gigabitethernet 1/5
   (config-if)# ipv6 dhcp relay destination 2001:db8:3::1
   (config-if)# exit

   クライアントと接続するインタフェースに，サーバ宛て DHCPv6 パケットの転送先としてサーバの IPv6 アドレスを設定します。

11.2.5　VRF（経路交換によるエクストラネット）構成での設定

[設定のポイント]

VRF（エクストラネット）構成では，VRF 間の経路交換を設定します。

[コマンドによる設定]

1. (config)# vrf definition 2
   (config-vrf)# exit
   (config)# interface gigabitethernet 1/5
   (config-if)# vrf forwarding 2
   (config-if)# ipv6 enable
   (config-if)# exit

   あらかじめ，VRF とクライアント側インタフェース（VRF 2）の VRF ID を設定しておきます。

2. (config)# vrf definition 3
   (config-vrf)# exit
   (config)# interface gigabitethernet 1/7
   (config-if)# vrf forwarding 3
   (config-if)# ipv6 enable
   (config-if)# ipv6 address 2001:db8:2::2/64
   (config-if)# exit

   サーバへ転送するインタフェース（VRF 3）にもあらかじめ VRF ID，IPv6 アドレスを設定しておきます。

3. (config)# interface loopback 2

```
(config-if)# vrf forwarding 2
(config-if)# ipv6 address 2001:db8:1::1
(config-if)# exit
```

ループバックインタフェースに，IPv6 アドレスを設定します。

4.
```
(config)# route-map VRF2PERMIT permit
(config-route-map)# match interface loopback 2
(config-route-map)# exit
(config)# vrf definition 3
(config-vrf)# ipv6 import inter-vrf VRF2PERMIT
(config-vrf)# exit
```

経路フィルタで VRF 2 のループバックインタフェースを許可して，ループバックインタフェース 2 の経路を VRF 3 に導入するように設定します。

5.
```
(config)# route-map VRF3PERMIT permit
(config-route-map)# match vrf 3
(config-route-map)# exit
(config)# vrf definition 2
(config-vrf)# ipv6 import inter-vrf VRF3PERMIT
(config-vrf)# exit
```

VRF 3 の経路へのアクセスを許可して，VRF 3 の経路を VRF 2 に導入するように設定します。

6.
```
(config)# interface gigabitethernet 1/5
(config-if)# ipv6 dhcp relay destination 2001:db8:2::1
```

クライアントと接続するインタフェース（VRF 2）に，DHCPv6 パケットの転送先として VRF 3 側のサーバの IPv6 アドレスを設定します。

11.3　オペレーション

11.3.1　運用コマンド一覧

DHCPv6 リレーエージェントの運用コマンド一覧を次の表に示します。

表 11-5　運用コマンド一覧

コマンド名	説明
show ipv6 dhcp relay statistics	DHCPv6 リレーエージェントの統計情報を表示します。
clear ipv6 dhcp relay statistics	DHCPv6 リレーエージェントの統計情報を削除します。
show ipv6 dhcp relay binding	DHCPv6 リレーエージェントのバインディング (IA_PD) を表示します。
clear ipv6 dhcp relay binding	DHCPv6 リレーエージェントのバインディング (IA_PD) を削除します。
restart ipv6-dhcp relay	DHCPv6 リレーエージェントプログラムを再起動します。
dump protocols ipv6-dhcp relay	DHCPv6 リレーエージェントプログラムで採取しているログをファイルへ出力します。

11.3.2　プレフィックス委任の確認

show ipv6 dhcp relay binding コマンドを実行して，サーバからクライアントへ委任されたプレフィックスを確認してください。

図 11-8　show ipv6 dhcp relay binding コマンドの実行結果

```
> show ipv6 dhcp relay binding
Date 20XX/04/09 12:00:00 UTC
Total : 2 prefixes
Interface        Prefix                                    Expire
Eth1/1           2001:db8:5678::/48                        23h59m
Eth1/2           2001:db8:1234::/48                        59m59s
>
```

11.3.3　IPv6 スタティック経路自動生成の確認

IPv6 スタティック経路を自動生成した場合，show ipv6 route コマンドを実行してプレフィックス委任に伴って自動生成された経路情報を確認してください。

図 11-9　show ipv6 route コマンドの実行結果

```
> show ipv6 route -s static
Date 20XX/04/09 12:00:00 UTC
Total: 2 routes
Destination                                Next Hop
Interface      Metric   Protocol  Age
2001:db8:1::/48                            fe80::1%Eth1/1
Eth1/1         0/0      Static     4m 33s , <Active Gateway Dhcp>
2001:db8:2::/48                            fe80::2%Eth1/2
Eth1/2         0/0      Static     4m 33s , <Active Gateway Dhcp>
>
```

12 VRRP

VRRP（Virtual Router Redundancy Protocol）はルータに障害が発生した場合でも, 同一イーサネット上の別ルータを経由して端末の通信経路を確保することを目的としたホットスタンバイ機能です。この章では VRRP について説明します。

12.1 解説

VRRP（Virtual Router Redundancy Protocol）はルータに障害が発生した場合でも，同一イーサネット上の別ルータを経由して端末の通信経路を確保することを目的としたホットスタンバイ機能です。

VRRP を使用すると，同一イーサネット上の複数のルータから構成される仮想ルータを設定できます。端末がデフォルトゲートウェイとしてこの仮想ルータを設定しておくと，ルータに障害が発生したときの別ルータへの切り替えを意識することなく，通信を継続できます。

仮想ルータは 1 から 255 までの仮想ルータ ID を持ち，同一イーサネット上の同一の仮想ルータ ID を持つ仮想ルータ同士が，パケットのルーティングを行う 1 台のマスタの仮想ルータと，パケットのルーティングを行わないホットスタンバイである 1 台以上のバックアップの仮想ルータを構成します。

12.1.1 仮想ルータの MAC アドレスと IP アドレス

仮想ルータは自身の物理的な MAC アドレスとは別に，仮想ルータ用の MAC アドレスとして仮想 MAC アドレスを持ちます。仮想 MAC アドレスは，仮想ルータ ID から自動的に生成されます。

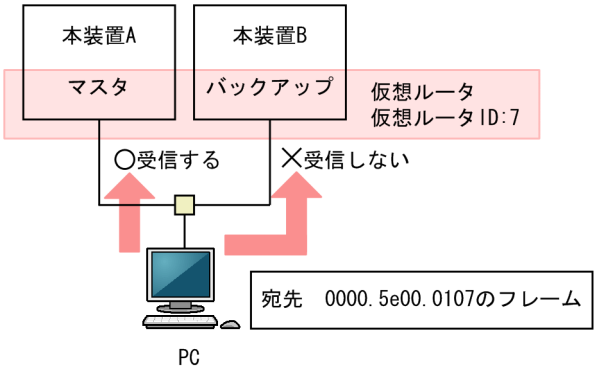
サポートしている VRRP の規格と仮想 MAC アドレスの対応を次の表に示します。

表 12-1 VRRP の規格と仮想 MAC アドレスの対応

規格		仮想 MAC アドレス
IPv4	RFC3768	0000.5e00.01{仮想ルータ ID}
	RFC5798	0000.5e00.01{仮想ルータ ID}
	draft-ietf-vrrp-unified-spec-02	0000.5e00.01{仮想ルータ ID}
IPv6	RFC5798	0000.5e00.02{仮想ルータ ID}
	draft-ietf-vrrp-ipv6-spec-02	0000.5e00.01{仮想ルータ ID}
	draft-ietf-vrrp-ipv6-spec-07	0000.5e00.02{仮想ルータ ID}
	draft-ietf-vrrp-unified-spec-02	0000.5e00.02{仮想ルータ ID}

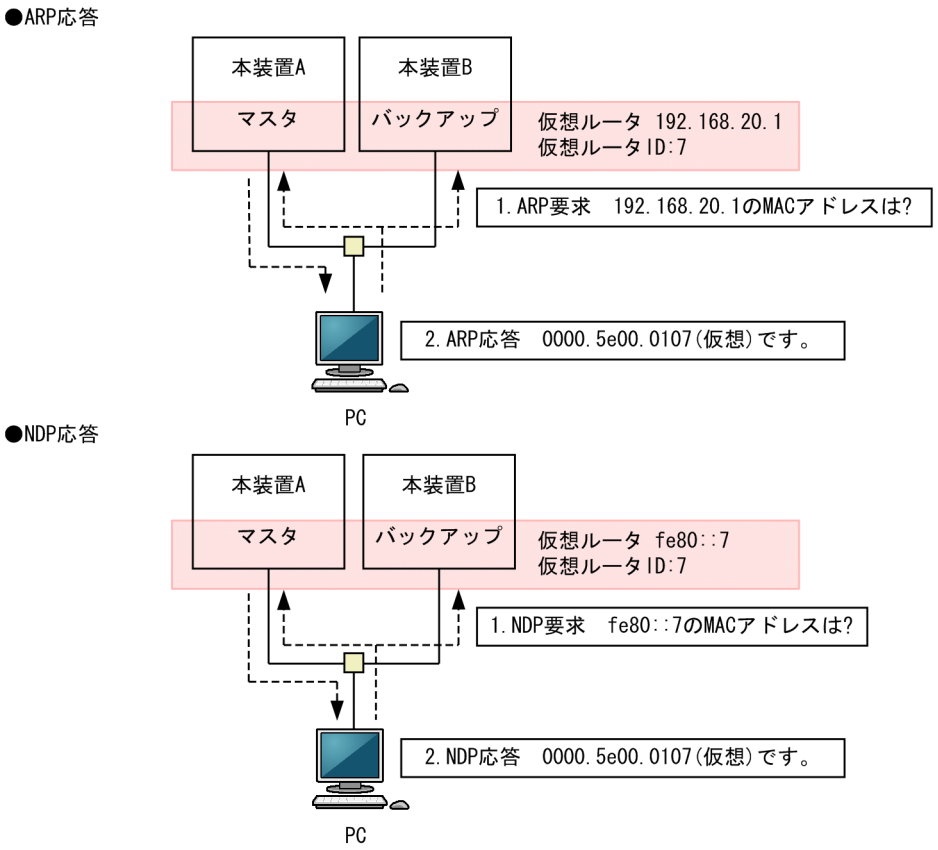
マスタの仮想ルータは仮想 MAC アドレス宛てのイーサネットフレームを受信してパケットをフォワーディングする能力を持ちますが，バックアップの仮想ルータは仮想 MAC アドレス宛てのフレームを受信しません。VRRP は仮想ルータの状態に応じて仮想 MAC アドレス宛てイーサネットフレームを受信するかどうかを制御します。マスタの仮想ルータは仮想 MAC 宛てフレームを受信すると，ルーティングテーブルに従って IP パケットのフォワーディング処理を行います。そのため，端末は仮想 MAC アドレスを宛先としてフレームを送信することで，マスタとバックアップが切り替わったあとでも通信を継続できます。仮想 MAC アドレス宛てフレームの受信を次の図に示します。

図 12-1　仮想 MAC 宛てフレームの受信



仮想ルータは仮想ルータ用の IP アドレスである仮想 IP アドレスを持ちます。マスタの仮想ルータは，仮想 IP アドレスに対する ARP 要求パケットまたは NDP 要求パケットを受信すると，常に仮想 MAC アドレスを使用して ARP 応答または NDP 応答します。仮想 MAC アドレスによる ARP 応答および NDP 応答を次の図に示します。

図 12-2　仮想 MAC アドレスによる ARP 応答および NDP 応答

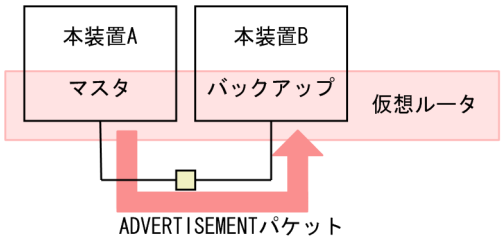


仮想ルータをデフォルトルータとして使用する PC などのホストは，自 ARP キャッシュテーブル内に仮想 IP アドレス宛てのフレームは仮想 MAC アドレス宛てに送信するように学習します。このように学習されたホストは常に仮想ルータへフレームを送信するときに仮想 MAC アドレスを宛先に指定するようになるため，VRRP のマスタ／バックアップの切り替えが発生した場合でも，通信を継続できます。

12.1.2　VRRP における障害検出の仕組み

マスタの仮想ルータは定期的な周期（デフォルト 1 秒）で ADVERTISEMENT パケットと呼ばれる稼働状態確認用のパケットを，仮想ルータを設定した IP インタフェースから送信します。バックアップの仮想ルータはマスタの仮想ルータが送信する ADVERTISEMENT パケットを受信することによって，マスタの仮想ルータに障害がないことを確認します。ADVERTISEMENT パケットの送信を次の図に示します。

図 12-3　ADVERTISEMENT パケットの送信



マスタの仮想ルータに障害が発生した場合，ADVERTISEMENT パケットを送信できません。例えば，装置全体がダウンしてしまった場合や，仮想ルータが設定されている IP インタフェースからパケットを送信できなくなるような障害が発生した場合，ケーブルの抜けなどの場合です。

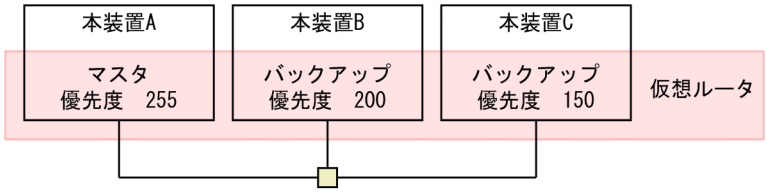
バックアップの仮想ルータは一定の間 ADVERTISEMENT パケットをマスタの仮想ルータから受信しなかった場合に，マスタの仮想ルータに障害が発生したと判断し，バックアップからマスタへと状態を変化させます。

12.1.3　マスタの選出方法

(1)　優先度

複数の仮想ルータの中からマスタの仮想ルータを選出するために，VRRP では優先度を使用します。この優先度は仮想ルータに設定できます。設定できる値は 1 から 255 までの数値で，デフォルトは 100 です。この数値が大きいほど優先度は高くなります。インタフェースに付与されている IP アドレスと仮想ルータの IP アドレスが等しい（IP アドレスの所有者）場合，最も優先度が高い 255 に自動的に設定されます。マスタの仮想ルータの選出を次の図に示します。

図 12-4　マスタの選出



この図の場合，優先度が最も高い仮想ルータ A がマスタになります。仮想ルータ A がダウンした場合は，次に優先度の高い仮想ルータ B がマスタへと変化します。仮想ルータ A と仮想ルータ B の両方がダウンした場合にだけ仮想ルータ C がマスタになります。

マスタになる装置を明確にするため，同じイーサネット上の同じ仮想ルータ ID の仮想ルータには，異なる優先度を設定してください。優先度の同じ仮想ルータが存在する場合は，どちらがマスタになるか不定のため，動作が期待どおりにならないおそれがあります。

(2) 自動切り戻しおよび自動切り戻しの抑止

VRRP では，優先度の高いバックアップの仮想ルータが，自ルータよりも優先度の低いマスタの仮想ルータを検出すると，自動的にマスタへ状態を変化させます。逆に，マスタの仮想ルータが，自ルータより優先度の高い仮想ルータの存在を検出したときは自動的にバックアップへと状態を変化させます。

「図 12-4　マスタの選出」の構成を例にしてみると，仮想ルータ A と仮想ルータ B がダウンし仮想ルータ C がマスタになっている状態から，仮想ルータ B が復旧すると，仮想ルータ C よりも優先度の高い仮想ルータ B がマスタに変化し，仮想ルータ C がマスタからバックアップへ状態を変化させることになります。

この自動切り戻しを抑止する設定ができます。切り戻し抑止には，次の 2 とおりの方法があります。

- PREEMPT モードによる抑止

  自動切り戻しさせたくない場合には，コンフィグレーションコマンド no vrrp preempt で PREEMPT モードを OFF に設定してください。PREEMPT モードを OFF に設定すれば，バックアップの仮想ルータが自ルータよりも優先度の低い仮想ルータがマスタになっていることを検出しても，状態をマスタへ変化させることはありません。

- 抑止タイマによる抑止

  自動切り戻しの開始を任意の時間遅延させたい場合には，コンフィグレーションコマンド vrrp preempt delay で抑止タイマを設定してください。本タイマ値は，自動切り戻し要因を検出してから自動切り戻し処理の開始時間を遅らせるものであり，状態が完全に切り変わるまでには，設定した時間プラス数秒の時間を要します。

PREEMPT モードを設定した場合も抑止タイマを設定した場合も，対象となる仮想ルータが IP アドレスの所有者（優先度 255）の場合は，切り戻しの抑止は有効になりません。

マスタの仮想ルータが故障などによって運用不可状態になったことを検出し，かつ残った仮想ルータの中で自ルータの優先度が最も高いことを検出した場合には，切り戻し抑止中であってもマスタに遷移します。

- 手動による切り戻し

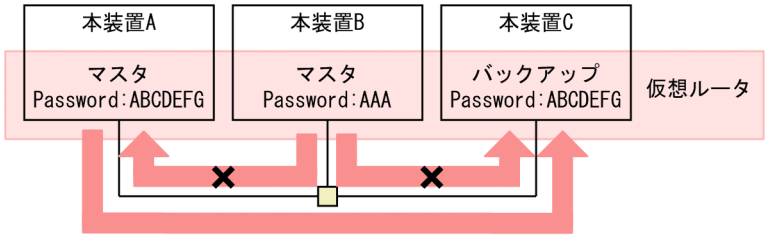
  自動切り戻し抑止中状態でも，運用コマンド swap vrrp によって仮想ルータの切り戻し処理を起動できます。

  自動切り戻し抑止によってバックアップ状態に留まっている装置に対して本コマンドを指定すると，コマンド実行時にマスタの仮想ルータよりコマンドを指定したバックアップの仮想ルータの優先度が高い場合は，コマンドを指定した仮想ルータがマスタ状態に遷移します。

12.1.4 ADVERTISEMENT パケットの認証

ADVERTISEMENT パケットはリンクローカルスコープのマルチキャストアドレス（IPv4 では 224.0.0.18，IPv6 では ff02::12）を使用します。また，仮想ルータは IP ヘッダの TTL または HopLimit が 255 以外のパケットを受信しないため，ルータ越えを伴う遠隔からの攻撃を防ぐことができます。さらに，本装置ではテキストパスワードによる VRRP の ADVERTISEMENT パケットの認証をサポートします。8 文字以内のパスワードを仮想ルータに設定すると，パスワードが異なる ADVERTISEMENT パケットを廃棄します。パスワードの不一致を次の図に示します。

図 12-5　パスワードの不一致



この図の例では仮想ルータ B のパスワードが仮想ルータ A および仮想ルータ C と異なっているため，仮想ルータ B から送信された ADVERTISEMENT パケットを仮想ルータ A や仮想ルータ C が受け取っても廃棄します。この場合，仮想ルータ C は仮想ルータ A からの ADVERTISEMENT パケットだけを受信して処理します。そのため，ADVERTISEMENT パケット認証に失敗するような，不正に設置された仮想ルータの動作を防止できます。

12.1.5　アクセプトモード

IP アドレス所有者でない仮想ルータは，マスタであっても仮想 IP アドレス宛てのパケットに対して応答しません。しかし，ping によってネットワーク機器の状態を確認することは一般的に行われます。

本装置は，アクセプトモードをサポートします。アクセプトモードは，マスタの仮想ルータが仮想 IP アドレス宛てのパケットに対して応答できるようにする機能です。仮想ルータの状態を外部から監視するために，コンフィグレーションコマンド vrrp accept でアクセプトモードを設定することで，マスタの仮想ルータがアドレス所有者でなくても，ICMP echo request パケットを受信し，ICMP echo reply パケットを返信できます。

12.1.6　VRRP のサポート規格

本装置では複数の VRRP の規格をサポートしているため，既存システムで採用されている規格に合わせて，柔軟に仮想ルータを設定できます。VRRP の規格を仮想ルータに適用するには，コンフィグレーションコマンド vrrp mode で VRRP 動作モードに対応するパラメータを設定します。

サポートしている VRRP の規格と対応する vrrp mode コマンドのパラメータを次の表に示します。

表 12-2　VRRP の規格と対応する vrrp mode コマンドのパラメータ

規格		パラメータ
IPv4	RFC3768	rfc3768
	RFC5798	rfc5798（デフォルト動作）
	draft-ietf-vrrp-unified-spec-02	ietf-unified-spec-02
IPv6	RFC5798	rfc5798（デフォルト動作）
	draft-ietf-vrrp-ipv6-spec-02	ietf-ipv6-spec-02
	draft-ietf-vrrp-ipv6-spec-07	ietf-ipv6-spec-07
	draft-ietf-vrrp-unified-spec-02	ietf-unified-spec-02

ADVERTISEMENT パケットのフォーマットやフィールドの意味は規格ごとに異なります。そのため，仮想ルータを構成する装置間で異なる設定にすると，ADVERTISEMENT パケットを不正パケットと判断し

て破棄してしまい，お互いがマスタ状態になることがあります。したがって，仮想ルータを構成する装置間では同じ規格に従うようにコンフィグレーションを設定してください。

(1) RFC3768 に従った動作の概要

IPv4 仮想ルータでサポートしています。

VRRP パケット Ver.2（RFC3768 で規定されているパケットフォーマット）を使用して ADVERTISEMENT を行い，ADVERTISEMENT パケットの認証機能が利用できます。

本装置に設定された ADVERTISEMENT パケットの送信間隔を基に，障害検出時間を決定します。

(2) RFC5798 に従った動作の概要（デフォルト動作）

IPv4/IPv6 仮想ルータでサポートしていて，IPv4/IPv6 仮想ルータでのデフォルト動作です。

VRRP パケット Ver.3（RFC5798 で規定されているパケットフォーマット）を使用して ADVERTISEMENT を行います。

マスタ装置からの ADVERTISEMENT パケットの受信によって得られるマスタ装置の ADVERTISEMENT パケットの送信間隔を基に，障害検出時間を決定します。

ADVERTISEMENT パケットの認証機能は利用できません。

(3) draft-ietf-vrrp-ipv6-spec-02 に従った動作の概要

IPv6 仮想ルータでサポートしています。

VRRP パケット Ver.3（draft-ietf-vrrp-ipv6-spec-02 で規定されているパケットフォーマット）を使用して ADVERTISEMENT を行い，ADVERTISEMENT パケットの認証機能が利用できます。

本装置に設定された ADVERTISEMENT パケットの送信間隔を基に，障害検出時間を決定します。

(4) draft-ietf-vrrp-ipv6-spec-07 に従った動作の概要

IPv6 仮想ルータでサポートしています。

VRRP パケット Ver.3（draft-ietf-vrrp-ipv6-spec-07 で規定されているパケットフォーマット）を使用して ADVERTISEMENT を行います。

本装置に設定された ADVERTISEMENT パケットの送信間隔を基に，障害検出時間を決定します。

ADVERTISEMENT パケットの認証機能は利用できません。

(5) draft-ietf-vrrp-unified-spec-02 に従った動作の概要

IPv4/IPv6 仮想ルータでサポートしています。

VRRP パケット Ver.3（draft-ietf-vrrp-unified-spec-02 で規定されているパケットフォーマット）を使用して ADVERTISEMENT を行います。

マスタ装置からの ADVERTISEMENT パケットの受信によって得られるマスタ装置の ADVERTISEMENT パケットの送信間隔を基に，障害検出時間を決定します。

ADVERTISEMENT パケットの認証機能は利用できません。

(6) 障害検出時間について

本装置では，仮想ルータが次に示す規格に従って動作している場合，ADVERTISEMENT パケットの送信間隔をミリ秒単位で指定すると，すばやく障害を検出して，仮想ルータを切り替えられます。

- RFC5798
- draft-ietf-vrrp-ipv6-spec-07
- draft-ietf-vrrp-unified-spec-02

すばやく VRRP を切り替えるためには，障害検出時間を短くする必要があります。障害検出時間は，ADVERTISEMENT パケットの送信間隔を基に，次の式で算出されます。

障害検出時間＝ ADVERTISEMENT パケット送信間隔×3 ＋ Skew_Time

なお，Skew_Time の算出方法は VRRP の規格ごとに異なります。VRRP の規格と Skew_Time の算出方法を次の表に示します。

表 12–3 VRRP の規格と Skew_Time 算出方法

VRRP の規格	ADVERTISEMENT パケット送信間隔の指定単位	Skew_Time
RFC3768	秒	(256 - Priority※1) / 256 (単位：秒)
RFC5798	1/100 秒	((256 - priority※1) * Master_Adver_Interval※2) /256 (単位：Master_Adver_Interval※2 と同じ)
draft-ietf-vrrp-ipv6-spec-02	秒	(256 - Priority※1) / 256 (単位：秒)
draft-ietf-vrrp-ipv6-spec-07	1/100 秒	((256 - priority※1) * Advertisement_Interval※3) / 256 (単位：Advertisement_Interval※3 と同じ)
draft-ietf-vrrp-unified-spec-02	1/100 秒	((256 - priority※1) * Master_Adver_Interval※2) /256 (単位：Master_Adver_Interval※2 と同じ)

注※1 仮想ルータの優先度

注※2 マスタ装置の ADVERTISEMENT パケット送信間隔

注※3 自装置に設定された ADVERTISEMENT パケット送信間隔

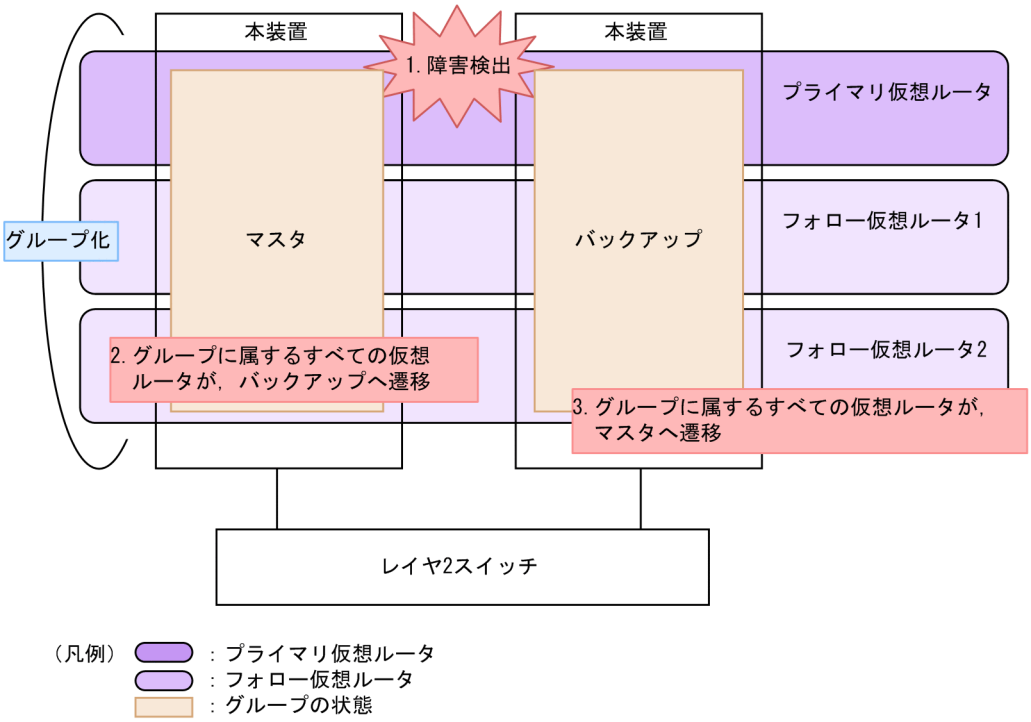
本装置では，仮想ルータが RFC5798，draft-ietf-vrrp-ipv6-spec-07，または draft-ietf-vrrp-unified-spec-02 で動作している場合，ADVERTISEMENT パケットの送信間隔に 250 ミリ秒以下を指定すると，障害検出時間を 1 秒以内に設定できます。

12.1.7　グループ切替機能

(1)　概要

本装置では独自の付加機能として，仮想ルータをグループ化できます。そのグループ単位で，マスタとバックアップの切り替えができます。グループは，プライマリ仮想ルータとフォロー仮想ルータから構成されます。グループ化すると，最大 16380 の仮想ルータを使用できます。仮想ルータのグループ化を次に示します。

図 12-6　仮想ルータのグループ化



1. マスタ装置とバックアップ装置のそれぞれの監視機能によって，障害を検出
2. マスタ装置では，障害を検出したグループの全仮想ルータがバックアップへ遷移
3. バックアップ装置では，障害を検出したグループの全仮想ルータがマスタへ遷移

仮想ルータの役割	仮想ルータが設定されたインタフェース	仮想ルータ ID	仮想ルータ名称	フォローするプライマリ仮想ルータ名称
プライマリ仮想ルータ	gigabitethernet 2/3	70	VRRPNAME	－
フォロー仮想ルータ 1	gigabitethernet 2/4	70	－	VRRPNAME
フォロー仮想ルータ 2	gigabitethernet 2/5	70	－	VRRPNAME

（凡例）－：該当なし

(2)　プライマリ仮想ルータ

ADVERTISEMENT パケットの送受信やトラッキング連携が動作し，マスタとバックアップを切り替える仮想ルータを，**プライマリ仮想ルータ**と呼びます。プライマリ仮想ルータの状態が，グループに属するすべての仮想ルータの状態を決定します。

(3) フォロー仮想ルータ

プライマリ仮想ルータの状態に従って自身の状態を決定する仮想ルータを，**フォロー仮想ルータ**と呼びます。フォロー仮想ルータは，ADVERTISEMENT パケットの送受信やトラッキング連携による状態遷移はしないで，プライマリ仮想ルータの状態に従います。プライマリ仮想ルータが動作していない場合は，イニシャル状態となります。また，自分自身を含むフォロー仮想ルータの状態に従うことはできません。フォロー仮想ルータはプライマリ仮想ルータの状態に従うため，アドレス所有者にはなれません。

フォロー仮想ルータのプライマリ仮想ルータと異なる機能について次の表に示します。

表 12-4 フォロー仮想ルータの機能

プライマリ仮想ルータと異なる機能	動作
マスタとバックアップの切り替え	ADVERTISEMENT パケットの送受信，トラッキング連携による状態遷移はしないで，プライマリ仮想ルータの状態に従います。
コンフィグレーション設定	マスタの選出方法のために利用する，次のコンフィグレーションコマンドは無効です。 • vrrp authentication • vrrp preempt • vrrp preempt delay • vrrp timers non-preempt-swap • vrrp priority
運用ログ	状態遷移に伴う運用ログは出力しません。 グループを構成するプライマリ仮想ルータが設定されていない場合，フォロー仮想ルータが無効である旨のログを出力して注意を促します。また，プライマリ仮想ルータが設定された場合に回復メッセージを出力します。
MIB 情報の取得	未サポートです。プライマリ仮想ルータだけ取得できます。
SNMP 通知の送信	未サポートです。プライマリ仮想ルータだけ送信します。

(4) MAC Learning フレーム

マスタ状態の仮想ルータは，下流の LAN スイッチに仮想 MAC アドレスを学習させる必要があります。

- プライマリ仮想ルータ

  プライマリ仮想ルータは ADVERTISEMENT パケットを送信します。下流の LAN スイッチは，それを受信することで仮想 MAC アドレスを学習します。

- フォロー仮想ルータ

  フォロー仮想ルータは ADVERTISEMENT パケットを送信しません。その代わりに，定期的に送信元 MAC アドレスを仮想 MAC アドレスとした MAC Learning フレームを送信します。下流の LAN スイッチは，この MAC Learning フレームを受信することで，仮想 MAC アドレスを学習します。

(5) 注意事項

1. 仮想ルータを構成する装置間では，仮想ルータのコンフィグレーションは同一にしてください。例えば，ある仮想ルータが，一方の装置でプライマリ仮想ルータ，他方の装置でフォロー仮想ルータとした場合，正しく動作しません。

2. MAC Learning フレームは，1 フォロー仮想ルータ当たり 2 分周期で送信されます。下流の LAN スイッチでは，MAC アドレステーブルのエージング時間を 2 分以下に設定した場合，エージングと MAC アドレス学習を繰り返します。エージング時間は 4 分以上に設定することを推奨します。

12.1.8 VRRP 使用時の注意事項

(1) ADVERTISEMENT パケット送信間隔について

次に示す状態の場合，本装置が送受信する VRRP ADVERTISEMENT パケットの破棄または処理遅延が発生して，状態遷移が発生するおそれがあります。状態遷移が頻発する場合は，VRRP ADVERTISEMENT パケットの送信間隔を大きい値に設定して運用してください。

- 本装置の CPU が過負荷状態の場合
- 本装置に設定した仮想ルータ数が多い場合
- ネットワークが過負荷状態の場合
- 仮想ルータを 3 台以上で構成している場合

(2) IPv6 VRRP と RA の連携について

IPv6 VRRP を設定したインタフェースで RA（Router Advertisement）が有効になっている場合，RA は VRRP と連携して次のように動作します。

- RA は IPv6 VRRP のマスタルータとなっている場合だけ情報を配布します。
- RA パケットの MAC ヘッダの送信元 MAC アドレスは，仮想ルータに設定した仮想 MAC アドレスになります。
- RA パケットの IPv6 ヘッダの送信元 IPv6 アドレスは，仮想ルータに設定した仮想 IPv6 アドレスになります。

これによって，端末は IPv6 自動構成機能で，仮想ルータをデフォルトルータとすることができます。

ただし，次のような場合，端末の動作によっては RA を使用したネットワーク運用に支障がでることがあるので注意してください。

- 一つのインタフェースに複数の仮想ルータを設定した場合，最小の VRID を使用しているマスタルータとだけ連携します。したがって，負荷分散のために VRRP を使用する場合，各端末でデフォルトルータを手動で設定してください。
- 次に示す規格を指定した仮想 IPv6 アドレスにグローバルアドレスを設定した場合，RA の送信元 IPv6 アドレスにはリンクローカルアドレスが必要なため，RA の送信元 IPv6 アドレスにはインタフェースに固有のリンクローカルアドレスを使用します。
  - draft-ietf-vrrp-ipv6-spec-02
  - draft-ietf-vrrp-ipv6-spec-07
  - draft-ietf-vrrp-unified-spec-02

  このため，VRRP と RA は連携できません。VRRP と RA を連携させる運用をする場合は，仮想 IPv6 アドレスにグローバルアドレスを設定しないでください。

(3) VRRP 状態遷移時間について

仮想ルータの状態遷移には，本装置内で同時に遷移する仮想ルータ数に応じて，次に示す状態遷移時間が必要です。

仮想ルータのアクセプトモードが無効な場合の目安値

　仮想ルータ数が 256 未満では 1 秒以下，512 以上では 2 秒以上

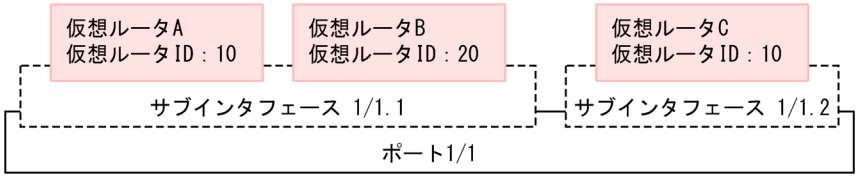
仮想ルータのアクセプトモードが有効な場合の目安値

　仮想ルータ数が 64 未満では 1 秒以下，256 以上では 2 秒以上

(4)　複数の仮想ルータの設定について

一つの IP インタフェースに複数の仮想ルータを設定して，その IP インタフェースが使用しているポートにほかの IP インタフェースを設定する場合，IP インタフェース間で重複する仮想ルータ ID を設定しないでください。重複する仮想ルータ ID を設定する場合は，グループ切替機能を使用して，一つの IP インタフェース上の仮想ルータの状態が一致するようにしてください。該当する構成例を次の図に示します。

図 12-7　VRRP の注意構成



この場合，仮想ルータ A および仮想ルータ B の仮想ルータ ID と，仮想ルータ C の仮想ルータ ID が重複しないように，仮想ルータ ID を変更してください。または，サブインタフェース 1/1.1 の仮想ルータ A と仮想ルータ B でグループ切替機能を使用して，サブインタフェース 1/1.1 上で仮想ルータの状態が一致するようにしてください。

12.2　コンフィグレーション

VRRP を設定するインタフェースには，IP アドレスが設定されている必要があります。インタフェースに IP アドレスが設定されていない場合，VRRP のコンフィグレーションコマンドを入力しても仮想ルータは動作しません。

仮想ルータを実際に運用する場合には，同様の仮想ルータの設定を本装置だけでなく，仮想ルータを構成するほかの装置にも行う必要があります。また，仮想ルータの設定のほかにルーティングの設定も必要です。

12.2.1　コンフィグレーションコマンド一覧

VRRP のコンフィグレーションコマンド一覧を次の表に示します。

表 12-5　コンフィグレーションコマンド一覧

コマンド名	説明
vrrp accept	アクセプトモードを設定します。
vrrp authentication	ADVERTISEMENT パケット認証のパスワードを設定します。
vrrp follow	プライマリ仮想ルータを指定し，仮想ルータをフォロー仮想ルータに設定します。
vrrp ip vrrp ipv6	仮想ルータへ IP アドレスを設定します。
vrrp mode	VRRP が準拠する動作を設定します。
vrrp name	仮想ルータ名称を設定します。
vrrp preempt	自動切り戻しを設定します。
vrrp preempt delay	自動切り戻し抑止時間を設定します。
vrrp priority	仮想ルータの優先度を設定します。
vrrp timers advertise	仮想ルータの ADVERTISEMENT パケット送信間隔を設定します。
vrrp timers non-preempt-swap	自動切り戻し抑止中に切り戻し処理を行う場合の切り戻し抑止時間を設定します。

12.2.2　VRRP のコンフィグレーションの流れ

(1)　あらかじめ，IP インタフェースを設定します。

インタフェースに対して，仮想ルータに設定しようとしている IP アドレスと同じアドレスファミリの IP アドレスを設定します。

インタフェースに初めて IPv6 アドレスを設定する場合は，続けて ipv6 enable コマンドを実行して IPv6 アドレスを有効にする必要があります。

(2)　仮想ルータへ IP アドレスを設定します。

IP インタフェースに設定した IP アドレスと同一の IP アドレスを仮想ルータへ設定すると，仮想ルータはアドレス所有者となり，優先度が 255 固定となります。

仮想ルータの IPv6 アドレスにグローバルアドレスを使用した場合の，仮想ルータのリンクローカルアドレスを次の表に示します。なお，IP インタフェースに設定したグローバルアドレスと同一のグローバルアドレスを仮想ルータに設定したときだけ，アドレス所有者となります。

表 12-6　グローバルアドレスを使用した場合の仮想ルータのリンクローカルアドレス

VRRP の規格	仮想ルータのリンクローカルアドレス
RFC5798	fe80::200:5eff:fe00:02{仮想ルータ ID}
draft-ietf-vrrp-ipv6-spec-02	設定されない
draft-ietf-vrrp-ipv6-spec-07	仮想ルータを設定したインタフェースのリンクローカルアドレス
draft-ietf-vrrp-unified-spec-02	

(3)　仮想ルータの優先度を設定します。

IP アドレス所有者ではない同一仮想ルータ ID の仮想ルータの優先度を，それぞれ異なる値に設定します。

(4)　ADVERTISEMENT パケット送信間隔を設定します。

バックアップの仮想ルータが ADVERTISEMENT パケットを頻繁に取りこぼす場合は，
ADVERTISEMENT パケットの送信間隔をマスタとバックアップの仮想ルータに設定します。

12.2.3　仮想ルータへの IPv4 アドレス設定

[設定のポイント]

仮想ルータへ仮想 IPv4 アドレスを設定します。仮想ルータへ仮想 IPv4 アドレスを設定すると，仮想ルータは動作を開始します。仮想ルータへ設定できる IPv4 アドレスは一つだけです。

仮想ルータに設定する IPv4 アドレスと仮想ルータを設定するインタフェースの IPv4 アドレスが同じ場合，仮想ルータは IP アドレス所有者となり，優先度が 255（固定）となります。

仮想 IPv4 アドレスを設定する仮想ルータ ID は，同一 IP サブネットワーク内でユニークとなるように設定してください。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 2/3**
   (config-if)# ip address 192.168.10.10 255.255.255.0
   ギガビット・イーサネットインタフェース 2/3 に仮想ルータを設定するため，まず gigabitethernet 2/3 のコンフィグレーションモードに移行します。イーサネットインタフェースへ IPv4 アドレスを設定していない場合は，ここで IPv4 アドレスを設定します。
2. **(config-if)# vrrp 1 ip 192.168.10.1**
   仮想ルータ ID 1 の仮想ルータへ仮想 IPv4 アドレス 192.168.10.1 を設定します。

[注意事項]

- 仮想ルータへ IP アドレスを設定すると，仮想ルータは動作を始めます。ほかの仮想ルータの優先度設定によっては，仮想ルータがマスタとして追加される場合もあります。
- 装置に仮想ルータを 64 個以上設定する場合は，「12.2.6　ADVERTISEMENT パケット送信間隔の設定」を参照して ADVERTISEMENT パケットの送信間隔を調整してください。

12.2.4 仮想ルータへの IPv6 アドレス設定

[設定のポイント]

仮想ルータへ仮想 IPv6 アドレスを設定します。仮想ルータへ仮想 IPv6 アドレスを設定すると，仮想ルータは動作を開始します。仮想ルータへ設定できる IPv6 アドレスは一つだけです。

仮想ルータに設定する IPv6 アドレスと仮想ルータを設定するインタフェースの IPv6 アドレスが同じ場合，仮想ルータは IP アドレス所有者となり，優先度が 255（固定）となります。

仮想 IPv6 アドレスを設定する仮想ルータ ID は，同一 IP サブネットワーク内でユニークとなるように設定してください。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 2/4**
   (config-if)# ipv6 address 2001:db8::1/32
   (config-if)# ipv6 enable
   ギガビット・イーサネットインタフェース 2/4 に仮想ルータを設定するため，まず gigabitethernet 2/4 のコンフィグレーションモードに移行します。イーサネットインタフェースへ IPv6 アドレスを設定していない場合は，ここで IPv6 アドレスを設定します。
2. **(config-if)# vrrp 3 ipv6 2001:db8::100**
   仮想ルータ ID 3 の仮想ルータへ仮想 IPv6 アドレス 2001:db8::100 を設定します。

[注意事項]

- 「12.2.3 仮想ルータへの IPv4 アドレス設定」の注意事項と同じです。

12.2.5 優先度の設定

仮想ルータの優先度を 1 から 254 の間で設定します。優先度のデフォルト値は，IP アドレス所有者でない場合は 100 です。仮想ルータが IP アドレス所有者の場合は優先度が 255（固定）となって変更できません。

仮想ルータを構成する装置のうちで最も優先度の大きい装置がマスタになります。また，マスタの仮想ルータがダウンした場合，バックアップの仮想ルータのうちで最も優先度の高い仮想ルータがマスタになります。

[設定のポイント]

マスタになる装置を明確にするために，同じ仮想ルータ ID の仮想ルータには異なる優先度を設定してください。

[コマンドによる設定]

1. **(config-if)# vrrp 1 priority 150**
   仮想ルータ ID 1 の仮想ルータの優先度を 150 に設定します。

12.2.6 ADVERTISEMENT パケット送信間隔の設定

(1) ADVERTISEMENT パケット送信間隔設定

ネットワークの負荷が高く，ADVERTISEMENT パケットの損失が多いために，仮想ルータのマスタとバックアップがたびたび切り替わる場合は，ADVERTISEMENT パケットの送信間隔を長くすると現象を軽減できることがあります。ただし，バックアップの仮想ルータは，ADVERTISEMENT パケットを 3 回

続けて受信できないときにマスタに変わるため，ADVERTISEMENT パケットの送信間隔を長くすると，マスタの仮想ルータで障害が発生した場合に，バックアップの仮想ルータがマスタに変わるまでの時間も長くなります。

[設定のポイント]

ADVERTISEMENT パケット送信間隔は，マスタおよびバックアップの仮想ルータへ同じ値を設定してください。

[コマンドによる設定]

1. **(config-if)# vrrp 1 timers advertise 3**

   仮想ルータ ID 1 の仮想ルータの ADVERTISEMENT パケット送信間隔を 3（秒）に設定します。

(2) 仮想ルータの高速切替設定

本装置では，仮想ルータが次に示す規格に従って動作している場合，ADVERTISEMENT パケットの送信間隔をミリ秒単位で指定すると，すばやく障害を検出して，仮想ルータを切り替えられます。

- RFC5798
- draft-ietf-vrrp-ipv6-spec-07
- draft-ietf-vrrp-unified-spec-02

装置に多くの仮想ルータを設定した場合，マスタとバックアップが切り替わることがあります。その場合は，次の表を基に ADVERTISEMENT パケット送信間隔を調整してください。

表 12-7 高速切替機能使用時の ADVERTISEMENT パケット送信間隔の設定目安値

装置当たりの仮想ルータ数※	ADVERTISEMENT パケット送信間隔
1～64	0.20 秒以上
65～128	0.40 秒以上
129～192	0.60 秒以上
193～255	0.80 秒以上

注※ グループ切替機能使用時は，プライマリ仮想ルータ数

[設定のポイント]

VRRP の仮想ルータを高速切替するためには，対応した VRRP 動作モードを設定して，ADVERTISEMENT パケット送信間隔をミリ秒単位で指定する必要があります。
ADVERTISEMENT パケット送信間隔は，マスタおよびバックアップの仮想ルータへ同じ値を設定してください。

[コマンドによる設定]

1. **(config-if)# vrrp 1 mode ietf-unified-spec-02**

   仮想ルータが，draft-ietf-vrrp-unified-spec-02 に従った動作になるように設定します。

2. **(config-if)# vrrp 1 timers advertise msec 200**

   仮想ルータの ADVERTISEMENT パケット送信間隔を 200 ミリ秒に設定します。

12.2.7 自動切り戻し抑止の設定

自動切り戻しはデフォルトで動作します。マスタの仮想ルータに障害が発生してバックアップに切り替わったあと，障害が復旧すると，はじめにマスタであった優先度の高いバックアップの仮想ルータが自動でマスタに切り替わります。自動切り戻しを抑止すると，優先度の高いバックアップの仮想ルータが自動でマスタに切り替わらなくなります。

[設定のポイント]

自動切り戻し抑止を設定する場合は，IP アドレス所有者でないマスタの仮想ルータに対して設定してください。

[コマンドによる設定]

1. **(config-if)# no vrrp 1 preempt**
   仮想ルータ ID 1 の仮想ルータの自動切り戻しを抑止します。

12.2.8 自動切り戻し抑止時間の設定

マスタの仮想ルータに障害が発生してバックアップに切り替わったあと，障害が復旧した場合，優先度の高いバックアップの仮想ルータが自動的にマスタに切り替え処理を開始するまでの時間を設定します。自動切り戻し抑止時間のデフォルト値は 0（秒）で，自動切り戻しを抑止しません。

[設定のポイント]

自動切り戻し抑止時間を設定する場合は，IP アドレス所有者でないマスタの仮想ルータに対して設定してください。

[コマンドによる設定]

1. **(config-if)# vrrp 1 preempt delay 60**
   仮想ルータ ID 1 の仮想ルータの自動切り戻し抑止時間を 60 秒に設定します。

12.2.9 VRRP 動作モードの設定

本装置では複数の VRRP の規格をサポートしているため，既存システムに採用されている規格に合わせて柔軟に導入できます。

コンフィグレーションの設定時は，仮想ルータを構成する装置間で相互運用できる VRRP 動作モードにしてください。なお，仮想ルータに設定された IP バージョンと VRRP 動作モードの IP バージョンが異なる場合，設定できません。

(1) RFC3768 に従った動作の設定

[設定のポイント]

仮想ルータを構成する装置がすべて RFC3768 に従って動作するように，コンフィグレーションを設定してください。

[コマンドによる設定]

1. **(config-if)# vrrp 1 mode rfc3768**
   IPv4 仮想ルータが RFC3768 に従った動作になるように設定します。

(2) draft-ietf-vrrp-ipv6-spec-02 に従った動作の設定

[設定のポイント]

仮想ルータを構成する装置がすべて draft-ietf-vrrp-ipv6-spec-02 に従って動作するように，コンフィグレーションを設定してください。

[コマンドによる設定]

1. **(config-if)# vrrp 1 mode ietf-ipv6-spec-02**

   IPv6 仮想ルータが draft-ietf-vrrp-ipv6-spec-02 に従った動作になるように設定します。

(3) draft-ietf-vrrp-ipv6-spec-07 に従った動作の設定

[設定のポイント]

仮想ルータを構成する装置がすべて draft-ietf-vrrp-ipv6-spec-07 に従って動作するように，コンフィグレーションを設定してください。

[コマンドによる設定]

1. **(config-if)# vrrp 1 mode ietf-ipv6-spec-07**

   IPv6 仮想ルータが draft-ietf-vrrp-ipv6-spec-07 に従った動作になるように設定します。

(4) draft-ietf-vrrp-unified-spec-02 に従った動作の設定

[設定のポイント]

仮想ルータを構成する装置がすべて draft-ietf-vrrp-unified-spec-02 に従って動作するように，コンフィグレーションを設定してください。

[コマンドによる設定]

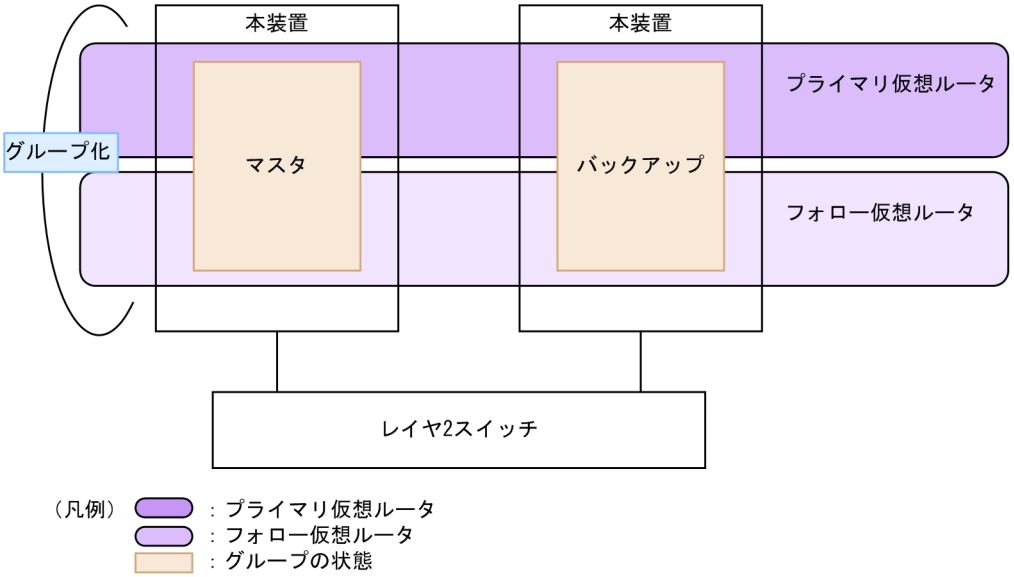
1. **(config-if)# vrrp 1 mode ietf-unified-spec-02**

   IPv4/IPv6 仮想ルータが draft-ietf-vrrp-unified-spec-02 に従った動作になるように設定します。

12.2.10 仮想ルータのグループ化

複数の仮想ルータをグループ化することで，最大 16380 の仮想ルータを使用できます。ここでは，次に示すグループ構成を設定する例を示します。

図 12-8　仮想ルータのグループ構成設定例



仮想ルータの役割	仮想ルータが設定されたインタフェース	仮想ルータID	仮想ルータ名称	フォローするプライマリ仮想ルータ名称
プライマリ仮想ルータ	gigabitethernet 2/3	1	VRRPNAME	－
フォロー仮想ルータ	gigabitethernet 2/4	1	－	VRRPNAME

（凡例）－：該当なし

(1)　プライマリ仮想ルータの設定

[設定のポイント]

プライマリ仮想ルータの状態は，グループに属するすべての仮想ルータの状態を決定します。設定後，プライマリ仮想ルータが正しく動作していることを確認してください。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 2/3**
   (config-if)# ip address 192.168.10.1 255.255.255.0
   gigabitethernet 2/3 のコンフィグレーションモードに移行します。イーサネットインタフェースへ IP アドレスを設定していない場合は，ここで IP アドレスを設定します。
2. **(config-if)# vrrp 1 ip 192.168.10.100**
   gigabitethernet 2/3，仮想ルータ ID 1 の仮想ルータに仮想 IP アドレス 192.168.10.100 を設定します。
3. **(config-if)# vrrp 1 name VRRPNAME**
   gigabitethernet 2/3，仮想ルータ ID 1 の仮想ルータに仮想ルータ名称 VRRPNAME を設定します。

(2)　フォロー仮想ルータの設定

[設定のポイント]

仮想ルータからプライマリ仮想ルータ名称を指定します。プライマリ仮想ルータを指定した仮想ルータはフォロー仮想ルータとなり，指定したプライマリ仮想ルータの状態に従います。

フォロー仮想ルータには，プライマリ仮想ルータと同じ仮想ルータ ID を設定することを推奨します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 2/4**
   (config-if)# ip address 192.168.20.1 255.255.255.0
   gigabitethernet 2/4 のコンフィグレーションモードに移行します。イーサネットインタフェースへ IP アドレスを設定していない場合は，ここで IP アドレスを設定します。
2. **(config-if)# vrrp 1 follow VRRPNAME**
   gigabitethernet 2/4，仮想ルータ ID 1 のフォロー仮想ルータが従うプライマリ仮想ルータ名称に VRRPNAME を指定します。
3. **(config-if)# vrrp 1 ip 192.168.20.100**
   gigabitethernet 2/4，仮想ルータ ID 1 の仮想ルータに仮想 IP アドレス 192.168.20.100 を設定します。

[注意事項]

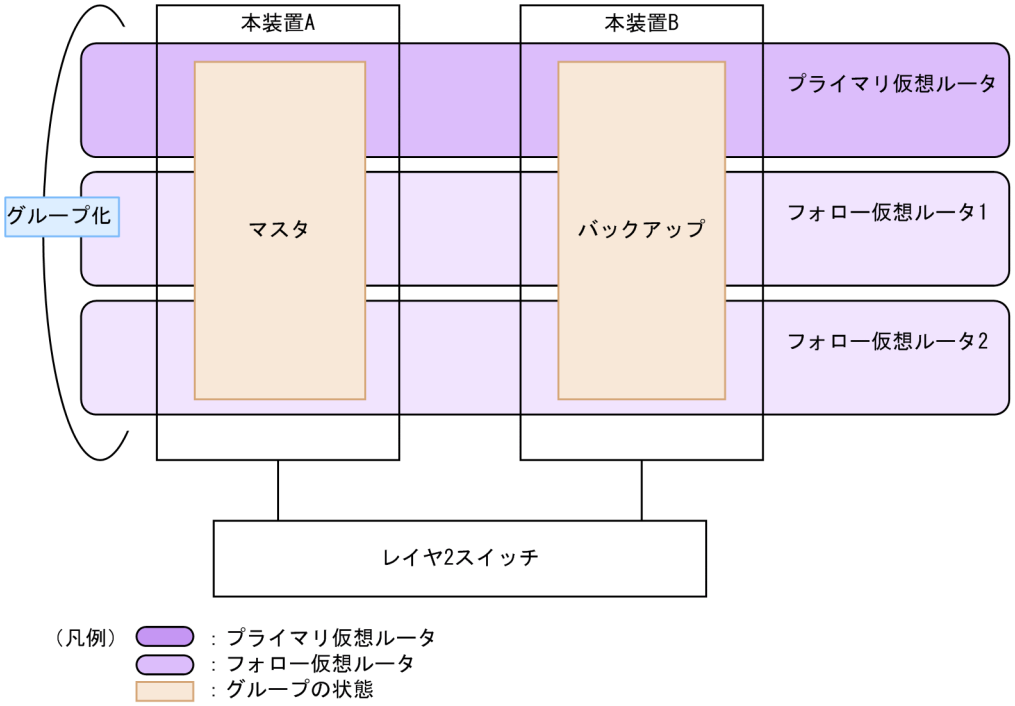
- プライマリ仮想ルータが 255 個設定されている状態でフォロー仮想ルータを追加する場合は，vrrp follow コマンドから設定を開始してください。
- 指定したプライマリ仮想ルータが存在しない場合，フォロー仮想ルータはイニシャル状態となります。
- フォロー仮想ルータは，アドレス所有者になれません。
- ほかの仮想ルータからプライマリ仮想ルータに指定されている場合，フォロー仮想ルータになれません。また，自分自身の仮想ルータ名称，およびほかのフォロー仮想ルータ名称を指定できません。

12.2.11 グループ構成の変更

プライマリ仮想ルータを別の仮想ルータへ変更する場合の手順を次に示します。この手順に従わない場合，両装置の仮想ルータがマスタ状態になるおそれがあります。

変更前と変更後の仮想ルータのグループ構成を次に示します。なお，本装置 A がマスタ装置，本装置 B がバックアップ装置とします。

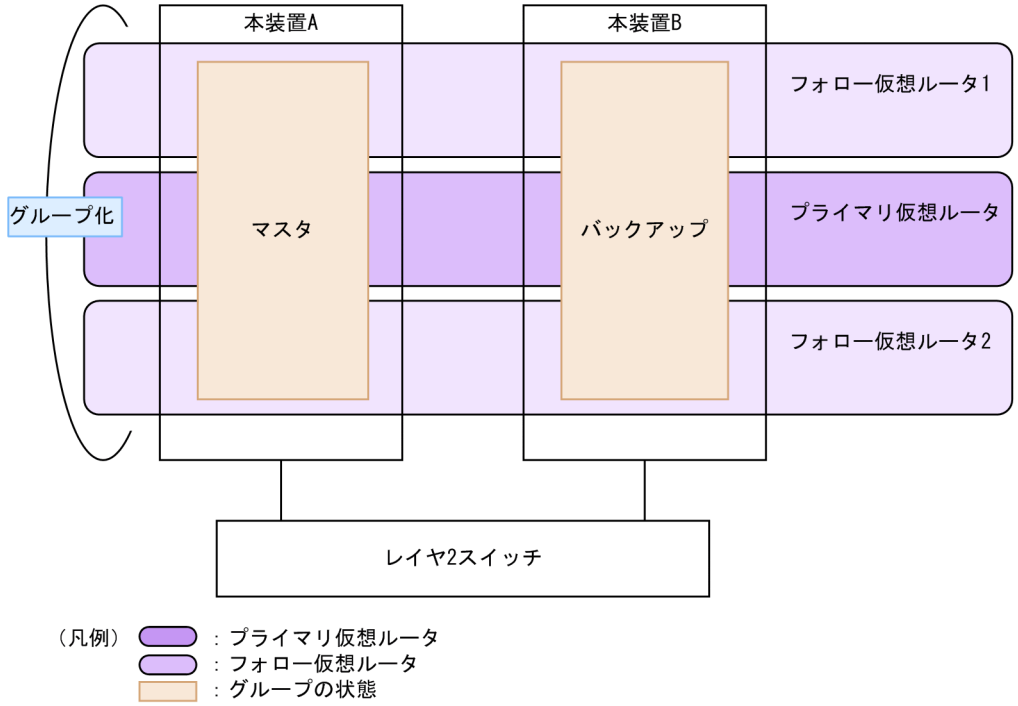
図 12-9　仮想ルータのグループ構成設定例（変更前）



仮想ルータの役割	仮想ルータが設定されたインタフェース	仮想ルータID	仮想ルータ名称	フォローするプライマリ仮想ルータ名称
プライマリ仮想ルータ	gigabitethernet 1/4	1	VRRPNAME	－
フォロー仮想ルータ 1	gigabitethernet 2/4	1	－	VRRPNAME
フォロー仮想ルータ 2	gigabitethernet 3/4	1	－	VRRPNAME

（凡例）－：該当なし

図 12-10　仮想ルータのグループ構成設定例（変更後）



仮想ルータの役割	仮想ルータが設定されたインタフェース	仮想ルータID	仮想ルータ名称	フォローするプライマリ仮想ルータ名称
フォロー仮想ルータ 1	gigabitethernet 1/4	1	VRRPNAME	NEW_VRRPNAME
プライマリ仮想ルータ	gigabitethernet 2/4	1	NEW_VRRPNAME	－
フォロー仮想ルータ 2	gigabitethernet 3/4	1	－	NEW_VRRPNAME

（凡例）－：該当なし

(1)　フォロー仮想ルータからプライマリ仮想ルータへ変更

[設定のポイント]

フォロー仮想ルータをプライマリ仮想ルータに変更します。マスタ装置（本装置 A）から設定を変更する必要があります。

バックアップ装置（本装置 B）から変更した場合，バックアップ装置（本装置 B）の仮想ルータは ADVERTISEMENT パケットを受信しないため，マスタ状態へ遷移します。また，マスタ装置（本装置 A）はマスタ状態であるプライマリ仮想ルータに従ってマスタ状態のままとなるため，両装置の仮想ルータがマスタ状態になります。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 2/4**

   gigabitethernet 2/4 のコンフィグレーションモードに移行します。

2. **(config-if)# no vrrp 1 follow**

   gigabitethernet 2/4，仮想ルータ ID 1 のフォロー仮想ルータをプライマリ仮想ルータとして動作させます。

   本装置 A，本装置 B の順に変更します。

3. **(config-if)# vrrp 1 name NEW_VRRPNAME**

   gigabitethernet 2/4，仮想ルータ ID 1 のプライマリ仮想ルータに仮想ルータ名称 NEW_VRRPNAME を設定します。

(2) フォロー仮想ルータの設定変更

[設定のポイント]

フォロー仮想ルータの従っているプライマリ仮想ルータを変更します。

フォロー仮想ルータは ADVERTISEMENT パケットを送受信しないでプライマリ仮想ルータの状態に従うため，どちらの装置からでも設定を変更できます。動作していないプライマリ仮想ルータを指定した場合，フォロー仮想ルータはイニシャル状態となります。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 3/4**

   gigabitethernet 3/4 のコンフィグレーションモードに移行します。

2. **(config-if)# vrrp 1 follow NEW_VRRPNAME**

   gigabitethernet 3/4，仮想ルータ ID 1 のフォロー仮想ルータが従うプライマリ仮想ルータを NEW_VRRPNAME に変更します。

(3) プライマリ仮想ルータからフォロー仮想ルータへ変更

[設定のポイント]

プライマリ仮想ルータをフォロー仮想ルータに変更します。バックアップ装置側から設定を変更する必要があります。

マスタ装置（本装置 A）から変更した場合，バックアップ装置（本装置 B）の仮想ルータは ADVERTISEMENT パケットを受信しないため，マスタ状態へ遷移します。また，マスタ装置（本装置 A）はマスタ状態であるプライマリ仮想ルータに従ってマスタ状態のままとなるため，両装置の仮想ルータがマスタ状態になります。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/4**

   gigabitethernet 1/4 のコンフィグレーションモードに移行します。

2. **(config-if)# vrrp 1 follow NEW_VRRPNAME**

   gigabitethernet 1/4，仮想ルータ ID 1 の仮想ルータをフォロー仮想ルータとして動作させます。

   本装置 B，本装置 A の順に変更します。

12.3 オペレーション

12.3.1 運用コマンド一覧

VRRP の運用コマンド一覧を次の表に示します。

表 12-8 運用コマンド一覧

コマンド名	説明
show vrrpstatus	仮想ルータの動作状態を表示します。
clear vrrpstatus	仮想ルータの統計情報を初期化します。
swap vrrp	自動切り戻しが抑止されているときに切り戻し処理を開始します。
restart vrrp	VRRP プログラムを再起動します。
dump protocols vrrp	VRRP プログラムで採取している詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。

12.3.2 仮想ルータの設定確認

仮想ルータの設定は，show vrrpstatus コマンドで確認します。

(1) 詳細情報の確認

detail パラメータを指定すると，仮想ルータの設定の詳細情報を確認できます。

図 12-11 show vrrpstatus コマンド（detail パラメータ指定時）の実行結果

```
> show vrrpstatus detail interface gigabitethernet 2/4 vrid 1
Date 20XX/07/15 12:00:00 UTC
gigabitethernet 2/4: VRID 1 VRF 2
   Virtual Router IP Address : 172.16.10.2
   Virtual MAC Address : 0000.5e00.0101
   Virtual Router Name : VRRPNAME1 (primary)
   Virtual Router Follow : -
   Number of Follow virtual routers : 4
   Current State : MASTER
   Admin State : enable
   Priority : 80 /100
   IP Address Count : 1
   Master Router's IP Address : 172.16.10.2
   Primary IP Address : 172.16.10.1
   Authentication Type : SIMPLE TEXT PASSWORD(Disable)
   Authentication Key : ABCDEFG(Disable)
   Advertisement Interval : 250 msec
   Master Advertisement Interval : 1000 msec
   Preempt Mode : ON
   Preempt Delay : 60
   Non Preempt swap timer : 30
   Accept Mode : ON
   Virtual Router Up Time : 20XX/02/04 10:00:00 UTC
   IPv4 Advertisement Type : ietf-unified-spec-02-mode
>
```

(2) グループ情報の確認

group パラメータを指定すると，仮想ルータの設定のグループ情報を確認できます。仮想ルータ名称がわかる場合，name パラメータを指定して仮想ルータ情報を確認できます。

図 12-12　show vrrpstatus コマンド（group パラメータおよび name パラメータ指定時）の実行結果（プライマリ仮想ルータの場合）

```
> show vrrpstatus group name VRRPNAME1
Date 20XX/05/01 12:00:00 UTC
gigabitethernet 2/4: VRID 1 VRF 2
    Virtual Router Name                : VRRPNAME1 (primary)
    Virtual Router Follow              : -
    Number of Follow virtual routers   : 4
    Followed by virtual routers        :
        gigabitethernet 2/1            : VRID 1 VRF 2
        port-channel 10                : VRID 1 VRF 2
        gigabitethernet 2/3            : VRID 1 VRF 2
        gigabitethernet 2/4.4095       : VRID 1 VRF 2
```

図 12-13　show vrrpstatus コマンド（group パラメータ指定時）の実行結果（フォロー仮想ルータの場合）

```
> show vrrpstatus group interface gigabitethernet 2/1 vrid 1
Date 20XX/05/01 12:00:00 UTC
gigabitethernet 2/1: VRID 1 VRF 2
    Virtual Router Name            : VRRPNAME2 (follow)
    Virtual Router Follow          : VRRPNAME1 (gigabitethernet 2/2: VRID 1 VRF 2 )
    Number of Follow virtual routers: 0
    Followed by virtual routers    : -
```

12.3.3　切り戻し処理の実行

マスタより優先度が高いのにバックアップに留まっている，自動切り戻しが抑止されている仮想ルータへ swap vrrp コマンドを実行すると，切り戻し処理を開始できます。ただし，swap vrrp コマンドを実行しても，優先度の低い仮想ルータをマスタにはできません。

13 ユニキャストルーティング

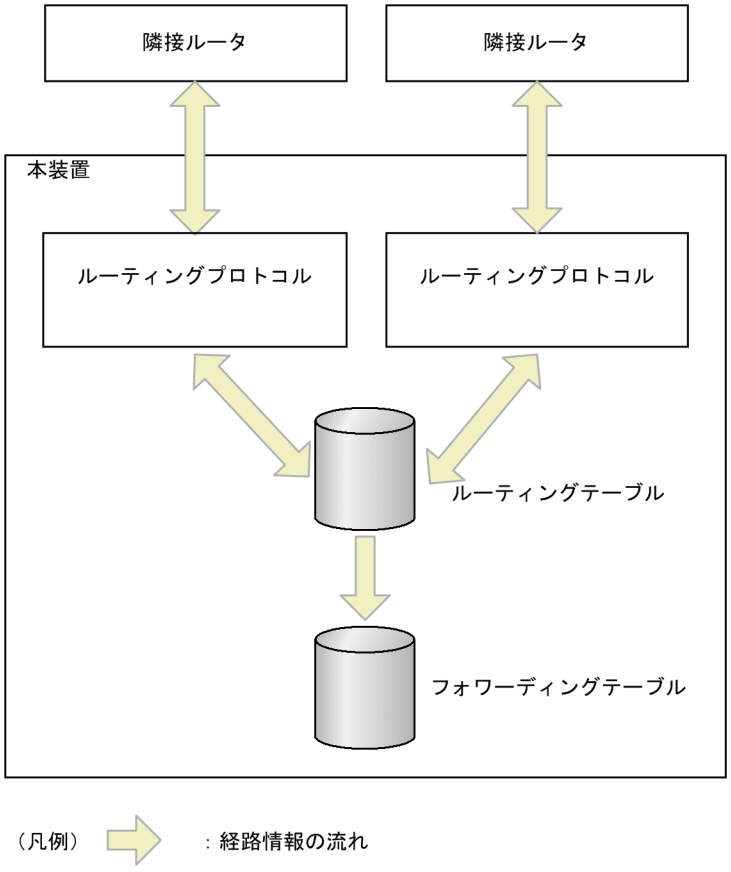
この章では，IPv4 および IPv6 のユニキャストルーティング共通の事項について説明します。

13.1　ユニキャストルーティング共通の解説

13.1.1　ルーティング概要

ルーティングプロトコルは，隣接ルータと経路情報を交換します。各ルーティングプロトコルで学習した経路情報はルーティングテーブルで保持されます。そして，宛先として最適な経路情報をフォワーディングテーブルに登録します。パケットはフォワーディングテーブルに従って中継されます。

図 13-1　ルーティングの概要



13.1.2　スタティックルーティングとダイナミックルーティング

パケットを中継するためにはルーティングテーブルを作成する必要があります。本装置のルーティングテーブルの作成方法は，大きく**スタティックルーティング**と**ダイナミックルーティング**に分類できます。

- スタティックルーティング
  ユーザがコンフィグレーションによって経路情報を設定する方法です。
- ダイナミックルーティング
  ネットワーク内のほかのルータと経路情報を交換して中継経路を決定する方法です。本装置は，次のルーティングプロトコルをサポートしています。
  - IPv4：RIP バージョン 1（以降，RIP-1）およびバージョン 2（以降，RIP-2），OSPF バージョン 2（以降，OSPF），BGP バージョン 4（以降，BGP4）
  - IPv6：RIPng，OSPFv3，BGP4+

13.1.3　経路情報

本装置が取り扱う経路情報（ルーティングの対象とするアドレスの種類）を次に示します。なお，本装置はサイトローカルアドレスをグローバルアドレスと同様に扱います。

表 13-1　経路情報（IPv4）

経路情報の種類		説明
通常の経路	デフォルト経路	すべてのネットワーク宛ての経路（宛先アドレス：0.0.0.0，ネットワークマスク：0.0.0.0）。
	ナチュラルマスク経路	アドレスクラスに対応したネットワークマスクの経路（ネットワークマスク：クラス A ＝ 8 ビット，クラス B ＝ 16 ビット，クラス C ＝ 24 ビット）。
	サブネット経路	特定のサブネット宛ての経路（ネットワークマスクがアドレスクラスに対応したネットワークマスクよりも長い経路）。
	ホスト経路	特定のホスト宛ての経路（ネットワークマスクが 32 ビットの経路）。
	可変長サブネットマスク	可変長サブネットマスク：VLSM（Variable Length Subnet Mask）を取り扱います。同一ネットワークアドレスで，長さの異なる複数のサブネットマスクを取り扱えます。
CIDR 対応の経路	スーパーネット経路	アドレスクラスに対応したネットワークマスクより短いネットワークマスクの経路情報を取り扱えます。例えば，クラス C のネットワークアドレス 192.168.8.0/24，192.168.9.0/24，192.168.10.0/24，192.168.11.0/24 の経路情報を一つのスーパーネット経路 192.168.8.0/22 に集約して取り扱えます。
	0 サブネット経路	サブネット番号が 0 のネットワークアドレスを一つのサブネットワークとして取り扱います。例えば，クラス B のネットワークアドレス 172.16.0.0/24 の経路情報を取り扱えます。
	-1 サブネット経路	サブネット番号が-1（All'1'）のネットワークアドレスを一つのサブネットワークとして取り扱います。例えば，クラス B のネットワークアドレス 172.16.255.0/24 の経路情報を取り扱えます。
	包括的サブネット	複数の経路情報間でネットワークアドレスが包括関係にある経路を別の経路情報として取り扱います。例えば，クラス B のネットワークアドレス 172.16.3.0/24 と 172.16.2.0/23 は個々の経路情報として取り扱えます。
ルーティング対象外の経路	IPv4 this network アドレス	宛先が 0.0.0.0，マスク長が 8 ビット以上のネットワーク。ただし，スタティック経路としてコンフィグレーションに設定した場合，通常のスタティック経路として動作します。
	ループバックアドレス	127.0.0.0/8 に含まれるネットワーク。
	クラス D アドレス	マルチキャストアドレス（224.0.0.0～）。

経路情報の種類		説明
	クラスＥアドレス	将来のために予約されているアドレス（240.0.0.0～）。
	制限ブロードキャストアドレス	255.255.255.255 のアドレス。

表 13-2　経路情報（IPv6）

経路情報の種類		説明
通常の経路	デフォルト経路	すべてのネットワーク宛ての経路(宛先プレフィックス:::/0)。
	プレフィックス長が 1～127 ビットのグローバル経路	特定のネットワーク宛てのグローバル経路および複数のネットワーク宛てのグローバル経路を集約した経路。
	ホスト経路	特定のホスト宛ての経路（プレフィックス長が 128 ビットのグローバル経路)。
ルーティング対象外の経路	リンクローカル経路	隣接装置との通信で使用する経路（プレフィックス：fe80::%インタフェース名/64)。
	マルチキャストアドレス	マルチキャスト通信で使用する経路（宛先プレフィックス：ff00::/8)。
	未指定アドレス	アドレスがないことを表すアドレス（宛先プレフィックス：::/128)。

13.1.4　ルーティングプロトコルごとの適用範囲

本装置がサポートするルーティングプロトコルについて取り扱う経路情報および機能の概要を次に示します。

表 13-3　ルーティングプロトコルごとの適用範囲（IPv4）

経路情報		ルーティング				
		スタティック	ダイナミック			
			RIP-1	RIP-2	OSPF	BGP4
経路情報	デフォルト経路	○	○	○	○	○
	ナチュラルマスク経路	○	○	○	○	○
	サブネット経路	○	○	○	○	○
	ホスト経路	○	○	○	○	○
	可変長サブネットマスク	○	×	○	○	○
	CIDR 対応	○	△	○	○	○
	マルチパス（最大 16 パス）	○	×	×	○	○

経路情報	ルーティング				
	スタティック	ダイナミック			
		RIP-1	RIP-2	OSPF	BGP4
経路選択	－	メトリック（経由するルータ数）		コスト（経由するルータ数および回線速度）	AS パス属性
ルーティングループ抑止	－	スプリットホライズン		○	○
認証機能	－	×	○	○	○

（凡例）

○：取り扱う

△：一部取り扱う（0 サブネット経路，-1 サブネット経路は取り扱う）

×：取り扱わない

－：該当しない

表 13-4　ルーティングプロトコルごとの適用範囲（IPv6）

経路情報		スタティック	ダイナミック		
			RIPng	OSPFv3	BGP4+
経路情報	デフォルト経路	○	○	○	○
	グローバル経路	○	○	○	○
	ホスト経路	○	○	○	○
	マルチパス	○	×	○	○
経路選択		－	メトリック（経由するルータ数）	コスト（経由するルータ数および回線速度）	AS パス属性
ルーティングループ抑止		－	スプリットホライズン	○	○
認証機能		－	×	×	○

（凡例）

○：取り扱う

×：取り扱わない

－：該当しない

13.1.5　ルーティングプロトコルの同時動作

スタティックルーティングおよびダイナミックルーティングの各プロトコルは同時に動作できます。

(1)　学習経路の優先度選択

複数のルーティングプロトコルが同時動作するとき，それぞれは独立した経路選択手順に従って，ある宛先アドレスへの経路情報から一つの最良の経路を選択します。直結経路や集約経路もルーティングプロトコルで学習した経路と同じように一つのプロトコル経路として扱います。その結果，本装置内ではある宛先ア

ドレスへの経路情報が複数存在することになります。このような場合，それぞれの経路情報のディスタンス値が比較されて優先度の高い経路がアクティブ経路になります。

本装置では，スタティック経路ごとおよびダイナミックルーティングのルーティングプロトコル（例えば，RIP）ごとに生成する経路情報のデフォルトのディスタンス（優先度）値をコンフィグレーションで設定できます。なお，ディスタンスは値の小さい方が優先度が高くなります。各プロトコルのディスタンスのデフォルト値を次の表に示します。

表 13-5　ディスタンスのデフォルト値

経路	デフォルトディスタンス値
直結経路	0（固定値）
スタティック経路	2
BGP4 または BGP4+の外部ピア学習経路	20
OSPF または OSPFv3 の AS 内経路	110
OSPF または OSPFv3 の AS 外経路	110
RIP または RIPng 経路	120
集約経路	130
BGP4 または BGP4+の内部ピア学習経路	200
BGP4 または BGP4+メンバー AS 間ピア学習経路	200
他 VRF またはグローバルネットワークからインポートした経路	210
内部生成経路	256

(2)　広告経路

複数のルーティングプロトコルが同時動作するとき，各ルーティングプロトコルで広告する経路情報は同一のルーティングプロトコルで学習した経路情報に限られます。異なるルーティングプロトコルから学習した経路情報は広告されません。

本装置では，あるルーティングプロトコルの経路情報をほかのルーティングプロトコルで広告したい場合や，特定の経路情報の広告をフィルタリングしたい場合には経路フィルタリングによって実現できます。なお，非アクティブ経路の経路情報はほかのルーティングプロトコルで広告できません。

経路フィルタリングについては，「23　経路フィルタリング」を参照してください。

(a)　RIP または RIPng での経路広告

RIP-1 と RIP-2 は同一のルーティングプロトコルです。RIP-1 と RIP-2 はお互いが学習した経路情報を広告します。

RIPng は一つのルーティングプロトコルとして動作します。

(b)　OSPF または OSPFv3 での経路広告

OSPF または OSPFv3 の各ドメインは，互いに異なるルーティングプロトコルとして動作します。そのため，一つの宛先アドレスに異なるドメインに由来する複数の AS 内経路，または AS 外経路が存在することがあります。OSPF または OSPFv3 の経路間でディスタンス値が同じ場合には，ドメイン番号の小さい経

路を優先します。AS 外経路および AS 内経路（エリア内経路，エリア間経路）は，ドメインごとにディスタンスのデフォルト値を変更できます。

経路フィルタリングを使用しない場合，本装置内の複数のドメイン間で互いに経路を広告しません。AS 内経路や AS 外経路をほかのドメインに AS 外経路として広告したい場合は，経路フィルタリングを設定してください。

(c)　BGP4 または BGP4+での経路広告

経路フィルタリングを設定していない場合，ある AS から学習した経路はほかの AS に広告されます。この場合，BGP4 または BGP4+以外のルーティングプロトコルで BGP4 または BGP4+経路と同じ宛先の経路が存在しても，BGP4 または BGP4+で選択された最適な BGP4 または BGP4+経路が広告されます。

経路フィルタリングを設定している場合，広告される経路情報はディスタンス値によって選択された最も優先度の高い経路が対象となります。

13.1.6　複数プロトコル同時動作時の注意事項

(1)　OSPF または RIP-2 と RIP-1 の同時動作

OSPF や RIP-2 は IP アドレスのクラス A，B，C を意識しないで可変長サブネットマスクを扱うルーティングプロトコルであるのに対して，RIP-1 はクラス A，B，C を前提としているため可変長サブネットマスクは扱えません。したがって，両者を同一ネットワークで混在して使用する場合には次に示す注意が必要です。ここでは OSPF と RIP-1 の関係を例に説明しますが，RIP-2 と RIP-1 の関係も同様です。

(a)　OSPF で学習したサブネット経路を RIP-1 で広告しない場合

サブネッティングされたネットワークへの経路は次に示すどちらかの条件に当てはまる場合，該当する経路を RIP-1 で広告しないので注意してください。

1. RIP を使用しているインタフェースのネットワークアドレスと異なるサブネットマスク長を持つサブネットへの経路。
2. RIP を使用しているインタフェースのネットワークアドレスと異なるネットワークアドレスのサブネットへの経路。

● 異なるサブネットマスク長のサブネット間の接続

次の図の本装置 A の場合，ネットワーク B への経路を自分のルーティングテーブルに登録します。このとき，ネットワーク B が前に示した 1 の条件に当てはまるため，ネットワーク A にネットワーク B の経路を広告しません。

図 13-2　異なるサブネットマスク長のサブネット間の接続

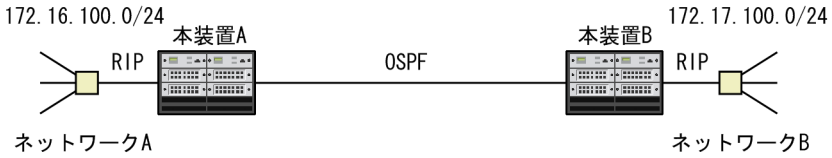


「図 13-5　サブネット間の接続の例」の本装置 A の場合，ネットワーク A とネットワーク B は同一ネットワーク内の同一サブネット長のサブネットのために経路を広告します。

● 異なるネットワークアドレスのサブネット間の接続

次の図の本装置 A の場合，ネットワーク B への経路を自分のルーティングテーブルに登録しますが，ネットワーク B が前に示した 2 の条件に当てはまるため，ネットワーク A にネットワーク B の経路を広告しません。

図 13-3　異なるネットワークアドレスのサブネット間の接続



「図 13-5　サブネット間の接続の例」の本装置 A の場合，ネットワーク A とネットワーク B は同一ネットワーク内の同一サブネット長のサブネットのために経路を広告します。

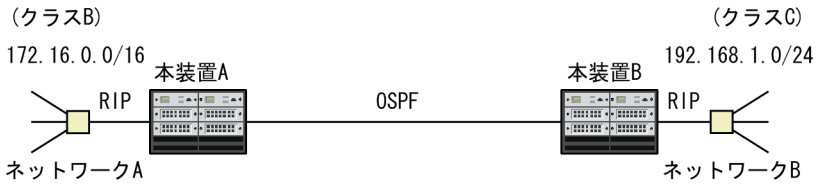
(b)　OSPF による RIP のネットワーク間接続

RIP が動作しているネットワーク間を OSPF で接続する場合は，次に示すどれかの構成で接続してください。

● サブネットを使用しない。

次の図の場合，ネットワーク A，ネットワーク B への経路情報は，それぞれネットワーク B，ネットワーク A に広告されます。

図 13-4　サブネットを使用しない例



● 同一ネットワークで同一サブネット長のサブネット間の接続に使用する。

次の図の場合，ネットワーク A，ネットワーク B への経路情報は，それぞれネットワーク B，ネットワーク A に広告されます。

図 13-5　サブネット間の接続の例



● デフォルトルートを広告する。

本装置 A および本装置 B に宛先がデフォルトルートのスタティック経路を設定して，RIP が動作しているネットワークに広告します。

次の図の場合，デフォルトルートの広告によって宛先アドレスが自ネットワークに一致しないパケットはデフォルトルートによって本装置 A および本装置 B に到達して，OSPF 経路経由で相手のネットワークに配送されます。

図 13-6　デフォルトルートの広告の例

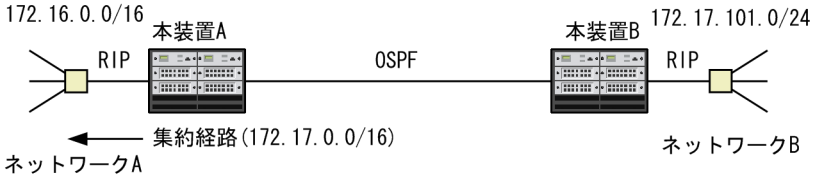


● 集約経路を広告する。

本装置 A に学習元が OSPF/OSPFASE（OSPF の AS 外経路）であるネットワーク B 宛ての経路をナチュラルマスクの経路に集約して，RIP が動作しているネットワークに広告するように指定します。

次の図の場合，集約経路の広告によってネットワーク B 宛てのパケットは本装置 A に到達して，OSPF/OSPFASE 経路経由で相手のネットワークに配送されます。

図 13-7　集約経路の広告の例

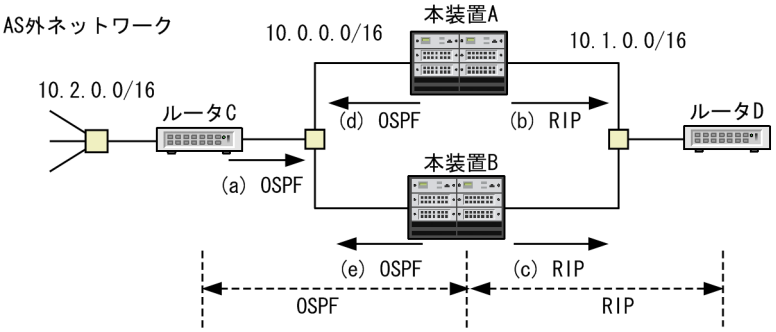


(2)　複数のプロトコルで同じ宛先の経路を学習する場合の注意事項

複数のプロトコルで同じ宛先の経路を学習すると，ネットワーク構成によってはルーティングループが発生することがあります。そのようなネットワーク構成では，経路のフィルタリングによってルーティングループが発生しないように注意してください。

次の図のネットワーク構成例では，10.0.0.0 のネットワークは OSPF を使用して，10.1.0.0 のネットワークでは RIP を使用しています。

図 13-8　ネットワーク構成例



ネットワーク 10.2.0.0 宛ての経路は次の 3 種類が生成されます。

1. ルータ C が広告する AS 外経路（図の（a））
2. OSPF から RIP に広告した経路（図の（b），（c））

3. RIP から OSPF に広告した経路（図の（d），（e））

この例では，本装置 B が（d）を選択して本装置 A が（c）を選択した場合，または本装置 A が（e）を選択して本装置 B が（b）を選択した場合に，ルーティングループ（ネクストホップがお互いのルータを向いている）が発生します。このようなケースでは，本装置 A や本装置 B が OSPF から RIP に広告した 10.2.0.0 宛ての経路を RIP から OSPF の AS 外経路として学習しないように，経路フィルタリングを設定する必要があります。

13.1.7　コンフィグレーション設定・変更時の留意事項

ユニキャストルーティングプロトコルに関するコンフィグレーションを設定または変更すると，保持する経路すべてについてコンフィグレーションに基づいた経路の再評価を実施します。この経路の再評価中はユニキャストルーティングプロトコルに関する運用コマンドの実行や SNMP による MIB 取得に時間が掛かる場合があります。

13.2　ユニキャストルーティング共通のオペレーション

13.2.1　運用コマンド一覧

ユニキャストルーティング共通の運用コマンド一覧を次の表に示します。

表 13-6　運用コマンド一覧

コマンド名	説明
show ip route	ルーティングテーブルで保持する IPv4 経路情報を表示します。
clear ip route	H/W の IPv4 フォワーディングエントリをクリアして再登録します。
show ip interface ipv4-unicast	ユニキャストルーティングプログラムが認識している本装置の IPv4 インタフェース情報を表示します。
debug ip	IPv4 ルーティングプロトコルが送受信するパケットをリアルタイムに表示します。
show ipv6 route	ルーティングテーブルで保持する IPv6 経路情報を表示します。
clear ipv6 route	H/W の IPv6 フォワーディングエントリをクリアして再登録します。
show ipv6 interface ipv6-unicast	ユニキャストルーティングプログラムが認識している本装置の IPv6 インタフェース情報を表示します。
debug ipv6	IPv6 ルーティングプロトコルが送受信するパケットをリアルタイムに表示します。
show system※1	運用状態を表示します。
show ip interface※2	IPv4 インタフェースの状態を表示します。
show netstat (netstat)※2	ネットワークの状態・統計を表示します。
ping※2	指定 IPv4 アドレスの装置へ試験パケットを送信して，通信できるかどうかを判定します。
traceroute※2	宛先ホストまで IPv4 データグラムが通ったルートを表示します。
show ipv6 interface※3	IPv6 インタフェースの状態を表示します。
ping ipv6※3	指定 IPv6 アドレスの装置へ試験パケットを送信して，通信できるかどうかを判定します。
show processes cpu unicast※4	ユニキャストルーティングプログラムの CPU 使用率を表示します。
restart unicast※4	ユニキャストルーティングプログラムを再起動します。
dump protocols unicast※4	ユニキャストルーティングプログラムで採取しているトレース情報や制御テーブル情報をファイルへ出力します。
erase protocol-dump unicast※4	ユニキャストルーティングプログラムが生成したトレース情報や制御テーブル情報のファイルを削除します。

注※1

「運用コマンドレファレンス Vol.1　11. 装置とソフトウェアの管理」を参照してください。

注※2

「運用コマンドレファレンス Vol.3　2. IPv4・ARP・ICMP」を参照してください。

注※3

「運用コマンドレファレンス Vol.3　3. IPv6・NDP・ICMPv6」を参照してください。

注※4

「運用コマンドレファレンス Vol.3　12. IPv4・IPv6 ルーティングプロトコル共通」を参照してください。

13.2.2　宛先アドレスへの経路確認

本装置で IPv4 ユニキャストルーティング情報を設定した場合は，show ip route コマンドを実行して宛先アドレスへの経路が存在していることを確認してください。IPv6 ユニキャストルーティング情報を設定した場合は，show ipv6 route コマンドで経路情報を確認できます。

図 13-9　show ip route コマンドの表示例

```
> show ip route
Date 20XX/03/14 12:00:00 UTC
Total: 13 routes
Destination        Next Hop        Interface      Metric   Protocol  Age
172.16/16          192.168.1.100   Eth1/1         2/0      RIP        8s <-1
192.168.1/24       192.168.1.1     Eth1/1         0/0      Connected  8s
     :
     :
>
```

1.宛先アドレスに対する経路が存在することを確認してください。

13.3　ネットワーク設計の考え方

この節では，ネットワークを設計する場合の考え方について説明します。

13.3.1　IPv4 ネットワークのアドレス設計

ローカルアドレスを使用するときに IPv4 アドレスの割り当てに余裕がある場合は，次のような考え方に従うと注意事項の多くを回避でき，比較的簡単にネットワークを設計できます。

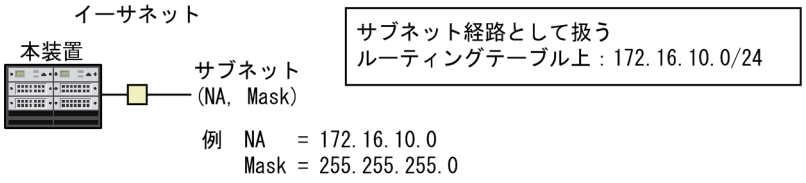
1. 複数のネットワークアドレスを使用しないで，大きな単一のネットワークアドレス（クラス A またはクラス B）をサブネット化して使用して，アドレス境界を作らないようにします。
2. サブネットマスクのビット数は同一とします（可変長サブネットマスクにならないようにします）。

1.および 2.のアドレッシング条件に合わないで RIP-1 によるルーティングをする場合は，経路広告条件に注意が必要です。

13.3.2　IPv4 ネットワークの直結経路の取り扱い

本装置はブロードキャスト型の回線を取り扱います。ブロードキャスト型ではネットワークアドレス（NA）とサブネットマスク（Mask）として扱います。ブロードキャスト型の直結経路の取り扱いを次の図に示します。

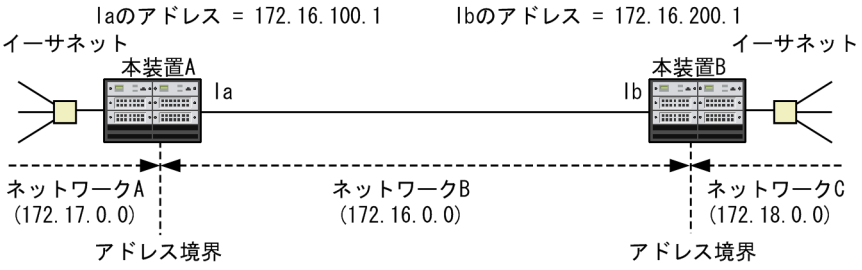
図 13-10　直結経路の取り扱い（IPv4 ネットワーク）



13.3.3　IPv4 ネットワークのアドレス境界の設計

複数のネットワークアドレスを使用する場合は，次の図に示すように本装置上にアドレス境界を置くようにしてください。アドレス境界とはナチュラルマスクに対応したネットワークアドレスの境界を意味します。アドレスクラスの境界ではありません。

図 13-11　通常のアドレス境界設計例



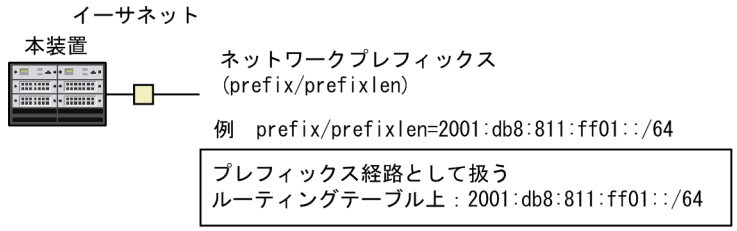
13.3.4　IPv6 ネットワークのアドレス設計

IPv6 アドレス割り当て時には，ネットワークトポロジの階層構造に従って分割すると注意事項の多くを回避でき，比較的簡単にネットワークを設計できます。

13.3.5　IPv6 ネットワークの直結経路の取り扱い

本装置はブロードキャスト型の回線を取り扱います。ブロードキャスト型ではネットワークプレフィックス（prefix）とプレフィックス長（prefixlen）として扱います。ブロードキャスト型の直結経路の扱いを次の図に示します。

図 13-12　直結経路の取り扱い（IPv6 ネットワーク）



13.4　ロードバランスの解説

13.4.1　ロードバランスの概要

ロードバランスは，マルチパス接続（宛先ネットワークアドレスに対して複数の経路を構築）によって，IP レイヤのルーティング制御で増大するトラフィックの負荷を分散する機能です。広帯域の回線にアップグレードしないで，既存の回線を集合して広帯域を供給します。

ここで説明するのはレイヤ 3 で実現するロードバランスです。

マルチパスを使用した負荷分散（隣接ルータが単一または複数の場合）を次の図に示します。この図では四つのパスを利用して，ネットワーク A からネットワーク B 内のサーバ宛てのパケットをハードウェア処理で高速に中継します。

図 13-13　マルチパスを使用した負荷分散（隣接ルータが単一の場合）

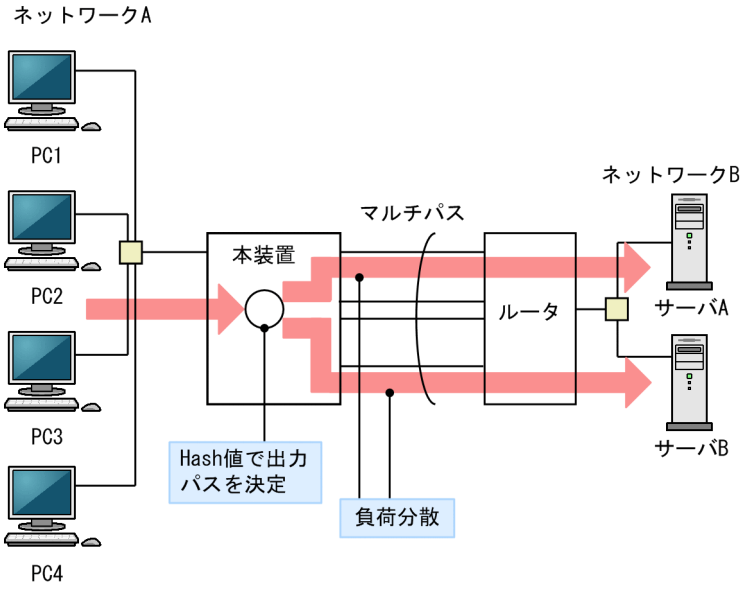
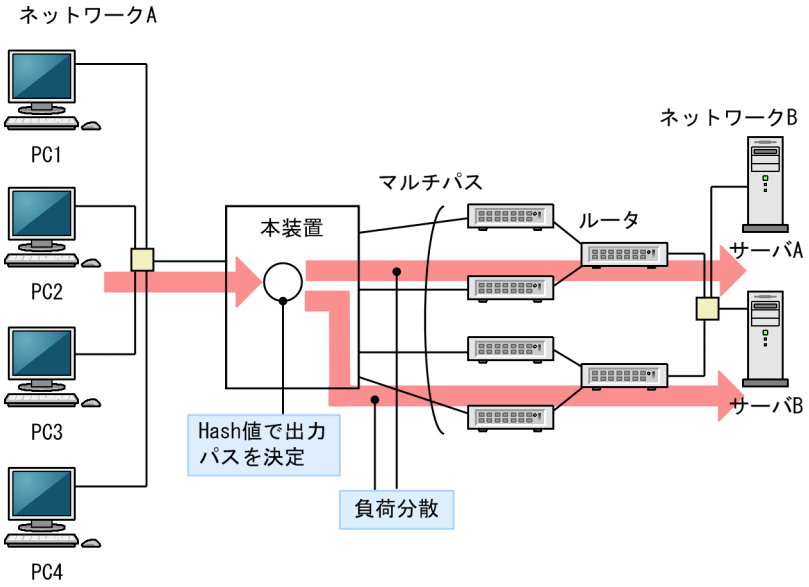


図 13-14　マルチパスを使用した負荷分散（隣接ルータが複数の場合）



13.4.2　ロードバランス仕様

本装置で実装するマルチパスの仕様とロードバランスの仕様を次の表に示します。

表 13-7　マルチパス仕様

項目	仕様	備考
一つの宛先ネットワークに対するマルチパス数	2～16	－
コンフィグレーションで指定できる最大マルチパス数	1～16（1 を指定したときはマルチパスを生成しません）	ルーティングプロトコル単位で指定します。
マルチパスを生成できるルーティングプロトコル	• スタティック • OSPF または OSPFv3 • BGP4 または BGP4+	－
デフォルトのコンフィグレーションでのマルチパス数	• スタティック：4 • OSPF または OSPFv3：4 • BGP4 または BGP4+：1（マルチパスを生成しません）	－
接続形態	回線種別およびインタフェース種別に関係なく使用できます。また，混在もできます。	複数の VRF 間でのマルチパスはサポートしません。

（凡例）　－：該当しない

表 13-8　ロードバランス仕様

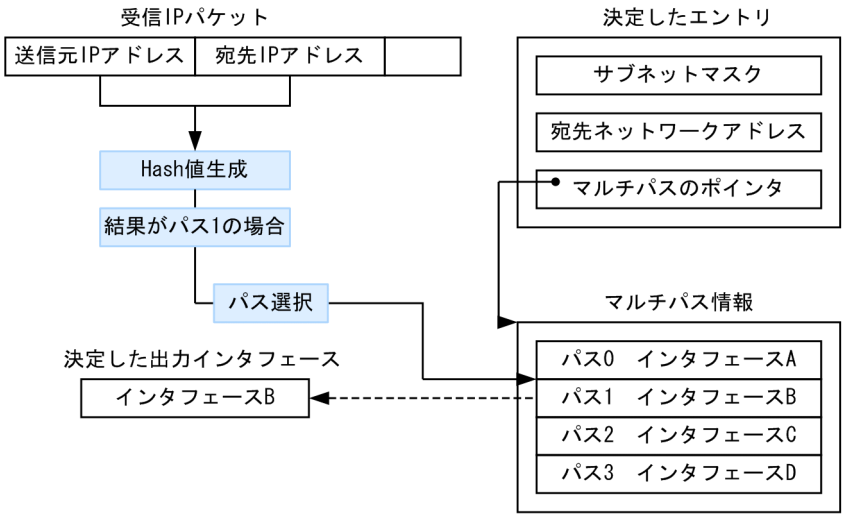
項目	仕様	備考
マルチパスの振り分け方法	宛先 IP アドレスと送信元 IP アドレスからパスに振り分ける値（Hash 値）を算出して，決定した出力パスに振り分けます。 宛先 IP アドレスと送信元 IP アドレスが同一のパケットは，同一出力パスを選択します。これによって，送信の順序性を保証します。	－
ルーティングテーブル内のマルチパス情報	ルーティングテーブルに設定する各出力インタフェースの Hash 値の割り当て比率は，ほぼ均等になります。	「13.4.4　ロードバランス使用時の注意事項」の 1 および 2 を参照
各パスの重み付け	できません。	「13.4.4　ロードバランス使用時の注意事項」の 1 を参照
出力帯域を超えたパケットの処理	別のパスに振り分けません。継続して帯域を超えた場合は装置内で保持しますが，保持しきれない場合はパケットを廃棄します。	－

（凡例）　－：該当しない

13.4.3　出力インタフェースの決定

ルーティングテーブルの検索で，宛先 IP アドレスに該当するエントリが決定すると，次に出力インタフェースを決定します。出力インタフェースは，受信した IP パケットの送信元 IP アドレス（Source IP Address）と宛先 IP アドレス（Destination IP Address）から Hash 値を生成して，それによってマルチパスの候補の一つを選択して決定します。出力インタフェースの決定を次の図に示します。

図 13-15　出力インタフェースの決定



13.4.4　ロードバランス使用時の注意事項

1. Hash 値によって一意に転送できるパスのうち 1 パスを選択するため，宛先ネットワークに対するそれぞれのパスのパケット分配比率は必ずしも均等になりません。

2. 各パスに対して重み付けをしないため，回線速度が異なる場合は速度に比例して分配しません。ただし，マルチホーム接続することによって回線速度の速い回線に重み付けできますが，障害の発生を考慮して冗長構成にする必要があります。
3. Hash 値によって選択した該当パスの出力帯域を超えて継続的にパケットを送信しようとした場合，パケット廃棄が発生します。別のパスには振り分けません。
4. traceroute コマンドによって，ロードバランスで使用する選択パスを確認する場合は次の注意が必要です。
   - traceroute コマンドを受信したインタフェースの IP アドレスを送信元 IP アドレスとして応答を返しますが，そのインタフェースを使用して応答を返すとは限りません。
   - traceroute コマンドを受信したインタフェースがマルチホームの場合，隣接装置がどのサブネットで送信したのか判断できません。そのため，マルチホーム内の 1 アドレスを送信元 IP アドレスとして応答します。
5. ロードバランス使用時に，特定の中継経路（ゲートウェイ）だけに通信が集中する場合，中継性能が極端に低下することがあります。その場合，すべての中継経路（ゲートウェイ）に対してスタティック ARP またはスタティック NDP を設定してください。
6. BGP4 または BGP4+経路が，Null インタフェースを指定した IGP 経路でネクストホップ解決されることによって BGP4 または BGP4+経路のマルチパスに Null インタフェースを含む場合，該当経路に一致したパケットを廃棄します。その場合，コンフィグレーションコマンド bgp nexthop で，Null インタフェースを指定した IGP 経路を BGP4 または BGP4+経路のネクストホップ解決に使用しないように設定してください。
7. コンフィグレーションでネクストホップに複数の VRF が混在するスタティック経路を設定できますが，生成される経路のマルチパスは単一の VRF だけで構成されます。

   パスは，現在有効でかつ最も高い weight 値を持つネクストホップを基準として，それと同じ VRF のネクストホップの中から選択されます。
8. スタティック経路のマルチパスに Null インタフェースは含みません。有効なネクストホップアドレスだけでマルチパスを構成します。
9. スタティック経路のマルチパスにリジェクト経路を含む場合，該当経路に一致したパケットを廃棄します。マルチパスにリジェクト経路を含まないように設定してください。

13.5　ロードバランスのコンフィグレーション

スタティック経路および各プロトコルでのロードバランスについては，次を参照してください。

- スタティック経路を使用したロードバランス
  「14.2.4　マルチパス経路の設定」
- OSPF でのロードバランス
  「17.2.6　マルチパスの設定」
- OSPFv3 でのロードバランス
  「19.2.6　マルチパスの設定」
- BGP4 でのロードバランス
  「22.2.3　BGP4 マルチパスの設定」
- BGP4+でのロードバランス
  「22.3.3　BGP4+マルチパスの設定」

13.6　ロードバランスのオペレーション

13.6.1　経路情報の確認

show ip route コマンドまたは show ipv6 route コマンドを実行して，マルチパス経路の設定内容が正しく反映されていることを確認してください。

図 13-16　マルチパスの経路情報表示

```
> show ip route
Date 20XX/03/14 12:00:00 UTC
Total: 13 routes
Destination        Next Hop        Interface      Metric   Protocol  Age
192.168.1/24       192.168.1.1     Eth1/1         0/0      Connected 19m 46s
192.168.1.1/32     192.168.1.1     Eth1/1         0/0      Connected 19m 46s
192.168.2/24       192.168.2.1     Eth1/2         0/0      Connected 19m 46s
192.168.2.1/32     192.168.2.1     Eth1/2         0/0      Connected 19m 46s
192.168.3/24       192.168.3.1     Eth1/3         0/0      Connected 19m 46s
192.168.3.1/32     192.168.3.1     Eth1/3         0/0      Connected 19m 46s
172.16/16          192.168.1.200   Eth1/1         0/0      Static     9s
                   192.168.2.200   Eth1/2         -        -         -
                   192.168.3.200   Eth1/3         -        -         -
     :
     :
>
```

13.6.2　宛先アドレスとの通信可否の確認

ping コマンドまたは ping ipv6 コマンドで specific-route パラメータと source パラメータを指定して，ロードバランスで使用する本装置のインタフェースが相手装置に対して通信できることを確認してください。コマンド実行時には送信元アドレスとして，ロードバランスで使用するインタフェースの本装置の自 IP アドレスを指定してください。

13.7　経路集約の解説

13.7.1　概要

経路集約は一つまたは複数の経路情報から，該当する経路情報を包含するネットワークマスクのより短い経路情報を生成します。これは複数の経路情報から該当する経路情報を包含する一つの経路情報を生成して，隣接ルータなどに集約経路を通知して，ネットワーク上の経路情報の数を少なくする方法です。例えば，172.16.178.0/24 の経路情報や 172.16.179.0/24 の経路情報を学習した場合に，172.16.0.0/16 の集約された経路情報を生成します。

経路集約はコンフィグレーションコマンド ip summary-address または ipv6 summary-address で明示的に指定する必要があります。集約経路にはディスタンス値を指定できます。ディスタンス値を指定していない場合は，デフォルト値（130）が使用されます。なお，集約元となる経路情報が学習されていない場合には集約経路情報は生成されません。

13.7.2　集約経路の転送方法

集約経路はリジェクト経路です。より優先する経路がないパケットは廃棄されます。

集約経路がリジェクト経路になっているのは，ルーティングループを防ぐためです。集約経路を広告すると，その集約経路宛てのパケットが本装置へ転送されてきます。ここで本装置が集約元経路のないパケットをデフォルト経路などの次善の経路に従って転送すると，デフォルト経路転送先装置と本装置の間でルーティングループが発生することがあります。これを防ぐため，集約経路はリジェクト経路になっています。

ただし，noinstall パラメータを指定した集約経路はパケットを廃棄しません。デフォルト経路など次善の経路がある場合は，その経路に従ってパケットを転送します。noinstall パラメータは，広告用に集約経路を設定したいが，その集約経路でパケットを廃棄するよりも次善の経路に従って転送する方がよい場合に使用します。

13.7.3　AS_PATH 属性の集約

BGP4 または BGP4+経路が集約元経路に含まれる場合，集約した経路に BGP4 または BGP4+経路のパス属性を付加します。集約元の BGP4 または BGP4+経路が複数ある場合は集約元経路間でパス属性を集約します。集約した経路の AS_PATH 属性と COMMUNITIES 属性について次の編集を行います。

(1)　AS_PATH 属性

集約元経路間で AS_PATH 属性の AS_SEQUENCE タイプ内 AS パスの先頭から共通の部分を，集約した経路の AS_PATH 属性の AS_SEQUENCE タイプに設定します。また，上記以外の AS_SEQUENCE タイプ内 AS パス，および AS_SEQUENCE タイプ以外の AS パスについては，コンフィグレーションコマンド ip summary-address または ipv6 summary-address で as_set パラメータが指定されている場合に限り，集約した経路の AS_PATH 属性の AS_SET タイプに設定します。

(2)　COMMUNITIES 属性

集約元となる BGP4 または BGP4+経路が持つすべてのコミュニティを，集約した経路の COMMUNITIES 属性に設定します。

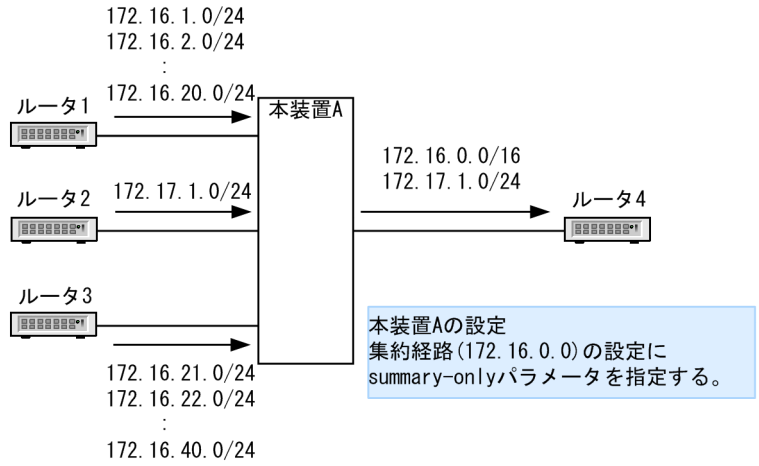
13.7.4　集約元経路の広告抑止

経路集約後，集約経路については広告するが集約元となった経路については広告対象外にできます。例えば，集約元経路以外の RIP 経路は広告したいが集約元の RIP 経路を広告しないなどです。

(1)　IPv4 経路情報での集約元経路の広告抑止

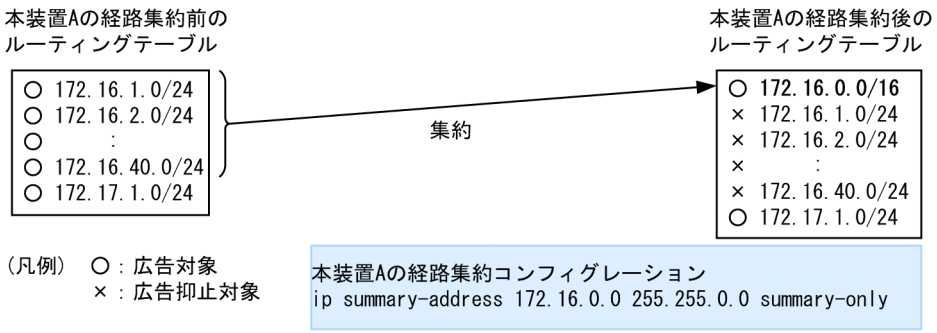
集約元経路の広告抑止は，コンフィグレーションコマンド ip summary-address の summary-only パラメータで指定します。集約元経路の広告抑止の適用例を次の図に示します。

図 13-17　IPv4 経路情報での集約元経路の広告抑止の適用例



本装置 A はルータ 1 から 172.16.1.0/24，172.16.2.0/24，…，172.16.20.0/24 を受信して，ルータ 2 から 172.17.1.0/24 を受信します。また，ルータ 3 から 172.16.21.0/24，172.16.22.0/24，…，172.16.40.0/24 を学習します。本装置 A では，集約経路 172.16.0.0/16 と学習経路 172.17.1.0/24 をルータ 4 へ広告するように広告経路フィルタを設定します。このとき，summary-only パラメータを指定して学習経路から集約経路 172.16.0.0/16 を生成するように設定した場合，広告経路フィルタに集約元経路の広告を抑止する設定が不要となります。経路集約のコンフィグレーション例と経路集約前後の経路を次の図に示します。

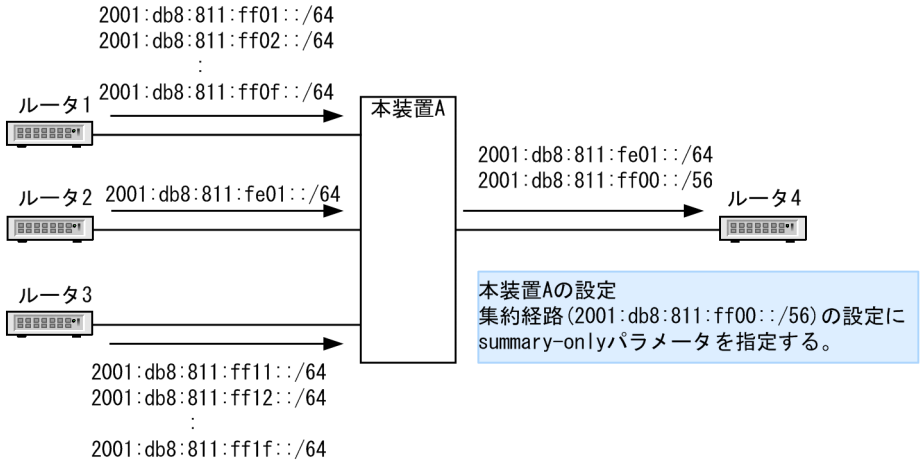
図 13-18　IPv4 経路集約のコンフィグレーション例と経路集約前後の経路



(2)　IPv6 経路情報での集約元経路の広告抑止

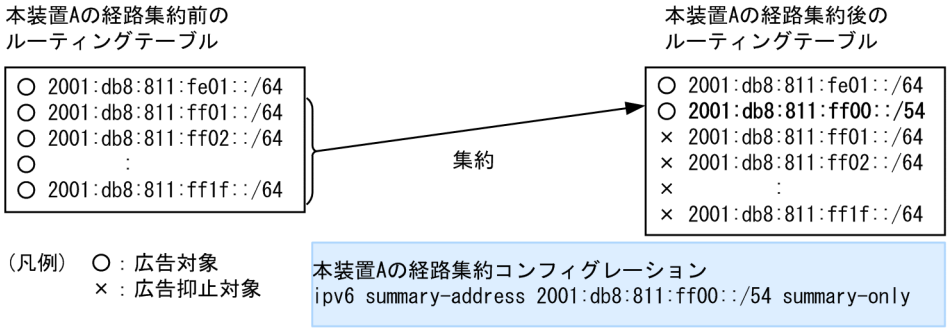
集約元経路の広告抑止は，コンフィグレーションコマンド ipv6 summary-address の summary-only パラメータで指定します。集約元経路の広告抑止の適用例を次の図に示します。

図 13-19　IPv6 経路情報での集約元経路の広告抑止の適用例



本装置 A はルータ 1 から 2001:db8:811:ff01::/64, 2001:db8:811:ff02::/64, …, 2001:db8:811:ff0f::/64 を受信して，ルータ 2 から 2001:db8:811:fe01::/64 を受信します。また，ルータ 3 から 2001:db8:811:ff11::/64, 2001:db8:811:ff12::/64, …, 2001:db8:811:ff1f::/64 を学習します。本装置 A では, 集約経路 2001:db8:811:ff00::/56 と学習経路 2001:db8:811:fe01::/64 をルータ 4 へ広告するように広告経路フィルタを設定します。このとき，summary-only パラメータを指定して学習経路から集約経路 2001:db8:811:ff00::/56 を生成するように設定した場合, 広告経路フィルタに集約元経路の広告を抑止する設定が不要となります。経路集約のコンフィグレーション例と経路集約前後の経路を次の図に示します。

図 13-20　IPv6 経路集約のコンフィグレーション例と経路集約前後の経路



13.8　経路集約のコンフィグレーション

13.8.1　コンフィグレーションコマンド一覧

経路集約のコンフィグレーションコマンド一覧を次の表に示します。

表 13-9　コンフィグレーションコマンド一覧

コマンド名	説明
ip summary-address	IPv4 の集約経路を生成します。
ipv6 summary-address	IPv6 の集約経路を生成します。
redistribute (BGP4)※	BGP4 から広告する経路のプロトコル種別を設定します。
redistribute (BGP4+)※	BGP4+から広告する経路のプロトコル種別を設定します。
redistribute (OSPF)※	OSPF から広告する経路のプロトコル種別を設定します。
redistribute (OSPFv3)※	OSPFv3 から広告する経路のプロトコル種別を設定します。
redistribute (RIP)※	RIP から広告する経路のプロトコル種別を設定します。
redistribute (RIPng)※	RIPng から広告する経路のプロトコル種別を設定します。

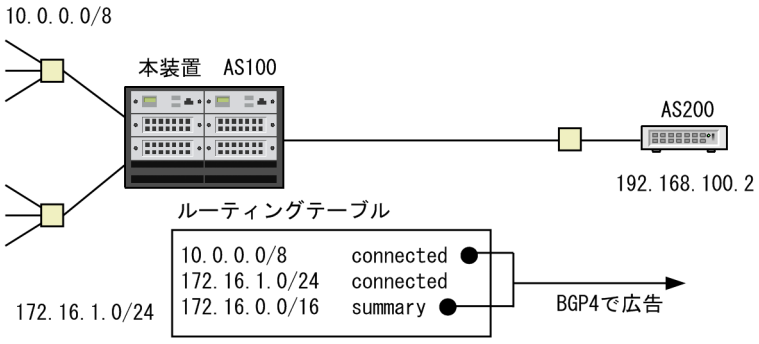
注※

「コンフィグレーションコマンドレファレンス Vol.3　22. 経路フィルタリング」を参照してください。

13.8.2　IPv4 経路集約と集約経路広告の設定

直結経路を集約元経路とする経路集約の設定をします。また，集約経路と直結経路を BGP4 に再広告するための設定をします。ただし，再広告の際は集約元となった直結経路を再広告しないようにします。

図 13-21　集約経路を BGP4 で広告する構成



[設定のポイント]

集約経路の生成には ip summary-address コマンドを使用します。また，BGP4 で集約経路を広告する設定には，redistribute summary コマンドを使用します。

[コマンドによる設定]

1. **(config)# ip summary-address 172.16.0.0 255.255.0.0 summary-only**

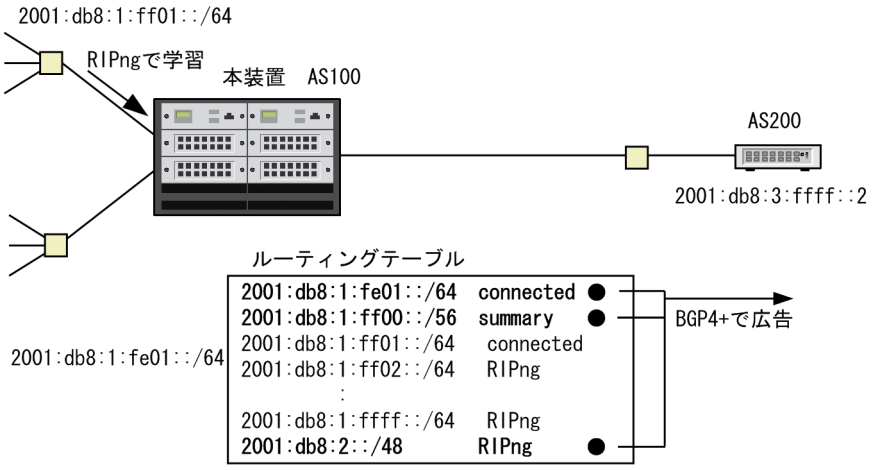
集約経路 172.16.0.0/16 を生成する設定をします。summary-only を指定して，集約元となる直結経路 172.16.1.0/24 の再広告を抑止します。

2. **(config)# router bgp 100**
   (config-router)# neighbor 192.168.100.2 remote-as 200
   隣接ルータ 192.168.100.2 に対して，BGP4 で接続する設定をします。
3. **(config-router)# redistribute summary**
   BGP4 で集約経路を再広告する設定をします。
4. **(config-router)# redistribute connected**
   BGP4 で直結経路を再広告する設定をします。

13.8.3　IPv6 経路集約と集約経路広告の設定

直結経路と RIPng 経路を集約元経路とする経路集約の設定をします。また，集約経路と直結経路を BGP4+に再広告するための設定をします。ただし，再広告の際は集約元となった直結経路および RIPng 経路を再広告しないようにします。

図 13-22　集約経路を BGP4+で広告する構成



[設定のポイント]

集約経路の生成には ipv6 summary-address コマンドを使用します。また，BGP4+で集約経路を広告する設定には，redistribute summary コマンドを使用します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   (config-if)# ipv6 address 2001:db8:1:fe01::1/64
   ポート 1/1 に IPv6 アドレス 2001:db8:1:fe01::1/64 を設定します。
2. **(config-if)# exit**
   (config)# interface gigabitethernet 1/2
   (config-if)# ipv6 address 2001:db8:1:ff01::1/64
   ポート 1/2 に IPv6 アドレス 2001:db8:1:ff01::1/64 を設定します。
3. **(config-if)# ipv6 rip enable**
   ポート 1/2 で RIPng パケットを送受信する設定をします。

4. **(config-if)# exit**

   (config)# ipv6 summary-address 2001:db8:1:ff00::/56 summary-only

   集約経路 2001:db8:1:ff00::/56 を生成する設定をします。summary-only を指定して，集約元となる経路の再広告を抑止します。

5. **(config)# router bgp 100**

   (config-router-af)# neighbor 2001:db8:3:ffff::2 remote-as 200

   隣接ルータ 2001:db8:3:ffff::2 に対して，BGP4+で接続する設定をします。

6. **(config-router)# address-family ipv6**

   (config-router-af)# redistribute summary

   BGP4+で集約経路を再広告する設定をします。

7. **(config-router-af)# redistribute connected**

   BGP4+で直結経路を再広告する設定をします。

8. **(config-router-af)# redistribute rip**

   BGP4+で RIPng 経路を再広告する設定をします。

9. **(config-router-af)# neighbor 2001:db8:3:ffff::2 activate**

   隣接ルータ 2001:db8:3:ffff::2 との経路交換を可能にします。

13.9　経路集約のオペレーション

13.9.1　運用コマンド一覧

IPv4 経路集約の運用コマンド一覧を次の表に示します。

表 13-10　運用コマンド一覧（IPv4）

コマンド名	説明
show ip route	ルーティングテーブルで保持する経路情報を表示します。
show ip rip	RIP プロトコルに関する情報を表示します。
show ip ospf	OSPF プロトコルに関する情報を表示します。
show ip bgp	BGP4 プロトコルに関する情報を表示します。

IPv6 経路集約の運用コマンド一覧を次の表に示します。

表 13-11　運用コマンド一覧（IPv6）

コマンド名	説明
show ipv6 route	ルーティングテーブルで保持する経路情報を表示します。
show ipv6 rip	RIPng プロトコルに関する情報を表示します。
show ipv6 ospf	OSPFv3 プロトコルに関する情報を表示します。
show ipv6 bgp	BGP4+プロトコルに関する情報を表示します。

13.9.2　IPv4 集約経路の確認

ルーティングテーブルに登録されている集約経路の情報を表示します。

図 13-23　集約経路の表示例

```
> show ip route summary_routes
Date 20XX/03/14 12:00:00 UTC
Total: 1 routes
Destination        Next Hop        Interface      Metric   Protocol  Age
172.16/16          ----            -              0/0      Summary   50s
```

特定のネットワーク（172.16.0.0/16）に含まれるアクティブ経路を表示します。

図 13-24　アクティブ経路の表示例

```
> show ip route 172.16.0.0/16 longer-prefixes
Date 20XX/03/14 12:00:00 UTC
Total: 3 routes
Destination        Next Hop        Interface      Metric   Protocol  Age
172.16/16          ----            -              0/0      Summary   56s
172.16.1/24        172.16.1.1      Eth1/1         0/0      Connected 365d
172.16.1.1/32      172.16.1.1      Eth1/1         0/0      Connected 365d
```

13.9.3　IPv6 集約経路の確認

ルーティングテーブルに登録されている集約経路の情報を表示します。

図 13-25　集約経路の表示例

```
> show ipv6 route brief summary_routes
Date 20XX/03/14 12:00:00 UTC
Total: 1 routes
Destination                 Next Hop                            Protocol
2001:db8:1:ff00::/56        ----                                Summary
```

特定のネットワーク（2001:db8:1:ff00::/56）に含まれるアクティブ経路を表示します。

図 13-26　アクティブ経路の表示例

```
> show ipv6 route brief 2001:db8:1:ff00::/56 longer-prefixes
Date 20XX/03/14 12:00:00 UTC
Total: 256 routes
Destination                 Next Hop                          Protocol
2001:db8:1:ff00::/56        ----                              Summary
2001:db8:1:ff01::/64        2001:db8:1:ff01::1                Connected
2001:db8:1:ff02::/64        2001:db8:1:ff01::2                RIPng
2001:db8:1:ff03::/64        2001:db8:1:ff01::2                RIPng
      :                           :                             :
2001:db8:1:ffff::/64        2001:db8:1:ff01::2                RIPng
```

13.10　ユニキャストルーティング高可用機能

13.10.1　概要

ユニキャストルーティング高可用機能は，系切替によって運用系 BCU が交替したときや，運用コマンドなどによってユニキャストルーティングプログラムが再起動したときに，ネットワークから経路が消えることによる通信の停止を防ぐための機能です。

(1)　ユニキャストルーティング高可用機能を使用しない場合の問題

本装置では，系切替によって運用系 BCU が交替したときや，運用コマンドなどによってユニキャストルーティングプログラムが再起動したときでも，本装置がパケット転送を中断することはありません。これは，本装置ではルーティングプログラムが交替しても以前のルーティングプログラムの経路を保留して動作し続けているためです。

しかし，ルーティングプロトコルを使用している場合は隣接ルータが本装置へパケットを転送しなくなるため，ネットワーク全体では通信が一時的に停止することがあります。これは次の理由によります。

- 新たに動作を始めたルーティングプログラムが隣接ルータと通信を開始すると，隣接ルータは新たな接続要求を受け取ります。これによって，隣接ルータでは以前の接続が切断したものと認識して，該当装置を経由する経路を削除します。
- 本装置が一部の経路を広告しません。これは，新しく動作を開始したルーティングプログラムが経路広告を開始した時点では，まだ経路情報の学習が完了していないためです。隣接ルータでは，本装置が広告しなかった経路を削除します。

(2)　サポート範囲

本装置は，ユニキャストルーティング高可用機能としてノンストップルーティングとグレースフル・リスタートをサポートしています。ユニキャストルーティング高可用機能のサポート範囲を次の表に示します。

表 13-12　ユニキャストルーティング高可用機能のサポート範囲

項目		ノンストップルーティング	グレースフル・リスタート
対象イベント	装置再起動	×	×
	系切替	○※1	○※2
	ユニキャストルーティングプログラム再起動	○	○※2
	TCP 高可用プログラム再起動	○	－
対象ルーティングプロトコル	OSPF	○	○
	OSPFv3	○	○
	BGP4	○	○
	BGP4+	○	○

（凡例）　○：取り扱う　×：取り扱わない　－：該当しない

注※1

系切替が連続した場合は，一部または全部の経路を引き継げないで，本装置を経由する通信が一時的に停止することがあります。

注※2

グレースフル・リスタート中に再度イベントが発生した場合は，グレースフル・リスタートの実行を中止します。または，グレースフル・リスタートが失敗します。

13.10.2　ノンストップルーティング

ノンストップルーティングは，系切替によって運用系 BCU が交替したときに系切替前のルーティングプロトコルの状態を引き継いで，新運用系 BCU で継続して動作することでネットワーク全体での通信を維持するための機能です。系切替後，本装置は隣接装置に再接続要求をしないで，系切替前の接続で動作します。そのため，系切替直後にネットワークの構成が変わった場合にも対応できます。ノンストップルーティングは装置単体で動作する機能のため，隣接ルータがノンストップルーティングをサポートしている必要はありません。

ノンストップルーティングの動作方式はプロトコルによって異なるため，動作条件も異なります。使用前に，各プロトコルのノンストップルーティング動作条件を確認してください。各プロトコルの個別機能については，次を参照してください。

- OSPF
  「18.5　ノンストップルーティングの解説」
- OSPFv3
  「20.3　ノンストップルーティングの解説」
- BGP4
  「22.1.11　ノンストップルーティング」
- BGP4+
  「22.1.11　ノンストップルーティング」

13.10.3　グレースフル・リスタート

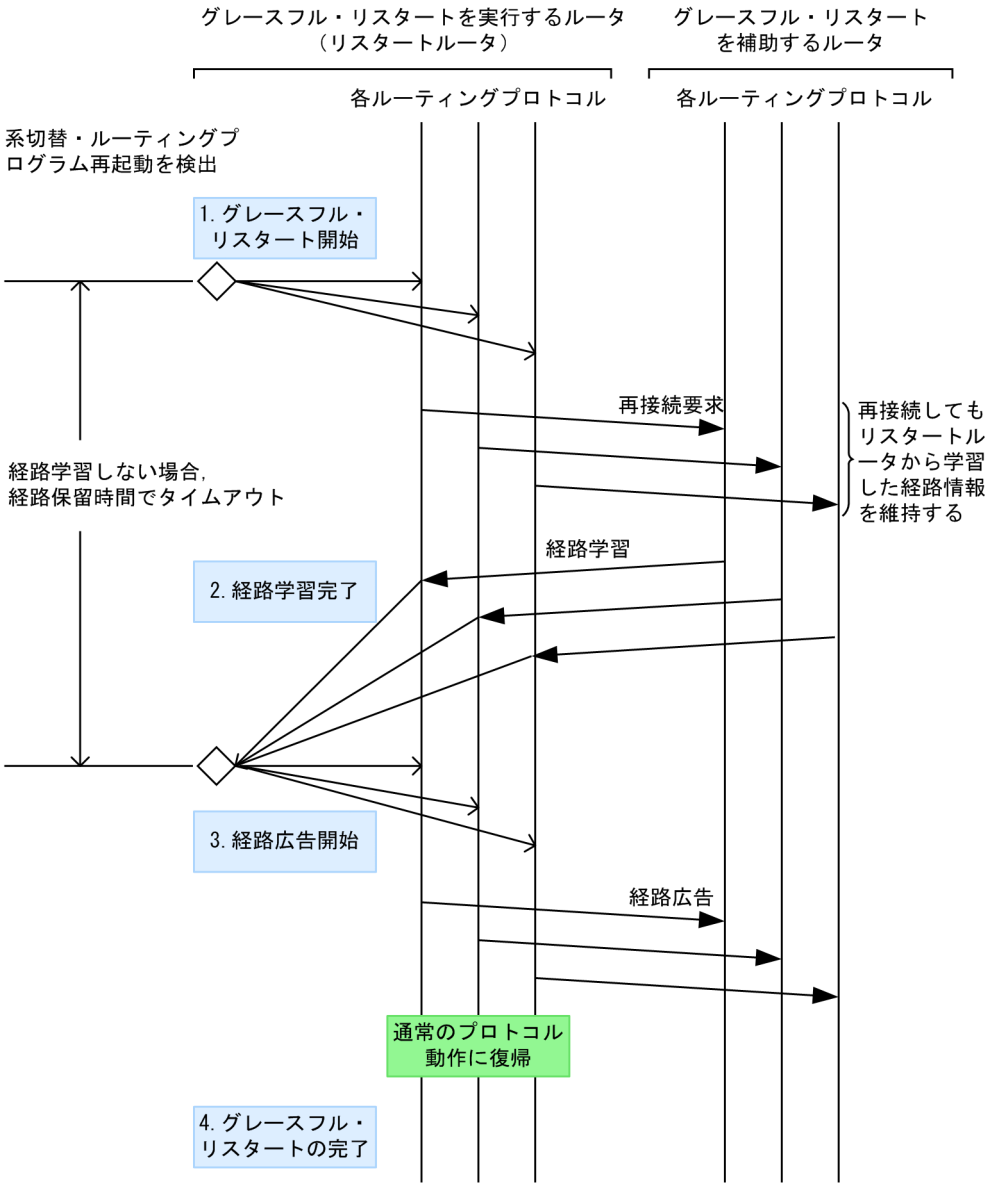
グレースフル・リスタートは，系切替によって運用系 BCU が交替したときや，運用コマンドなどによってユニキャストルーティングプログラムが再起動したときに，隣接装置と連携して本装置を中継する通信を維持するための機能です。グレースフル・リスタートの具体的な実現方法を次に示します。

- 隣接ルータに，グレースフル・リスタートを補助する機能を用意します。グレースフル・リスタートによる接続要求を受け取ったときに，以前の接続を切断して再接続するのではなく，以前の接続を継続しているものと認識する機能を追加します。これによって，ルーティングプログラム交替時にも隣接ルータとの接続が切断しなくなるため，隣接ルータも経路を保持したまま動作します。
- 経路学習および経路広告の処理順序を固定します。グレースフル・リスタートをするときに，まず隣接ルータから経路情報を学習して，経路学習が完了してから経路広告を開始します。これによって，一部経路しか広告しないことで隣接ルータから経路が消えることがなくなります。

なお，グレースフル・リスタートを実施するルータのことをリスタートルータと呼びます。

本装置のグレースフル・リスタート動作手順を次の図に示します。

図 13-27　グレースフル・リスタート手順



1. 系切替またはルーティングプログラムの再起動を検出すると，各プロトコルがグレースフル・リスタートを開始します。各プロトコルはグレースフル・リスタートによって再接続して，経路を学習します。
2. グレースフル・リスタート対象の各プロトコルが経路学習を完了します。ただし，グレースフル・リスタートを開始してから，グレースフル・リスタート時の経路保留時間（コンフィグレーションコマンド routing options graceful-restart time-limit の指定値）内に経路学習が完了しなかった場合は，経路学習を中断して，経路広告を開始します。
3. 経路学習の完了後，グレースフル・リスタート対象の各プロトコルは経路広告を開始します。ただし，エクストラネットを使用している場合は，次の状態になってもすぐに経路広告は開始しません。30 秒経過してから，各プロトコルは経路広告を開始します。
   - 各プロトコルの経路学習が完了
   - グレースフル・リスタートの経路保留時間内の経路学習がタイムアウト

4. 各プロトコルは，経路広告を完了すると通常のプロトコル動作に戻ります。全プロトコルが経路を広告し終わった時点で，装置全体のグレースフル・リスタートが完了します。

グレースフル・リスタートの動作方式はプロトコルによって異なるため，動作条件も異なります。使用前に，各プロトコルのグレースフル・リスタート動作条件を確認してください。各プロトコルの個別機能については，次を参照してください。

- OSPF
  「18.7　グレースフル・リスタートの解説」
- OSPFv3
  「20.5　グレースフル・リスタートの解説」
- BGP4
  「22.1.12　グレースフル・リスタート」
- BGP4+
  「22.1.12　グレースフル・リスタート」

13.10.4　ユニキャストルーティング高可用機能使用時の注意事項

(1)　ノンストップルーティングとグレースフル・リスタートの同時使用時の注意事項

ノンストップルーティングとグレースフル・リスタートのリスタート機能は排他で動作します。各ルーティングプロトコルの設定単位内で同時に設定が有効な場合，ノンストップルーティングだけが動作して，リスタート機能は無効になります。異なる設定単位間では，ノンストップルーティングとリスタート機能を使い分けられます。

(2)　ノンストップルーティング使用時の注意事項

- ノンストップルーティング使用時，ルーティングプロトコルの状態の同期が完了していない場合，運用コマンド redundancy force-switchover による系切替はできません。運用系 BCU の障害による系切替など，運用コマンド以外の契機で系切替が発生すると，ノンストップルーティングに失敗することがあります。
  ルーティングプロトコルの状態の同期状況は，運用コマンド show nsr unicast で確認してください。
- ノンストップルーティング使用時，隣接装置との接続関係が変化した場合，運用コマンド redundancy force-switchover による系切替は 1 分以上時間を空けることを推奨します。1 分以内に系切替が発生すると，新運用系 BCU で隣接装置との接続関係が変化したことを再度検知することがあります。

(3)　グレースフル・リスタート使用時の注意事項

- グレースフル・リスタート中はコンフィグレーションを変更しないでください。グレースフル・リスタート中にコンフィグレーションを変更するとグレースフル・リスタートに失敗することがあります。
- グレースフル・リスタート中は，グレースフル・リスタートの補助機能が動作しません。
- グレースフル・リスタート中に隣接ルータで障害が発生した場合，グレースフル・リスタートに失敗することがあります。
- グレースフル・リスタート手順が成功しても，隣接装置で本装置から学習した経路情報を保持できなかった場合，通信が停止することがあります。
- 障害による系切替の場合，系切替が完了しグレースフル・リスタートによる再学習を始めるよりも前に，隣接装置が切断を検出することがあります。各プロトコルの切断検出時間は，系切替所要時間より

も長くなるようにしてください。デフォルト値で運用したときのプロトコル別の切断検出までの最短時間の目安値を次に示します。

- OSPF および OSPFv3：25 秒
- BGP4 および BGP4+：100 秒

- 系切替所要時間はインタフェース数に依存します。系切替所要時間の目安値を次の表に示します。

表 13-13　系切替所要時間の目安値

インタフェース数※	系切替所要時間（秒）
4000	30
8000	45
16000	80

注※　同一インタフェースそれぞれに IPv4 アドレスと IPv6 アドレスを設定した場合。

なお，この目安値は，VRRP，NTP，マルチキャストルーティングプロトコルなど，ほかのレイヤ 3 機能が同時動作していない場合のものです。これらの機能が同時に動作する場合は，系切替所要時間が長くなることがあります。

- 運用コマンドによる系切替でグレースフル・リスタートを使用する場合，各プロトコルのリスタート時間を，系切替所要時間よりも長くなるように指定してください。
- OSPF および OSPFv3 のリスタート時間を，系切替所要時間と経路学習時間の合計よりも長くしてください。これは，経路情報を同期するためには，系切替を完了して IP インタフェースの Up/Down 状態が確認できるようになる必要があるためです。
- BGP4 および BGP4+のリスタート時間を，系切替所要時間とコネクション確立に掛かる時間の合計よりも長くしてください。これは，ピアのコネクションを確立するには，系切替を完了して IP インタフェースの状態を確認できるようになる必要があるためです。さらに，BGP4 および BGP4+で直接接続されていない内部ピア接続によってピアアドレス宛ての経路情報を IGP で交換している場合，BGP4 および BGP4+のリスタート時間を，OSPF および OSPFv3 のリスタート時間とピアのコネクション確立に掛かる時間の合計よりも長くしてください。これは，ピアのコネクションを確立するには，ピアアドレスを解決する IGP がグレースフル・リスタートによって経路を学習しておく必要があるためです。
- グレースフル・リスタート時の経路保留時間（コンフィグレーションコマンド routing options graceful-restart time-limit の指定値）を，各プロトコルのリスタート時間よりも長く設定してください。OSPF および OSPFv3 では，リスタート時間が，経路計算の実施を待つ時間の上限となります。したがって，経路保留時間がリスタート時間以下の場合，経路計算によってフォワーディングテーブルを更新するより先に，保留経路（更新されていないフォワーディングテーブル）が削除されるため，通信が停止します。また，BGP4 および BGP4+では，リスタート時間がコネクションの再確立を待つ時間の上限となるため，再確立が最も遅い場合は，リスタート時間後にピアからの経路学習を開始します。経路学習およびフォワーディングテーブルを更新する時間のため，BGP4 および BGP4+のリスタート時間は経路保留時間より 60 秒程度短い値を設定してください。なお，目安の設定値は経路数および隣接するピア数に依存します。

13.11　高速経路切替機能

13.11.1　概要

高速経路切替機能は，同一の宛先を持つ複数の経路が存在する場合に，最も優先度が高い経路情報（第 1 優先経路と呼ぶ）と，第 1 優先経路の次に優先される経路（第 2 優先経路と呼ぶ）をあらかじめルーティングテーブルに登録しておき，インタフェースダウンなどによって第 1 優先経路が使用できなくなったとき，素早く第 2 優先経路をフォワーディングテーブルに登録することで，通信停止時間の短縮を図る機能です。本機能はコンフィグレーションの設定がなくても動作します。

高速経路切替のサポート範囲を次の表に示します。

表 13-14　高速経路切替のサポート範囲

切替契機	切替内容
インタフェースダウン	第 2 優先経路への切り替え
	マルチパス経路の縮退
インタフェースダウンを伴わない IGP 経路の変更による BGP4 または BGP4+経路のネクストホップ変更※	第 2 優先経路への切り替え
	マルチパス経路の縮退
インタフェースダウンを伴わないピア切断による BGP4 または BGP4+経路のネクストホップ変更※	第 2 優先経路への切り替え
	マルチパス経路の縮退

注※　BFD によるダウンを検出した場合も含みます。

高速経路切替を適用する経路の組み合わせを次の表に示します。

表 13-15　高速経路切替を適用する経路の組み合わせ

項目		第 1 優先経路					
		RIP/RIPng	OSPF/OSPFv3	BGP4※/BGP4+※	スタティック※	集約経路	直結経路
第 2 優先経路	RIP/RIPng	○	○	○	○	×	×
	OSPF/OSPFv3	○	−	○	○	×	×
	BGP4/BGP4+	○	○	○	○	×	×
	スタティック※	○	○	○	○	×	×
	集約経路	×	×	×	×	−	×
	直結経路	×	×	×	×	×	−

（凡例）　○：適用する　×：適用しない　−：この組み合わせは発生しない

注※

次の経路の場合，高速経路切替を適用しません。

1. コンフィグレーションコマンド ip route または ipv6 route のパラメータとして次を指定した場合
   - reject
   - noinstall

2. 送信先インタフェースが次の場合
   ・ループバックインタフェース
   ・Null インタフェース
   ・マネージメントポート

13.11.2　使用上の注意事項

第 2 優先経路のネクストホップが ARP または NDP によってアドレス解決できていない場合，その経路に対する高速経路切替は適用されません。

第 2 優先経路が OSPF，OSPFv3，BGP4，BGP4+などのルーティングプロトコルを使用して学習した経路の場合は，隣接ルータからの定常的な制御パケットのトラフィックがあるため，経路のネクストホップは通常，ARP または NDP によって動的にアドレス解決された状態にあります。しかし，自ルータとの間でトラフィックが発生しない隣接ルータをネクストホップとするスタティック経路などに関しては，ネクストホップが動的にアドレス解決されないため，スタティック ARP またはスタティック NDP の設定などの措置が必要となります。

なお，内部生成経路は第 2 優先経路として使用しません。

13.12　VRF の解説

VRF はルーティング空間を論理的に分割する技術です。一つの装置内にルーティングテーブルの複数のインスタンスを保持して，各ルーティングテーブルに従って同時に転送できます。

VRF は IP アドレス空間を分離するため，各 VRF インスタンスは同じ IP アドレスを重複して使用できます。また，ルーティングプロトコルは VRF インスタンス単位に独立して動作します。

13.12.1　サポート範囲

VRF でサポートするルーティングプロトコルの機能を次の表に示します。

表 13-16　VRF でサポートする機能

機能		サポート
スタティックルーティング		○
ダイナミックルーティング	RIP-1	○
	RIP-2	○
	RIPng	○
	OSPF	○
	OSPFv3	○
	BGP4	○
	BGP4+	○
マルチパス／ロードバランス		○※
経路集約		○
ユニキャストルーティング高可用機能		○
高速経路切替機能		○
経路数の制限		○
エクストラネット	VRF 間の経路交換	○
	VRF 間にわたるスタティックルーティング	○

（凡例）　○：サポートする

注※　VRF 間にわたるマルチパスはサポートしません。

13.12.2　経路数の制限

VRF 単位で，収容する経路数を制限できます。収容経路数には，次の経路を含みます。

- スタティック ARP
- IPv4 内部生成経路（グローバルネットワークの場合：5 経路，VRF の場合：4 経路）
- スタティック NDP
- IPv6 内部生成経路（グローバルネットワークの場合：2 経路，VRF の場合：4 経路）

- IPv6 リンクローカル経路（ネットワーク経路と自インタフェースのアドレスの 2 経路）

(1)　経路追加の抑止

VRF ごとの経路数が指定した最大経路数を超えた場合，その後新たに学習した経路のフォワーディングテーブルへの追加を抑止します。

追加を抑止した経路はルーティングテーブル中に保持して，追加された経路が削除されてフォワーディングテーブルに空きができた時点で順次追加します。

(2)　警告のシステムメッセージ出力

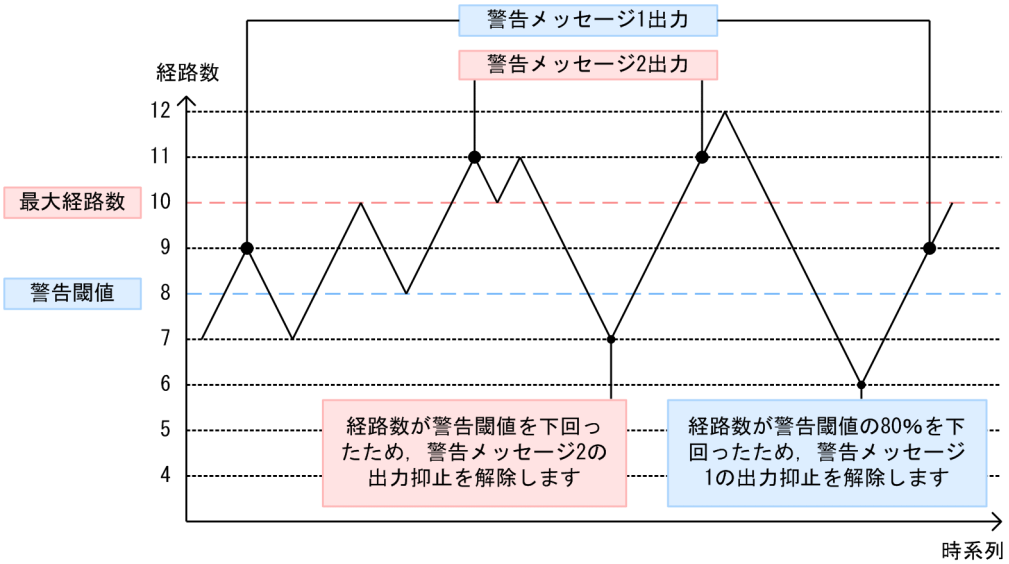
VRF ごとの経路数が指定した警告閾値および最大経路数を超過した場合，警告のシステムメッセージを出力します。

警告閾値を超過したときのメッセージ（警告メッセージ 1）の再出力は，経路数が警告閾値の 80%を下回るまで抑止されます。

また，最大経路数を超過したときのメッセージ（警告メッセージ 2）の再出力は，経路数が警告閾値を下回るまで抑止されます。

経路数とシステムメッセージ出力の関係を次の図に示します。

図 13-28　経路数とシステムメッセージ出力の関係



(3)　注意事項

コンフィグレーションで最大経路数を小さく変更した場合に，すでにフォワーディングテーブルに登録されている経路数が変更後の最大経路数を超過しているときは，フォワーディングテーブルに登録されている経路数を指定した最大経路数まですぐには減らしません。

フォワーディングテーブルに登録されている経路数を強制的に指定した最大経路数まで引き下げるときは，運用コマンド clear ip route または clear ipv6 route を実行してください。

13.12.3　エクストラネット

エクストラネットを実現するには次の二つの方法があります。

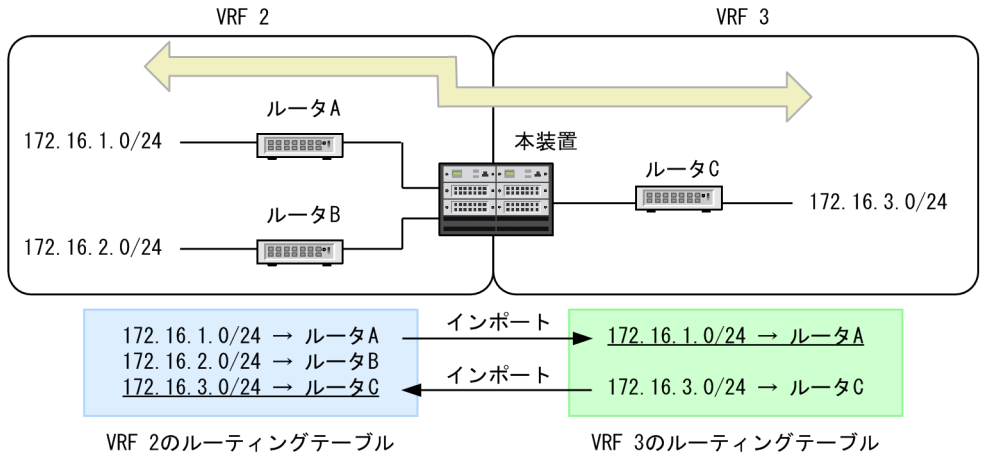
- VRF 間の経路交換
- VRF 間にわたるスタティックルーティング

ここでは，ルーティングテーブルを操作する VRF 間の経路交換，および VRF 間にわたるスタティックルーティングについて説明します。また，VRF 間でインポートできる経路について説明します。

(1)　VRF 間の経路交換

各 VRF が持つ経路情報を交換して，エクストラネットを実現します。VRF 間の経路交換を次の図に示します。

図 13-29　VRF 間の経路交換

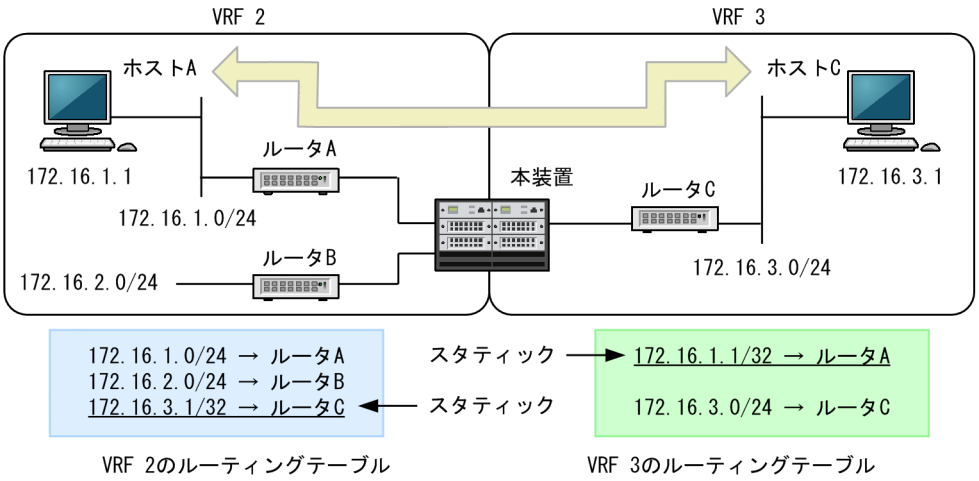


VRF 2 の経路（172.16.1.0/24）と VRF 3 の経路（172.16.3.0/24）を交換して，特定ネットワーク間で通信できます。

(2)　VRF 間にわたるスタティックルーティング

他 VRF のゲートウェイをネクストホップとするスタティック経路を生成して，エクストラネットを実現します。VRF 間にわたるスタティックルーティングを次の図に示します。

図 13-30　VRF 間にわたるスタティックルーティング



VRF 2 のルーティングテーブルにホスト C への経路を，VRF 3 のルーティングテーブルにホスト A への経路をスタティックで生成すると，特定ホスト間だけで通信できます。

(3)　VRF 間でインポートできる経路

他 VRF またはグローバルネットワークからインポートできる経路種別を次の表に示します。複数の経路種別に一致する場合は，一致したすべての経路種別がインポートできるときだけインポートできます。

表 13-17　他 VRF またはグローバルネットワークからインポートできる経路種別（IPv4）

経路種別	インポートの可否
非アクティブ経路	×
削除保留中の経路	×
エクストラネット用にインポートした経路	×
集約経路	○
ループバックインタフェースに設定した経路	○
イーサネットインタフェースの直結経路	○
イーサネットサブインタフェースの直結経路	○
ポートチャネルインタフェースの直結経路	○
ポートチャネルサブインタフェースの直結経路	○
マネージメントポートの直結経路	×
AUX インタフェースの直結経路	×
出力インタフェースがイーサネットインタフェースとなる経路	○
出力インタフェースがイーサネットサブインタフェースとなる経路	○
出力インタフェースがポートチャネルインタフェースとなる経路	○
出力インタフェースがポートチャネルサブインタフェースとなる経路	○

経路種別	インポートの可否
出力インタフェースがループバックインタフェースとなる経路	○
出力インタフェースが Null インタフェースとなる経路	○
出力インタフェースがマネージメントポートとなる経路	×
出力インタフェースが AUX インタフェースとなる経路	×

（凡例）　○：インポートできる　×：インポートできない

表 13-18　他 VRF またはグローバルネットワークからインポートできる経路種別（IPv6）

経路種別	インポートの可否
非アクティブ経路	×
削除保留中の経路	×
エクストラネット用にインポートした経路	×
集約経路	○
ループバックインタフェースに設定した経路	○
イーサネットインタフェースの直結経路（グローバルアドレス）	○
イーサネットインタフェースの直結経路（リンクローカルアドレス）	×
イーサネットサブインタフェースの直結経路（グローバルアドレス）	○
イーサネットサブインタフェースの直結経路（リンクローカルアドレス）	×
ポートチャネルインタフェースの直結経路（グローバルアドレス）	○
ポートチャネルインタフェースの直結経路（リンクローカルアドレス）	×
ポートチャネルサブインタフェースの直結経路（グローバルアドレス）	○
ポートチャネルサブインタフェースの直結経路（リンクローカルアドレス）	×
マネージメントポートの直結経路	×
出力インタフェースがイーサネットインタフェースとなる経路	○
出力インタフェースがイーサネットサブインタフェースとなる経路	○
出力インタフェースがポートチャネルインタフェースとなる経路	○
出力インタフェースがポートチャネルサブインタフェースとなる経路	○
出力インタフェースがループバックインタフェースとなる経路	○
出力インタフェースが Null インタフェースとなる経路	○
出力インタフェースがマネージメントポートとなる経路	×

（凡例）　○：インポートできる　×：インポートできない

13.13　VRF のコンフィグレーション

13.13.1　コンフィグレーションコマンド一覧

VRF のコンフィグレーションコマンド一覧を次の表に示します。

表 13-19　コンフィグレーションコマンド一覧

コマンド名	説明
import inter-vrf※1	他 VRF またはグローバルネットワークからの IPv4 の経路インポートをフィルタに従って制御します。
ipv6 import inter-vrf※1	他 VRF またはグローバルネットワークからの IPv6 の経路インポートをフィルタに従って制御します。
ipv6 maximum routes※1	VRF での IPv6 の最大経路数と警告のシステムメッセージ出力の閾値を設定します。
maximum routes※1	VRF での IPv4 の最大経路数と警告のシステムメッセージ出力の閾値を設定します。
vrf definition※1	VRF を設定します。
ip route※2	IPv4 スタティック経路を生成します。
ipv6 route※3	IPv6 スタティック経路を生成します。
match vrf※4	route-map に VRF によるフィルタ条件を設定します。
route-map※4	route-map を設定します。

注※1

「コンフィグレーションコマンドレファレンス Vol.3　5. VRF」を参照してください。

注※2

「コンフィグレーションコマンドレファレンス Vol.3　15. スタティックルーティング（IPv4)」を参照してください。

注※3

「コンフィグレーションコマンドレファレンス Vol.3　16. スタティックルーティング（IPv6)」を参照してください。

注※4

「コンフィグレーションコマンドレファレンス Vol.3　22. 経路フィルタリング」を参照してください。

13.13.2　最大経路数の設定

VRF の最大経路数と警告のシステムメッセージ出力の閾値を設定します。

[設定のポイント]

maximum routes コマンドを使用して, 最大経路数と警告のシステムメッセージ出力の閾値を設定します。IPv6 の最大経路数と警告のシステムメッセージ出力の閾値を設定するには，ipv6 maximum routes コマンドを使用してください。

[コマンドによる設定]

1. **(config)# vrf definition 2**

   VRF 2 の設定モードに移行します。

2. **(config-vrf)# maximum routes 1000 80**

   VRF 2 で収容できる IPv4 の最大経路数として 1000 を設定します。また，警告のシステムメッセージを出力する閾値を 80%に設定します。

13.13.3　エクストラネットの設定

IPv4 ネットワークでのエクストラネットの設定については，「14.2.7　VRF 間にわたるスタティック経路の設定」および「23.2.8　エクストラネット」を参照してください。

IPv6 ネットワークでのエクストラネットの設定については，「14.2.7　VRF 間にわたるスタティック経路の設定」および「23.3.8　エクストラネット」を参照してください。

13.14　VRF のオペレーション

13.14.1　運用コマンド一覧

VRF の運用コマンド一覧を次の表に示します。

表 13-20　運用コマンド一覧

コマンド名	説明
show ip route	ルーティングテーブルで保持する IPv4 経路情報を表示します。
show ip static	IPv4 スタティック経路に関する情報を表示します。
show ip vrf	VRF の IPv4 情報を表示します。
show ipv6 route	ルーティングテーブルで保持する IPv6 経路情報を表示します。
show ipv6 static	IPv6 スタティック経路に関する情報を表示します。
show ipv6 vrf	VRF の IPv6 情報を表示します。

13.14.2　最大経路数の確認

VRF のフォワーディングテーブルに登録されている現在の経路数と，収容可能な最大経路数を show ip vrf コマンドで表示します。VRF の IPv6 情報は show ipv6 vrf コマンドで確認してください。

図 13-31　show ip vrf コマンドの実行結果

```
> show ip vrf 2
Date 20XX/12/20 12:00:00 UTC
VRF              Routes        ARP
2                270/1000      7/50              <-1
>
```

1. 分子が現在の経路数，分母が最大経路数を表します。

図 13-32　show ip vrf detail コマンドの実行結果

```
> show ip vrf 2 detail
Date 20XX/12/20 12:00:00 UTC
VRF 2
  Maximum routes: 1000, Warn threshold: 80%, Current routes: 270     <-1
  Maximum ARP entries: 50, Current ARP entries: 7
  Import inter-vrf: -
Interface
Name           Local              Remote          Status
Eth1/1         192.168.10.1/24    192.168.10.255  Up
loopback2      10.10.10.1/32      10.10.10.1      Up
loopback2      127.0.0.1/8        127.0.0.1       Up
>
```

1. 最大経路数，警告のシステムメッセージ出力の閾値，現在の経路数の順に表示します。

13.14.3　エクストラネットの確認

エクストラネットの確認については，「23.4.6　エクストラネットの確認」を参照してください。

14 スタティックルーティング

この章では，IPv4 および IPv6 の経路を対象とするスタティックルーティングについて説明します。

14.1　解説

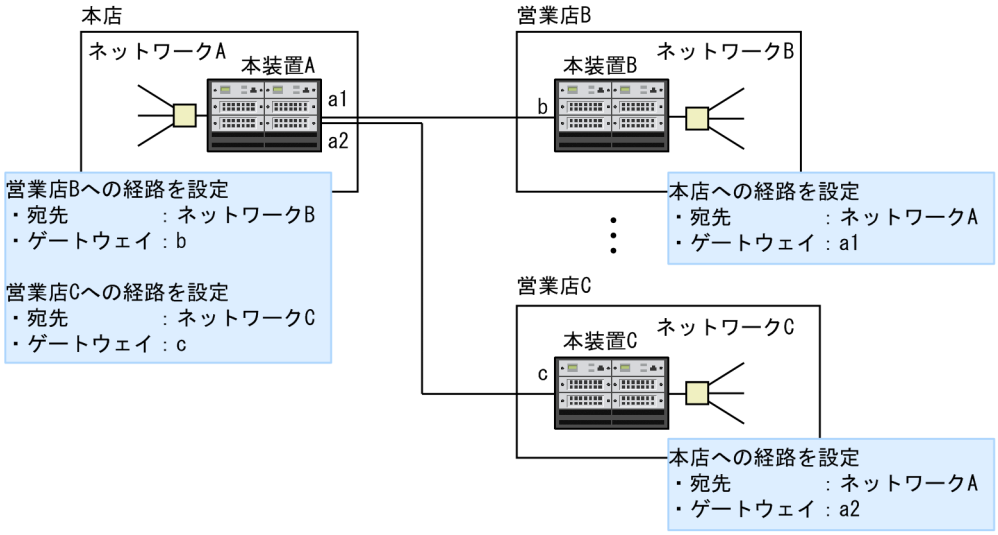
14.1.1　概要

スタティックルーティングはコンフィグレーションで設定した経路情報（スタティック経路）に従ってパケットを中継する機能です。

本装置のスタティック経路は，デフォルトルートを含む一つの宛先（サブ）ネットワークまたはホストごとに，複数の中継経路を設定できます。

スタティックルーティングのネットワーク構成例を次の図に示します。本店からは各営業店へのスタティック経路を設定して，営業店からは本店へのスタティック経路を設定します。この設定例では，営業店間は通信できません。

図 14-1　スタティックルーティングのネットワーク構成例



14.1.2　経路選択基準

スタティックルーティングでは，宛先ネットワークを同一とする複数のスタティック経路を，同一のディスタンス値を持つ単位でグループに分けて，そのうち，ディスタンス値の最も小さい経路グループの中から経路を選択します。

マルチパス数の最大が 1 より大きい場合は，次の表に示す優先順に従って，複数の経路が選択されてマルチパスを構成します。マルチパス数の最大が 1 の場合は，最も優先順が高い一つの経路を選択します。

マルチパス数の最大はデフォルトで 4 ですが，コンフィグレーションコマンド ip route static maximum-paths または ipv6 route static maximum-paths で変更できます。

表 14-1　経路選択の優先順位

優先順位	内容
高	weight 値が最も大きい経路を選択します。
低	ネクストホップアドレスが最も小さい経路を選択します。

14.1.3　スタティック経路の中継経路指定

中継経路（ゲートウェイ）には，直接接続された隣接ゲートウェイと，直接接続されない遠隔ゲートウェイを設定できます。隣接ゲートウェイは，該当するゲートウェイに対して，直接接続されたインタフェースの状態によって経路の生成および削除を制御します。遠隔ゲートウェイは，該当するゲートウェイへの経路の有無によって経路の生成および削除を制御します。ただし，遠隔ゲートウェイを使用しているスタティック経路を利用して，遠隔ゲートウェイを解決できません。

本装置のデフォルトのゲートウェイタイプは，遠隔ゲートウェイです。コンフィグレーションコマンド ip route または ipv6 route で指定するゲートウェイを隣接ゲートウェイとする場合は，noresolve パラメータを指定してください。

さらに，上記指定の経路について，2 種類の追加パラメータを選択できます。どちらもパケット転送をしないパラメータです。また，中継経路に Null インタフェースを指定した場合も，パケットを転送しません。

- noinstall パラメータ

  noinstall パラメータを指定したスタティック経路はパケット転送に使用しません。デフォルト経路など次善の経路がある場合は，その経路に従ってパケットを転送します。noinstall パラメータは，広告用のスタティック経路を設定したいが，パケット転送にはこのスタティック経路を使用しないでほかの経路に従ってほしい場合に使用します。

- reject パラメータ

  reject パラメータを指定したスタティック経路はリジェクト経路になります。その経路にマッチしたパケットは廃棄されます。このとき，ICMP（Unreachable）によって送信元へパケット廃棄を通知します。reject パラメータは，広告用のスタティック経路を設定したいが，このスタティック経路よりも優先する経路が本装置にないパケットを廃棄したい場合に使用します。また，特定のアドレスや宛先に対してパケットを転送したくない場合にも使用します。

- Null インタフェース

  スタティック経路の中継経路として，ゲートウェイを指定しないで Null インタフェースだけを指定すると，結果としてパケットが廃棄されます。また，reject パラメータによる廃棄と異なり，ICMP を送信しません。reject パラメータと同じ動作をさせたいが，廃棄による ICMP パケットを返したくない場合に使用します。Null インタフェースの詳細は「6　Null インタフェース」を参照してください。

14.1.4　動的監視機能

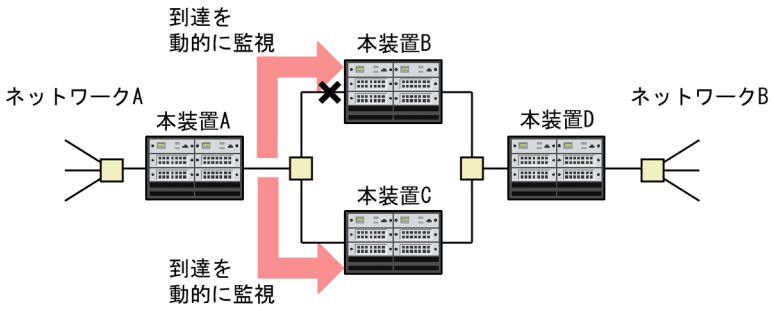
スタティック経路は，ゲートウェイと直接接続されたインタフェースの状態またはゲートウェイへの経路の有無によって，経路の生成および削除を制御します。したがって，経路が生成されている場合でも，該当するゲートウェイへの到達保証はありません。本装置は，生成されたスタティック経路のゲートウェイに対する，ICMP のエコー要求およびエコー応答メッセージを使用した周期的なポーリングによって，到達性を動的に監視する機能を持ちます。この機能を使用すると，「14.1.3　スタティック経路の中継経路指定」の経路生成および削除条件に加えて，該当するゲートウェイへの到達性が確保できている場合だけ，スタティック経路を生成するように制御できます。

また，該当するゲートウェイへ到達不可能から到達可能となった場合でも，その時点で経路を生成するのではなく，一定期間該当するゲートウェイへの到達性を監視して安定性が認められた場合に経路を再生成できます。

(1)　スタティック経路の動的監視による経路切り替え

スタティック経路の動的監視の例を次の図に示します。

図 14-2　スタティック経路の動的監視の例



この図では，本装置 A でネットワーク B へのスタティック経路が本装置 B 経由（優先），本装置 C（非優先）で設定されているものとします。動的監視をしていない状態で，本装置 A と本装置 B 間の本装置 B 側のインタフェースに障害が発生した場合，本装置 A 側のインタフェースは正常なため，本装置 B 経由のスタティック経路は削除されません。そのため，本装置 C 経由のスタティック経路へ切り替えられないで，本装置 A－ネットワーク B 間の通信が停止します。

動的監視をしている場合，本装置 A 側のインタフェースが正常であっても，動的監視機能によって本装置 B への到達不可を検知すると本装置 B 経由のスタティック経路を削除します。これによって，本装置 C 経由のスタティック経路へ切り替えられ，本装置 A－ネットワーク B 間の通信を確保できます。

(2)　スタティック経路の動的監視による経路の生成，削除および再生成タイミング

スタティック経路の動的監視による経路の生成，削除および再生成タイミングは次に示すコンフィグレーションコマンドの設定値に依存します。

IPv4

- ip route static poll-interval
- ip route static poll-multiplier

IPv6

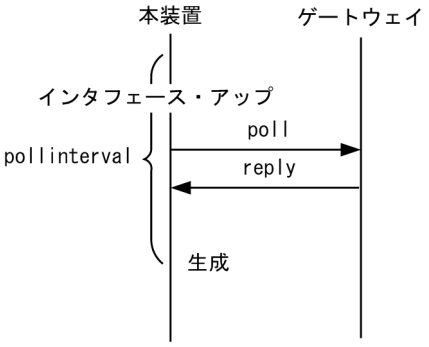
- ipv6 route static poll-interval
- ipv6 route static poll-multiplier

以降，ip route static poll-interval および ipv6 route static poll-interval の設定値を pollinterval，ip route static poll-multiplier および ipv6 route static poll-multiplier の設定値をそれぞれ invalidcount，restorecount と表します。

(a)　経路生成タイミング

インタフェースアップなどの経路生成要因を契機としてゲートウェイにポーリングします。該当するポーリングに対する応答を受信した場合，次のポーリング周期（pollinterval）に経路を生成します。スタティック経路の動的監視による経路生成の例を次の図に示します。

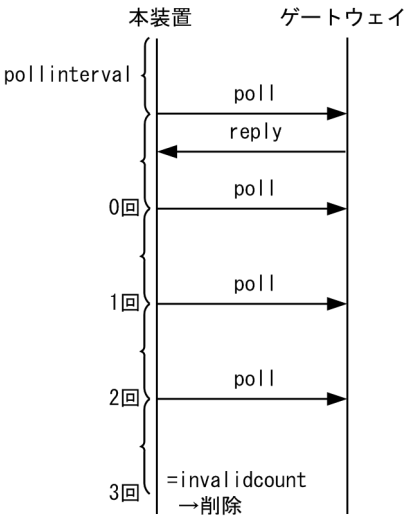
図 14-3　スタティック経路の動的監視による経路生成



(b)　経路削除タイミング

pollinterval 周期でのポーリングに対して，invalidcount 回数連続して応答がない場合に経路を削除します。invalidcount ＝ 3 の場合，ポーリングに対して 3 回連続して応答がなければ経路を削除します。なお，インタフェースダウンなどの経路生成要因がなくなった場合にも，ポーリングを使用しない（poll パラメータ未指定）スタティック経路と同様に，経路を削除します。スタティック経路の動的監視による経路削除の例を次の図に示します。

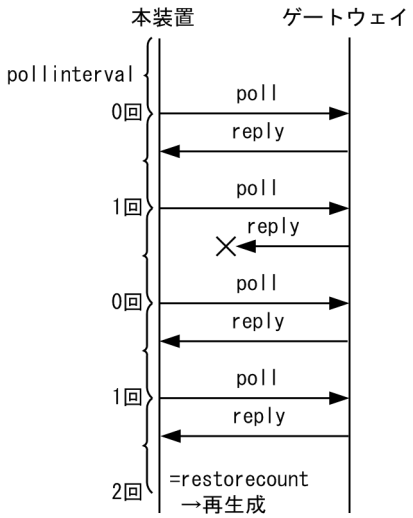
図 14-4　スタティック経路の動的監視による経路削除（invalidcount ＝ 3 の場合）



(c)　経路再生成タイミング

スタティック経路の動的監視によって削除された経路のゲートウェイへの pollinterval 周期のポーリングに対して，restorecount 回数連続して応答があった場合に経路を再生成します。restorecount ＝ 2 の場合，ポーリングに対して 2 回連続して応答があれば経路を再生成します。スタティック経路の動的監視による経路再生成の例を次の図に示します。

図 14-5　スタティック経路の動的監視による経路再生成（restorecount ＝ 2 の場合）



14.2　コンフィグレーション

14.2.1　コンフィグレーションコマンド一覧

スタティックルーティングのコンフィグレーションコマンド一覧を次の表に示します。

表 14-2　コンフィグレーションコマンド一覧

コマンド名	説明
ip route	IPv4 スタティック経路を生成します。
ip route static poll-interval	IPv4 スタティック経路のポーリング間隔時間を指定します。
ip route static poll-multiplier	IPv4 スタティック経路のポーリング回数，連続応答回数を指定します。
ipv6 route	IPv6 スタティック経路を生成します。
ipv6 route static poll-interval	IPv6 スタティック経路のポーリング間隔時間を指定します。
ipv6 route static poll-multiplier	IPv6 スタティック経路のポーリング回数，連続応答回数を指定します。

14.2.2　デフォルト経路の設定

スタティックのデフォルト経路を設定します。

(1)　IPv4 の場合

[設定のポイント]

スタティック経路の設定には ip route コマンドを使用します。宛先アドレスに 0.0.0.0，マスクに 0.0.0.0 を指定することによって，デフォルト経路が設定されます。

[コマンドによる設定]

1. **(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.50**

   デフォルト経路のネクストホップとして，遠隔ゲートウェイ 10.1.1.50 を指定します。

(2)　IPv6 の場合

[設定のポイント]

スタティック経路の設定には ipv6 route コマンドを使用します。プレフィックスに::/0 を指定することによって，デフォルト経路が設定されます。

[コマンドによる設定]

1. **(config)# ipv6 route ::/0 2001:db8:1:1::2**

   デフォルト経路のネクストホップとして，遠隔ゲートウェイ 2001:db8:1:1::2 を指定します。

14.2.3　シングルパス経路の設定

シングルパスのスタティック経路を設定します。ディスタンス値によって，複数の経路の優先度を調整します。

(1)　IPv4 の場合

[設定のポイント]

代替経路として設定するスタティック経路には，優先経路より大きいディスタンス値を指定します。

[コマンドによる設定]

1. **(config)# ip route 192.168.1.0 255.255.255.0 10.1.1.100 100**

   スタティック経路 192.168.1.0/24 のネクストホップとして，遠隔ゲートウェイ 10.1.1.100 を指定します。ディスタンス値として 100 を指定します。

2. **(config)# ip route 192.168.1.0 255.255.255.0 172.16.1.100 200 noresolve**

   スタティック経路 192.168.1.0/24 のネクストホップとして，隣接ゲートウェイ 172.16.1.100 を指定します。また，ディスタンス値として 200 を指定します。この経路はゲートウェイ 10.1.1.100 宛ての経路が無効となった場合の代替経路となります。

(2)　IPv6 の場合

[設定のポイント]

代替経路として設定するスタティック経路には，優先経路より大きいディスタンス値を指定します。

[コマンドによる設定]

1. **(config)# ipv6 route 2001:db8:ffff:1::/64 2001:db8:1:2::2 100**

   スタティック経路 2001:db8:ffff:1::/64 のネクストホップとして，遠隔ゲートウェイ 2001:db8:1:2::2 を指定します。ディスタンス値として 100 を指定します。

2. **(config)# ipv6 route 2001:db8:ffff:1::/64 fe80::2 gigabitethernet 1/1 200 noresolve**

   スタティック経路 2001:db8:ffff:1::/64 のネクストホップとして，隣接ゲートウェイにポート 1/1 のリンクローカルアドレス fe80::2 を指定します。また，ディスタンス値として 200 を指定します。この経路はゲートウェイ 2001:db8:1:2::2 宛ての経路が無効となった場合の代替経路となります。

14.2.4　マルチパス経路の設定

マルチパスのスタティック経路を設定します。

(1)　IPv4 の場合

[設定のポイント]

ip route コマンドによる同一宛先の複数スタティック経路の設定で，ディスタンス値の指定を省略するか，または同一のディスタンス値を指定すると，マルチパスを構成できます。

[コマンドによる設定]

1. **(config)# ip route 192.168.2.0 255.255.255.0 172.16.1.100 noresolve**

   スタティック経路 192.168.2.0/24 のネクストホップとして，隣接ゲートウェイ 172.16.1.100 を指定します。

2. **(config)# ip route 192.168.2.0 255.255.255.0 172.16.2.100 noresolve**

   スタティック経路 192.168.2.0/24 のネクストホップとして，隣接ゲートウェイ 172.16.2.100 を指定します。スタティック経路 192.168.2.0/24 は隣接ゲートウェイ 172.16.1.100 と 172.16.2.100 の間でマルチパスを構成します。

(2)　IPv6 の場合

[設定のポイント]

ipv6 route コマンドによる同一宛先の複数スタティック経路の設定で，ディスタンス値の指定を省略するか，または同一のディスタンス値を指定すると，マルチパスを構成できます。

[コマンドによる設定]

1. **(config)# ipv6 route 2001:db8:ffff:2::/64 2001:db8:2:1::2 noresolve**
   スタティック経路 2001:db8:ffff:2::/64 のネクストホップとして，隣接ゲートウェイ 2001:db8:2:1::2 を指定します。
2. **(config)# ipv6 route 2001:db8:ffff:2::/64 2001:db8:2:2::2 noresolve**
   スタティック経路 2001:db8:ffff:2::/64 のネクストホップとして，隣接ゲートウェイ 2001:db8:2:2::2 を指定します。スタティック経路 2001:db8:ffff:2::/64 は隣接ゲートウェイ 2001:db8:2:1::2 と 2001:db8:2:2::2 の間でマルチパスを構成します。

14.2.5　動的監視機能の適用

監視対象のゲートウェイに対するポーリング間隔と，経路削除および生成のタイミングを調整したあとで，スタティック経路に動的監視機能を適用します。

(1)　IPv4 の場合

[設定のポイント]

ポーリング間隔と回数の設定には ip route static poll-interval コマンドおよび ip route static poll-multiplier コマンドを使用します。スタティック経路に動的監視機能を適用する場合は，ip route コマンドで poll パラメータを指定します。

[コマンドによる設定]

1. **(config)# ip route static poll-interval 10**
   動的監視機能のポーリング間隔として，10 秒を指定します。
2. **(config)# ip route static poll-multiplier 4 2**
   動的監視機能の連続失敗回数（invalidcount）として 4 回，連続応答回数（restorecount）として 2 回を指定します。
3. **(config)# ip route 192.168.3.0 255.255.255.0 10.2.1.100 poll**
   (config)# ip route 192.168.4.0 255.255.255.0 10.2.1.101 poll
   スタティック経路 192.168.3.0/24 と 192.168.4.0/24 に動的監視機能を適用します。

(2)　IPv6 の場合

[設定のポイント]

ポーリング間隔と回数の設定には ipv6 route static poll-interval コマンドおよび ipv6 route static poll-multiplier コマンドを使用します。スタティック経路に動的監視機能を適用する場合は，ipv6 route コマンドで poll パラメータを指定します。

[コマンドによる設定]

1. **(config)# ipv6 route static poll-interval 10**
   動的監視機能のポーリング間隔として，10 秒を指定します。

2. **(config)# ipv6 route static poll-multiplier 4 2**

   動的監視機能の連続失敗回数（invalidcount）として 4 回，連続応答回数（restorecount）として 2 回を指定します。

3. **(config)# ipv6 route 2001:db8:ffff:3::/64 2001:db8:3:1::2 poll**

   (config)# ipv6 route 2001:db8:ffff:4::/64 2001:db8:3:1::3 poll

   スタティック経路 2001:db8:ffff:3::/64 と 2001:db8:ffff:4::/64 に動的監視機能を適用します。

14.2.6　VRF でのスタティック経路の設定

VRF でスタティック経路を設定します。

(1)　IPv4 の場合

[設定のポイント]

ip route コマンドの vrf パラメータで，VRF を指定します。

[コマンドによる設定]

1. **(config)# ip route vrf 2 172.16.2.0 255.255.255.0 10.2.1.100 noresolve**

   VRF 2 にスタティック経路 172.16.2.0/24 を生成します。ネクストホップとして，隣接ゲートウェイ 10.2.1.100 を指定します。

(2)　IPv6 の場合

[設定のポイント]

ipv6 route コマンドの vrf パラメータで，VRF を指定します。

[コマンドによる設定]

1. **(config)# ipv6 route vrf 2 2001:db8:ffff:20::/64 2001:db8:20:1::2 noresolve**

   VRF 2 にスタティック経路 2001:db8:ffff:20::/64 を生成します。ネクストホップとして，隣接ゲートウェイ 2001:db8:20:1::2 を指定します。

14.2.7　VRF 間にわたるスタティック経路の設定

VRF 間にわたるスタティック経路を設定して，特定ホスト間のエクストラネットを実現します。

(1)　IPv4 の場合

[設定のポイント]

ip route コマンドのネクストホップアドレスに続く vrf パラメータで，相手 VRF を指定します。

[コマンドによる設定]

1. **(config)# ip route vrf 2 172.16.3.1 255.255.255.255 10.3.1.100 vrf 3 noresolve**

   VRF 2 にスタティック経路 172.16.3.1/32 を生成します。ネクストホップとして VRF 3 の隣接ゲートウェイ 10.3.1.100 を指定します。

2. **(config)# ip route vrf 3 172.16.1.1 255.255.255.255 10.1.1.100 vrf 2 noresolve**

   VRF 3 にスタティック経路 172.16.1.1/32 を生成します。ネクストホップとして VRF 2 の隣接ゲートウェイ 10.1.1.100 を指定します。

(2)　IPv6 の場合

[設定のポイント]

ipv6 route コマンドのネクストホップアドレスに続く vrf パラメータで，相手 VRF を指定します。

[コマンドによる設定]

1. **(config)# ipv6 route vrf 2 2001:db8:ffff:31::1/128 2001:db8:30:1::2 vrf 3 noresolve**
   VRF 2 にスタティック経路 2001:db8:ffff:31::1/128 を生成します。ネクストホップとして VRF 3 の隣接ゲートウェイ 2001:db8:30:1::2 を指定します。
2. **(config)# ipv6 route vrf 3 2001:db8:ffff:21::1/128 2001:db8:20:1::2 vrf 2 noresolve**
   VRF 3 にスタティック経路 2001:db8:ffff:21::1/128 を生成します。ネクストホップとして VRF 2 の隣接ゲートウェイ 2001:db8:20:1::2 を指定します。

14.2.8　IPv6 リンクローカルアドレスをネクストホップとした VRF 間にわたるスタティック経路の設定

IPv6 リンクローカルアドレスをネクストホップアドレスとした VRF 間にわたるスタティック経路を設定して，特定ホスト間のエクストラネットを実現します。

[設定のポイント]

ipv6 route コマンドのネクストホップアドレスに IPv6 リンクローカルアドレスを指定して，続くインタフェースパラメータでインタフェースを指定します。スタティック経路の VRF とインタフェースの VRF が異なる場合に，VRF 間にわたるスタティック経路が生成されます。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/2**
   (config-if)# vrf forwarding 2
   (config-if)# ipv6 enable
   (config-if)# ipv6 address 2001:db8:ffff:ffff::1/64
   ポート 1/2 に VRF 2 と IPv6 アドレスを指定します。
2. **(config)# interface gigabitethernet 1/3**
   (config-if)# vrf forwarding 3
   (config-if)# ipv6 enable
   (config-if)# ipv6 address 2001:db8:ffff:fff0::1/64
   ポート 1/3 に VRF 3 と IPv6 アドレスを設定します。
3. **(config)# ipv6 route vrf 2 2001:db8:ffff:41::1/128 fe80::3 gigabitethernet 1/3 noresolve**
   VRF 2 にスタティック経路 2001:db8:ffff:41::1/128 を生成します。ネクストホップとして隣接ゲートウェイにポート 1/3 のリンクローカルアドレス fe80::3 を指定します。
4. **(config)# ipv6 route vrf 3 2001:db8:ffff:51::1/128 fe80::4 gigabitethernet 1/2 noresolve**
   VRF 3 にスタティック経路 2001:db8:ffff:51::1/128 を生成します。ネクストホップとして隣接ゲートウェイにポート 1/2 のリンクローカルアドレス fe80::4 を指定します。

14.3　オペレーション

14.3.1　運用コマンド一覧

IPv4 スタティックルーティングの運用コマンド一覧を次の表に示します。

表 14-3　運用コマンド一覧（IPv4）

コマンド名	説明
show ip route	ルーティングテーブルで保持する経路情報を表示します。
clear ip route	H/W の IPv4 フォワーディングエントリをクリアして再登録します。
show ip static	IPv4 スタティック経路に関する情報を表示します。
clear ip static-gateway	IPv4 スタティック経路の動的監視によって無効とされた経路のゲートウェイに対してポーリングをして，応答がある場合は経路を生成します。
show ip vrf	VRF の IPv4 情報を表示します。
show ip interface ipv4-unicast	ユニキャストルーティングプログラムが認識している本装置の IPv4 インタフェース情報を表示します。

IPv6 スタティックルーティングの運用コマンド一覧を次の表に示します。

表 14-4　運用コマンド一覧（IPv6）

コマンド名	説明
show ipv6 route	ルーティングテーブルで保持する経路情報を表示します。
clear ipv6 route	H/W の IPv6 フォワーディングエントリをクリアして再登録します。
show ipv6 static	IPv6 スタティック経路に関する情報を表示します。
clear ipv6 static-gateway	IPv6 スタティック経路の動的監視によって無効とされた経路のゲートウェイに対してポーリングをして，応答がある場合は経路を生成します。
show ipv6 vrf	VRF の IPv6 情報を表示します。
show ipv6 interface ipv6-unicast	ユニキャストルーティングプログラムが認識している本装置の IPv6 インタフェース情報を表示します。

14.3.2　経路情報の確認

スタティック経路に関する情報は，IPv4 の場合 show ip static コマンドで，IPv6 の場合 show ipv6 static コマンドで，route パラメータを指定して確認します。

図 14-6　show ip static route の実行結果

```
> show ip static route
Date 20XX/03/14 12:00:00 UTC
Status Codes: * valid, > active, r RIB failure
   Destination        Next Hop       Distance Weight Status      Flag
*> 0.0.0.0/0          10.1.1.50       2        0      IFdown      -
*> 192.168.1/24       10.1.1.100      100      0      Act         -
*  192.168.1/24       172.16.1.100    200      0      Act         NoResolve
*> 192.168.2/24       172.16.1.100    2        0      Act         NoResolve
                      172.16.2.100    2        0      Act         NoResolve
```

```
*> 192.168.3/24       10.2.1.100      2       0       Act Reach   Poll
   192.168.4/24       10.2.1.101      2       0       UnReach     Poll
```

[確認のポイント]

- ルーティングテーブルに設定されている経路は，行先頭の Status Codes に「*」および「>」が表示されます。
- ルーティングテーブルに設定されていない代替経路は，Status Codes に「>」が表示されませんが，経路として有効な場合には「*」が表示されます。
- Status Codes に「*」および「>」が表示されていない無効経路は，Status に障害要因が表示されます。「IFdown」は，インタフェース障害が要因で経路が無効となっていることを示します。また，「UnReach」は，動的監視で到達性が確認されていないことを示します。

14.3.3　ゲートウェイ情報の確認

スタティック経路のゲートウェイに関する情報は，IPv4 の場合 show ip static コマンドで，IPv6 の場合 show ipv6 static コマンドで，gateway パラメータを指定して確認します。

図 14-7　show ip static gateway の実行結果

```
> show ip static gateway
Date 20XX/03/14 12:00:00 UTC
Gateway         Status  Success     Failure     Transition
10.1.1.50       IFdown  -           -           -
10.1.1.100      -       -           -           -
10.2.1.100      Reach   -           0/4         13m 39s
10.2.1.101      UnReach 1/2         -           21s
172.16.1.100    -       -           -           -
172.16.2.100    -       -           -           -
```

[確認のポイント]

- 動的監視をしているゲートウェイは，Status に到達性状態が表示されます。到達性が確認されている場合は「Reach」，到達性が確認されていない場合は「UnReach」が表示されます。
- 動的監視で到達性が確認されていない場合（Status に「UnReach」が表示される場合）は，Success カウンタでゲートウェイの監視状況を確認してください。この実行結果では，ゲートウェイ 10.2.1.101 の Success カウンタは「1/2」と表示されています。これは，連続 2 回の応答で到達性が確認される設定で，現在連続 1 回まで成功していることを示しています。

15 RIP

この章では，IPv4 のルーティングプロトコルの RIP について説明します。

15.1 解説

15.1.1 概要

RIP（Routing Information Protocol）は，ネットワークで接続したルータ間で使用するルーティングプロトコルです。各ルータは RIP を使用して自ルータから到達できるネットワークとそのネットワークへのホップ数（メトリック）を通知し合うことによって経路情報を生成します。

本装置は RIP のバージョン 1 とバージョン 2 をサポートしています。バージョン 0 のメッセージを受信した場合は，破棄します。バージョン 3 以上のメッセージを受信した場合は，バージョン 2 のメッセージとして扱います。

RIP の機能を次の表に示します。

表 15-1 RIP の機能

機能	RIP
triggered update	○
スプリットホライズン	○
ルートポイズニング	○
ポイズンリバース	×
ホールドダウン	×
RIP 広告経路自動集約	○
ルートタグ	○
指定ネクストホップの取り込み	○
平文パスワード認証	○
暗号認証（Keyed-MD5）	○

（凡例） ○：取り扱う ×：取り扱わない

(1) メッセージの種類

RIP で使用するメッセージの種類にはリクエストとレスポンスの 2 種類があります。ルータがほかのルータに経路情報を要求する場合にはリクエストを使用して，ほかのルータからのリクエストに応答する場合，および定期的またはトポロジ変化時に自分の経路情報をほかのルータに通知する場合にレスポンスを使用します。

(2) 運用時の処理

本装置の立ち上げ時，本装置はリクエストメッセージをすべての隣接ルータに送信して，隣接ルータが持つすべての経路情報を通知するように要求します。運用に入ると，本装置は次の三つの要因でレスポンスを送信します。

- 隣接ルータからリクエストを受信した場合で，リクエストの内容によって自分が持つ経路情報をリクエストの送信元にレスポンスで応答します。

- 定期的に行う経路情報の通知です。本装置は 30 秒ごとに自分が持つ経路情報をすべて含むレスポンスを送信して，隣接ルータに通知します。
- 経路の変化を検出したときに行う経路情報の通知です。本装置は経路の変化を検出した場合，変化した経路に関連する経路情報を含むレスポンスを送信して，隣接ルータに通知します。

各隣接ルータが送信したレスポンスを受信して，経路の変更を検出した場合は自分が持つ経路情報を更新します。レスポンスは隣接ルータとの送信の確認にも使用します。180 秒以上レスポンスを応答しないルータに対しては通信不可能と判断して，代替ルートがあるときはルーティングテーブルをその代替ルートに更新します。代替ルートがないときはルートを削除します。

(3) ルーティングループの抑止処理

本装置は中継経路のループを抑止するために**スプリットホライズン**を使用します。スプリットホライズンとは，受信した情報を受け取ったインタフェースには送信しない処理のことです。

15.1.2 経路選択基準

本装置は，各プロトコルで学習した同じ宛先への経路情報をそれぞれ独立した経路選択手順に従って一つの最良の経路を選択します。同じ宛先への経路情報が各プロトコルで生成されることによって複数存在する場合，それぞれの経路情報のディスタンス値が比較されて優先度の最も高い経路情報が有効になります。

RIP では，自プロトコルを使用し学習した同じ宛先への広告元の異なる複数の経路情報から，経路選択の優先順位に従って一つの最良の経路を選択します。経路選択の条件を，優先順位が高い順に次に示します。

1. メトリック値が最も小さい経路を選択します。
2. エージングタイムがタイマ値の 1/2 秒以内の経路を選択します（メトリック値が同じ場合）。
3. ネクストホップアドレスが最も小さい経路を選択します。
4. 経路情報に含まれるネクストホップアドレスと経路情報の送信元ゲートウェイアドレスが一致する経路を選択します。
   この条件は，同一ネットワーク内にある異なる隣接装置から，経路情報に含まれるネクストホップアドレスが同一となる経路情報を学習する場合に適用されます。
5. そのほかの場合，新しく学習した経路を無視します。

その後，同じ宛先への経路情報が各プロトコル（OSPF，BGP4，スタティック）で学習した経路によって複数存在する場合は，それぞれの経路情報のディスタンス値が比較され，優先度の最も高い経路情報をルーティングテーブルに設定します。

(1) 第 2 優先経路の生成

コンフィグレーションコマンド generate-secondary-route を指定することによって，異なる隣接装置から学習した同一宛先への経路情報を二つ（第 1 優先経路と第 2 優先経路）まで生成します。第 2 優先経路を生成する条件を次の表に示します。

表 15-2 第 2 優先経路の生成条件

条件		第 2 優先経路の生成
コンフィグレーションコマンド generate-secondary-route の指定	ディスタンス値	
×	−	生成しない

条件		第 2 優先経路の生成
コンフィグレーションコマンド generate-secondary-route の指定	ディスタンス値	
○	第 1 優先経路と第 2 優先経路の値が異なる	生成しない
○	第 1 優先経路と第 2 優先経路の値が同じ	生成する

（凡例） ○：コンフィグレーションあり　×：コンフィグレーションなし　－：該当なし

第 2 優先経路の生成を指定した場合，経路選択の優先順位に従って同じ宛先への経路情報の優先度を決定します。第 2 優先経路の経路選択の条件を，優先順位が高い順に次に示します。ただし，ネクストホップアドレスが同じ場合は第 1 優先経路だけを生成します。

1. メトリック値が小さい経路を選択します。
2. エージングタイムがタイマ値の 1/2 秒以内の経路を選択します（メトリック値が同じ場合）。
3. ネクストホップアドレスが小さい経路を選択します。
   なお，第 2 優先経路が登録されている状態で新経路を学習した場合，この条件は適用されません。
4. 経路情報に含まれるネクストホップアドレスと経路情報の送信元ゲートウェイアドレスが一致する経路を選択します。
   この条件は，同一ネットワーク内にある異なる隣接装置から，経路情報に含まれるネクストホップアドレスが同一となる経路情報を学習する場合に適用されます。
5. 今まで第 1 優先だった経路を選択します。
6. そのほかの場合，新しく学習した経路を無視します。

15.1.3 経路情報の広告

(1) 広告対象経路

(a) 学習プロトコル

RIP では，広告経路フィルタを設定していない場合，学習した RIP 経路および RIP が動作するネットワーク範囲内の直結経路を広告します。広告経路フィルタを設定した場合は，広告経路フィルタの動作に従って広告動作を行います。RIP で広告対象の学習プロトコルを次の表に示します。

表 15-3 広告対象の学習プロトコル

学習プロトコル		広告経路フィルタの設定がない場合の広告動作	広告メトリックの適用順序※5
直結経路※1	RIP が動作するネットワークの範囲内	広告します	1. 広告経路フィルタの指定値 2. デフォルト値（metric 値：1）
	RIP が動作するネットワークの範囲外	広告しません	
集約経路		広告しません	
スタティック経路		広告しません	1. 広告経路フィルタの指定値

学習プロトコル	広告経路フィルタの設定がない場合の広告動作	広告メトリックの適用順序※5
		2. default-metric の指定値 3. デフォルト値（metric 値：1）
RIP※2	広告します	1. 広告経路フィルタの指定値 2. ルーティングテーブルの値
OSPF	広告しません	1. 広告経路フィルタの指定値 2. inherit-metric の設定がある場合は，ルーティングテーブルの値※3 3. default-metric の指定値※4
BGP	広告しません	
他 VRF またはグローバルネットワークからインポートした経路	広告しません	

注※1

セカンダリアドレスも広告対象となります。

注※2

スプリットホライズンが適用されます。

注※3

ルーティングテーブルのメトリック値が 16 以上の場合は，経路を広告しません。

注※4

広告経路フィルタ，inherit-metric または default-metric によるメトリックの指定がない場合は，経路を広告しません。

注※5

metric-offset out コマンドの設定がある場合は，選択したメトリック値に対してさらに metric-offset out コマンドの指定値を加算します。加算した結果，メトリック値が 16 以上となった場合は，経路を広告しません。

(b) アドレス種別

RIP で広告対象のアドレス種別を次の表に示します。

表 15-4 広告対象のアドレス種別

アドレス種別	定義	例	広告可否	
			RIP-1	RIP-2
デフォルト経路情報	すべてのネットワーク宛ての経路情報	0.0.0.0/0	○	○
ナチュラルマスク経路情報	IP アドレスのクラスに対応したネットワークマスクの経路情報 （クラス A：8 ビット） （クラス B：16 ビット） （クラス C：24 ビット）	172.16.0.0/16 • クラス B • ネットマスク：16 ビット（255.255.0.0）	○	○
サブネット経路情報	特定のサブネット宛ての経路情報	172.16.10.0/24 • クラス B • ネットマスク：24 ビット（255.255.255.0）	△※1※2	○※2

アドレス種別	定義	例	広告可否	
			RIP-1	RIP-2
スーパーネット経路情報	複数のネットワークを包含する経路情報	172.0.0.0/8 • クラス B • ネットマスク：8 ビット（255.0.0.0）	×	○
ホスト経路情報	特定のホスト宛ての経路情報	172.16.10.1/32 • ネットマスク：32 ビット（255.255.255.255）	○	○

（凡例） ○：広告可能 ×：広告不可 △：一部広告可

注※1

RIP-1 では広告できるサブネット経路に制約があります。詳細は「15.1.5 RIP-1 (1) RIP-1 での経路情報の広告」を参照してください。

注※2

コンフィグレーションコマンド auto-summary が設定されている場合は，広告サブネット経路情報を自動的に一つのナチュラルマスク経路情報として集約して広告します。詳細は「(4) RIP 広告経路の自動集約」を参照してください。

(2) 経路情報の広告先

RIP では，コンフィグレーションコマンド network によって指定したネットワーク上のすべての隣接ルータに対して，経路情報を広告します。ただし，サブネットマスクが 31 ビットのネットワークへの経路情報の広告は未サポートです。RIP の広告先には，サブネットマスクが 31 ビットに設定されているインタフェースアドレスが含まれないようにする必要があります。このため，コンフィグレーションコマンド network で指定するネットワーク範囲に，該当するアドレスを含まないように設定してください。

RIP での経路情報の広告先を次の表に示します。

表 15-5 経路情報の広告先

広告先	宛先アドレス
RIP が動作するネットワーク※1※2	マルチキャストアドレス（RIP-2）またはサブネットブロードキャストアドレス（RIP-1）
特定の隣接ルータ※3	ユニキャストアドレス

注※1 passive-interface の指定があるインタフェースに対しては，レスポンスパケットの送信が抑止されます。

注※2 セカンダリアドレスも対象です。

注※3 隣接ルータは RIP が動作するネットワークに含まれている必要があります。

(3) 経路情報の広告タイミング

RIP による経路広告タイミングは，次の表に示す機能が関係します。

表 15-6 経路広告タイミング

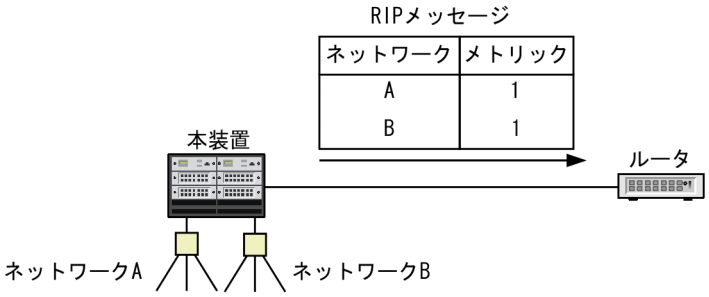
機能	内容
周期的な経路情報広告	自装置が持つ経路情報を隣接ルータに周期的に通知します。

機能	内容
triggered update	自装置の経路情報に変更があったときに定期的な広告を待たないで通知します。
隣接ルータからのリクエストに対する応答	リクエストパケットを送信した隣接ルータに対して通知します。
ルートポイズニング	経路情報が削除されたことを隣接ルータに一定時間通知します。

(a)　周期的な経路情報広告

RIP は自装置が持つ経路情報を周期的に隣接のルータに広告します。周期的な経路情報広告を次の図に示します。

図 15-1　周期的な経路情報広告

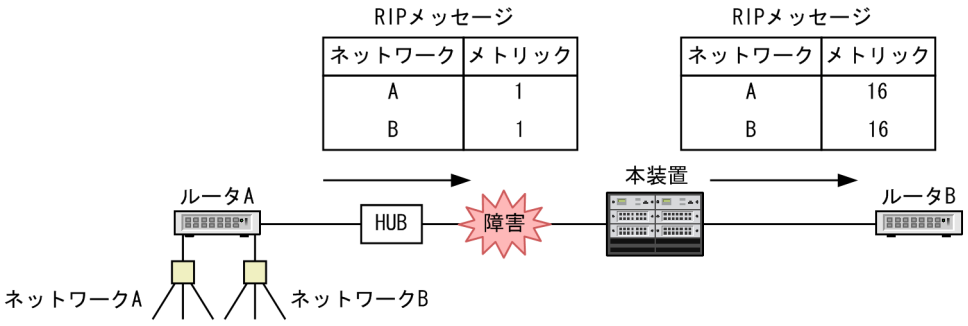


本装置はネットワーク A および B に関する経路情報を 30 秒周期（周期広告タイマ）でルータに広告します。

(b)　triggered update

自装置の経路情報の変化を認識したときに定期的な配布周期を待たないで経路情報を配布します。triggered update による経路情報の広告を次の図に示します。

図 15-2　triggered update による経路情報の広告

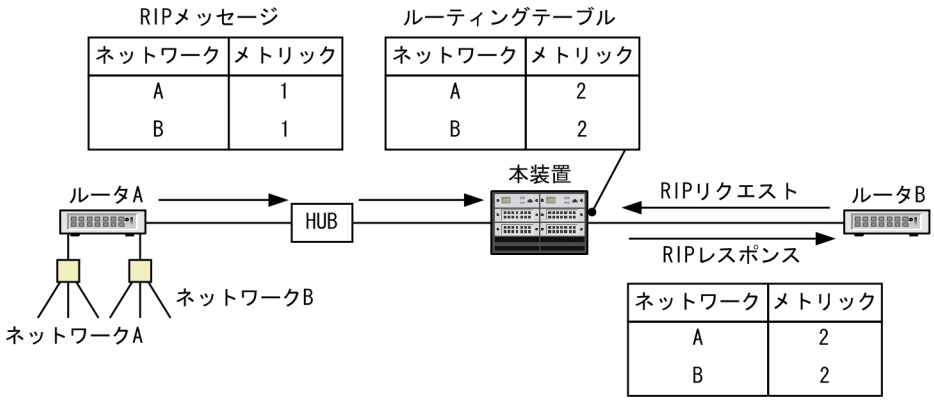


本装置は HUB と本装置間の障害を検出すると，ルーティングテーブルからネットワーク A および B の経路情報を削除します。同時に，ルータ B に対してネットワーク A および B の経路情報をメトリック 16（到達不可）で広告します。

(c)　リクエストパケットに対する応答

本装置はリクエストパケットを受信すると，リクエストパケットを送信した隣接ルータに対して経路情報を広告します。リクエストパケット受信による経路情報の広告を次の図に示します。

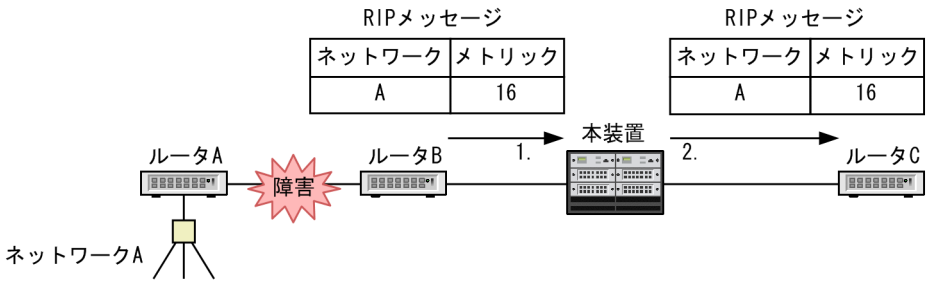
図 15-3　リクエストパケット受信による経路情報の広告



(d)　ルートポイズニング

到達できる状態から到達できない状態（メトリック 16 受信または，インタフェース障害によって該当するインタフェースから学習した経路を削除）となった経路に対して，一定時間（60 秒：ガーベジコレクトタイマ）はメトリック 16（到達できない）で隣接ルータに広告します。ルートポイズニングを次の図に示します。

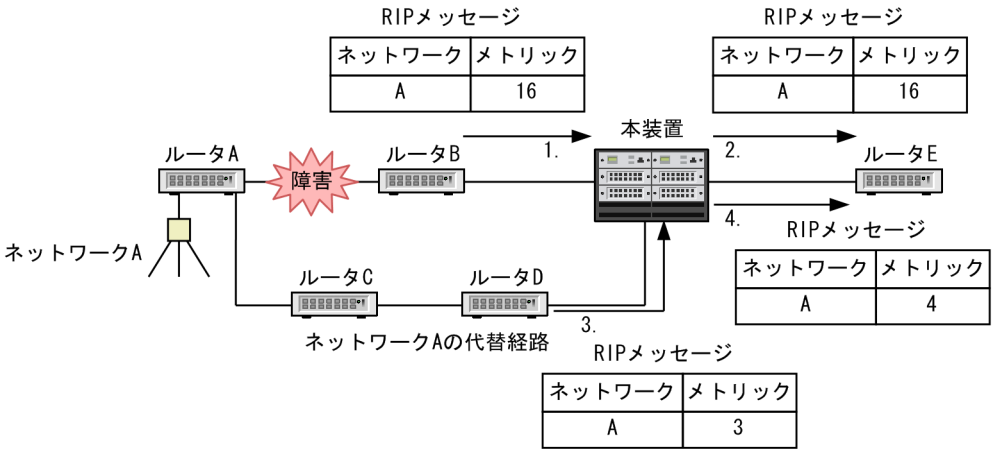
図 15-4　ルートポイズニング



1. 本装置はルータ A とルータ B 間の障害を検出すると，ルータ B からメトリック 16（到達不可）のネットワーク A の経路情報を受信して，ルーティングテーブルからネットワーク A の経路情報を削除します。
2. 1.を受信するとすぐに，本装置はルータ C にメトリック 16（到達不可）のネットワーク A の経路情報を広告します。代替経路が存在しない場合，本装置は該当経路をメトリック 16（到達不可）でルータ C に広告します。

ルートポイズニング期間中に，該当する宛先への新しい経路を再学習した場合は，新しい経路を広告します。ルートポイズニング期間中の再学習を次の図に示します。

図 15-5　ルートポイズニング期間中の再学習



1. 本装置はルータ A とルータ B 間の障害を検出すると，ルータ B からメトリック 16（到達不可）のネットワーク A の経路情報を受信して，ルーティングテーブルからネットワーク A の経路情報を削除します。
2. 同時に，本装置はルータ E にメトリック 16（到達不可）のネットワーク A の経路情報を広告します。
3. 本装置はルータ D からの周期広告でネットワーク A の経路情報を受信して，ルーティングテーブルに追加します。切り替え時間はルータ D の周期広告時間に依存します。
4. 本装置はルータ E に対して，ネットワーク A の経路情報を広告します。

(4)　RIP 広告経路の自動集約

RIP ではコンフィグレーションコマンド auto-summary を設定することで，隣接装置に対して広告する複数のサブネット経路情報を，自動的に一つのナチュラルマスク経路情報として集約して広告できます。このコンフィグレーションコマンドは RIP-1，RIP-2 共に有効となります。

広告経路の自動集約対象になるアドレス種別を次の表に示します。

表 15-7　広告経路の自動集約対象となるアドレス種別

アドレス種別	集約可否	
	RIP-1	RIP-2
デフォルト経路情報	×	×
ナチュラルマスク経路情報	×	×
サブネット経路情報	○※1	○※2
スーパーネット経路情報	×	×
ホスト経路情報	×	×

（凡例）○：集約可能　×：集約不可

注※1

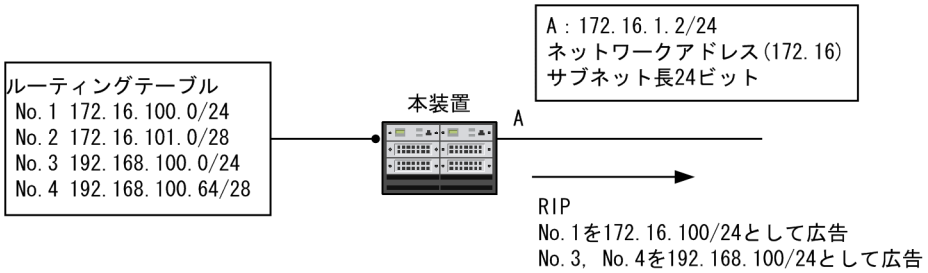
RIP-1 では広告経路情報のナチュラルネットワークと広告先インタフェースのナチュラルネットワークが同一であり，広告経路情報のマスク長と広告先インタフェースのマスク長が同一である場合は，自動集約をしないでサブネット経路情報として隣接装置に広告します。詳細は「図 15-6　RIP-1 使用時の広告経路自動集約」を参照してください。

注※2

RIP-2 では広告経路情報のナチュラルネットワークと広告先インタフェースのナチュラルネットワークが同一である場合は，自動集約をしないでサブネット経路情報として隣接装置に広告します。詳細は「図 15-7　RIP-2 使用時の広告経路自動集約」を参照してください。

RIP-1 使用時のサブネット経路の自動集約を次に示します。

図 15-6　RIP-1 使用時の広告経路自動集約



本装置のルーティングテーブル上の各経路情報の取り扱いは次のとおりです。

No.1

インタフェース A のネットワークアドレスと一致してサブネット長も一致するため，集約しないで広告します。

No.2

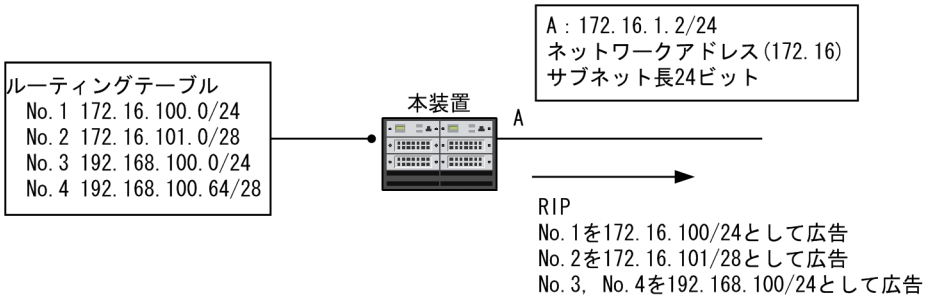
インタフェース A のネットワークアドレスと一致するが，サブネット長が一致しないため広告しません。

No.3 および No.4

インタフェース A とネットワーク境界が異なるため，ナチュラルマスク経路に集約して広告します。

RIP-2 使用時のサブネット経路の自動集約を次の図に示します。

図 15-7　RIP-2 使用時の広告経路自動集約



本装置のルーティングテーブル上の各経路情報の取り扱いは次のとおりです。

No.1

インタフェース A のネットワークアドレスと一致するため，集約しないで広告します。

No.2

インタフェース A のネットワークアドレスと一致するため，集約しないで広告します。

No.3 および No.4

インタフェース A とネットワーク境界が異なるため，ナチュラルマスク経路に集約して広告します。

(a) 自動集約時の広告メトリック

集約元となるサブネット経路情報のうち，いちばん小さなメトリック値を使用して広告されます。

(b) 自動集約時の広告ルートタグ（RIP-2 使用時だけ）

広告ルートタグは 0 となります。

(c) 自動集約時の広告ネクストホップ（RIP-2 使用時だけ）

広告ネクストホップは 0 となります。

15.1.4 経路情報の学習

(1) 経路情報の学習元

RIP では，コンフィグレーションコマンド network によって指定したネットワーク上のすべての隣接ルータ（インタフェースのセカンダリアドレスが属するネットワーク上のルータも含む）から，経路情報を学習できます。ただし，サブネットマスクが 31 ビットに設定されているネットワーク上での経路情報の学習は未サポートです。

(2) 経路情報学習・切り替えのタイミング

RIP で学習した経路情報の切り替えは，次の表に示す機能が関係します。

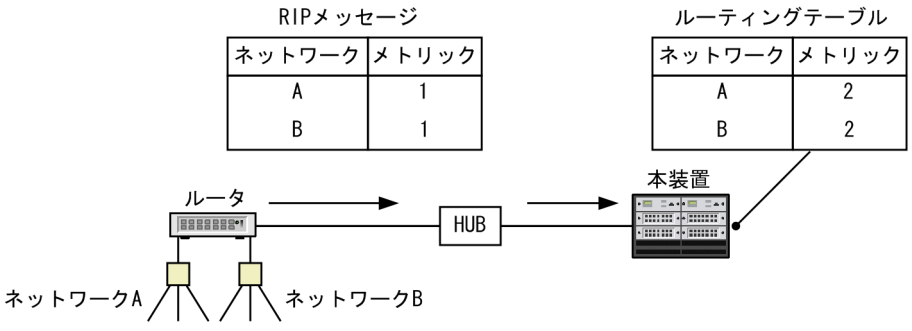
表 15-8 経路情報の学習・切り替えのタイミング

機能	内容
隣接ルータからのレスポンスパケット受信	隣接ルータからの通知に従って，経路情報を追加，変更または削除します。
エージングタイムアウト	隣接ルータから通知された経路情報の周期的な通知が一定時間ない場合に，経路情報を削除します。
インタフェース障害の認識	RIP が動作しているインタフェースの障害を認識した際に，該当インタフェースから学習した経路情報を削除します。

(a) レスポンスパケットの受信

RIP は隣接から受信したレスポンスパケットの経路情報を，自装置のルーティングテーブルに取り込みます。レスポンスパケット受信による経路情報の生成を次の図に示します。

図 15-8 レスポンスパケット受信による経路情報の生成

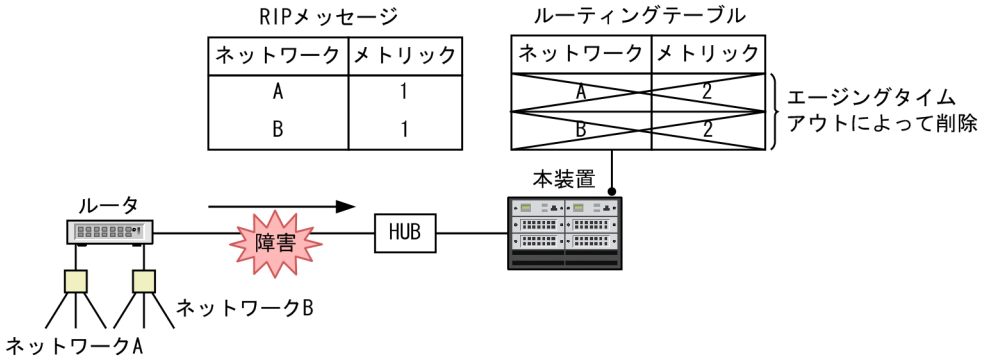


本装置は隣接ルータから学習したネットワーク A および B に関する経路情報を，ルーティングテーブルに追加します。

(b)　エージングタイムアウト

レスポンスパケット受信によって生成された経路情報はエージングタイマによって監視されます。エージングタイマは隣接からの周期的な広告によってリセット（クリア）されます。隣接ルータの障害や自装置と隣接ルータ間の回線障害などによって，隣接から該当する経路情報の広告が 180 秒（エージングタイムアウト値）間発生しない場合，該当する経路情報を自装置のルーティングテーブルから削除します。エージングタイムアウトによる経路情報の削除を次の図に示します。

図 15-9　エージングタイムアウトによる経路情報の削除

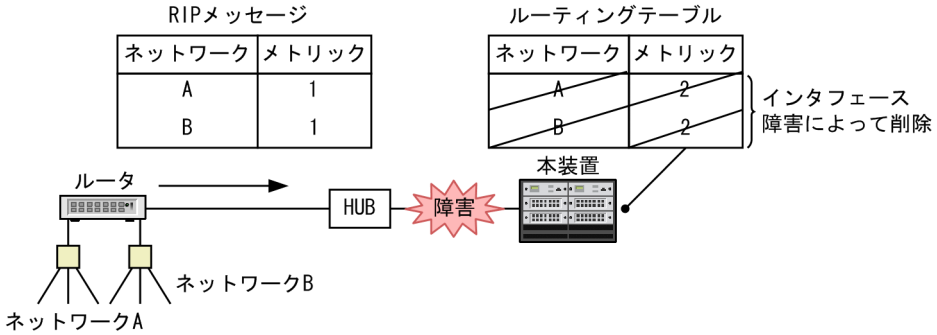


ルータと HUB の間で障害が発生すると，本装置にネットワーク A および B の経路情報が広告されません。本装置は 180 秒（エージングタイムアウト値）間広告のない経路情報を，ルーティングテーブルから削除します。

(c)　インタフェース障害の認識

隣接ルータと接続する自装置のインタフェース障害を認識すると，該当するインタフェースから学習したすべての経路情報を削除します。インタフェース障害による経路情報の削除を次の図に示します。

図 15-10　インタフェース障害による経路情報の削除



本装置は隣接ルータに接続するインタフェースの障害を認識すると，該当するインタフェースから学習したすべての経路情報をルーティングテーブルから削除します。

15.1.5　RIP-1

(1)　RIP-1 での経路情報の広告

RIP-1 を使用する場合は，RIP メッセージを送信するポートのサブネットマスク値によって，広告する経路情報のエントリに制限が付きます。同一ネットワークアドレス内ですべて同一のサブネットマスクを使用する場合は問題ありません。しかし，サブネットマスクを 2 種類以上使用する場合（可変長サブネットマスク：VLSM（Variable Length Subnet Mask））は問題になります。VLSM となるネットワークではルーティングプロトコルに RIP-2（RFC2453 準拠）を使用する必要があります。この場合，一部で RIP-1 も併用する場合には次の表に示す RIP-1 の経路情報の広告条件に注意してください。

表 15-9　RIP-1 の経路情報の広告条件

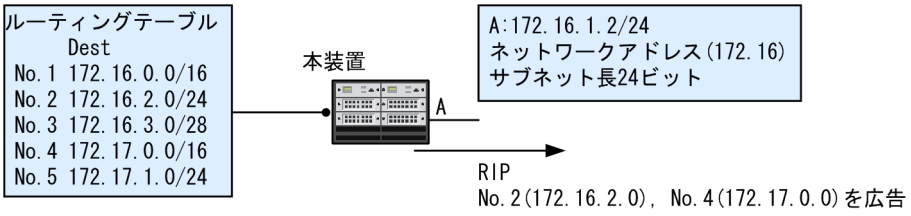
広告する経路情報	広告条件
デフォルト経路情報	無条件に広告します。ただし，RIP 以外で学習したデフォルト経路情報は広告経路フィルタの設定が必要です。
ナチュラルマスク経路情報	本装置が保持しているナチュラルマスク経路情報とインタフェースのネットワークアドレス（アドレスクラスに対応したネットワークアドレス）が異なるとき。
サブネット経路情報※	本装置が保持しているサブネット経路情報のネットワークアドレス（アドレスクラスに対応したネットワークアドレス）とインタフェースのネットワークアドレスが一致して，該当するサブネット経路情報のサブネット長とインタフェースアドレスのサブネット長が一致したとき。
ホスト経路情報	無条件に広告します。

注※　コンフィグレーションコマンド auto-summary が設定されている場合，サブネット経路情報は自動的に一つのナチュラルマスク経路情報に集約され広告されます。

(a)　ナチュラルマスク経路およびサブネットマスク経路情報の広告

RIP で広告するナチュラルマスク経路およびサブネットマスク経路情報を次の図に示します。

図 15-11　RIP で広告するナチュラルマスク経路およびサブネットマスク経路情報



本装置のルーティングテーブル上の各経路情報の取り扱いは次のとおりです。

No.1

インタフェース A のネットワークアドレスと一致するナチュラルマスク経路情報のため広告されません。

No.2

インタフェース A のネットワークアドレスと一致してサブネット長も一致するサブネット経路情報のため広告されます。

No.3

インタフェース A のネットワークアドレスと一致するがサブネット長が異なるサブネット経路情報のため広告されません。

No.4

インタフェース A のネットワークアドレスと一致しないナチュラルマスク経路情報のため広告されます。

No.5

インタフェース A のネットワークアドレスと一致しないサブネット経路情報のため広告されません。

また，この図での広告条件を次の表に示します。

表 15-10 ナチュラルマスク経路およびサブネットマスク経路の広告条件

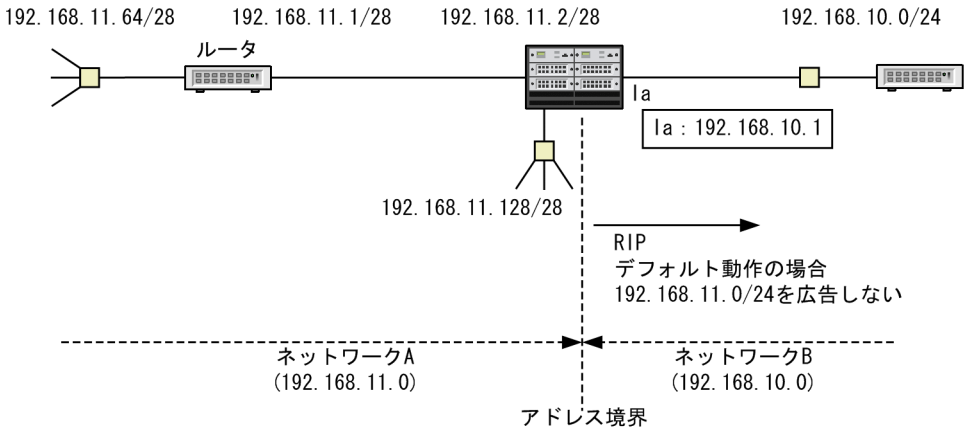
経路情報の種類	ルーティングテーブル上の経路情報	広告条件		広告の有無
		インタフェース D のネットワークアドレスとの一致／不一致	インタフェース D のサブネット長との一致／不一致	
ナチュラルマスク経路	172.16.0.0/16（No.1）	一致	−	×
	172.17.0.0/16（No.4）	不一致	−	○
サブネット経路	172.17.1.0/24（No.5）	不一致	一致	×
	172.16.2.0/24（No.2）	一致	一致	○
	172.16.3.0/28（No.3）	一致	不一致	×

（凡例） ○：広告する ×：広告しない −：該当しない

(b) サブネット経路情報の広告に関する注意事項

本装置では，コンフィグレーションコマンド auto-summary が設定されていない場合，該当する装置の各インタフェースが持つ IP アドレスに対するナチュラルマスク経路情報を自動生成しないで，サブネット経路情報だけを生成します。アドレス境界を越える場合, RIP-1 ではサブネット経路情報を広告しないため注意が必要です。構成例を次の図に示します。

図 15-12 直結経路を広告しない構成例



注意すべき構成

- ルーティングプロトコルは RIP-1。
- コンフィグレーションコマンド auto-summary が設定されていない。
- 本装置上にアドレス境界を生成する。
- インタフェースのサブネットマスクが，ナチュラルマスクではない。

対策 1

- コンフィグレーションコマンド auto-summary を設定する。

対策 2

- コンフィグレーションで，経路集約（サブネット経路情報およびホスト経路情報をナチュラルマスク経路情報に集約する）を設定する。
- コンフィグレーションで，広告経路フィルタ（集約経路を RIP に再配布する）を設定する。

対策 3

- コンフィグレーションで，サブネットワーク化されたインタフェースに対応するナチュラルマスクの直結経路を生成するように設定する（コンフィグレーションコマンド ip auto-class-route）。
- 上記経路は直結経路として取り扱っているので，デフォルト（再配布フィルタの設定なし）で広告される。

(2) RFC との差分

本装置の RIP-1 は RFC1058 に準拠していますが，ソフトウェアの機能制限から一部 RFC との差分があります。RFC との差分を次の表に示します。

表 15-11 RFC との差分

RFC			本装置
RFC1058	サブネットの広告	サブネット化されたネットワークと接続している境界ゲートウェイは，ほかの隣接ゲートウェイに対して全体のネットワーク経路だけを広告します。	サブネットワーク経路からネットワーク経路を生成したい場合は，RIP 広告経路自動集約機能を使用する必要があります。
		一般に全体のネットワークのメトリックは，サブネットの中でいちばん小さいメトリックが採用されます。	サブネットワーク経路からネットワーク経路を生成したい場合は，RIP 広告経路自動集約機能を使用する必要があります。
		境界ゲートウェイは直接接続されたネットワークにあるホスト経路をほかのネットワークに対して広告してはなりません。	本装置では直接接続されたネットワークにあるホスト経路を，ルーティングテーブルに追加および広告します。
	レスポンス受信	すでに存在するネットワーク経路またはサブネットワーク経路に含まれるホスト経路は追加しないことが望ましいです。	本装置ではレスポンスによってホスト経路を受信した場合，ルーティングテーブルに追加します。

15.1.6 RIP-2

(1) RIP-2 の諸機能

RIP-2 は広告する経路情報に該当する経路のサブネットマスクを設定するため，RIP-1 のような経路広告上の制限はなく，可変長サブネットを取り扱うことができます。RIP-2 固有の機能を次に示します。

(a) ルートタグ

本装置ではレスポンスメッセージで通知された経路情報のルートタグ情報が設定されている場合，ルーティングテーブルにルートタグ情報を取り込みます。本装置から通知するレスポンスメッセージの経路情報のルートタグ情報は，ルーティングテーブルの該当する経路のルートタグを設定します。なお，設定できる範囲は 1～65535（10 進数）です。

(b) サブネットマスク

本装置ではレスポンスメッセージで通知された経路情報のサブネットマスク情報が設定されている場合，ルーティングテーブルに該当するサブネットマスク情報を取り込みます。サブネットマスク情報が設定されていない場合，RIP-1 での経路情報受信と同様に扱います。

本装置から通知するレスポンスメッセージの経路情報のサブネットマスク情報は，ルーティングテーブルの該当する経路のサブネットマスクを設定します。

(c) ネクストホップ

本装置ではレスポンスメッセージで通知された経路情報のネクストホップ情報が設定されている場合，ルーティングテーブルに該当するネクストホップ情報を取り込みます。ネクストホップ情報が設定されていない場合，送信元のゲートウェイをネクストホップとして認識します。

本装置から通知するレスポンスメッセージの経路情報のネクストホップ情報は，通知する経路情報のネクストホップが送信先ゲートウェイと同一のネットワーク上にある場合，ルーティングテーブルの該当する経路のネクストホップを設定します。同一のネットワーク上にない場合，送信インタフェースのアドレスを設定します。

(d) マルチキャストアドレスの使用

本装置では RIP-2 メッセージを受信しないホストでの不要な負荷を軽減するために，マルチキャストアドレスをサポートします。RIP-2 メッセージ送信時に使用するマルチキャストアドレスは 224.0.0.9 を使用します。

(e) 認証機能

RIP では，ルータ間のメッセージ交換時にメッセージを送信したルータが同じ管理下にあることを検証するために，認証を使用できます。隣接ルータとの間で認証を使用することで，不正な経路情報を送信することによる経路制御上の攻撃から，認証管理下にあるルータを保護できます。

認証方式には，平文パスワード認証と暗号認証があります。暗号認証の認証アルゴリズムとして Keyed-MD5 をサポートします。

コンフィグレーションでは，インタフェースごとに認証方式と認証キーを指定します。コンフィグレーションの指定がない場合，認証しません。

● 平文パスワード認証の認証手順

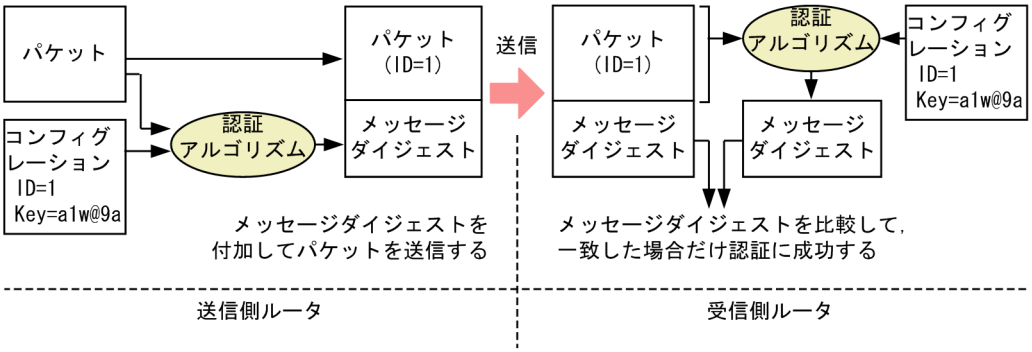
平文パスワード認証では，メッセージにコンフィグレーションで設定した認証キーをそのままパスワードとして埋め込んで送信します。コンフィグレーションで複数の認証キーが設定されている場合は，すべての認証キーごとにメッセージを複製して送信します。

メッセージの受信時には，メッセージ中のパスワードと，設定してある認証キーのどれかが一致した場合，認証に成功したと見なします。認証に失敗したメッセージは破棄します。

● 暗号認証の認証手順

暗号認証では，メッセージダイジェストを比較することで，メッセージを認証します。暗号認証のデータフローを次の図に示します。

図 15-13　暗号認証のデータフロー



メッセージの送信時には，認証キーとメッセージ本体から認証アルゴリズム（Keyed-MD5）を使用してメッセージダイジェストを生成して，これをメッセージとともに送信します。コンフィグレーションで複数の認証キーが設定されている場合は，すべての認証キーごとにメッセージを複製して送信します。

メッセージの受信時には，メッセージ中に含まれるキー識別子と同じキー識別子を持つ認証キーを使用して認証します。この認証キーを使用して送信時と同様の手順を経てメッセージダイジェストを生成して，生成したメッセージダイジェストが受信したメッセージダイジェストと一致した場合，認証に成功したと見なします。認証に失敗したメッセージは破棄します。

● 認証キーの変更手順

RIP-2 ネットワークで認証を使用する場合，通常は各ルータで単一の認証キーを使用して運用しますが，認証キーを変更するときは一時的に複数の認証キーを使用します。

認証キーの変更手順を次に示します。

1. 認証を使用するネットワーク中の各ルータで，旧認証キーと新認証キーの両方を有効にしてください。
   本装置では，コンフィグレーションで指定したすべてのキーが有効になります。
2. 認証を使用するネットワーク中の各ルータで，旧認証キーを削除，または無効にしてください。

● 暗号認証使用時の注意事項

暗号認証を使用しているメッセージには，リプレイ攻撃防止のためシーケンス番号が付いています。シーケンス番号には前回送信した番号より大きい値を設定する必要があり，本装置では，1970/1/1 0:00 からの経過秒数を設定しています。

なお，運用コマンド set clock などでシステムの現在時刻を後退させても，隣接装置で認証が失敗しないように，本装置では，前回送信したシーケンス番号より大きい値に調整して送信します。ただし，装置を再起動すると番号を調整できなくなるため，再起動前に送信したメッセージのシーケンス番号よりも小さいシーケンス番号でメッセージを送信することがあります。この場合は，メッセージを受信した隣接装置で認証に失敗します。特に，暗号認証の使用中に現在時刻を大きく後退させたあとは，装置の再起動後に，隣接装置での認証に失敗する可能性が高くなりますので，注意してください。

また，認証の失敗が継続する場合は，ネットワーク内のすべてのルータで認証キーを変更してください。

(2) RFC との差分

本装置の RIP-2 は RFC2453 および RFC4822 に準拠していますが，ソフトウェアの機能制限から一部 RFC との差分があります。RFC との差分を次の表に示します。

表 15-12 RFC との差分

RFC		本装置
RFC2453	RIP-2 ルータが RIP-1 のリクエストを受信した場合，RIP-1 のレスポンスで応答すべきです。RIP-2 だけを送信するように設定されている場合，レスポンスは送信すべきではありません。	本装置は RIP-2 インタフェースでは RIP-2 のレスポンスだけを送信します。そのため，RIP-1 のリクエストを受信した場合，リクエストに対するレスポンスは送信しません。
	受信制御スイッチ（RIP-1 だけを許す，RIP-2 だけを許す，両方許す，受信を受け付けない）を持つべきです。これらはインタフェース単位に行います。	本装置ではインタフェース単位で RIP の受信を制御できますが，RIP-1，RIP-2 を区別した受信制御はできません。
RFC4822	認証キーとキー識別子を含む認証コンフィグレーションパラメータのセットには，キーの有効期限とそれに関連するコンフィグレーションパラメータを有します。	本装置ではキーの有効期限設定はサポートしません。
	すべての適合した実装は，Keyed-MD5 認証アルゴリズムと，HMAC-SHA1 認証アルゴリズムを実装しなければなりません。	本装置では Keyed-MD5 認証アルゴリズムだけサポートします。

(3) マルチホーム・ネットワーク設計時の注意事項

セカンダリアドレスが設定されたインタフェース上で RIP-2 を使用する場合は，次のことに留意してください。

RIP-2 では送信するパケットにマルチキャストアドレスを使用します。マルチキャストアドレスが指定されたパケットは，プライマリネットワークまたはセカンダリネットワークに属するすべてのルータに対して送達されるため，RIP 受信を必要としないルータに不要な負荷が掛かることになります。

15.2 コンフィグレーション

15.2.1 コンフィグレーションコマンド一覧

RIP のコンフィグレーションコマンド一覧を次の表に示します。

表 15-13 コンフィグレーションコマンド一覧

コマンド名	説明
address-family ipv4	VRF 単位の情報を設定します。config-router-af モードへ移行します。
auto-summary	RIP で広告するサブネット経路情報を自動的にナチュラルマスク経路情報として集約して広告することを指定します。
default-metric	ほかのプロトコルで学習した経路情報を RIP で広告する場合のメトリック値を指定します。
disable	RIP が動作しないことを指定します。
distance	RIP で学習した経路情報のディスタンス値を指定します。
generate-secondary-route	第 2 優先経路をルーティングテーブルに登録します。
inherit-metric	ほかのルーティングプロトコルの経路情報を RIP で広告する際，メトリック値を引き継ぐことを指定します。
ip rip authentication key	RIP バージョン 2 パケットの認証方式および認証キーを指定します。
ip rip v2-broadcast	指定インタフェースから送信するパケットの宛先アドレスに，ブロードキャストアドレスを使用することを指定します。
ip rip version	指定インタフェースで使用する RIP のバージョンを指定します。
metric-offset	指定インタフェースで RIP パケットを送受信する際に，メトリック値に加算する値を指定します。
neighbor	RIP パケットを送信する隣接ルータを指定します。
network	RIP 送受信先ネットワークを指定します。
passive-interface	指定インタフェースからレスポンスパケットを送信しないことを指定します。
router rip	RIP に関する動作情報を設定します。
timers basic	RIP の各種タイマ値を指定します。
version	RIP のバージョンを指定します。
distribute-list in (RIP)※	RIP で学習した経路をルーティングテーブルに取り込むかどうかをフィルタに従って制御します。
distribute-list out (RIP)※	RIP で広告する経路をフィルタに従って制御します。
ip prefix-list※	ip prefix-list を設定します。
redistribute (RIP)※	RIP で広告する経路のプロトコルを指定します。
route-map※	route-map を設定します。

注※
「コンフィグレーションコマンドレファレンス Vol.3　22. 経路フィルタリング」を参照してください。

15.2.2 RIP の適用

RIP パケットを送受信するネットワークおよび RIP バージョンを設定します。

[設定のポイント]

network コマンドで RIP を動作させるネットワークを指定します。また，RIP のバージョンの指定には，version コマンドを使用します。

[コマンドによる設定]

1. **(config)# router rip**
   (config-router)# network 192.168.1.0 0.0.0.255
   ネットワーク 192.168.1.0/24 で RIP パケットの送受信を有効にします。
2. **(config-router)# network 192.168.2.0 0.0.0.255**
   ネットワーク 192.168.2.0/24 で RIP パケットの送受信を有効にします。
3. **(config-router)# version 2**
   RIP バージョンを RIP-2 に設定します。

15.2.3 メトリックの設定

(1) RIP 以外の経路情報を広告するときのメトリック値の設定

ほかのプロトコルで学習した経路情報を RIP で広告する場合のメトリック値を設定します。

[設定のポイント]

RIP によって OSPF 経路または BGP4 経路を広告する場合は，コンフィグレーションによるメトリック値の設定が必須となります。メトリック値の設定には default-metric コマンドを使用します。

[コマンドによる設定]

1. **(config)# router rip**
   (config-router)# network 192.168.1.0 0.0.0.255
   (config-router)# network 192.168.2.0 0.0.0.255
   (config-router)# default-metric 3
   ほかのプロトコルで学習した経路情報を RIP で広告する場合のメトリック値として 3 を設定します。
2. **(config-router)# redistribute static**
   RIP でスタティック経路を広告することを設定します。
3. **(config-router)# redistribute ospf**
   RIP で OSPF 経路を広告することを設定します。

(2) パケット送受信時にメトリック値に加算する値の設定

RIP パケットを送受信する際にメトリック値に加算する値を設定します。

[設定のポイント]

特定のインタフェースで送信または受信する経路のメトリック値に加算する値の設定には，metric-offset コマンドを使用します。

[コマンドによる設定]

1. **(config)# router rip**
   (config-router)# network 192.168.1.0 0.0.0.255
   (config-router)# network 192.168.2.0 0.0.0.255
   (config-router)# metric-offset 2 gigabitethernet 1/1 out
   ポート 1/1 から送信する RIP パケットのメトリック値に 2 を加算する設定をします。
2. **(config-router)# metric-offset 2 gigabitethernet 1/2 in**
   ポート 1/2 から受信する RIP パケットのメトリック値に 2 を加算する設定をします。

15.2.4 タイマの調整

RIP の周期広告タイマ値，エージングタイマ値，およびルーティングテーブルから削除するまでの時間を調整します。

経路変更時の収束時間を短縮するためには，周期広告タイマ値，エージングタイマ値をデフォルト値より小さく設定します。また，RIP の周期広告のトラフィックを少なくしたい場合は周期広告タイマ値をデフォルト値より大きく設定します。

なお，RIP のタイマ値を変更する場合は，RIP ネットワーク上のすべてのルータに対しても，同じタイマ値を適用してください。

[設定のポイント]

RIP のタイマ値の変更には timers basic コマンドを使用します。

[コマンドによる設定]

1. **(config)# router rip**
   (config-router)# network 192.168.1.0 0.0.0.255
   (config-router)# network 192.168.2.0 0.0.0.255
   (config-router)# timers basic 40 200 100
   RIP の周期広告タイマを 40 秒，エージングタイマを 200 秒，ルーティングテーブルから削除するまでの時間を 100 秒に設定します。

15.2.5 RIP パケットの送信抑止

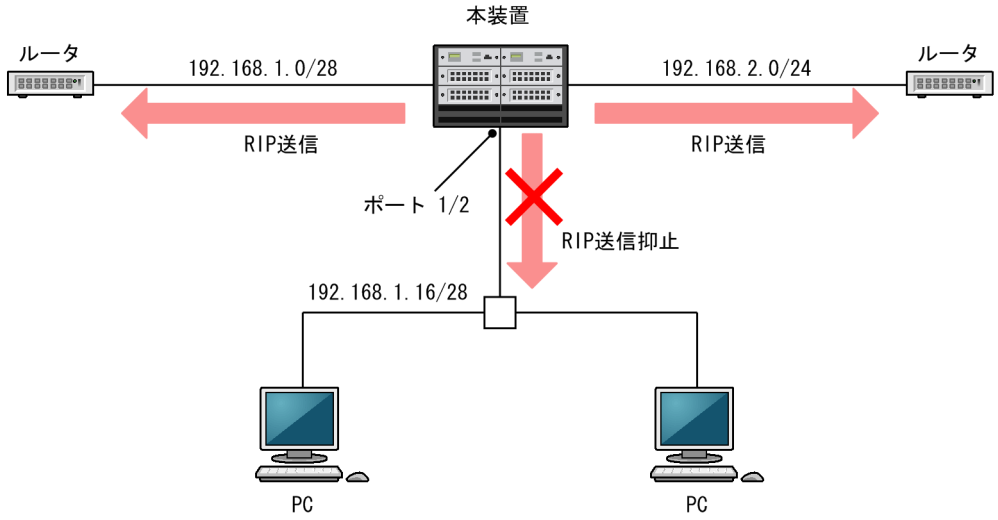
(1) 特定インタフェースからレスポンスパケットの送信を抑止する設定

レスポンスパケットの送信抑止をインタフェース単位に設定します。

[設定のポイント]

インタフェース単位にレスポンスパケットの送信を抑止するには passive-interface コマンドを設定します。

図 15-14　RIP パケットの送信抑止



PC は本装置向きにデフォルト経路を設定しているため，RIP の学習は不要です。

[コマンドによる設定]

1. **(config)# router rip**
   (config-router)# network 192.168.1.0 0.0.0.255
   (config-router)# network 192.168.2.0 0.0.0.255
   (config-router)# passive-interface gigabitethernet 1/2
   ポート 1/2 でレスポンスパケットの送信を抑止する設定をします。

(2)　特定インタフェースだけレスポンスパケットを送信する設定

レスポンスパケットを送信できるすべてのインタフェースで送信を抑止して，特定のインタフェースにだけレスポンスパケットを送信できるように設定します。

[設定のポイント]

passive-interface コマンドで default パラメータを設定したあと，レスポンスパケットを送信するインタフェースにだけ no passive-interface コマンドを設定します。

[コマンドによる設定]

1. **(config)# router rip**
   (config-router)# passive-interface default
   すべてのインタフェースでレスポンスパケットの送信を抑止する設定をします。
2. **(config-router)# no passive-interface gigabitethernet 1/1**
   ポート 1/1 でレスポンスパケットを送信する設定をします。

15.2.6　RIP パケット送信相手の限定

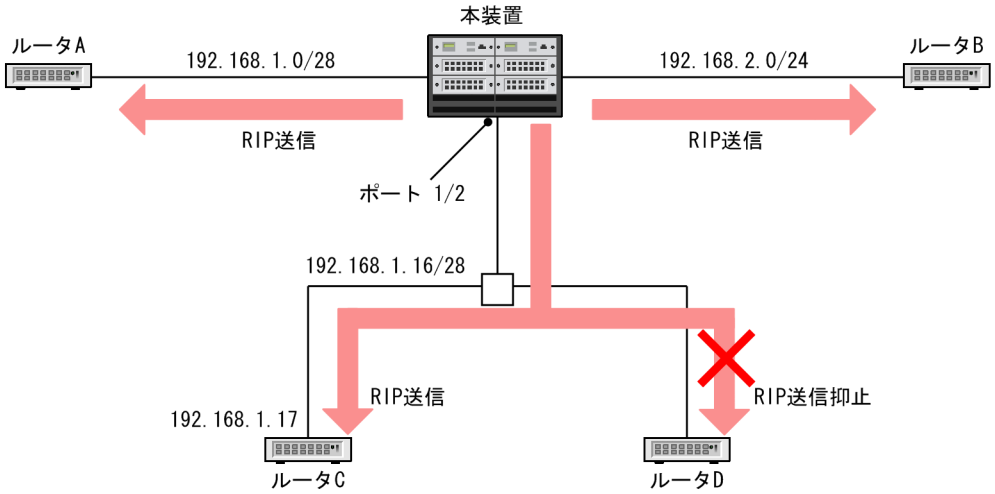
特定の隣接ルータに対して，ユニキャストによる経路広告を行う設定をします。

[設定のポイント]

特定の隣接ルータに対する経路広告の設定には neighbor コマンドを使用します。

設定の際は，あらかじめ passive-interface コマンドで，インタフェースに対するブロードキャスト（またはマルチキャスト）による広告を抑止しておきます。

図 15-15　RIP パケット送信相手の限定



RIP による学習をしていないルータ D に対するレスポンスパケットの送信を抑止します。

[コマンドによる設定]

1. **(config)# router rip**
   (config-router)# network 192.168.1.0 0.0.0.255
   (config-router)# network 192.168.2.0 0.0.0.255
   (config-router)# passive-interface gigabitethernet 1/2
   ポート 1/2 でレスポンスパケットの送信を抑止する設定をします。
2. **(config-router)# neighbor 192.168.1.17**
   隣接ルータ 192.168.1.17 に対してユニキャストで経路広告を行うことを設定します。

15.2.7　認証の適用

特定のインタフェースで送受信する RIP-2 パケットに，認証機能を適用します。

[設定のポイント]

ip rip authentication key コマンドを使用して，キー識別子，認証方式，認証キーを設定します。認証キーは，同一ネットワーク内のすべてのルータで単一のものを使用してください。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   (config-if)# ip rip authentication key 1 md5 a1w@9a
   (config-if)# ip rip version 2
   ポート 1/1 で RIP-2 の認証を適用します。
   キー識別子に 1，認証方式に暗号認証（Keyed-MD5），認証キーに a1w@9a を設定します。

15.2.8　VRF での RIP の適用

VRF で RIP を適用します。

[設定のポイント]

address-family ipv4 vrf コマンドで config-router-af モードへ移行して，必要な情報を指定します。

[コマンドによる設定]

1. **(config)# router rip**
   (config-router)# address-family ipv4 vrf 2
   config-router-af モードへ移行して，VRF 2 で動作する RIP の情報を指定します。
2. **(config-router-af)# network 172.16.2.0 0.0.0.255**
   ネットワーク 172.16.2.0/24 で RIP パケットの送受信を有効にします。
3. **(config-router-af)# version 2**
   RIP バージョンを RIP-2 に設定します。
4. **(config-router-af)# exit**
   config-router-af モードを終了します。

15.3　オペレーション

15.3.1　運用コマンド一覧

RIP の運用コマンド一覧を次の表に示します。

表 15-14　運用コマンド一覧

コマンド名	説明
show ip route	ルーティングテーブルで保持する経路情報を表示します。
clear ip route	H/W の IPv4 フォワーディングエントリをクリアして再登録します。
show ip rip	RIP プロトコルに関する情報を表示します。
clear counters rip ipv4-unicast	RIP プロトコルに関する情報をクリアします。
show ip vrf	VRF の IPv4 情報を表示しまず。
show ip interface ipv4-unicast	ユニキャストルーティングプログラムが認識している本装置の IPv4 インタフェース情報を表示します。
debug ip	IPv4 ルーティングプロトコルが送受信するパケットをリアルタイムに表示します。

15.3.2　RIP の動作状況の確認

RIP プロトコルに関する情報を表示します。

図 15-16　show ip rip の実行結果

```
> show ip rip
Date 20XX/03/14 12:00:00 UTC
RIP Flags: <ON>
Default Metric: 1, Distance: 120
Timers (seconds)
  Update             : 30
  Aging              : 180
  Garbage-Collection : 60
```

15.3.3　送信先情報の確認

RIP の送信先情報を表示します。

図 15-17　show ip rip target の実行結果

```
> show ip rip target
Date 20XX/03/14 12:00:00 UTC
Source Address  Destination     Flags
192.168.1.1     192.168.1.100   <V1 Unicast>
192.168.1.1     192.168.1.200   <V1 Unicast>
192.168.1.1     192.168.1.255   <V1 Passive>
192.168.2.1     192.168.2.255   <V2 Multicast>
```

15.3.4　学習経路情報の確認

(1)　ネットワーク単位の確認

指定ネットワークに含まれる RIP で学習した，ルーティングテーブルで保持する経路情報を表示します。

図 15-18 show ip rip route の実行結果

```
> show ip rip route 172.0.0.0/8
Date 20XX/03/14 12:00:00 UTC
Status Codes: * valid, > active, r RIB failure
   Destination        Next Hop        Interface       Metric Tag   Timer
*> 172.16/16          192.168.1.100   Eth1/1          3      0      4s
*> 172.17/16          192.168.2.2     Eth1/2          4      0     10s
*> 172.18/16          192.168.2.2     Eth1/2          3      0     10s
*> 172.19/16          192.168.1.200   Eth1/1          5      0     17s
```

(2) ゲートウェイ単位の確認

指定ゲートウェイから学習した，ルーティングテーブルで保持する経路情報を表示します。

図 15-19 show ip rip received-routes の実行結果

```
> show ip rip received-routes 192.168.2.2
Date 20XX/03/14 12:00:00 UTC
Status Codes: * valid, > active, r RIB failure

Neighbor Address: 192.168.2.2
   Destination        Next Hop        Interface       Metric Tag   Timer
*> 172.17/16          192.168.2.2     Eth1/2          4      0     15s
*> 172.18/16          192.168.2.2     Eth1/2          3      0     15s
*> 192.168.3/24       192.168.2.2     Eth1/2          2      0     15s
*> 192.168.5/24       192.168.2.2     Eth1/2          4      0     15s
```

15.3.5 広告経路情報の確認

(1) 宛先単位の確認

指定ターゲットへ送信している経路情報を表示します。

図 15-20 show ip rip advertised-routes の実行結果（宛先単位）

```
> show ip rip advertised-routes 192.168.2.255
Date 20XX/03/14 12:00:00 UTC
Target Address: 192.168.2.255
Destination        Next Hop        Interface       Metric Tag   Age
172.16/16          192.168.1.100   Eth1/1          4      0     19s
172.19/16          192.168.1.200   Eth1/1          6      0      2s
192.168.4/24       192.168.1.200   Eth1/1          3      0      2s
192.168.6/24       192.168.1.100   Eth1/1          5      0     19s
```

(2) ネットワーク単位の確認

指定ネットワークに含まれる RIP で送信しているすべての経路情報を，ターゲット単位に表示します。

図 15-21 show ip rip advertised-routes の実行結果（ネットワーク単位）

```
> show ip rip advertised-routes 172.0.0.0/8
Date 20XX/03/14 12:00:00 UTC
Target Address: 192.168.1.100
Destination        Next Hop        Interface       Metric Tag   Age
172.17/16          192.168.2.2     Eth1/2          5      0      1s
172.18/16          192.168.2.2     Eth1/2          4      0      1s
172.19/16          192.168.1.200   Eth1/1          6      0      7s
Target Address: 192.168.1.200
Destination        Next Hop        Interface       Metric Tag   Age
172.16/16          192.168.1.100   Eth1/1          4      0     24s
172.17/16          192.168.2.2     Eth1/2          5      0      1s
172.18/16          192.168.2.2     Eth1/2          4      0      1s
Target Address: 192.168.2.255
Destination        Next Hop        Interface       Metric Tag   Age
172.16/16          192.168.1.100   Eth1/1          4      0     24s
172.19/16          192.168.1.200   Eth1/1          6      0      7s
```

16 RIPng

この章では，IPv6 のルーティングプロトコルの RIPng について説明します。

16.1 解説

16.1.1 概要

RIPng はネットワークで接続したルータ間で使用するルーティングプロトコルです。各ルータは RIPng を使用して自ルータから到達できるネットワークとそのネットワークへのホップ数（メトリック）を通知し合うことによって経路情報を生成します。RIPng はバージョン 1（RFC2080 準拠）をサポートしています。

(1) メッセージの種類

RIPng で使用するメッセージの種類にはリクエストとレスポンスの 2 種類があります。ルータがほかのルータに経路情報を要求する場合にはリクエストを使用して，ほかのルータからのリクエストに応答する場合，および定期的またはトポロジ変化時に自ルータの経路情報をほかのルータに通知する場合にレスポンスを使用します。

(2) 運用時の処理

本装置の立ち上げ時，本装置はリクエストメッセージをすべての隣接ルータに送信して，隣接ルータが持つすべての経路情報を通知するように要求します。運用に入ると，本装置は次の三つの要因でレスポンスを送信します。

- 隣接ルータからリクエストを受信した場合で，リクエストの内容によって自分が持つ経路情報をリクエストの送信元にレスポンスで応答します。
- 定期的に行う経路情報の通知です。本装置は 30 秒ごとに自分が持つ経路情報をすべて含むレスポンスを送信して，隣接ルータに通知します。
- 経路の変化を検出したときに行う経路情報の通知です。本装置は経路の変化を検出した場合，変化した経路に関連する経路情報を含むレスポンスを送信して，隣接ルータに通知します。

各隣接ルータが送信したレスポンスを受信して，経路の変更を検出した場合は自分が持つ経路情報を更新します。レスポンスは隣接ルータとの送信の確認にも使用します。180 秒以上レスポンスを応答しないルータに対しては通信不可能と判断して，代替ルートがあるときはルーティングテーブルをその代替ルートに更新します。代替ルートがないときはルートを削除します。

(3) ルーティングループの抑止処理

本装置は中継経路のループを抑止するために**スプリットホライズン**を使用します。スプリットホライズンとは，受信した情報を受け取ったインタフェースには送信しない処理のことです。

(4) RIPng（IPv6）と RIP（IPv4）の機能差分

RIPng（IPv6）と RIP（IPv4）の機能差分を次の表に示します。

表 16-1 RIPng（IPv6）と RIP（IPv4）の機能差分

機能	RIPng（IPv6）	RIP（IPv4）
triggered update	○	○
スプリットホライズン	○	○
ルートポイズニング	○	○

機能	RIPng（IPv6）	RIP（IPv4）
ポイズンリバース	×	×
ホールドダウン	×	×
ルートタグ	○	○
指定ネクストホップの取り込み	○	○
平文パスワード認証	×	○
暗号認証（Keyed-MD5）	×	○
既存経路と同じメトリックの経路を異なるゲートウェイから受信したときに，既存経路のエージングタイムがタイマ値の 1/2 秒以上経過している場合，新しく学習した経路に変更する	×	○

（凡例）　○：取り扱う　×：取り扱わない

16.1.2　経路選択基準

本装置は，各プロトコルで学習した同じ宛先への経路情報をそれぞれ独立した経路選択手順に従って一つの最良の経路を選択します。同じ宛先への経路情報が各プロトコルで生成されることによって複数存在する場合，それぞれの経路情報のディスタンス値が比較されて優先度の最も高い経路情報が有効になります。

RIPng では，自プロトコルを使用し学習した同じ宛先への広告元の異なる複数の経路情報から，経路選択の優先順位に従って一つの最良の経路を選択します。経路選択の条件を，優先順位が高い順に次に示します。

1. メトリック値が最も小さい経路を選択します。
2. ネクストホップアドレスが最も小さい経路を選択します。
3. 経路情報に含まれるネクストホップアドレスと経路情報の送信元ゲートウェイアドレスが一致する経路を選択します。

   この条件は，同一ネットワーク内にある異なる隣接装置から，経路情報に含まれるネクストホップアドレスが同一となる経路情報を学習する場合に適用されます。
4. そのほかの場合，新しく学習した経路を無視します。

その後，同じ宛先への経路情報が各プロトコル（OSPFv3，BGP4+，スタティック）で学習した経路によって複数存在する場合は，それぞれの経路情報のディスタンス値が比較され，優先度の最も高い経路情報をルーティングテーブルに設定します。

(1)　第 2 優先経路の生成

コンフィグレーションコマンド generate-secondary-route を指定することによって，異なる隣接装置から学習した同一宛先への経路情報を二つ（第 1 優先経路と第 2 優先経路）まで生成します。第 2 優先経路を生成する条件を次の表に示します。

表 16-2 第 2 優先経路の生成条件

条件		第 2 優先経路の生成
コンフィグレーションコマンド generate-secondary-route の指定	ディスタンス値	
×	−	生成しない
○	第 1 優先経路と第 2 優先経路の値が異なる	生成しない
○	第 1 優先経路と第 2 優先経路の値が同じ	生成する

（凡例） ○：コンフィグレーションあり ×：コンフィグレーションなし −：該当なし

第 2 優先経路の生成を指定した場合，経路選択の優先順位に従って同じ宛先への経路情報の優先度を決定します。第 2 優先経路の経路選択の条件を，優先順位が高い順に次に示します。ただし，ネクストホップアドレスが同じ場合は第 1 優先経路だけを生成します。

1. メトリック値が小さい経路を選択します。
2. ネクストホップアドレスが小さい経路を選択します。
   なお，第 2 優先経路が登録されている状態で新経路を学習した場合，この条件は適用されません。
3. 経路情報に含まれるネクストホップアドレスと経路情報の送信元ゲートウェイアドレスが一致する経路を選択します。
   この条件は，同一ネットワーク内にある異なる隣接装置から，経路情報に含まれるネクストホップアドレスが同一となる経路情報を学習する場合に適用されます。
4. 今まで第 1 優先だった経路を選択します。
5. そのほかの場合，新しく学習した経路を無視します。

16.1.3 経路情報の広告

(1) 広告対象経路

(a) 学習プロトコル

RIPng では，広告経路フィルタを設定していない場合，学習した RIPng 経路および RIPng が動作するインタフェースの直結経路を広告します。広告経路フィルタを設定した場合は，広告経路フィルタの動作に従って広告動作を行います。RIPng で広告対象の学習プロトコルを次の表に示します。

表 16-3 広告対象の学習プロトコル

学習プロトコル		広告経路フィルタの設定がない場合の広告動作	広告メトリックの適用順序※5
直結経路※1	RIPng が動作するインタフェース	広告します	1. 広告経路フィルタの指定値 2. デフォルト値（metric 値：1）
	RIPng が動作するインタフェース以外	広告しません	
集約経路		広告しません	

学習プロトコル	広告経路フィルタの設定がない場合の広告動作	広告メトリックの適用順序※5
スタティック経路	広告しません	1. 広告経路フィルタの指定値 2. default-metric の指定値 3. デフォルト値（metric 値：1）
RIPng※2	広告します	1. 広告経路フィルタの指定値 2. ルーティングテーブルの値
OSPFv3	広告しません	1. 広告経路フィルタの指定値 2. inherit-metric の設定がある場合は，ルーティングテーブルの値※3 3. default-metric の指定値※4
BGP4+	広告しません	
他 VRF またはグローバルネットワークからインポートした経路	広告しません	

注※1

インタフェースに設定されているすべてのグローバルアドレスを広告します。

注※2

スプリットホライズンが適用されます。

注※3

ルーティングテーブルのメトリック値が 16 以上の場合は，経路を広告しません。

注※4

広告経路フィルタ，inherit-metric または default-metric によるメトリックの指定がない場合は，経路を広告しません。

注※5

metric-offset out コマンドの設定がある場合は，選択したメトリック値に対してさらに metric-offset out コマンドの指定値を加算します。加算した結果，メトリック値が 16 以上となった場合は，経路を広告しません。

(b)　アドレス種別

RIPng で広告対象のアドレス種別を次の表に示します。

表 16-4　経路情報の種類

経路情報の種類	定義	例	広告可否
デフォルト経路情報	すべてのネットワーク宛ての経路情報	::/0	○
ネットワーク経路情報	特定のネットワーク宛てのグローバル経路情報	2001:db8:1:1::/64 2001:db8:1::/56	○※
ホスト経路情報	特定のホスト宛てのグローバル経路情報	2001:db8:1:1::1/128	○※

（凡例）　○：広告できる

注※　グローバルアドレスだけ広告できます。

(2)　経路情報の広告先

RIPng では，コンフィグレーションコマンド ipv6 rip enable を指定したインタフェースと接続するすべての隣接ルータに対して，経路情報を広告します。

(3) 経路情報の広告タイミング

RIPng による経路広告タイミングは，次の表に示す機能が関係します。

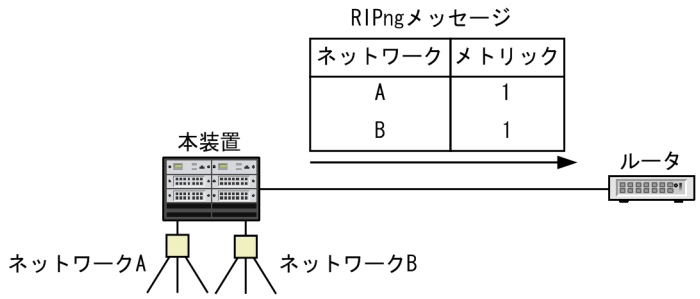
表 16-5 経路広告タイミング

機能	内容
周期的な経路情報広告	自装置が持つ経路情報を隣接ルータに周期的に通知します。
triggered update	自装置の経路情報に変更があったときに定期的な広告を待たないで通知します。
隣接ルータからのリクエストに対する応答	リクエストパケットを送信した隣接ルータに対して通知します。
ルートポイズニング	経路情報が削除されたことを隣接ルータに一定時間通知します。

(a) 周期的な経路情報広告

RIPng は自装置が持つすべての経路情報を周期的に隣接のルータに広告します。周期的な経路情報広告を次の図に示します。

図 16-1 周期的な経路情報広告

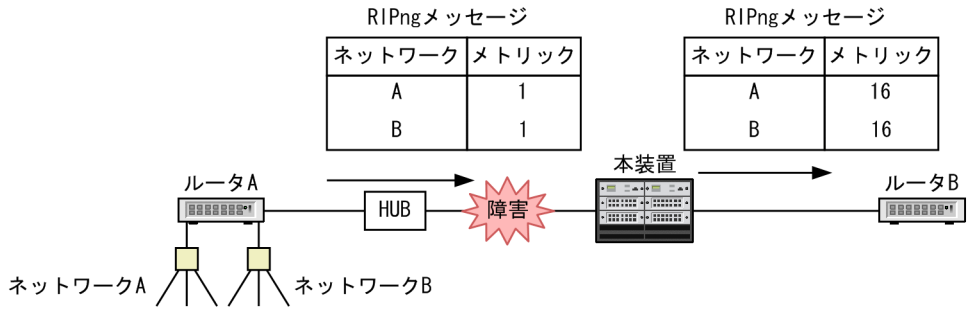


本装置はネットワーク A および B に関する経路情報を 30 秒周期（周期広告タイマ）でルータに広告します。

(b) triggered update

自装置の経路情報の変化を認識したときに定期的な配布周期を待たないで経路情報を配布します。
triggered update による経路情報の広告を次の図に示します。

図 16-2 triggered update による経路情報の広告

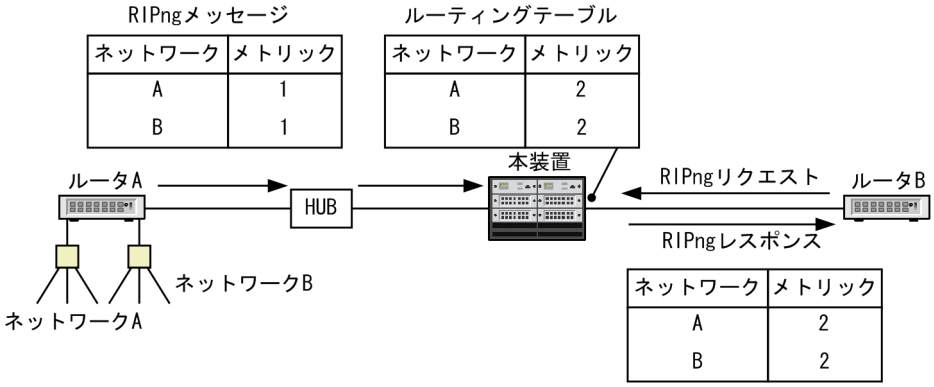


本装置は HUB と本装置間の障害を検出すると，ルーティングテーブルからネットワーク A および B の経路情報を削除します。同時に，ルータ B に対してネットワーク A および B の経路情報をメトリック 16（到達不可）で広告します。

(c)　リクエストパケットに対する応答

本装置はリクエストパケットを受信すると，リクエストパケットを送信した隣接ルータに対して経路情報を広告します。リクエストパケット受信による経路情報の広告を次の図に示します。

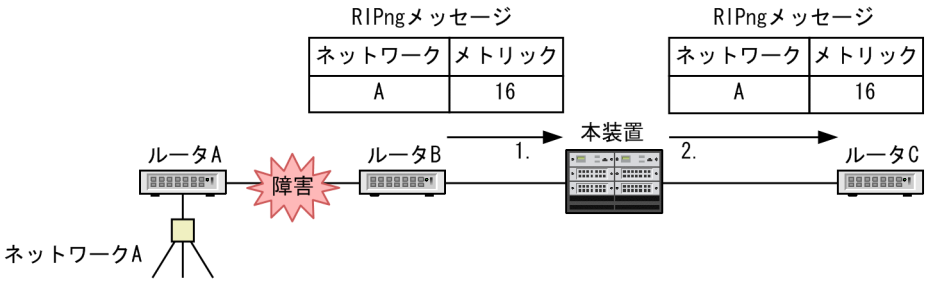
図 16-3　リクエストパケット受信による経路情報の広告



(d)　ルートポイズニング

到達できる状態から到達できない状態（メトリック 16 受信または，インタフェース障害によって該当するインタフェースから学習した経路を削除）となった経路に対して，一定時間（60 秒：ガーベジコレクトタイマ）はメトリック 16（到達できない）で隣接ルータに広告します。ルートポイズニングを次の図に示します。

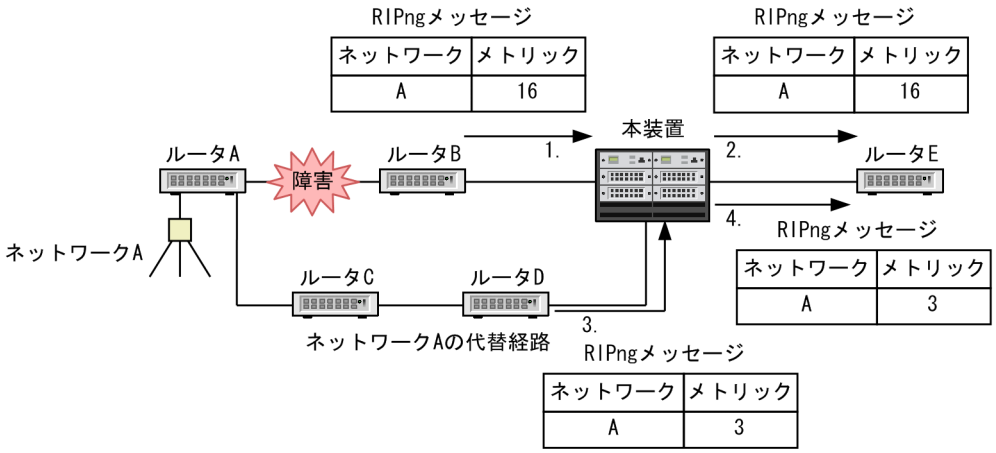
図 16-4　ルートポイズニング



1. 本装置はルータ A とルータ B 間の障害を検出すると，ルータ B からメトリック 16（到達不可）のネットワーク A の経路情報を受信して，ルーティングテーブルからネットワーク A の経路情報を削除します。
2. 1.を受信するとすぐに，本装置はルータ C にメトリック 16（到達不可）のネットワーク A の経路情報を広告します。代替経路が存在しない場合，本装置は該当経路をメトリック 16（到達不可）でルータ C に広告します。

ルートポイズニング期間中に，該当する宛先への新しい経路を再学習した場合は，新しい経路を広告します。ルートポイズニング期間中の再学習を次の図に示します。

図 16-5　ルートポイズニング期間中の再学習



1. 本装置はルータ A とルータ B 間の障害を検出すると，ルータ B からメトリック 16（到達不可）のネットワーク A の経路情報を受信して，ルーティングテーブルからネットワーク A の経路情報を削除します。
2. 同時に，本装置はルータ E にメトリック 16（到達不可）のネットワーク A の経路情報を広告します。
3. 本装置はルータ D からの周期広告でネットワーク A の経路情報を受信して，ルーティングテーブルに追加します。切り替え時間はルータ D の周期広告時間に依存します。
4. 本装置はルータ E に対して，ネットワーク A の経路情報を広告します。

16.1.4　経路情報の学習

(1)　経路情報の学習元

RIPng では，コンフィグレーションコマンド ipv6 rip enable を指定したインタフェースと接続するすべての隣接ルータから，経路情報を学習できます。

(2)　経路情報学習・切り替えのタイミング

RIPng で学習した経路情報の切り替えは，次の表に示す機能が関係します。

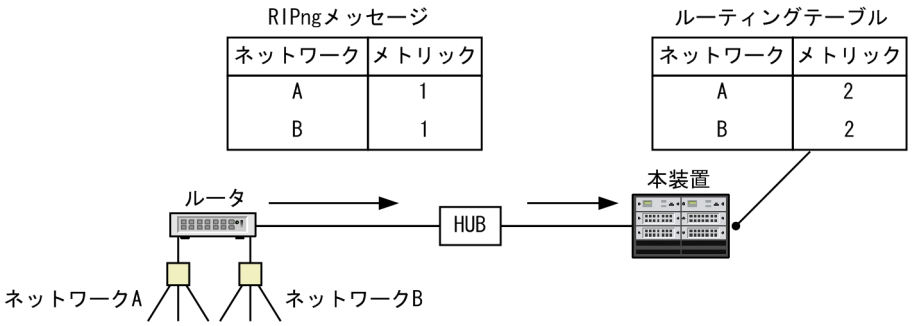
表 16-6　経路情報の学習・切り替えのタイミング

機能	内容
隣接ルータからのレスポンスパケット受信	隣接ルータからの通知に従って，経路情報を追加，変更または削除します。
エージングタイムアウト	隣接ルータから通知された経路情報の周期的な通知が一定時間ない場合に，経路情報を削除します。
インタフェース障害の認識	RIPng が動作しているインタフェースの障害を認識した際に，該当インタフェースから学習した経路情報を削除します。

(a)　レスポンスパケットの受信

RIPng は隣接から受信したレスポンスパケットの経路情報を，自装置のルーティングテーブルに取り込みます。レスポンスパケット受信による経路情報の生成を次の図に示します。

図 16-6　レスポンスパケット受信による経路情報の生成

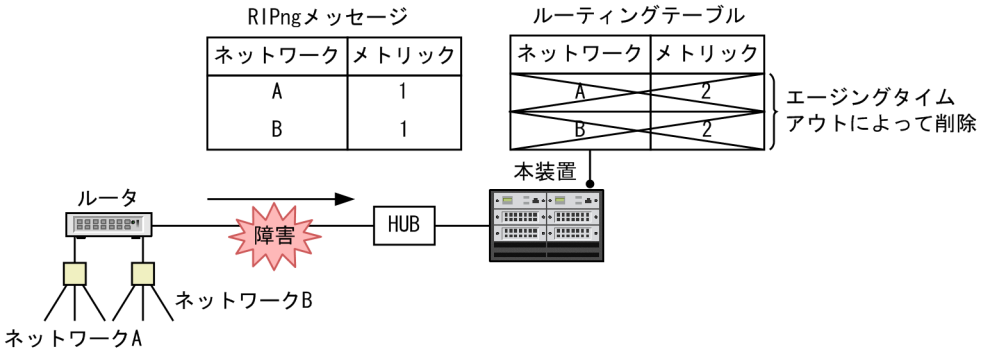


本装置は隣接ルータから学習したネットワーク A および B に関する経路情報を，ルーティングテーブルに追加します。

(b)　エージングタイムアウト

レスポンスパケット受信によって生成された経路情報が最良の経路である場合，自装置のルーティングテーブルに取り込みます。取り込んだ経路情報は**エージングタイマ**によって監視されます。エージングタイマは隣接からの周期的な広告によってリセット（クリア）されます。隣接ルータの障害や自装置と隣接ルータ間の回線障害などによって，隣接から該当する経路情報の広告が 180 秒（エージングタイムアウト値）間発生しない場合，該当する経路情報を自装置のルーティングテーブルから削除します。エージングタイムアウトによる経路情報の削除を次の図に示します。

図 16-7　エージングタイムアウトによる経路情報の削除

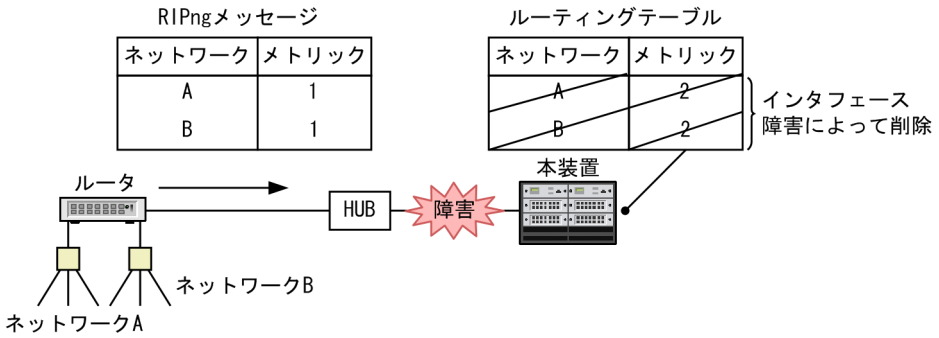


ルータと HUB の間で障害が発生すると，本装置にネットワーク A および B の経路情報が広告されません。本装置は 180 秒（エージングタイムアウト値）間広告のない経路情報を，ルーティングテーブルから削除します。

(c)　インタフェース障害の認識

隣接ルータと接続する自装置のインタフェース障害を認識すると，該当するインタフェースから学習したすべての経路情報を削除します。インタフェース障害による経路情報の削除を次の図に示します。

図 16-8 インタフェース障害による経路情報の削除



本装置は隣接ルータに接続するインタフェースの障害を認識すると，該当するインタフェースから学習したすべての経路情報をルーティングテーブルから削除します。

16.1.5 RIPng の諸機能

RIPng は広告する経路情報に該当する経路のプレフィックス長を設定するため，可変プレフィックス長を取り扱うことができます。RIPng の機能を次に示します。

(1) 認証機能

本装置では認証機能をサポートしていません。

(2) ルートタグ

本装置ではレスポンスメッセージで通知された経路情報のルートタグ情報が設定されている場合，ルーティングテーブルにルートタグ情報を取り込みます。本装置から通知するレスポンスメッセージの経路情報のルートタグ情報はルーティングテーブルの該当する経路のルートタグを設定します。なお，使用できる範囲は 1～65535（10 進数）です。

また，RIPng ではインポート・フィルタでのルートタグ情報によるフィルタ，およびエクスポート・フィルタ（そのほかのプロトコルから RIPng に経路を配布する）でのルートタグ情報の変更はサポートしていません。

(3) プレフィックス

本装置では，レスポンスメッセージで通知された経路情報のプレフィックス長をルーティングテーブルに取り込みます。本装置から通知するレスポンスメッセージの経路情報のプレフィックス長は，ルーティングテーブルの該当する経路のプレフィックス長を設定します。

(4) ネクストホップ

本装置ではレスポンスメッセージで通知された経路情報のネクストホップ情報が設定されている場合，ルーティングテーブルに該当するネクストホップ情報を取り込みます。ネクストホップ情報が設定されていない場合，送信元のゲートウェイをネクストホップとして認識します。

本装置から通知するレスポンスメッセージでは経路情報のネクストホップ情報を設定しません。そのため，本装置から RIPng で経路を受信したルータは，送信インタフェースのアドレスをネクストホップとして使用します。

(5)　リンクローカルマルチキャストアドレスの使用

本装置では RIPng メッセージを受信しないホストでの不要な負荷を軽減するために，リンクローカルマルチキャストアドレスをサポートします。RIPng メッセージの送信時に使用するリンクローカルマルチキャストアドレスは，全 RIPng ルータマルチキャストアドレス（ff02::9）です。

16.1.6　注意事項

RIPng を使用したネットワークを構成する場合には次の制限事項に留意してください。

(1)　RFC との差分

本装置は RFC2080（RIPng バージョン 1）に準拠していますが，ソフトウェアの機能制限から一部 RFC との差分があります。RFC との差分を次の表に示します。

表 16-7　RFC2080 との差分

RFC		本装置
must be zero フィールド	処理については特に明記されていません。	本装置では，must be zero フィールドの値をチェックしません。また，送信時には，must be zero フィールドを 0 にします。
ネットワークプレフィックス	プレフィックス長以降のアドレスフィールドの状態については特に明記されていません。	受信した RIPng パケットで，プレフィックス長以降のアドレスフィールドが 0 にクリアされていない経路情報を受信したときは，プレフィックス長以降のアドレスは 0 にクリアされます。
triggered update	triggered update 後，1～5 秒のランダムタイマを設定するべきであり，タイムアウト前にアップデートを送信する変更があっても，タイムアウトした際にアップデートを行います。	triggerd update 後に 1～5 秒のランダムタイマは設定しないで，経路情報に変更があった際は随時 triggered update を行います。
	triggered update 後の 1～5 秒のランダムタイマ起動中に通常のアップデートがある場合，triggered update は抑止されるかもしれません。	triggered update の抑止は行いません。
スプリットホライズン	スプリットホライズン機能はインタフェース単位で設定変更を可能とするべきです。	本装置ではスプリットホライズン機能のインタフェース単位での設定変更はサポートしていません。
経路のネクストホップ情報指定	経路のネクストホップを明示的に指定できます。	本装置から送信する RIPng パケットにはネクストホップ情報は含まれません。本装置がネクストホップ情報を明示的に指定した RIPng パケットを受信した場合は，その値をネクストホップとして採用します。
応答パケットの送信先	ff02::9 宛てでは不適切な場合（例.NBMA ネットワーク）については実装依存とします。	本装置では，NBMA ネットワークでの RIPng 動作はサポートしていません。

RFC		本装置
認証	IPv6 認証ヘッダおよび暗号化ヘッダを使用してパケットを認証します。	本装置では IPv6 認証ヘッダ，暗号化ヘッダによるパケット認証はサポートしていません。
送信元ポート 521 以外のユニキャストによるリクエストパケット受信時のレスポンスパケット返送	送信元アドレスに対して直接返送できます。	本装置では，送信元アドレスにリンクローカルアドレスを指定したリクエストパケットに対してだけレスポンスパケットを返送します。

16.2　コンフィグレーション

16.2.1　コンフィグレーションコマンド一覧

RIPng のコンフィグレーションコマンド一覧を次の表に示します。

表 16-8　コンフィグレーションコマンド一覧

コマンド名	説明
default-metric	ほかのプロトコルで学習した経路情報を RIPng で広告する場合のメトリック値を指定します。
disable	RIPng が動作しないことを指定します。
distance	RIPng で学習した経路情報のディスタンス値を指定します。
generate-secondary-route	第 2 優先経路をルーティングテーブルに登録します。
inherit-metric	ほかのルーティングプロトコルの経路情報を RIPng で広告する際，メトリック値を引き継ぐことを指定します。
ipv6 rip enable	指定インタフェースで RIPng パケットを送受信を行います。
ipv6 rip metric-offset	指定インタフェースで RIPng パケットを送受信する際に，メトリック値に加算する値を指定します。
ipv6 router rip	RIPng に関する動作情報を設定します。
passive-interface	指定インタフェースからレスポンスパケットを送信しないことを指定します。
timers basic	RIPng の各種タイマ値を指定します。
distribute-list in (RIPng)※	RIPng で学習した経路をルーティングテーブルに取り込むかどうかをフィルタに従って制御します。
distribute-list out (RIPng)※	RIPng で広告する経路をフィルタに従って制御します。
ipv6 prefix-list※	ipv6 prefix-list を設定します。
redistribute (RIPng)※	RIPng で広告する経路のプロトコルを指定します。
route-map※	route-map を設定します。

注※
「コンフィグレーションコマンドレファレンス Vol.3　22. 経路フィルタリング」を参照してください。

16.2.2　RIPng の適用

RIPng パケットを送受信するインタフェースを設定します。

[設定のポイント]

RIPng の適用には，ipv6 rip enable コマンドを使用します。

[コマンドによる設定]

1.
```
(config)# interface gigabitethernet 1/1
(config-if)# ipv6 address 2001:db8:1:1::1/64
```

```
(config-if)# ipv6 enable
```

ポート 1/1 に IPv6 アドレス 2001:db8:1:1::1/64 を設定します。

2. `(config-if)# ipv6 rip enable`

   ポート 1/1 で RIPng パケットの送受信を有効にします。

3. `(config-if)# exit`

   ```
   (config)# interface gigabitethernet 1/2
   (config-if)# ipv6 address 2001:db8:1:2::1/64
   ```

   ポート 1/2 に IPv6 アドレス 2001:db8:1:2::1/64 を設定します。

4. `(config-if)# ipv6 rip enable`

   ポート 1/2 で RIPng パケットの送受信を有効にします。

5. `(config-if)# exit`

16.2.3 メトリックの設定

(1) RIPng 以外の経路情報を広告するときのメトリック値の設定

ほかのプロトコルで学習した経路情報を RIPng で広告する場合のメトリック値を設定します。

[設定のポイント]

RIPng によって OSPFv3 経路または BGP4+経路を広告する場合は，コンフィグレーションによるメトリック値の設定が必須となります。メトリック値の設定には default-metric コマンドを使用します。

[コマンドによる設定]

1.
   ```
   (config)# ipv6 router rip
   (config-rtr-rip)# default-metric 10
   ```

   ほかのプロトコルで学習した経路情報を RIPng で広告する場合のメトリック値として 10 を設定します。

2. `(config-rtr-rip)# redistribute static`

   RIPng でスタティック経路を広告することを設定します。

3. `(config-rtr-rip)# redistribute ospf`

   RIPng で OSPFv3 経路を広告することを設定します。

(2) パケット送受信時にメトリック値に加算する値の設定

RIPng パケットを送受信する際にメトリック値に加算する値を設定します。

[設定のポイント]

特定のインタフェースで送信または受信する経路のメトリック値に加算する値の設定には，ipv6 rip metric-offset コマンドを使用します。

[コマンドによる設定]

1.
   ```
   (config)# interface gigabitethernet 1/1
   (config-if)# ipv6 rip metric-offset 2 out
   ```

   ポート 1/1 から送信する RIPng パケットのメトリック値に 2 を加算する設定をします。

16.2.4 タイマの調整

RIPng の周期広告タイマ値，エージングタイマ値，およびルーティングテーブルから削除するまでの時間を調整します。

経路変更時の収束時間を短縮するためには，周期広告タイマ値，エージングタイマ値をデフォルト値より小さく設定します。また，RIPng の周期広告のトラフィックを少なくしたい場合は周期広告タイマ値をデフォルト値より大きく設定します。

なお，RIPng のタイマ値を変更する場合は，RIPng ネットワーク上のすべてのルータに対しても，同じタイマ値を適用してください。

[設定のポイント]

RIPng のタイマ値の変更には timers basic コマンドを使用します。

[コマンドによる設定]

1. **(config)# ipv6 router rip**
   (config-rtr-rip)# timers basic 40 200 100
   RIPng の周期広告タイマを 40 秒，エージングタイマを 200 秒，ルーティングテーブルから削除するまでの時間を 100 秒に設定します。

16.2.5 VRF での RIPng の適用

VRF で RIPng を適用します。

[設定のポイント]

VRF のインタフェースで ipv6 rip enable コマンドを指定して, RIPng パケットの送受信を有効にします。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   (config-if)# vrf forwarding 2
   (config-if)# ipv6 address 2001:db8:1:1::1/64
   (config-if)# ipv6 enable
   (config-if)# ipv6 rip enable
   (config-if)# exit
   VRF 2 のポート 1/1 に IPv6 アドレス 2001:db8:1:1::1/64 を設定して, RIPng パケットの送受信を有効にします。
2. **(config)# interface gigabitethernet 1/2**
   (config-if)# vrf forwarding 2
   (config-if)# ipv6 address 2001:db8:1:2::1/64
   (config-if)# ipv6 enable
   (config-if)# ipv6 rip enable
   (config-if)# exit
   VRF 2 のポート 1/2 に IPv6 アドレス 2001:db8:1:2::1/64 を設定して, RIPng パケットの送受信を有効にします。
3. **(config)# ipv6 router rip vrf 2**

config-rtr-rip モードへ移行して，VRF 2 で動作する RIPng の情報を指定します。

4. **(config-rtr-rip)# default-metric 10**
   (config-rtr-rip)# redistribute static
   (config-rtr-rip)# exit
   ほかのプロトコルで学習した経路情報を RIPng で広告する場合のメトリック値として 10 を設定します。また，RIPng でスタティック経路を広告する設定をします。

16.3　オペレーション

16.3.1　運用コマンド一覧

RIPng の運用コマンド一覧を次の表に示します。

表 16-9　運用コマンド一覧

コマンド名	説明
show ipv6 route	ルーティングテーブルで保持する経路情報を表示します。
clear ipv6 route	H/W の IPv6 フォワーディングエントリをクリアして再登録します。
show ipv6 rip	RIPng プロトコルに関する情報を表示します。
clear counters rip ipv6-unicast	RIPng プロトコルに関する情報をクリアします。

16.3.2　RIPng の動作状況の確認

RIPng プロトコルに関する情報を表示します。

図 16-9　show ipv6 rip の実行結果

```
> show ipv6 rip
Date 20XX/03/14 12:00:00 UTC
RIPng Flags: <ON>
Default Metric: 10, Distance: 120
Timers (seconds)
  Update             : 40
  Aging              : 200
  Garbage-Collection : 100
```

16.3.3　送信先情報の確認

RIPng の送信先情報を表示します。

図 16-10　show ipv6 rip target の実行結果

```
> show ipv6 rip target
Date 20XX/03/14 12:00:00 UTC
Source Address                          Destination    Flags
fe80::212:e2ff:fe86:5300%Eth1/1         Eth1/1         <Multicast>
fe80::212:e2ff:fe86:5300%Eth1/2         Eth1/2         <Multicast>
```

16.3.4　学習経路情報の確認

(1)　ネットワーク単位の確認

指定ネットワークに含まれる RIPng で学習した，ルーティングテーブルで保持する経路情報を表示します。

図 16-11　show ipv6 rip route の実行結果

```
> show ipv6 rip route brief 2001:db8::/16
Date 20XX/03/14 12:00:00 UTC
Status Codes: * valid, > active, r RIB failure
   Destination                          Interface      Metric Tag   Timer
*> 2001:db8:21f7:2910::/64              Eth1/1         3      0      4s
*> 2001:db8:64b9:4ba6::/64              Eth1/2         4      0     10s
*> 2001:db8:652c:7a78::/64              Eth1/2         3      0      9s
*> 2001:db8:ddd9:158::/64               Eth1/1         5      0      4s
```

(2) ゲートウェイ単位の確認

指定ネットワークに含まれる RIPng で受信した，ルーティングテーブルで保持する経路情報を，ゲートウェイ単位に表示します。

図 16-12 show ipv6 rip received-routes の実行結果

```
> show ipv6 rip received-routes brief 2001:db8::/16
Date 20XX/03/14 12:00:00 UTC
Status Codes: * valid, > active, r RIB failure
Neighbor Address: fe80::212:e2ff:fe86:5301%Eth1/1
   Destination                              Interface      Metric Tag   Timer
*> 2001:db8:21f7:2910::/64                  Eth1/1         3      0      9s
*> 2001:db8:ddd9:158::/64                   Eth1/1         5      0      9s
Neighbor Address: fe80::212:e2ff:fe86:5302%Eth1/2
   Destination                              Interface      Metric Tag   Timer
*> 2001:db8:64b9:4ba6::/64                  Eth1/2         4      0     15s
*> 2001:db8:652c:7a78::/64                  Eth1/2         3      0     14s
```

16.3.5 広告経路情報の確認

指定インタフェースへ送信している経路情報を表示します。

図 16-13 show ipv6 rip advertised-routes の実行結果

```
> show ipv6 rip advertised-routes brief interface gigabitethernet 1/1
Date 20XX/03/14 12:00:00 UTC
Target Interface: Eth1/1
Destination                              Interface      Metric Tag  Age
*> 2001:db8:1:2::/64                     Eth1/2         1      0    22m 37s
*> 2001:db8:64b9:4ba6::/64               Eth1/2         5      0    21s
*> 2001:db8:652c:7a78::/64               Eth1/2         4      0    20s
```

17 OSPF

この章では，IPv4 のルーティングプロトコルの OSPF について説明します。

17.1 OSPF 基本機能の解説

OSPF（Open Shortest Path First）は，ルータ間の接続状態から構成されるトポロジと Dijkstra アルゴリズムによる最短経路計算に基づくルーティングプロトコルです。

17.1.1 OSPF の特長

OSPF は，通常一つの AS 内で経路を決定するときに使用します。OSPF では，AS 内のすべての接続状態から構成するトポロジのデータベースが各ルータにあり，このデータベースに基づいて最短経路を計算します。そのため，OSPF は RIP と比較して，次に示す特長があります。

- 経路情報トラフィックの削減

  OSPF では，ルータ間の接続状態が変化したときだけ，接続状態の情報をほかのルータに通知します。そのため，OSPF は RIP のように定期的にすべての経路情報を通知するルーティングプロトコルと比較して，ルーティングプロトコルが占有するトラフィックが小さくなります。なお，OSPF では 30 分周期で，自ルータの接続状態の情報だけを他ルータに通知します。

- ルーティングループの抑止

  OSPF を使用しているすべてのルータは，同じデータから成るデータベースを保持しています。各ルータは共通のデータに基づいて経路を選択します。したがって，RIP のようなルーティングループ（中継経路の循環）は発生しません。

- コストに基づく経路選択

  OSPF では，宛先まで到達できる経路が複数存在する場合，宛先までの経路上のコストの合計が最も小さい経路を選択します。これによって，RIP と異なり経路へのコストを柔軟に設定できるため，中継段数に関係なく望ましい経路を選択できます。

- 大規模なネットワークの運用

  OSPF では，コストの合計が 16777214 以内の経路を扱えます。そのため，メトリックが 1～15 の範囲である RIP と比較して，より大規模で経由ルータ数の多い経路が存在するネットワークの運用に適しています。

- 可変長サブネット

  OSPF は経路情報にサブネットマスクを含むため，RIP-1 とは異なりサブネット分割してあるネットワークを宛先として取り扱えます。

17.1.2 OSPF の機能

OSPF の機能を次の表に示します。

表 17-1 OSPF の機能

機能	OSPF
AS 外経路のフォワーディングアドレス	○
NSSA	○
認証	○
非ブロードキャスト（NBMA）ネットワーク	○
イコールコストマルチパス	○

機能	OSPF
仮想リンク	○
マルチバックボーン	○
ユニキャストルーティング高可用機能	○
スタブルータ	○

（凡例）　○：取り扱う

本装置では，1 台のルータ上で AS を複数の OSPF ネットワークに分割して，OSPF ネットワークごとに個別に経路の交換，計算，生成ができます。この機能を OSPF マルチバックボーンと呼びます。この独立した各 OSPF ネットワークのことを，OSPF ドメインと呼びます。

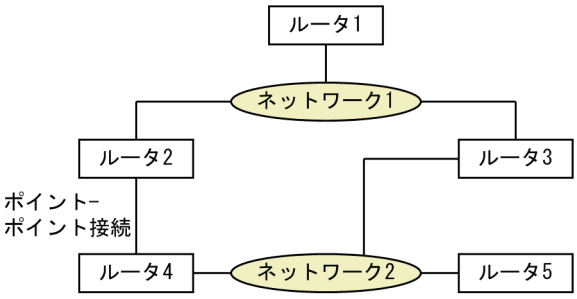
OSPF のコンフィグレーションは，OSPF ドメインごとに設定します。

17.1.3　経路選択アルゴリズム

OSPF では，経路選択のアルゴリズムとして，SPF（Shortest Path First）アルゴリズムを使用します。各ルータには，OSPF が動作しているすべてのルータと，ルーターールータ間およびルーターネットワーク間のすべての接続から成るデータベースがあります。このデータベースから，ルータおよびネットワークを頂点として，ルーターールータ間およびルーターネットワーク間の接続を辺とするトポロジを構成します。このトポロジに SPF アルゴリズムを適用して最短経路木を生成して，これを基に各頂点およびアドレスへの経路を決定します。

ネットワーク構成例を次の図に示します。

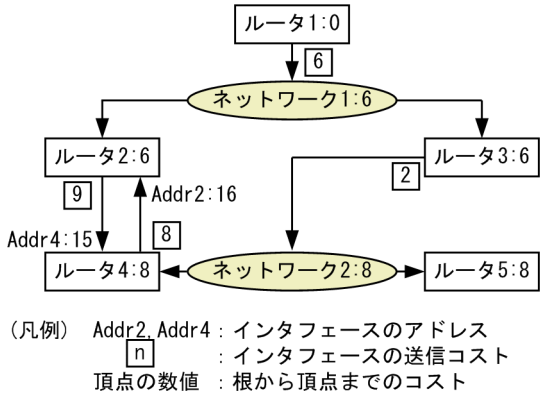
図 17-1　ネットワーク構成例



ルータ 1 を根として生成した最短経路木を次の図に示します。この図では，OSPF のトポロジと，頂点間のコストの設定例を示します。ルーターネットワーク間の接続では，ルータからネットワークへの接続だけにコストを設定できます。ネットワークからルータへのコストは常に 0 です。

ある宛先へのコストは，経路が経由する各インタフェースの送信コストの合計となります。例えば，ルータ 1 からネットワーク 2 宛ての経路のコストは，6（ルータ 1−ネットワーク 1）＋ 0（ネットワーク 1−ルータ 3）＋ 2（ルータ 3−ネットワーク 2）＝ 8 となります。

図 17-2　ルータ 1 を根とする最短木



OSPF では，コストを基に最適な経路を選択します。ある構成で適切ではない経路を選択してしまう場合には，望ましくないネットワークのインタフェースのコストを上げるか，より望ましいネットワークのインタフェースのコストを下げることによって，適切な経路を指示できます。このときコストが小さ過ぎると，コストは 1 未満にできないため，このインタフェースを除く全ルータのインタフェースにかかるコストを上げなければならないことがあります。大規模なネットワークでは，将来最適化するときに任意のインタフェースのコストを減らせるように，インタフェースのコストをあまり小さく設定しないことをお勧めします。

17.1.4　LSA の広告

(1)　LSA の種類

OSPF では経路情報のことを，Link State Advertise（LSA）と呼びます。

主な LSA は，次の三つに分類されます。

(a)　エリア内経路情報

SPF アルゴリズムに使用するルータおよびネットワークの状態を通知します。

(b)　エリア間経路情報

別エリアの経路を通知します。

(c)　AS 外経路情報

OSPF ルータが AS 外の経路情報を認識している場合，この経路を OSPF を使用してそのほかすべての OSPF ルータに通知できます。AS 外経路を OSPF 内に導入するルータを AS 境界ルータと呼びます。

(2)　AS 外経路

コンフィグレーションで経路の再配布フィルタを設定した場合，AS 外経路を広告します。導入元の AS 境界ルータは，次の情報を付加して LSA を広告します。

- メトリック

  メトリックは，経路を学習するルータでほかの LSA との経路選択に使用されます。メトリックのデフォルト値は，default-metric コマンドで設定します。
- メトリックタイプ

Type1 と Type2 の 2 種類があります。Type1 と Type2 の経路では，経路の優先順位，およびメトリックを経路の選択に使用するときの計算方法が異なります。メトリックタイプのデフォルト値は，Type2 です。

- フォワーディングアドレス（転送先）
  転送先として使用する OSPF で到達できるアドレスです。OSPF で到達できない場合 0.0.0.0 を設定します。
- タグ
  付加情報としてタグを広告できます。

(3)　ドメイン間での AS 外経路の広告

1 台のルータが接続している複数の OSPF ドメインは，それぞれ独立した OSPF ネットワークとして動作します。そのため，経路再配布についてのコンフィグレーションの設定がない場合は，一方の OSPF ドメイン上の経路が他方の OSPF ドメインへ配布されません。コンフィグレーションで別ドメインで学習した OSPF 経路の再配布フィルタを設定した場合，別ドメインの経路を AS 外経路として広告します。フィルタ属性には，次の表に示すデフォルト値を適用します。

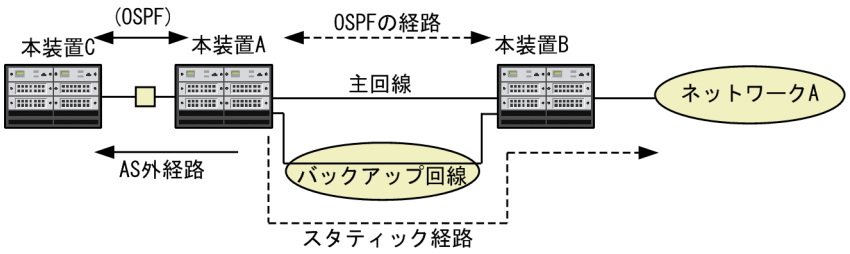
表 17-2　別ドメインの経路を再配布する場合のフィルタ属性

属性	デフォルト値	
	AS 外経路	エリア内，エリア間経路
メトリック値	default-metric コマンドで設定した値。 default-metric 設定がない場合は 20。	default-metric コマンドで設定した値。 default-metric 設定がない場合は 20。
メトリックタイプ	AS 外経路または NSSA 経路の Type2。	
タグ値	経路のタグ値を引き継ぎます。	0

17.1.5　AS 外経路の導入例

バックアップ回線を使用した構成での例を次の図に示します。

図 17-3　バックアップ回線を使用した構成での AS 外経路の導入例



OSPF では，隣接するルータを検出するために，定期的にパケットを交換します。そのため，バックアップ回線を OSPF のトポロジの一部として使用した場合，この回線でパケットを継続して交換するため，バックアップ回線も常に運用状態になります。バックアップ回線上での通信が必要ではない場合にバックアップ回線を休止状態にするには，次のように設定します。

本装置 A では主回線で OSPF を動作させ，バックアップ回線にネットワーク A へのスタティック経路を設定します。さらに，スタティック経路のディスタンス値を，OSPF のエリア内経路のディスタンス値よりも大きな値（優先度が低い）に設定します。これによって，ネットワーク A への経路は OSPF で学習した AS

内経路が選択されます。主回線障害時，本装置 A では該当する AS 内経路が削除されてスタティック経路を再選択しますが，本装置 C ではネットワーク A への経路情報が存在しなくなります。本装置 A でのネットワーク A へのスタティック経路情報を AS 外経路として本装置 C に広告するためには，本装置 A で経路再配布のコンフィグレーションを設定する必要があります。こうすることで，バックアップ回線上で Hello パケットを交換しないで主回線障害時にも OSPF にネットワーク A への有用な経路情報を導入できます。

17.1.6 経路選択の基準

OSPF では，LSA の生成や学習によって LSA が更新されるたびに，SPF 計算を実行します。SPF 計算では SPF アルゴリズムに基づいて経路を選択します。SPF アルゴリズムによって宛先への到達性がなくなった場合，経路を削除します。

エリアボーダルータでは，所属しているすべてのエリアについて，個別に SPF アルゴリズムに基づいて経路を選択します。

OSPF での経路選択の判断基準を，優先順位が高い順に次に示します。なお，この優先順位は変更できません。

1. 経路情報の種類

   OSPF の AS 内経路（エリア内経路，またはエリア間経路）を，AS 外経路より優先します。

2. 学習元ドメイン

   複数ドメインに経路が存在する場合，ディスタンス値が最小である経路を選択します。ディスタンス値が等しい場合，OSPF ドメイン番号が最小の経路を選択します。

3. 経路の宛先タイプ

   - AS 内経路

     エリア内経路を，エリア間経路より優先します。

   - AS 外経路

     エリア内の AS 境界ルータが広告している経路を，別エリアの AS 境界ルータが広告している経路より優先します。

4. AS 外経路タイプ

   メトリックタイプが Type1 の AS 外経路を，Type2 の AS 外経路より優先します。

5. AS 外経路で経由するエリア

   エリアボーダであるルータでは，宛先の AS 境界ルータが複数のエリアに接続している場合，AS 境界ルータまでのコスト値が最も小さいエリアを選択します。コスト値が等しい場合，エリア ID の最も大きいエリアを選択します。

6. コスト

   - AS 内経路

     宛先までのコスト値が最も小さい経路を優先します。

   - Type1 の AS 外経路

     AS 外経路情報のメトリック値と AS 境界ルータまでのコスト値の合計が最も小さい経路を優先します。

   - Type2 の AS 外経路

     AS 外経路情報のメトリック値が最も小さい経路を選択します。メトリック値が等しい場合，AS 境界ルータまでのコスト値が最も小さい経路を選択します。

7. ネクストホップアドレス

ネクストホップアドレスが最も小さいアドレスを選択します。

(1)　ディスタンス値

本装置では，同一宛先への経路が各プロトコルによって複数存在する場合，それぞれの経路のディスタンス値が比較されて優先度の最も高い経路が有効になります。

OSPF では，ディスタンス値のデフォルト値をドメインごとに設定できます。このディスタンス値は，AS 外経路，エリア内経路，エリア間経路で，それぞれ別の値を設定できます。ディスタンス値は，distance コマンドで変更できます。

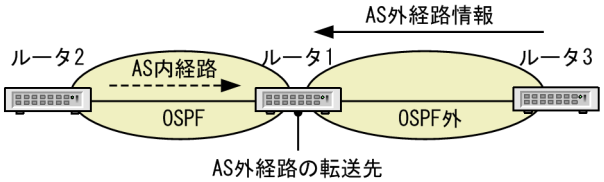
(2)　AS 外経路のネクストホップ選択

AS 外経路の転送先（ネクストホップアドレス）は，OSPF の隣接ルータのアドレス，または LSA で広告しているフォワーディングアドレスのどちらかになります。詳細を次に示します。

(a)　AS 境界ルータを目標とする場合

AS 境界ルータを目標とする場合のシステム構成例を次の図に示します。この例では，ルータ 1 がルータ 3 から学習した経路を AS 外経路として導入するときに，転送先をルータ 1 にします。ルータ 1 までの経路には，AS 内経路選択で選択した経路を使用します。

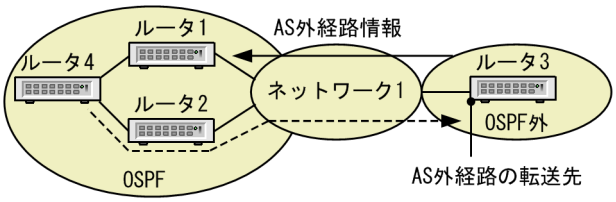
図 17–4　システム構成例（AS 境界ルータを目標とする場合）



(b)　フォワーディングアドレスを目標とする場合

フォワーディングアドレスを目標とする場合のシステム構成例を次の図に示します。この例では，ルータ 1（AS 境界ルータ）がルータ 3 から学習した経路を AS 外経路として導入するときに，転送先をルータ 3 のネットワーク 1 へのインタフェースのアドレス（フォワーディングアドレス）にします。ルータ 4 からネットワーク 1 へ転送する場合，ルータ 2 経由の経路の方がコストが少ないときは，導入した外部経路宛てのパケットの転送にルータ 2 経由の経路を選択します。

図 17–5　システム構成例（フォワーディングアドレスを目標とする場合）

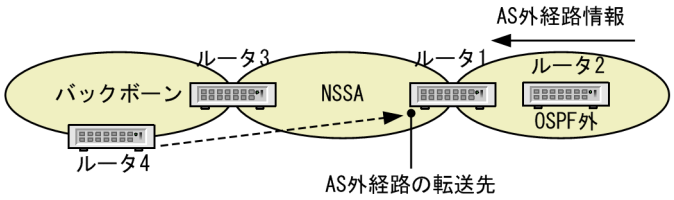


(3)　NSSA 内の AS 外経路のパケット転送先

経路情報を AS 外経路として導入する場合，必ず AS 外経路に転送先アドレスを記します。経路情報の導入元がブロードキャスト型の OSPF インタフェースである場合，転送先は導入元アドレスになります。そのほかの条件では，転送先は NSSA 内の任意のインタフェースアドレスになります。任意のインタフェースを目標とする場合のシステム構成例を次の図に示します。この例では，ルータ 1 がルータ 2 から学習した

経路を AS 外経路として導入するときに，転送先を NSSA 内の任意のインタフェースにします。ルータ 4 は AS 外経路に記された転送先への経路を，エリア間経路選択によって選択します。

図 17-6 システム構成例（任意のインタフェースを目標とする場合）



(4) NSSA についての注意事項

AS 外経路の転送先アドレスは，NSSA 内の OSPF が動作しているインタフェースの中から選択します。インタフェースがダウンした場合は変更します。転送先アドレスの変更後，新しい AS 外経路を広告するまでの間，経路がいったん削除されることがあります。転送先を固定するため，経路情報の導入元であるブロードキャスト型インタフェースを OSPF インタフェースとして設定することをお勧めします。

17.1.7 イコールコストマルチパス

OSPF では，自ルータからある宛先についてイコールコストマルチパスが存在して，次の転送先ルータが複数ある場合，その宛先へのパケットの転送を複数のネクストホップへ分散することによってトラフィックを分散できます。

本装置では，AS 内経路について，学習元ドメインと宛先タイプ（エリア内，またはエリア間経路）とコストが等しい複数のパスを選択します。AS 外経路についても同様に，学習元ドメインと AS 外経路タイプとコストとメトリックが等しい複数のパスを選択します。

maximum-paths コマンドで最大パス数を変更できます。デフォルト値は 4 です。

17.1.8 注意事項

(1) ルータ ID，ネットワークアドレスに関する注意事項

OSPF では，ネットワークのトポロジを構築するときに，ルータの識別にルータ ID を使用します。

ネットワークの設計時に次に示すような不正がある場合，正確なトポロジを構築できません。

- 同一ドメイン内の複数のルータに同じ値のルータ ID を設定した場合
- 異なるネットワークに同一ネットワークアドレスを割り当てた場合

これらの不正がある場合，不正確なトポロジに基づいてネットワーク設計するため，正確な経路選択ができなくなります。ルータ ID の決定方法として，次の方法をお勧めします。

ルータ ID の決定方法

該当ルータで OSPF が動作しているインタフェースに割り当ててある IP アドレスから一つ選択して，これをルータ ID として使用してください（ルータ ID は基本的に任意の 32 ビットの数値です）。この方法を使用すると，OSPF ネットワーク設計時のミスなどによるルータ ID の重複を防げます。

なお，1 台のルータが複数の OSPF ドメインに接続している場合，すべてのドメインで同一のルータ ID を使用しても問題ありません。

(2) 経路の再配布フィルタと学習フィルタの注意事項

OSPF では，隣接ルータから学習したすべての LSA をほかの隣接ルータへ広告します。再配布フィルタによって，OSPF で学習した経路の同一ドメイン内での広告を抑止できません。また，経路集約機能（ip summary-address コマンド）を使用して OSPF 経路を集約する場合，集約元経路の広告を抑止する設定をしても，同一ドメイン内での LSA 広告は抑止されません。

distribute-list in コマンドでは，フィルタ条件に一致する AS 外経路の学習を抑止できます。ただし，LSA の学習，広告を制御できません。そのため，学習しなかった経路も OSPF で広告されます。

(3) マルチバックボーン機能使用時の注意事項

(a) マルチバックボーン使用についての注意

ネットワークを複数の OSPF ドメインに分割して運用した場合，ルーティングループの抑止やコストに基づいた経路選択などの OSPF の特長が，OSPF ドメイン間の経路の選択や配布によって失われます。新規ネットワーク構築時など，ネットワークを複数の OSPF ドメインに分割して運用する必要がない場合は，単一の OSPF ネットワークとして構築することをお勧めします。

(b) 複数ドメインの設定についての注意

ループバックインタフェースに設定したアドレスを複数の OSPF ドメインに広告する必要がある場合は，OSPF AS 外経路として広告してください。コンフィグレーションで，一つのインタフェースを同時に複数の OSPF ドメインに設定できません。

17.2　OSPF 基本機能のコンフィグレーション

17.2.1　コンフィグレーションコマンド一覧

OSPF 基本機能のコンフィグレーションコマンド一覧を次に示します。

表 17-3　OSPF 適用に関係するコンフィグレーションコマンド一覧

コマンド名	説明
disable	OSPF 動作の抑止を設定します。
ip ospf area	インタフェース単位での OSPF 動作制御を設定します。
network	OSPF が動作するネットワークアドレス範囲（アドレスとワイルドカードマスク）と，所属するエリア ID を設定します。
router-id	ルータ ID（ルータの識別子）を設定します。

表 17-4　AS 外経路広告に関係するコンフィグレーションコマンド一覧

コマンド名	説明
default-metric	宛先までのメトリック値を設定します。
suppress-fa	フォワーディングアドレスの広告の抑止を設定します。
distribute-list out (OSPF)※	広告する経路を制御するための再配布フィルタを設定します。
redistribute (OSPF)※	AS 外経路を広告するための再配布フィルタを設定します。

注※
「コンフィグレーションコマンドレファレンス Vol.3　22. 経路フィルタリング」を参照してください。

表 17-5　経路選択や経路学習に関係するコンフィグレーションコマンド一覧

コマンド名	説明
distance ospf	OSPF 経路のディスタンス値を設定します。
ip ospf cost	コスト値を設定します。
maximum-paths	イコールコストマルチパスの最大パス数を設定します。
timers spf	LSA の生成や学習から SPF 計算までの遅延時間および実行間隔を設定します。
distribute-list in (OSPF)※	AS 外経路の学習抑止を設定します。

注※
「コンフィグレーションコマンドレファレンス Vol.3　22. 経路フィルタリング」を参照してください。

17.2.2　コンフィグレーションの流れ

(1)　OSPF 基本機能の設定手順

1. あらかじめ，IP インタフェースを設定します。
2. OSPF を適用する設定をします。

各ルータに，重複しないルータ ID を割り当ててください。

ルータ ID は自動選択させることができます。

3. AS 外経路広告の設定をします。

他プロトコルの経路を OSPF で広告する場合，設定が必要です。

また，マルチバックボーン機能を使用してドメイン間で経路を再配布する場合，設定が必要です。

4. 経路選択の設定をします。

特定のインタフェースを経由する経路に重み付けが必要な場合，ip ospf cost コマンドでコスト値を設定します。

17.2.3 OSPF 適用の設定

[設定のポイント]

network コマンドで指定した範囲に一致するインタフェースアドレスを持つインタフェース上で，隣接ルータと LSA を交換します。

エリア分割をしない場合，エリア ID は全 OSPF ルータで同じ値にしてください。

[コマンドによる設定]

1. **(config)# router ospf 1**

ospf モードへ移行します。ドメイン番号を 1 にします。

2. **(config-router)# router-id 100.1.1.1**

ルータ ID として 100.1.1.1 を使用します。

3. **(config-router)# network 10.0.0.0 0.255.255.255 area 0**

ネットワーク 10.0.0.0/8 の範囲内のインタフェースは，エリア 0 に所属します。

17.2.4 AS 外経路広告の設定

[設定のポイント]

redistribute コマンドでは，再配布経路に付加する情報（メトリック値，タグ，メトリックタイプ）を設定できます。redistribute コマンドでメトリック値の指定を省略した場合，default-metric コマンドの設定値が有効になります。

なお，OSPF で学習した経路について，同一ドメイン内での経路の再配布は制御できません。また，suppress-fa コマンドを指定した場合，フォワーディングアドレスは 0.0.0.0（固定）になります。

[コマンドによる設定]

1. **(config)# router ospf 1**

ospf モードへ移行します。

2. **(config-router)# default-metric 10**

デフォルトメトリックを 10 に設定します。

3. **(config-router)# redistribute static**

スタティック経路を上記のデフォルトメトリック値で広告します。

17.2.5 経路選択の設定

[設定のポイント]

コストの設定は ip ospf cost コマンドを使用して，インタフェース単位で設定します。

なお，maximum-paths コマンドで 1 を設定した場合，経路のコスト値が等しい場合でも，イコールコストマルチパスを構築しません。

ここでは，シングルパスの経路を使用する場合の設定例を示します。

[コマンドによる設定]

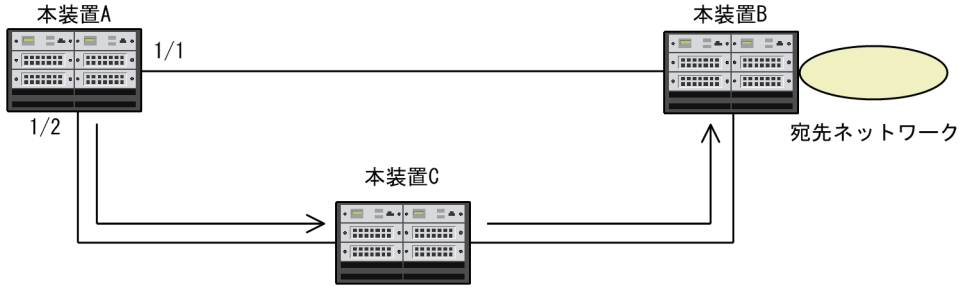
1. **(config)# router ospf 1**
   (config-router)# maximum-paths 1
   OSPF 最大パス数を 1 に設定します。
2. **(config-router)# network 10.0.0.0 0.255.255.255 area 0**
   (config-router)# exit
   ネットワーク 10.0.0.0/8 の範囲内のインタフェースは，エリア 0 に所属します。
3. **(config)# interface gigabitethernet 1/1**
   (config-if)# ip ospf cost 10
   (config-if)# exit
   コストを 10 に設定します。
4. **(config)# interface gigabitethernet 1/2**
   (config-if)# ip ospf cost 2
   コストを 2 に設定します。ポート 1/2 のコスト値をポート 1/1 のコスト値よりも小さくすることによって，ポート 1/2 を経由する経路が優先されます。

17.2.6 マルチパスの設定

[設定のポイント]

コスト値を調整することで，経路が経由するルータ数に関係なく，宛先へのイコールコストマルチパスを構築できます。

図 17-7 マルチパスの構成



本装置 C を経由する場合，宛先までのコストは 2 です。ここでは，本装置 A でイコールコストマルチパスを構築する例を示します。

[コマンドによる設定]

1. **(config)# router ospf 1**
   (config-router)# network 10.0.0.0 0.255.255.255 area 0

(config-router)# exit

ネットワーク 10.0.0.0/8 の範囲内のインタフェースは，エリア 0 に所属します。

2. **(config)# interface gigabitethernet 1/1**

   (config-if)# ip ospf cost 2

   ポート 1/1 のコスト値を 2 とすることで，ポート 1/2 を経由する経路とコストを等しくします。

17.2.7 VRF での OSPF の適用

[設定のポイント]

router ospf コマンドで，vrf パラメータを指定します。ループバックアドレスをルータ ID として使用して，VRF 2 で OSPF を適用します。

[コマンドによる設定]

1. **(config)# interface loopback 2**

   インタフェースモードへ移行して，ループバック 2 の情報を指定します。

2. **(config-if)# vrf forwarding 2**

   (config-if)# ip address 172.16.1.1

   VRF 2 を指定して，IP アドレスを 172.16.1.1 にします。

3. **(config-if)# ip ospf 1 area 0**

   (config-if)# exit

   ドメイン 1 のエリア 0 で動作することを指定します。

4. **(config)# router ospf 1 vrf 2**

   ospf モードへ移行して，VRF 2 で動作する OSPF の情報を指定します。ドメイン番号を 1 にします。

5. **(config-router)# network 10.0.0.0 0.255.255.255 area 0**

   ネットワーク 10.0.0.0/8 の範囲内のインタフェースは，エリア 0 に所属します。

17.3 インタフェースの解説

17.3.1 OSPF インタフェース種別

OSPF では，OSPF パケットの送受信上，ルータ間を接続するインタフェースを 3 種類に分類します。

- ブロードキャスト
  ブロードキャスト型ネットワーク上で，マルチキャストを使用してインタフェース上の複数の近隣ルータを統一的に管理します。
- non-broadcast（NBMA）
  ブロードキャスト型ネットワーク上で，ブロードキャストやマルチキャストを使用しないで複数の近隣ルータを統一的に管理します。
- ポイントーポイント
  近隣ルータを 1 台だけ管理します。なお，仮想リンク上では，ポイントーポイントインタフェースとして動作します。

(1) マルチホーム・ネットワーク

本装置では，インタフェースに設定したセカンダリアドレス上でも OSPF を動作させることができます。このような構成で，マルチホーム接続されたルータ間で複数の IP ネットワーク上で OSPF を使用する場合，次のことに注意してください。

- NBMA でないインタフェースでは，マルチキャストアドレスで指定されたルーティングパケットがマルチホーム接続されたすべてのルータに対して送信されるため，ルータやネットワークに不要な負荷が掛かります。ネットワークに不要なトラフィックを増やしたくない場合，NBMA インタフェースにしてください。

(2) OSPF を使用するインタフェースの設定についての注意事項

OSPF では，インタフェースに設定してある送信時パケットの最大長（MTU）と同じ長さのパケットを送信する場合があります。ここで，受信側のインタフェースに設定してある受信時パケットの最大長（MRU：特に記述がなければ MTU と同一）よりも長い場合，通常のトラフィックでは顕在化しないルータ間の相互通信不可能の問題が発生することがあります。そのため，OSPF を使用する場合は，特にすべてのネットワークおよびネットワークに接続しているすべてのルータのインタフェースについて，MTU がほかのすべてのインタフェースの MRU 以下に設定してあることの確認をお勧めします。

17.3.2 隣接ルータとの接続

(1) Hello パケット

OSPF が動作しているルータは，ルータ間の接続性を検出するため，インタフェースごとに Hello パケットを送信します。Hello パケットを他ルータから受信することで，ルータ間で OSPF が動作していることを認識します。

(2) 隣接ルータとの接続条件

ルータ間を直接接続するネットワークのそれぞれで，接続するルータのインタフェースでのパラメータは，次に示す項目が一致している必要があります。これが一致していないルータ間では，OSPF 上は接続していないことになります。

(a) インタフェースアドレス

同一ネットワークへ接続しているすべてのルータのインタフェースは，IP ネットワークアドレスとマスクが同じである必要があります。

(b) 認証の方式と認証の鍵

OSPF では，接続しているルータからの経路情報がそのルータからの正しいものかどうかを検証するために，認証を使用できます。認証を使用する場合は，同一ネットワークへ接続しているすべてのルータの，このネットワークへのインタフェースに設定した認証方式と鍵が一致している必要があります。

(c) エリア ID

ルータ間の直接接続では，両ルータのインタフェースに設定したエリアが一致している必要があります。

(d) Hello Interval と Dead Interval

Hello Interval は Hello パケットの送信間隔です。Dead Interval は，あるルータからの Hello パケットを受信できないことを理由にそのルータとの接続が切れたと判断するまでの時間です。検出と切断を適切に判断するためには，直接接続しているルータのインタフェースに設定した，この二つの値が一致している必要があります。

(e) エリアの設定

スタブエリアと NSSA，そのどちらでもないエリアとでは，エリアに通知される情報が異なります。そのため，OSPF が二つのルータを直接接続していると判断するには，インタフェースが所属しているエリアのスタブについての設定が一致している必要があります。

17.3.3 ブロードキャスト型ネットワークと指定ルータ

ブロードキャスト型ネットワークでは，トポロジ上の頂点であるネットワークとネットワークに直接接続しているルータ間の接続情報を管理するために，指定ルータ（Designated Router）とバックアップ指定ルータを選択します。指定ルータの障害時には，ネットワークの接続情報の管理ルータを速やかに移行するために，バックアップ指定ルータが指定ルータになります。

(1) 指定ルータおよびバックアップ指定ルータの選択

各ルータは，Hello パケットで該当するインタフェース上での指定ルータになる優先度（priority）を広告します。

インタフェース上に指定ルータもバックアップ指定ルータも存在しない場合は，最も priority の高いルータを指定ルータに選択します。指定ルータは存在するがバックアップ指定ルータが存在しない場合，指定ルータを除いて最も priority の高いルータをバックアップ指定ルータに選択します。両ルータとも存在する場合，新しくより priority の高いルータが現れても，選択は変更しません。

あるルータのあるインタフェースの priority を 0 に設定すると，このルータは該当するインタフェースが接続しているエリアでは，指定ルータにもバックアップ指定ルータにも選択されません。

ブロードキャスト型ネットワーク上に複数のルータがあり，このネットワークをトラフィックの転送に使用する場合は，どれかのルータのネットワークに接続しているインタフェースの priority を 1 以上にする必要があります。

17.3.4 LSA の送信

OSPF では, 隣接ルータとの間で互いに所持していない LSA を送信し合います。新たに LSA を生成または受信した場合，これを全隣接ルータに送信します。これによって，本装置と隣接ルータとの間で同じデータベースを保持するようにします。LSA の送受信によってデータベースの同期をとる関係を隣接関係と呼びます。

LSA 同期手順によって，本装置の LSA はすべての隣接ルータに送信されます。また，隣接ルータでは，隣接ルータのすべての隣接ルータに本装置の LSA を送信します。隣接ルータの隣接ルータでは，さらにその全隣接ルータに LSA を送信します。この手順によって, 本装置の LSA は該当エリア上の全ルータに配布されます。

(1) LSA の Age

Age は LSA を生成してからの経過時間です。Age が 3600 秒になるか，生成元のルータによって削除されるまで, LSA を保持します。保持している LSA の Age に遅延時間（ip ospf transmit-delay コマンドの設定値）を加算した値が，送信する LSA の Age フィールド値になります。

17.3.5 パッシブインタフェース

OSPF の隣接ルータが存在しないインタフェースをパッシブインタフェースとして設定できます。また，ループバックインタフェースに OSPF を適用した場合，パッシブインタフェースになります。

パッシブインタフェースでは，OSPF パケットを送受信しません。

パッシブインタフェースの直結経路を，エリア内経路またはエリア間経路として広告します。

17.4　インタフェースのコンフィグレーション

17.4.1　コンフィグレーションコマンド一覧

OSPF パケット，NBMA 設定に関するコンフィグレーションコマンド一覧を次の表に示します。

表 17-6　コンフィグレーションコマンド一覧

コマンド名	説明
ip ospf dead-interval	隣接ルータから Hello パケットを受信できなくなったときに隣接関係を維持する時間を設定します。
ip ospf hello-interval	Hello パケットの送信間隔を設定します。
ip ospf network	インタフェース種別（ブロードキャスト，NBMA またはポイントーポイント）を設定します。
ip ospf priority	指定ルータになる優先度を設定します。
ip ospf retransmit-interval	LSA の再送間隔を設定します。
ip ospf transmit-delay	OSPF パケットを送信するのに必要な遅延時間を設定します。
message-size (OSPF)	本装置が送信する OSPF パケットの最大長を設定します。
neighbor (OSPF)	隣接ルータのアドレスを設定します。
passive-interface (OSPF)	パッシブインタフェースを設定します。

OSPF 動作に関係するコンフィグレーションコマンド一覧を次の表に示します。

OSPF では，エラーパケット受信，OSPF 状態変更の SNMP 通知を送信できます。

表 17-7　コンフィグレーションコマンド一覧（OSPF 動作に関係するコマンド）

コマンド名	説明
snmp-server host※1	SNMP 通知を送信する宛先のネットワーク管理装置を設定します。
system mtu※2	装置の MTU を設定します。
ip mtu※3	インタフェースでの送信 IP MTU 長を設定します。
interface loopback※4	ループバックインタフェースを設定します（OSPF のパッシブインタフェースとして使用できます）。

注※1
「コンフィグレーションコマンドレファレンス Vol.1　14. SNMP」を参照してください。

注※2
「コンフィグレーションコマンドレファレンス Vol.1　16. イーサネット」を参照してください。

注※3
「コンフィグレーションコマンドレファレンス Vol.3　2. IPv4・ARP・ICMP」を参照してください。

注※4
「コンフィグレーションコマンドレファレンス Vol.3　4. ループバックインタフェース」を参照してください。

17.4.2 コンフィグレーションの流れ

(1) NBMA インタフェースの設定手順

1. あらかじめ，IP インタフェースを設定します。
2. 基本機能を設定します。
   OSPF を適用する設定などをします。詳細は，「17.2 OSPF 基本機能のコンフィグレーション」を参照してください。
3. インタフェースを設定します。
   ip ospf network コマンドで，インタフェースの種別を NBMA に設定します。
   必要に応じて，Hello パケットの送信間隔などのパラメータを変更します。
4. neighbor コマンドで，隣接ルータを設定します。

(2) ブロードキャストインタフェースの設定手順

1. あらかじめ，IP インタフェースを設定します。
2. 基本機能を設定します。
   OSPF を適用する設定などをします。詳細は，「17.2 OSPF 基本機能のコンフィグレーション」を参照してください。
3. インタフェースを設定します。
   Hello パケットの送信間隔などのパラメータを変更できます。

17.4.3 NBMA での隣接ルータの設定

[設定のポイント]

neighbor コマンドは，NBMA インタフェースでだけ有効になります。

neighbor コマンドの priority パラメータで，隣接ルータの指定ルータになる資格の有無を指定します。priority が 0 の場合，指定ルータになる資格がないことを意味します。隣接ルータが指定ルータになる資格がある場合，必ず priority を指定してください。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   (config-if)# ip ospf 1 area 0
   OSPF を適用します。
2. **(config-if)# ip ospf network non-broadcast**
   (config-if)# exit
   インタフェースの種別を NBMA に設定します。
3. **(config)# router ospf 1**
   (config-router)# neighbor 192.168.1.1 priority 2
   (config-router)# neighbor 192.168.1.2 priority 2
   ドメイン内の隣接ルータのインタフェースアドレスを設定します。同時に，隣接ルータの priority を 2 に設定します。

17.4.4 インタフェースパラメータ変更の設定

OSPF を適用したインタフェースでは，コンフィグレーションのデフォルト値に従って Hello パケットの送信などをします。priority や passive-interface コマンドを設定することで，動作を変更できます。

(1) 指定ルータになる優先度

接続しているルータ数が多いネットワークでは，指定ルータの負荷は高くなります。そのため，このようなネットワークに複数接続しているルータが存在する場合，このルータが複数のネットワークの指定ルータにならないように priority を設定することをお勧めします。

[設定のポイント]

priority は，値が大きいほど優先度が高くなります。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   (config-if)# ip ospf 1 area 0
   (config-if)# ip ospf priority 10
   priority を 10 に設定します。

(2) パッシブインタフェース

[設定のポイント]

passive-interface コマンドを使用します。ip ospf cost コマンドを指定した場合，指定したコスト値で直結経路を広告します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/2**
   (config-if)# ip ospf 1 area 0
   (config-if)# ip ospf cost 10
   (config-if)# exit
   OSPF を適用します。
2. **(config)# router ospf 1**
   (config-router)# passive-interface gigabitethernet 1/2
   ポート 1/2 をパッシブインタフェースに設定します。

17.5 OSPF のオペレーション

17.5.1 運用コマンド一覧

OSPF の運用コマンド一覧を次の表に示します。

表 17-8 運用コマンド一覧

コマンド名	説明
show ip route	ルーティングテーブルに登録されている内容を表示します。
clear ip route	H/W の IPv4 フォワーディングエントリをクリアして再登録します。
show ip ospf	ドメイン，隣接ルータ情報，インタフェース情報，LSA などを表示します。
clear ip ospf	OSPF プロトコルに関する情報をクリアします。
show ip vrf	VRF の IPv4 情報を表示します。
show ip interface ipv4-unicast	ユニキャストルーティングプログラムが認識している本装置の IPv4 インタフェース情報を表示します。

17.5.2 ドメインの確認

OSPF が動作中の場合，ルータ ID やディスタンス値などの設定内容は show ip ospf コマンドで確認します。

図 17-8 show ip ospf コマンドの実行結果

```
>show ip ospf
Date 20XX/03/14 12:00:00 UTC
Domain: 1
Router ID: 172.16.1.1
Distance:
  Intra Area: 10, Inter Area: 10, External: 150
Flags: <AreaBorder ASBoundary>
SPF Interval: 7s, SPF Delay: 3s
Area            Interfaces  Network Range      State
0               1           -                  -
10              1           192.168.1/24       Advertise
                            172.19/18          DoNotAdvertise
```

17.5.3 隣接ルータ情報の確認

隣接ルータの IP アドレス（Address），隣接状態（State），ルータ ID（Router ID），Priority は，show ip ospf neighbor コマンドで確認します。

OSPF インタフェースでは，指定ルータ（Designated Router）とそのほかのルータの間で隣接関係を確立します。この進行状況は，隣接状態によって確認できます。

隣接関係が確立した場合，隣接状態は Full になります。Full でない状態では，隣接関係を確立している途中であり，そのインタフェースでは OSPF 経路を学習しません。

詳細は，show ip ospf interface または show ip ospf neighbor detail コマンドで確認します。インタフェース状態（State）や Network Type，隣接ルータとの接続性を確認できます。

- Network Type の OSPF ネットワーク種別が，隣接ルータの OSPF ネットワーク種別と同じであることを確認してください。
- インタフェースの状態が DR または P to P の場合，Neighbor List 内の全隣接ルータ状態が Full となっていることを確認してください。
  - Full でない場合，隣接ルータとの隣接関係が確立していません。隣接ルータを調査してください。
- インタフェースの状態が BackupDR または DR Other の場合，Neighbor List 内に DR となる隣接ルータが存在するか確認してください。
  - DR が存在して DR の隣接ルータ状態が Full でない場合，DR との隣接関係が確立していません。隣接ルータを調査してください。
  - DR が存在しない場合は，自装置および隣接ルータの Priority が設定されていない可能性があります。自装置および隣接ルータの Priority を確認してください。

図 17-9 show ip ospf neighbor コマンドの実行結果

```
>show ip ospf neighbor
Date 20XX/03/14 12:00:00 UTC
Domain: 1
Area: 0
Address         State               RouterID      DeadTime Interface
172.16.10.11    Full/BackupDR        172.16.1.1         10  172.16.10.10
172.16.10.12    Full/DR Other        172.16.1.2         20  172.16.10.10
172.26.110.111  Exch Start/BackupDR  172.26.123.111      5  172.26.120.130
```

図 17-10 show ip ospf interface コマンド（IP アドレス指定）の実行結果

```
>show ip ospf interface 192.168.50.1
Date 20XX/05/30 12:00:00 UTC
Domain: 1
Index: 2, Name: Eth1/1, Address: 192.168.50.1, State: BackupDR
Auth Type: Simple
MTU: 1436, DDinPacket: 70, LSRinPacket: 117, ACKinPacket: 70
Router ID: 192.168.50.1, Network Type: Broadcast
Area: 0, DR: 172.17.1.1, Backup DR: 172.16.1.1
Priority: 0, Cost: 1
Transmit Delay: 1s
Intervals:
  Hello: 10s, Dead: 40s, Retransmit: 5s

Neighbor List (1):
Address         State      RouterID     Priority DR             Backup DR
192.168.50.2    Full       192.168.50.2    0     none           none
>
```

図 17-11 show ip ospf neighbor コマンド（detail パラメータ指定）の実行結果

```
>show ip ospf neighbor detail
Date 20XX/05/30 12:00:00 UTC
Domain: 1
Area: 0
Interface Address: 172.16.10.10, Interface State: BackupDR
    Interface Name: Eth1/2
    Neighbor Router ID: 172.16.1.1, Neighbor State: Full/DR
    Neighbor Address: 172.16.10.11, Priority: 1, Poll Interval: 0s
    DeadTime: 6s, Up: 1d 12h, Adjacent: 1d 12h
    DR: 172.16.10.11, Backup DR: 172.16.10.10
    DS: 0, LSR: 0, Retrans: 0, <Master>
    Track Name: -, Track ID: -, Track State: -

    Neighbor Router ID: 172.16.1.2, Neighbor State: Full/DR Other
    Neighbor Address: 172.16.10.12, Priority: 1, Poll Interval: 0s
    DeadTime: 36s, Up: 10h 11m, Adjacent: 10h 11m
    DR: 172.16.10.11, Backup DR: 172.16.10.10
    DS: 0, LSR: 0, Retrans: 0, <>
    Track Name: -, Track ID: -, Track State: -
>
```

17.5.4 インタフェース情報の確認

OSPF が動作しているインタフェースのアドレス（Address），状態（State），Priority，コスト値（Cost）などは，show ip ospf interface コマンドで確認します。

なお，IP インタフェースがダウンしている場合，インタフェースの情報は表示されません。

図 17-12 show ip ospf interface コマンドの実行結果

```
>show ip ospf interface
Date 20XX/03/14 12:00:00 UTC
Domain: 1
Area 0
Address         State    Priority Cost  Neighbor DR              Backup DR
172.16.10.10    DR       1        1     1        172.17.1.1      172.16.1.1
Area 1
Address         State    Priority Cost  Neighbor DR              Backup DR
172.18.10.11    DR       1        1     1        172.18.1.1      172.16.1.1
```

17.5.5 LSA の確認

(1) LSA の数の確認

OSPF で保持している LSA の数は，show ip ospf database database-summary コマンドで確認します。

図 17-13 show ip ospf database database-summary コマンドの実行結果

```
>show ip ospf database database-summary
Date 20XX/03/14 12:00:00 UTC

Domain: 1
Local Router ID: 172.16.1.1
Area            Router Network Summary Asb-     NSSA   Area   External Opaque-
                                       summary         Total           link
0               4      2       1       2        0      9      2        1
```

(2) LSA の広告情報の確認

show ip ospf database コマンドでは LSA の一覧を表示して，LSA の種別ごとに LSA の広告情報や Age を確認できます。

本装置が次に示す LSA を広告していることを確認してください。

1. Router Link を広告していること
   表示される LSID はルータ ID です。
2. 本装置が指定ルータとなっているインタフェースのアドレスを，Network Link として広告していること
   表示される LSID はインタフェースアドレスです。
3. 本装置が AS 境界ルータである場合，広告対象の経路を AS External Link として広告していること

図 17-14 show ip ospf database コマンドの実行結果

```
>show ip ospf database
Date 20XX/03/14 12:00:00 UTC

Domain: 1
Local Router ID: 10.1.2.8
Area : 1
  LS Database: Router Link
   Router ID          LSID            ADV Router      Age  Sequence Link Count
   10.1.2.8           10.1.2.8        10.1.2.8        3    80000021 1
   10.1.10.11         10.1.10.11      10.1.10.11      2    80000002 1
```

```
LS Database: Network Link
 DR Interface       LSID            ADV Router          Age  Sequence
 100.1.2.2/24       100.1.2.2       10.1.2.8            3    80000001

LS Database: AS External Link
 Network Address    LSID            AS Boundary Router Age  Sequence
 10.1.1.0/24        10.1.1.0        10.1.2.8           778  80000005
```

18 OSPF 拡張機能

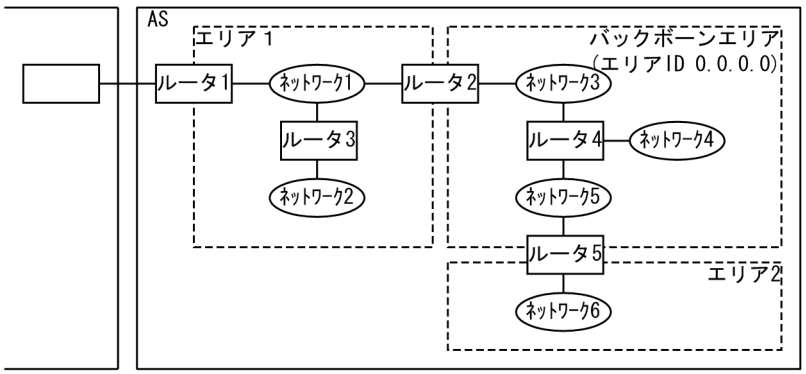
この章では，OSPF の拡張機能について説明します。

18.1　エリアとエリア分割機能の解説

18.1.1　エリアボーダ

OSPF では，ルーティングに必要なトラフィックと，経路選択に使用するアルゴリズムの処理に必要な時間を削減するために，AS を複数のエリアに分割できます。エリア分割を使用した OSPF ネットワークトポロジの例を次の図に示します。

図 18-1　エリア分割を使用した OSPF ネットワークトポロジの例



ルータ 2 やルータ 5 のように，複数のエリアに所属するルータをエリアボーダルータと呼びます。

あるエリア内の接続状態の情報は，ほかのエリアには通知されません。また，ルータには，接続していないエリアの接続状態の情報はありません。

(1)　バックボーン

エリア ID が 0 であるエリアをバックボーンと呼びます。AS が複数のエリアに分割されている場合，バックボーンには特別な役割があります。AS を複数のエリアに分割する場合は，エリアのどれか一つをバックボーンエリアとして設定する必要があります。ただし，一つの AS にバックボーンを二つ以上ある構成にしないでください。そのような構成の場合，情報がそれぞれのバックボーンに分散されるため，到達不能である経路が発生したり，最適な経路を選択しなかったりすることがあります。

エリアボーダルータは，バックボーンを通じてエリア間の経路情報を交換するため，必ずバックボーンに所属する必要があります。

(2)　エリア分割についての注意事項

エリア分割をすると，ルータや経路情報トラフィックの負荷が減る一方で，OSPF のアルゴリズムが複雑になります。特に，障害に対して適切な動作をする構成が困難になります。ルータやネットワークの負荷に問題がない場合は，エリア分割をしないことをお勧めします。

(3)　エリアボーダルータについての注意事項

- エリアボーダルータでは，所属しているエリアの数だけ SPF アルゴリズムを動作させます。エリアボーダルータには，あるエリアのトポロジ情報を要約してほかのエリアへ通知する機能があります。そのため，所属するエリアの数が多くなるとエリアボーダルータの負荷が高くなります。そのため，エリアボーダルータにあまり多くのエリアを所属させないようなネットワーク構成にすることをお勧めします。

- あるエリアにエリアボーダルータが一つしかない場合，このエリアボーダルータに障害が発生すると，バックボーンから切り放されてほかのエリアとの接続性が失われます。重要な機能を提供するサーバや重要な接続のある AS 境界ルータの存在するエリアには複数のエリアボーダルータを配置して，エリアボーダルータの配置に対して十分な迂回路が存在するように，ネットワークを構築することをお勧めします。

18.1.2　エリア分割した場合の経路制御

エリアボーダルータは，バックボーンを除くすべての所属しているエリアの経路情報を要約した上で，バックボーンに所属するすべてのルータへ通知します。また，バックボーンの経路情報の要約と，バックボーンに流れている要約されたほかのエリアの経路情報を，バックボーン以外の接続しているエリアのルータへ通知します。

あるルータが，あるアドレスについて要約された経路情報を基に経路を決定した場合，このアドレス宛ての経路は要約された経路情報の通知元であるエリアボーダルータを経由します。そのため，異なるエリア間を結ぶ経路は必ずバックボーンを経由します。

エリアボーダルータでは，あるエリアの経路情報をほかのエリアに広告するに当たってルータやネットワーク間の接続状態と接続のコストによるトポロジ情報を，エリアボーダルータからルータやネットワークへのコストに要約します。これらの要約された情報をエリア間経路情報と呼びます（ネットワークの情報は Type3LSA で，AS 境界ルータの情報は Type4LSA で広告します）。

(1)　エリアボーダルータでの経路の集約

経路の集約および抑止とエリア外への要約を次の表に示します。

表 18-1　経路の集約および抑止とエリア外への要約

エリア内のネットワークアドレス	集約および抑止の設定	エリア外へ通知する要約
10.0.1.0/24 10.0.2.0/25 10.0.2.128/25 10.0.3.0/24	なし	10.0.1.0/24 10.0.2.0/25 10.0.2.128/25 10.0.3.0/24
10.0.1.0/24 10.0.2.0/25 10.0.2.128/25 10.0.3.0/24	10.0.0.0/23 10.0.2.0/24	10.0.0.0/23 10.0.2.0/24 10.0.3.0/24
10.0.1.0/24 10.0.2.0/25 10.0.2.128/25 10.0.3.0/24 192.168.3.0/26 192.168.3.64/26 192.168.3.128/26	10.0.0.0/8 （抑止） 192.168.3.0/24	192.168.3.0/24

エリアボーダルータでのエリア内のトポロジ情報を要約するに当たって，アドレスの範囲をコンフィグレーションで設定するとその範囲に含まれる経路情報を一つに集約できます。アドレスの範囲は，area range コマンドでマスク付のアドレスを設定します。また，広告を抑止するパラメータを指定できます。

コンフィグレーションで設定したマスク付アドレスの範囲に含まれるネットワークがエリア内一つでもあった場合, 範囲に含まれるすべてのネットワークをこのマスク付アドレスを宛先とする経路情報へ集約してほかのエリアへ通知します。範囲に含まれる各ネットワークは, このエリアボーダルータからほかのエリアへは通知されません。このとき, 集約した経路情報のコストには範囲に含まれるネットワーク中の最も大きなコストを使用します。

広告を抑止した場合，範囲内の各ネットワークをほかのエリアへは通知しない上に，マスク付アドレスに集約した経路もほかのエリアへは通知しません。この結果, ほかのエリアからはこのエリアボーダルータ経由で指定した範囲に含まれるアドレスへの経路は存在しないように見えます。

18.1.3　スタブエリア

バックボーンではなく，AS 境界ルータが存在しないエリアをスタブエリアとして設定できます。この設定にはコンフィグレーションコマンド area stub を使用します。

AS 外経路は，スタブエリアとして設定したエリアに広告されません。これによってスタブエリア内では経路情報を減らして，ルータの情報の交換や経路選択の負荷を減らせます。エリアボーダルータは，AS 外経路の代わりとして，スタブエリアにデフォルトルートを導入します。

area stub コマンドで no-summary パラメータを指定した場合，エリア外の経路（エリア間経路情報）の広告を抑止します（エリア外への経路はデフォルトルートだけとなります)。

18.1.4　NSSA

バックボーンではないエリアを NSSA として設定できます。この設定にはコンフィグレーションコマンド area nssa を使用します。

スタブエリアと同様に，NSSA ではほかのエリアで学習した AS 外経路は広告されません。

広告経路フィルタ（コンフィグレーションコマンド redistribute）が設定されていても，area nssa コマンドで no-redistribution パラメータを指定した場合，エリアボーダルータは AS 外経路を NSSA 内に導入しません。これによって NSSA 内では経路情報を減らして，ルータの情報の交換や経路選択の負荷を減らせます。

また，area nssa コマンドで no-summary パラメータを指定した場合，エリアボーダルータはエリア外の経路（エリア間経路情報）の広告を抑止して，その代わりの経路としてデフォルトルートを導入します。このデフォルトルートは，エリア間経路情報（Type3LSA）として NSSA に広告されます。

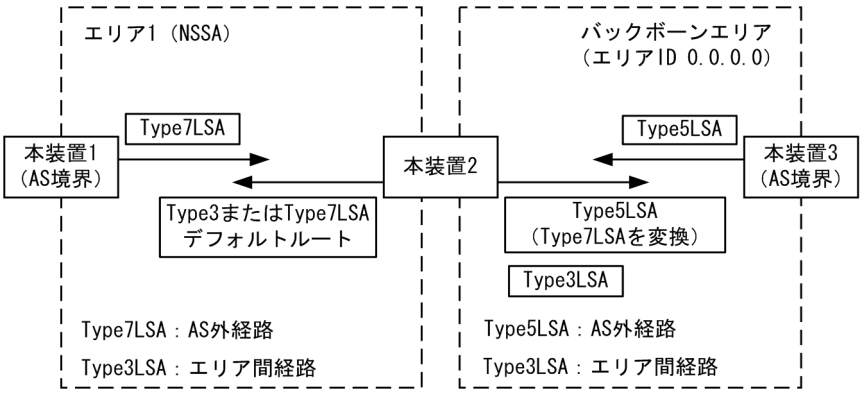
(1)　AS 外経路広告

NSSA 内の AS 境界ルータは，AS 外経路を Type7（NSSA external）LSA として生成します。この LSA は同一エリア内のルータだけに広告されます。

area nssa コマンドで default-information-originate パラメータを指定した場合，エリアボーダルータは Type7LSA で NSSA 内にデフォルトルートを導入します。NSSA 内に Type7LSA でデフォルトルートを広告するルータが複数存在する場合，AS 外経路として優先度の高い経路を選択します。

エリアボーダルータは, NSSA 内で学習した AS 外経路を Type5LSA に変換して NSSA ではないエリアへ広告します。この際，タグとフォワーディングアドレスを Type7LSA から引き継いで広告します。なお，AS 外経路の導入元である NSSA でコンフィグレーションコマンド area nssa translate type7 suppress-fa を指定した場合，Type5LSA に変換後，フォワーディングアドレスには常に 0.0.0.0 が設定されます。NSSA とバックボーンの間での経路交換を次の図に示します。

図 18-2　NSSA とバックボーンの間での経路交換



(2)　制限事項

本装置は，RFC3101（The OSPF Not-So-Stubby Area (NSSA) Option）に準拠していますが，ソフトウェアの機能制限によって，次に示す機能はサポートしていません。

- Type-7 Address Ranges
- Type-7 Translator Election

そのため，NSSA から学習した AS 外経路を常に NSSA でないエリアに広告します。

18.1.5　仮想リンク

OSPF では，スタブエリアまたは NSSA として設定してなくてバックボーンでもないエリア上のある二つのエリアボーダルータで, このエリア上の二つのルータ間の経路をポイントーポイント型回線と仮想することによって, バックボーンのインタフェースとして使用できます。この仮想の回線のことを仮想リンクと呼びます。仮想リンクの実際の経路があるエリアのことを，仮想リンクの通過エリアと呼びます。

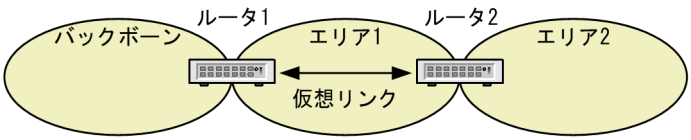
仮想リンクの使い方として，次に示す三つの例を挙げます。

- バックボーンに物理的に接続していないエリアの仮想接続
- 複数のバックボーンの結合
- バックボーンの障害による分断に対する経路の予備

(a)　バックボーンに物理的に接続していないエリアの仮想接続

次の図で，エリア 2 はバックボーンに接続していません。この場合，ルータ 1 とルータ 2 の間にエリア 1 を通過エリアとする仮想リンクを設定すると，ルータ 2 はバックボーンに接続するエリアボーダルータとなって，エリア 2 をバックボーンに接続していると見なせるようになります。

図 18-3　エリアのバックボーンへの接続



(b)　複数のバックボーンの結合

次の図では，AS 内にバックボーンであるエリアが二つ存在します。この状態では，バックボーンの分断による経路到達不能などの障害が発生することがあります。この場合，ルータ 1 とルータ 2 の間にエリア 1 を通過エリアとする仮想リンクを設定すると，バックボーンが結合されてこの障害を回避できます。

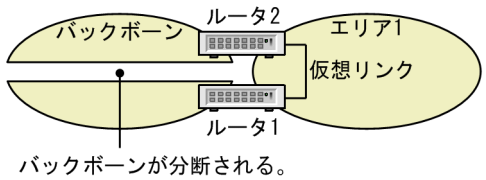
図 18-4　バックボーン間の接続



(c)　バックボーンの障害による分断に対する経路の予備

次の図では，バックボーンでネットワークの障害が発生してルータ 1 とルータ 2 の間の接続が切断された場合，バックボーンが分断されます。この場合，ルータ 1 とルータ 2 の間にエリア 1 を通過エリアとする仮想リンクを設定すると，これがバックボーンの分断に対する予備の経路（バックボーンでのルータ 1－ルータ 2 のコストと比較して，仮想リンクのコストが十分に小さい場合には，主な経路）になります。

図 18-5　バックボーン分断に対する予備経路



18.1.6　仮想リンクの動作

仮想リンクは，仮想リンクの両端のルータで共に設定する必要があります。仮想リンクの両端のルータは，仮想リンク上で OSPF パケットを送受信してバックボーンの経路を学習します。

仮想リンクを運用するに当たって，次のことに注意してください。

- 仮想リンクのコストは，通過エリアでの仮想リンクの両端のルータ間の経路コストになります。
- 通過エリアで，仮想リンクの両端のルータ間の経路がイコールコストマルチパスの場合，一般のトラフィックと仮想リンク上の経路情報トラフィックでは経路が異なることがあります。

(1)　隣接ルータとの接続

仮想リンクがアップしている間，ルータ間の接続性を検出するため，仮想リンクの隣接ルータに Hello パケットを送信します。なお，通過エリア内に仮想リンクの相手ルータへ到達するパスがあるとき，仮想リンクがアップします。

Hello パケットを他ルータから受信することによって，ルータ間で OSPF が動作していることを認識します。

Hello パケットに関するコンフィグレーションは，area virtual-link コマンドで設定します。dead-interval は，通過エリア上での仮想リンクの両端ルータ間の経路を構成する各ネットワーク上の，各インタフェースのインターバル値（ip ospf dead-interval コマンドの設定値）のどれよりも長くする必要があります。この値をどれよりも短く設定した場合，通過エリア内の経路上のネットワーク障害に当たって，通過

エリア内の代替経路への交替に基づいて仮想リンクが使用する経路が交替するよりも先に，仮想リンクが切断することがあります。

LSA の再送間隔（area virtual-link コマンドの retransmit-interval パラメータ）は，仮想リンクの両端ルータ間をパケットが往復するのに必要な時間よりも十分に長く設定する必要があります。

18.2　エリアのコンフィグレーション

18.2.1　コンフィグレーションコマンド一覧

スタブエリア，NSSA を使用する場合と，エリアボーダルータとして動作する場合のコンフィグレーションコマンド一覧を次に示します。

なお，「17　OSPF」で解説している機能のコマンドは，「表 17-4　AS 外経路広告に関係するコンフィグレーションコマンド一覧」，「表 17-5　経路選択や経路学習に関係するコンフィグレーションコマンド一覧」，「表 17-6　コンフィグレーションコマンド一覧」を参照してください。

表 18-2　area に関係するコンフィグレーションコマンド一覧

コマンド名	説明
area default-cost	スタブエリアに広告するデフォルトルートのコスト値を設定します。
area nssa	NSSA として動作するエリアを設定します。
area range	エリアボーダルータでエリア間経路を，指定したマスク付きアドレスに集約して広告します。
area stub	スタブエリアとして動作するエリアを設定します。
area virtual-link	仮想リンクを設定します。

表 18-3　OSPF 適用に関係するコンフィグレーションコマンド一覧

コマンド名	説明
disable	OSPF 動作の抑止を設定します。
ip ospf area	インタフェース単位での OSPF 動作制御を設定します。
network	OSPF が動作するネットワークアドレス範囲（アドレスとワイルドカードマスク）と，所属するエリア ID を設定します。
router-id	ルータ ID（ルータの識別子）を設定します。

18.2.2　コンフィグレーションの流れ

(1)　エリアボーダでない場合のスタブエリア，NSSA の設定手順

1. あらかじめ，IP インタフェースを設定します。
2. スタブエリア，または NSSA を設定します。
3. OSPF を適用する設定をします。

(2)　エリアボーダルータの設定手順

1. あらかじめ，IP インタフェースを設定します。
2. スタブエリア，または NSSA として動作するエリアを設定します。
   スタブエリアでは，広告するデフォルトルートのコスト値を設定します。
   NSSA では，AS 外経路としてデフォルトルートの広告を行えます。
3. 経路集約の設定をします。

4. OSPF を適用する設定をします。

   複数のエリアを設定します。この際，エリア 0（バックボーン）に所属するインタフェースの設定，または仮想リンクの設定が必要です。

5. 仮想リンクの設定をします。

18.2.3　スタブエリアの設定

[設定のポイント]

エリアボーダルータは，area stub コマンドを設定したエリア内にデフォルトルートを広告します。

スタブエリアや NSSA の設定は，同一エリア内の全ルータに設定する必要があります。

[コマンドによる設定]

1. **(config)# router ospf 1**

   ospf モードへ移行します。ドメイン番号を 1 にします。

2. **(config-router)# area 1 stub**

   エリア 1 をスタブエリアに設定します。

3. **(config-router)# router-id 172.16.1.1**

   ルータ ID として 172.16.1.1 を使用します。

4. **(config-router)# network 10.0.0.0 0.255.255.255 area 1**

   ネットワーク 10.0.0.0/8 の範囲内のインタフェースは，エリア 1 に所属します。

18.2.4　エリアボーダルータの設定

[設定のポイント]

area range コマンドでは，not-advertise パラメータを指定することで，このマスク付きアドレスの範囲に含まれるネットワークのエリア外への広告を抑止できます。

集約および抑止するアドレスの範囲は，一つのエリアについて複数設定できます。また，エリア内にどの設定の範囲にも含まれないアドレスを使用しているルータやネットワークが存在してもかまいません。ただし，ネットワークを構成するに当たって，トポロジと合ったアドレスを割り当てた上でトポロジに応じた範囲を使用して集約を設定すると，選択する経路の適切さを損なわないで，効率的に OSPF の経路情報トラフィックを削減できます。

ここでは，エリア 0 とエリア 1 に属するエリアボーダルータでの経路集約の設定例を示します。

[コマンドによる設定]

1. **(config)# router ospf 1**

   (config-router)# area 0 range 10.0.0.0 255.255.254.0

   エリア 0 でネットワーク 10.0.0.0，マスク 255.255.254.0 の範囲内の経路を学習した場合，エリア 1 に集約経路を広告します。

2. **(config-router)# area 1 range 10.0.2.0 255.255.255.0**

   エリア 1 でネットワーク 10.0.2.0，マスク 255.255.255.0 の範囲内の経路を学習した場合，エリア 0 に集約経路を広告します。

3. **(config-router)# network 10.0.0.0 0.0.0.255 area 0**

   ネットワーク 10.0.0.0/24 の範囲内のインタフェースは，エリア 0 に所属します。

4. **(config-router)# network 10.0.2.0 0.0.0.255 area 1**

ネットワーク 10.0.2.0/24 の範囲内のインタフェースは，エリア 1 に所属します。

18.2.5　仮想リンクの設定

[設定のポイント]

area virtual-link コマンドで，相手ルータのルータ ID を指定します。

[コマンドによる設定]

1. **(config)# router ospf 1**
   (config-router)# network 10.0.0.0 0.0.0.255 area 0
   ネットワーク 10.0.0.0/24 の範囲内のインタフェースは，エリア 0 に所属します。
2. **(config-router)# network 10.0.2.0 0.0.0.255 area 1**
   ネットワーク 10.0.2.0/24 の範囲内のインタフェースは，エリア 1 に所属します。
3. **(config-router)# area 1 virtual-link 10.0.0.1**
   (config-router)# area 1 virtual-link 10.0.0.2
   通過エリア 1 の相手ルータを設定します。

18.3　隣接ルータ認証の解説

OSPF では，ルータ間の経路情報の交換時に情報を送信したルータが同じ管理下にあることを検証するために，認証を使用できます。隣接ルータとの間で認証を使用すると，OSPF の経路情報を送信されることによる経路制御上の攻撃から，認証管理下にあるルータを保護できます。

- **認証方式**

  認証方式には，平文パスワードによる認証と MD5 による認証があります。

  コンフィグレーションで，エリアの認証方式，またはインタフェース単位の認証方式を指定します。どちらのコンフィグレーションも指定していない場合，認証をしません。また，認証方式を指定しても，認証キーが指定されていないインタフェースでは，認証をしません。仮想リンクの認証方式は，エリア 0 に設定した認証方式になります。

18.3.1　認証手順

認証方式には，平文パスワードによる認証と MD5 による認証があります。

(1)　平文パスワード認証

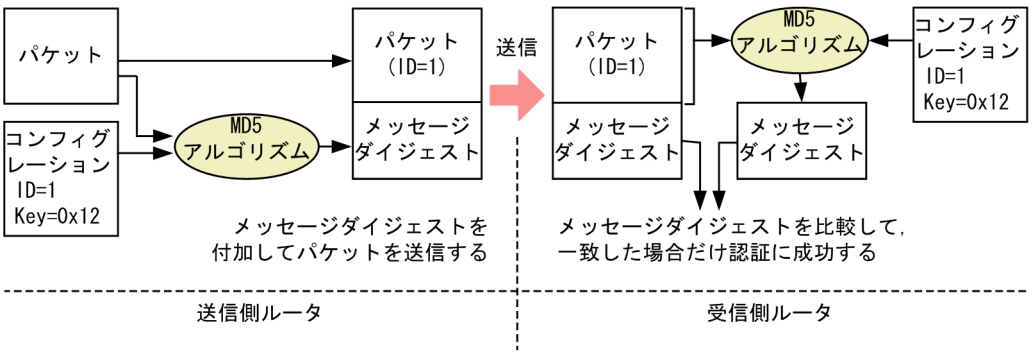
平文パスワード認証では，経路情報の送信時には，コンフィグレーションで設定した認証鍵をそのままパスワードとして埋め込んで送信します。

経路情報の受信時には，経路情報中のパスワードと設定してある認証鍵が一致した場合，認証に成功したと見なします。認証に失敗した情報は破棄されます。

(2)　MD5 認証

MD5 認証では，経路情報に基づく MD5 アルゴリズムによるメッセージダイジェストを比較して情報を認証します。MD5 認証のデータフローを次の図に示します。

図 18-6　MD5 認証のデータフロー



経路情報の送信時には，認証鍵，認証鍵の ID，および経路情報自体から，MD5 ハッシュアルゴリズムを使用してメッセージダイジェストを生成して，これを経路情報とともに送信します。

経路情報の受信時には，コンフィグレーションで設定した認証鍵のうち，経路情報中に含まれる認証鍵の ID 番号と同じ ID 番号の認証鍵をすべて試します。この認証鍵を使用して送信時と同様の手順を経てメッセージダイジェストを生成して，どれかの認証鍵から生成したメッセージダイジェストが経路情報とともに受信したメッセージダイジェストと一致した場合，認証に成功したと見なします。受信した情報について有効な鍵をすべて使用しても認証に成功しなかった場合は，この情報の認証に失敗したと見なします。認証に失敗した情報は破棄されます。

18.4　隣接ルータ認証のコンフィグレーション

18.4.1　コンフィグレーションコマンド一覧

隣接ルータ認証のコンフィグレーションコマンド一覧を次の表に示します。なお，SNMP のコンフィグレーションを設定することで，認証失敗などのエラーパケット受信の SNMP 通知を送信できます。

表 18-4　コンフィグレーションコマンド一覧

コマンド名	説明
area authentication	認証方式（平文パスワードまたは MD5 認証）を設定します。
area virtual-link	authentication-key パラメータ，message digest-key md5 パラメータで認証キーを設定します。
ip ospf authentication	認証方式（平文パスワードまたは MD5 認証）を設定します。
ip ospf authentication-key	認証キーを設定します。
ip ospf message-digest-key	MD5 の認証キーを設定します。
snmp-server host※	SNMP 通知を送信する宛先のネットワーク管理装置を設定します。

注※

「コンフィグレーションコマンドレファレンス Vol.1　14. SNMP」を参照してください。

18.4.2　MD5 認証キーの変更

認証キーを移行するために，MD5 の認証キーを複数設定できます。

次の手順で新しいキーへ移行できます。

1. 現在使用中の ID 番号とは異なる ID 番号で，新しい鍵を設定します。
2. 隣接ルータのすべてに，新しい鍵を設定します。
3. 古い認証鍵を削除します。

18.4.3　平文パスワード認証の設定

[設定のポイント]

area authentication コマンドではエリアの認証方式を設定します。

[コマンドによる設定]

1. **(config)# router ospf 1**
   (config-router)# area 1 authentication
   (config-router)# exit
   エリア 1 で，平文パスワード認証をする設定をします。
2. **(config)# interface gigabitethernet 1/1**
   (config-if)# ip ospf authentication-key a1w@9a
   認証鍵を a1w@9a に設定します。ポート 1/1 がエリア 1 に設定されている場合，ポート 1/1 で送受信する OSPF パケットを，平文パスワードで認証します。

18.4.4　MD5 認証の設定

[設定のポイント]

認証鍵の設定には，認証鍵自体と，認証鍵の ID 番号を必ず指定します。

[コマンドによる設定]

1. **(config)# router ospf 1**
   (config-router)# area 1 authentication message-digest
   (config-router)# exit
   エリア 1 で，MD5 認証をする設定をします。
2. **(config)# interface gigabitethernet 1/1**
   (config-if)# ip ospf message-digest-key 1 md5 a1w@9a
   ID 番号を 1 に，認証鍵を a1w@9a に設定します。ポート 1/1 がエリア 1 に設定されている場合，ポート 1/1 で送受信する OSPF パケットを，メッセージダイジェストを使用して認証します。

18.5 ノンストップルーティングの解説

18.5.1 概要

ノンストップルーティングは，系切替によって運用系 BCU が交替したときに系切替前のルーティングプロトコルの状態を引き継いで，新運用系 BCU で継続して動作することでネットワーク全体での通信を維持するための機能です。

上記の実現のために，OSPF ではあらかじめルーティングプロトコルの状態を他系 BCU 間で同期します。系切替時には，新運用系 BCU が Hello パケットや LSA の送受信を継続することで，系切替を隣接ルータから隠します。

ノンストップルーティングは装置単体で動作する機能のため，隣接ルータがノンストップルーティングをサポートしている必要はありません。

18.5.2 注意事項

ノンストップルーティングを使用する場合，ルータ ID を固定するためにコンフィグレーションコマンド router-id を設定するか，ループバックインタフェースに IPv4 アドレスを設定してください。どちらも設定しない場合，ノンストップルーティングによる系切替の前後で，ルータ ID が変更されるおそれがあります。ルータ ID が変更されると，ノンストップルーティングに失敗します。

18.6　ノンストップルーティングのコンフィグレーション

18.6.1　コンフィグレーションコマンド一覧

ノンストップルーティングのコンフィグレーションコマンド一覧を次の表に示します。

表 18-5　コンフィグレーションコマンド一覧

コマンド名	説明
nsr	ノンストップルーティングを有効にします。

18.6.2　ノンストップルーティングの設定

[設定のポイント]

ユニキャストルーティングプログラムの再起動時に系切替することを指定して，ノンストップルーティングを有効にします。

[コマンドによる設定]

1. **(config)# failure-action software unicast switchover**
   ユニキャストルーティングプログラムの再起動時に系切替します。
2. **(config)# router ospf 1**
   (config-router)# router-id 192.168.1.100
   (config-router)# nsr
   ノンストップルーティングを使用する設定をします。

18.7　グレースフル・リスタートの解説

18.7.1　概要

グレースフル・リスタートは，系切替によって運用系 BCU が交替したときや，運用コマンドなどによってユニキャストルーティングプログラムが再起動したときに，ネットワークから経路が消えることによる本装置を中継する通信の停止を防ぐための機能です。

OSPF では，グレースフル・リスタートによって OSPF を再起動する装置のことをリスタートルータと呼びます。リスタートルータにあるグレースフル・リスタートをする機能をリスタート機能と呼びます。また，グレースフル・リスタートを補助する隣接装置をヘルパールータと呼びます。ヘルパールータにあるグレースフル・リスタートを補助する機能をヘルパー機能と呼びます。

本装置は，リスタート機能とヘルパー機能をサポートしています。

18.7.2　ヘルパー機能

本装置はヘルパールータとして動作している場合，グレースフル・リスタートをしている間リスタートルータを経由する経路を維持します。

(1)　ヘルパー機能の動作条件

ヘルパー機能が動作する条件を次に示します。

- すでに同一ドメイン内で別のリスタートルータのヘルパーとなっていないこと
  同一ドメイン内で，複数のルータのグレースフル・リスタートに対して同時にヘルパールータとして動作できません。ただし，リスタートルータが 1 台しかない場合，そのリスタートルータと接続しているすべてのインタフェースでヘルパールータとして動作します。
- リスタートルータに送信した OSPF の Update パケットに対する Ack 待ちの状態でないこと

(2)　ヘルパー機能が失敗するケース

ヘルパールータとしての動作は，隣接が確立するまで，または，リスタートルータから終了の通知を受信するまで継続します。

しかし，次のイベントが発生した場合，リスタートルータが維持している経路と不整合が発生するおそれがあるため，ヘルパー機能を中断して経路を再計算します。

- 隣接ルータから新しい LSA（定期更新を除く）を学習して，リスタートルータへ広告した場合
- OSPF インタフェースがダウンした場合
- リスタートルータ以外のルータとの隣接関係の切断または確立によって LSA を更新した場合
- OSPF の同一ドメイン内で，複数のルータが同時に再起動した場合
- graceful-restart mode コマンドでコンフィグレーションを削除して，ヘルパー機能を削除した場合

18.7.3　リスタート機能

次の契機で，OSPF のリスタート機能が動作します。

- 系切替によって運用系 BCU が交替したとき

- ユニキャストルーティングプログラムが再起動したとき

(1)　OpaqueLSA

本装置は，グレースフル・リスタートの開始や終了を通知するために，Type9 の OpaqueLSA を広告します。ただし，Type9 の OpaqueLSA については，OSPF のグレースフル・リスタートに使用する grace-LSA 以外の機能はサポートしていません。

(2)　グレースフル・リスタートの手順

OSPF のグレースフル・リスタート手順を次の図および表に示します。

図 18-7　OSPF グレースフル・リスタート手順

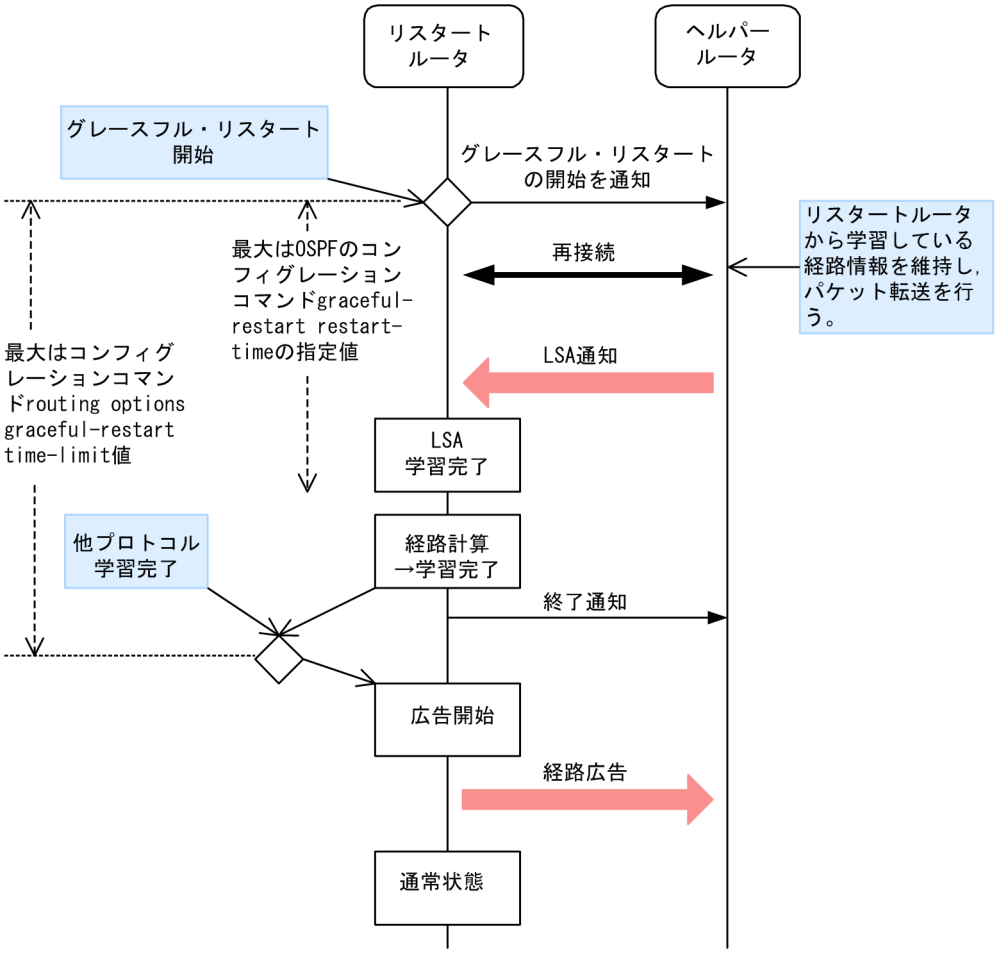


表 18-6　OSPF グレースフル・リスタート手順

項番	項目	契機	処理内容
1	グレースフル・リスタートの開始	系切替によって運用系 BCU が交替したとき。	グレースフル・リスタートを開始します。通常の接続手順と同様に，各インタフェースで OSPF 情報のパケットを交換します。
		ユニキャストルーティングプログラムが再起動したとき。	
2	経路計算	ドメイン内の全 OSPF インタフェースについて再接続が完了して，隣接	ドメインごとに経路計算をして，ルーティングテーブルを更新します。複数のドメイン

項番	項目	契機	処理内容
		ルータからすべての LSA を学習したとき。	が存在する場合，経路計算は接続の終わったドメインから随時します。経路計算が全ドメインで終了したとき，OSPF の経路学習が完了します。
		1 インタフェースでもグレースフル・リスタートに失敗したとき。	その時点での同一ドメイン内の各インタフェースの接続状態に基づいて，経路計算をします。
3	広告開始	OSPF の経路学習が完了して，かつほかのルーティングプロトコルの経路学習が完了したとき。	AS 外経路の広告を開始します。広告完了後，通常の OSPF 動作に戻ります。
		OSPF のグレースフル・リスタートに失敗したとき。	

(3) グレースフル・リスタートが失敗するケース

OSPF のグレースフル・リスタートが失敗するケースを次に示します。

- グレースフル・リスタートの開始をヘルパールータへ通知してからリスタート時間（OSPF のコンフィグレーションコマンド graceful-restart restart-time の指定値）が経過しても LSA 学習を完了できなかった場合
- 再接続しているインタフェースがダウンした場合
- OSPF ドメイン上で LSA が変更された場合
- OSPF ドメイン上の別のルータがグレースフル・リスタートした場合
- グレースフル・リスタートを開始してから経路保持時間（コンフィグレーションコマンド routing options graceful-restart time-limit の指定値）が経過しても全プロトコルの経路学習が完了しなかった場合
- コンフィグレーションコマンド graceful-restart mode を変更して，リスタート機能を削除した場合

(4) 注意事項

- リスタートルータとしてグレースフル・リスタートを開始しても，一部のヘルパールータがヘルパー動作を開始しない場合や途中で止めた場合，同一ドメイン内の全インタフェースでグレースフル・リスタートを止めます。
- OSPF のリスタート時間を，系切替所要時間＋ LSA 学習時間を超えるように設定してください。これは，OSPF が LSA を学習するためには，系切替が完了して IP インタフェースの Up/Down が確認できるようになっている必要があるためです。グレースフル・リスタート開始後，リスタート時間が経過した時点で LSA の学習が終わってない場合，OSPF のグレースフル・リスタートに失敗します。
- 系切替によって運用系 BCU が交替したときのルーティングエントリ保持時間を，OSPF のリスタート時間よりも長く設定してください。OSPF のリスタート時間よりもルーティングエントリ保持時間のほうが短い場合，経路学習前に系切替前のルーティングエントリが削除されることがあります。
- BGP4 の内部ピアがグレースフル・リスタートを使用している場合，内部ピアのリスタート時間を OSPF のリスタート時間よりも長く設定してください。内部ピアのリスタート時間のほうが短い場合，OSPF が経路学習を完了する前に内部ピアを接続できなくなって，内部ピアのグレースフル・リスタートに失敗することがあります。

18.8　グレースフル・リスタートのコンフィグレーション

18.8.1　コンフィグレーションコマンド一覧

本装置の OSPF 隣接ルータで OSPF リスタート機能を使用する場合，本装置に OSPF ヘルパー機能を設定してください。

リスタート機能を使用する場合，OSPF のリスタート時間（graceful-restart restart-time コマンドの設定値）を，系切替所要時間＋ LSA 学習時間を超えるように設定してください。

グレースフル・リスタートのコンフィグレーションコマンド一覧を次の表に示します。

表 18–7　コンフィグレーションコマンド一覧

コマンド名	説明
graceful-restart mode	ヘルパー機能またはリスタート機能を設定します。
graceful-restart restart-time	リスタート時間（ヘルパーとの再接続の許容時間）を設定します。
graceful-restart strict-lsa-checking	ヘルパールータで，リスタートルータとの間で LSA データベースが同期していない状況になった場合，グレースフル・リスタートを止めます。
max-metric router-lsa	リスタートルータとしての経路学習に失敗した後，スタブルータとして動作します。
routing options graceful-restart time-limit※	経路を保留する時間の上限値を指定します。

注※
「コンフィグレーションコマンドレファレンス Vol.3　13. ルーティングオプション」を参照してください。

18.8.2　リスタート機能の設定

[設定のポイント]
リスタート機能を使用することを指定します。

[コマンドによる設定]

1. **(config)# router ospf 1**
   (config-router)# graceful-restart mode both
   モードとして，リスタート機能とヘルパー機能の両方を設定します。

18.8.3　ヘルパー機能の設定

[設定のポイント]
ヘルパー機能を使用することを指定します。設定しない場合，ヘルパーとして動作しません。

[コマンドによる設定]

1. **(config)# router ospf 1**
   (config-router)# graceful-restart mode helper

ヘルパー機能を使用します。

18.9　スタブルータの解説

18.9.1　概要

隣接ルータとの接続が完了していなかったり，安定していなかったりすると，ネットワーク全体のルーティングが不安定になることがあります。ルータの起動および再起動時やネットワークにルータを追加するときに，このような状況が起こることがあります。OSPF ではこのような状況下，周辺の装置でルーティングにできるだけ使用されないように，経路情報を通知できます。OSPF では，このような通知をしているルータをスタブルータと呼びます。この機能によって，装置の状態が不安定であっても，ネットワークのルーティングが不安定になることを防げます。

(1)　スタブルータ動作時の OSPF インタフェースのコスト値

スタブルータは，接続する OSPF インタフェースのコスト値を最大値（65535）にして広告します。このため，スタブルータを経由する OSPF 経路は優先されなくなります。ただし，隣接ルータの存在しないインタフェース（スタブネットワーク）の経路については，コンフィグレーションコマンドで指定したコスト値を広告します。スタブネットワークや AS 外経路は，スタブルータが広告している経路が優先されることがあります。

周辺装置ではメトリックを比較して，スタブルータを経由しない代替経路を優先します。また，スタブルータ自身のループバックインタフェースに設定したアドレスを使用して，telnet および SNMP による管理や BGP4 による経路交換ができます。

18.9.2　スタブルータの動作

コンフィグレーションコマンド max-metric router-lsa では，ドメインごとにスタブルータ機能を動作させるかどうかを指定します。さらに，動作条件として，スタブルータとして常時動作させるか，または起動後に動作させるかを選択できます。

(1)　常時動作する場合

常時，コストを最大値にします。スタブルータのコンフィグレーションを削除するまで，動作し続けます。

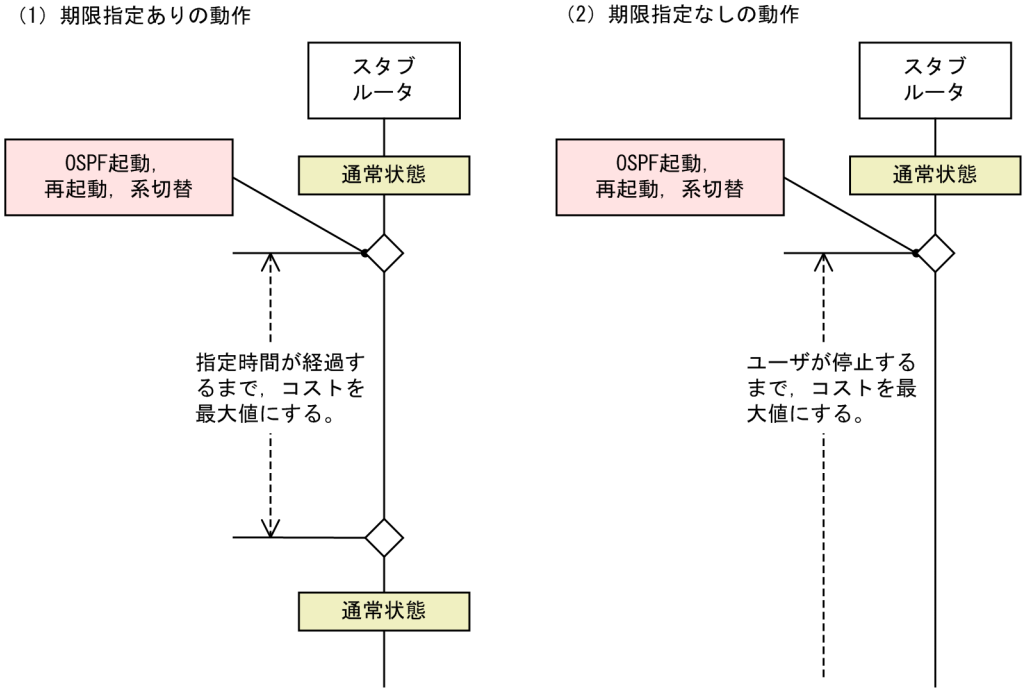
(2)　起動後にスタブルータとして動作する場合

次に示す契機でコストを最大値にします。コンフィグレーションで指定した期限が経過するまで，継続します。

- 装置起動
- 系切替による運用系 BCU の交替後
  ただし，次の場合を除きます。
  - ノンストップルーティング使用時の系切替で，隣接状態を正しく引き継いで隣接装置と再接続しない場合
  - グレースフル・リスタート使用時の系切替で，グレースフル・リスタートに成功した場合
- ユニキャストルーティングプログラムの再起動後
  ただし，次の場合を除きます。
  - グレースフル・リスタート使用時の系切替で，グレースフル・リスタートに成功した場合

動作中に運用コマンド clear ip ospf stub-router を実行するか，コンフィグレーションを削除することで停止できます。スタブルータの動作を次の図に示します。

図 18-8　スタブルータの動作



(3)　注意事項

- グレースフル・リスタートのヘルパールータとして動作しているとき，スタブルータのコンフィグレーションを変更しないでください。設定を変更すると，スタブルータが動作を開始したり終了したりして，ヘルパー動作に失敗することがあります。
- スタブルータとして常時動作する設定になっているとき，起動後に動作するように変更すると，すぐにスタブルータを終了します。
- スタブルータを通過する仮想リンクは，使用できません。

  通過エリアでのコストが 65535 よりも大きい場合，仮想ネイバーはその仮想リンクを到達不能とみなします。
- 古い OSPF 規格の RFC1247 の仕様では，最大メトリックの経路情報は SPF 計算に使用されません。このため，新しい OSPF 規格に対応していない装置では，スタブルータを経由する経路は登録されません。

18.10　スタブルータのコンフィグレーション

18.10.1　コンフィグレーションコマンド一覧

本装置を経由する経路を優先させたくない場合, スタブルータを設定してください。スタブルータを経由する経路のメトリックを大きく設定できます。

スタブルータのコンフィグレーションコマンド一覧を次の表に示します。

表 18-8　コンフィグレーションコマンド一覧

コマンド名	説明
max-metric router-lsa	スタブルータとして動作します。

18.10.2　スタブルータ機能の設定

[設定のポイント]

スタブルータとして動作することを指定します。on-startup パラメータを指定しない場合, スタブルータとして常時動作します。

[コマンドによる設定]

1. **(config)# router ospf 1**
   (config-router)# max-metric router-lsa
   スタブルータ機能を使用します。

18.11　OSPF 拡張機能のオペレーション

18.11.1　運用コマンド一覧

OSPF 拡張機能の運用コマンド一覧を次の表に示します。

表 18-9　運用コマンド一覧

コマンド名	説明
show ip ospf	ドメインの情報（エリアボーダの状態，グレースフル・リスタートの状態など）や，エリアを表示します。
clear ip ospf	OSPF プロトコルに関する情報をクリアします。stub-router パラメータでスタブルータの動作を停止します。
show nsr unicast※	ユニキャストルーティングプロトコルのノンストップルーティングの同期状態を表示します。
show graceful-restart unicast※	ユニキャストルーティングプロトコルのグレースフル・リスタートのリスタートルータの動作状態を表示します。

注※
「運用コマンドレファレンス Vol.3　12. IPv4・IPv6 ルーティングプロトコル共通」を参照してください。

18.11.2　エリアボーダの確認

show ip ospf コマンドを実行して，エリアボーダルータではルータの種別（Flags）に「AreaBorder」が含まれていることを確認してください。また, エリア間の経路集約が正しく反映されていることを確認してください。

図 18-9　show ip ospf コマンドの実行結果

```
>show ip ospf
Date 20XX/03/14 12:00:00 UTC
Domain: 1
Router ID: 172.16.1.1
Distance:
  Intra Area: 10, Inter Area: 10, External: 150
Flags: <AreaBorder ASBoundary>
SPF Interval: 7s, SPF Delay: 3s
Graceful Restart: Helper
  Last Helper Status : Finished  20XX/02/15 14:12:22
Area            Interfaces  Network Range      State
0               1           -                  -
10              1           192.168.1/24       Advertise
                            172.19/18          DoNotAdvertise
```

18.11.3　エリアの確認

コンフィグレーションで設定したエリアが正しく反映されていることを確認してください。show ip ospf コマンドで area パラメータを指定すると，エリアの一覧を表示します。

図 18-10　show ip ospf コマンド（area パラメータ指定）の実行結果

```
>show ip ospf area
Date 20XX/03/14 12:00:00 UTC
Domain: 1
ID              Neighbor   SPFcount   Flags
0               2          14         <ASBoundary>
```

```
1               2          8          <NSSA>
>
```

18.11.4　ノンストップルーティングの確認

(1)　動作状態の確認

show ip ospf コマンドを実行して，ノンストップルーティングの動作状態を確認してください。

図 18-11　show ip ospf コマンドの実行結果

```
>show ip ospf
Date 20XX/03/14 12:00:00 UTC
Domain: 1
Router ID: 172.16.1.1
Distance:
  Intra Area: 10, Inter Area: 10, External: 150
Flags: <AreaBorder ASBoundary>
SPF Interval: 7s, SPF Delay: 3s
Nonstop Routing: Enable, Sync Status: Synchronized
Area            Interfaces  Network Range      State
0               1           -                  -
10              1           192.168.1/24       Advertise
>
```

(2)　同期状態の詳細の確認

他系 BCU との同期状態を確認してください。show ip ospf コマンドで nsr パラメータを指定すると，ノンストップルーティングの同期状態の詳細を表示します。

図 18-12　show ip ospf コマンド（nsr パラメータ指定）の実行結果

```
>show ip ospf nsr
Date 20XX/03/14 12:00:00 UTC
Total of Domain: 1
Status: Synchronized
Sync Time: 20XX/03/10 12:00:00
Nonstop-Routing Control Information
  Waited Request : 0
  Total  Request : 28
>
```

(3)　ノンストップルーティング対象プロトコルの同期状態の確認

show nsr unicast コマンドを実行して，ノンストップルーティングが動作しているプロトコルの状態を確認してください。

図 18-13　show nsr unicast コマンドの実行結果

```
>show nsr unicast
Date 20XX/04/14 12:00:00 UTC
Status:  Synchronized
Protocol      Total    Asynchronous    Synchronizing   Synchronized
BGP4          5        0               0               5
OSPF          10       0               0               10
BGP4+         5        0               0               5
OSPFv3        10       0               0               10
>
```

18.11.5　グレースフル・リスタートの確認

(1)　動作モードや進行状態の確認

show ip ospf コマンドを実行して，グレースフル・リスタートの状態を確認してください。

図 18-14 show ip ospf コマンドの実行結果

```
>show ip ospf
Date 20XX/03/14 12:00:00 UTC
Domain: 1
Router ID: 172.16.1.1
Distance:
  Intra Area: 10, Inter Area: 10, External: 150
Flags: <AreaBorder ASBoundary>
SPF Interval: 7s, SPF Delay: 3s
Graceful Restart: Helper
  Last Helper Status : Finished  20XX/02/15 14:12:22
Area            Interfaces  Network Range      State
0               1           -                  -
10              1           192.168.1/24       Advertise
```

(2) リスタートルータの動作確認

show graceful-restart unicast コマンドを実行して，リスタートルータとして動作しているプロトコルの状態を確認してください。

図 18-15 show graceful-restart unicast コマンドの実行結果

```
>show graceful-restart unicast
Date 20XX/04/14 12:00:00 UTC
Status: Completed
Graceful Restart Time Limit: 180s
Start Time: 20XX/04/08 17:01:23
End Time  : 20XX/04/08 17:01:23
OSPF  : Restart State <Finished>
        Total of Domain: 2 (Succeeded: 2)
BGP   : Restart State <Finished>
        Total of Peer  : 25 (Succeeded: 25)
OSPFv3: Restart State <Finished>
        Total of Domain: 2 (Succeeded: 2)
BGP4+ : Restart State <Finished>
        Total of Peer  : 20 (Succeeded: 20)
```

19 OSPFv3

この章では, 主にイントラネットに適用されるルーティングプロトコルである OSPFv3 について説明します。

19.1 OSPFv3 基本機能の解説

OSPFv3 はルータ間の接続状態から構成されるトポロジと Dijkstra アルゴリズムによる最短経路計算に基づく IPv6 用のルーティングプロトコルです。

19.1.1 OSPFv3 の特長

OSPFv3 は，通常一つの AS 内での経路決定に使用されます。OSPFv3 では，AS 内のすべての接続状態から構成するトポロジのデータベースが各ルータにあり，このデータベースに基づいて最短経路を計算します。そのため，OSPFv3 は RIPng と比較して，次に示す特長があります。

- 経路情報トラフィックの削減

  OSPFv3 では，ルータ間の接続状態が変化したときだけ，接続状態の情報をほかのルータに通知します。そのため，OSPFv3 は RIPng のように定期的にすべての経路情報を通知するルーティングプロトコルと比較して，ルーティングプロトコルが占有するトラフィックが小さくなります。なお，OSPFv3 では 30 分周期で，自ルータの接続状態の情報を他ルータに通知します。

- ルーティングループの抑止

  OSPFv3 を使用しているすべてのルータは，同じデータから成るデータベースを保持しています。各ルータは共通のデータに基づいて経路を選択します。したがって，RIPng のようなルーティングループ（中継経路の循環）は発生しません。

- コストに基づく経路選択

  OSPFv3 では，宛先まで到達できる経路が複数存在する場合，宛先までの経路上のコストの合計が最も小さい経路を選択します。これによって，RIPng と異なり経路へのコストを柔軟に設定できるため，中継段数に関係なく望ましい経路を選択できます。

- 大規模なネットワークの運用

  OSPFv3 では，コストの合計が 16777214 以内の経路を扱えます。そのため，メトリックが 1～15 の範囲である RIPng と比較して，より大規模で経由ルータ数の多い経路が存在するネットワークの運用に適しています。

19.1.2 OSPFv3 の機能

OSPFv3 は，OSPF と似たプロトコルですが，OSPF と OSPFv3 はそれぞれ独立して動作します。

(1) OSPF との機能差分

OSPFv3（IPv6）と OSPF（IPv4）との機能差分を次の表に示します。

表 19-1 OSPFv3（IPv6）と OSPF（IPv4）の機能差分

機能	OSPFv3（IPv6）	OSPF（IPv4）
AS 外経路のフォワーディングアドレス	×	○
NSSA	×	○
認証	×	○
非ブロードキャスト（NBMA）ネットワーク	×	○
イコールコストマルチパス	○※	○

機能	OSPFv3（IPv6）	OSPF（IPv4）
仮想リンク	○	○
マルチバックボーン	○	○
ユニキャストルーティング高可用機能	○	○
スタブルータ	○	○

（凡例）　○：取り扱う　×：取り扱わない

注※

経路選択方法は，OSPF（IPv4）と OSPFv3（IPv6）で異なります。イコールコスト時，OSPF（IPv4）では最小のネクストホップアドレスを選択しますが，OSPFv3（IPv6）ではルータ ID が最小であるネクストホップアドレスを選択します。同一ルータ ID のネクストホップアドレスが複数ある場合，Hello パケットで最小のインタフェース ID を広告しているネクストホップアドレスを選択します。

(2)　ドメイン

本装置では，1 台のルータ上で AS を複数の OSPFv3 ネットワークに分割して，OSPFv3 ネットワークごとに個別に経路の交換，計算，生成ができます。この機能を OSPFv3 マルチバックボーンと呼びます。この独立した各 OSPFv3 ネットワークのことを，OSPFv3 ドメインと呼びます。

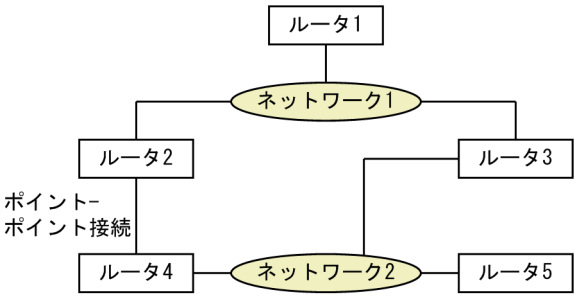
OSPFv3 のコンフィグレーションは，OSPFv3 ドメインごとに設定します。

19.1.3　経路選択アルゴリズム

OSPFv3 では，経路選択のアルゴリズムとして，SPF（Shortest Path First）アルゴリズムを使用します。各ルータには，OSPFv3 が動作しているすべてのルータと，ルーターールータ間およびルーターネットワーク間のすべての接続から成るデータベースがあります。このデータベースから，ルータおよびネットワークを頂点として，ルーターールータ間およびルーターネットワーク間の接続を辺とするトポロジを構成します。このトポロジに SPF アルゴリズムを適用して最短経路木を生成して，これを基に各頂点への経路を決定します。

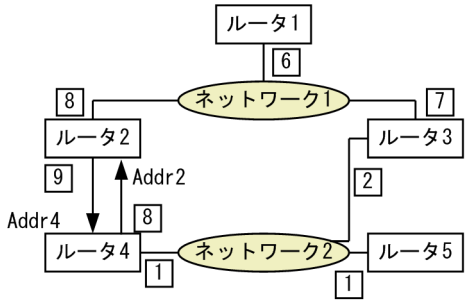
ネットワーク構成の例を次の図に示します。

図 19-1　ネットワーク構成例



この図のネットワーク上で OSPFv3 を使用した場合のトポロジとコストの設定例を次の図に示します。

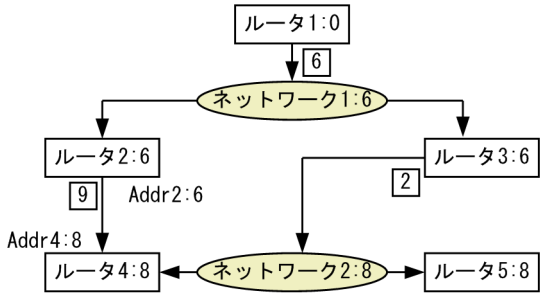
図 19-2 トポロジとコストの設定例



コスト値は，パケット送信方向によって異なってもかまいません。「図 19-2 トポロジとコストの設定例」のルータ 2－ルータ 4 間のポイント－ポイント型接続では，ルータ 2 からルータ 4 へはコスト 9，ルータ 4 からルータ 2 へはコスト 8 となっています。ルーター－ネットワーク間の接続では，ルータからネットワークへの接続だけ，コストを設定できます。ネットワークからルータへのコストは常に 0 です。

「図 19-2 トポロジとコストの設定例」のトポロジを基に，ルータ 1 を根として生成した最短経路木を次の図に示します。ある宛先へのコストは，経路が経由する各インタフェースの送信コストの合計となります。例えば，ルータ 1 からネットワーク 2 宛ての経路のコストは，6（ルータ 1－ネットワーク 1）＋ 0（ネットワーク 1－ルータ 3）＋ 2（ルータ 3－ネットワーク 2）＝ 8 となります。

図 19-3 ルータ 1 を根とする最短木



19.1.4 LSA の広告

(1) LSA の種類

OSPFv3 では経路情報のことを，Link State Advertise（LSA）と呼びます。

主な LSA は，次の三つに分類されます。

(a) エリア内経路情報

SPF アルゴリズムに使用するルータおよびネットワークの状態を通知します。

(b) エリア間経路情報

別エリアの経路を通知します。

(c)　AS 外経路情報

OSPFv3 ルータが AS 外の経路情報を認識している場合，この経路を OSPFv3 を使用してそのほかすべての OSPFv3 ルータに通知できます。AS 外経路を OSPFv3 内に導入するルータを AS 境界ルータと呼びます。

(2)　AS 外経路

コンフィグレーションで経路の再配布フィルタを設定した場合，AS 外経路を広告します。導入元の AS 境界ルータは，次の情報を付加して LSA を広告します。

- メトリック
  メトリックは，経路を学習するルータでほかの LSA との経路選択に使用されます。メトリックのデフォルト値は，default-metric コマンドで設定します。
- AS 外経路メトリックタイプ
  Type1 と Type2 の 2 種類があります。Type1 と Type2 の経路では，経路の優先順位，およびメトリックを経路の選択に使用するときの計算方法が異なります。メトリックタイプのデフォルト値は，Type2 です。
- フォワーディングアドレス（転送先）
  本装置では設定しません。
- タグ
  付加情報としてタグを広告できます。

(3)　ドメイン間での AS 外経路の広告

1 台のルータが接続している複数の OSPFv3 ドメインは，それぞれ独立した OSPFv3 ネットワークとして動作します。そのため，経路再配布についてのコンフィグレーションの設定がない場合は，一方の OSPFv3 ドメイン上の経路が他方の OSPFv3 ドメインへ配布されません。コンフィグレーションで別ドメインで学習した OSPFv3 経路の再配布フィルタを設定した場合，別ドメインの経路を AS 外経路として広告します。フィルタ属性には，次の表に示すデフォルト値を適用します。

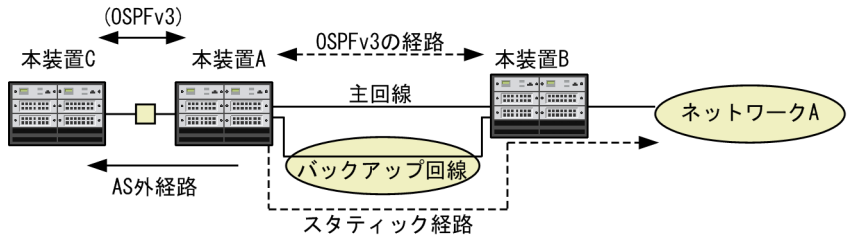
表 19–2　別ドメインの経路を再配布する場合のフィルタ属性

属性	デフォルト値	
	AS 外経路	エリア内，エリア間経路
メトリック値	default-metric コマンドで設定した値。 default-metric 設定がない場合は 20。	default-metric コマンドで設定した値。 default-metric 設定がない場合は 20。
メトリックタイプ	AS 外経路の Type2。	
タグ値	経路のタグ値を引き継ぎます。	広告しません。

19.1.5　AS 外経路の導入例

バックアップ回線を使用した構成での AS 外経路の導入例を次の図に示します。

図 19-4 バックアップ回線を使用した構成での AS 外経路の導入例



OSPFv3 では，隣接するルータを検出するために，定期的にパケットを交換します。そのため，バックアップ回線を OSPFv3 のトポロジの一部として使用した場合，この回線でパケットを継続して交換するため，バックアップ回線も常に運用状態になります。バックアップ回線上での通信が必要ではない場合にバックアップ回線を休止状態にするには，次のように設定します。

本装置 A では主回線で OSPFv3 を動作させ，バックアップ回線にネットワーク A へのスタティック経路を設定します。さらに，スタティック経路のディスタンス値を，OSPFv3 のエリア内経路のディスタンス値よりも大きな値（優先度が低い）に設定します。これによって，ネットワーク A への経路は OSPFv3 で学習した AS 内経路が選択されます。主回線障害時，本装置 A では該当する AS 内経路が削除されてスタティック経路を再選択しますが，本装置 C ではネットワーク A への経路情報が存在しなくなります。本装置 A でのネットワーク A へのスタティック経路情報を AS 外経路として本装置 C に広告するためには，本装置 A で経路再配布のコンフィグレーションを設定する必要があります。こうすることで，バックアップ回線上で Hello パケットを交換しないで主回線障害時にも OSPFv3 にネットワーク A への有用な経路情報を導入できます。

19.1.6 経路選択の基準

OSPFv3 では，LSA の生成や学習によって LSA が更新されるたびに，SPF 計算を実行します。SPF 計算では SPF アルゴリズムに基づいて経路を選択します。SPF アルゴリズムによって宛先への到達性がなくなった場合，経路を削除します。

エリアボーダルータでは，所属しているすべてのエリアについて，個別に SPF アルゴリズムに基づいて経路を選択します。

OSPFv3 での経路選択の判断基準を，優先順位が高い順に次に示します。なお，この優先順位は変更できません。

1. 経路情報の種類

   OSPFv3 の AS 内経路（エリア内経路，またはエリア間経路）を，AS 外経路より優先します。

2. 学習元ドメイン

   複数ドメインに経路が存在する場合，ディスタンス値が最小である経路を選択します。ディスタンス値が等しい場合，OSPFv3 ドメイン番号が最小の経路を選択します。

3. 経路の宛先タイプ

   - AS 内経路

     エリア内経路を，エリア間経路より優先します。

   - AS 外経路

     エリア内の AS 境界ルータが広告している経路を，別エリアの AS 境界ルータが広告している経路より優先します。

4. AS 外経路タイプ

メトリックタイプが Type1 の AS 外経路を，Type2 の AS 外経路より優先します。

5. AS 外経路で経由するエリア

エリアボーダであるルータでは，宛先の AS 境界ルータが複数のエリアに接続している場合，AS 境界ルータまでのコスト値が最も小さいエリアを選択します。コスト値が等しい場合，エリア ID の最も大きいエリアを選択します。

6. コスト

- AS 内経路

  宛先までのコスト値が最も小さい経路を優先します。

- Type1 の AS 外経路

  AS 外経路情報のメトリック値と AS 境界ルータまでのコスト値の合計が最も小さい経路を選択します。

- Type2 の AS 外経路

  AS 外経路情報のメトリック値が最も小さい経路を選択します。メトリック値が等しい場合，AS 境界ルータまでのコスト値が最も小さい経路を選択します。

7. ルータ ID

ネクストホップであるルータのルータ ID が最も小さい経路を選択します。

8. インタフェース ID

ネクストホップであるルータから，Hello パケットで最も小さいインタフェース ID を学習したインタフェースを選択します。

(1) ディスタンス値

本装置では，同一宛先への経路が各プロトコルによって複数存在する場合，それぞれの経路のディスタンス値が比較されて優先度の最も高い経路が有効になります。

OSPFv3 では，ディスタンス値のデフォルト値をドメインごとに設定できます。このディスタンス値は，AS 外経路，エリア内経路，エリア間経路で，それぞれ別の値を設定できます。

19.1.7 イコールコストマルチパス

OSPFv3 では，自ルータからある宛先についてイコールコストマルチパスが存在して，次の転送先ルータが複数ある場合，その宛先へのパケットの転送を複数のネクストホップへ分散することによって，トラフィックを分散できます。

本装置では，AS 内経路について，学習元ドメインと宛先タイプ（エリア内，またはエリア間経路）とコストが等しい複数のパスを選択します。AS 外経路についても同様に，学習元ドメインと AS 外経路タイプとコストとメトリックが等しい複数のパスを選択します。

maximum-paths コマンドで最大パス数を変更できます。デフォルト値は 4 です。

19.1.8 注意事項

(1) ルータ ID についての注意事項

OSPFv3 では，ネットワークのトポロジを構築するときに，ルータの識別にルータ ID を使用します。

ネットワークの設計時に異なるルータに同じ値のルータ ID を設定した場合，正確な経路選択ができなくなります。そのため，ネットワーク設計時には各ルータに重複しないルータ ID を割り当ててください。

なお，1 台のルータが複数の OSPFv3 ドメインに接続している場合，すべてのドメインで同一のルータ ID を使用しても問題ありません。

(2) 経路の再配布フィルタと学習フィルタの注意事項

OSPFv3 では，隣接ルータから学習したすべての LSA をほかの隣接ルータへ広告します。再配布フィルタによって，OSPFv3 で学習した経路の同一ドメイン内での広告を抑止できません。また，経路集約機能（ipv6 summary-address コマンド）を使用して OSPFv3 経路を集約する場合，集約元経路の広告を抑止する設定をしても，同一ドメイン内での LSA 広告は抑止されません。

distribute-list in コマンドでは，フィルタ条件に一致する AS 外経路の学習を抑止できます。ただし，LSA の学習，広告を制御できません。このため，学習しなかった経路も OSPFv3 で広告されます。

(3) マルチバックボーン機能使用時の注意事項

(a) マルチバックボーン使用についての注意

ネットワークを複数の OSPFv3 ドメインに分割して運用した場合，ルーティングループの抑止やコストに基づいた経路選択などの OSPFv3 の特長が，OSPFv3 ドメイン間の経路の選択や配布によって失われます。新規ネットワーク構築時など，ネットワークを複数の OSPFv3 ドメインに分割して運用する必要がない場合は，単一の OSPFv3 ネットワークとして構築することをお勧めします。

(b) 複数ドメインの設定についての注意

ループバックインタフェースに設定したアドレスを複数の OSPFv3 ドメインに広告する必要がある場合は，OSPFv3 AS 外経路として広告してください。コンフィグレーションで，一つのインタフェースを同時に複数の OSPFv3 ドメインに設定できません。

(4) OSPFv3 の制限事項

本装置は，RFC5340（OSPF for IPv6）に準拠しています。しかし，ソフトウェアの機能制限によって，次に示す機能はサポートしていません。

- AS 外経路のフォワーディングアドレスに基づく経路選択
- 非ブロードキャスト（NBMA）ネットワーク
- NSSA
- 認証

19.2　OSPFv3 基本機能のコンフィグレーション

19.2.1　コンフィグレーションコマンド一覧

OSPFv3 基本機能のコンフィグレーションコマンド一覧を次の表に示します。

表 19-3　OSPFv3 適用に関係するコンフィグレーションコマンド一覧

コマンド名	説明
disable	OSPFv3 動作を抑止します。
ipv6 ospf area	OSPFv3 が動作するドメイン番号とエリア ID を設定します。
router-id	ルータ ID（ルータの識別子）を設定します。

表 19-4　AS 外経路広告に関係するコンフィグレーションコマンド一覧

コマンド名	説明
default-metric	宛先までのメトリック値を設定します。
distribute-list out (OSPFv3)※	広告する経路を制御するための再配布フィルタを設定します。
redistribute (OSPFv3)※	AS 外経路を広告するための再配布フィルタを設定します。

注※
「コンフィグレーションコマンドレファレンス Vol.3　22. 経路フィルタリング」を参照してください。

表 19-5　経路選択や経路学習に関係するコンフィグレーションコマンド一覧

コマンド名	説明
distance ospf	OSPFv3 経路のディスタンス値を設定します。
ipv6 ospf cost	コスト値を設定します。
maximum-paths	イコールコストマルチパスの最大パス数を設定します。
timers spf	LSA の生成や学習から SPF 計算までの遅延時間と実行間隔を設定します。
distribute-list in (OSPFv3)※	AS 外経路の学習抑止を設定します。

注※
「コンフィグレーションコマンドレファレンス Vol.3　22. 経路フィルタリング」を参照してください。

19.2.2　コンフィグレーションの流れ

(1)　OSPFv3 基本機能の設定手順

1. あらかじめ，IPv6 インタフェースを設定します。
2. OSPFv3 を適用する設定をします。
   各ルータに，重複しないルータ ID を割り当ててください。
   IPv4 インタフェースが存在する場合，ルータ ID を自動選択できます。
3. AS 外経路広告の設定をします。

他プロトコルの経路を OSPFv3 で広告する場合，設定が必要です。

また，マルチバックボーン機能を使用してドメイン間で経路を再配布する場合，設定が必要です。

4.経路選択の設定をします。

特定インタフェースを経由する経路に重み付けが必要な場合，ipv6 ospf cost コマンドでコスト値を設定します。

19.2.3 OSPFv3 適用の設定

[設定のポイント]

ipv6 ospf area コマンドを指定したインタフェース上で，隣接ルータと LSA を交換します。

エリア分割をしない場合，エリア ID は全 OSPFv3 ルータで同じ値としてください。

[コマンドによる設定]

1. **(config)# ipv6 router ospf 1**

   ospfv3 モードへ移行します。ドメイン番号を 1 にします。

2. **(config-rtr)# router-id 172.16.1.1**

   (config-rtr)# exit

   ルータ ID として 172.16.1.1 を使用します。

3. **(config)# interface gigabitethernet 1/1**

   (config-if)# ipv6 ospf 1 area 0

   ドメイン 1 のエリア 0 で動作することを指定します。

19.2.4 AS 外経路広告の設定

[設定のポイント]

redistribute コマンドでは，再配布経路に付加する情報（メトリック値，タグ，メトリックタイプ）を設定できます。redistribute コマンドでメトリック値の指定を省略した場合，default-metric コマンドの設定値が有効になります。

なお，OSPFv3 で学習した経路について，同一ドメイン内での経路の再配布は制御できません。

[コマンドによる設定]

1. **(config)# ipv6 router ospf 1**

   (config-rtr)# default-metric 10

   デフォルトメトリックを 10 に設定します。

2. **(config-rtr)# redistribute static**

   スタティック経路を上記のデフォルトメトリック値で広告します。

19.2.5 経路選択の設定

[設定のポイント]

コストの設定は ipv6 ospf cost コマンドを使用して，インタフェース単位で設定します。

なお，maximum-paths コマンドで 1 を設定した場合，経路のコスト値が等しい場合でも，イコールコストマルチパスを構築しません。

ここでは，シングルパスの経路を使用する場合の設定例を示します。

[コマンドによる設定]

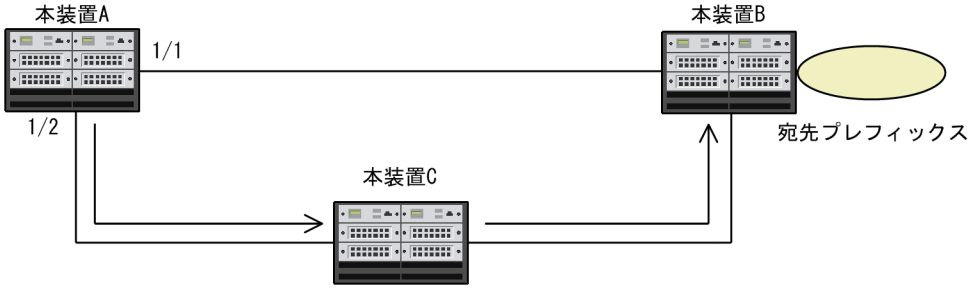
1. (config)# ipv6 router ospf 1
   (config-rtr)# maximum-paths 1
   (config-rtr)# exit
   OSPFv3 最大パス数を 1 に設定します。
2. (config)# interface gigabitethernet 1/1
   (config-if)# ipv6 ospf 1 area 0
   (config-if)# ipv6 ospf cost 10
   (config-if)# exit
   コストを 10 に設定します。
3. (config)# interface gigabitethernet 1/2
   (config-if)# ipv6 ospf 1 area 0
   (config-if)# ipv6 ospf cost 2
   コストを 2 に設定します。ポート 1/2 のコスト値をポート 1/1 のコスト値よりも小さくすることによって，ポート 1/2 を経由する経路が優先されます。

19.2.6　マルチパスの設定

[設定のポイント]

コスト値を調整することで，経路が経由するルータ数に関係なく宛先へのイコールコストマルチパスを構築できます。

図 19-5　マルチパスの構成



本装置 C を経由する場合，宛先までのコストは 2 です。ここでは，本装置 A でイコールコストマルチパスを構築する例を示します。

[コマンドによる設定]

1. (config)# interface gigabitethernet 1/2
   (config-if)# ipv6 ospf 1 area 0
   (config-if)# exit
2. (config)# interface gigabitethernet 1/1
   (config-if)# ipv6 ospf 1 area 0
   (config-if)# ipv6 ospf cost 2
   ポート 1/1 のコスト値を 2 とすることで，ポート 1/2 を経由する経路とコストを等しくします。

19.2.7 VRF での OSPFv3 の適用

[設定のポイント]

ipv6 ospf area コマンドを使用します。ループバックアドレスをルータ ID として使用して，VRF 2 で OSPFv3 を適用します。

[コマンドによる設定]

1. **(config)# interface loopback 2**
   インタフェースモードへ移行して，ループバック 2 の情報を指定します。
2. **(config-if)# vrf forwarding 2**
   (config-if)# ip address 172.16.1.1
   (config-if)# exit
   VRF2 を指定して，IP アドレスを 172.16.1.1 にします。
3. **(config)# interface gigabitethernet 1/1**
   インタフェースモードへ移行して，ポート 1/1 の情報を指定します。
4. **(config-if)# vrf forwarding 2**
   (config-if)# ipv6 address 2001:db8:1:1::1/64
   (config-if)# ipv6 enable
   VRF 2 を指定して，IPv6 アドレスを 2001:db8:1:1::1/64 にします。
5. **(config-if)# ipv6 ospf 1 area 0**
   ドメイン 1 のエリア 0 で OSPFv3 が動作することを指定します。

19.3　インタフェースの解説

19.3.1　OSPFv3 インタフェース種別

OSPFv3 では，OSPFv3 パケットの送受信上，ルータ間を接続するインタフェースを 3 種類に分類します。

- ブロードキャスト
  ブロードキャスト型ネットワーク上で，マルチキャストを使用してインタフェース上の複数の近隣ルータを統一的に管理します。
- non-broadcast（NBMA）（未サポート）
  ブロードキャスト型ネットワーク上で，ブロードキャストやマルチキャストを使用しないで複数の近隣ルータを統一的に管理します。
- ポイントーポイント
  近隣ルータを 1 台だけ管理します。なお，仮想リンク上では，ポイントーポイントインタフェースとして動作します。

(1)　OSPFv3 を使用するインタフェースの設定についての注意事項

OSPFv3 では，インタフェースに設定してある送信時パケットの最大長（MTU）と同じ長さのパケットを送信する場合があります。ここで，受信側のインタフェースに設定してある受信時パケットの最大長（MRU：特に記述がなければ MTU と同一）よりも長い場合，通常のトラフィックでは顕在化しないルータ間の相互通信不可能の問題が発生することがあります。そのため，OSPFv3 を使用する場合は，特にすべてのネットワークおよびネットワークに接続しているすべてのルータのインタフェースについて，MTU がほかのすべてのインタフェースの MRU 以下に設定してあることの確認をお勧めします。

19.3.2　隣接ルータとの接続

(1)　Hello パケット

OSPFv3 が動作しているルータは，ルータ間の接続性を検出するため，インタフェースごとに Hello パケットを送信します。Hello パケットを他ルータから受信することで，ルータ間で OSPFv3 が動作していることを認識します。

(2)　ルータ間接続条件

ルータ間を直接接続するネットワークのそれぞれで，接続するルータのインタフェースでのパラメータは，次に示す項目が一致している必要があります。これが一致していないルータ間では，OSPFv3 上は接続していないことになります。

(a)　エリア ID

ルータ間の直接接続では，両ルータのインタフェースに設定したエリアが一致している必要があります。

(b)　Hello Interval と Dead Interval

OSPFv3 では，直接接続しているルータに，自ルータを検出させるために Hello パケットを送信します。Hello Interval は Hello パケットの送信間隔です。Dead Interval は，あるルータからの Hello パケットを受信できないことを理由にそのルータとの接続が切れたと判断するまでの時間です。検出と切断を適切に判断するためには，直接接続しているルータのインタフェースに設定した，この二つの値が一致している必要があります。

(c) エリアの設定

スタブエリアとスタブでないエリアとでは，エリアに通知される情報が異なります。そのため，OSPFv3 が二つのルータを直接接続していると判断するには，インタフェースが所属しているエリアのスタブについての設定が一致している必要があります。

(d) インスタンス ID

OSPFv3 では，接続しているルータを複数のグループに分けるためにグループの識別子としてインスタンス ID を広告します。インスタンス ID は，経路情報を交換するルータのインタフェースに設定したインスタンス ID と一致している必要があります。

19.3.3 ブロードキャスト型ネットワークと指定ルータ

ブロードキャスト型ネットワークでは，トポロジ上の頂点であるネットワークとネットワークに直接接続しているルータ間の接続情報を管理するために，指定ルータ（Designated Router）とバックアップ指定ルータを選択します。指定ルータの障害時には，ネットワークの接続情報の管理ルータを速やかに移行するために，バックアップ指定ルータが指定ルータになります。

(1) 指定ルータおよびバックアップ指定ルータの選択

各ルータは，Hello パケットで該当するインタフェース上での指定ルータになる優先度（priority）を広告します。

インタフェース上に指定ルータもバックアップ指定ルータも存在しない場合は，最も priority の高いルータを指定ルータに選択します。指定ルータは存在するがバックアップ指定ルータが存在しない場合，指定ルータを除いて最も priority の高いルータをバックアップ指定ルータに選択します。両ルータとも存在する場合，新しくより priority の高いルータが現れても，選択は変更しません。

あるルータのあるインタフェースの priority を 0 に設定すると，このルータは該当するインタフェースが接続しているエリアでは，指定ルータにもバックアップ指定ルータにも選択されません。

ブロードキャスト型ネットワーク上に複数のルータがあり，このネットワークをトラフィックの転送に使用する場合は，どれかのルータのネットワークに接続しているインタフェースの priority を 1 以上にする必要があります。

19.3.4 LSA の送信

OSPFv3 では，隣接ルータとの間で互いに所持していない LSA を送信し合います。新たに LSA を生成または受信した場合，これを全隣接ルータに送信します。これによって，本装置と隣接ルータとの間で同じデータベースを保持するようにします。LSA の送受信によってデータベースの同期をとる関係を隣接関係と呼びます。

LSA 同期手順によって，本装置の LSA はすべての隣接ルータに送信されます。また，隣接ルータでは，隣接ルータのすべての隣接ルータに本装置の LSA を送信します。隣接ルータの隣接ルータでは，さらにその全隣接ルータに LSA を送信します。この手順によって，本装置の LSA は該当エリア上の全ルータに配布されます。

(1) LSA の Age

Age は LSA を生成してからの経過時間です。Age が 3600 秒になるか，生成元のルータによって削除されるまで，LSA を保持します。保持している LSA の Age に遅延時間（ipv6 ospf transmit-delay コマンドの設定値）を加算した値が，送信する LSA の Age フィールド値になります。

19.3.5 パッシブインタフェース

OSPFv3 の隣接ルータが存在しないインタフェースをパッシブインタフェースとして設定できます。また，ループバックインタフェースに OSPFv3 を適用した場合，パッシブインタフェースになります。

パッシブインタフェースでは，OSPFv3 パケットを送受信しません。

パッシブインタフェースの直結経路を，エリア内経路またはエリア間経路として広告します。

19.4 インタフェースのコンフィグレーション

19.4.1 コンフィグレーションコマンド一覧

OSPFv3 インタフェースのコンフィグレーションコマンド一覧を次の表に示します。

表 19-6 コンフィグレーションコマンド一覧

コマンド名	説明
ipv6 ospf dead-interval	隣接ルータから Hello パケットを受信できなくなったときに隣接関係を維持する時間を設定します。
ipv6 ospf hello-interval	Hello パケットの送信間隔を設定します。
ipv6 ospf network	インタフェース種別（ブロードキャストまたはポイントーポイント）を設定します。
ipv6 ospf priority	指定ルータになる優先度を設定します。
ipv6 ospf retransmit-interval	LSA の再送間隔を設定します。
ipv6 ospf transmit-delay	OSPFv3 パケットを送信するのに必要な遅延時間を設定します。
message-size (OSPFv3)	本装置が送信する OSPFv3 パケットの最大長を設定します。
passive-interface (OSPFv3)	パッシブインタフェースを設定します。

OSPFv3 動作に関係するコンフィグレーションコマンド一覧を次の表に示します。

表 19-7 コンフィグレーションコマンド一覧（OSPFv3 動作に関係するコマンド）

コマンド名	説明
system mtu※1	装置の MTU を設定します。
ip mtu※2	インタフェースでの送信 IP MTU 長を設定します。
interface loopback※3	ループバックインタフェースを設定します（OSPFv3 のパッシブインタフェースとして使用できます）。

注※1
「コンフィグレーションコマンドレファレンス Vol.1　16. イーサネット」を参照してください。

注※2
「コンフィグレーションコマンドレファレンス Vol.3　2. IPv4・ARP・ICMP」を参照してください。

注※3
「コンフィグレーションコマンドレファレンス Vol.3　4. ループバックインタフェース」を参照してください。

19.4.2 インタフェースパラメータ変更の設定

OSPFv3 を適用したインタフェースでは，コンフィグレーションのデフォルト値に従って Hello パケットの送信などをします。priority や passive-interface コマンドを設定することで，動作を変更できます。

(1) 指定ルータになる優先度

接続しているルータ数の多いネットワークでは，指定ルータの負荷は高くなります。そのため，このようなネットワークに複数接続しているルータが存在する場合，このルータが複数のネットワークの指定ルータにならないように priority を設定することをお勧めします。

[設定のポイント]

priority は，値が大きいほど優先度が高くなります。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   (config-if)# ipv6 ospf 1 area 0
   (config-if)# ipv6 ospf priority 10
   priority を 10 に設定します。

(2) パッシブインタフェース

[設定のポイント]

passive-interface コマンドを使用します。ipv6 ospf cost コマンドを指定した場合，指定したコスト値で直結経路を広告します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/2**
   (config-if)# ipv6 ospf 1 area 0
   (config-if)# ipv6 ospf cost 10
   (config-if)# exit
   OSPFv3 を適用します。
2. **(config)# ipv6 router ospf 1**
   (config-rtr)# passive-interface gigabitethernet 1/2
   ポート 1/2 をパッシブインタフェースに設定します。

19.5 OSPFv3 のオペレーション

19.5.1 運用コマンド一覧

OSPFv3 の運用コマンド一覧を次の表に示します。

表 19-8 運用コマンド一覧

コマンド名	説明
show ipv6 route	ルーティングテーブルに登録されている内容を表示します。
clear ipv6 route	H/W の IPv6 フォワーディングエントリをクリアして再登録します。
show ipv6 ospf	ドメイン，隣接ルータ情報，インタフェース情報，LSA などを表示します。
clear ipv6 ospf	OSPFv3 プロトコルに関する情報をクリアします。

19.5.2 ドメインの確認

OSPFv3 が動作中の場合，ルータ ID やディスタンス値などの設定内容は show ipv6 ospf コマンドで確認します。

図 19-6 show ipv6 ospf コマンドの実行結果

```
>show ipv6 ospf
Date 20XX/03/14 12:00:00 UTC
Domain: 1
Router ID: 172.16.1.1
Distance:
  Intra Area: 10, Inter Area: 10, External: 150
Flags: <AreaBorder ASBoundary>
SPF Interval: 7s, SPF Delay: 3s
Area: 1, Interfaces: 1
    Network Range                                 State
    -                                             -
```

19.5.3 隣接ルータ情報の確認

隣接ルータのリンクローカルアドレス（Neighbor Address），隣接状態（State），ルータ ID（Router ID），Priority は，show ipv6 ospf neighbor コマンドで確認します。

OSPFv3 インタフェースでは，指定ルータ（Designated Router）とそのほかのルータの間で隣接関係を確立します。この進行状況は，隣接状態によって確認できます。

隣接関係が確立した場合，隣接状態は Full になります。Full でない状態では，隣接関係を確立している途中であり，そのインタフェースでは OSPFv3 経路を学習しません。

詳細は，show ipv6 ospf interface または show ipv6 ospf neighbor detail コマンドで確認します。インタフェース状態（State）や Network Type，隣接ルータとの接続性を確認できます。

- Network Type の OSPFv3 ネットワーク種別が，隣接ルータの OSPFv3 ネットワーク種別と同じであることを確認してください。
- インタフェースの状態が DR または P to P の場合，Neighbor List 内の全隣接ルータ状態が Full となっていることを確認してください。
  - Full でない場合，隣接ルータとの隣接関係が確立していません。隣接ルータを調査してください。

- インタフェースの状態が BackupDR または DR Other の場合，Neighbor List 内に DR となる隣接ルータが存在するか確認してください。
  - DR が存在して DR の隣接ルータ状態が Full でない場合，DR との隣接関係が確立していません。隣接ルータを調査してください。
  - DR が存在しない場合は，自装置および隣接ルータの Priority が設定されていない可能性があります。自装置および隣接ルータの Priority を確認してください。

図 19-7 show ipv6 ospf neighbor コマンドの実行結果

```
>show ipv6 ospf neighbor
Date 20XX/03/14 12:00:00 UTC
Domain: 1
Area: 0
Neighbor Address          State               Router ID   DeadTime Interface
fe80::212:e2ff:fe86:5303  Full/BackupDR       172.16.10.12      10 Eth1/3
fe80::212:e2ff:fe86:5304  Full/DR Other       172.16.10.13      20 Eth1/3
fe80::212:e2ff:fe86:5305  Exch Start/DR Other 172.26.10.14       5 Eth1/3
```

図 19-8 show ipv6 ospf interface コマンド（個別インタフェース指定）の実行結果

```
>show ipv6 ospf interface gigabitethernet 1/1
Date 20XX/05/30 12:00:00 UTC
Domain: 1
Area: 0
Interface ID: 2,Link Local Address : fe80::212:e2ff:fe86:5300%Eth1/1
    IPv6 Address: -
    MTU: 1460, DDinPacket: 71, LSRinPacket: 120, ACKinPacket:72
    Router ID: 172.16.1.1, Network Type: P to P, State: P to P
    DR: none, Backup DR: none
    Priority: 0, Cost: 1, Instance: 0
    Transmit Delay: 1s
    Intervals:
        Hello: 10s, Dead: 40s, Retransmit: 5s

  Neighbor List (1):
    Address                   State        Router ID         Priority
    fe80::212:e2ff:fe86:5301  Full         172.16.1.2           0
>
```

図 19-9 show ipv6 ospf neighbor コマンド（detail パラメータ指定）の実行結果

```
>show ipv6 ospf neighbor detail
Date 20XX/05/30 12:00:00 UTC
Domain: 1
Area: 0
Interface: Eth1/2, Interface State: Backup DR
    Neighbor Address: fe80::212:e2ff:fe86:5302, State: Full/DR
    Neighbor Router ID: 172.16.10.11, Priority: 1
    Neighbor Interface ID: 2
    DR: 172.16.10.11, Backup DR: 172.16.10.10
    DeadTime: 6s, Up: 45d 12h, Adjacent: 45d 12h
    Last Hello: 6s, Last Exchange: 45d 12h
    DS: 0, LSR: 0, Retrans: 0, <Master>
    Track Name: -, Track ID: -, Track State: -
    Neighbor Address: fe80::212:e2ff:fe86:5312, State: Full/DR Other
    Neighbor Router ID: 172.16.10.12, Priority: 1
    Neighbor Interface ID: 404
    DR: 172.16.10.11, Backup DR: 172.16.10.10
    DeadTime: 36s, Up: 10d 12h, Adjacent: 10h 11m
    DS: 0, LSR: 0, Retrans: 1, <>
    Track Name: -, Track ID: -, Track State: -
>
```

19.5.4 インタフェース情報の確認

OSPFv3 が動作しているインタフェース名（Interface），状態（State），Priority，コスト値（Cost），隣接ルータ数（Neighbor）は，show ipv6 ospf interface コマンドで確認します。

なお，IPv6 インタフェースがダウンしている場合，インタフェースの情報は表示されません。

図 19–10 show ipv6 ospf interface コマンドの実行結果

```
>show ipv6 ospf interface
Date 20XX/03/14 12:00:00 UTC
Domain: 1
Area: 0
  Interface         State     Priority  Cost   Neighbor
  Eth1/3            DR           1      1      1

Area: 1
  Interface         State     Priority  Cost   Neighbor
  Eth1/4            BackupDR     10     20     10
```

19.5.5 LSA の確認

(1) LSA 数

OSPFv3 で保持している LSA の数は，show ipv6 ospf database database-summary コマンドで確認します。

図 19–11 show ipv6 ospf database database-summary コマンドの実行結果

```
>show ipv6 ospf database database-summary
Date 20XX/03/14 12:00:00 UTC
Domain: 1
Local Router ID: 172.16.251.141
Area: 0
  [Linklocal scope]
    Link             :     1
    Opaque-Link      :     1
    Grace            :     0
    -----------------------
    Total                  2
  [Area scope]
    Router           :     2
    Network          :     0
    Inter-Area-Prefix:     0
    Inter-Area-Router:     1
    Intra-Area-Prefix:     1
    -----------------------
    Total                  4

[AS scope]
    External:     1
>
```

(2) LSA の広告情報

show ipv6 ospf database コマンドでは LSA の一覧を表示して，LSA の種別ごとに LSID や Age を確認できます。各 LSA は，広告元ルータ ID（Advertising Router）と LSID によって区別できます。

本装置が次に示す LSA を広告していることを確認してください。

1. Router-LSA を広告していること
   表示される LSID は LSA の識別子です。本装置が広告元の Router-LSA では，常に 0 になります。
2. 本装置が指定ルータとなっているインタフェースが存在する場合，Network-LSA を広告していること
   表示される LSID はインタフェース ID（Link-LSA の LSID と同じ値）です。
3. 各インタフェースに Link-LSA を広告していること
   表示される LSID はインタフェース ID です。
4. 本装置が AS 境界ルータである場合，広告対象の経路を AS-external-LSA として広告していること

広告している経路の宛先を確認する場合，show ipv6 ospf database external コマンドで詳細情報を表示してください。

図 19-12 show ipv6 ospf database コマンドの実行結果

```
>show ipv6 ospf database
Date 20XX/03/14 12:00:00 UTC
Domain: 1
Local Router ID: 172.16.251.141
Area: 0
  LS Database: Router-LSA
    Advertising Router  LSID      Age   Sequence  Checksum  Length
    10.0.1.3            00000000  221   8000000b  0dad      40
    172.16.251.141      00000000  275   80000002  6d7a      24
  LS Database: Network-LSA
    Advertising Router  LSID      Age   Sequence  Checksum  Length
    10.0.1.3            00000000  221   8000000b  0dad      40
    172.16.251.141      00000002  226   80000002  94f6      32
  LS Database: Inter-Area-Prefix-LSA
    Advertising Router  LSID      Age   Sequence  Checksum  Length
    10.0.1.3            00000001  210   80000002  7d89      32
    192.168.217.123     00000001  210   80000003  7d89      32
  LS Database: Inter-Area-Router-LSA
    Advertising Router  LSID      Age   Sequence  Checksum  Length
    172.16.251.141      0301000a  262   80000002  4e74      32
    172.16.251.143      0301000a  262   80000002  4e74      32
  LS Database: Link-LSA
  Interface: Eth1/3
    Advertising Router  LSID      Age   Sequence  Checksum  Length
    10.0.1.3            00000001  336   80000001  87f0      44
    172.16.251.141      00000001  399   80000002  7e8d      44
  Interface: Eth1/4
    Advertising Router  LSID      Age   Sequence  Checksum  Length
    172.16.251.141      00000002  399   80000002  7e8d      44
  LS Database: Intra-Area-Prefix-LSA
    Advertising Router  LSID      Age   Sequence  Checksum  Length
    172.16.251.141      00000001  275   80000002  0d9a      52

AS:
  LS Database: AS-external-LSA
    Advertising Router  LSID      Age   Sequence  Checksum  Length
    172.16.251.141      00000001  275   80000002  0d9a      52
```

show ipv6 ospf database external コマンドでは，AS 外経路の宛先 Prefix，メトリックなどを確認できます。

図 19-13 show ipv6 ospf database external コマンドの実行結果

```
> show ipv6 ospf database external
Date 20XX/03/14 12:00:00 UTC
Domain: 1
Local Router ID: 172.16.251.141
LS Database: AS-external-LSA
Advertising Router: 172.16.251.141
    LSID: 00000000, Age: 6, Length: 44
    Sequence: 80000001, Checksum: 5373
    Prefix: 2001:db8:4:1::1/128
       Prefix Options: <LocalAddress>
       Type: 2, Metric: 20, Tag: ----
```

20 OSPFv3 拡張機能

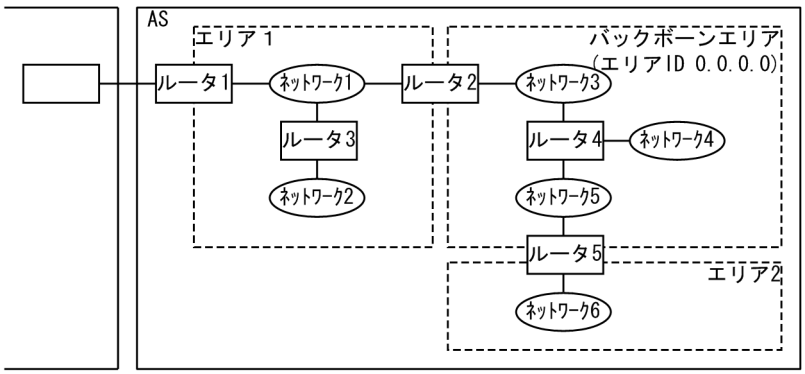
この章では，OSPFv3 の拡張機能について説明します。

20.1　エリアとエリア分割機能の解説

20.1.1　エリアボーダ

OSPFv3 では，ルーティングに必要なトラフィックと，経路選択に使用するアルゴリズムの処理に必要な時間を削減するために，AS を複数のエリアに分割できます。エリア分割を使用した OSPFv3 ネットワークトポロジの例を次の図に示します。

図 20-1　エリア分割を使用した OSPFv3 ネットワークトポロジの例



ルータ 2 やルータ 5 のように，複数のエリアに所属するルータをエリアボーダルータと呼びます。

あるエリア内の接続状態の情報は，ほかのエリアには通知されません。また，ルータには，接続していないエリアの接続状態の情報はありません。

(1)　バックボーン

エリア ID が 0.0.0.0 であるエリアをバックボーンと呼びます。AS が複数のエリアに分割されている場合，バックボーンには特別な役割があります。AS を複数のエリアに分割する場合は，エリアのどれか一つをバックボーンエリアとして設定する必要があります。ただし，一つの AS にバックボーンを二つ以上ある構成にしないでください。そのような構成の場合，情報がそれぞれのバックボーンに分散されるため，到達不能である経路が発生したり，最適な経路を選択しなかったりすることがあります。

エリアボーダルータは，バックボーンを通じてエリア間の経路情報を交換するため，必ずバックボーンに所属する必要があります。

(2)　エリア分割についての注意事項

エリア分割をすると，ルータや経路情報トラフィックの負荷が減る一方で，OSPFv3 のアルゴリズムが複雑になります。特に，障害に対して適切な動作をする構成が困難になります。ルータやネットワークの負荷に問題がない場合は，エリア分割をしないことをお勧めします。

(3)　エリアボーダルータについての注意事項

- エリアボーダルータでは，所属しているエリアの数だけ SPF アルゴリズムを動作させます。エリアボーダルータには，あるエリアのトポロジ情報を要約してほかのエリアへ通知する機能があります。そのため，所属するエリアの数が多くなるとエリアボーダルータの負荷が高くなります。そのため，エリアボーダルータにあまり多くのエリアを所属させないようなネットワーク構成にすることをお勧めします。

- あるエリアにエリアボーダルータが一つしかない場合，このエリアボーダルータに障害が発生すると，バックボーンから切り放されてほかのエリアとの接続性が失われます。重要な機能を提供するサーバや重要な接続のある AS 境界ルータの存在するエリアには複数のエリアボーダルータを配置して，エリアボーダルータの配置に対して十分な迂回路が存在するように，ネットワークを構築することをお勧めします。

20.1.2　エリア分割した場合の経路制御

エリアボーダルータは，バックボーンを除くすべての所属しているエリアの経路情報を要約した上で，バックボーンに所属するすべてのルータへ通知します。また，バックボーンの経路情報の要約と，バックボーンに流れている要約されたほかのエリアの経路情報を，バックボーン以外の接続しているエリアのルータへ通知します。

あるルータが，あるアドレスについて要約された経路情報を基に経路を決定した場合，このアドレス宛ての経路は要約された経路情報の通知元であるエリアボーダルータを経由します。そのため，異なるエリア間を結ぶ経路は必ずバックボーンを経由します。

エリアボーダルータでは，あるエリアの経路情報をほかのエリアに広告するに当たってルータやネットワーク間の接続状態と接続のコストによるトポロジ情報を，エリアボーダルータからルータやネットワークへのコストに要約します。これらの要約された情報をエリア間経路情報と呼びます（ネットワークの情報は Type3LSA で，AS 境界ルータの情報は Type4LSA で広告します）。

(1)　エリアボーダルータでの経路の集約

経路の集約および抑止とエリア外への要約を次の表に示します。

表 20-1　経路の集約および抑止とエリア外への要約

エリア内のネットワークアドレス	集約および抑止の設定	エリア外へ通知する要約
2001:db8:811:10::/60 2001:db8:811:20::/61 2001:db8:811:28::/61 2001:db8:811:30::/60	なし	2001:db8:811:10::/60 2001:db8:811:20::/61 2001:db8:811:28::/61 2001:db8:811:30::/60
2001:db8:811:10::/60 2001:db8:811:20::/61 2001:db8:811:28::/61 2001:db8:811:30::/60	2001:db8:811::/59 2001:db8:811:20::/60	2001:db8:811::/59 2001:db8:811:20::/60 2001:db8:811:30::/60
2001:db8:811:10::/60 2001:db8:811:20::/61 2001:db8:811:28::/61 2001:db8:811:30::/60 2001:db8:811:ff00::/58	2001:db8:811::/58（抑止） 2001:db8:811:ff00::/56	2001:db8:811:ff00::/56

エリアボーダルータでのエリア内のトポロジ情報を要約するに当たって，アドレスの範囲をコンフィグレーションで設定するとその範囲に含まれる経路情報を一つに集約できます。アドレスの範囲は，area range コマンドでプレフィックスとプレフィックス長を設定します。また，広告を抑止するパラメータを指定できます。

コンフィグレーションで設定したプレフィックスの範囲に含まれるネットワークがエリア内に一つでもあった場合，範囲に含まれるすべてのネットワークをこのプレフィックスを宛先とする経路情報へ集約して

ほかのエリアへ通知します。範囲に含まれる各ネットワークは，このエリアボーダルータからほかのエリアへは通知されません。このとき，集約した経路情報のコストには範囲に含まれるネットワーク中の最も大きなコストを使用します。

広告を抑止した場合，範囲内の各ネットワークをほかのエリアへは通知しない上に，プレフィックスに集約した経路もほかのエリアへは通知しません。この結果，ほかのエリアからはこのエリアボーダルータ経由で指定した範囲に含まれるアドレスへの経路は存在しないように見えます。

20.1.3　スタブエリア

バックボーンではなく，AS 境界ルータが存在しないエリアをスタブエリアとして設定できます。この設定には，コンフィグレーションコマンド area stub を使用します。

エリアボーダルータは，スタブエリアとして設定したエリアに AS 外経路を導入しません。これによってスタブエリア内では経路情報を減らして，ルータの情報の交換や経路選択の負荷を減らせます。エリアボーダルータは，AS 外経路の代わりとして，スタブエリアにデフォルトルートを導入します。

area stub コマンドで no-summary パラメータを指定した場合，エリア外の経路（エリア間経路情報）の広告を抑止します（エリア外への経路はデフォルトルートだけとなります）。

20.1.4　仮想リンク

OSPFv3 では，スタブエリアとして設定してなくてバックボーンでもないエリア上のある二つのエリアボーダルータで，このエリア上の二つのルータ間の経路をポイントーポイント型回線と仮想することによって，バックボーンのインタフェースとして使用できます。この仮想の回線のことを仮想リンクと呼びます。仮想リンクの実際の経路があるエリアのことを，仮想リンクの通過エリアと呼びます。

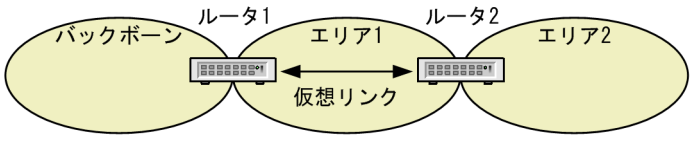
仮想リンクの使い方として，次に示す三つの例を挙げます。

- バックボーンに物理的に接続していないエリアの仮想接続
- 複数のバックボーンの結合
- バックボーンの障害による分断に対する経路の予備

(a)　バックボーンに物理的に接続していないエリアの仮想接続

次の図で，エリア 2 はバックボーンに接続していません。この場合，ルータ 1 とルータ 2 の間にエリア 1 を通過エリアとする仮想リンクを設定すると，ルータ 2 はバックボーンに接続するエリアボーダルータとなって，エリア 2 をバックボーンに接続していると見なせるようになります。

図 20-2　エリアのバックボーンへの接続



(b)　複数のバックボーンの結合

次の図では，AS 内にバックボーンであるエリアが二つ存在します。この状態では，バックボーンの分断による経路到達不能などの障害が発生することがあります。この場合，ルータ 1 とルータ 2 の間にエリア 1 を通過エリアとする仮想リンクを設定すると，バックボーンが結合されてこの障害を回避できます。

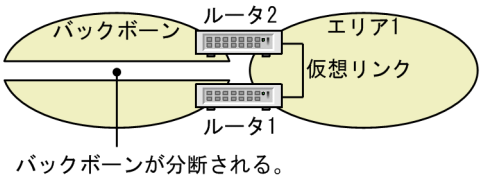
図 20-3　バックボーン間の接続



(c)　バックボーンの障害による分断に対する経路の予備

次の図では，バックボーンでネットワークの障害が発生してルータ 1 とルータ 2 の間の接続が切断された場合，バックボーンが分断されます。この場合，ルータ 1 とルータ 2 の間にエリア 1 を通過エリアとする仮想リンクを設定すると，これがバックボーンの分断に対する予備の経路（バックボーンでのルータ 1－ルータ 2 のコストと比較して，仮想リンクのコストが十分に小さい場合には，主な経路）となります。

図 20-4　バックボーン分断に対する予備経路



20.1.5　仮想リンクの動作

仮想リンクは，仮想リンクの両端のルータで共に設定する必要があります。仮想リンクの両端のルータは，IPv6 グローバルアドレスを使用して仮想リンクの隣接ルータと OSPFv3 パケットを送受信します。このアドレスには，通過エリアに属しているインタフェースに設定されている IPv6 アドレスを使用します。

仮想リンクを運用するに当たって，次のことに注意してください。

- 通過エリア上の任意のインタフェースに IPv6 グローバルアドレスが設定されている必要があります。IPv6 グローバルアドレスを一つも広告していない隣接ルータとは仮想リンクは動作しません。
- 仮想リンクのコストは，通過エリアでの仮想リンクの両端のルータ間の経路コストになります。
- 通過エリアで，仮想リンクの両端のルータ間の経路がイコールコストマルチパスの場合，一般のトラフィックと仮想リンク上の経路情報トラフィックでは経路が異なることがあります。

(1)　隣接ルータとの接続

仮想リンクがアップしている間，ルータ間の接続性を検出するため，仮想リンクの隣接ルータに Hello パケットを送信します。なお，通過エリア内に仮想リンクの相手ルータへ到達するパスがあるとき，仮想リンクがアップします。

Hello パケットを他ルータから受信することによって，ルータ間で OSPFv3 が動作していることを認識します。

Hello パケットに関するコンフィグレーションは，area virtual-link コマンドで設定します。dead-interval は，通過エリア上での仮想リンクの両端ルータ間の経路を構成する各ネットワーク上の，各インタフェースのインターバル値（ipv6 ospf dead-interval コマンドの設定値）のどれよりも長くする必要があります。この値をどれよりも短く設定した場合，通過エリア内の経路上のネットワーク障害に当たって，通過エリア内の代替経路への交替に基づいて仮想リンクが使用する経路が交替するよりも先に，仮想リンクが切断することがあります。

LSA の再送間隔（area virtual-link コマンドの retransmit-interval パラメータ）は，仮想リンクの両端ルータ間をパケットが往復するのに必要な時間よりも十分に長く設定する必要があります。

20.2　エリアのコンフィグレーション

20.2.1　コンフィグレーションコマンド一覧

スタブエリアを使用する場合と，エリアボーダルータとして動作する場合のコンフィグレーションコマンド一覧を次に示します。

なお，「19　OSPFv3」で解説している機能のコマンドは，「表 19–4　AS 外経路広告に関係するコンフィグレーションコマンド一覧」，「表 19–5　経路選択や経路学習に関係するコンフィグレーションコマンド一覧」，「表 19–6　コンフィグレーションコマンド一覧」を参照してください。

表 20–2　エリアに関係するコンフィグレーションコマンド一覧

コマンド名	説明
area default-cost	スタブエリアに広告するデフォルトルートのコスト値を設定します。
area range	エリアボーダルータでエリア間経路を，指定したプレフィックスに集約して広告します。
area stub	スタブエリアとして動作します。
area virtual-link	仮想リンクを設定します。

表 20–3　OSPFv3 適用に関係するコンフィグレーションコマンド一覧

コマンド名	説明
disable	OSPFv3 動作の抑止を設定します。
ipv6 ospf area	OSPFv3 が動作するドメイン番号とエリア ID を設定します。
router-id	ルータ ID（ルータの識別子）を設定します。

20.2.2　コンフィグレーションの流れ

(1)　エリアボーダでない場合のスタブエリアの設定

1. あらかじめ，IPv6 インタフェースを設定します。
2. スタブエリアの設定をします。
3. OSPFv3 を適用する設定をします。

(2)　エリアボーダルータの設定手順

1. あらかじめ，IPv6 インタフェースを設定します。
2. スタブエリアとして動作するエリアを設定します。
3. 経路集約の設定をします。
4. OSPFv3 を適用する設定をします。

   複数のエリアを設定します。この際，エリア 0（バックボーン）に所属するインタフェースの設定，または仮想リンクの設定が必要です。
5. 仮想リンクの設定をします。

20.2.3　スタブエリアの設定

[設定のポイント]

エリアボーダルータは，area stub コマンドを設定したエリア内にデフォルトルートを広告します。

スタブエリアの設定は，同一エリア内の全ルータに設定する必要があります。

[コマンドによる設定]

1. **(config)# ipv6 router ospf 1**

   ospfv3 モードへ移行します。ドメイン番号を 1 にします。

2. **(config-rtr)# area 1 stub**

   エリア 1 をスタブエリアに設定します。

3. **(config-rtr)# router-id 172.16.1.1**

   (config-rtr)# exit

   ルータ ID として 172.16.1.1 を使用します。

4. **(config)# interface gigabitethernet 1/2**

   (config-if)# ipv6 ospf 1 area 1

   ドメイン 1 のエリア 1 で動作することを指定します。

20.2.4　エリアボーダルータの設定

[設定のポイント]

area range コマンドでは，not-advertise パラメータを指定することで，このプレフィックスの範囲に含まれるネットワークのエリア外への広告を抑止できます。

集約および抑止するアドレスの範囲は，一つのエリアについて複数設定できます。また，エリア内にどの設定の範囲にも含まれないアドレスを使用しているルータやネットワークが存在してもかまいません。ただし，ネットワークを構成するに当たって，トポロジと合ったアドレスを割り当てた上でトポロジに応じた範囲を使用して集約を設定すると，選択する経路の適切さを損なわないで，効率的に OSPFv3 の経路情報トラフィックを削減できます。

ここでは，エリア 0 とエリア 1 に属するエリアボーダルータでの経路集約の設定例を示します。

[コマンドによる設定]

1. **(config)# ipv6 router ospf 1**

   (config-rtr)# area 0 range 2001:db8:811::/59

   エリア 0 でプレフィックス 2001:db8:811::/59 の範囲内の経路を学習した場合，エリア 1 に集約経路を広告します。

2. **(config-rtr)# area 1 range 2001:db8:811:20::/60**

   (config-rtr)# exit

   エリア 1 でプレフィックス 2001:db8:811:20::/60 の範囲内の経路を学習した場合，エリア 0 に集約経路を広告します。

3. **(config)# interface gigabitethernet 1/3**

   (config-if)# ipv6 ospf 1 area 0

   (config-if)# exit

   (config)# interface gigabitethernet 1/1

   (config-if)# ipv6 ospf 1 area 1

OSPFv3 を適用するインタフェースを設定することによって，エリア 0 とエリア 1 のエリアボーダとなります。

20.2.5　仮想リンクの設定

[設定のポイント]

area virtual-link コマンドで，相手ルータのルータ ID を指定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   (config-if)# ipv6 ospf 1 area 1
   (config-if)# exit
   OSPFv3 を適用します。
2. **(config)# ipv6 router ospf 1**
   (config-rtr)# area 1 virtual-link 10.0.0.1
   (config-rtr)# area 1 virtual-link 10.0.0.2
   通過エリア 1 の相手ルータを設定します。

20.3　ノンストップルーティングの解説

20.3.1　概要

ノンストップルーティングは，系切替によって運用系 BCU が交替したときに系切替前のルーティングプロトコルの状態を引き継いで，新運用系 BCU で継続して動作することでネットワーク全体での通信を維持するための機能です。

上記の実現のために，OSPFv3 ではあらかじめルーティングプロトコルの状態を他系 BCU 間で同期します。系切替時には，新運用系 BCU が Hello パケットや LSA の送受信を継続することで，系切替を隣接ルータから隠します。

ノンストップルーティングは装置単体で動作する機能のため，隣接ルータがノンストップルーティングをサポートしている必要はありません。

20.3.2　注意事項

ノンストップルーティングを使用する場合，ルータ ID を固定するためにコンフィグレーションコマンド router-id を設定するか，ループバックインタフェースに IPv4 アドレスを設定してください。どちらも設定しない場合，ノンストップルーティングによる系切替の前後で，ルータ ID が変更されるおそれがあります。ルータ ID が変更されると，ノンストップルーティングに失敗します。

20.4　ノンストップルーティングのコンフィグレーション

20.4.1　コンフィグレーションコマンド一覧

ノンストップルーティングのコンフィグレーションコマンド一覧を次の表に示します。

表 20-4　コンフィグレーションコマンド一覧

コマンド名	説明
nsr	ノンストップルーティングを有効にします。

20.4.2　ノンストップルーティングの設定

[設定のポイント]

ユニキャストルーティングプログラムの再起動時に系切替することを指定して，ノンストップルーティングを有効にします。

[コマンドによる設定]

1. **(config)# failure-action software unicast switchover**
   ユニキャストルーティングプログラムの再起動時に系切替します。
2. **(config)# ipv6 router ospf 1**
   (config-rtr)# router-id 192.168.1.100
   (config-rtr)# nsr
   ノンストップルーティングを使用する設定をします。

20.5　グレースフル・リスタートの解説

20.5.1　概要

グレースフル・リスタートは，系切替によって運用系 BCU が交替したときや，運用コマンドなどによってユニキャストルーティングプログラムが再起動したときに，ネットワークから経路が消えることによる本装置を中継する通信の停止を防ぐための機能です。

OSPFv3 では，グレースフル・リスタートによって OSPFv3 を再起動する装置のことをリスタートルータと呼びます。リスタートルータにあるグレースフル・リスタートをする機能をリスタート機能と呼びます。また，グレースフル・リスタートを補助する隣接装置をヘルパールータと呼びます。ヘルパールータにあるグレースフル・リスタートを補助する機能をヘルパー機能と呼びます。

本装置は，リスタート機能とヘルパー機能をサポートしています。

20.5.2　ヘルパー機能

本装置はヘルパールータとして動作している場合，グレースフル・リスタートをしている間リスタートルータを経由する経路を維持します。

(1)　ヘルパー機能の動作条件

ヘルパー機能が動作する条件を次に示します。

- すでに同一ドメイン内で別のリスタートルータのヘルパーとなっていないこと
  同一ドメイン内で，複数ルータのグレースフル・リスタートに対して同時にヘルパールータとして動作できません。ただし，リスタートルータが 1 台しかない場合，そのリスタートルータと接続しているすべてのインタフェースでヘルパールータとして動作します。
- 自ルータがリスタートルータとして，グレースフル・リスタートを実行していないこと
- リスタートルータに送信した OSPFv3 の Update パケットに対する Ack 待ちの状態でないこと

(2)　ヘルパー機能が失敗するケース

ヘルパールータとしての動作は，隣接が確立するまで，または，リスタートルータから終了の通知を受信するまで継続します。

しかし，次のイベントが発生した場合，リスタートルータが維持している経路と不整合が発生するおそれがあるため，ヘルパー機能を中断して経路を再計算します。

- 隣接ルータから新しい LSA（定期更新を除く）を学習して，リスタートルータへ広告した場合
- OSPFv3 インタフェースがダウンした場合
- リスタートルータ以外のルータとの隣接関係の切断または確立によって LSA を更新した場合
- OSPFv3 の同一ドメイン内で，複数のルータが同時に再起動した場合
- graceful-restart mode コマンドでコンフィグレーションを削除して，ヘルパー機能を削除した場合

20.5.3　リスタート機能

次の契機で，OSPFv3 のリスタート機能が動作します。

- 系切替によって運用系 BCU が交替したとき
- ユニキャストルーティングプログラムが再起動したとき

(1)　GraceLSA

本装置は，グレースフル・リスタートの開始や終了を通知するために，Type11 の GraceLSA を広告します。この LSA フォーマットは，draft-ietf-ospf-ospfv3-graceful-restart に準拠しています。

(2)　グレースフル・リスタートの手順

OSPFv3 のグレースフル・リスタート手順を次の図および表に示します。

図 20-5　OSPFv3 グレースフル・リスタート手順

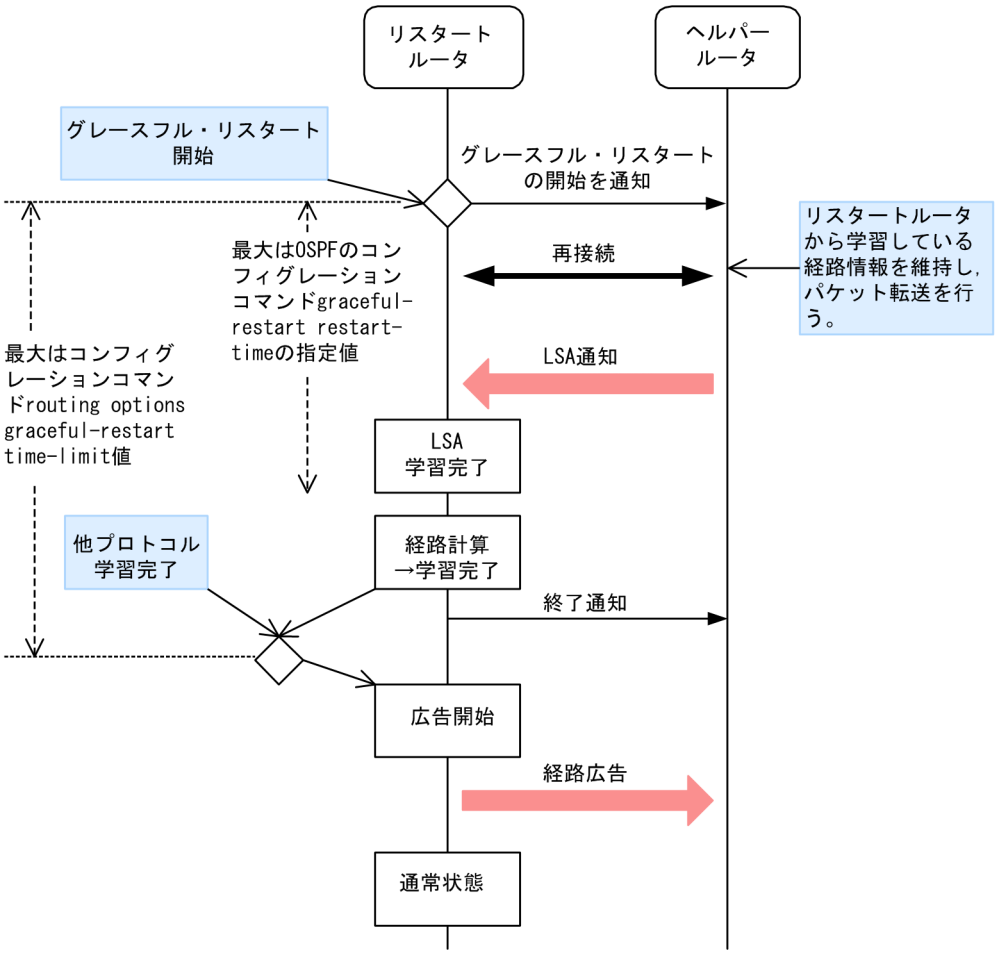


表 20-5　OSPFv3 グレースフル・リスタート手順

項番	項目	契機	処理内容
1	グレースフル・リスタートの開始	系切替によって運用系 BCU が交替したとき。	グレースフル・リスタートを開始します。通常の接続手順と同様に，各インタフェースで OSPFv3 情報のパケットを交換します。
		ユニキャストルーティングプログラムが再起動したとき。	

項番	項目	契機	処理内容
2	経路計算	ドメイン内の全 OSPFv3 インタフェースについて再接続が完了して，隣接ルータからすべての LSA を学習したとき。	ドメインごとに経路計算をして，ルーティングテーブルを更新します。複数のドメインが存在する場合，経路計算は接続の終わったドメインから随時します。経路計算が全ドメインで終了したとき，OSPFv3 の経路学習が完了します。
		1 インタフェースでもグレースフル・リスタートに失敗したとき。	その時点での同一ドメイン内の各インタフェースの接続状態に基づいて，経路計算をします。
3	広告開始	OSPFv3 の経路学習が完了して，かつほかのルーティングプロトコルの経路学習が完了したとき。	AS 外経路の広告を開始します。広告完了後，通常の OSPFv3 動作に戻ります。
		OSPFv3 のグレースフル・リスタートに失敗したとき。	

(3) グレースフル・リスタートが失敗するケース

OSPFv3 のグレースフル・リスタートが失敗するケースを次に示します。

- グレースフル・リスタートの開始をヘルパールータへ通知してからリスタート時間（OSPFv3 のコンフィグレーションコマンド graceful-restart restart-time の指定値）が経過しても LSA 学習を完了できなかった場合
- 再接続しているインタフェースがダウンした場合
- OSPFv3 ドメイン上で LSA が変更された場合
- OSPFv3 ドメイン上の別のルータがグレースフル・リスタートした場合
- グレースフル・リスタートを開始してから経路保持時間（コンフィグレーションコマンド routing options graceful-restart time-limit の指定値）が経過しても全プロトコルの経路学習が完了しなかった場合
- コンフィグレーションコマンド graceful-restart mode を変更して，リスタート機能を削除した場合

(4) 注意事項

- リスタートルータとしてグレースフル・リスタートを開始しても，一部のヘルパールータがヘルパー動作を開始しない場合や途中で止めた場合，同一ドメイン内の全インタフェースでグレースフル・リスタートを止めます。
- OSPFv3 のリスタート時間を，系切替所要時間＋ LSA 学習時間を超えるように設定してください。これは，OSPFv3 が LSA を学習するためには，系切替が完了して IP インタフェースの Up/Down が確認できるようになっている必要があるためです。グレースフル・リスタート開始後，リスタート時間が経過した時点で LSA の学習が終わってない場合，OSPFv3 のグレースフル・リスタートに失敗します。
- 系切替によって運用系 BCU が交替したときのルーティングエントリ保持時間を，OSPFv3 のリスタート時間よりも長く設定してください。OSPFv3 のリスタート時間よりもルーティングエントリ保持時間のほうが短い場合，経路学習前に系切替前のルーティングエントリが削除されることがあります。
- BGP4+の内部ピアがグレースフル・リスタートを使用している場合，内部ピアのリスタート時間を OSPFv3 のリスタート時間よりも長く設定してください。内部ピアのリスタート時間のほうが短い場

合，OSPFv3 が経路学習を完了する前に内部ピアを接続できなくなって，内部ピアのグレースフル・リスタートに失敗することがあります。

20.6　グレースフル・リスタートのコンフィグレーション

20.6.1　コンフィグレーションコマンド一覧

本装置の OSPFv3 隣接ルータで OSPFv3 リスタート機能を使用する場合，本装置に OSPFv3 ヘルパー機能を設定してください。

リスタート機能を使用する場合，OSPFv3 のリスタート時間（graceful-restart restart-time コマンドの設定値）を，系切替所要時間＋ LSA 学習時間を超えるように設定してください。

グレースフル・リスタートのコンフィグレーションコマンド一覧を次の表に示します。

表 20–6　コンフィグレーションコマンド一覧

コマンド名	説明
graceful-restart mode	ヘルパー機能またはリスタート機能を動作させます。
graceful-restart restart-time	リスタート時間（ヘルパーとの再接続の許容時間）を設定します。
graceful-restart strict-lsa-checking	ヘルパールータで，リスタートルータとの間で LSA データベースが同期していない状況になった場合，グレースフル・リスタートを止めます。
max-metric router-lsa	リスタートルータとしての経路学習に失敗した後，スタブルータとして動作します。
routing options graceful-restart time-limit※	経路を保留する時間の上限値を指定します。

注※
「コンフィグレーションコマンドレファレンス Vol.3　13. ルーティングオプション」を参照してください。

20.6.2　リスタート機能の設定

[設定のポイント]
リスタート機能を使用することを指定します。

[コマンドによる設定]

1. **(config)# ipv6 router ospf 1**
   (config-rtr)# graceful-restart mode both
   モードとして，リスタート機能とヘルパー機能の両方を設定します。

20.6.3　ヘルパー機能の設定

[設定のポイント]
ヘルパー機能を使用することを指定します。設定しない場合，ヘルパーとして動作しません。

[コマンドによる設定]

1. **(config)# ipv6 router ospf 1**
   (config-rtr)# graceful-restart mode helper

ヘルパー機能を使用します。

20.7　スタブルータの解説

20.7.1　概要

隣接ルータとの接続が完了していなかったり，安定していなかったりすると，ネットワーク全体のルーティングが不安定になることがあります。ルータの起動および再起動時やネットワークにルータを追加するときに，このような状況が起こることがあります。OSPFv3 ではこのような状況下，周辺の装置でルーティングにできるだけ使用されないように，経路情報を通知できます。OSPFv3 では，このような通知をしているルータをスタブルータと呼びます。この機能によって，装置の状態が不安定であっても，ネットワークのルーティングが不安定になることを防げます。

(1)　スタブルータ動作時の OSPFv3 インタフェースのコスト値

スタブルータは，接続する OSPFv3 インタフェースのコスト値を最大値（65535）にして広告します。このため，スタブルータを経由する OSPFv3 経路は優先されなくなります。ただし，隣接ルータの存在しないインタフェース（スタブネットワーク）の経路については，コンフィグレーションコマンドで指定したコスト値を広告します。スタブネットワークや AS 外経路は，スタブルータが広告している経路が優先されることがあります。

周辺装置ではメトリックを比較して，スタブルータを経由しない代替経路を優先します。また，スタブルータ自身のループバックインタフェースに設定したアドレスを使用して，telnet による管理や BGP4+による経路交換ができます。

20.7.2　スタブルータの動作

コンフィグレーションコマンド max-metric router-lsa では，ドメインごとにスタブルータ機能を動作させるかどうかを指定します。さらに，動作条件として，スタブルータとして常時動作させるか，または起動後に動作させるかを選択できます。

(1)　常時動作する場合

常時，コストを最大値にします。スタブルータのコンフィグレーションを削除するまで，動作し続けます。

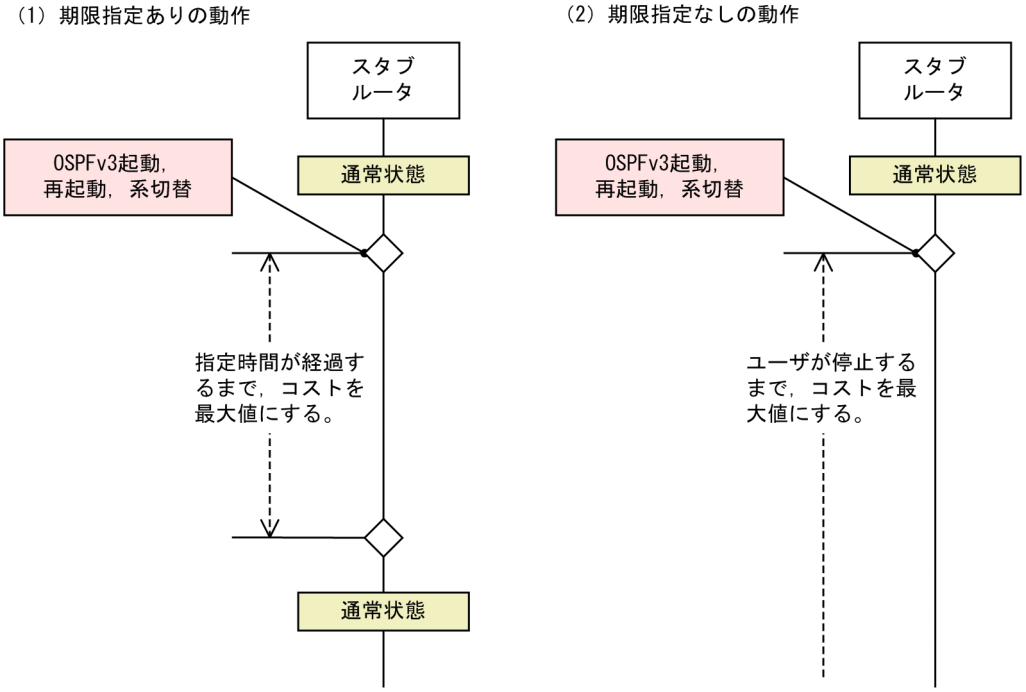
(2)　起動後にスタブルータとして動作する場合

次に示す契機でコストを最大値にします。コンフィグレーションで指定した期限が経過するまで，継続します。

- 装置起動
- 系切替による運用系 BCU の交替後
  ただし，次の場合を除きます。
  - ノンストップルーティング使用時の系切替で，隣接状態を正しく引き継いで隣接装置と再接続しない場合
  - グレースフル・リスタート使用時の系切替で，グレースフル・リスタートに成功した場合
- ユニキャストルーティングプログラムの再起動後
  ただし，次の場合を除きます。
  - グレースフル・リスタート使用時の系切替で，グレースフル・リスタートに成功した場合

動作中に運用コマンド clear ipv6 ospf stub-router を実行するか，コンフィグレーションを削除することで停止できます。スタブルータの動作を次の図に示します。

図 20-6　スタブルータの動作



(3)　注意事項

- グレースフル・リスタートのヘルパールータとして動作しているとき，スタブルータのコンフィグレーションを変更しないでください。設定を変更すると，スタブルータが動作を開始したり終了したりして，ヘルパー動作に失敗することがあります。
- スタブルータとして常時動作する設定になっているとき，起動後に動作するように変更すると，すぐにスタブルータを終了します。
- スタブルータを通過する仮想リンクは，使用できません。

  通過エリアでのコストが 65535 よりも大きい場合，仮想ネイバーはその仮想リンクを到達不能とみなします。

20.8　スタブルータのコンフィグレーション

20.8.1　コンフィグレーションコマンド一覧

本装置を経由する経路を優先させたくない場合, スタブルータを設定してください。スタブルータを経由する経路のメトリックを大きく設定できます。

スタブルータのコンフィグレーションコマンド一覧を次の表に示します。

表 20-7　コンフィグレーションコマンド一覧

コマンド名	説明
max-metric router-lsa	スタブルータとして動作します。

20.8.2　スタブルータ機能の設定

[設定のポイント]

スタブルータとして動作することを指定します。on-startup パラメータを指定しない場合, スタブルータとして常時動作します。

[コマンドによる設定]

1. **(config)# ipv6 router ospf 1**
   (config-rtr)# max-metric router-lsa
   スタブルータ機能を使用します。

20.9　OSPFv3 拡張機能のオペレーション

20.9.1　運用コマンド一覧

OSPFv3 拡張機能の運用コマンド一覧を次の表に示します。

表 20-8　運用コマンド一覧

コマンド名	説明
show ipv6 ospf	ドメインの情報（エリアボーダの状態，グレースフル・リスタートの状態など）や，エリアを表示します。
clear ipv6 ospf	OSPFv3 プロトコルに関する情報をクリアします。stub-router パラメータでスタブルータの動作を停止します。
show nsr unicast※	ユニキャストルーティングプロトコルのノンストップルーティングの同期状態を表示します。
show graceful-restart unicast※	ユニキャストルーティングプロトコルのグレースフル・リスタートのリスタートルータの動作状態を表示します。

注※
「運用コマンドレファレンス Vol.3　12. IPv4・IPv6 ルーティングプロトコル共通」を参照してください。

20.9.2　エリアボーダの確認

show ipv6 ospf コマンドを実行して，エリアボーダルータではルータの種別（Flags）に「AreaBorder」が含まれていることを確認してください。また，エリア間の経路集約が正しく反映されていることを確認してください。

図 20-7　show ipv6 ospf コマンドの実行結果

```
>show ipv6 ospf
Date 20XX/03/14 12:00:00 UTC
Domain: 1
Router ID: 172.16.1.1
Distance:
  Intra Area: 10, Inter Area: 10, External: 150
Flags: <AreaBorder ASBoundary>
SPF Interval: 7s, SPF Delay: 3s
Graceful Restart: Helper
    Last Helper Status : Finished  20XX/03/08 14:12:22
Area: 0, Interfaces: 2
    Network Range                                 State
    2001:db8:ffff:100::/64                        DoNotAdvertise
    2001:db8:ffff:200::/64                        Advertise
Area: 1, Interfaces: 1
    Network Range                                 State
    -                                             -
```

20.9.3　エリアの確認

コンフィグレーションで設定したエリアが正しく反映されていることを確認してください。show ipv6 ospf コマンドで area パラメータを指定すると，エリアの一覧を表示します。

図 20-8　show ipv6 ospf コマンド（area パラメータ指定）の実行結果

```
>show ipv6 ospf area
Date 20XX/03/14 12:00:00 UTC
Domain: 1
```

```
ID              Neighbor  SPFcount  Flags
0               3         14        <ASBoundary>
10              2         8         <Stub>
>
```

20.9.4　ノンストップルーティングの確認

(1)　動作状態の確認

show ipv6 ospf コマンドを実行して，ノンストップルーティングの動作状態を確認してください。

図 20-9　show ipv6 ospf コマンドの実行結果

```
>show ipv6 ospf
Date 20xx/03/14 12:00:00 UTC
Domain: 1
Router ID: 172.16.1.1
Distance:
  Intra Area: 10, Inter Area: 10, External: 150
Flags: <AreaBorder ASBoundary>
SPF Interval: 7s, SPF Delay: 3s
Nonstop Routing: Enable, Sync Status: Synchronized
Area: 0, Interfaces: 2
    Network Range                                 State
    2001:db8:ffff:100::/64                        DoNotAdvertise
Area: 1, Interfaces: 1
    Network Range                                 State
    -                                             -
>
```

(2)　同期状態の詳細の確認

他系 BCU との同期状態を確認してください。show ipv6 ospf コマンドで nsr パラメータを指定すると，ノンストップルーティングの同期状態の詳細を表示します。

図 20-10　show ipv6 ospf コマンド（nsr パラメータ指定）の実行結果

```
>show ipv6 ospf nsr
Date 20XX/03/14 12:00:00 UTC
Total of Domain: 1
Status: Synchronized
Sync Time: 20XX/03/10 12:00:00
Nonstop-Routing Control Information
  Waited Request : 0
  Total  Request : 28
>
```

(3)　ノンストップルーティング対象プロトコルの同期状態の確認

show nsr unicast コマンドを実行して，ノンストップルーティングが動作しているプロトコルの状態を確認してください。

図 20-11　show nsr unicast コマンドの実行結果

```
>show nsr unicast
Date 20XX/04/14 12:00:00 UTC
Status:  Synchronized
Protocol      Total    Asynchronous    Synchronizing   Synchronized
BGP4          5        0               0               5
OSPF          10       0               0               10
BGP4+         5        0               0               5
OSPFv3        10       0               0               10
>
```

20.9.5　グレースフル・リスタートの確認

(1)　動作モードや進行状態の確認

show ipv6 ospf コマンドを実行して，グレースフル・リスタートの状態を確認してください。

図 20-12　show ipv6 ospf コマンドの実行結果

```
>show ipv6 ospf
Date 20XX/03/14 12:00:00 UTC
Domain: 1
Router ID: 172.16.1.1
Distance:
  Intra Area: 10, Inter Area: 10, External: 150
Flags: <AreaBorder ASBoundary>
SPF Interval: 7s, SPF Delay: 3s
Graceful Restart: Helper
    Last Helper Status : Finished  20XX/03/08 14:12:22
Area: 0, Interfaces: 2
    Network Range                                 State
    2001:db8:ffff:100::/64                        DoNotAdvertise
Area: 1, Interfaces: 1
    Network Range                                 State
    -                                             -
```

(2)　リスタートルータの動作確認

show graceful-restart unicast コマンドを実行して，リスタートルータとして動作しているプロトコルの状態を確認してください。

図 20-13　show graceful-restart unicast コマンドの実行結果

```
>show graceful-restart unicast
Date 20XX/04/14 12:00:00 UTC
Status: Completed
Graceful Restart Time Limit: 180s
Start Time: 20XX/04/08 17:01:23
End Time  : 20XX/04/08 17:01:23
OSPF  : Restart State <Finished>
        Total of Domain: 2 (Succeeded: 2)
BGP   : Restart State <Finished>
        Total of Peer  : 25 (Succeeded: 25)
OSPFv3: Restart State <Finished>
        Total of Domain: 2 (Succeeded: 2)
BGP4+ : Restart State <Finished>
        Total of Peer  : 20 (Succeeded: 20)
```

21 BGP4/BGP4+

この章では，IPv4 のルーティングプロトコル BGP4 および IPv6 のルーティングプロトコル BGP4+について説明します。

21.1　解説

21.1.1　概要

IPv4 のルーティングプロトコルである BGP4 は，プロバイダ間の多大な経路情報のやり取りが必要なインターネット接続に適用されるルーティングプロトコルで，階層型のネットワークの概念に基づいて作成されています。BGP4 はインターネットのバックボーン上で，プロバイダ間でルーティングテーブルを交換するときに使用されます。また，イントラネットを二つ以上の ISP に接続する場合に使用されます。

AS 内のルータ間での経路情報の交換には，RIP や OSPF のような IGP（Interior Gateway Protocol）を使用します。BGP4 は，AS 間のルーティングプロトコルであり，EGP（Exterior Gateway Protocol）の一つです。BGP4 はインターネット上で使用されているすべての経路情報を扱えます。

IPv6 のルーティングプロトコルとして使用する BGP4+は，BGP4 を IPv4 以外のプロトコルにも使用できるように拡張したものです。BGP4 と同様に，インターネット上で使用されているすべての経路情報を扱えます。

BGP4 と BGP4+の機能を次の表に示します。

表 21-1　BGP4 と BGP4+の機能

機能	BGP4	BGP4+
EBGP，IBGP ピアリング，経路配信	○	○
経路フィルタ，BGP 属性変更	○	○
コミュニティ	○	○
ルート・リフレクション	○	○
コンフェデレーション	○	○
サポート機能のネゴシエーション	○	○
ルート・リフレッシュ	○	○
マルチパス	○	○
ピアグループ※1	○	○
ルート・フラップ・ダンプニング※2	○	○
BGP4 MIB※2	○	×
TCP MD5 認証	○	○
ユニキャストルーティング高可用機能	○	○
学習経路数制限	○	○
4 バイト AS 番号	○	○

（凡例）　○：取り扱う　×：取り扱わない

注※1　外部ピアおよびメンバー AS 間ピア同士，または内部ピア同士のグルーピングです。

注※2　VRF では取り扱いません。

21.1.2　ピアの種別と接続形態

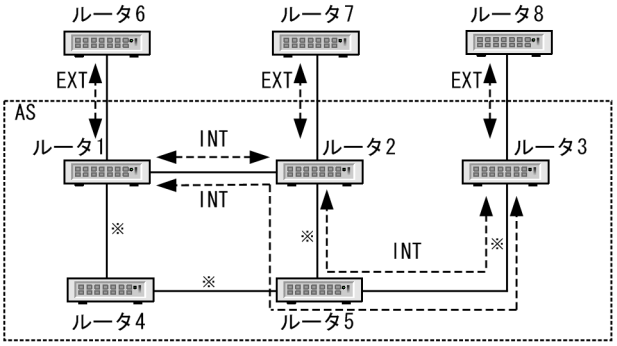
BGP4 および BGP4+のどちらも，ピアの種別と接続形態は同じです。以降，BGP4 と BGP4+をまとめて BGP と表します。

BGP は AS 間のルーティングプロトコルなので，扱う経路情報は宛先ネットワークへの AS パス情報（パケットが宛先のネットワークに到達するまでに通過する AS の列）で構成されます。BGP が動作するルータを BGP スピーカと呼びます。この BGP スピーカは，そのほかの BGP スピーカと経路情報を交換するためにピアを形成します。

本装置で使用されるピアの種類には，外部ピアと内部ピアがあります。コンフェデレーション構成時は，これら二つのピアに加えて，メンバー AS 間ピアが追加されます。ネットワーク構成に合わせてピアを使用してください。なお，メンバー AS 間ピアについては，「22.1.10　コンフェデレーション」を参照してください。

外部ピアと内部ピアを次の図に示します。

図 21-1　内部ピアと外部ピア



（凡例）　ルータ1，ルータ2，ルータ3：内部BGPスピーカ
ルータ6，ルータ7，ルータ8：外部BGPスピーカ
ルータ4，ルータ5　　：内部非BGPスピーカ
INT　：内部ピア
EXT　：外部ピア

注※　IGP が動作します。

(1)　外部ピア

外部ピアは，異なる AS に属する BGP スピーカ間に形成するピアです。ピアリングに使用する IP アドレスには，IPv4 アドレスの場合は直接接続されたインタフェースのアドレスを，IPv6 アドレスの場合は直接接続されたインタフェースのリンクローカルアドレスまたはグローバルアドレスを使用します。

なお，コンフィグレーションコマンド neighbor ebgp-multihop を使用すると，直接接続されたインタフェース以外のアドレス（例えば，ループバックインタフェースに設定したアドレス）で接続できます。

「図 21-1　内部ピアと外部ピア」のルータ 1－ルータ 6 間，ルータ 2－ルータ 7 間，ルータ 3－ルータ 8 間に形成されるピアが外部ピアです。

(2)　内部ピア

内部ピアは，同じ AS に属する BGP スピーカ間に形成するピアです。BGP はピア間のコネクションを確立するために TCP（ポート 179）を使用します。そのため，すべての BGP スピーカが物理的にフルメッシュで接続される必要はありませんが，内部ピアは AS 内の各 BGP スピーカ間で論理的にフルメッシュに形成

される必要があります。これは，内部ピアで受信した経路情報をそのほかの内部ピアに通知しないためです。なお，ルート・リフレクションやコンフェデレーションの機能を使用すると，この条件は緩和されます。

「図 21-1　内部ピアと外部ピア」のルータ 1－ルータ 2 間，ルータ 1－ルータ 3 間，ルータ 2－ルータ 3 間に形成されるピアが内部ピアです。

(3) ループバックインタフェースに設定したアドレスを使用したピアリング

本装置ではループバックインタフェースに設定したアドレスを外部ピアや内部ピアの IP アドレスとして使用すると，特定の物理インタフェースの状態に依存したピアリング（TCP コネクション）への影響を排除できます。

例えば，「図 21-1　内部ピアと外部ピア」でルータ 1－ルータ 2 間の内部ピアにインタフェースの IP アドレスを使用すると，ルータ 1－ルータ 2 間に障害が発生してインタフェースが使用できない場合にルータ 1－ルータ 2 間の内部ピアを確立できません。しかし，内部ピアの IP アドレスとしてループバックインタフェースに設定したアドレスを使用すると，ルータ 1－ルータ 2 間のインタフェースが使用できない場合でもルータ 4，ルータ 5 経由で内部ピアを確立できます。

[ループバックインタフェースに設定したアドレスを使用する場合の注意事項]

ループバックインタフェースに設定した IPv4 アドレスを使用する場合，そのアドレスへの経路情報をスタティックまたは IGP（RIP，OSPF）で互いに学習している必要があります。また，IPv6 アドレスを使用する場合，そのアドレスへの経路情報をスタティックまたは IGP（RIPng，OSPFv3）で互いに学習している必要があります。なお，本装置はループバックインタフェースに設定したアドレスを直結経路情報として扱います。

[内部ピアで非 BGP スピーカを経由する場合の注意事項]

内部ピアで非 BGP スピーカを経由して経路情報を通知する（例えば，ルータ 2 からルータ 3 に通知する）場合，非 BGP スピーカで IGP 経由でその経路情報を学習している必要があります。これは該当する経路情報の通知によって通知先 BGP スピーカから入ってくる該当宛先への IP パケットが，該当する経路を学習していない非 BGP スピーカのルータで廃棄されるのを防ぐためです。例えば，「図 21-1　内部ピアと外部ピア」ではルータ 3 からルータ 5 に入ってくる IP パケットがルータ 5 で廃棄されるのを防ぐためです。

21.1.3 経路選択

本装置は，各プロトコルで学習した同じ宛先への経路情報から，それぞれ独立した経路選択手順に従って一つの最適の経路を選択します。同じ宛先への経路情報が各プロトコルでの生成によって複数存在する場合，それぞれの経路情報のディスタンス値が比較されて優先度の最も高い経路情報が有効になります。

BGP4 では，自プロトコルを使用して学習した同じ宛先への複数の経路情報から経路選択の優先順位に従って一つの最適の経路を選択します。そのあと，同じ宛先への経路情報が各プロトコル（RIP，OSPF，スタティック）での経路選択によって複数存在する場合は，それぞれの経路情報のディスタンス値が比較されて，優先度の最も高い経路情報をルーティングテーブルに設定します。

経路選択の条件を，優先順位が高い順に次に示します。

1. weight 値が最も大きい経路を選択します。
2. LOCAL_PREF 属性の値が最も大きい経路を選択します。
3. AS_PATH 属性の AS 数が最も短い経路を選択します。
   AS_PATH 属性上のパスタイプ AS_SET は，全体で一つの AS としてカウントします。

4. ORIGIN 属性の値で IGP，EGP，Incomplete の順で選択します。
5. MED 属性の値が最も小さい経路を選択します。
   MED 属性値による経路選択は，同一隣接 AS から学習した重複経路に対してだけ有効です。なお，コンフィグレーションコマンド bgp always-compare-med を設定すると，異なる隣接 AS から学習した重複経路に対しても有効となります。
6. 外部ピアで学習した経路，内部ピアで学習した経路の順で選択します。
7. ネクストホップが最も近い（ネクストホップ解決時に使用した IGP 経路のメトリック値が最も小さい）経路を選択します。
8. 相手 BGP 識別子（ルータ ID）が最も小さい経路を選択します。ただし，ORIGINATOR_ID 属性を持つ経路は，相手 BGP 識別子（ルータ ID）の代わりに ORIGINATOR_ID 属性の値を比較します。
   外部ピアから受信した経路間で相手 BGP 識別子（ルータ ID）の値が異なる場合は，相手 BGP 識別子（ルータ ID）および学習元ピアアドレスによる経路選択をしないで，すでに選択されている経路を採用します。なお，コンフィグレーションコマンド bgp bestpath compare-routerid を設定すると，外部ピアから受信した経路間で相手 BGP 識別子（ルータ ID）の値が異なる場合にも相手 BGP 識別子（ルータ ID）による経路選択ができます。
9. CLUSTER_LIST 属性長が最も短い経路を選択します。
   CLUSTER_LIST 属性を持たない経路は，CLUSTER_LIST 属性長を 0 として比較します。
10. 学習元ピアのアドレスが小さい経路を選択します。
    外部ピアから受信した経路間で相手 BGP 識別子（ルータ ID）の値が異なる場合は，相手 BGP 識別子（ルータ ID）および学習元ピアアドレスによる経路選択をしないで，すでに選択されている経路を採用します。なお，コンフィグレーションコマンド bgp bestpath compare-routerid を設定すると，外部ピアから受信した経路間で相手 BGP 識別子（ルータ ID）の値が異なる場合にも相手 BGP 識別子（ルータ ID）による経路選択ができます。

BGP4+でも，RIPng，OSPFv3，スタティックなどの IPv6 ルーティングによる同じ宛先への経路情報が複数存在する場合，同様に扱います。

なお，コンフェデレーション構成での経路選択は，「22.1.10　コンフェデレーション」を参照してください。

weight 値と，経路選択に関連する経路情報に含まれる BGP 属性の概念を次に説明します。BGP 属性のうち，LOCAL_PREF 属性，AS_PATH 属性，ORIGIN 属性，および MED 属性は BGP4 と BGP4+で同じです。NEXT_HOP 属性は BGP4 で，MP_REACH_NLRI 属性は BGP4+で使用します。

(1)　weight 値

weight 値は学習元のピア単位に指定する経路の重み付けで，コンフィグレーションコマンド neighbor weight を使用して設定します。より大きい値の weight 値を持つ経路が優先されます。

本装置で使用できる weight 値は 0～255 の範囲です。デフォルト値は 0 です。

(a)　weight の変更

本装置ではコンフィグレーションコマンド neighbor weight を使用して，ピアから学習した経路の weight 値を変更できます。

(2)　LOCAL_PREF 属性

LOCAL_PREF 属性は，同じ AS 内のルータ間で通知される属性です。同じ宛先ネットワークに対して複数の経路がある場合，LOCAL_PREF 属性は該当する宛先ネットワークに対する優先経路を示します。より大きい LOCAL_PREF 属性値を持つ経路が優先されます。

本装置で使用できる LOCAL_PREF 属性値は 0～65535 の範囲です。デフォルト値は 100 です。

(a)　LOCAL_PREF 属性のデフォルト値の変更

本装置ではコンフィグレーションコマンド bgp default local-preference を使用して，外部ピアから自装置内に取り込む経路情報の LOCAL_PREF 属性値を変更できます。

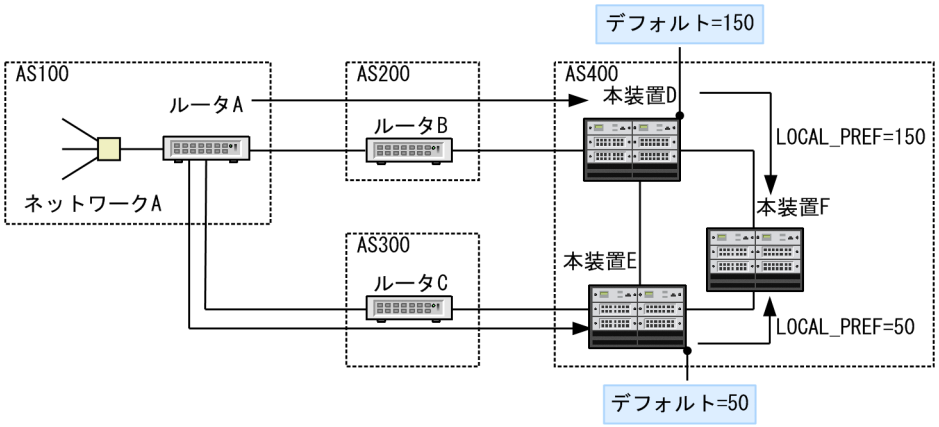
(b)　LOCAL_PREF 属性のフィルタ単位での変更

本装置では学習経路フィルタや広告経路フィルタとコンフィグレーションコマンド set local-preference を組み合わせると，自装置内に取り込む経路情報や通知する経路情報の LOCAL_PREF 属性を変更できます。

(c)　LOCAL_PREF 属性による経路選択の例

LOCAL_PREF 属性による経路選択を次の図に示します。

図 21-2　LOCAL_PREF 属性による経路選択



この図で，AS400 は AS200 と AS300 からネットワーク A に対する経路情報を受信します。本装置 D の LOCAL_PREF 値を 150 に，本装置 E の LOCAL_PREF 値を 50 に設定した場合，本装置 D は AS200 からの経路情報を本装置 F に通知するとき LOCAL_PREF 値を 150 に，本装置 E は AS300 からの経路情報を本装置 F に通知するとき LOCAL_PREF 値を 50 に設定します。この結果，本装置 D からの経路情報が本装置 E からの経路情報より大きい LOCAL_PREF 属性値を持つため，本装置 F ではネットワーク A への経路情報として，本装置 D からの経路情報（AS200 経由の経路情報）を選択します。

(3)　ORIGIN 属性

ORIGIN 属性は，経路情報の生成元を示します。ORIGIN 属性を次の表に示します。

表 21-2　ORIGIN 属性

ORIGIN 属性	内容
IGP	該当する経路が AS 内部で生成されたことを示します。

ORIGIN 属性	内容
EGP	該当する経路が EGP 経由で学習されたことを示します。
Incomplete	該当する経路が上記以外の方法で学習されたことを示します。

経路選択では，同一宛先への複数の経路が存在する場合，IGP，EGP，Incomplete の順で選択します。

(a)　ORIGIN 属性の変更

本装置では経路フィルタとコンフィグレーションコマンド set origin を組み合わせると，自装置内に取り込む経路情報や通知する経路情報の ORIGIN 属性を変更できます。

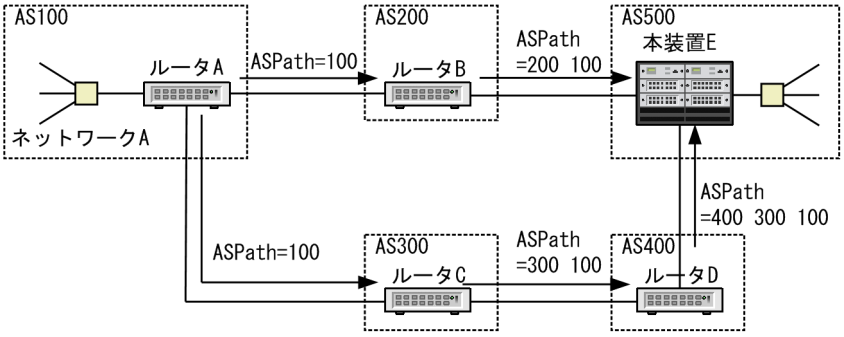
(4)　AS_PATH 属性

AS_PATH 属性は，経路情報の宛先ネットワークに到達するまでに通過する AS 番号のリストです。経路情報がほかの AS に通知されるとき，その経路情報の AS_PATH 属性に自 AS 番号を追加します。また，学習フィルタ情報，広告フィルタ情報とコンフィグレーションコマンド set as-path prepend count を組み合わせると，複数の自 AS 番号を AS_PATH 属性に追加できます。これは，ある宛先ネットワークへの経路が複数ある場合に特定の経路を選択するのに有効です。

(a)　AS_PATH 属性による経路選択の例

AS_PATH 属性による経路選択を次の図に示します。

図 21-3　AS_PATH 属性による経路選択

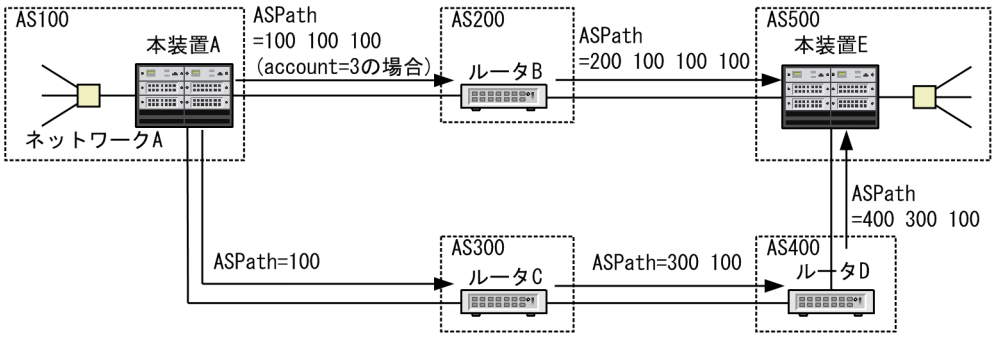


ルータ A が自 AS に存在するネットワーク A を AS200 経由で通知するとき，AS500 に到達する経路情報の AS_PATH 属性は「200 100」を持ちます。ルータ A が自 AS 内のネットワーク A を AS300，AS400 経由で通知するとき，AS500 に到達する経路情報の AS_PATH 属性は「400 300 100」を持ちます。したがって，AS500 の本装置 E は最も短い AS_PATH 属性を持つ AS200 経由で到達した経路を選択します。

(b)　set as-path prepend count コマンド使用時の経路選択

コンフィグレーションコマンド set as-path prepend count の使用例を次の図に示します。

図 21-4　set as-path prepend count コマンドの使用例



この図で，本装置 A が本装置 E に対して AS300 AS400 経由の経路を選択させたい場合，AS200 に通知する経路情報の AS_PATH 属性に複数の自 AS 番号を追加します。例えば，自 AS 番号を三つ追加した場合，AS200 経由で AS500 に到達する経路情報の AS_PATH 属性は「200 100 100 100」を持つため，本装置 E は最も短い AS_PATH 属性を持つ AS300 AS400 経由で到達した経路を選択します。

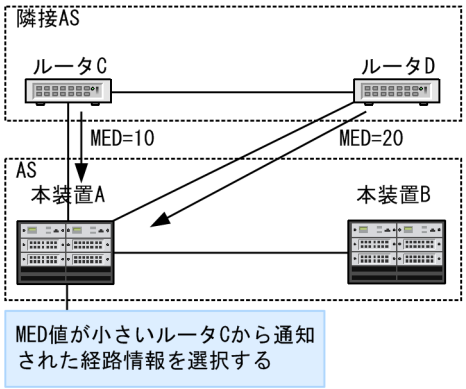
(5)　MED 属性

MED 属性は，同一の隣接 AS から学習した，ある宛先への複数の BGP 経路の優先度を決定する属性です。より小さい MED 属性値を持つ経路情報が優先されます。コンフィグレーションコマンド bgp always-compare-med を設定して，異なる隣接 AS から学習した BGP 経路間の優先度選択に使用できます。

(a)　MED 属性による経路選択の例

MED 属性による経路選択を次の図に示します。

図 21-5　MED 属性による経路選択



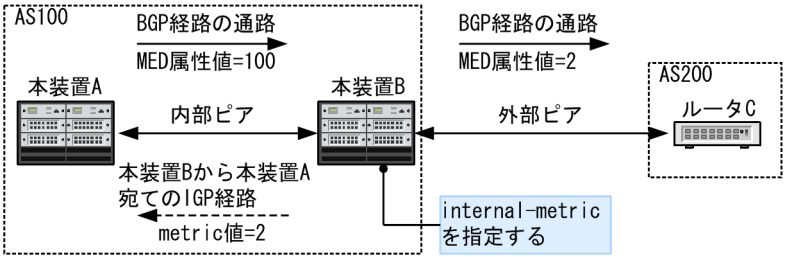
ある宛先ネットワークに対する経路情報を，ルータ C は MED 属性値 10 で，ルータ D は MED 属性値 20 で本装置 A に通知しているものとします。この場合，本装置 A はルータ C から通知された経路情報を該当する宛先ネットワークへの経路として選択します。

(b)　MED 属性値の変更

本装置では学習フィルタ情報や広告フィルタ情報とコンフィグレーションコマンド set metric を組み合わせると，自装置内に取り込む経路情報や通知する経路情報の MED 属性値を変更できます。

また，コンフィグレーションコマンド set metric-type で internal パラメータを指定した場合，ネクストホップ解決に使用している IGP 経路のメトリック値を，通知する BGP 経路の MED 属性値にできます。set metric-type internal の使用例を次の図に示します。

図 21-6　set metric-type internal の使用例



この図で，本装置 A と本装置 B の間は内部ピアを形成しています。MED 属性値＝ 100 で本装置 A から通知された BGP の経路情報を本装置 B がルータ C に通知するとき，本装置 B から本装置 A までの IGP 経路のメトリック値＝ 2 を MED 属性値として使用する場合，本装置 B で set metric-type internal を設定します。

(6)　NEXT_HOP 属性

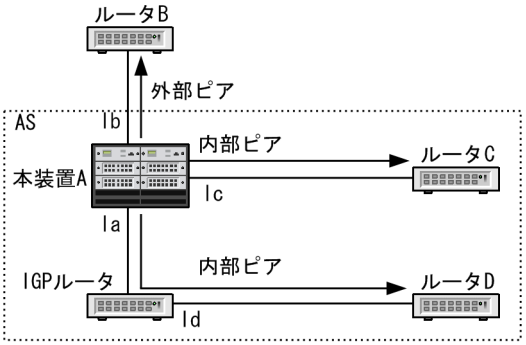
BGP4 では，NEXT_HOP 属性の値を経路のネクストホップとして採用します。

NEXT_HOP 属性は，ある宛先ネットワークに到達するために使用されるネクストホップの IP アドレスです。本装置では外部ピアに経路情報を通知する場合，NEXT_HOP 属性にピアリングに使用した自側の IP アドレスを設定します。内部ピアおよびメンバー AS 間ピアに経路情報を通知する場合は NEXT_HOP 属性を書き替えません。

(a)　NEXT_HOP 属性の設定例

BGP4 ピアから学習した経路を広告する場合に通知する経路情報の NEXT_HOP 属性の設定例を次の図に示します。

図 21-7　BGP4 ピアから学習した経路を広告する場合に通知する経路情報の NEXT_HOP 属性の設定例



- 外部ピアを形成するルータ B への経路情報

  NEXT_HOP 属性は，本装置 A とルータ B 間のインタフェースで本装置 A 側のインタフェースアドレス Ib になります。

- 内部ピアを形成するルータ C への経路情報

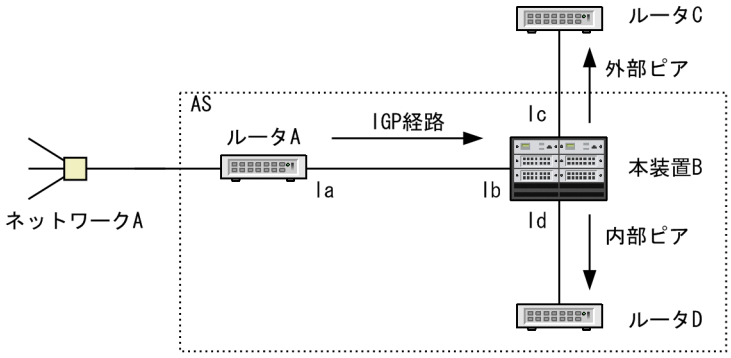
  NEXT_HOP 属性は，ルータ B から受信した経路情報に設定されている NEXT_HOP 属性になります。

- 内部ピアを形成するルータ D への経路情報

  NEXT_HOP 属性は，ルータ B から受信した経路情報に設定されている NEXT_HOP 属性になります。

IGP 経路を BGP4 で広告する場合に通知する経路情報の NEXT_HOP 属性の設定例を次の図に示します。

図 21-8 IGP 経路を BGP4 で広告する場合に通知する経路情報の NEXT_HOP 属性の設定例



- 外部ピアを形成するルータ C への経路情報
  NEXT_HOP 属性は，本装置 B とルータ C 間のインタフェースで本装置 B 側のインタフェースアドレス Ic になります。
- 内部ピアを形成するルータ D への経路情報
  NEXT_HOP 属性は，IGP 経路が解決するネットワーク A へのネクストホップアドレスである，ルータ A のインタフェースアドレス Ia になります。

(b) NEXT_HOP 属性を書き替える場合

本装置では次に示すコンフィグレーションコマンドを使用して，NEXT_HOP 属性を書き換えられます。

- neighbor next-hop-self コマンド
  BGP4 ピアから受信した経路情報を BGP4 ピアへ広告する際の NEXT_HOP 属性を，ピアリングに使用している自側アドレスに書き替えます。ただし，ルート・リフレクションや IGP 経路を BGP4 で内部ピアへ広告する場合は除きます。
- neighbor always-nexthop-self コマンド
  ルート・リフレクションや IGP 経路を BGP4 で広告する場合を含めて，内部ピアへ広告する際の NEXT_HOP 属性を，ピアリングに使用している自側アドレスに書き替えます。
- neighbor set-nexthop-peer コマンド
  学習した経路情報の NEXT_HOP 属性を，ピアリングに使用している相手側アドレスに書き替えます。

(c) NEXT_HOP 属性の解決

内部ピアから BGP4 経路情報を学習した場合，NEXT_HOP 属性で示されたアドレスへ到達するためのパスを，IGP 経路，スタティック経路，および直結経路によって解決します。ネクストホップへ到達できる BGP4 経路の中から宛先のマスク長が最も長い経路を選択して，その経路のパスを BGP4 経路のパスとして使用します。また，コンフィグレーションコマンド bgp nexthop を使用して，NEXT_HOP 属性の解決に使用する経路のプロトコル種別およびプレフィックスを指定できます。

なお，ネクストホップを解決した経路がスタティック経路で，noinstall または reject パラメータの指定がある場合，該当する BGP4 経路を抑止します。

(7) MP_REACH_NLRI 属性のネクストホップ情報

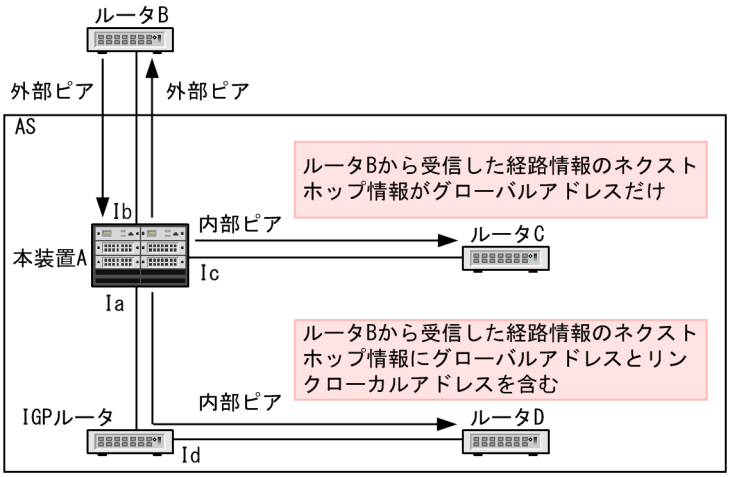
BGP4+では BGP4+ピアから受信した NEXT_HOP 属性の値を無視します。その代わりに MP_REACH_NLRI 属性のネクストホップ情報を経路のネクストホップとして採用します。

BGP4+では相手 BGP4+スピーカに経路情報を通知する場合，IPv6 グローバルアドレスでピアリングしたときだけ，MP_REACH_NLRI 属性のネクストホップ情報としてピアリングに使用した自側インタフェースのグローバルアドレスとリンクローカルアドレス（外部ピアの場合だけ）を設定します。

(a)　ネクストホップ情報の設定例

BGP4+ピアから学習した経路を広告する場合に通知する経路情報のネクストホップ情報の設定例を次の図に示します。

図 21-9　BGP4+ピアから学習した経路を広告する場合に通知する経路情報のネクストホップ情報の設定例



- **外部ピアを形成するルータ B への経路情報**

  MP_REACH_NLRI 属性のネクストホップ情報には，本装置 A とルータ B 間のインタフェースの，本装置 A 側のグローバルアドレスおよびリンクローカルアドレス Ib が設定されます。ルータ B が実際のネクストホップとしてどちらを採用するかは，本装置 A は関知しません。

- **直接接続された外部ピアを形成するルータ B からの経路情報**

  MP_REACH_NLRI 属性のネクストホップ情報にグローバルアドレスとリンクローカルアドレスとのどちらか一方だけが設定されていた場合は，そのアドレスをネクストホップとして使用します。両方のアドレスが設定されていた場合は，リンクローカルアドレスをネクストホップとして使用します。

- **内部ピアを形成するルータ C への経路情報**

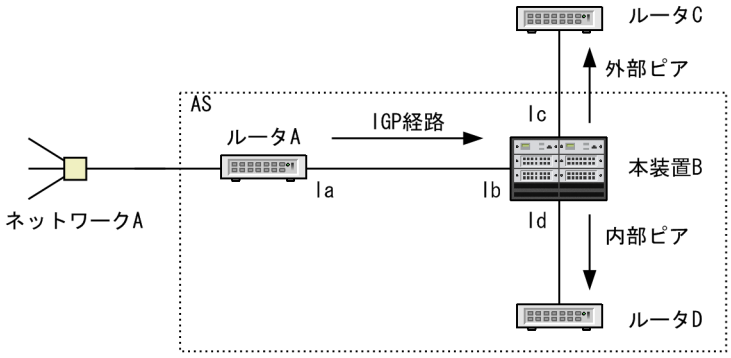
  ルータ B から受信した経路情報の MP_REACH_NLRI 属性のネクストホップ情報にグローバルアドレスだけが設定されている場合，MP_REACH_NLRI 属性のネクストホップ情報には，ルータ B から受信したグローバルアドレスを設定します。

- **内部ピアを形成するルータ D への経路情報**

  ルータ B から受信した経路情報の MP_REACH_NLRI 属性のネクストホップ情報にグローバルアドレスとリンクローカルアドレスが設定されている場合，MP_REACH_NLRI 属性のネクストホップ情報には，本装置 A とルータ D 間との BGP セッションで使用する本装置のアドレスが設定されます。

IGP 経路を BGP4+で広告する場合に通知する経路情報のネクストホップ情報の設定例を次の図に示します。

図 21-10 IGP 経路を BGP4+で広告する場合に通知する経路情報のネクストホップ情報の設定例



- 外部ピアを形成するルータ C への経路情報

  MP_REACH_NLRI 属性のネクストホップ情報には，本装置 B とルータ C 間のインタフェースの，本装置 B 側のグローバルアドレスおよびリンクローカルアドレス Ic が設定されます。ルータ C が実際のネクストホップとしてどちらを採用するかは，本装置 B は関知しません。

- 内部ピアを形成するルータ D への経路情報

  MP_REACH_NLRI 属性のネクストホップ情報には，IGP 経路が解決するネットワーク A へのネクストホップアドレスである，ルータ A のインタフェースアドレス Ia が設定されます。ただし，Ia がリンクローカルアドレスの場合，MP_REACH_NLRI 属性のネクストホップ情報には，本装置 B とルータ D 間のインタフェースの本装置 B 側のグローバルアドレス Id が設定されます。

(b) ネクストホップ情報を書き替える場合

本装置では次に示すコンフィグレーションコマンドを使用して，MP_REACH_NLRI 属性のネクストホップ情報を書き換えられます。

- neighbor next-hop-self コマンド

  BGP4+ピアから受信した経路情報の MP_REACH_NLRI 属性のネクストホップ情報にグローバルアドレスだけが設定されている場合，BGP4+ピアへ広告する際の MP_REACH_NLRI 属性のネクストホップ情報を，ピアリングに使用している自側アドレスに書き替えます。ただし，ルート・リフレクションや IGP 経路を BGP4+で内部ピアへ広告する場合は除きます。

- neighbor always-nexthop-self コマンド

  ルート・リフレクションや IGP 経路を BGP4+で広告する場合を含めて，内部ピアへ広告する際の MP_REACH_NLRI 属性のネクストホップ情報を，ピアリングに使用している自側アドレスに書き替えます。

- neighbor set-nexthop-peer コマンド

  学習した経路情報の MP_REACH_NLRI 属性のネクストホップ情報を，ピアリングに使用している相手側アドレスに書き替えます。

(c) ネクストホップの解決

内部ピアから BGP4+経路情報を学習した場合，MP_REACH_NLRI 属性のネクストホップ情報で示されたアドレスへ到達するためのパスを，IGP 経路，スタティック経路，および直結経路によって解決します。ネクストホップへ到達できる BGP4+経路の中から宛先のマスク長が最も長い経路を選択して，その経路のパスを BGP4+経路のパスとして使用します。また，コンフィグレーションコマンド bgp nexthop を使用して，ネクストホップの解決に使用する経路のプロトコル種別およびプレフィックスを指定できます。

なお，ネクストホップを解決した経路がスタティック経路で，noinstall または reject パラメータの指定がある場合，該当する BGP4+経路を抑止します。

21.1.4　VRF での BGP4 または BGP4+

(1)　概要

BGP4 および BGP4+は VRF 機能によって論理的に分割されたネットワーク単位で独立して動作します。

(2)　VRF で BGP4 または BGP4+を使用する場合の注意事項

本装置で，異なる VRF またはグローバルネットワークからインポートした経路は，インポート元経路の AS_PATH 属性をそのまま引き継ぎます。このため，本装置から該当経路を広告した場合，隣接装置で経路ループを検出するおそれがあります。

1. 異なる VRF またはグローバルネットワークで同一の AS 番号を使用する場合の注意事項

   経路のインポート元の VRF またはグローバルネットワークと同一の AS 番号を使用しているインポート先の VRF またはグローバルネットワークに該当経路を広告する場合，その経路は隣接装置で AS ループを検出して，有効な経路として取り扱われません。本装置では，VRF またはグローバルネットワークに経路の AS_PATH 属性上の先頭 AS 番号を自装置の AS 番号で上書きするコンフィグレーションコマンド neighbor as-override を設定できます。同一の AS 番号を持つ VRF またはグローバルネットワークとの接続に BGP4 または BGP4+を使用する場合は，本コマンドを設定してください。

   また，本装置が直接接続していない VRF またはグローバルネットワーク内で同一の AS 番号を使用している場合，コンフィグレーションコマンド neighbor as-override を設定しても，隣接装置で AS ループを解決できません。本装置（隣接装置）では，AS ループ経路を有効な経路として取り扱うコンフィグレーションコマンド neighbor permit-asloop を設定できます。VRF またはグローバルネットワーク内で同一の AS 番号を使用する場合は，本コマンドを設定してください。なお，本コマンドを設定した場合は，経路ループが発生するおそれが高くなるためネットワーク設計に十分注意してください。

2. 異なる VRF またはグローバルネットワークで同一のルータ ID，クラスタ ID を使用する場合（ルート・リフレクション）の注意事項

   異なる VRF またはグローバルネットワークで同一のルータ ID（オリジネータ ID）を使用している場合，もしくは異なる VRF またはグローバルネットワーク内のルート・リフレクタで同一のクラスタ ID を使用している場合，その経路はルート・リフレクタでループを検出して有効な経路として取り扱われません。ネットワーク設計に十分注意してください。

3. 異なる VRF 間のピアから学習した経路は Active 経路になりません。

21.1.5　BGP4 または BGP4+使用時の注意事項

BGP4 または BGP4+を使用したネットワークを構成する場合は次の事項に注意してください。

(1)　BGP4 および BGP4+の制限事項

本装置の BGP4 および BGP4+は RFC4271（BGP バージョン 4 仕様），RFC1997（コミュニティ仕様），RFC5492（サポート機能の広告仕様），RFC2918（ルート・リフレッシュ仕様），RFC4456（ルート・リフレクション仕様），RFC5065（コンフェデレーション仕様）に準拠しています。さらに，BGP4+は RFC4760（BGP4 マルチプロトコル拡張仕様），RFC2545（RFC4760 の IPv6 適用方法の仕様）に準拠していますが，ソフトウェアの機能制限から一部 RFC との差分があります。RFC との差分を次の表に示します。なお，本装置は BGP バージョン 4 だけをサポートしています。

表 21-3 RFC との差分

RFC 番号	RFC		本装置
RFC4271	パス属性：NEXT_HOP	経路を広告される外部ピアが，広告している BGP スピーカのインタフェースの一つとサブネットを共有している場合，スピーカはそのようなインタフェースに関連した IP アドレスを，NEXT_HOP 属性に使用することができます。これは“ファーストパーティ”NEXT_HOP 属性として知られています。	“ファーストパーティ”NEXT_HOP 属性はサポートしません。
		外部ピアへメッセージを送信する場合で，かつ，ピアがスピーカから複数 IP ホップはなれている場合（別名“マルチホップ EBGP”）BGP スピーカは，NEXT_HOP 属性を変更しないで伝えるような設定ができます。	外部ピアの場合，広告時に NEXT_HOP 属性を自ルータのアドレスに変更します。
	パス属性：MULTI_EXIT_DISC	BGP スピーカは MULTI_EXIT_DISC 属性を，ローカル・コンフィグレーションに基づいて経路から削除できる機構を実装しなければなりません。もし，BGP スピーカが MULTI_EXIT_DISC を経路から削除するように設定されているならば，この削除は，経路の優先度の決定，および経路選択の実行に先立って実行されなければなりません。	MULTI_EXIT_DISC 属性を経路から削除できる機構は実装していません。
	コネクション衝突の発見	OPEN メッセージを受信したとき，ローカルシステムは OpenConfirm 状態にあるすべてのコネクションを検査する必要があります。また，プロトコル以外の手段によってピアの BGP 識別子を確認できれば，OpenSent 状態のコネクションも検査します。	OPEN メッセージを受信したとき，OpenSent 状態または Connect 状態にあるすべてのコネクションを検査します。
	BGP FSM：IDLE 状態	エラーのために Idle 状態へ遷移したピアについて，続く Start までの間の時間は（Start イベントが自動的に生成されるなら），指数的に増大するべきです。その最初のタイマ値は 60 秒です。時間はリトライごとに 2 倍にされるべきです。	本装置では Idle 状態から start までの間の最初のタイマは 16～36 秒になります。
	BGP FSM：Active 状態	トランスポート・プロトコル・コネクションが成功した場合，ローカルシステムは Connect Retry タイマをクリアし，初期設定を完了し，そのピアへ OPEN メッセージを送信し，その Hold タイマをセットし，状態を Open Sent へ変えます。Hold タイマの値は 4 分が提案されています。	本装置では Hold タイマはデフォルトで 180 秒（3 分），コンフィグレーションで指定されている場合はコンフィグレーションの値を使用します。
	経路広告の頻度	Min Route Advertisement Interval は，単一の BGP スピーカからの特定の宛先への経路広告の間隔の最小時間を決めます。このレート制限処理は，宛先ごとにされます。しかし，Min Route Advertisement Interval の値は，BGP ピアごとに設定されます。	本装置では Min Route Advertisement Interval はサポートしていません。
		Min AS Origination Interval は，広告する BGP スピーカ自身の AS 中の変化を報告するための連続した UPDATE メッセージ広告の間に経過しなければならない最小時間を決めます	本装置では Min AS Origination Interval はサポートしていません。

RFC番号	RFC		本装置
	ジッタ	ある BGP スピーカによる BGP メッセージの配布がピークを含む可能性を最小にするために，Min AS Origination Interval，Keep Alive，Min Route Advertisement Interval に関係したタイマにジッタを適用すべきです。	本装置ではジッタを適用していません。
	経路集約	異なる MULTI_EXIT_DISC 属性を持つ経路は，集約してはなりません。	異なる MULTI_EXIT_DISC 属性を持つ経路を集約します。
		異なる NEXT_HOP を持つ経路を集約するときは，集約経路の NEXT_HOP 属性は，集約を実行する BGP スピーカ上のインタフェースを識別しなければなりません。	集約経路には NEXT_HOP 属性を設定しません。
	BGP タイマ	Connect Retry タイマの提案されている値は 120 秒です。	本装置では Connect Retry 回数によって変化する可変値（16～148 秒）になります。
		Hold Time の提案されている値は 90 秒です。	デフォルトの Hold Time は 180 秒です。コンフィグレーションに Hold Time が設定されている場合は，その値を使用します。
		Keep Alive タイマの提案されている値は 30 秒です。	デフォルトの Keep Alive タイマは Hold Time の 1/3 になります。コンフィグレーションに Keep Alive タイマ設定されている場合は，その値を使用します
		BGP によって，二つのオプションタイマ（DelayOpenTimer，IdleHoldTimer）をサポートすることができます。	DelayOpenTimer，IdleHoldTimer はサポートしていません。
RFC2545	通知するネクストホップと通知先のピアとが同じネットワーク上にある場合に限り，リンクローカルネクストホップも通知します。		本装置では外部ピアが直結ネットワークで接続されている場合だけ RFC と同じ処理を行います。
	トランスポート・プロトコル	BGP4+セッションに使用する TCP コネクションは IPv4 または IPv6 です。	本装置では IPv6 TCP による IPv6 経路情報通知だけサポートします。
	ピアリングアドレス種別	BGP4+ピアリングに IPv4 または IPv6 アドレスを使用します。	本装置では IPv6 アドレスだけサポートします。内部ピアでは IPv6 リンクローカルアドレスでの BGP4+接続はサポートしていません。
RFC5065	コンフェデレーションのメンバーとして参加しているすべての BGP スピーカは，AS_CONFED_SET と AS_CONFED_SEQUENCE のパスタイプを認識できなければなりません。		本装置は AS_CONFED_SET をサポートしません。AS_CONFED_SET を含む経路を受信した場合，該当パスタイプを無視します。

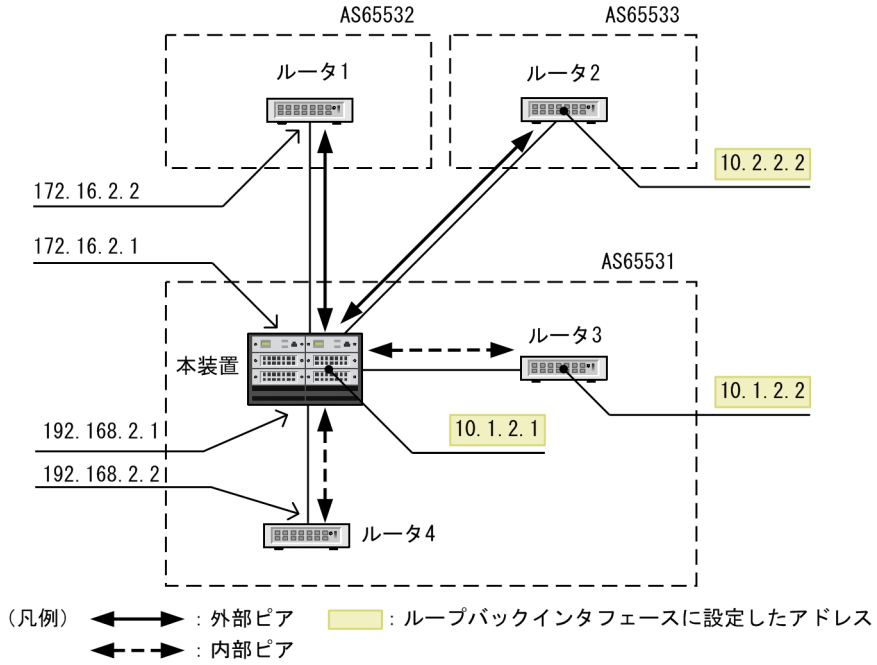
(2) 直接接続されたインタフェース上でピアリングする場合の注意事項

BGP4+では，直接接続されたインタフェース上の BGP スピーカ間で本装置が外部ピアまたはメンバー AS 間ピアを使用して，かつ同一インタフェース上で本装置が OSPFv3 仮想リンクの通過エリアとなる構成の場合，ピアとのコネクションが確立しません。この場合，コンフィグレーションコマンド neighbor ebgp-multihop を設定するとコネクションが確立します。

21.2　BGP4 のコンフィグレーション

次の図に示す構成例を基にコンフィグレーションを説明します。

図 21-11　接続構成例



- 本装置－ルータ 1 間：インタフェースのアドレスを使用
- 本装置－ルータ 2 間：ループバックインタフェースに設定したアドレスを使用
- 本装置－ルータ 3 間：ループバックインタフェースに設定したアドレスを使用
- 本装置－ルータ 4 間：インタフェースのアドレスを使用

21.2.1　コンフィグレーションコマンド一覧

BGP4 のコンフィグレーションコマンド一覧と運用コマンド一覧を次に示します。

表 21-4　コンフィグレーションコマンド一覧

コマンド名	説明
address-family ipv4	VRF 単位の情報を設定します。config-router-af（ipv4 vrf）モードへ移行します。
bgp always-compare-med	異なる AS から学習した MED 属性を比較することを設定します。
bgp bestpath compare-routerid※1	外部ピアから学習した経路間で相手 BGP 識別子（ルータ ID）によって経路選択することを設定します。
bgp default local-preference	BGP4 で広告する経路の LOCAL_PREF 属性のデフォルト値を設定します。
bgp nexthop	BGP4 経路のネクストホップ解決に使用する経路を指定します。
bgp router-id※1	自ルータの識別子を設定します。

コマンド名	説明
default-information originate	デフォルト経路を全ピアへ広告します。
default-metric	BGP4 で広告する経路の MED 属性のデフォルト値を設定します。
disable※1	BGP4 および BGP4+の動作を抑止します。
distance bgp	BGP4 で学習した経路のディスタンス値を設定します。
neighbor description	ピアの補足説明を設定します。
neighbor ebgp-multihop	インタフェースで直接接続されない外部ピアおよびメンバー AS 間ピアとの接続を許容することを設定します。
neighbor enforce-first-as-disable	外部ピアから受信した経路情報の AS_PATH 属性の先頭 AS 番号がピアの AS 番号以外でも，経路情報を正常に取り扱います。本コマンドはピアがルートサーバである場合に指定します。
neighbor local-as	外部ピアとのピアリングで使用する自 AS 番号を設定します。
neighbor next-hop-self	BGP4 ピアから学習した経路を BGP4 ピアへ広告する際に NEXT_HOP 属性をピアリングに使用する自側アドレスに書き替えることを設定します。
neighbor remote-as	BGP4 ピアを設定します。
neighbor remove-private-as	BGP4 ピアへ広告する際にプライベート AS 番号を取り除くことを指定します。
neighbor shutdown	ピアとの接続を抑止します。
neighbor soft-reconfiguration	入力ポリシーで抑止した経路も保持します。
neighbor timers	ピアとの接続に使用する KEEPALIVE メッセージの送信間隔とホールドタイマ値を設定します。
neighbor update-source	ピアリングに使用する自側アドレスにループバックインタフェースに設定したアドレスを設定します。
neighbor weight	ピアから学習する経路の重み付けを設定します。
router bgp※1	ルーティングプロトコルの BGP4 および BGP4+に関する動作情報を設定します。
timers bgp※1	全ピアに適用する KEEPALIVE メッセージの送信間隔とホールドタイマ値を設定します。
routing options auto-update-filter※1※2	BGP4 に関する経路フィルタの設定内容をランニングコンフィグレーションに反映するときに，BGP4 の学習経路フィルタリングと広告経路フィルタリングに適用します。
distribute-list in (BGP4)※3	BGP4 の学習経路フィルタリングの条件として使用する経路フィルタを指定します。
distribute-list out (BGP4)※3	BGP4 の広告経路フィルタリングの条件として使用する経路フィルタを指定します。
neighbor in (BGP4)※3	BGP4 の特定のピアにだけ，学習経路フィルタリングの条件として使用する経路フィルタを指定します。

コマンド名	説明
neighbor out (BGP4)※3	BGP4 の特定のピアにだけ，広告経路フィルタリングの条件として使用する経路フィルタを指定します。
redistribute (BGP4)※3	BGP4 で広告する経路のプロトコルを指定します。

注※1

BGP4+ピアと共用のコマンドです。

注※2

「コンフィグレーションコマンドレファレンス Vol.3　13. ルーティングオプション」を参照してください。

注※3

「コンフィグレーションコマンドレファレンス Vol.3　22. 経路フィルタリング」を参照してください。

表 21-5　コンフィグレーションに使用する運用コマンド一覧

コマンド名	説明
clear ip bgp	パラメータに * in を指定した場合 • BGP4 学習経路フィルタリングに最新の経路フィルタ設定を適用します。 • 全 BGP4 ピアに BGP4 経路の再広告要求をします。
	パラメータに * out を指定した場合 • BGP4 広告経路フィルタリングに最新の経路フィルタ設定を適用します。 • neighbor remove-private-as コマンドの設定を運用に反映します。 • 全 BGP4 ピアに BGP4 経路の再広告をします。
	パラメータに * both を指定した場合 • BGP4 学習経路フィルタリングと広告経路フィルタリングに最新の経路フィルタ設定を適用します。 • neighbor remove-private-as コマンドの設定を運用に反映します。 • 全 BGP4 ピアに BGP4 経路の再広告要求と再広告をします。
	パラメータに * を指定した場合 • 全 BGP4 ピアを切断します。

21.2.2　コンフィグレーションの流れ

1. あらかじめ，IPv4 インタフェースを設定します。
2. あらかじめ，ループバックインタフェースにアドレスを設定します。
3. BGP4 ピアを設定します。
4. BGP4 経路の学習ポリシーを設定します。
5. BGP4 経路の広告ポリシーを設定します。
6. 学習用経路フィルタを設定します。
7. 広告用経路フィルタを設定します。
8. 学習経路フィルタリングの条件を設定します。
9. 広告経路フィルタリングの条件を設定します。
10. 経路フィルタリングを運用に反映させます。

[注意事項]

- BGP4 ピアのコンフィグレーション設定時に経路フィルタリングのコンフィグレーションが設定されていない場合，ピアが確立すると自動的に経路の学習と経路の広告をします。意図しない経路の学習と経路の広告を抑止させたい場合，neighbor remote-as コマンドの設定前に disable コマンドを設定して，BGP4 の動作を抑止してください。経路フィルタリングのコンフィグレーション設定後，BGP4 を動作させる場合は disable コマンドを削除してください。
- routing options auto-update-filter コマンドを設定している場合，コミットモードは手動コミットモードで運用してください。逐次コミットモードで運用した場合，BGP4 に関する経路フィルタリングのコンフィグレーションを変更するたびに運用に反映します。

21.2.3 BGP4 ピアの設定

[設定のポイント]

ピアの設定では最初に neighbor remote-as コマンドでピアの相手側アドレスと相手側の AS 番号を設定したあと，該当ピアのほかの情報を設定してください。

[コマンドによる設定]

1. **(config)# router bgp 65531**
   ルーティングプロトコルに BGP4 および BGP4+を適用します。パラメータに自ルータが所属する AS 番号（65531）を指定します。
2. **(config-router)# bgp router-id 192.168.1.100**
   自ルータ識別子（192.168.1.100）を設定します。
3. **(config-router)# neighbor 172.16.2.2 remote-as 65532**
   外部ピア（相手側アドレス：172.16.2.2，AS 番号：65532）を設定します。
4. **(config-router)# neighbor 10.2.2.2 remote-as 65533**
   外部ピア（相手側アドレス：10.2.2.2，AS 番号：65533）を設定します。
5. **(config-router)# neighbor 10.2.2.2 ebgp-multihop**
   ピアリングに使用するアドレスにピアと直接接続されたインタフェースのアドレスを使用しないことを設定します。
6. **(config-router)# neighbor 10.2.2.2 update-source loopback 0**
   ピアリングに使用する自側アドレスとしてループバックインタフェースに設定したアドレスを指定します。
7. **(config-router)# neighbor 192.168.2.2 remote-as 65531**
   内部ピア（相手側アドレス：192.168.2.2）を設定します。
8. **(config-router)# neighbor 10.1.2.2 remote-as 65531**
   内部ピア（相手側アドレス：10.1.2.2）を設定します。
9. **(config-router)# neighbor 10.1.2.2 update-source loopback 0**
   ピアリングに使用する自側アドレスとしてループバックインタフェースに設定したアドレスを指定します。

21.2.4 BGP4 経路の学習ポリシーの設定

[設定のポイント]

ピアごとに学習経路の優先度を設定する場合は，各ピアに weight 値を設定します。

[コマンドによる設定]

1. (config-router)# bgp always-compare-med
   異なる AS から受信した経路の MED 属性も経路選択の比較対象にします。
2. (config-router)# neighbor 172.16.2.2 weight 20
   (config-router)# neighbor 10.2.2.2 weight 20
   (config-router)# neighbor 10.1.2.2 weight 10
   (config-router)# neighbor 192.168.2.2 weight 10
   各ピアから学習した経路に weight 値を指定します。
   外部ピアから学習した経路が内部ピアから学習した経路より優先となるように設定します。

21.2.5　BGP4 経路の広告ポリシーの設定

[設定のポイント]

広告先ルータでの経路選択に使用する BGP4 のパス属性を設定します。

[コマンドによる設定]

1. (config-router)# default-metric 100
   広告する経路の MED 属性値に 100 を設定します。
2. (config-router)# bgp default local-preference 80
   (config-router)# exit
   内部ピアへ広告する LOCAL_PREF 属性値に 80 を設定します。

21.2.6　学習用経路フィルタの設定

[設定のポイント]

学習した BGP4 経路の優先度を設定する場合，route-map を使用して条件と設定値を指定します。

[コマンドによる設定]

1. (config)# ip prefix-list EXT_IN seq 10 permit 10.10.0.0/16
   (config)# route-map SET_LOCPREF_IN permit 10
   (config-route-map)# match ip address prefix-list EXT_IN
   (config-route-map)# set local-preference 120
   (config-route-map)# exit
   (config)# route-map SET_LOCPREF_IN permit 20
   (config-route-map)# exit
   宛先ネットワークが 10.10.0.0/16 の LOCAL_PREF 属性値に 120 を設定します。
2. (config)# ip as-path access-list 10 permit "_65529$"
   (config)# route-map SET_ASPREPEND_IN permit 10
   (config-route-map)# match as-path 10
   (config-route-map)# set as-path prepend count 1
   (config-route-map)# exit
   (config)# route-map SET_ASPREPEND_IN permit 20
   (config-route-map)# exit

AS_PATH 属性の AS 配列の最終が 65529 の場合に AS 配列の AS 数を 1 個追加します。

3.
```
(config)# ip prefix-list INT_IN_1 seq 10 permit 172.20.0.0/16
(config)# route-map SET_ORIGIN_IN permit 10
(config-route-map)# match ip address prefix-list INT_IN_1
(config-route-map)# set origin incomplete
(config-route-map)# exit
(config)# route-map SET_ORIGIN_IN permit 20
(config-route-map)# exit
```
宛先ネットワークが 172.20.0.0/16 の場合，ORIGIN 属性に INCOMPLETE を設定します。

4.
```
(config)# ip prefix-list INT_IN_2 seq 10 permit 172.30.0.0/16
(config)# route-map SET_MED_IN permit 10
(config-route-map)# match ip address prefix-list INT_IN_2
(config-route-map)# set metric 100
(config-route-map)# exit
(config)# route-map SET_MED_IN permit 20
(config-route-map)# exit
```
宛先ネットワークが 172.30.0.0/16 の場合，MED 属性値に 100 を設定します。

21.2.7 広告用経路フィルタの設定

[設定のポイント]

広告する BGP4 経路の優先度を設定する場合，route-map を使用して条件と設定値を指定します。

[コマンドによる設定]

1.
```
(config)# ip prefix-list MY_NET_1 seq 10 permit 192.168.10.0/24
(config)# ip prefix-list MY_NET_2 seq 10 permit 192.168.20.0/24
(config)# route-map SET_EXT_OUT permit 10
(config-route-map)# match ip address prefix-list MY_NET_1
(config-route-map)# set metric 120
(config-route-map)# exit
(config)# route-map SET_EXT_OUT permit 20
(config-route-map)# match ip address prefix-list MY_NET_2
(config-route-map)# exit
```
宛先ネットワークが 192.168.10.0/24 の場合，MED 属性値に 120 を設定します。
宛先ネットワークが 192.168.20.0/24 も広告対象にします。

21.2.8 学習経路フィルタリングの条件の設定

[設定のポイント]

ピアごとに学習用経路フィルタを適用する場合，neighbor in コマンドで適用するフィルタを指定します。

[コマンドによる設定]

1. (config)# router bgp 65531
   (config-router)# neighbor 172.16.2.2 route-map SET_LOCPREF_IN in
   ピア（相手側アドレス：172.16.2.2）から学習した宛先ネットワークが 10.10.0.0/16 の経路の LOCAL_PREF 属性値に 120 を設定して，ほかのピアから学習した経路より優先に設定します。
2. (config-router)# neighbor 10.2.2.2 route-map SET_ASPREPEND_IN in
   ピア（相手側アドレス：10.2.2.2）から学習した AS_PATH 属性の AS 配列の最終が 65529 の場合に AS 配列の AS 数を 1 個追加して，ほかのピアから学習した経路より非優先に設定します。
3. (config-router)# neighbor 10.1.2.2 route-map SET_ORIGIN_IN in
   ピア（相手側アドレス：10.1.2.2）から学習した宛先ネットワークが 172.20.0.0/16 の経路の ORIGIN 属性に INCOMPLETE を設定して，ほかのピアから学習した経路より非優先に設定します。
4. (config-router)# neighbor 192.168.2.2 route-map SET_MED_IN in
   ピア（相手側アドレス：192.168.2.2)から学習した宛先ネットワークが 172.30.0.0/16 の経路の MED 属性に 100 を設定します。

21.2.9　広告経路フィルタリングの条件の設定

[設定のポイント]

全ピアに同一の広告用経路フィルタを適用する場合，distribute-list out コマンドで適用するフィルタを指定します。

[コマンドによる設定]

1. (config-router)# distribute-list route-map SET_EXT_OUT out
   (config-router)# exit
   (config)# exit
   全外部ピアへ宛先ネットワークが 192.168.10.0/24 と 192.168.20.0/24 の経路を広告します。

21.2.10　経路フィルタリングの運用への反映

[設定のポイント]

コミットモードが逐次コミットモードの場合，運用コマンド clear ip bgp を使用して，学習経路フィルタリングの条件および広告経路フィルタリングの条件として設定した経路フィルタを運用に反映します。コミットモードが手動コミットモードの場合，routing options auto-update-filter コマンドを設定して，commit コマンドで運用に反映します。

[コマンドによる設定]

1. # clear ip bgp * both
   コミットモードが逐次コミットモードの場合に，学習用経路フィルタと広告用経路フィルタを運用に反映します。

[注意事項]

運用コマンド clear ip bgp（* in，* out，* both 指定）は経路フィルタの変更反映とルート・リフレッシュ（「22.1.5　ルート・リフレッシュ」参照）の両方を実行します。ルート・リフレッシュのネゴシエーションが成立していない場合，経路再学習のためのルート・リフレッシュ要求はしませんが，経路フィルタの変更は反映します。

21.2.11 VRF での BGP4 の設定

[設定のポイント]

VRF の BGP4 は config-router-af（ipv4 vrf）モードで設定します。

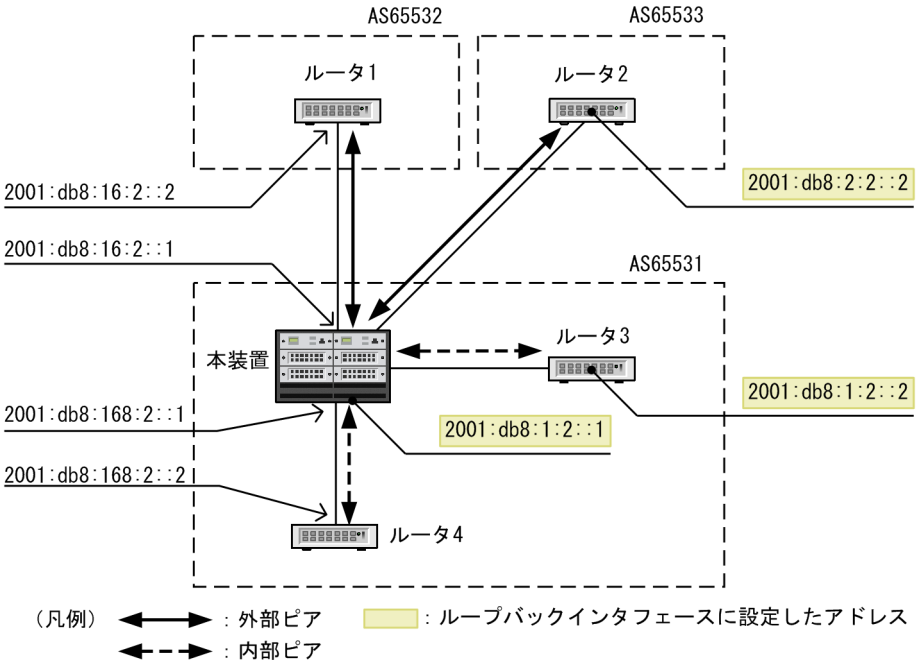
[コマンドによる設定]

1. **(config)# router bgp 65531**
   自 AS 番号（65531）を指定します。
2. **(config-router)# address-family ipv4 vrf 10**
   VRF 10 の config-router-af（ipv4 vrf）モードへ移行します。
3. **(config-router-af)# bgp router-id 192.168.1.100**
   自ルータ識別子（192.168.1.100）を指定します。
4. **(config-router-af)# neighbor 10.1.2.2 remote-as 65531**
   内部ピア（相手側アドレス：10.1.2.2）を指定します。
5. **(config-router-af)# neighbor 172.16.2.2 remote-as 65532**
   外部ピア（相手側アドレス：172.16.2.2）を指定します。

21.3　BGP4+のコンフィグレーション

次の図に示す構成例を基にコンフィグレーションを説明します。

図 21-12　接続構成例



- 本装置－ルータ 1 間：インタフェースのアドレスを使用
- 本装置－ルータ 2 間：ループバックインタフェースに設定したアドレスを使用
- 本装置－ルータ 3 間：ループバックインタフェースに設定したアドレスを使用
- 本装置－ルータ 4 間：インタフェースのアドレスを使用

21.3.1　コンフィグレーションコマンド一覧

BGP4+のコンフィグレーションコマンド一覧と運用コマンド一覧を次に示します。

表 21-6　コンフィグレーションコマンド一覧

コマンド名	説明
address-family ipv6	グローバルネットワークの情報を設定する config-router-af（ipv6）モード，または VRF の情報を設定する config-router-af（ipv6 vrf）モードへ移行します。
bgp always-compare-med	異なる AS から学習した MED 属性を比較することを設定します。
bgp bestpath compare-routerid※1	外部ピアから学習した経路間で相手 BGP 識別子（ルータ ID）によって経路選択することを設定します。
bgp default local-preference	BGP4+で広告する経路の LOCAL_PREF 属性のデフォルト値を設定します。
bgp nexthop	BGP4+経路のネクストホップ解決に使用する経路を指定します。

コマンド名	説明
bgp router-id※1	自ルータの識別子を設定します。
default-information originate	デフォルト経路を全ピアへ広告します。
default-metric	BGP4+で広告する経路の MED 属性のデフォルト値を設定します。
disable※1	BGP4 および BGP4+の動作を抑止します。
distance bgp	BGP4+で学習した経路のディスタンス値を設定します。
neighbor activate	ピアとの IPv6 アドレスファミリの経路交換を可能にします。
neighbor description	ピアの補足説明を設定します。
neighbor ebgp-multihop	インタフェースで直接接続されない外部ピアおよびメンバー AS 間ピアとの接続を許容することを設定します。
neighbor enforce-first-as-disable	外部ピアから受信した経路情報の AS_PATH 属性の先頭 AS 番号がピアの AS 番号以外でも，経路情報を正常に取り扱います。本コマンドはピアがルートサーバである場合に指定します。
neighbor local-as	外部ピアとのピアリングで使用する自 AS 番号を設定します。
neighbor next-hop-self	BGP4+ピアから学習した経路を BGP4+ピアへ広告する際に MP_REACH_NLRI 属性のネクストホップ情報をピアリングに使用する自側アドレスに書き替えることを設定します。
neighbor password	ピアとの接続に TCP MD5 認証を使用することを設定します。
neighbor remote-as	BGP4+ピアを設定します。
neighbor remove-private-as	BGP4+ピアへ広告する際にプライベート AS 番号を取り除くことを指定します。
neighbor shutdown	ピアとの接続を抑止します。
neighbor soft-reconfiguration	入力ポリシーで抑止した経路も保持します。
neighbor timers	ピアとの接続に使用する KEEPALIVE メッセージの送信間隔とホールドタイマ値を設定します。
neighbor update-source	ピアリングに使用する自側アドレスにループバックインタフェースに設定したアドレスを設定します。
neighbor weight	ピアから学習する経路の重み付けを設定します。
router bgp※1	ルーティングプロトコルの BGP4 および BGP4+に関する動作情報を設定します。
timers bgp※1	全ピアに適用する KEEPALIVE メッセージの送信間隔とホールドタイマ値を設定します。
routing options auto-update-filter※1※2	BGP4+に関する経路フィルタの設定内容をランニングコンフィグレーションに反映するときに，BGP4+の学習経路フィルタリングと広告経路フィルタリングに適用します。
distribute-list in (BGP4+)※3	BGP4+の学習経路フィルタリングの条件として使用する経路フィルタを指定します。

コマンド名	説明
distribute-list out (BGP4+)※3	BGP4+の広告経路フィルタリングの条件として使用する経路フィルタを指定します。
neighbor in (BGP4+)※3	BGP4+の特定のピアにだけ，学習経路フィルタリングの条件として使用する経路フィルタを指定します。
neighbor out (BGP4+)※3	BGP4+の特定のピアにだけ，広告経路フィルタリングの条件として使用する経路フィルタを指定します。
redistribute (BGP4+)※3	BGP4+で広告する経路のプロトコルを指定します。

注※1

BGP4 ピアと共用のコマンドです。

注※2

「コンフィグレーションコマンドレファレンス Vol.3　13. ルーティングオプション」を参照してください。

注※3

「コンフィグレーションコマンドレファレンス Vol.3　22. 経路フィルタリング」を参照してください。

表 21-7　コンフィグレーションに使用する運用コマンド一覧

コマンド名	説明
clear ipv6 bgp	パラメータに * in を指定した場合 • BGP4+学習経路フィルタリングに最新の経路フィルタ設定を適用します。 • 全 BGP4+ピアに BGP4+経路の再広告要求をします。
	パラメータに * out を指定した場合 • BGP4+広告経路フィルタリングに最新の経路フィルタ設定を適用します。 • neighbor remove-private-as コマンドの設定を運用に反映します。 • 全 BGP4+ピアに BGP4+経路の再広告をします。
	パラメータに * both を指定した場合 • BGP4+学習経路フィルタリングと広告経路フィルタリングに最新の経路フィルタ設定を適用します。 • neighbor remove-private-as コマンドの設定を運用に反映します。 • 全 BGP4+ピアに BGP4+経路の再広告要求と再広告をします。
	パラメータに * を指定した場合 • 全 BGP4+ピアを切断します。

21.3.2　コンフィグレーションの流れ

1. あらかじめ，IPv6 インタフェースを設定します。
2. あらかじめ，ループバックインタフェースにアドレスを設定します。
3. BGP4+ピアを設定します。
4. BGP4+経路の学習ポリシーを設定します。
5. BGP4+経路の広告ポリシーを設定します。
6. 学習用経路フィルタを設定します。

7. 広告用経路フィルタを設定します。
8. 学習経路フィルタリングの条件を設定します。
9. 広告経路フィルタリングの条件を設定します。
10. 経路フィルタリングを運用に反映させます。

[注意事項]

- BGP4+ピアと接続する場合は neighbor activate コマンドを設定して，IPv6 アドレスファミリを有効にしてください。IPv6 アドレスファミリが有効でない場合，BGP4+ピアと接続できません。
- BGP4+ピアのコンフィグレーション設定時に経路フィルタリングのコンフィグレーションが設定されていない場合，ピアが確立すると自動的に経路の学習と経路の広告をします。意図しない経路の学習と経路の広告を抑止させたい場合，neighbor remote-as コマンドの設定前に disable コマンドを設定して，BGP4+の動作を抑止してください。経路フィルタリングのコンフィグレーション設定後，BGP4+を動作させる場合は disable コマンドを削除してください。
- routing options auto-update-filter コマンドを設定している場合，コミットモードは手動コミットモードで運用してください。逐次コミットモードで運用した場合，BGP4+に関する経路フィルタリングのコンフィグレーションを変更するたびに運用に反映します。

21.3.3 BGP4+ピアの設定

[コマンドによる設定]

1. **(config)# router bgp 65531**
   ルーティングプロトコルに BGP および BGP4+を適用します。パラメータに自ルータが所属する AS 番号（65531）を指定します。
2. **(config-router)# bgp router-id 192.168.1.100**
   自ルータ識別子（192.168.1.100）を設定します。
3. **(config-router)# neighbor 2001:db8:16:2::2 remote-as 65532**
   外部ピア（相手側アドレス：2001:db8:16:2::2，AS 番号：65532）を設定します。
4. **(config-router)# neighbor 2001:db8:2:2::2 remote-as 65533**
   外部ピア（相手側アドレス：2001:db8:2:2::2，AS 番号：65533）を設定します。
5. **(config-router)# neighbor 2001:db8:2:2::2 ebgp-multihop**
   ピアリングに使用するアドレスにピアと直接接続されたインタフェースのアドレスを使用しないことを設定します。
6. **(config-router)# neighbor 2001:db8:2:2::2 update-source loopback 0**
   ピアリングに使用する自側アドレスとしてループバックインタフェースに設定したアドレスを指定します。
7. **(config-router)# neighbor 2001:db8:168:2::2 remote-as 65531**
   内部ピア（相手側アドレス：2001:db8:168:2::2）を設定します。
8. **(config-router)# neighbor 2001:db8:1:2::2 remote-as 65531**
   内部ピア（相手側アドレス：2001:db8:1:2::2）を設定します。
9. **(config-router)# neighbor 2001:db8:1:2::2 update-source loopback 0**
   ピアリングに使用する自側アドレスとしてループバックインタフェースに設定したアドレスを指定します。
10. **(config-router)# address-family ipv6**

config-router-af（ipv6）モードへ移行します。

11. **(config-router-af)# neighbor 2001:db8:16:2::2 activate**
    外部ピア（相手側アドレス：2001:db8:16:2::2）の IPv6 アドレスファミリを有効にします。
12. **(config-router-af)# neighbor 2001:db8:2:2::2 activate**
    外部ピア（相手側アドレス：2001:db8:2:2::2）の IPv6 アドレスファミリを有効にします。
13. **(config-router-af)# neighbor 2001:db8:168:2::2 activate**
    内部ピア（相手側アドレス：2001:db8:168:2::2）の IPv6 アドレスファミリを有効にします。
14. **(config-router-af)# neighbor 2001:db8:1:2::2 activate**
    内部ピア（相手側アドレス：2001:db8:1:2::2）の IPv6 アドレスファミリを有効にします。

21.3.4　BGP4+経路の学習ポリシーの設定

[設定のポイント]

ピアごとに学習経路の優先度を設定する場合は，ピアごとに weight 値を設定します。

[コマンドによる設定]

1. **(config-router-af)# bgp always-compare-med**
   異なる AS から受信した経路の MED 属性も経路選択の比較対象にします。
2. **(config-router-af)# neighbor 2001:db8:16:2::2 weight 20**
   (config-router-af)# neighbor 2001:db8:2:2::2 weight 20
   (config-router-af)# neighbor 2001:db8:1:2::2 weight 10
   (config-router-af)# neighbor 2001:db8:168:2::2 weight 10
   各ピアから学習した経路に weight 値を指定します。
   外部ピアから学習した経路が内部ピアから学習した経路より優先となるように設定します。

21.3.5　BGP4+経路の広告ポリシーの設定

[設定のポイント]

広告先ルータでの経路選択に使用する BGP4+のパス属性を設定します。

[コマンドによる設定]

1. **(config-router-af)# default-metric 120**
   広告する経路の MED 属性値に 120 を設定します。
2. **(config-router-af)# bgp default local-preference 80**
   (config-router-af)# exit
   (config-router)# exit
   内部ピアへ広告する LOCAL_PREF 属性値に 80 を設定します。

21.3.6　学習用経路フィルタの設定

[設定のポイント]

学習した BGP4+経路の優先度を設定する場合，route-map を使用して条件と設定値を指定します。

[コマンドによる設定]

1. (config)# ipv6 prefix-list EXT_IN seq 10 permit 2001:db8:10::/64
   (config)# route-map SET_LOCPREF_IN permit 10
   (config-route-map)# match ipv6 address prefix-list EXT_IN
   (config-route-map)# set local-preference 120
   (config-route-map)# exit
   (config)# route-map SET_LOCPREF_IN permit 20
   (config-route-map)# exit
   宛先ネットワークが 2001:db8:10::/64 の LOCAL_PREF 属性値に 120 を設定します。
2. (config)# ip as-path access-list 10 permit "_65529$"
   (config)# route-map SET_ASPREPEND_IN permit 10
   (config-route-map)# match as-path 10
   (config-route-map)# set as-path prepend count 1
   (config-route-map)# exit
   (config)# route-map SET_ASPREPEND_IN permit 20
   (config-route-map)# exit
   AS_PATH 属性の AS 配列の最終が 65529 の場合に AS 配列の AS 数を 1 個追加します。
3. (config)# ipv6 prefix-list INT_IN_1 seq 10 permit 2001:db8:20::/64
   (config)# route-map SET_ORIGIN_IN permit 10
   (config-route-map)# match ipv6 address prefix-list INT_IN_1
   (config-route-map)# set origin incomplete
   (config-route-map)# exit
   (config)# route-map SET_ORIGIN_IN permit 20
   (config-route-map)# exit
   宛先ネットワークが 2001:db8:20::/64 の場合，ORIGIN 属性に INCOMPLETE を設定します。
4. (config)# ipv6 prefix-list INT_IN_2 seq 10 permit 2001:db8:30::/64
   (config)# route-map SET_MED_IN permit 10
   (config-route-map)# match ipv6 address prefix-list INT_IN_2
   (config-route-map)# set metric 100
   (config-route-map)# exit
   (config)# route-map SET_MED_IN permit 20
   (config-route-map)# exit
   宛先ネットワークが 2001:db8:30::/64 の場合，MED 属性値に 100 を設定します。

21.3.7 広告用経路フィルタの設定

[設定のポイント]

広告する BGP4+経路の優先度を設定する場合，route-map を使用して条件と設定値を指定します。

[コマンドによる設定]

1. (config)# ipv6 prefix-list MY_NET_1 seq 10 permit 2001:db8:169:10::/64
   (config)# ipv6 prefix-list MY_NET_2 seq 10 permit 2001:db8:169:20::/64
   (config)# route-map SET_EXT_OUT permit 10
   (config-route-map)# match ipv6 address prefix-list MY_NET_1

```
(config-route-map)# set metric 120
(config-route-map)# exit
(config)# route-map SET_EXT_OUT permit 20
(config-route-map)# match ipv6 address prefix-list MY_NET_2
(config-route-map)# exit
```

宛先ネットワークが 2001:db8:169:10::/64 の場合，MED 属性値に 120 を設定します。

宛先ネットワークが 2001:db8:169:20::/64 も広告対象にします。

21.3.8　学習経路フィルタリングの条件の設定

[設定のポイント]

ピアごとに学習用経路フィルタを適用する場合，neighbor in コマンドで適用するフィルタを指定します。

[コマンドによる設定]

1.
```
(config)# router bgp 65531
(config-router)# address-family ipv6
(config-router-af)# neighbor 2001:db8:16:2::2 route-map SET_LOCPREF_IN in
```
ピア（相手側アドレス：2001:db8:16:2::2）から学習した宛先ネットワークが 2001:db8:10::/64 の経路の LOCAL_PREF 属性値に 120 を設定して，ほかのピアから学習した経路より優先にします。

2.
```
(config-router-af)# neighbor 2001:db8:2:2::2 route-map SET_ASPREPEND_IN in
```
ピア（相手側アドレス：2001:db8:2:2::2）から学習した AS_PATH 属性の AS 配列の最終が 65529 の場合に AS 配列の AS 数を 1 個追加して，ほかのピアから学習した経路より非優先に設定します。

3.
```
(config-router-af)# neighbor 2001:db8:1:2::2 route-map SET_ORIGIN_IN in
```
ピア（相手側アドレス：2001:db8:1:2::2）から学習した宛先ネットワークが 2001:db8:20::/64 の経路の ORIGIN 属性に INCOMPLETE を設定して，ほかのピアから学習した経路より非優先に設定します。

4.
```
(config-router-af)# neighbor 2001:db8:168:2::2 route-map SET_MED_IN in
```
ピア（相手側アドレス：2001:db8:168:2::2）から学習した宛先ネットワークが 2001:db8:30::/64 の経路の MED 属性に 100 を設定します。

21.3.9　広告経路フィルタリングの条件の設定

[設定のポイント]

全ピアに同一の広告用経路フィルタを適用する場合，distribute-list out コマンドで適用するフィルタを指定します。

[コマンドによる設定]

1.
```
(config-router-af)# distribute-list route-map SET_EXT_OUT out
(config-router-af)# exit
(config-router)# exit
(config)# exit
```
全外部ピアへ宛先ネットワークが 2001:db8:169:10::/64 と 2001:db8:169:20::/64 の経路を広告します。

21.3.10 経路フィルタリングの運用への反映

[設定のポイント]

コミットモードが逐次コミットモードの場合，運用コマンド clear ipv6 bgp を使用して，学習経路フィルタリングの条件および広告経路フィルタリングの条件として設定した経路フィルタを運用に反映します。コミットモードが手動コミットモードの場合，routing options auto-update-filter コマンドを設定して，commit コマンドで運用に反映します。

[コマンドによる設定]

1. **# clear ipv6 bgp * both**
   コミットモードが逐次コミットモードの場合に，学習用経路フィルタと広告用経路フィルタを運用に反映します。

[注意事項]

運用コマンド clear ipv6 bgp（* in，* out，* both 指定）は経路フィルタの変更反映とルート・リフレッシュ（「22.1.5 ルート・リフレッシュ」参照）の両方を実行します。ルート・リフレッシュのネゴシエーションが成立していない場合，経路再学習のためのルート・リフレッシュ要求はしませんが経路フィルタの変更は反映します。

21.3.11 VRF での BGP4+の設定

[設定のポイント]

VRF の BGP4+は config-router-af（ipv6 vrf）モードで設定します。

[コマンドによる設定]

1. **(config)# router bgp 64496**
   自 AS 番号（64496）を指定します。
2. **(config-router)# address-family ipv6 vrf 10**
   VRF 10 の config-router-af（ipv6 vrf）モードへ移行します。
3. **(config-router-af)# bgp router-id 192.168.1.100**
   自ルータ識別子（192.168.1.100）を指定します。
4. **(config-router-af)# neighbor 2001:db8:1::2 remote-as 64511**
   外部ピア（相手側アドレス：2001:db8:1::2，AS 番号：64511）を指定します。
5. **(config-router-af)# neighbor 2001:db8:2::2 remote-as 64496**
   内部ピア（相手側アドレス：2001:db8:2::2，AS 番号：64496）を指定します。
6. **(config-router-af)# neighbor 2001:db8:1::2 activate**
   外部ピア（相手側アドレス：2001:db8:1::2）の IPv6 アドレスファミリを有効にします。
7. **(config-router-af)# neighbor 2001:db8:2::2 activate**
   内部ピア（相手側アドレス：2001:db8:2::2）の IPv6 アドレスファミリを有効にします。

21.4　オペレーション

21.4.1　運用コマンド一覧

BGP4 の運用コマンド一覧を次の表に示します。

表 21-8　運用コマンド一覧（BGP4）

コマンド名	説明
show ip route	ルーティングテーブルで保持する IPv4 経路情報を表示します。
clear ip route	H/W の IPv4 フォワーディングエントリをクリアして再登録します。
show ip bgp	BGP4 プロトコルに関する情報を表示します。
clear ip bgp	BGP4 セッションもしくは BGP4 プロトコルに関する情報のクリア，または新しい BGP フィルタ情報を使用して受信経路と送信経路のフィルタリングをします。また，BGP4 学習経路数制限によって，切断している BGP4 セッションを再接続します。
show ip vrf	VRF の IPv4 情報を表示します。

BGP4+の運用コマンド一覧を次の表に示します。

表 21-9　運用コマンド一覧（BGP4+）

コマンド名	説明
show ipv6 route	ルーティングテーブルで保持する IPv6 経路情報を表示します。
clear ipv6 route	H/W の IPv6 フォワーディングエントリをクリアして再登録します。
show ipv6 bgp	BGP4+プロトコルに関する情報を表示します。
clear ipv6 bgp	BGP4+セッションもしくは BGP4+プロトコルに関する情報のクリア，または新しい BGP フィルタ情報を使用して受信経路と送信経路のフィルタリングをします。また，BGP4+学習経路数制限によって，切断している BGP4+セッションを再接続します。
show ipv6 vrf	VRF の IPv6 情報を表示します。

21.4.2　ピアの種別と接続形態の確認

ピアの接続情報は，show ip bgp コマンドまたは show ipv6 bgp コマンドで neighbors パラメータを指定して表示します。詳細情報を表示する場合は，さらに detail パラメータを指定します。

図 21-13　show ip bgp コマンド（neighbors パラメータ指定）の実行結果

```
> show ip bgp neighbors
Date 20XX/03/18 22:45:55 UTC
Peer Address     Peer AS  Local Address    Local AS  Type      Status
10.1.2.2         65531    10.1.2.1         65531     Internal  Established
192.168.2.2      65531    192.168.2.1      65531     Internal  Established
10.2.2.2         65533    10.1.2.1         65531     External  Established
172.16.2.2       65532    172.16.2.1       65531     External  Established
```

図 21-14　show ip bgp コマンド（neighbors detail パラメータ指定）の実行結果

```
> show ip bgp neighbors detail
Date 20XX/03/17 15:52:14 UTC
BGP Peer: 10.1.2.2       , Remote AS: 65531
Remote Router ID: 10.1.2.102
```

```
    BGP Status: Established         HoldTime: 180  , Keepalive: 60
    Established Transitions: 1      Established Date: 20XX/03/17 15:51:00
    BGP Version: 4                  Type: Internal
    Local Address: 10.1.2.1         Local AS: 65531
    Local Router ID: 192.168.1.100
    Next Connect Retry: -           Connect Retry Timer: -
    Last Keep Alive Sent: 15:52:00  Last Keep Alive Received: 15:52:00
    BGP Message  UpdateIn   UpdateOut  TotalIn    TotalOut
                 0          0          2          4
    BGP Capability Negotiation: <IPv4-Uni Refresh Refresh(v)>
      Send   : <IPv4-Uni Refresh Refresh(v)>
      Receive: <IPv4-Uni Refresh Refresh(v)>
    Password: UnConfigured
    Track Name: -, Track ID: -, Track State: -

BGP Peer: 192.168.2.2    , Remote AS: 65531
Remote Router ID: 192.168.1.102
    BGP Status: Established         HoldTime: 180  , Keepalive: 60
    Established Transitions: 1      Established Date: 20XX/03/17 15:50:43
    BGP Version: 4                  Type: Internal
    Local Address: 192.168.2.1      Local AS: 65531
    Local Router ID: 192.168.1.100
    Next Connect Retry: -           Connect Retry Timer: -
    Last Keep Alive Sent: 15:51:43  Last Keep Alive Received: 15:51:43
    BGP Message  UpdateIn   UpdateOut  TotalIn    TotalOut
                 0          0          2          4
    BGP Capability Negotiation: <IPv4-Uni Refresh Refresh(v)>
      Send   : <IPv4-Uni Refresh Refresh(v)>
      Receive: <IPv4-Uni Refresh Refresh(v)>
    Password: UnConfigured
    Track Name: -, Track ID: -, Track State: -
      :
      :
>
```

21.4.3 経路選択結果の確認

経路選択の結果は，show ip bgp コマンドまたは show ipv6 bgp コマンドで確認できます。

図 21-15 show ip bgp コマンドの実行結果

```
> show ip bgp
Date 20XX/03/18 22:44:23 UTC
Local AS: 65531, Local Router ID: 192.168.1.100
Status Codes: d dampened, * valid, > active, S Stale, r RIB failure
Origin Codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop      MED   LocalPref Weight Path
*> 10.10/16         172.16.2.2    -     120       20     65532 65528 i      <-1
*  10.10/16         10.2.2.2      -     80        20     65533 65533 65529 i<-2
*  10.10/16         10.1.2.2      -     80        10     65534 i            <-3
*> 10.20/16         172.16.2.2    -     80        20     65532 65528 i      <-4
*  10.20/16         10.2.2.2      -     80        20     65533 65533 65529 i<-5
*> 172.20/16        192.168.2.2   -     100       10     65530    i         <-6
*  172.20/16        10.1.2.2      -     100       10     65534 65530 ?      <-7
*> 172.30/16        10.1.2.2      -     100       10     65534 i            <-8
*  172.30/16        192.168.2.2   100   100       10     65530 i            <-9
*> 192.168.10/24    10.1.2.2      -     100       10     65534 i           <-10
*  192.168.10/24    192.168.2.2   -     100       10     65530 i           <-11
*> 192.168.20/24    192.168.2.2   -     100       10           i           <-12
*> 192.168.30/24    192.168.2.2   -     100       10           i           <-13
```

1～3. 10.10/16 の経路選択

weight 値の比較によって 1 と 2 が優先され，次に LOCAL_PREF 属性の比較によって 1 が選択されています。

4～5. 10.20/16 の経路選択

AS_PATH 属性長の比較によって 4 が選択されています。

6～7.　172.20/16 の経路選択

ORIGIN 属性の比較によって 6 が選択されています。

8～9.　172.30/16 の経路選択

MED 属性の比較によって 8 が選択されています。

10～11.　192.168.10/24 の経路選択

相手 BGP 識別子の比較によって 10 が選択されています。

12～13.　192.168.20/24，192.168.30/24 の経路選択

ほかに同一宛先経路がないため 12，13 が選択されています。

21.4.4　経路の広告内容の確認

広告した経路のパス属性は，show ip bgp コマンドまたは show ipv6 bgp コマンドで advertised-routes パラメータを指定して確認します。

図 21-16　show ip bgp コマンド（advertised-routes パラメータ指定）の実行結果

```
> show ip bgp advertised-routes
Date 20XX/03/18 22:44:54 UTC
BGP Peer: 10.2.2.2       , Remote AS: 65533
Local AS: 65531, Local Router ID: 192.168.1.100
Origin Codes: i - IGP, e - EGP, ? - incomplete
Network              Next Hop        MED    LocalPref Path
192.168.20/24        192.168.2.2     120    -         65531 i          <-1
192.168.30/24        192.168.2.2     100    -         65531 i
BGP Peer: 172.16.2.2     , Remote AS: 65532
Local AS: 65531, Local Router ID: 192.168.1.100
Origin Codes: i - IGP, e - EGP, ? - incomplete
Network              Next Hop        MED    LocalPref Path
192.168.20/24        192.168.2.2     120    -         65531 i          <-2
192.168.30/24        192.168.2.2     100    -         65531 i
```

1～2.：広告した経路に MED 属性（値：120）が設定されています。

22 BGP4/BGP4+拡張機能

この章では，IPv4 のルーティングプロトコル BGP4 および IPv6 のルーティングプロトコル BGP4+の拡張機能について説明します。

22.1　解説

22.1.1　ピアグループ

ピアグループとは，ピアをグループ化して，グループ単位にコンフィグレーションコマンド neighbor で設定することで，設定を簡略化する機能です。ピアグループに設定した neighbor コマンドはピアグループに所属するすべてのピアに適用できます。また，ピアグループに所属するピアには個別にも neighbor コマンドを設定でき，その場合はピアグループの設定よりもピアの設定が優先されます。

ピアグループは BGP4 と BGP4+ごとに外部ピアおよびメンバー AS 間ピア単位，または内部ピア単位に設定できます。ピアグループは複数設定でき，ピアはそのうち一つのピアグループに所属できます。所属するピアグループを変更したピアには，BGP4 は運用コマンド clear ip bgp * {both | in | out}で，BGP4+は運用コマンド clear ipv6 bgp * {both | in | out}で，新しいピアグループの経路フィルタリングを反映します。

22.1.2　コミュニティ

本装置の BGP4 および BGP4+は経路情報に付いた COMMUNITIES 属性を使用して，経路情報の広告範囲を制限できます。

(1)　コミュニティの種類

本装置で取り扱うコミュニティの値は，次の 2 種類に分けられます。

- RFC1997 であらかじめ定義された値（コード）

  通知された経路情報に RFC1997 であらかじめ定義された値のコミュニティが付いている場合，その値に従って経路情報を広告します。RFC1997 で定義され，本装置で使用できるコミュニティについては，「表 22-1　本装置で使用できるコミュニティ」を参照してください。
- コンフィグレーションの学習経路フィルタまたは広告経路フィルタで指定された任意の値

  通知された経路情報に，コンフィグレーションの学習経路フィルタまたは広告経路フィルタで指定された任意の値のコミュニティが付いている場合，コンフィグレーションに従ってその経路情報を取り込むかどうか（学習経路フィルタ時），または広告するかどうか（広告経路フィルタ時）を制御します。

また，学習経路フィルタおよび広告経路フィルタによって，本装置が通知する経路情報に任意のコミュニティを付けられます。

RFC1997 で定義され，本装置で使用できるコミュニティを次の表に示します。

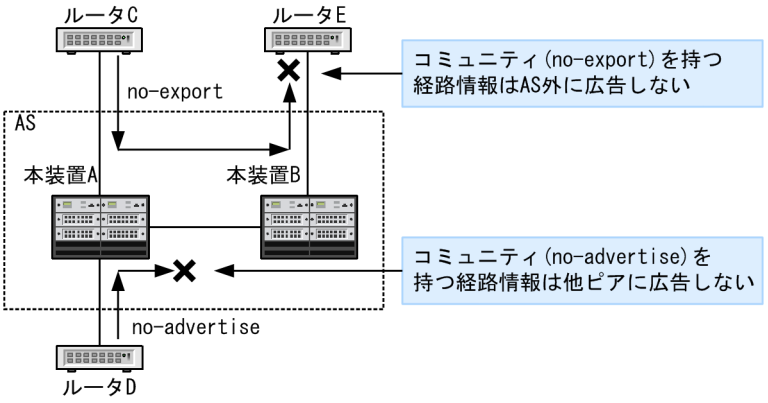
表 22-1　本装置で使用できるコミュニティ

コミュニティ	内容
no-export	この経路情報を AS 外に広告しません。
no-advertise	この経路情報をほかのピアに広告しません。
local-AS	この経路情報を他 AS を含めてメンバー AS 外に広告しません。

注　通常構成ではコミュニティの no-export と local-AS は同じ意味を持ちます。

また，コミュニティを持つ経路情報の広告範囲を次の図に示します。

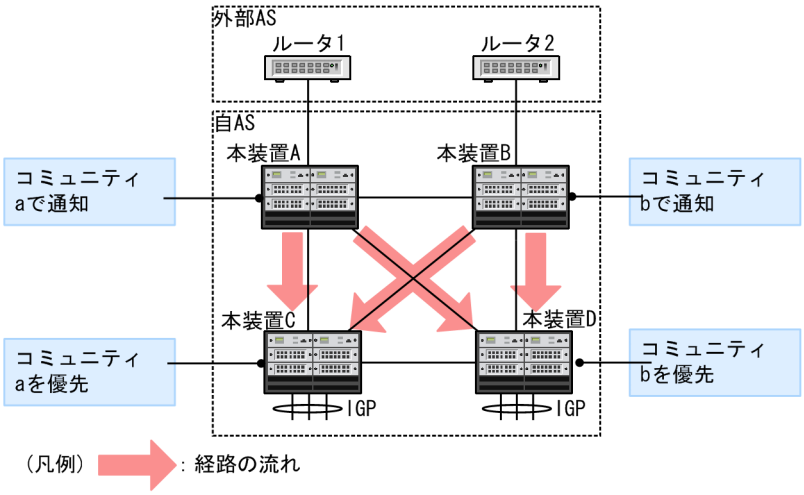
図 22-1　COMMUNITIES 属性を持つ経路情報の広告範囲



(2)　学習経路フィルタリングと COMMUNITIES 属性の使用例

学習経路フィルタリングと COMMUNITIES 属性の使用例を次の図に示します。

図 22-2　学習経路フィルタリングと COMMUNITIES 属性の使用例



この図で，一つの外部 AS に 2 台のルータ（本装置 A と本装置 B）が接続されているものとします。AS 外へのトラフィックの負荷分散を考慮して，本装置 C からのトラフィックは本装置 A を経由して AS 外に，本装置 D からのトラフィックは本装置 B を経由して AS 外に優先して中継するものとします。この場合，各ルータに次のような設定をすると，負荷分散できるようになります。

1. 本装置 A から内部ピアに通知する経路情報に，コミュニティ a を付けます（広告経路フィルタで指定できます）。
2. 本装置 B から内部ピアに通知する経路情報に，コミュニティ b を付けます（広告経路フィルタで指定できます）。
3. 本装置 C では，受信した経路情報がコミュニティ a を持つ場合，該当する経路情報の LOCAL_PREF 値を x（x ＞ y）に設定して，受信した経路情報がコミュニティ b を持つ場合，該当する経路情報の LOCAL_PREF 値を y（x ＞ y）に設定します。つまり，本装置 A から通知された LOCAL_PREF 値が大きい経路情報を優先します（学習経路フィルタで指定できます）。
4. 本装置 D では，受信した経路情報がコミュニティ a を持つ場合，該当する経路情報の LOCAL_PREF 値を y（x ＞ y）に設定して，受信した経路情報がコミュニティ b を持つ場合，該当する経路情報の

LOCAL_PREF 値を x（x ＞ y）に設定します。つまり，本装置 B から通知された LOCAL_PREF 値が大きい経路情報を優先します（学習経路フィルタで指定できます）。

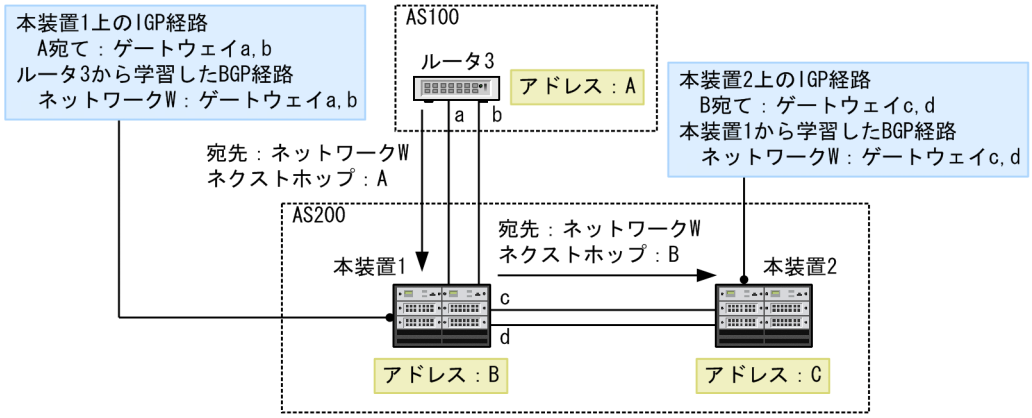
22.1.3　マルチパス

マルチパスは，一つの宛先ネットワークに対して複数の経路（パス）を生成して，トラフィックの負荷分散を実現します。本装置での BGP 経路のマルチパス生成は BGP4 と BGP4+で同じです。

(1)　IGP 経路のマルチパス化による BGP 経路のマルチパス

本装置は BGP 経路のネクストホップを IGP 経路に基づいて解決します。ネクストホップ解決時，BGP 経路の NEXT_HOP 属性値に対応する IGP 経路がマルチパス化されている場合は BGP 経路もマルチパス化されます。IGP 経路のマルチパス化による BGP 経路のマルチパス化を次の図に示します。

図 22-3　IGP 経路のマルチパス化による BGP 経路のマルチパス化



（凡例）　：ループバックインタフェースに設定したアドレス

各ルータ間は物理的に 2 本のインタフェースが接続されているものとします。各ルータ間のピアリングには装置自体に設定されたアドレスを使用するように構成します。本装置ではループバックインタフェースを指定したコンフィグレーションコマンド ip address で，装置自体にアドレスを設定できます。また，コンフィグレーションコマンド neighbor update-source を使用して，ピアリングの自側アドレスにループバックインタフェースに設定したアドレスを指定できます。なお，外部ピアおよびメンバー AS 間ピアでコンフィグレーションコマンド neighbor update-source を使用する場合は，コンフィグレーションコマンド neighbor ebgp-multihop も合わせて指定してください。

AS100 から本装置 1 に通知された BGP 経路（宛先：ネットワーク W，ネクストホップ：A）は，ネクストホップ解決時に IGP 経路を参照します。ネクストホップ：A 宛ての IGP 経路のゲートウェイが「a」および「b」となっているため，BGP 経路のゲートウェイも「a」および「b」になります。同様に，本装置 1 から本装置 2 に通知された BGP 経路（宛先：ネットワーク W，ネクストホップ：B）は，ネクストホップ B 宛ての IGP 経路のゲートウェイが「c」および「d」となっているため，BGP 経路のゲートウェイも「c」および「d」になります。

IGP 経路のマルチパス化に伴う BGP マルチパスの注意事項

本装置の BGP4 でマルチパス化できる IGP 経路はスタティック経路および OSPF 経路，BGP4+でマルチパス化できる IGP 経路はスタティック経路および OSPFv3 経路です。スタティック経路のマルチパス化については，「14.1　解説」を，OSPF 経路のマルチパス化については，「17.1.7　イコールコストマルチパス」を，OSPFv3 経路のマルチパス化については，「19.1.7　イコールコストマルチパス」を参照してください。

(2)　複数のピアから学習した BGP 経路のマルチパス

本装置はコンフィグレーションコマンド maximum-paths を使用して，同一隣接 AS と接続された複数のピアから学習したタイブレーク状態にある同一宛先への BGP 経路をマルチパス化できます。また，コンフィグレーションコマンド maximum-paths に all-as パラメータを指定すると，異なる隣接 AS から学習した BGP 経路をマルチパス化できます。タイブレーク条件を次の表に示します。

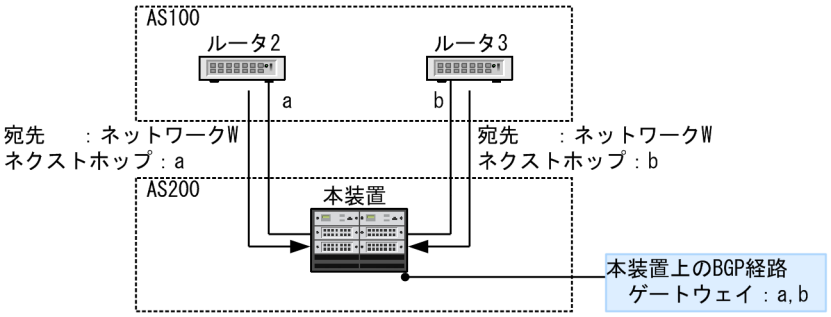
表 22-2　タイブレーク条件

条件	備考
weight 値が等しい	－
LOCAL_PREF 属性の値が等しい	－
AS_PATH 属性の取り扱い属性の AS 数が等しい	AS_PATH 属性の取り扱い属性上のパスタイプ AS_SET は，全体で一つの AS としてカウントします。
ORIGIN 属性の値が等しい	－
MED 属性の値が等しい	MED 属性値によるタイブレーク条件は，同一隣接 AS から学習した重複経路に対してだけ有効になります。なお，コンフィグレーションコマンド bgp always-compare-med を指定すると，異なる隣接 AS から学習した重複経路に対しても有効になります。
同一ピアタイプ（外部ピア，メンバー AS 間ピア，内部ピア）で学習している	－
ネクストホップ解決時に使用した IGP メトリックが等しい	－

（凡例）　－：該当しない

複数のピアから学習した BGP 経路のマルチパス化を次の図に示します。

図 22-4　複数のピアから学習した BGP 経路のマルチパス化



AS100 のルータ 2，およびルータ 3 から本装置 1 に通知された BGP 経路（ルータ 2 の経路：宛先 ネットワーク W，ネクストホップ a，ルータ 3 の経路：宛先 ネットワーク W，ネクストホップ b）がタイブレーク状態である場合，本装置 1 は各 BGP 経路が持っている NEXT_HOP 属性を基にゲートウェイを生成します。この図の例では，ゲートウェイは「a」および「b」となります。なお，該当する BGP 経路を本装置 1 からそのほかのピアに広告する場合は，今まで示した 2 経路のうち最優先経路を広告します。

22.1.4　サポート機能のネゴシエーション

サポート機能のネゴシエーション（Capability Negotiation）は，BGP コネクション確立時の OPEN メッセージに Capability 情報を付けることで，ピア間で使用できる機能をネゴシエーションする機能です。互いに広告した Capability 情報で一致する（互いにサポートする）機能を，該当するピアで使用できます。

本装置の BGP4 でネゴシエーションできる機能を次の表に示します。なお，ピアから Capability 情報を持たない OPEN メッセージを受信した場合，確立した BGP4 コネクションは，「IPv4 ユニキャスト経路の送受信」だけをします。

表 22-3　ネゴシエーションできる機能（BGP4）

機能名称	OPEN メッセージの Capability 情報	内容
IPv4 ユニキャスト経路の送受信	Capability Code：1 Capability Value の AFI：1 Capability Value の SAFI：1	IPv4 ユニキャスト経路を該当するピア間で送受信します。
ルート・リフレッシュ	Capability Code：2 Capability Value の AFI：1※	IPv4 経路のルート・リフレッシュを使用します。
	Capability Code：128 Capability Value の AFI：1※	
グレースフル・リスタート	Capability Code：64 Capability Value の AFI：1 Capability Value の SAFI：1	グレースフル・リスタートを使用します。

注※　どちらか一方のネゴシエーションが成立していれば IPv4 経路のルート・リフレッシュを使用できます。

本装置の BGP4+でネゴシエーションできる機能を次の表に示します。なお，ピアから Capability 情報を持たない OPEN メッセージを受信した場合，確立した BGP4+コネクションは，「IPv6 ユニキャスト経路の送受信」だけをします。

表 22-4　ネゴシエーションできる機能（BGP4+）

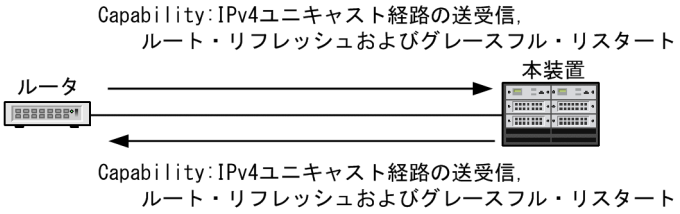
機能名称	OPEN メッセージの Capability 情報	内容
IPv6 ユニキャスト経路の送受信	Capability Code：1 Capability Value の AFI：2 Capability Value の SAFI：1	IPv6 ユニキャスト経路を該当するピア間で送受信します。
ルート・リフレッシュ	Capability Code：2 Capability Value の AFI：2※	IPv6 経路のルート・リフレッシュを使用します。
	Capability Code：128 Capability Value の AFI：2※	
グレースフル・リスタート	Capability Code：64 Capability Value の AFI：1 Capability Value の SAFI：2	グレースフル・リスタートを使用します。

注※　どちらか一方のネゴシエーションが成立していれば IPv6 経路のルート・リフレッシュを使用できます。

また，BGP4 を例としたネゴシエーションの動作を次の図に示します。

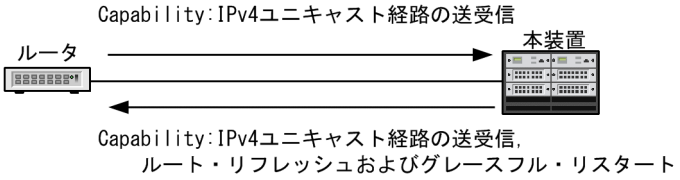
図 22-5　ネゴシエーションの動作

●互いに同一のCapability情報を広告した場合の例



注　ピア間でIPv4ユニキャスト経路の送受信，ルート・リフレッシュおよびグレースフル・リスタートが使用できる。

●互いに異なるCapability情報を広告した場合の例



注　ピア間でIPv4ユニキャスト経路の送受信機能だけが使用できる。

22.1.5　ルート・リフレッシュ

ルート・リフレッシュは，変化が発生した経路だけを広告することを基本とする BGP で，すでに広告された経路を強制的に再広告させる機能です。

ルート・リフレッシュには，自装置側から経路を再広告する機能と，ピアである相手装置側から経路を再広告させる機能があります。また，再広告の経路種別を選択できます。この機能は，BGP4 では clear ip bgp コマンドで，BGP4+では clear ipv6 bgp コマンドで実行されます。

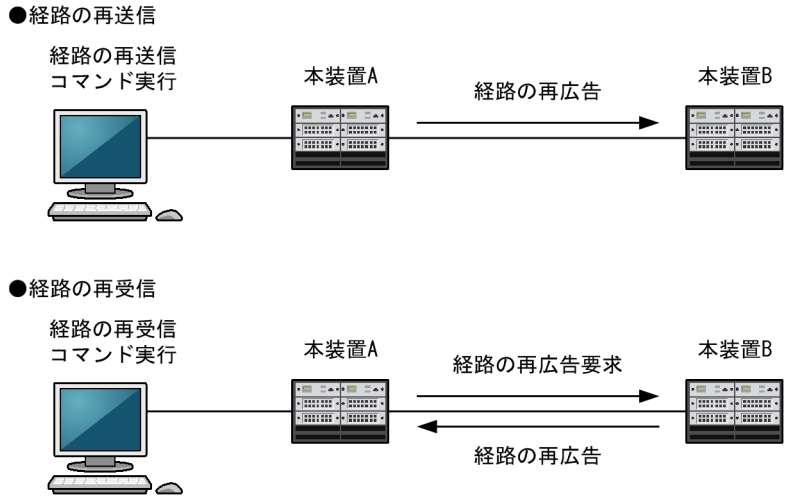
ルート・リフレッシュの機能を次の表に示します。

表 22-5　ルート・リフレッシュの機能

経路種別	機能種別	再広告方向
IPv4 ユニキャスト経路	IPv4 ユニキャスト経路の再送信	自装置側からピアリングされた相手装置に経路を再広告します。
	IPv4 ユニキャスト経路の再受信	ピアリングされた相手装置側から自装置に経路を再広告させます。
IPv6 ユニキャスト経路	IPv6 ユニキャスト経路の再送信	自装置側からピアリングされた相手装置に経路を再広告します。
	IPv6 ユニキャスト経路の再受信	ピアリングされた相手装置側から自装置に経路を再広告させます。

また，ルート・リフレッシュの動作を次の図に示します。

図 22–6　ルート・リフレッシュの動作



(1)　ルート・リフレッシュ使用時の注意事項

相手装置側から経路を再送信するには，ピアリングされた両ルータがルート・リフレッシュをサポートしている必要があります。ルート・リフレッシュを使用するためには，ピア確立時にルート・リフレッシュの使用を両ルータ間でネゴシエーションしておく必要があります。

また，コンフィグレーションコマンド neighbor soft-reconfiguration で inbound パラメータの指定がある場合，学習経路フィルタで抑止した経路を無効経路として保持しているため，相手装置側から自装置へ経路再広告のためのルート・リフレッシュ要求をしません。

本装置のルート・リフレッシュは RFC2918 に準拠しています。ネゴシエーションで使用するルート・リフレッシュ用の Capability Code は RFC2918 準拠のコード（値＝ 2）とプライベートなコード（値＝ 128）です。なお，ほかのベンダーによって RFC2434 で定義されているプライベートなコードである Capability Code（値＝ 128～255）を使用されることがあります。

本装置と他装置間でルート・リフレッシュを使用するときは注意してください。

22.1.6　TCP MD5 認証

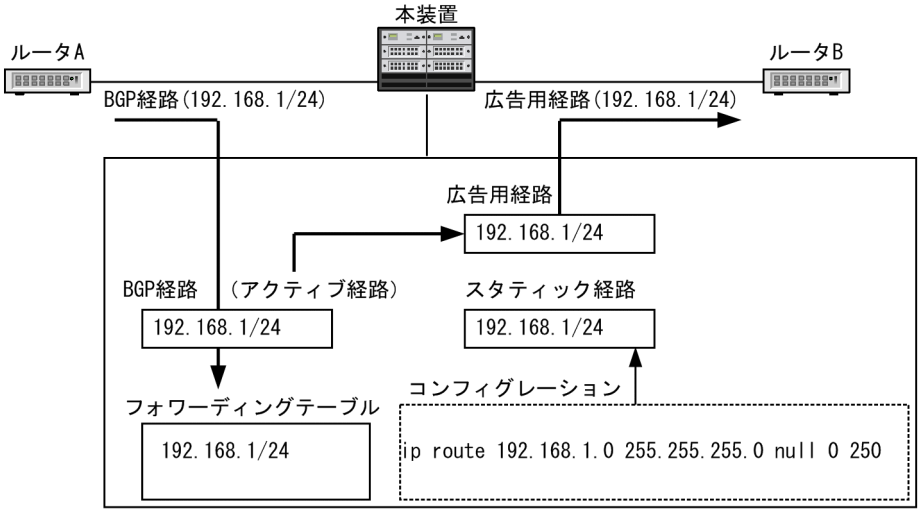
本装置の BGP4 および BGP4+は，RFC2385（TCP MD5 認証による BGP セッション保護）に準拠しています。TCP MD5 認証機能によって，BGP コネクションで受信した TCP セグメントが正当な送信元（ピア）から送信されてきたことを保証できます。TCP MD5 認証はピアごとに指定できます。ピアとの BGP コネクションに TCP MD5 認証を適用する場合，コンフィグレーションコマンド neighbor password で認証キーを指定します。なお，認証キーは該当するピア間で一致させる必要があります。一致していない場合は該当するピア間の BGP コネクションが確立しません。

22.1.7　広告用経路生成

広告用経路生成とは，BGP4 経路または BGP4+経路と同じ宛先の経路情報を自装置内のアクティブ経路から生成して，BGP4 または BGP4+で広告する機能です。パケットのフォワーディングには実際の BGP 経路を使用して，他装置への広告には生成した広告用経路を使用することによって，BGP 経路を宛先とするフォワーディングと安定した経路広告ができます。この機能の使用例を次に示します。

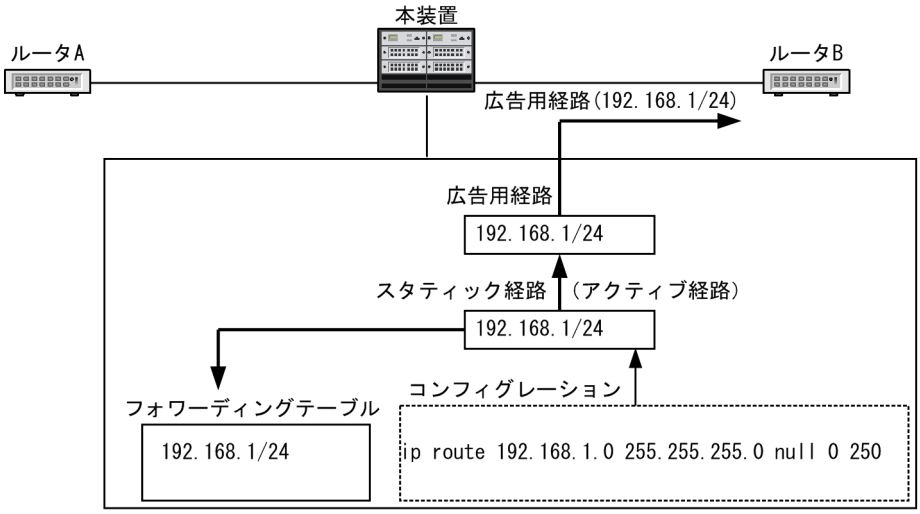
通常はルータ A から受信した BGP 経路をフォワーディングテーブルに設定して，該当経路から生成された広告用経路をルータ B に広告します。経路フィルタリングを設定していない場合，ルータ A から受信した BGP 経路と該当経路から生成された広告用経路のうち，ルータ A から受信した BGP 経路が広告の対象経路になります。そのため，ルータ A から受信した BGP 経路の広告を抑止して，広告用経路が広告されるように経路フィルタリングを設定してください。

図 22-7　広告用経路生成と広告（通常の場合）



ルータ A から学習していた BGP 経路が削除された場合は，スタティック経路がアクティブ経路となり，このスタティック経路から生成された広告用経路をルータ B に広告します。

図 22-8　広告用経路生成と広告（BGP 経路が削除された場合）



このように設定することで，通常のフォワーディングには BGP 経路が使用され，かつルータ A から受信する BGP 経路がフラップした場合でもルータ B への BGP 経路広告に影響しません。

なお，広告用経路の生成には次のどちらかのコンフィグレーションコマンドを使用します。

- network
- ip route の generate-bgp-route パラメータ

広告用経路は明示的に経路フィルタリングを設定しないかぎり，すべてのピアに広告します。BGP 経路から生成された同じ宛先の広告用経路を BGP 経路の学習元（ここではルータ A）に広告した場合，経路ループが発生するおそれがあるため，経路フィルタリングで広告を抑止してください。

22.1.8　ルート・フラップ・ダンプニング

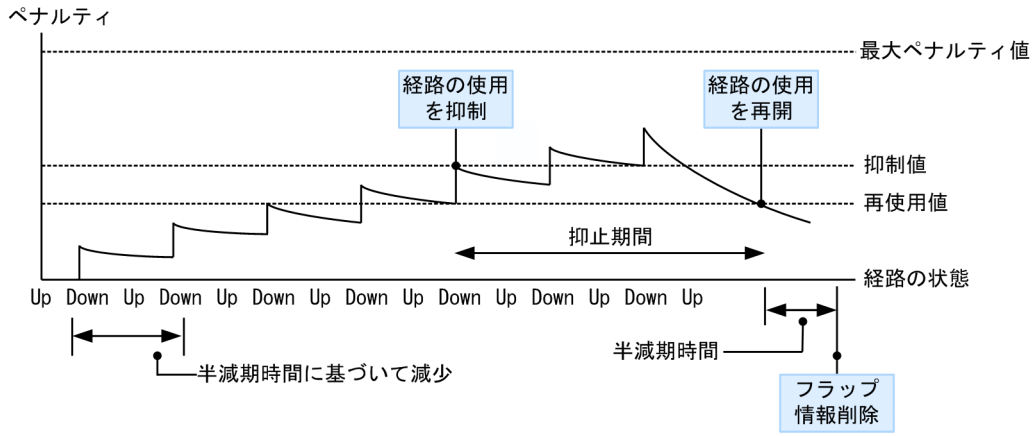
ルート・フラップ・ダンプニングは，経路情報が頻発してフラップするような場合に，一時的に該当する経路の使用を抑制してネットワークの不安定さを最小限にする機能で，BGP4 と BGP4+で同じ動作です。なお，VRF では本機能をサポートしていません。ルート・フラップ・ダンプニングの構成要素を次の表に示します。

表 22-6　ルート・フラップ・ダンプニングの構成要素

構成要素	内容
ペナルティ	該当する経路の使用を抑制または再利用するための動的制御変数。経路のフラップによって増加して，時間経過とともに減少します。ペナルティの増加はフラップ（到達不可への変化）当たり 1 固定で，ペナルティの減少は半減期時間に基づきます。ペナルティの最大値は次の計算式で決定します。 最大ペナルティ値＝再使用値×2^（最大抑止時間／半減期時間）
抑制値	ペナルティがこの値以上の場合，該当する経路の使用を抑制します。
再使用値	ペナルティがこの値以下の場合，該当する経路の使用を開始します。
半減期時間	ペナルティが半減（50%）するために必要な時間。
最大抑止時間	経路の使用を抑止する最大時間。この値は最大ペナルティの値に到達した場合に，再使用値に達するまでの経過時間です。

ルート・フラップ・ダンプニングの概念を次の図に示します。

図 22-9　ルート・フラップ・ダンプニングの概念



22.1.9　ルート・リフレクション

ルート・リフレクションは，AS 内でピアを形成する内部ピアの数を減らすための方法です。BGP4 および BGP4+は，内部ピアで配布された経路情報をそのほかの内部ピアに配布しません。このため，内部ピアは AS 内の各 BGP スピーカ間で論理的にフルメッシュに形成される必要があります。ルート・リフレクショ

ンはこの制限を緩和して，内部ピアで配布された経路情報をほかの内部ピアに再配布して，AS 内の内部ピアの数を減らします。

(1)　ルート・リフレクションの概念と経路情報の流れ

ルート・リフレクションは，ルート・リフレクタ（RR）とそのルート・リフレクタに対するクライアントでクラスタを形成します。クラスタ内に複数のルート・リフレクタを持つこともできます。AS 内のそのほかの BGP スピーカをノンクライアントと呼びます。

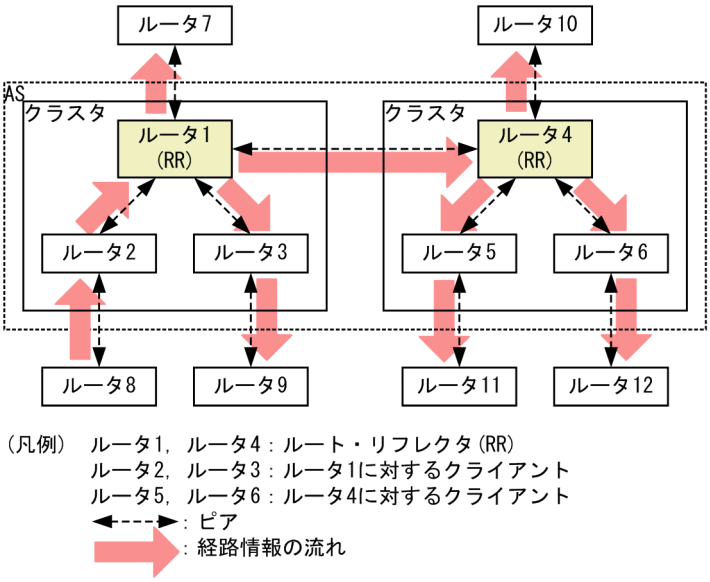
ルート･リフレクタはクラスタ内のクライアントから受信した UPDATE メッセージをすべてのノンクライアントおよび送信元のクライアントを含むクラスタ内のクライアントに配布します。また，ルート・リフレクタはノンクライアントから受信した UPDATE メッセージをクラスタ内のすべてのクライアントに配布します。これによって，クラスタ内のクライアントからノンクライアントに対する内部ピアと，クラスタ内のクライアント間の内部ピアを不要とします。

なお，外部ピアおよびメンバー AS 間ピアから配布された経路情報，ならびに外部ピアおよびメンバー AS 間ピアへ配布する経路情報の取り扱いは通常の動作と同じです。

(2)　クラスタ内に一つのルート・リフレクタを置く場合

クラスタ内に一つのルート・リフレクタを置く例を次の図に示します。

図 22-10　クラスタ内に一つのルート・リフレクタを置く例



ルータ 1（ルート・リフレクタ）とルータ 2，ルータ 3（クライアント）でクラスタを形成しています。また，ルータ 4（ルート・リフレクタ）とルータ 5，ルータ 6（クライアント）でクラスタを形成しています。ルータ 2 からルータ 1 に通知された経路情報は，クライアント（ルータ 2 とルータ 3）とすべてのノンクライアント（ルータ 4）に配布されます。また，ルータ 1 からルータ 4 に通知された経路情報は，すべてのクライアント（ルータ 5，ルータ 6）に配布されます。

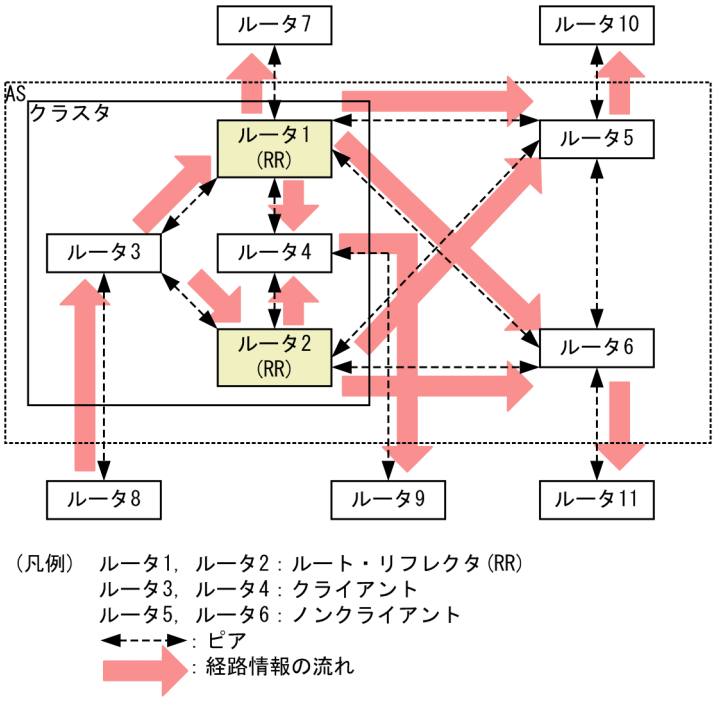
(3)　クラスタ内に複数のルート・リフレクタを置く場合

クラスタは，一つ以上のルート・リフレクタを持てます。複数のルート・リフレクタを持つことによって，一方のルート・リフレクタが障害となった場合にもルート・リフレクションの機能の停止を防げます。

それぞれのルート・リフレクタは，クライアントおよびノンクライアントと内部ピアを形成します。それぞれのルート・リフレクタは，「図 22-10　クラスタ内に一つのルート・リフレクタを置く例」で説明したとおり，クライアントまたはノンクライアントから通知された経路情報を再配布します。これによって，一方のルート・リフレクタが障害となった場合にも，他方のルート・リフレクタの再配布によって経路情報を通知できます。なお，クラスタ内に複数のルート・リフレクタがある場合，コンフィグレーションコマンド bgp cluster-id でそれぞれのルート・リフレクタに同一のクラスタ ID を設定する必要があります。

ルート・リフレクタの冗長構成の例を次の図に示します。

図 22-11　ルート・リフレクタの冗長構成の例



クラスタ内には二つのルート・リフレクタ（ルータ 1 とルータ 2）が存在しています。それぞれのルート・リフレクタはクライアントであるルータ 3，ルータ 4，およびノンクライアントであるルータ 5，ルータ 6 と内部ピアを形成します。例えば，クライアントであるルータ 3 から通知された経路情報は，それぞれのルート・リフレクタ（ルータ 1 およびルータ 2）でクライアントであるルータ 3，ルータ 4，およびノンクライアントであるルータ 5，ルータ 6 に再配布します。一方のルート・リフレクタが障害となった場合にも，他方のルート・リフレクタの再配布によって経路情報は通知されます。なお，AS 内にはクラスタに属さない BGP スピーカ（ルータ 5，ルータ 6）も共存できます。

22.1.10　コンフェデレーション

コンフェデレーションは，ルート・リフレクタと同様に AS 内でピアを形成する内部ピアの数を減らすためのもう一つの方法で，BGP4 と BGP4+で同じ動作です。コンフェデレーションは，AS を複数のメンバー AS に分割して，AS 内のピア数を減らします。

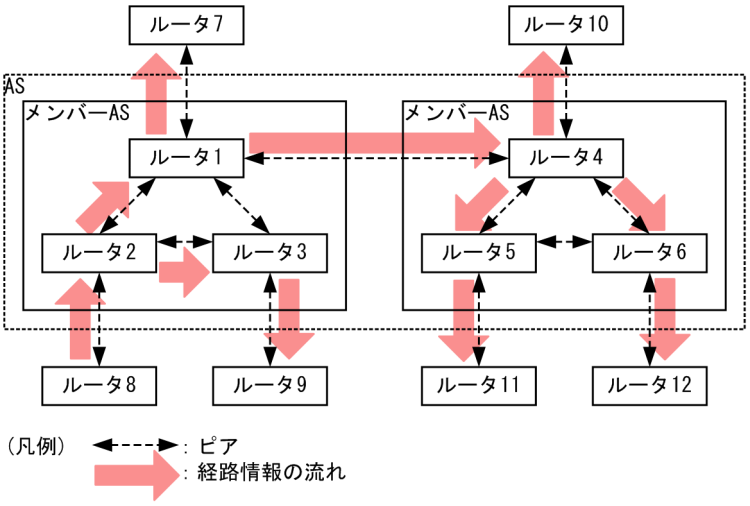
(1)　コンフェデレーションの概念と経路情報の流れ

コンフェデレーションは AS を複数のメンバー AS に分割します。メンバー AS 内の BGP スピーカはフルメッシュに内部ピアを形成する必要があり，通常の内部ピアの取り扱いと同様です。メンバー AS 間は通常の外部ピアと同様にピアを形成すればよく，メンバー AS 間の各 BGP スピーカでフルメッシュにピアを形

成する必要はありません。これによって AS 内のピア数を減らします。なお，本装置ではメンバー AS 間のピアをメンバー AS 間ピアと呼びます。

コンフェデレーション構成での経路情報の流れを次の図に示します。

図 22-12　コンフェデレーション構成での経路情報の流れ



ルータ 1，ルータ 2，およびルータ 3 でメンバー AS を形成しています。また，ルータ 4，ルータ 5，およびルータ 6 でメンバー AS を形成しています。ルータ 8 から通知された経路情報はルータ 2 によってメンバー AS 内のほかの BGP スピーカ（ルータ 1，ルータ 3）に配布されます。ルータ 2 からルータ 1 に通知された経路情報はほかのメンバー AS（ルータ 4）に配布されます。さらに，ルータ 1 からルータ 4 に通知された経路情報は，メンバー AS 内のほかの BGP スピーカ（ルータ 5，ルータ 6）に配布されます。これによって，AS 内のすべての BGP スピーカに経路情報を配布します。

(2)　コンフェデレーション構成での経路選択

コンフェデレーション構成での経路選択は，ピア種別（メンバー AS 間ピア）の追加によって通常構成（非コンフェデレーション構成）での経路選択と一部異なります。通常構成では「外部ピアで学習した経路，内部ピアで学習した経路の順」で選択しますが，コンフェデレーション構成では「外部ピアで学習した経路，メンバー AS 間ピアで学習した経路，内部ピアで学習した経路の順」で選択します。

コンフェデレーション構成での経路選択の条件を，優先順位が高い順に次に示します。

1. weight 値が最も大きい経路を選択します。
2. LOCAL_PREF 属性の値が最も大きい経路を選択します。
3. AS_PATH 属性の AS 数が最も短い経路を選択します。

   AS_PATH 属性上のパスタイプ AS_SET は，全体で一つの AS としてカウントします。AS_PATH 属性上のパスタイプ AS_CONFED_SEQUENCE および AS_CONFED_SET は，AS パス長に含まれません。
4. ORIGIN 属性の値で IGP，EGP，Incomplete の順で選択します。
5. MED 属性の値が最も小さい経路を選択します。

   MED 属性値による経路選択は，同一隣接 AS から学習した重複経路に対してだけ有効です。なお，コンフィグレーションコマンド bgp always-compare-med を設定すると，異なる隣接 AS から学習した重複経路に対しても有効となります。

6. 外部ピアで学習した経路，メンバー AS 間ピアで学習した経路，内部ピアで学習した経路の順で選択します。
7. ネクストホップが最も近い（ネクストホップ解決時に使用した IGP 経路のメトリック値が最も小さい）経路を選択します。
8. 相手 BGP 識別子（ルータ ID）が最も小さい経路を選択します。ただし，ORIGINATOR_ID 属性を持つ経路は，相手 BGP 識別子（ルータ ID）の代わりに ORIGINATOR_ID 属性の値を比較します。

   外部ピアから受信した経路間で相手 BGP 識別子（ルータ ID）の値が異なる場合は，相手 BGP 識別子（ルータ ID）および学習元ピアアドレスによる経路選択をしないで，すでに選択されている経路を採用します。なお，コンフィグレーションコマンド bgp bestpath compare-routerid を設定すると，外部ピアから受信した経路間で相手 BGP 識別子（ルータ ID）の値が異なる場合にも相手 BGP 識別子（ルータ ID）による経路選択ができます。
9. CLUSTER_LIST 属性長が最も短い経路を選択します。

   CLUSTER_LIST 属性を持たない経路は，CLUSTER_LIST 属性長を 0 として比較します。
10. 学習元ピアのアドレスが小さい経路を選択します。

    外部ピアから受信した経路間で相手 BGP 識別子（ルータ ID）の値が異なる場合は，相手 BGP 識別子（ルータ ID）および学習元ピアアドレスによる経路選択をしないで，すでに選択されている経路を採用します。なお，コンフィグレーションコマンド bgp bestpath compare-routerid を設定すると，外部ピアから受信した経路間で相手 BGP 識別子（ルータ ID）の値が異なる場合にも相手 BGP 識別子（ルータ ID）による経路選択ができます。

(3)　コンフェデレーション構成での BGP 属性の取り扱い

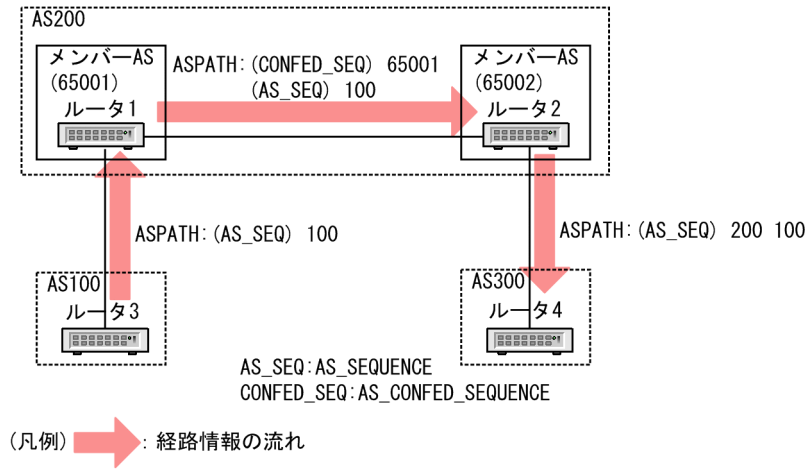
コンフェデレーション構成での BGP 属性の取り扱いは，通常構成（非コンフェデレーション構成）での BGP 属性の取り扱いとほぼ同様ですが，AS_PATH 属性，および COMMUNITIES 属性について一部動作が異なります。なお，メンバー AS 間ピアでの BGP 属性の取り扱いは，内部ピアでの BGP 属性の取り扱いと同様です。

(4)　コンフェデレーション構成での AS_PATH 属性の取り扱い

コンフェデレーション構成での AS_PATH 属性の取り扱いは，メンバー AS 間ピアに経路情報を通知するとき，AS_PATH 属性にパスタイプ AS_CONFED_SEQUENCE で自メンバー AS 番号を追加します。また，ほかの AS（外部ピア）に経路情報を通知するとき，AS_PATH 属性からパスタイプ AS_CONFED_SEQUENCE を取り除いて，パスタイプ AS_SEQUENCE で自 AS 番号を追加します。そのほかの AS_PATH 属性の取り扱いは，通常構成と同様です。

AS_PATH 属性の取り扱いを次の図に示します。

図 22-13　AS_PATH 属性の取り扱い



ルータ 1 は AS100 から通知された ASPATH:（AS_SEQUENCE）100 の経路情報をほかのメンバー AS であるルータ 2 に配布するとき，AS_PATH 属性にパスタイプ AS_CONFED_SEQUENCE で自メンバー AS 番号（65001）を追加します。ルータ 2 はルータ 1 から通知された ASPATH:（AS_CONFED_SEQUENCE）65001，（AS_SEQUENCE）100 の経路情報を AS300 に配布するとき，AS_PATH 属性のパスタイプ AS_CONFED_SEQUENCE を取り除いて，パスタイプ AS_SEQUENCE で自 AS 番号（200）を追加します。

(5)　コンフェデレーション構成での COMMUNITIES 属性の取り扱い

コンフェデレーション構成では RFC1997 で定義されるウェルノウン・コミュニティについて，次のように取り扱います。そのほかのコミュニティの取り扱いは，通常構成と同様です。

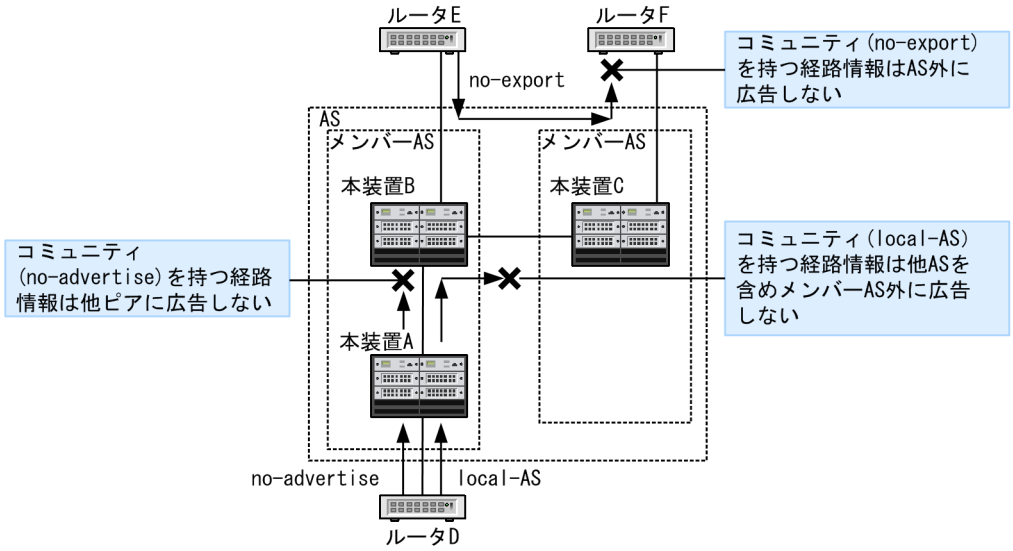
RFC1997 で定義されるウェルノウン・コミュニティを次の表に示します。

表 22-7　RFC1997 で定義されるウェルノウン・コミュニティ

コミュニティ	内容
no-export	この経路情報を AS 外に広告しません。
no-advertise	この経路情報をほかのピアに広告しません。
local-AS	この経路情報をメンバー AS 外に広告しません。

コンフェデレーション構成での，COMMUNITIES 属性を持つ経路情報の広告範囲を次の図に示します。

図 22-14　COMMUNITIES 属性を持つ経路情報の広告範囲



22.1.11　ノンストップルーティング

(1)　概要

ノンストップルーティングは，系切替によって運用系 BCU が交替したときに系切替前のルーティングプロトコルの状態を引き継いで，新運用系 BCU で継続して動作することでネットワーク全体での通信を維持するための機能です。

上記の実現のために，BGP4 および BGP4+ではあらかじめルーティングプロトコルの状態を他系 BCU 間で同期します。系切替時には，新運用系 BCU が KEEPALIVE メッセージや UPDATE メッセージの送受信を継続することで，系切替を BGP ピアから隠します。

ノンストップルーティングは装置単体で動作する機能のため，隣接ルータがノンストップルーティングをサポートしている必要はありません。

(2)　ノンストップルーティング使用時の注意事項

- ノンストップルーティングを使用する場合，コンフィグレーションコマンド neighbor soft-reconfiguration で inbound パラメータを設定して，学習経路フィルタで抑止した経路を無効経路として保持することを推奨します。この設定がないと，系切替後に運用コマンド clear ip bgp または clear ipv6 bgp による経路の再学習が必要になります。
- マネージメントポートに設定したアドレスを使用して確立した BGP4 ピアまたは BGP4+ピアにノンストップルーティングを設定すると，運用を継続できないことがあります。ノンストップルーティングを設定した場合は，該当ピアのノンストップルーティングの設定を削除することで復旧します。
- スパニングツリーを設定している VLAN インタフェースを使用して確立する BGP4 ピアまたは BGP4+ピアに，ノンストップルーティングを設定しないでください。系切替時に該当ピアを維持できないことや，運用コマンド redundancy force-switchover で系切替できないことがあります。

22.1.12　グレースフル・リスタート

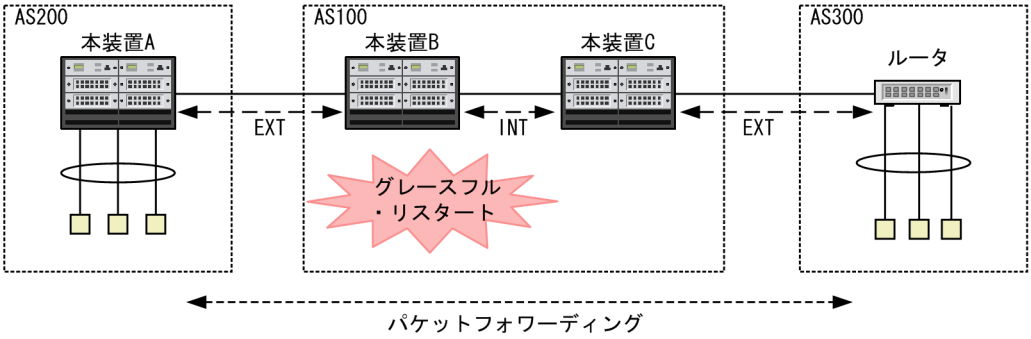
(1)　概要

グレースフル・リスタートは，系切替によって運用系 BCU が交替したり，運用コマンドなどによってルーティングプログラムが再起動したりしたときに，ネットワークから経路が消えることによる本装置を中継する通信の停止を防ぐための機能で，BGP4 と BGP4+で同じ動作です。

BGP では，グレースフル・リスタートによって BGP を再起動する装置のことをリスタートルータといいます。また，グレースフル・リスタートを補助する隣接装置をレシーブルータといいます。

本装置は，リスタートルータ機能とレシーブルータ機能をサポートしています。本装置でのグレースフル・リスタートの例を次の図に示します。

図 22-15　グレースフル・リスタートの例



（凡例）INT：内部ピア（ループバックインタフェースに設定したアドレスをピアアドレスに使用する）
EXT：外部ピア（直接接続されたインタフェースのアドレスをピアアドレスに使用する）

注　AS100 内では，IGP によってループバックインタフェースに設定したアドレス宛ての経路情報を交換します。

AS100 の本装置 B，本装置 C はループバックインタフェースに設定したアドレスをピアアドレスとする内部ピアの BGP コネクションを確立していて，本装置 B は AS200 の本装置 A と，また本装置 C は AS300 のルータとそれぞれインタフェースのアドレスをピアアドレスとする外部ピアの BGP コネクションを確立しているとします。それぞれの BGP コネクションでは，グレースフル・リスタートのネゴシエーションが成立しているとします。本装置 B がグレースフル・リスタートしたとき，該当する装置との BGP コネクションを持っている本装置 A および本装置 C はレシーブルータとして動作して，本装置 B を経由するパケットのフォワーディングを停止しないで継続します。これによって本装置 B を経由するエンド・エンドの通信を維持できます。

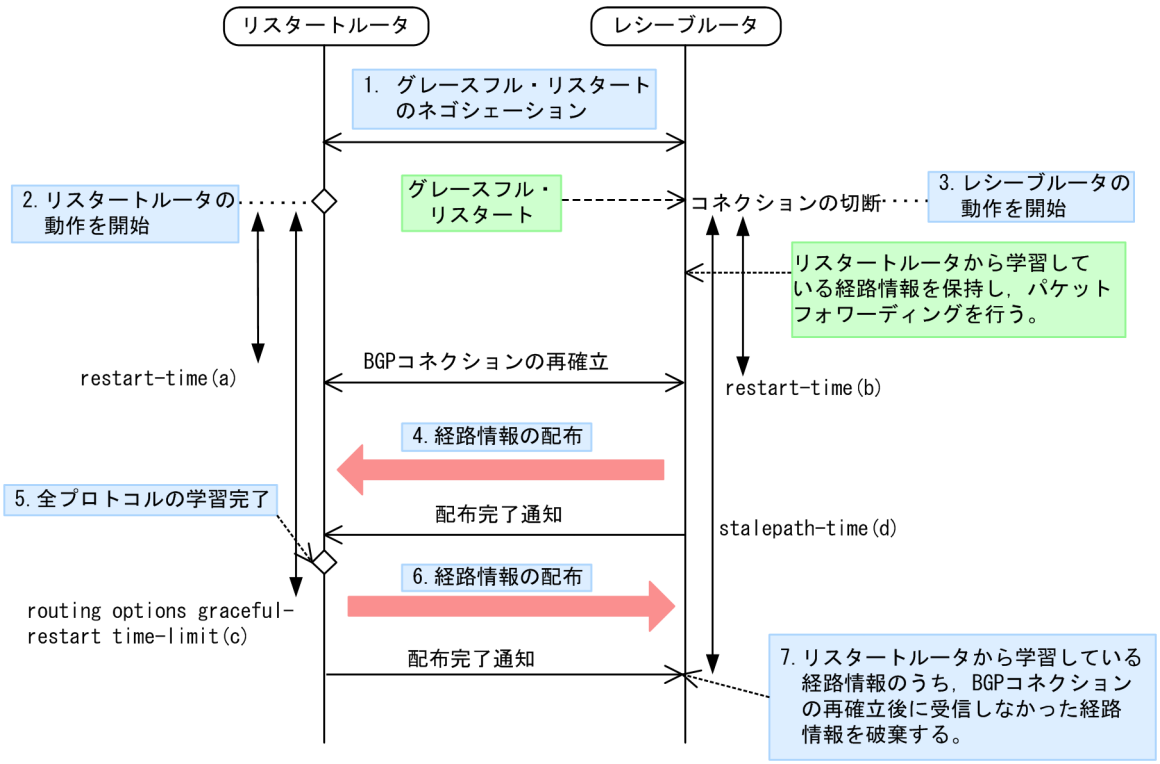
BGP のグレースフル・リスタートが正しく動作するための条件を次に示します。次の条件を満たさない場合，通常のリスタート動作となって通信が停止します。

- 本装置をリスタートルータとして動作させるときは，コンフィグレーションコマンド bgp graceful-restart mode の restart パラメータまたは both パラメータが設定されていること。
- 本装置をレシーブルータとして動作させるときは，コンフィグレーションコマンド bgp graceful-restart mode の receive パラメータまたは both パラメータが設定されていること。
- グレースフル・リスタートを実施する装置と，レシーブルータの役割を実行する装置との BGP コネクションで，グレースフル・リスタートのネゴシエーションが成立していること。

(2)　グレースフル・リスタートの動作手順

BGP によるグレースフル・リスタートの動作シーケンスを次の図に示します。

図 22-16　グレースフル・リスタートのシーケンス



1. グレースフル・リスタートするルータとその隣接ルータの間で，BGP コネクションを確立するときにグレースフル・リスタートのネゴシエーションをして，グレースフル・リスタートを実施する準備をします。
2. ルータがグレースフル・リスタートを実施すると，リスタートルータの動作を開始します。
3. 隣接ルータは，BGP のコネクションが切断したとき，レシーブルータの動作を開始して，リスタートルータから学習している経路情報を保持してパケットのフォワーディングを継続します。
4. BGP コネクションが再確立すると，最初にレシーブルータからリスタートルータへ経路情報を配布します。
5. リスタートルータで，グレースフル・リスタートを実行しているすべてのプロトコルの学習が完了すると，リスタートルータからレシーブルータへ経路情報を配布します。
6. 5.と同じ。
7. 最後にレシーブルータは，リスタートルータから学習している経路情報のうちで，BGP コネクションの再確立後に受信しなかった，古い経路情報を破棄します。

(3)　リスタートルータの機能

(a)　動作契機

本装置で BGP のリスタートルータの機能が動作する契機を次に示します。

- 系切替によって運用系 BCU が交替したとき

- ユニキャストルーティングプログラムが再起動したとき

(b)　リスタートルータの機能

グレースフル・リスタートの開始後に，BGP コネクションが再確立するまでの待ち時間の上限を，コンフィグレーションコマンド bgp graceful-restart restart-time の指定に従って監視します（「図 22–16　グレースフル・リスタートのシーケンス」の（a））。この時間内に BGP コネクションが再確立しない場合，リスタートルータは該当するレシーブルータからの経路情報配布を待たないで，自ルータからの経路情報配布を開始します。これによって，不安定な状態とみられる該当レシーブルータが経路収束へ影響することを回避します。

リスタートルータが経路情報の受信完了を待ち，経路配布を開始する時間の上限は，コンフィグレーションコマンド routing options graceful-restart time-limit の指定値に従います（「図 22–16　グレースフル・リスタートのシーケンス」の（c））。

各パラメータを設定する場合は，一般に次のようにしてください。

- ループバックインタフェースに設定したアドレスをピアアドレスとする内部ピアを使用している場合，コンフィグレーションコマンド bgp graceful-restart restart-time を，OSPF または OSPFv3 のリスタート時間＋コネクション確立時間よりも長く設定する。

  ピアアドレスを IGP 経路によって解決する構成では，BGP ピアのコネクションを再確立するために IGP 経路が必要になります。このため，コンフィグレーションコマンド bgp graceful-restart restart-time を，IGP のリスタート時間＋コネクション確立時間よりも長く設定してください。
- コンフィグレーションコマンド routing options graceful-restart time-limit はコンフィグレーションコマンド bgp graceful-restart restart-time より大きい値を設定する。

また，BGP 経路情報の NEXT_HOP 属性を IGP 経路によって解決する構成では，次のように設定してください。

- IGP の restart-time は bgp の restart-time より小さい値を設定

(c)　グレースフル・リスタートが失敗するケース

BGP のグレースフル・リスタートが失敗するケースを次に示します。

- グレースフル・リスタートを開始してから，restart-time の時間が経過しても隣接装置との間で BGP コネクションが再確立しなかった場合，該当するピア装置を経由する通信が停止します。
- 本装置のグレースフル・リスタート中に，レシーブルータ機能を実行するピア装置がリスタートした場合，該当するピア装置を経由する通信が停止します。
- レシーブルータ機能を実行するピア装置が，グレースフル・リスタートの開始前に，本装置から学習した経路情報を保持できなかった場合，該当するピア装置を経由する通信が停止します。
- グレースフル・リスタートの開始後に，すべてのレシーブルータへの経路情報の配布が完了する前に BGP コネクションが再び切断した場合，該当するピア装置を経由する通信が停止します。
- グレースフル・リスタートの開始後に，リスタートルータから学習した経路数が学習経路数制限機能による上限値を超え，BGP コネクションが再切断した場合，リスタートルータを経由する通信が停止します。

(4)　レシーブルータの機能

(a)　動作契機

本装置で BGP のレシーブルータの機能が動作する契機を次に示します。

- BGP コネクションが確立しているピアから，NOTIFICATION メッセージを受信しないで，該当するコネクションが使用している TCP セッションの切断を検出したとき
- BGP コネクションが確立しているピアから，新規の TCP セッションが接続され，OPEN メッセージを受信したとき

(b)　レシーブルータの機能

グレースフル・リスタートの開始後に，BGP コネクションが再確立するまでの待ち時間の上限を，コンフィグレーションコマンド bgp graceful-restart restart-time の指定に従って監視します（「図 22-16　グレースフル・リスタートのシーケンス」の (b)）。この時間内に BGP コネクションが再確立しない場合，レシーブルータは，リスタートルータから学習している経路情報を破棄して，リスタートルータを経由するパケットのフォワーディングを停止します。

restart-time の値は，グレースフル・リスタートのネゴシエーションをするときに，ピアへ通知されます。本装置では，ピアから通知された restart-time の値が，自装置の設定値より小さいとき，通知された restart-time の値を使用して監視します。

レシーブルータがリスタートルータの再起動前に学習した経路情報を保持しておく時間の上限はコンフィグレーションコマンド bgp graceful-restart stalepath-time で指定します（「図 22-16　グレースフル・リスタートのシーケンス」の（d））。

(c)　レシーブルータ機能が失敗するケース

BGP のグレースフル・リスタートが失敗するケースを次に示します。

- グレースフル・リスタートを開始してから，restart-time の時間が経過しても BGP コネクションが再確立しなかった場合，リスタートルータを経由する通信が停止します。
- レシーブルータ機能を実行中に自装置がリスタートした場合，リスタートルータを経由する通信が停止します。
- グレースフル・リスタートしているピア装置が，グレースフル・リスタートの開始前に学習していた経路情報を保持できなかった場合，リスタートルータを経由する通信が停止します。
- グレースフル・リスタートの開始後に再確立した BGP コネクション上で，リスタートルータからの経路情報の配布が完了する前に再び切断した場合，リスタートルータを経由する通信が停止します。
- グレースフル・リスタートの開始後に，リスタートルータから学習した経路数が学習経路数制限による上限値を超え，BGP コネクションが再切断した場合，リスタートルータを経由する通信が停止します。

(5)　グレースフル・リスタート使用時の注意事項

- TCP MD5 の併用について

  グレースフル・リスタートをサポートする BGP コネクションが確立している場合，ピアから新しいコネクションの要求を受けたとき，プロトコルの規定によって，確立中の BGP コネクションを破棄して新しい BGP コネクションを使用します。この動作によるセキュリティ上の問題を防ぐために，TCP MD5 認証を併用してください。
- IGP へ依存する環境でのグレースフル・リスタートについて

  直接接続されていない内部ピア接続でピアアドレス宛ての経路情報を IGP によって交換している場合や，ルート・リフレクションを使用する構成などで，BGP 経路情報の NEXT_HOP 属性を IGP 経路によって解決する場合は，該当する IGP についてもグレースフル・リスタートを設定してください。

22.1.13　学習経路数制限

学習経路数制限とは，ピアから学習する BGP4 経路および BGP4+経路の数を制限して，大量の経路学習による本装置のメモリ不足や，特定ピアからの大量経路学習によってほかのピアから経路を学習できなくなることを回避するための機能です。

この機能を適用すると，ピアから学習した BGP 経路の数が設定した閾値を超えた場合，警告のシステムメッセージを出力します。さらに，上限値を超えた場合は，警告のシステムメッセージを出力したあとでピアを切断します。この機能によるピア切断後は，設定した期間が経過するか，BGP4 は運用コマンド clear ip bgp，BGP4+は運用コマンド clear ipv6 bgp を実行すると，ピアを再接続します。また，学習経路数が上限値を超えても，警告のシステムメッセージを出力するだけでピアを切断しない設定もできます。

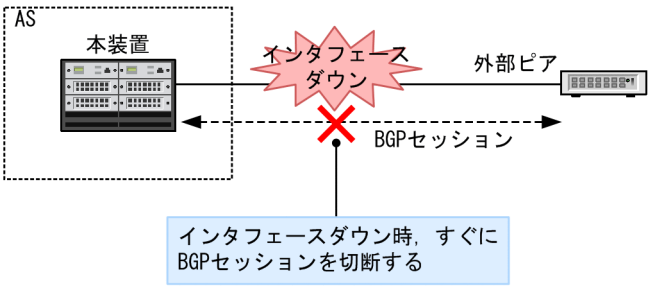
22.1.14　インタフェースダウン時の外部ピア即時切断機能

インタフェースダウン時の外部ピア即時切断機能は，直接接続された外部ピアとのインタフェースがダウンすると，すぐに該当ピアとの BGP セッションを切断する機能です。

この機能は，BGP4 および BGP4+についてデフォルトで有効です。直接接続された外部ピアとのインタフェースがダウンしてもすぐに該当ピアとの BGP セッションを切断しない場合は，コンフィグレーションコマンド no bgp fast-external-fallover を設定してください。ただし，インタフェースダウンによってホールドタイムアウトが発生した場合は，bgp fast-external-fallover の設定に関係なく，BGP セッションを切断します。

インタフェースダウン時の外部ピア即時切断機能適用時の動作を次の図に示します。

図 22-17　インタフェースダウン時の外部ピア即時切断機能適用時の動作



インタフェースダウン時の BGP セッションの扱いを次の表に示します。

表 22-8　インタフェースダウン時の BGP セッションの扱い

ピア接続種別		no bgp fast-external-fallover 指定	
		なし	あり
外部ピア	直接接続である	すぐに BGP セッションを切断する	確立状態を保持する
	直接接続ではない	確立状態を保持する	確立状態を保持する
内部ピア		確立状態を保持する	確立状態を保持する

22.1.15　4 バイト AS 番号

(1)　概要

本装置ではコンフィグレーションで，自 AS 番号および接続先のピアの AS 番号に 4 バイト AS 番号を指定できます。4 バイト AS 番号は 4 バイトの 10 進数（整数）で表記し，65536～4294967295 の範囲で指定します。なお，4 バイト AS 番号は 2 バイト AS 番号で指定できる範囲を含むため，設定できる AS 番号の範囲は 1～4294967295 となります。

接続先のピアが 4 バイト AS 番号をサポートしているかどうかは，コンフィグレーションコマンド capability 4-byte-as を設定したピアとの接続時の機能ネゴシエーションで確認します。ネゴシエーションで互いに 4 バイト AS 番号をサポートしていることが確認できたとき，該当ピアが 4 バイト AS 番号をサポートしていると見なします。外部ピアで，本装置の AS 番号が 4 バイト AS 番号でかつ接続先のピアが 4 バイト AS 番号をサポートしていない場合は，自 AS 番号に AS_TRANS（23456）を使用します。4 バイト AS 番号を使用したピア接続を次の図に示します。

図 22-18　4 バイト AS 番号を使用したピア接続

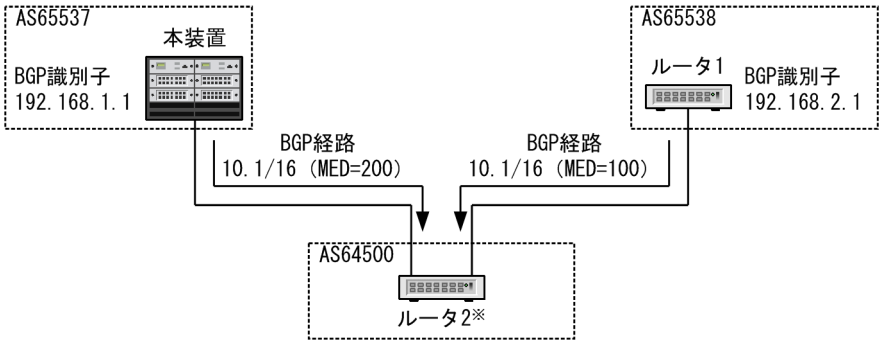


(2)　4 バイト AS 番号使用時の注意事項

(a)　MED 属性による経路選択

4 バイト AS 番号をサポートしていないピアと接続する場合，自 AS 番号に AS_TRANS（23456）を使用するため，接続先のピアで MED 属性による経路選択ができないおそれがあります。4 バイト AS 番号をサポートしていないピアでの経路選択例を次の図に示します。

図 22-19　4 バイト AS 番号をサポートしていないピアでの経路選択例



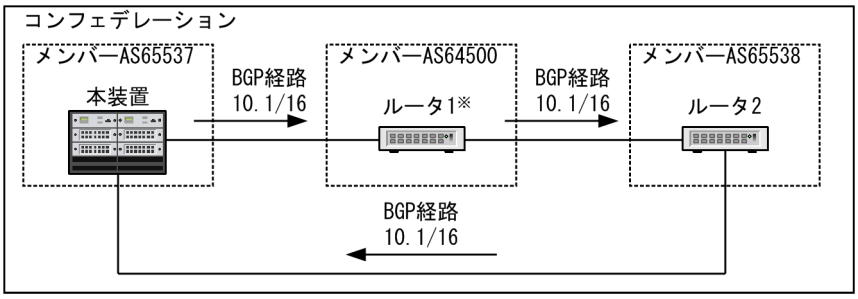
注※　4 バイト AS 番号未サポート

この例では，AS65537 の本装置と AS65538 のルータ 1 から，MED 属性を付けた同一宛先の経路を AS64500 のルータ 2 へ広告しています。ルータ 2 では 4 バイト AS 番号をサポートしていないため，本装置とルータ 1 が同一 AS（AS_TRANS）であると判断して，MED 属性値によって経路を選択することがあります。その結果，本来 BGP 識別子の小さい本装置から学習した経路を選択するはずが，MED 属性値の小さいルータ 1 から学習した経路を選択してしまうおそれがあります。

(b)　コンフェデレーション構成

コンフェデレーション構成で接続先のピアが 4 バイト AS 番号をサポートしていない場合，接続先のピアへ広告する経路の AS パス情報に 4 バイト AS 番号のメンバー AS 番号を付けないため，AS ループを検出できないおそれがあります。このため，4 バイト AS 番号をサポートしていないピアとコンフェデレーションを構成しないでください。AS ループを検出できないコンフェデレーション構成例を次の図に示します。

図 22-20　AS ループを検出できないコンフェデレーション構成例



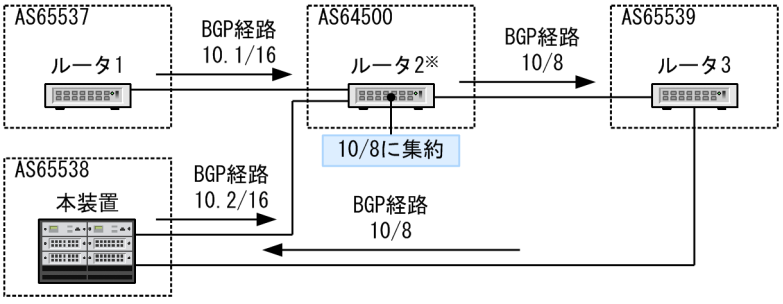
注※　4 バイト AS 番号未サポート

この例では，メンバー AS65537 の本装置からメンバー AS64500 のルータ 1 を経由してメンバー AS65538 のルータ 2 へ BGP 経路を広告して，さらにルータ 2 から本装置へ BGP 経路を広告する，AS ループ構成になっています。ルータ 1 が 4 バイト AS 番号をサポートしていないため，本装置はルータ 1 に広告する経路の AS パス情報に 4 バイト AS 番号のメンバー AS 番号を付けません。したがって，本装置はルータ 2 から経路を学習しても，AS ループを検出できません。

(c)　経路集約

4 バイト AS 番号をサポートしているルータが広告した経路を，4 バイト AS 番号をサポートしていないルータで経路集約した場合，4 バイト AS 番号が消えるため，AS ループを検出できないおそれがあります。経路集約による 4 バイト AS 番号消失の構成例を次の図に示します。

図 22-21　経路集約による 4 バイト AS 番号消失の構成例



注※　4 バイト AS 番号未サポート

この例では，AS65537 のルータ 1 と AS65538 の本装置から，同一宛先の BGP 経路を AS64500 のルータ 2 へ広告しています。それらの経路をルータ 2 で集約したあと，該当する集約経路を AS65539 のルータ 3 経由で本装置が学習する，AS ループ構成になっています。ルータ 2 が 4 バイト AS 番号をサポートしていないため，集約経路の AS パス情報に 4 バイト AS 番号を付けません。したがって，本装置では AS ループを検出できません。

(d) MIB での AS 情報の扱い

BGP 情報の MIB に含まれる AS 情報には，4 バイト AS 番号ではなく，AS_TRANS（23456）が設定されます。

(e) プライベート AS 番号の削除

4 バイト AS 番号をサポートしていないルータでは，ピアへ広告する際にプライベート AS 番号を取り除く設定をしていても，AS4_PATH 属性に存在する 4 バイト AS 番号空間のプライベート AS 番号を削除しません。

(f) 拡張コミュニティの扱い

本装置は，RFC5668 で規定されている拡張 COMMUNITIES 属性を，認識できない属性として取り扱います。そのため，拡張 COMMUNITIES 属性を持つ経路を受信してピアに広告する場合，拡張 COMMUNITIES 属性を付けたまま広告します。

22.2　BGP4 拡張機能のコンフィグレーション

22.2.1　BGP4 ピアグループの設定

(1)　コンフィグレーションコマンド一覧

BGP4 ピアグループのコンフィグレーションコマンド一覧を次の表に示します。

表 22-9　コンフィグレーションコマンド一覧

コマンド名	説明
neighbor peer-group (assigning members)	ピアをピアグループに所属させます。
neighbor peer-group (creating)	ピアグループを設定します。

(2)　BGP4 ピアグループの設定

[設定のポイント]

ピアグループは neighbor peer-group（creating）コマンドで設定します。ピアグループに設定したピアの AS 番号やオプション，広告経路フィルタなどはピアグループに所属するすべてのピアに適用されます。

[コマンドによる設定]

1. **(config)# router bgp 65531**
   (config-router)# bgp router-id 172.16.2.100
   (config-router)# neighbor INTERNAL-GROUP peer-group
   neighbor peer-group（creating）コマンドでピアグループ（グループ識別子：INTERNAL-GROUP）を設定します。
2. **(config-router)# neighbor INTERNAL-GROUP remote-as 65531**
   (config-router)# neighbor INTERNAL-GROUP soft-reconfiguration inbound
   (config-router)# neighbor INTERNAL-GROUP timers 30 90
   ピアグループ（グループ識別子：INTERNAL-GROUP）にピアの AS 番号（AS：65531）および各種オプションを設定します。
3. **(config-router)# neighbor EXTERNAL-GROUP peer-group**
   (config-router)# neighbor EXTERNAL-GROUP send-community
   (config-router)# neighbor EXTERNAL-GROUP maximum-prefix 10000
   (config-router)# exit
   neighbor peer-group（creating）コマンドでピアグループ（グループ識別子：EXTERNAL-GROUP）を設定します。また，各種オプションを設定します。
4. **(config)# route-map SET_COM permit 10**
   (config-route-map)# set community 1000:1001
   (config-route-map)# exit
   コミュニティ値 1000:1001 を指定した route-map を設定します。
5. **(config)# router bgp 65531**
   (config-router)# neighbor EXTERNAL-GROUP route-map SET_COM out

ピアグループ（グループ識別子：EXTERNAL-GROUP）に広告経路フィルタを設定します。

(3)　BGP4 ピアをピアグループに所属させる設定

[設定のポイント]

ピアをピアグループに所属させる場合は neighbor peer-group（assigning members）コマンドを設定します。

[コマンドによる設定]

1. **(config-router)# neighbor 172.16.2.2 peer-group INTERNAL-GROUP**

   neighbor peer-group（assigning members）コマンドでピア（相手側アドレス：172.16.2.2）をピアグループ（グループ識別子：INTERNAL-GROUP）に所属させます。ピアの AS 番号はピアグループに指定した 65531 を使用します。

2. **(config-router)# neighbor 172.17.3.3 peer-group INTERNAL-GROUP**

   neighbor peer-group（assigning members）コマンドでピア（相手側アドレス：172.17.3.3）をピアグループ（グループ識別子：INTERNAL-GROUP）に所属させます。ピアの AS 番号はピアグループに指定した 65531 を使用します。

3. **(config-router)# neighbor 192.168.4.4 remote-as 65533**

   (config-router)# neighbor 192.168.4.4 peer-group EXTERNAL-GROUP

   ピア（相手側アドレス：192.168.4.4）を設定して，ピアグループ（グループ識別子：EXTERNAL-GROUP）に所属させます。ピアの AS 番号はピアに指定した 65533 を使用します。

4. **(config-router)# neighbor 192.168.5.5 remote-as 65534**

   (config-router)# neighbor 192.168.5.5 peer-group EXTERNAL-GROUP

   ピア（相手側アドレス：192.168.5.5）を設定して，ピアグループ（グループ識別子：EXTERNAL-GROUP）に所属させます。ピアの AS 番号はピアに指定した 65534 を使用します。

22.2.2　コミュニティの設定

(1)　コンフィグレーションコマンド一覧

コミュニティのコンフィグレーションコマンド一覧を次の表に示します。

表 22-10　コンフィグレーションコマンド一覧

コマンド名	説明
neighbor send-community	ピアへ広告する経路の COMMUNITIES 属性を削除しないことを設定します。
distribute-list in (BGP4)※	BGP4 の学習経路フィルタリングの条件として使用する経路フィルタを指定します。
distribute-list out (BGP4)※	BGP4 の広告経路フィルタリングの条件として使用する経路フィルタを指定します。
neighbor in (BGP4)※	route-map パラメータで，BGP4 の特定のピアにだけ，学習経路フィルタリングの条件として使用する経路フィルタを指定します。
neighbor out (BGP4)※	route-map パラメータで，BGP4 の特定のピアにだけ，広告経路フィルタリングの条件として使用する経路フィルタを指定します。
redistribute (BGP4)※	BGP4 で広告する経路のプロトコルを指定します。

注※
「コンフィグレーションコマンドレファレンス Vol.3　22. 経路フィルタリング」を参照してください。

(2)　コミュニティの設定

[設定のポイント]

広告する BGP4 経路に COMMUNITIES 属性を付ける場合，該当するピアに neighbor send-community コマンドを設定してください。

[コマンドによる設定]

1. **(config)# router bgp 65531**
   (config-router)# bgp router-id 192.168.1.100
   (config-router)# neighbor 192.168.2.2 remote-as 65531
   (config-router)# neighbor 172.16.2.2 remote-as 65532
   (config-router)# neighbor 10.2.2.2 remote-as 65533
   BGP4 ピアを設定します。
2. **(config-router)# neighbor 172.16.2.2 send-community**
   (config-router)# neighbor 10.2.2.2 send-community
   (config-router)# exit
   ピアに広告する BGP4 経路に COMMUNITIES 属性を付けることを指定します。
3. **(config)# ip community-list 10 permit 1000:1002**
   (config)# ip community-list 20 permit 1000:1003
   (config)# route-map SET_LOCPREF permit 10
   (config-route-map)# match community 10
   (config-route-map)# set local-preference 120
   (config-route-map)# exit
   (config)# route-map SET_LOCPREF permit 20
   (config-route-map)# match community 20
   (config-route-map)# set local-preference 80
   (config-route-map)# exit
   (config)# route-map SET_LOCPREF permit 30
   (config-route-map)# exit
   コミュニティ値 1000:1002 を含む COMMUNITIES 属性を持つ経路の LOCAL_PREF 属性値に 120 を設定して，コミュニティ値 1000:1003 を含む COMMUNITIES 属性を持つ経路の LOCAL_PREF 属性値に 80 を設定します。
4. **(config)# ip prefix-list MY_NET seq 10 permit 192.168.0.0/16 ge 16 le 30**
   (config)# route-map SET_COM permit 10
   (config-route-map)# match ip address prefix-list MY_NET
   (config-route-map)# set community 1000:1001
   (config-route-map)# exit
   宛先ネットワークが 192.168.0.0/16（マスク長が 16～30）の経路にコミュニティ値 1000:1001 が設定された COMMUNITIES 属性を設定します。
5. **(config)# router bgp 65531**
   (config-router)# distribute-list route-map SET_LOCPREF in

```
(config-router)# distribute-list route-map SET_COM out
(config-router)# exit
```

全ピアに学習用経路フィルタと広告用経路フィルタを適用します。

(3)　経路フィルタリングの運用への反映

[設定のポイント]

運用コマンド clear ip bgp を使用して，学習経路フィルタリングの条件および広告フィルタリングの条件として設定した経路フィルタを運用に反映します。

[コマンドによる設定]

1.
```
# clear ip bgp * both
```

コミュニティを使用した経路フィルタを運用に反映します。

22.2.3　BGP4 マルチパスの設定

(1)　コンフィグレーションコマンド一覧

BGP4 マルチパスのコンフィグレーションコマンド一覧を次の表に示します。

表 22-11　コンフィグレーションコマンド一覧

コマンド名	説明
bgp always-compare-med	異なる AS から学習した MED 属性を比較することを設定します（本コマンドが未設定の場合，maximum-paths コマンドの all-as パラメータを設定できません）。
maximum-paths	マルチパスを設定します。

(2)　BGP4 マルチパスの設定

[設定のポイント]

maximum-paths コマンドで all-as パラメータを指定する場合は，あらかじめ bgp always-compare-med コマンドを設定しておいてください。

[コマンドによる設定]

1.
```
(config)# router bgp 65531
(config-router)# bgp router-id 192.168.1.100
(config-router)# neighbor 172.16.2.2 remote-as 65532
(config-router)# neighbor 172.17.2.2 remote-as 65533
```

マルチパスを形成するピアを設定します。この例では，AS65532 と AS65533 から学習した経路間でマルチパスを形成します。

2.
```
(config-router)# bgp always-compare-med
(config-router)# maximum-paths 4 all-as
(config-router)# exit
```

異なる AS から学習した経路を含めて最大 4 パスのマルチパスを形成することを指定します。

22.2.4　TCP MD5 認証の設定

(1)　コンフィグレーションコマンド一覧

TCP MD5 認証のコンフィグレーションコマンド一覧を次の表に示します。

表 22-12　コンフィグレーションコマンド一覧

コマンド名	説明
neighbor password	ピアとの接続に TCP MD5 認証を適用することを設定します。

(2)　TCP MD5 認証の設定

[設定のポイント]

TCP MD5 認証は neighbor password コマンドを使用して認証キーを設定します。

[コマンドによる設定]

1. **(config)# router bgp 65531**
   (config-router)# bgp router-id 192.168.1.100
   (config-router)# neighbor 172.16.2.2 remote-as 65532
   (config-router)# neighbor 192.168.2.2 remote-as 65531
   BGP4 ピアを設定します。
2. **(config-router)# neighbor 172.16.2.2 password "authmd5_65532"**
   (config-router)# exit
   相手側アドレスが 172.16.2.2 のピアに，認証キーが"authmd5_65532"の TCP MD5 認証を設定します。

22.2.5　BGP4 広告用経路生成の設定

(1)　コンフィグレーションコマンド一覧

BGP4 広告用経路生成のコンフィグレーションコマンド一覧を次の表に示します。

表 22-13　コンフィグレーションコマンド一覧

コマンド名	説明
network	BGP4 広告用経路を生成することを設定します。
ip route※	generate-bgp-route パラメータで，BGP4 広告用経路を生成することを設定します。

注※

「コンフィグレーションコマンドレファレンス Vol.3　15. スタティックルーティング（IPv4)」を参照してください。

(2)　network コマンドを使用した BGP4 広告用経路生成の設定

[設定のポイント]

BGP4 広告用経路を経路フィルタリングする場合は，route-map の match route-type コマンドで local パラメータを指定します。

[コマンドによる設定]

1. **(config)# router bgp 65531**
   (config-router)# bgp router-id 192.168.2.100
   (config-router)# neighbor 172.16.2.2 remote-as 65532
   (config-router)# neighbor 192.168.2.2 remote-as 65531
   (config-router)# exit
   BGP4 ピアを設定します。
2. **(config)# route-map ADV_NET permit 10**
   (config-route-map)# match route-type local
   (config-route-map)# exit
   BGP4 広告用経路を許可することを指定します。
3. **(config)# route-map ADV_NET deny 20**
   (config-route-map)# match protocol bgp
   (config-route-map)# exit
   BGP プロトコルを拒否することを指定します。
4. **(config)# router bgp 65531**
   (config-router)# neighbor 172.16.2.2 route-map ADV_NET out
   (config-router)# exit
   相手側アドレスが 172.16.2.2 のピアへ BGP4 広告用経路だけを広告すること（学習した BGP4 経路は広告しないこと）を指定します。
5. **(config)# route-map DENY_NET deny 10**
   (config-route-map)# match route-type local
   (config-route-map)# exit
   BGP4 広告用経路を拒否することを指定します。
6. **(config)# router bgp 65531**
   (config-router)# neighbor 192.168.2.2 route-map DENY_NET out
   (config-router)# exit
   相手側アドレスが 192.168.2.2 のピアへ BGP4 広告用経路を広告しないことを指定します。
7. **(config)# ip route 192.168.1.0 255.255.255.0 null 0 250**
   Null インタフェースをネクストホップとするスタティック経路を生成します。
8. **(config)# router bgp 65531**
   (config-router)# network 192.168.1.0/24
   (config-router)# exit
   BGP4 広告用経路のネットワークアドレスを指定すると，BGP4 広告用経路を生成します。

(3) ip route コマンドを使用した BGP4 広告用経路生成の設定

[設定のポイント]

BGP4 広告用経路を経路フィルタリングする場合は，route-map の match route-type コマンドで local パラメータを指定します。

[コマンドによる設定]

1. (config)# router bgp 65531
   (config-router)# bgp router-id 192.168.2.100
   (config-router)# neighbor 172.16.2.2 remote-as 65532
   (config-router)# neighbor 192.168.2.2 remote-as 65531
   (config-router)# exit
   BGP4 ピアを設定します。
2. (config)# route-map ADV_NET permit 10
   (config-route-map)# match route-type local
   (config-route-map)# exit
   BGP4 広告用経路を許可することを指定します。
3. (config)# route-map ADV_NET deny 20
   (config-route-map)# match protocol bgp
   (config-route-map)# exit
   BGP プロトコルを拒否することを指定します。
4. (config)# router bgp 65531
   (config-router)# neighbor 172.16.2.2 route-map ADV_NET out
   (config-router)# exit
   相手側アドレスが 172.16.2.2 のピアへ BGP4 広告用経路だけを広告すること（学習した BGP4 経路は広告しないこと）を指定します。
5. (config)# route-map DENY_NET deny 10
   (config-route-map)# match route-type local
   (config-route-map)# exit
   BGP4 広告用経路を拒否することを指定します。
6. (config)# router bgp 65531
   (config-router)# neighbor 192.168.2.2 route-map DENY_NET out
   (config-router)# exit
   相手側アドレスが 192.168.2.2 のピアへ BGP4 広告用経路を広告しないことを指定します。
7. (config)# ip route 192.168.2.0 255.255.255.0 null 0 250 generate-bgp-route
   スタティック経路と BGP4 広告用経路を同時に生成します。

(4)　経路フィルタリングの運用への反映

[設定のポイント]

運用コマンド clear ip bgp を使用して，広告経路フィルタリングの条件として設定した経路フィルタを運用に反映します。

[コマンドによる設定]

1. # clear ip bgp * out
   広告用経路フィルタを運用に反映します。

22.2.6　ルート・フラップ・ダンプニングの設定

(1)　コンフィグレーションコマンド一覧

ルート・フラップ・ダンプニングのコンフィグレーションコマンド一覧を次の表に示します。

表 22-14　コンフィグレーションコマンド一覧

コマンド名	説明
bgp dampening	ルート・フラップしている経路の使用を一時的に抑止して，ルート・フラップによる影響を軽減します。※

注※　グローバルネットワークだけの指定です。config-router モードの設定は VRF に適用されません。

(2)　ルート・フラップ・ダンプニングの設定

[設定のポイント]

BGP4 経路にルート・フラップ・ダンプニングを適用する場合は，config-router モードで bgp dampening コマンドを設定します。

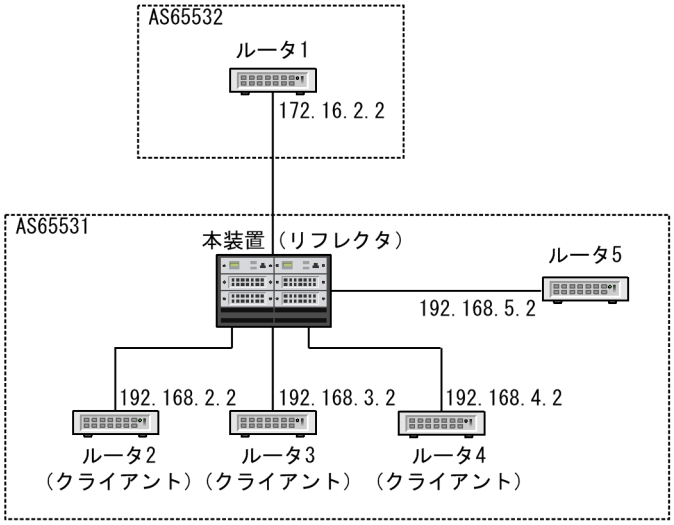
[コマンドによる設定]

1. **(config)# router bgp 65531**
   (config-router)# bgp router-id 192.168.1.100
   (config-router)# neighbor 172.16.2.2 remote-as 65532
   (config-router)# neighbor 172.17.2.2 remote-as 65533
   BGP4 ピアを設定します。
2. **(config-router)# bgp dampening**
   ルート・フラップ・ダンプニングを適用します。

22.2.7　ルート・リフレクションの設定

次の図に示す構成例を基に説明します。

図 22-22　ルート・リフレクション構成例



(1)　コンフィグレーションコマンド一覧

ルート・リフレクションのコンフィグレーションコマンド一覧を次の表に示します。

表 22-15　コンフィグレーションコマンド一覧

コマンド名	説明
bgp client-to-client reflection	ルート・リフレクタ・クライアント間で BGP4 経路をリフレクトすることを指定します。
bgp cluster-id	ルート・リフレクションで使用するクラスタ ID を指定します。
bgp router-id	bgp cluster-id の設定がない場合に，ルート・リフレクションのクラスタ ID として使用します。
neighbor always-nexthop-self	内部ピアへ広告する経路の NEXT_HOP 属性を，強制的に内部ピアとのピアリングに使用している自側アドレスに書き替えることを指定します（ルート・リフレクションの場合を含む）。
neighbor route-reflector-client	ルート・リフレクタ・クライアントを指定します。

(2)　ルート・リフレクションの設定

[設定のポイント]

bgp client-to-client reflection コマンドはデフォルトで有効なため，設定は不要です。なお，ルート・リフレクタでは，ルート・リフレクタ・クライアント間で BGP4 経路をリフレクトさせない場合，config-router モードで no bgp client-to-client reflection コマンドを指定してください。

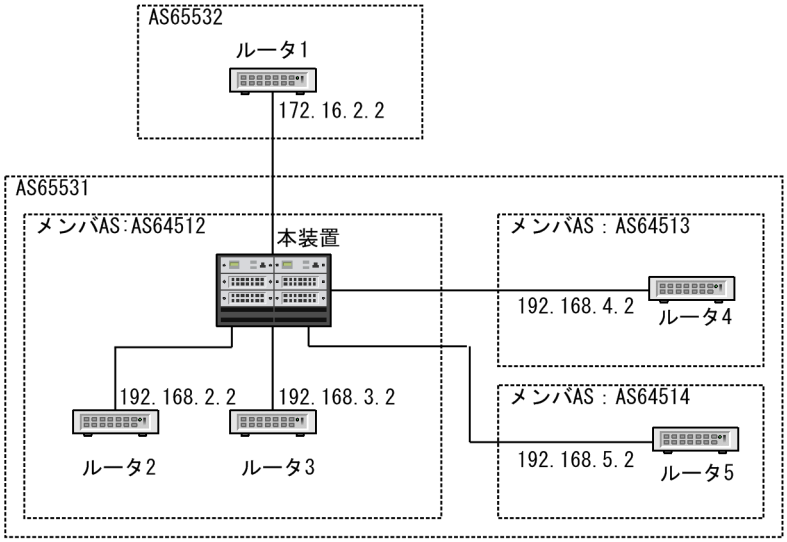
[コマンドによる設定]

1. **(config)# router bgp 65531**
   (config-router)# bgp router-id 192.168.1.100
   (config-router)# neighbor 172.16.2.2 remote-as 65532
   (config-router)# neighbor 192.168.2.2 remote-as 65531
   (config-router)# neighbor 192.168.3.2 remote-as 65531
   (config-router)# neighbor 192.168.4.2 remote-as 65531
   (config-router)# neighbor 192.168.5.2 remote-as 65531
   ルータ 1 を外部ピア，ルータ 2，ルータ 3，ルータ 4，およびルータ 5 を内部ピアとして BGP4 ピアを設定します。
2. **(config-router)# bgp cluster-id 10.1.2.1**
   クラスタ ID を設定します。
3. **(config-router)# neighbor 192.168.2.2 route-reflector-client**
   (config-router)# neighbor 192.168.3.2 route-reflector-client
   (config-router)# neighbor 192.168.4.2 route-reflector-client
   ルータ 2，ルータ 3，およびルータ 4 をルート・リフレクタ・クライアントに指定します。

22.2.8　コンフェデレーションの設定

次の図に示す構成例を基に説明します。

図 22-23　コンフェデレーション構成例



(1)　コンフィグレーションコマンド一覧

コンフェデレーションのコンフィグレーションコマンド一覧を次の表に示します。

表 22-16　コンフィグレーションコマンド一覧

コマンド名	説明
bgp confederation identifier	コンフェデレーション構成時の，自コンフェデレーションの AS 番号を指定します。※
bgp confederation peers	コンフェデレーション構成時の，接続先メンバー AS 番号を指定します。
neighbor remote-as	BGP4 ピアを設定します。コンフェデレーション構成時の，自メンバー AS 番号を設定します。

注※　VRF とグローバルネットワーク共通の指定です。

(2)　コンフェデレーションの設定

[設定のポイント]

自メンバー AS 番号を router bgp コマンドで指定して，接続するほかのメンバー AS 番号は config-router モードで bgp confederation peers コマンドを設定します。

[コマンドによる設定]

1. **(config)# router bgp 64512**
   自メンバー AS 番号（64512）を指定します。
2. **(config-router)# bgp router-id 192.168.1.100**
   ルータ ID を指定します。
3. **(config-router)# bgp confederation identifier 65531**
   自コンフェデレーションの AS 番号（65531）を指定します。
4. **(config-router)# bgp confederation peers 64513 64514**
   接続するほかのメンバー AS 番号（64513，64514）を指定します。

5. (config-router)# neighbor 172.16.2.2 remote-as 65532
   (config-router)# neighbor 192.168.2.2 remote-as 64512
   (config-router)# neighbor 192.168.3.2 remote-as 64512
   (config-router)# neighbor 192.168.4.2 remote-as 64513
   (config-router)# neighbor 192.168.5.2 remote-as 64514
   ルータ 1 を外部ピア，ルータ 2 およびルータ 3 を内部ピア，ルータ 4 およびルータ 5 をメンバー AS 間ピアとして BGP4 ピアを設定します。

22.2.9　ノンストップルーティングの設定

(1)　コンフィグレーションコマンド一覧

ノンストップルーティングのコンフィグレーションコマンド一覧を次の表に示します。

表 22-17　コンフィグレーションコマンド一覧

コマンド名	説明
neighbor ha-mode nsr	ノンストップルーティングを有効にします。

(2)　ノンストップルーティングの設定

[設定のポイント]

ユニキャストルーティングプログラムと TCP 高可用プログラムの再起動時に系切替することを指定します。さらに，neighbor ha-mode nsr コマンドを設定して，ノンストップルーティングを有効にします。

[コマンドによる設定]

1. (config)# failure-action software unicast switchover
   (config)# failure-action software tcp-ha switchover
   ユニキャストルーティングプログラムと TCP 高可用プログラムの再起動時に系切替します。
2. (config)# router bgp 65531
   (config-router)# bgp router-id 192.168.1.100
   (config-router)# neighbor 172.16.2.2 remote-as 65532
   (config-router)# neighbor 192.168.2.2 remote-as 65531
   BGP4 ピアを設定します。
3. (config-router)# neighbor 172.16.2.2 soft-reconfiguration inbound
   (config-router)# neighbor 192.168.2.2 soft-reconfiguration inbound
   学習経路フィルタで抑止した経路を無効経路として保持することを指定します。
4. (config-router)# neighbor 172.16.2.2 ha-mode nsr
   (config-router)# neighbor 192.168.2.2 ha-mode nsr
   ノンストップルーティングを使用することを指定します。

22.2.10　グレースフル・リスタートの設定

(1)　コンフィグレーションコマンド一覧

グレースフル・リスタートのコンフィグレーションコマンド一覧を次の表に示します。

表 22-18　コンフィグレーションコマンド一覧

コマンド名	説明
bgp graceful-restart mode	グレースフル・リスタートを使用することを指定します。※1
bgp graceful-restart restart-time	隣接ルータがグレースフル・リスタートを開始してからピアが再接続するまでの最大時間を指定します。※1
bgp graceful-restart stalepath-time	隣接ルータがグレースフル・リスタートを開始してからグレースフル・リスタート開始以前の経路を保持する最大時間を指定します。※1
routing options graceful-restart time-limit※2	本装置が経路を保留する時間の上限値を指定します。

注※1

VRF とグローバルネットワーク共通の指定です。config-router モードの設定が VRF にも適用されます。

注※2

「コンフィグレーションコマンドレファレンス Vol.3　13. ルーティングオプション」を参照してください。

(2)　グレースフル・リスタートの設定

[設定のポイント]

- グレースフル・リスタートのリスタートルータ機能を使用する場合は config-router モードで bgp graceful-restart mode コマンドの restart パラメータまたは both パラメータを設定します。bgp graceful-restart restart-time コマンドおよび bgp graceful-restart stalepath-time コマンドを設定する必要がある場合は，bgp graceful-restart mode コマンドを設定したあとで設定します。
- グレースフル・リスタートのレシーブルータ機能を使用する場合は config-router モードで bgp graceful-restart mode コマンドの receive パラメータまたは both パラメータを設定します。bgp graceful-restart restart-time コマンドおよび bgp graceful-restart stalepath-time コマンドを設定する必要がある場合は，bgp graceful-restart mode コマンドを設定したあとで設定します。

[コマンドによる設定]

1. **(config)# router bgp 65531**
   (config-router)# bgp router-id 192.168.1.100
   (config-router)# neighbor 172.16.2.2 remote-as 65532
   (config-router)# neighbor 192.168.2.2 remote-as 65531
   BGP4 ピアを設定します。
2. **(config-router)# bgp graceful-restart mode both**
   グレースフル・リスタートのリスタートルータ機能とレシーブルータ機能を使用することを指定します。

22.2.11　BGP4 学習経路数制限の設定

(1)　コンフィグレーションコマンド一覧

BGP4 学習経路数制限のコンフィグレーションコマンド一覧を次の表に示します。

表 22-19　コンフィグレーションコマンド一覧

コマンド名	説明
neighbor maximum-prefix	該当ピアから学習する経路数を制限します。

(2)　BGP4 学習経路数制限の設定

[設定のポイント]

該当ピアに BGP4 学習経路数制限を適用する場合は，neighbor maximum-prefix コマンドを設定します。

[コマンドによる設定]

1. **(config)# router bgp 65531**
   (config-router)# bgp router-id 192.168.1.100
   (config-router)# neighbor 172.16.2.2 remote-as 65532
   (config-router)# neighbor 192.168.2.2 remote-as 65531
   BGP4 ピアを設定します。
2. **(config-router)# neighbor 172.16.2.2 maximum-prefix 10000 80 restart 60**
   外部ピア（相手側アドレス：172.16.2.2）から学習する経路数の上限値を 10000 経路，警告のシステムメッセージを出力する閾値を 80%，上限値を超えてピア切断した場合は 60 分後に再接続する設定をします。
3. **(config-router)# neighbor 192.168.2.2 maximum-prefix 1000 warning-only**
   内部ピア（相手側アドレス：172.16.2.2）から学習する経路数の上限値を 1000 経路，上限値を超えた場合でもピアを切断しない設定をします。

22.2.12　インタフェースダウン時の外部ピア即時切断機能の設定

(1)　コンフィグレーションコマンド一覧

インタフェースダウン時の外部ピア即時切断機能のコンフィグレーションコマンド一覧を次の表に示します。

表 22-20　コンフィグレーションコマンド一覧

コマンド名	説明
bgp fast-external-fallover	直接接続された外部ピアとのインタフェースダウン時，すぐに該当ピアを切断します。

(2) インタフェースダウン時の外部ピア即時切断機能の設定

[設定のポイント]

bgp fast-external-fallover コマンドはデフォルトで有効なため，設定は不要です。なお，直接接続された外部ピアとのインタフェースダウン時すぐにピアを切断しない場合は，config-router モードで no bgp fast-external-fallover コマンドを指定してください。

[コマンドによる設定]

1. **(config)# router bgp 65531**
   (config-router)# bgp router-id 192.168.1.100
   (config-router)# neighbor 172.16.2.2 remote-as 65532
   (config-router)# neighbor 192.168.2.2 remote-as 65531
   BGP4 ピアを設定します。
2. **(config-router)# no bgp fast-external-fallover**
   直接接続されている外部ピアとのインタフェースダウン時，すぐに該当ピアを切断しないことを設定します。

22.3　BGP4+拡張機能のコンフィグレーション

22.3.1　BGP4+ピアグループの設定

(1)　コンフィグレーションコマンド一覧

BGP4+ピアグループのコンフィグレーションコマンド一覧を次の表に示します。

表 22-21　コンフィグレーションコマンド一覧

コマンド名	説明
neighbor peer-group (assigning members)	ピアをピアグループに所属させます。
neighbor peer-group (creating)	ピアグループを設定します。

(2)　BGP4+ピアグループの設定

[設定のポイント]

ピアグループは neighbor peer-group（creating）コマンドで設定します。ピアグループに設定したピアの AS 番号やオプション，広告経路フィルタなどはピアグループに所属するすべてのピアに適用されます。

[コマンドによる設定]

1. **(config)# router bgp 65531**
   (config-router)# bgp router-id 172.16.2.100
   (config-router)# neighbor INTERNAL-GROUP peer-group
   neighbor peer-group（creating）コマンドでピアグループ（グループ識別子：INTERNAL-GROUP）を設定します。
2. **(config-router)# neighbor INTERNAL-GROUP remote-as 65531**
   (config-router)# address-family ipv6
   (config-router-af)# neighbor INTERNAL-GROUP soft-reconfiguration inbound
   (config-router-af)# exit
   (config-router)# neighbor INTERNAL-GROUP timers 30 90
   ピアグループ（グループ識別子：INTERNAL-GROUP）にピアの AS 番号（AS：65531）および各種オプションを設定します。
3. **(config-router)# neighbor EXTERNAL-GROUP peer-group**
   (config-router)# address-family ipv6
   (config-router-af)# neighbor EXTERNAL-GROUP activate
   (config-router-af)# neighbor EXTERNAL-GROUP send-community
   (config-router-af)# top
   neighbor peer-group（creating）コマンドでピアグループ（グループ識別子：EXTERNAL-GROUP）を設定します。また，各種オプションを設定します。
4. **(config)# route-map SET_COM permit 10**
   (config-route-map)# set community 1000:1001
   (config-route-map)# exit

コミュニティ値 1000:1001 を指定した route-map を設定します。

5. **(config)# router bgp 65531**
   (config-router)# address-family ipv6
   (config-router-af)# neighbor EXTERNAL-GROUP route-map SET_COM out
   (config-router-af)# exit
   ピアグループ（グループ識別子：EXTERNAL-GROUP）に広告経路フィルタを設定します。

(3)　BGP4+ピアをピアグループに所属させる設定

[設定のポイント]

ピアをピアグループに所属させる場合は neighbor peer-group（assigning members）コマンドを設定します。

[コマンドによる設定]

1. **(config-router)# neighbor 2001:db8:16:2::2 peer-group INTERNAL-GROUP**
   neighbor peer-group（assigning members）コマンドでピア（相手側アドレス：2001:db8:16:2::2）をピアグループ（グループ識別子：INTERNAL-GROUP）に所属させます。ピアの AS 番号はピアグループに指定した 65531 を使用します。
2. **(config-router)# neighbor 2001:db8:17:3::3 peer-group INTERNAL-GROUP**
   neighbor peer-group（assigning members）コマンドでピア（相手側アドレス：2001:db8:17:3::3）をピアグループ（グループ識別子：INTERNAL-GROUP）に所属させます。ピアの AS 番号はピアグループに指定した 65531 を使用します。
3. **(config-router)# neighbor 2001:db8:168:4::4 remote-as 65533**
   (config-router)# neighbor 2001:db8:168:4::4 peer-group EXTERNAL-GROUP
   ピア（相手側アドレス：2001:db8:168:4::4）を設定して，ピアグループ（グループ識別子：EXTERNAL-GROUP）に所属させます。ピアの AS 番号はピアに指定した 65533 を使用します。
4. **(config-router)# neighbor 2001:db8:168:5::5 remote-as 65534**
   (config-router)# neighbor 2001:db8:168:5::5 peer-group EXTERNAL-GROUP
   ピア（相手側アドレス：2001:db8:168:5::5）を設定して，ピアグループ（グループ識別子：EXTERNAL-GROUP）に所属させます。ピアの AS 番号はピアに指定した 65534 を使用します。

22.3.2　コミュニティの設定

(1)　コンフィグレーションコマンド一覧

コミュニティのコンフィグレーションコマンド一覧を次の表に示します。

表 22-22　コンフィグレーションコマンド一覧

コマンド名	説明
neighbor send-community	ピアへ広告する経路の COMMUNITIES 属性を削除しないことを指定します。
distribute-list in (BGP4+)※	BGP4+の学習経路フィルタリングの条件として使用する経路フィルタを指定します。
distribute-list out (BGP4+)※	BGP4+の広告経路フィルタリングの条件として使用する経路フィルタを指定します。

コマンド名	説明
neighbor in (BGP4+)※	route-map パラメータで，BGP4+の特定のピアにだけ，学習経路フィルタリングの条件として使用する経路フィルタを指定します。
neighbor out (BGP4+)※	route-map パラメータで，BGP4+の特定のピアにだけ，広告経路フィルタリングの条件として使用する経路フィルタを指定します。
redistribute (BGP4+)※	BGP4+で広告する経路のプロトコルを指定します。

注※
「コンフィグレーションコマンドレファレンス Vol.3　22. 経路フィルタリング」を参照してください。

(2)　コミュニティの設定

[設定のポイント]

広告する BGP4+経路に COMMUNITIES 属性を付ける場合，該当するピアに neighbor send-community コマンドを設定してください。

[コマンドによる設定]

1. **(config)# router bgp 65531**
   (config-router)# bgp router-id 192.168.1.100
   (config-router)# neighbor 2001:db8:168:2::2 remote-as 65531
   (config-router)# neighbor 2001:db8:16:2::2 remote-as 65532
   (config-router)# neighbor 2001:db8:2:2::2 remote-as 65533
   BGP4+ピアを設定します。
2. **(config-router)# address-family ipv6**
   config-router-af モードへ移行します。
3. **(config-router-af)# neighbor 2001:db8:16:2::2 send-community**
   (config-router-af)# neighbor 2001:db8:2:2::2 send-community
   (config-router-af)# exit
   (config-router)# exit
   ピアに広告する BGP4+経路に COMMUNITIES 属性を付けることを指定します。
4. **(config)# ip community-list 10 permit 1000:1002**
   (config)# ip community-list 20 permit 1000:1003
   (config)# route-map SET_LOCPREF permit 10
   (config-route-map)# match community 10
   (config-route-map)# set local-preference 120
   (config-route-map)# exit
   (config)# route-map SET_LOCPREF permit 20
   (config-route-map)# match community 20
   (config-route-map)# set local-preference 80
   (config-route-map)# exit
   (config)# route-map SET_LOCPREF permit 30
   (config-route-map)# exit

コミュニティ値 1000:1002 を含む COMMUNITIES 属性を持つ経路の LOCAL_PREF 属性値に 120 を設定して，コミュニティ値 1000:1003 を含む COMMUNITIES 属性を持つ経路の LOCAL_PREF 属性値に 80 を設定します。

5. **(config)# ipv6 prefix-list MY_NET seq 10 permit 2001:db8:168::/48 ge 32 le 64**
   (config)# route-map SET_COM permit 10
   (config-route-map)# match ipv6 address prefix-list MY_NET
   (config-route-map)# set community 1000:1001
   (config-route-map)# exit
   宛先ネットワークが 2001:db8:168::/48（プレフィックス長が 32～64）の経路にコミュニティ値 1000:1001 が設定された COMMUNITIES 属性を設定します。
6. **(config)# router bgp 65531**
   (config-router)# address-family ipv6
   (config-router-af)# distribute-list route-map SET_LOCPREF in
   (config-router-af)# distribute-list route-map SET_COM out
   全ピアに学習用経路フィルタと広告用経路フィルタを適用します。
7. **(config-router-af)# neighbor 2001:db8:168:2::2 activate**
   (config-router-af)# neighbor 2001:db8:16:2::2 activate
   (config-router-af)# neighbor 2001:db8:2:2::2 activate
   IPv6 アドレスファミリを有効にします。

(3)　経路フィルタリングの運用への反映

[設定のポイント]

運用コマンド clear ipv6 bgp を使用して，学習経路フィルタリングの条件および広告フィルタリングの条件として設定した経路フィルタを運用に反映します。

[コマンドによる設定]

1. **# clear ipv6 bgp * both**
   コミュニティを使用した経路フィルタを運用に反映します。

22.3.3　BGP4+マルチパスの設定

(1)　コンフィグレーションコマンド一覧

BGP4+マルチパスのコンフィグレーションコマンド一覧を次の表に示します。

表 22-23　コンフィグレーションコマンド一覧

コマンド名	説明
bgp always-compare-med	異なる AS から学習した MED 属性を比較することを設定します（本コマンドが未設定の場合，maximum-paths コマンドの all-as パラメータを設定できません）。
maximum-paths	マルチパスを設定します。

(2)　BGP4+のマルチパスの設定

[設定のポイント]

maximum-paths コマンドで all-as パラメータを指定する場合は，あらかじめ bgp always-compare-med コマンドを設定しておいてください。

[コマンドによる設定]

1. **(config)# router bgp 65531**
   (config-router)# bgp router-id 192.168.1.100
   (config-router)# neighbor 2001:db8:16:2::2 remote-as 65532
   (config-router)# neighbor 2001:db8:17:2::2 remote-as 65533
   マルチパスを形成するピアを設定します。この例では，AS65532 と AS65533 から学習した経路間でマルチパスを形成します。
2. **(config-router)# address-family ipv6**
   config-router-af（ipv6）モードへ移行します。
3. **(config-router-af)# bgp always-compare-med**
   (config-router-af)# maximum-paths 4 all-as
   異なる AS から学習した経路を含めて最大４パスのマルチパスを形成することを指定します。
4. **(config-router-af)# neighbor 2001:db8:16:2::2 activate**
   (config-router-af)# neighbor 2001:db8:17:2::2 activate
   IPv6 アドレスファミリを有効にします。

22.3.4　TCP MD5 認証の設定

(1)　コンフィグレーションコマンド一覧

TCP MD5 認証のコンフィグレーションコマンド一覧を次の表に示します。

表 22-24　コンフィグレーションコマンド一覧

コマンド名	説明
neighbor password	ピアとの接続に TCP MD5 認証を適用することを設定します。

(2)　TCP MD5 認証の設定

[設定のポイント]

TCP MD5 認証は neighbor password コマンドを使用して認証キーを設定します。

[コマンドによる設定]

1. **(config)# router bgp 65531**
   (config-router)# bgp router-id 192.168.1.100
   (config-router)# neighbor 2001:db8:16:2::2 remote-as 65532
   (config-router)# neighbor 2001:db8:168:2::2 remote-as 65531
   BGP4+ピアを設定します。
2. **(config-router)# neighbor 2001:db8:16:2::2 password ”authmd5_65532”**

相手側アドレスが 2001:db8:16:2::2 のピアに，認証キーが"authmd5_65532"の TCP MD5 認証を設定します。

3. **(config-router)# address-family ipv6**

   config-router-af（ipv6）モードへ移行します。

4. **(config-router-af)# neighbor 2001:db8:16:2::2 activate**

   (config-router-af)# neighbor 2001:db8:168:2::2 activate

   IPv6 アドレスファミリを有効にします。

22.3.5　BGP4+広告用経路生成の設定

(1)　コンフィグレーションコマンド一覧

BGP4+広告用経路生成のコンフィグレーションコマンド一覧を次の表に示します。

表 22-25　コンフィグレーションコマンド一覧

コマンド名	説明
network	BGP4+広告用経路を生成することを設定します。
ipv6 route※	generate-bgp-route パラメータで，BGP4+広告用経路を生成することを設定します。

注※

「コンフィグレーションコマンドレファレンス Vol.3　16. スタティックルーティング（IPv6）」を参照してください。

(2)　network コマンドを使用した BGP4+広告用経路生成の設定

[設定のポイント]

BGP4+広告用経路を経路フィルタリングする場合は，route-map の match route-type コマンドで local パラメータを指定します。

[コマンドによる設定]

1. **(config)# router bgp 65531**

   (config-router)# bgp router-id 192.168.2.100

   (config-router)# neighbor 2001:db8:16:2::2 remote-as 65532

   (config-router)# neighbor 2001:db8:168:2::2 remote-as 65531

   (config-router)# exit

   BGP4+ピアを設定します。

2. **(config)# route-map ADV_NET permit 10**

   (config-route-map)# match route-type local

   (config-route-map)# exit

   BGP4+広告用経路を許可することを指定します。

3. **(config)# route-map ADV_NET deny 20**

   (config-route-map)# match protocol bgp

   (config-route-map)# exit

   BGP プロトコルを拒否することを指定します。

4. **(config)# router bgp 65531**

```
(config-router)# neighbor 2001:db8:16:2::2 route-map ADV_NET out
(config-router)# exit
```

相手側アドレスが 2001:db8:16:2::2 のピアへ BGP4+広告用経路だけを広告すること（学習した BGP4+経路は広告しないこと）を指定します。

5.
```
(config)# route-map DENY_NET deny 10
(config-route-map)# match route-type local
(config-route-map)# exit
```

BGP4+広告用経路を拒否することを指定します。

6.
```
(config)# router bgp 65531
(config-router)# neighbor 2001:db8:168:2::2 route-map DENY_NET out
(config-router)# exit
```

相手側アドレスが 2001:db8:168:2::2 のピアへ BGP4+広告用経路を広告しないことを指定します。

7.
```
(config)# ipv6 route 2001:db8:168:1::/64 null 0 250
```

Null インタフェースをネクストホップとするスタティック経路を生成します。

8.
```
(config)# router bgp 65531
(config-router)# address-family ipv6
(config-router)# network 2001:db8:168:1::/64
(config-router)# exit
```

BGP4+広告用経路のネットワークアドレスを指定すると，BGP4+広告用経路を生成します。

(3)　ipv6 route コマンドを使用した BGP4+広告用経路生成の設定

[設定のポイント]

BGP4+広告用経路を経路フィルタリングする場合は，route-map の match route-type コマンドで local パラメータを指定します。

[コマンドによる設定]

1.
```
(config)# router bgp 65531
(config-router)# bgp router-id 192.168.2.100
(config-router)# neighbor 2001:db8:16:2::2 remote-as 65532
(config-router)# neighbor 2001:db8:168:2::2 remote-as 65531
(config-router)# exit
```

BGP4+ピアを設定します。

2.
```
(config)# route-map ADV_NET permit 10
(config-route-map)# match route-type local
(config-route-map)# exit
```

BGP4+広告用経路を許可することを指定します。

3.
```
(config)# route-map ADV_NET deny 20
(config-route-map)# match protocol bgp
(config-route-map)# exit
```

BGP プロトコルを拒否することを指定します。

4.
```
(config)# router bgp 65531
(config-router)# neighbor 2001:db8:16:2::2 route-map ADV_NET out
```

```
(config-router)# exit
```

相手側アドレスが 2001:db8:16:2::2 のピアへ BGP4+広告用経路だけを広告すること（学習した BGP4+経路は広告しないこと）を指定します。

5.
```
(config)# route-map DENY_NET deny 10
(config-route-map)# match route-type local
(config-route-map)# exit
```

BGP4+広告用経路を拒否することを指定します。

6.
```
(config)# router bgp 65531
(config-router)# neighbor 2001:db8:168:2::2 route-map DENY_NET out
(config-router)# exit
```

相手側アドレスが 2001:db8:168:2::2 のピアへ BGP4+広告用経路を広告しないことを指定します。

7.
```
(config)# ipv6 route 2001:db8:168:1::/64 null 0 250 generate-bgp-route
```

スタティック経路と BGP4+広告用経路を同時に生成します。

(4)　経路フィルタリングの運用への反映

[設定のポイント]

運用コマンド clear ipv6 bgp を使用して，広告経路フィルタリングの条件として設定した経路フィルタを運用に反映します。

[コマンドによる設定]

1.
```
# clear ipv6 bgp * out
```

広告用経路フィルタを運用に反映します。

22.3.6　ルート・フラップ・ダンプニングの設定

(1)　コンフィグレーションコマンド一覧

ルート・フラップ・ダンプニングのコンフィグレーションコマンド一覧を次の表に示します。

表 22-26　コンフィグレーションコマンド一覧

コマンド名	説明
bgp dampening	ルート・フラップしている経路の使用を一時的に抑止して，ルート・フラップによる影響を軽減します。※

注※　グローバルネットワークだけの指定です。

(2)　ルート・フラップ・ダンプニングの設定

[設定のポイント]

BGP4+経路にルート・フラップ・ダンプニングを適用する場合は，config-router-af（ipv6）モードで bgp dampening コマンドを設定します。

[コマンドによる設定]

1.
```
(config)# router bgp 65531
(config-router)# bgp router-id 192.168.1.100
```

```
(config-router)# neighbor 2001:db8:16:2::2 remote-as 65532
(config-router)# neighbor 2001:db8:17:2::2 remote-as 65533
```

BGP4+ピアを設定します。

2. **(config-router)# address-family ipv6**

   config-router-af（ipv6）モードへ移行します。

3. **(config-router-af)# bgp dampening**

   ルート・フラップ・ダンプニングを適用します。

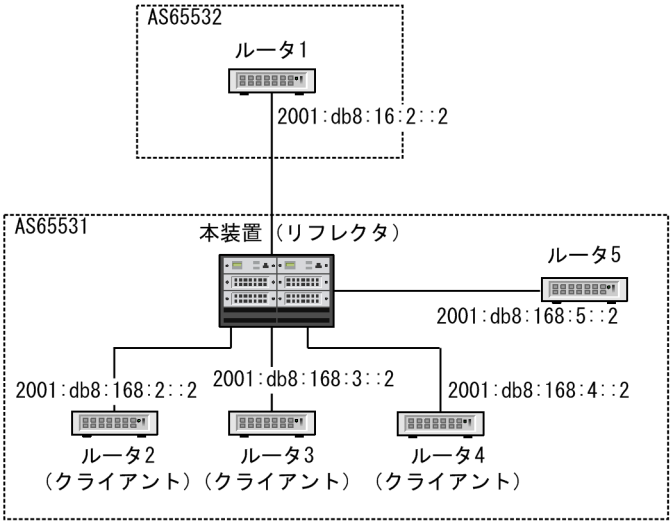
4. **(config-router-af)# neighbor 2001:db8:16:2::2 activate**
   (config-router-af)# neighbor 2001:db8:17:2::2 activate

   IPv6 アドレスファミリを有効にします。

22.3.7　ルート・リフレクションの設定

次の図に示す構成例を基に説明します。

図 22-24　ルート・リフレクション構成例



(1)　コンフィグレーションコマンド一覧

ルート・リフレクションのコンフィグレーションコマンド一覧を次の表に示します。

表 22-27　コンフィグレーションコマンド一覧

コマンド名	説明
bgp client-to-client reflection	ルート・リフレクタ・クライアント間で BGP4+経路をリフレクトすることを指定します。
bgp cluster-id	ルート・リフレクションで使用するクラスタ ID を指定します。
bgp router-id	bgp cluster-id の設定がない場合に，ルート・リフレクションのクラスタ ID として使用します。
neighbor always-nexthop-self	内部ピアへ広告する経路の MP_REACH_NLRI 属性のネクストホップ情報を，強制的に内部ピアとのピアリングに使用している自側アドレスに書き替えることを指定します（ルート・リフレクションの場合を含む）。

コマンド名	説明
neighbor route-reflector-client	ルート・リフレクタ・クライアントを指定します。

(2)　ルート・リフレクションの設定

[設定のポイント]

bgp client-to-client reflection コマンドはデフォルトで有効なため，設定は不要です。なお，ルート・リフレクタでは，ルート・リフレクタ・クライアント間で BGP4+経路をリフレクトさせない場合，config-router-af（ipv6）モードまたは config-router-af（ipv6 vrf）モードで no bgp client-to-client reflection コマンドを指定してください。

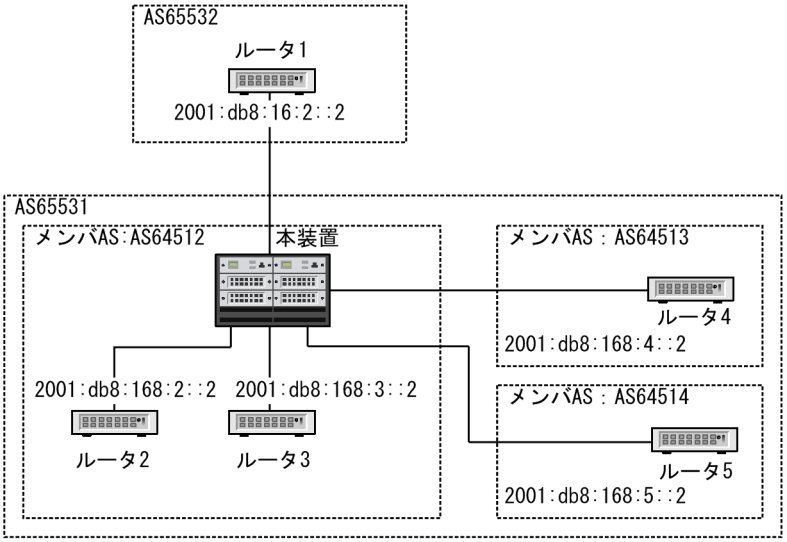
[コマンドによる設定]

1. **(config)# router bgp 65531**
   (config-router)# bgp router-id 192.168.1.100
   (config-router)# neighbor 2001:db8:16:2::2 remote-as 65532
   (config-router)# neighbor 2001:db8:168:2::2 remote-as 65531
   (config-router)# neighbor 2001:db8:168:3::2 remote-as 65531
   (config-router)# neighbor 2001:db8:168:4::2 remote-as 65531
   (config-router)# neighbor 2001:db8:168:5::2 remote-as 65531
   ルータ 1 を外部ピア，ルータ 2，ルータ 3，ルータ 4，およびルータ 5 を内部ピアとして BGP4+ピアを設定します。
2. **(config-router)# bgp cluster-id 10.1.2.1**
   クラスタ ID を設定します。
3. **(config-router)# address-family ipv6**
   config-router-af（ipv6）モードへ移行します。
4. **(config-router-af)# neighbor 2001:db8:168:2::2 route-reflector-client**
   (config-router-af)# neighbor 2001:db8:168:3::2 route-reflector-client
   (config-router-af)# neighbor 2001:db8:168:4::2 route-reflector-client
   ルータ 2，ルータ 3，およびルータ 4 をルート・リフレクタ・クライアントに指定します。
5. **(config-router-af)# neighbor 2001:db8:16:2::2 activate**
   (config-router-af)# neighbor 2001:db8:168:2::2 activate
   (config-router-af)# neighbor 2001:db8:168:3::2 activate
   (config-router-af)# neighbor 2001:db8:168:4::2 activate
   (config-router-af)# neighbor 2001:db8:168:5::2 activate
   IPv6 アドレスファミリを有効にします。

22.3.8　コンフェデレーションの設定

次の図に示す構成例を基に説明します。

図 22-25　コンフェデレーション構成例



(1)　コンフィグレーションコマンド一覧

コンフェデレーションのコンフィグレーションコマンド一覧を次の表に示します。

表 22-28　コンフィグレーションコマンド一覧

コマンド名	説明
bgp confederation identifier	コンフェデレーション構成時の，自コンフェデレーションの AS 番号を指定します。※
bgp confederation peers	コンフェデレーション構成時の，接続先メンバー AS 番号を指定します。
neighbor remote-as	BGP4+ピアを設定します。コンフェデレーション構成時の，自メンバー AS 番号を設定します。

注※　VRF とグローバルネットワーク共通の指定です。

(2)　コンフェデレーションの設定

[設定のポイント]

自メンバー AS 番号を router bgp コマンドで指定して，接続するほかのメンバー AS 番号は config-router モードで bgp confederation peers コマンドを設定します。

[コマンドによる設定]

1. **(config)# router bgp 64512**
   自メンバー AS 番号（64512）を指定します。
2. **(config-router)# bgp router-id 192.168.1.100**
   ルータ ID を指定します。
3. **(config-router)# bgp confederation identifier 65531**
   自コンフェデレーションの AS 番号（65531）を指定します。
4. **(config-router)# bgp confederation peers 64513 64514**
   接続するほかのメンバー AS 番号（64513，64514）を指定します。

5. **(config-router)# neighbor 2001:db8:16:2::2 remote-as 65532**
   (config-router)# neighbor 2001:db8:168:2::2 remote-as 64512
   (config-router)# neighbor 2001:db8:168:3::2 remote-as 64512
   (config-router)# neighbor 2001:db8:168:4::2 remote-as 64513
   (config-router)# neighbor 2001:db8:168:5::2 remote-as 64514
   ルータ 1 を外部ピア，ルータ 2 およびルータ 3 を内部ピア，ルータ 4 およびルータ 5 をメンバー AS 間ピアとして，BGP4+ピアを設定します。
6. **(config-router)# address-family ipv6**
   config-router-af（ipv6）モードへ移行します。
7. **(config-router-af)# neighbor 2001:db8:16:2::2 activate**
   (config-router-af)# neighbor 2001:db8:168:2::2 activate
   (config-router-af)# neighbor 2001:db8:168:3::2 activate
   (config-router-af)# neighbor 2001:db8:168:4::2 activate
   (config-router-af)# neighbor 2001:db8:168:5::2 activate
   IPv6 アドレスファミリを有効にします。

22.3.9　ノンストップルーティングの設定

(1)　コンフィグレーションコマンド一覧

ノンストップルーティングのコンフィグレーションコマンド一覧を次の表に示します。

表 22-29　コンフィグレーションコマンド一覧

コマンド名	説明
neighbor ha-mode nsr	ノンストップルーティングを有効にします。

(2)　ノンストップルーティングの設定

[設定のポイント]

ユニキャストルーティングプログラムと TCP 高可用プログラムの再起動時に系切替することを指定します。さらに，neighbor ha-mode nsr コマンドを設定して，ノンストップルーティングを有効にします。

[コマンドによる設定]

1. **(config)# failure-action software unicast switchover**
   (config)# failure-action software tcp-ha switchover
   ユニキャストルーティングプログラムと TCP 高可用プログラムの再起動時に系切替します。
2. **(config)# router bgp 65531**
   (config-router)# bgp router-id 192.168.1.100
   (config-router)# neighbor 2001:db8:16:2::2 remote-as 65532
   (config-router)# neighbor 2001:db8:168:2::2 remote-as 65531
   BGP4+ピアを設定します。
3. **(config-router)# address-family ipv6**
   config-router-af（ipv6）モードへ移行します。

4. **(config-router-af)# neighbor 2001:db8:16:2::2 soft-reconfiguration inbound**
   (config-router-af)# neighbor 2001:db8:168:2::2 soft-reconfiguration inbound
   学習経路フィルタで抑止した経路を無効経路として保持することを指定します。
5. **(config-router-af)# neighbor 2001:db8:16:2::2 ha-mode nsr**
   (config-router-af)# neighbor 2001:db8:168:2::2 ha-mode nsr
   ノンストップルーティングを使用することを指定します。
6. **(config-router-af)# neighbor 2001:db8:16:2::2 activate**
   (config-router-af)# neighbor 2001:db8:168:2::2 activate
   IPv6 アドレスファミリを有効にします。

22.3.10　グレースフル・リスタートの設定

(1)　コンフィグレーションコマンド一覧

グレースフル・リスタートのコンフィグレーションコマンド一覧を次の表に示します。

表 22-30　コンフィグレーションコマンド一覧

コマンド名	説明
bgp graceful-restart mode	グレースフル・リスタートを使用することを指定します。※1
bgp graceful-restart restart-time	隣接ルータがグレースフル・リスタートを開始してからピアが再接続するまでの最大時間を指定します。※1
bgp graceful-restart stalepath-time	隣接ルータがグレースフル・リスタートを開始してからグレースフル・リスタート開始以前の経路を保持する最大時間を指定します。※1
routing options graceful-restart time-limit※2	本装置が経路を保留する時間の上限値を指定します。

注※1
VRF とグローバルネットワーク共通の指定です。

注※2
「コンフィグレーションコマンドレファレンス Vol.3　13. ルーティングオプション」を参照してください。

(2)　グレースフル・リスタートの設定

[設定のポイント]
グレースフル・リスタートを使用する場合は，config-router モードで bgp graceful-restart mode コマンドを設定します。

[コマンドによる設定]

1. **(config)# router bgp 65531**
   (config-router)# bgp router-id 192.168.1.100
   (config-router)# neighbor 2001:db8:16:2::2 remote-as 65532
   (config-router)# neighbor 2001:db8:168:2::2 remote-as 65531
   BGP4+ピアを設定します。
2. **(config-router)# bgp graceful-restart mode both**

グレースフル・リスタートのリスタートルータ機能とレシーブルータ機能を使用することを指定します。

3. **(config-router)# address-family ipv6**
   config-router-af（ipv6）モードへ移行します。
4. **(config-router-af)# neighbor 2001:db8:16:2::2 activate**
   (config-router-af)# neighbor 2001:db8:168:2::2 activate
   IPv6 アドレスファミリを有効にします。

22.3.11　BGP4+学習経路数制限の設定

(1)　コンフィグレーションコマンド一覧

BGP4+学習経路数制限のコンフィグレーションコマンド一覧を次の表に示します。

表 22-31　コンフィグレーションコマンド一覧

コマンド名	説明
neighbor maximum-prefix	該当ピアから学習する経路数を制限します。

(2)　BGP4+学習経路数制限の設定

[設定のポイント]

該当ピアに BGP4+学習経路数制限を適用する場合は，neighbor maximum-prefix コマンドを設定します。

[コマンドによる設定]

1. **(config)# router bgp 65531**
   (config-router)# bgp router-id 192.168.1.100
   (config-router)# neighbor 2001:db8:16:2::2 remote-as 65532
   (config-router)# neighbor 2001:db8:168:2::2 remote-as 65531
   BGP4+ピアを設定します。
2. **(config-router)# address-family ipv6**
   config-router-af（ipv6）モードへ移行します。
3. **(config-router-af)# neighbor 2001:db8:16:2::2 maximum-prefix 1000 80 restart 60**
   外部ピア（相手側アドレス：2001:db8:16:2::2）から学習する経路数の上限値を 1000 経路，警告のシステムメッセージを出力する閾値を 80%，上限値を超えてピア切断した場合は 60 分後に再接続する設定をします。
4. **(config-router-af)# neighbor 2001:db8:168:2::2 maximum-prefix 100 warning-only**
   内部ピア（相手側アドレス：2001:db8:16:2::2）から学習する経路数の上限値を 100 経路，上限値を超えた場合でもピアを切断しない設定をします。
5. **(config-router-af)# neighbor 2001:db8:16:2::2 activate**
   (config-router-af)# neighbor 2001:db8:168:2::2 activate
   IPv6 アドレスファミリを有効にします。

22.3.12　インタフェースダウン時の外部ピア即時切断機能の設定

(1)　コンフィグレーションコマンド一覧

インタフェースダウン時の外部ピア即時切断機能のコンフィグレーションコマンド一覧を次の表に示します。

表 22-32　コンフィグレーションコマンド一覧

コマンド名	説明
bgp fast-external-fallover	直接接続された外部ピアとのインタフェースダウン時，すぐに該当ピアを切断します。

(2)　インタフェースダウン時の外部ピア即時切断機能の設定

[設定のポイント]

bgp fast-external-fallover コマンドはデフォルトで有効なため，設定は不要です。なお，直接接続された外部ピアとのインタフェースダウン時すぐにピアを切断しない場合は，config-router モードで no bgp fast-external-fallover コマンドを指定してください。

[コマンドによる設定]

1. **(config)# router bgp 65531**
   (config-router)# bgp router-id 192.168.1.100
   (config-router)# neighbor 2001:db8:172:16:2::2 remote-as 65532
   (config-router)# neighbor 2001:db8:192:168:2::2 remote-as 65531
   BGP4+ピアを設定します。
2. **(config-router)# no bgp fast-external-fallover**
   直接接続されている外部ピアとのインタフェースダウン時，すぐに該当ピアを切断しないことを設定します。
3. **(config-router)# address-family ipv6**
   config-router-af（ipv6）モードへ移行します。
4. **(config-router-af)# neighbor 2001:db8:172:16:2::2 activate**
   (config-router-af)# neighbor 2001:db8:192:168:2::2 activate
   IPv6 アドレスファミリを有効にします。

22.4　オペレーション

22.4.1　ピアグループの確認

(1)　運用コマンド一覧

ピアグループの運用コマンド一覧を次の表に示します。

表 22-33　運用コマンド一覧

コマンド名	説明
show ip bgp	BGP4 プロトコルに関する情報を表示します。
show ipv6 bgp	BGP4+プロトコルに関する情報を表示します。

(2)　ピアグループの確認

ピアグループに所属するピアのピアリング情報は, show ip bgp コマンドまたは show ipv6 bgp コマンドで peer-group パラメータを指定して確認します。

図 22-26　show ip bgp コマンド（peer-group パラメータ指定）の実行結果

```
>show ip bgp peer-group INTERNAL-GROUP
Date 20XX/07/17 18:40:00 UTC
Local AS: 65531, Local Router ID: 172.16.2.100
BGP Peer        AS     Received   Sent       Up/Down              Status
172.16.2.2      65531  36         42         20XX/07/16 18:42:26  Established
172.16.3.3      65531  51         63         20XX/07/16 12:42:31  Established
```

(3)　ピアグループに所属するピアの確認

ピアグループに所属するピアの情報は，show ip bgp コマンドまたは show ipv6 bgp コマンドで neighbors パラメータを指定して確認します。

図 22-27　show ip bgp コマンド（neighbors パラメータ指定）の実行結果

```
>show ip bgp neighbors EXTERNAL-GROUP
Date 20XX/07/17 18:45:09 UTC
Peer Address    Peer AS  Local Address    Local AS  Type      Status
192.168.4.4     65533    192.168.4.214    65531     External  Established
192.168.5.5     65534    192.168.5.189    65531     External  Active
```

(4)　ピアが所属するピアグループの確認

ピアが所属するピアグループは，show ip bgp コマンドまたは show ipv6 bgp コマンドで neighbors パラメータに<peer address>または<host name>を指定して確認します。

図 22-28　show ip bgp コマンド（neighbors <peer address>パラメータ指定）の実行結果

```
>show ip bgp neighbors 172.16.2.2
Date 20XX/07/17 18:45:09 UTC
BGP Peer: 172.16.2.2, Remote AS: 65531
Remote Router ID: 172.16.2.20, Peer Group: INTERNAL-GROUP                    <-1
    BGP Status:Established          HoldTime: 90   , Keepalive: 30
    Established Transitions: 1      Established Date: 20XX/07/16 18:42:26
    BGP Version: 4                  Type: Internal
    Local Address: 172.16.2.214,  Local AS: 65531
    Local Router ID: 172.16.2.100
    Next Connect Retry: -,          Connect Retry Timer: -
    Last Keep Alive Sent: 18:42:20, Last Keep Alive Received: 18:42:20
    BGP Message  UpdateIn UpdateOut TotalIn TotalOut
                 12       14        36      42
```

```
  BGP Capability Negotiation: <IPv4-Uni Refresh Refresh(v)>>
    Send   : <IPv4-Uni Refresh Refresh(v)>
    Receive: <IPv4-Uni Refresh Refresh(v)>>
  Password : UnConfigured
  Track Name: -, Track ID: -, Track State: -
```

1. ピアグループ INTERNAL-GROUP に所属しています。

22.4.2　コミュニティの確認

(1)　運用コマンド一覧

コミュニティの運用コマンド一覧を次の表に示します。

表 22-34　運用コマンド一覧

コマンド名	説明
show ip route	ルーティングテーブルで保持する IPv4 経路情報を表示します。
show ip bgp	BGP4 プロトコルに関する情報を表示します。
show ipv6 route	ルーティングテーブルで保持する IPv6 経路情報を表示します。
show ipv6 bgp	BGP4+プロトコルに関する情報を表示します。

(2)　学習経路のコミュニティ表示

特定のコミュニティを持つ経路は，show ip bgp コマンドまたは show ipv6 bgp コマンドで community パラメータを指定して表示します。

図 22-29　show ip bgp コマンド（community パラメータ指定）の実行結果

```
> show ip bgp community 1000:1002
Date 20XX/03/20 21:00:18 UTC
Local AS: 65531, Local Router ID: 192.168.1.100
Status Codes: d dampened, * valid, > active, S Stale, r RIB failure
Origin Codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop        MED    LocalPref Weight Path
*> 10.10/16           172.16.2.2      0      -         0      65532 i
*> 10.20/16           172.16.2.2      0      -         0      65532 i
```

経路が持つコミュニティは, show ip bgp コマンドまたは show ipv6 bgp コマンドで route パラメータを指定して表示します。

図 22-30　show ip bgp コマンド（route パラメータ指定）の実行結果

```
> show ip bgp route 10.10/16
Date 20XX/03/20 21:09:12 UTC
BGP Peer: 172.16.2.2   , Remote AS: 65532
Local AS: 65531, Local Router ID: 192.168.1.100
Status Codes: d dampened, * valid, > active, S Stale, r RIB failure
Route 10.10/16
*> Next Hop 172.16.2.2
     MED: -, LocalPref: 100, Weight: 0, Type: External route
     Origin: IGP, IGP Metric: 0
     Path: 65532
     Communities: 1000:1002
```

(3)　学習経路フィルタリング結果の表示

COMMUNITIES 属性を使用した学習経路フィルタリングの結果は，show ip bgp コマンドまたは show ipv6 bgp コマンドで表示します。

図 22-31　show ip bgp コマンドの実行結果

```
> show ip bgp
Date 20XX/03/20 21:10:09 UTC
Local AS: 65531, Local Router ID: 192.168.1.100
Status Codes: d dampened, * valid, > active, S Stale, r RIB failure
Origin Codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop        MED    LocalPref Weight Path
*> 10.10/16           172.16.2.2      -      120       0      65532 i
*  10.10/16           10.2.2.2        -       80       0      65533 i
*> 10.20/16           172.16.2.2      -      120       0      65532 i
*  10.20/16           10.2.2.2        -       80       0      65533 i
*> 192.168.20/24      192.168.2.2     -      100       0      i
*> 192.168.30/24      192.168.2.2     -      100       0      i
```

(4)　広告経路のコミュニティ表示

広告した BGP 経路の COMMUNITIES 属性は，show ip bgp コマンドまたは show ipv6 bgp コマンドで advertised-routes パラメータを指定して表示します。

図 22-32　show ip bgp コマンド（advertised-routes パラメータ指定）の実行結果

```
> show ip bgp advertised-routes 192.168.20/24
Date 20XX/03/20 21:10:25 UTC
BGP Peer: 172.16.2.2    , Remote AS: 65532
Local AS: 65531, Local Router ID: 192.168.1.100
Status Codes: d dampened, * valid, > active, S Stale, r RIB failure
Route 192.168.20/24
*> Next Hop 192.168.2.2
     MED: -, LocalPref: -,  Type: Internal route
     Origin: IGP
     Path: 65531
     Next Hop Attribute: 172.16.2.1
     Communities: 1000:1001

BGP Peer: 10.2.2.2     , Remote AS: 65533
Local AS: 65531, Local Router ID: 192.168.1.100
Status Codes: d dampened, * valid, > active, S Stale, r RIB failure
Route 192.168.20/24
*> Next Hop 192.168.2.2
     MED: -, LocalPref: -, Type: Internal route
     Origin: IGP
     Path: 65531
     Next Hop Attribute: 10.1.2.1
     Communities: 1000:1001
```

22.4.3　マルチパスの確認

(1)　運用コマンド一覧

マルチパスの運用コマンド一覧を次の表に示します。

表 22-35　運用コマンド一覧

コマンド名	説明
show ip route	ルーティングテーブルで保持する IPv4 経路情報を表示します。
show ip bgp	BGP4 プロトコルに関する情報を表示します。
show ipv6 route	ルーティングテーブルで保持する IPv6 経路情報を表示します。
show ipv6 bgp	BGP4+プロトコルに関する情報を表示します。

(2)　マルチパスの表示

マルチパスの設定は，show ip route コマンドまたは show ipv6 route コマンドで表示します。

図 22-33　show ip route コマンドの実行結果

```
> show ip route
Date 20XX/03/20 21:40:39 UTC
Total: 19 routes
Destination       Next Hop        Interface     Metric   Protocol  Age
10.10/16          172.17.2.2      Eth1/6        -/-      BGP       33m 31s  <-1
                  172.16.2.2      Eth1/5        -        -         -
10.20/16          172.17.2.2      Eth1/6        -/-      BGP       33m 31s  <-2
                  172.16.2.2      Eth1/5        -        -         -
172.17/16         172.17.2.2      Eth1/6        0/0      Connected 42m 43s
172.17.2.1/32     172.17.2.2      Eth1/6        0/0      Connected 42m 43s
172.16/16         172.16.2.2      Eth1/5        0/0      Connected 42m 43s
172.16.2.1/32     172.16.2.2      Eth1/5        0/0      Connected 42m 43s
172.20/16         172.17.2.2      Eth1/6        -/-      BGP        3s      <-3
                  172.16.2.2      Eth1/5        -        -         -
172.30/16         172.17.2.2      Eth1/6        -/-      BGP        3s      <-4
                  172.16.2.2      Eth1/5        -        -         -
192.168.1.100/32  192.168.1.100   loopback0     0/0      Connected 42m 45s
```

1～4.：マルチパス化された経路です。

22.4.4　サポート機能のネゴシエーションの確認

(1)　運用コマンド一覧

サポート機能のネゴシエーションの運用コマンド一覧を次の表に示します。

表 22-36　運用コマンド一覧

コマンド名	説明
show ip bgp	BGP4 プロトコルに関する情報を表示します。
show ipv6 bgp	BGP4+プロトコルに関する情報を表示します。

(2)　ネゴシエーションの確認

サポート機能のネゴシエーションは, show ip bgp コマンドまたは show ipv6 bgp コマンドで neighbors パラメータに detail を指定して表示します。

図 22-34　show ip bgp コマンド（neighbors detail パラメータ指定）の実行結果

```
> show ip bgp neighbors detail
Date 20XX/03/17 15:52:14 UTC
BGP Peer: 10.1.2.2       , Remote AS: 65531
Remote Router ID: 10.1.2.102
    BGP Status: Established         HoldTime: 180  , Keepalive: 60
    Established Transitions: 1      Established Date: 20XX/03/17 15:51:00
    BGP Version: 4                  Type: Internal
    Local Address: 10.1.2.1         Local AS: 65531
    Local Router ID: 192.168.1.100
    Next Connect Retry: -           Connect Retry Timer: -
    Last Keep Alive Sent: 15:52:00  Last Keep Alive Received: 15:52:00
    BGP Message  UpdateIn   UpdateOut  TotalIn    TotalOut
                 0          0          2          4
    BGP Capability Negotiation: <IPv4-Uni Refresh Refresh(v)>            <-1
      Send   : <IPv4-Uni Refresh Refresh(v)>
      Receive: <IPv4-Uni Refresh Refresh(v)>
    Password: UnConfigured
    Track Name: -, Track ID: -, Track State: -
BGP Peer: 192.168.2.2    , Remote AS: 65531
```

```
Remote Router ID: 192.168.1.102
    BGP Status: Established         HoldTime: 180  , Keepalive: 60
    Established Transitions: 1      Established Date: 20XX/03/17 15:50:43
    BGP Version: 4                  Type: Internal
    Local Address: 192.168.2.1      Local AS: 65531
    Local Router ID: 192.168.1.100
    Next Connect Retry: -           Connect Retry Timer: -
    Last Keep Alive Sent: 15:51:43  Last Keep Alive Received: 15:51:43
    BGP Message  UpdateIn   UpdateOut  TotalIn    TotalOut
                 0          0          2          4
    BGP Capability Negotiation: <IPv4-Uni Refresh>                          <-2
      Send   : <IPv4-Uni Refresh Refresh(v)>
      Receive: <IPv4-Uni Refresh >
    Password: UnConfigured
    Track Name: -, Track ID: -, Track State: -

BGP Peer: 10.2.2.2       , Remote AS: 65533
Remote Router ID: 10.2.2.102
    BGP Status: Established         HoldTime: 180  , Keepalive: 60
    Established Transitions: 1      Established Date: 20XX/03/17 15:50:30
    BGP Version: 4                  Type: External
    Local Address: 10.1.2.1         Local AS: 65531
    Local Router ID: 192.168.1.100
    Next Connect Retry: -           Connect Retry Timer: -
    Last Keep Alive Sent: 15:51:30  Last Keep Alive Received: 15:51:30
    BGP Message  UpdateIn   UpdateOut  TotalIn    TotalOut
                 0          0          2          4
    BGP Capability Negotiation: <IPv4-Uni>                                  <-3
      Send   : <IPv4-Uni Refresh Refresh(v)>
      Receive: <IPv4-Uni>
    Password: UnConfigured
    Fast-external-fallover : Enabled
    Track Name: -, Track ID: -, Track State: -

BGP Peer: 172.16.2.2     , Remote AS: 65532
Remote Router ID: 172.16.1.102
    BGP Status: Established         HoldTime: 180  , Keepalive: 60
    Established Transitions: 1      Established Date: 20XX/03/17 15:49:35
    BGP Version: 4                  Type: External
    Local Address: 172.16.2.1       Local AS: 65531
    Local Router ID: 192.168.1.100
    Next Connect Retry: -           Connect Retry Timer: -
    Last Keep Alive Sent: 15:51:35  Last Keep Alive Received: 15:51:35
    BGP Message  UpdateIn   UpdateOut  TotalIn    TotalOut
                 0          0          3          5
    BGP Capability Negotiation: <>                                          <-4
      Send   : <IPv4-Uni Refresh Refresh(v)>
      Receive: <>
    Password: UnConfigured
    Fast-external-fallover : Enabled
    Track Name: -, Track ID: -, Track State: -

>
```

1. IPv4-Uni:「IPv4 ユニキャスト経路の送受信」，Refresh:「ルート・リフレッシュ（RFC2918 準拠)」，Refresh(v):「ルート・リフレッシュ（Capability Code=128)」についてネゴシエーションが成立しています。
2. IPv4-Uni:「IPv4 ユニキャスト経路の送受信」，Refresh:「ルート・リフレッシュ（RFC2918 準拠)」についてネゴシエーションが成立しています。
3. IPv4-Uni:「IPv4 ユニキャスト経路の送受信」についてネゴシエーションが成立しています。
4. 成立しているサポート機能のネゴシエーションがありません。

22.4.5 ルート・リフレッシュの確認

(1) 運用コマンド一覧

ルート・リフレッシュの運用コマンド一覧を次の表に示します。

表 22-37　運用コマンド一覧

コマンド名	説明
show ip route	ルーティングテーブルで保持する IPv4 経路情報を表示します。
show ip bgp	BGP4 プロトコルに関する情報を表示します。
clear ip bgp	BGP4 セッションもしくは BGP4 プロトコルに関する情報のクリア，または新しい BGP フィルタ情報を使用して受信経路と送信経路のフィルタリングをします。
show ipv6 route	ルーティングテーブルで保持する IPv6 経路情報を表示します。
show ipv6 bgp	BGP4+プロトコルに関する情報を表示します。
clear ipv6 bgp	BGP4+セッションもしくは BGP4+プロトコルに関する情報のクリア，または新しい BGP フィルタ情報を使用して受信経路と送信経路のフィルタリングをします。

(2)　ルート・リフレッシュのネゴシエーションの確認

まず，show ip bgp コマンドまたは show ipv6 bgp コマンドで neighbors パラメータを指定して，BGP 経路の再広告要求をするピア間でルート・リフレッシュのネゴシエーションが成立していることを確認します。ネゴシエーションが成立していない場合は経路再学習のためのルート・リフレッシュ要求をしません。

図 22-35　show ip bgp コマンド（neighbors パラメータ指定）の実行結果

```
> show ip bgp neighbors 172.16.2.2
Date 20XX/03/17 15:52:14 UTC
BGP Peer: 172.16.2.2     , Remote AS: 65532
Remote Router ID: 172.16.1.102
    BGP Status: Established         HoldTime: 180  , Keepalive: 60
    Established Transitions: 1      Established Date: 20XX/03/17 15:49:35
    BGP Version: 4                  Type: External
    Local Address: 172.16.2.1       Local AS: 65531
    Local Router ID: 192.168.1.100
    Next Connect Retry: -           Connect Retry Timer: -
    Last Keep Alive Sent: 15:51:35  Last Keep Alive Received: 15:51:35
    BGP Message  UpdateIn   UpdateOut  TotalIn    TotalOut
                 1          1          4          6
    BGP Capability Negotiation: <IPv4-Uni Refresh Refresh(v)>            <-1
      Send   : <IPv4-Uni Refresh Refresh(v)>
      Receive: <IPv4-Uni Refresh Refresh(v)>
    Password: UnConfigured
    Fast-external-fallover : Enabled
    Track Name: -, Track ID: -, Track State: -
```

1. ルート・リフレッシュのネゴシエーションが成立しています。

(3)　BGP 経路の再広告要求と再広告

全ピアに対して BGP 経路の再広告要求と再広告をする場合は，clear ip bgp コマンドまたは clear ipv6 bgp コマンドで* both パラメータを指定します。

図 22-36　clear ip bgp コマンドの実行結果

```
#clear ip bgp * both
```

(4)　BGP 経路の再学習と再広告の確認

ルート・リフレッシュによる BGP 経路の再学習と再広告は，show ip bgp コマンドまたは show ipv6 bgp コマンドで neighbors パラメータを指定して確認します。

図 22-37　show ip bgp コマンド（neighbors パラメータ指定）の実行結果

```
> show ip bgp neighbors 172.16.2.2
Date 20XX/03/17 15:58:12 UTC
BGP Peer: 172.16.2.2     , Remote AS: 65532
Remote Router ID: 172.16.1.102
    BGP Status: Established         HoldTime: 180  , Keepalive: 60
    Established Transitions: 1      Established Date: 20XX/03/17 15:49:35
    BGP Version: 4                  Type: External
    Local Address: 172.16.2.1       Local AS: 65531
    Local Router ID: 192.168.1.100
    Next Connect Retry: -           Connect Retry Timer: -
    Last Keep Alive Sent: 15:57:35  Last Keep Alive Received: 15:57:35
    BGP Message  UpdateIn   UpdateOut  TotalIn    TotalOut
                 2          2          11          14                    <-1
    BGP Capability Negotiation: <IPv4-Uni Refresh Refresh(v)>
      Send   : <IPv4-Uni Refresh Refresh(v)>
      Receive: <IPv4-Uni Refresh Refresh(v)>
    Password: UnConfigured
    Fast-external-fallover : Enabled
    Track Name: -, Track ID: -, Track State: -
```

1.受信 UPDATE メッセージ数と送信 UPDATE メッセージ数が増加しています。

[注意事項]

clear ip bgp コマンドおよび clear ipv6 bgp コマンド（* in，* out，* both 指定）は経路フィルタの変更反映とルート・リフレッシュ（「22.1.5　ルート・リフレッシュ」参照）の両方を実行します。ルート・リフレッシュのネゴシエーションが成立していない場合，経路再学習のためのルート・リフレッシュ要求はしませんが，経路フィルタの変更は反映します。

22.4.6　TCP MD5 認証の確認

(1)　運用コマンド一覧

TCP MD5 認証の運用コマンド一覧を次の表に示します。

表 22-38　運用コマンド一覧

コマンド名	説明
show ip bgp	BGP4 プロトコルに関する情報を表示します。
show ipv6 bgp	BGP4+プロトコルに関する情報を表示します。

(2)　TCP MD5 認証の確認

TCP MD5 認証は，show ip bgp コマンドまたは show ipv6 bgp コマンドで neighbors パラメータに detail を指定して表示します。

図 22-38　show ip bgp コマンド（neighbors detail パラメータ指定）の実行結果

```
> show ip bgp neighbors detail
Date 20XX/03/07 21:24:24 UTC
BGP Peer: 192.168.2.2    , Remote AS: 65531
Remote Router ID: 192.168.2.100
    BGP Status: Established         HoldTime: 180  , Keepalive: 60
    Established Transitions: 1      Established Date: 20XX/03/07 21:23:48
    BGP Version: 4                  Type: Internal
    Local Address: 192.168.2.1      Local AS: 65531
    Local Router ID: 192.168.1.100
    Next Connect Retry: -           Connect Retry Timer: -
    Last Keep Alive Sent: 21:23:48  Last Keep Alive Received: 21:23:48
    BGP Message  UpdateIn   UpdateOut  TotalIn    TotalOut
                 0          0          0          3
    BGP Capability Negotiation: <IPv4-Uni Refresh Refresh(v)>
```

```
      Send   : <IPv4-Uni Refresh Refresh(v)>
      Receive: <IPv4-Uni Refresh Refresh(v)>
    Password: UnConfigured                                          <-1
    Track Name: -, Track ID: -, Track State: -

BGP Peer: 172.16.2.2     , Remote AS: 65532
Remote Router ID: 172.16.2.100
    BGP Status: Established         HoldTime: 180  , Keepalive: 60
    Established Transitions: 1      Established Date: 20XX/03/07 21:23:58
    BGP Version: 4                  Type: External
    Local Address: 172.16.2.1       Local AS: 65531
    Local Router ID: 192.168.1.100
    Next Connect Retry: -           Connect Retry Timer: -
    Last Keep Alive Sent: 21:23:58  Last Keep Alive Received: 21:23:58
    BGP Message  UpdateIn   UpdateOut  TotalIn    TotalOut
                 0          0          1          3
    BGP Capability Negotiation: <IPv4-Uni Refresh Refresh(v)>
      Send   : <IPv4-Uni Refresh Refresh(v)>
      Receive: <IPv4-Uni Refresh Refresh(v)>
    Password: Configured                                            <-2
    Fast-external-fallover : Enabled
    Track Name: -, Track ID: -, Track State: -
```

1. 相手側アドレスが 192.168.2.2 とのピア接続で MD5 認証を適用していません。
2. 相手側アドレスが 172.16.2.2 とのピア接続で MD5 認証を適用しています。

[注意事項]

TCP MD5 認証が失敗した場合はピアが確立しません（BGP Status が Established 状態以外）。TCP MD5 認証が失敗したかどうかはシステムメッセージを確認してください。

22.4.7　広告用経路生成の確認

(1)　運用コマンド一覧

広告用経路生成の運用コマンド一覧を次の表に示します。

表 22-39　運用コマンド一覧

コマンド名	説明
show ip route	ルーティングテーブルで保持する IPv4 経路情報を表示します。
show ip bgp	BGP4 プロトコルに関する情報を表示します。
show ipv6 route	ルーティングテーブルで保持する IPv6 経路情報を表示します。
show ipv6 bgp	BGP4+プロトコルに関する情報を表示します。

(2)　生成した広告用経路の表示

生成した広告用経路は，show ip bgp コマンドまたは show ipv6 bgp コマンドで表示します。この例では，172.16/16 と 192.168.20/24 が生成した BGP4 広告用経路です。

図 22-39　show ip bgp コマンドの実行結果

```
> show ip bgp
Date 20XX/03/20 22:43:26 UTC
Local AS: 65531, Local Router ID: 192.168.1.100
Status Codes: d dampened, * valid, > active, S Stale, r RIB failure
Origin Codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop        MED    LocalPref Weight Path
*  172.16/16          ----            -      100       0      i
*  192.168.20/24      ----            -      100       0      i
```

(3)　広告用経路の広告表示

生成した広告用経路が広告されていることは，show ip bgp コマンドまたは show ipv6 bgp コマンドで advertised-routes パラメータを指定して確認します。

図 22-40　show ip bgp コマンド（advertised-routes パラメータ指定）の実行結果

```
> show ip bgp advertised-routes 172.16/16
Date 20XX/03/20 22:44:54 UTC
BGP Peer: 172.16.2.2    , Remote AS: 65532
Local AS: 65531, Local Router ID: 192.168.1.100
Status Codes: d dampened, * valid, > active, S Stale, r RIB failure
Route 172.16/16
*  Next Hop ----
     MED: -, LocalPref: -, Type: Internal route
     Origin: IGP
     Path: 65531
     Next Hop Attribute: 172.16.2.1

> show ip bgp advertised-routes 192.168.20/24
Date 20XX/03/18 22:44:58 UTC
BGP Peer: 172.16.2.2     , Remote AS: 65532
Local AS: 65531, Local Router ID: 192.168.1.100
Status Codes: d dampened, * valid, > active, S Stale, r RIB failure
Route 192.168.20/24
*  Next Hop ----
     MED: -, LocalPref: -, Type: Internal route
     Origin: IGP
     Path: 65531
     Next Hop Attribute: 172.16.2.1
```

22.4.8　ルート・フラップ・ダンプニングの確認

(1)　運用コマンド一覧

ルート・フラップ・ダンプニングの運用コマンド一覧を次の表に示します。

表 22-40　運用コマンド一覧

コマンド名	説明
show ip route	ルーティングテーブルで保持する IPv4 経路情報を表示します。
show ip bgp	BGP4 プロトコルに関する情報を表示します。
clear ip bgp	抑止されている BGP4 経路の抑止状態の解除や，ルート・フラップ統計情報をクリアします。
show ipv6 route	ルーティングテーブルで保持する IPv6 経路情報を表示します。
show ipv6 bgp	BGP4+プロトコルに関する情報を表示します。
clear ipv6 bgp	抑止されている BGP4+経路の抑止状態の解除や，ルート・フラップ統計情報をクリアします。

(2)　ルート・フラップ・ダンプニングの確認

ルート・フラップ・ダンプニングによって抑止されている経路は，show ip bgp コマンドまたは show ipv6 bgp コマンドで dampened-routes パラメータ（グローバルネットワークだけ）を指定して表示します。

図 22-41　show ip bgp コマンド（dampened-routes パラメータ指定）の実行結果

```
>show ip bgp neighbors 172.16.2.2 dampened-routes
Date 20XX/01/17 11:53:14 UTC
Status Codes: d dampened, h history, * valid, > active
   Network            Peer Address      ReUse
```

```
 d 172.20.211/24      172.16.2.2        00:07:11                      <-1
 d 172.21.211/24      172.16.2.2        00:19:10                      <-1
```

1.ルート・フラップ・ダンプニングによって使用が抑止されている経路です。

フラップが発生している経路は，show ip bgp コマンドまたは show ipv6 bgp コマンドで flap-statistics パラメータ（グローバルネットワークだけ）を指定して表示します。

図 22-42　show ip bgp コマンド（flap-statistics パラメータ指定）の実行結果

```
>show ip bgp flap-statistics
Date 20XX/01/17 11:56:28 UTC
Status Codes: d dampened, h history, * valid, > active
   Network           Peer Address    Flaps      Duration ReUse    Penalty
 d 172.20.211/24     172.16.2.2      114        00:12:30 00:07:11 5.0
 d 172.21.212/24     172.16.2.2      108        00:12:30 00:19:10 4.0
 h 172.27.119/24     192.168.2.2     2          00:11:20          1.7
 h 172.27.191/24     192.168.2.2     2          00:11:20          1.7
*> 172.30.189/24     192.168.79.188  1          00:05:10          0.6
*> 172.30.192/24     192.168.79.188  3          00:05:10          0.6
>
```

22.4.9　ルート・リフレクションの確認

(1)　運用コマンド一覧

ルート・リフレクションの運用コマンド一覧を次の表に示します。

表 22-41　運用コマンド一覧

コマンド名	説明
show ip route	ルーティングテーブルで保持する IPv4 経路情報を表示します。
show ip bgp	BGP4 プロトコルに関する情報を表示します。
show ipv6 route	ルーティングテーブルで保持する IPv6 経路情報を表示します。
show ipv6 bgp	BGP4+プロトコルに関する情報を表示します。

(2)　ルート・リフレクションの確認

ルート・リフレクタ・クライアントは，show ip bgp コマンドまたは show ipv6 bgp コマンドで neighbors パラメータに detail を指定して表示します。

図 22-43　show ip bgp コマンド（neighbors detail パラメータ指定）の実行結果

```
> show ip bgp neighbors detail
Date 20XX/03/17 15:52:14 UTC
BGP Peer: 192.168.2.2       , Remote AS: 65531
Remote Router ID: 192.168.100.2
    BGP Status: Established         HoldTime: 180  , Keepalive: 60
    Established Transitions: 1      Established Date: 20XX/03/17 15:51:00
    BGP Version: 4                  Type: Internal RRclient             <-1
    Local Address: 192.168.2.1      Local AS: 65531
    Local Router ID: 192.168.1.100
    Next Connect Retry: -           Connect Retry Timer: -
    Last Keep Alive Sent: 15:52:00  Last Keep Alive Received: 15:52:00
    BGP Message  UpdateIn   UpdateOut  TotalIn    TotalOut
                 0          0          2          4
    BGP Capability Negotiation: <IPv4-Uni Refresh Refresh(v)>
      Send   : <IPv4-Uni Refresh Refresh(v)>
      Receive: <IPv4-Uni Refresh Refresh(v)>
    Password: UnConfigured
    Fast-external-fallover : Enabled
    Track Name: -, Track ID: -, Track State: -
```

```
        :
        :
>
```

1.ルート・リフレクタ・クライアントとして指定されています。

リフレクトした経路は，show ip bgp コマンドまたは show ipv6 bgp コマンドで advertised-routes パラメータを指定して表示します。

図 22-44　show ip bgp コマンド（advertised-routes パラメータ指定）の実行結果

```
> show ip bgp advertised-routes
Date 20XX/01/17 22:44:54 UTC
BGP Peer: 192.168.3.2       , Remote AS: 65531
Local AS: 65531, Local Router ID: 192.168.1.100
Origin Codes: i - IGP, e - EGP, ? - incomplete
Network              Next Hop        MED    LocalPref Path
192.168.20/24        192.168.2.2     120    100       i
192.168.30/24        192.168.2.2     100    100       i
BGP Peer: 192.168.4.2       , Remote AS: 65531
Local AS: 65531, Local Router ID: 192.168.1.100
Origin Codes: i - IGP, e - EGP, ? - incomplete
Network              Next Hop        MED    LocalPref Path
192.168.20/24        192.168.2.2     120    100       65532 i
192.168.30/24        192.168.2.2     100    100       65532 i
```

22.4.10　コンフェデレーションの確認

(1)　運用コマンド一覧

コンフェデレーションの運用コマンド一覧を次の表に示します。

表 22-42　運用コマンド一覧

コマンド名	説明
show ip route	ルーティングテーブルで保持する IPv4 経路情報を表示します。
show ip bgp	BGP4 プロトコルに関する情報を表示します。
show ipv6 route	ルーティングテーブルで保持する IPv6 経路情報を表示します。
show ipv6 bgp	BGP4+プロトコルに関する情報を表示します。

(2)　コンフェデレーションの確認

コンフェデレーションは，show ip bgp コマンドまたは show ipv6 bgp コマンドで neighbors パラメータに detail を指定して表示します。

図 22-45　show ip bgp コマンド（neighbors detail パラメータ指定）の実行結果

```
> show ip bgp neighbors detail
Date 20XX/03/17 15:52:14 UTC
BGP Peer: 192.168.2.2    , Remote AS: 64512                              <-2
Remote Router ID: 192.168.100.2
    BGP Status: Established         HoldTime: 180  , Keepalive: 60
    Established Transitions: 1      Established Date: 20XX/03/17 15:51:00
    BGP Version: 4                  Type: Internal
    Local Address: 192.168.2.1      Local AS: 64512
    Local Router ID: 192.168.1.100
    Next Connect Retry: -           Connect Retry Timer: -
    Last Keep Alive Sent: 15:52:00  Last Keep Alive Received: 15:52:00
    BGP Message  UpdateIn   UpdateOut  TotalIn    TotalOut
                 0          0          2          4
    BGP Capability Negotiation: <IPv4-Uni Refresh Refresh(v)>
      Send   : <IPv4-Uni Refresh Refresh(v)>
```

```
      Receive: <IPv4-Uni Refresh Refresh(v)>
    Password: UnConfigured
    Track Name: -, Track ID: -, Track State: -

Confederation ID: 65531, Member AS: 64512                              <-1
BGP Peer: 192.168.4.2    , Remote AS: 64513                            <-2
Remote Router ID: 192.168.1.104
    BGP Status: Established         HoldTime: 180  , Keepalive: 60
    Established Transitions: 1      Established Date: 20XX/03/17 15:50:30
    BGP Version: 4                  Type: ConfedExt                    <-3
    Local Address: 192.168.4.1      Local AS: 64512
    Local Router ID: 192.168.1.100
    Next Connect Retry: -           Connect Retry Timer: -
    Last Keep Alive Sent: 15:51:30  Last Keep Alive Received: 15:51:30
    BGP Message  UpdateIn   UpdateOut  TotalIn    TotalOut
                 0          0          2          4
    BGP Capability Negotiation: <IPv4-Uni Refresh>
      Send   : <IPv4-Uni Refresh Refresh(v)>
      Receive: <IPv4-Uni Refresh Refresh(v)>
    Password: UnConfigured
    Track Name: -, Track ID: -, Track State: -
       :
       :
>
```

1. 自ルータがコンフェデレーションのメンバー AS に属しています。
2. 接続先のメンバー AS 番号を表示します。
3. 接続先ピア種別がメンバー AS 間ピアです。

22.4.11　ノンストップルーティングの確認

(1)　運用コマンド一覧

ノンストップルーティングの運用コマンド一覧を次の表に示します。

表 22-43　運用コマンド一覧

コマンド名	説明
show ip bgp	BGP4 プロトコルに関する情報を表示します。
show ipv6 bgp	BGP4+プロトコルに関する情報を表示します。
show nsr unicast※	ユニキャストルーティングプロトコルのノンストップルーティングの動作状態を表示します。

注※
「運用コマンドレファレンス Vol.3　12. IPv4・IPv6 ルーティングプロトコル共通」を参照してください。

(2)　ノンストップルーティングの確認

ノンストップルーティングを適用していることは, show ip bgp コマンドまたは show ipv6 bgp コマンドで neighbors パラメータに detail を指定して確認します。

図 22-46　show ip bgp コマンド（neighbors detail パラメータ指定）の実行結果

```
> show ip bgp neighbors detail
Date 20XX/04/17 15:52:14 UTC
BGP Peer: 192.168.2.2       , Remote AS: 65531
Remote Router ID: 192.168.100.2
    BGP Status: Established         HoldTime: 180  , Keepalive: 60
    Established Transitions: 1      Established Date: 20XX/04/17 15:51:00
    BGP Version: 4                  Type: Internal
    Local Address: 192.168.2.1      Local AS: 65531
```

```
Local Router ID: 192.168.1.100
Next Connect Retry: -           Connect Retry Timer: -
Last Keep Alive Sent: 15:52:00  Last Keep Alive Received: 15:52:00
Nonstop Routing: Enable,        Sync Status: Synchronized           <-1
BGP Message  UpdateIn   UpdateOut  TotalIn    TotalOut
             0          0          2          4
BGP Capability Negotiation: <IPv4-Uni Refresh Refresh(v)>
  Send   : <IPv4-Uni Refresh Refresh(v)>
  Receive: <IPv4-Uni Refresh Refresh(v)>
Password: UnConfigured
Track Name: -, Track ID: -, Track State: -
  :
  :
```

1.ノンストップルーティングが動作しています。また，他系 BCU 間で同期が完了しています。

他系 BCU との同期状態の詳細は，show ip bgp コマンドまたは show ipv6 bgp コマンドで nsr パラメータを指定して確認します。BGP ピア単位の同期状態が表示されます。

図 22-47　show ip bgp コマンド（nsr パラメータ指定）の実行結果

```
> show ip bgp nsr
Date 20XX/01/17 19:12:23 UTC
Local AS: 65531, Local Router ID: 192.168.1.100
BGP Peer        Peer AS     Status         Progress         Sync Time
192.0.2.1       64496       Synchronizing  3/10             -
192.0.2.2       64511       Asynchronous   -                -
172.16.0.1      65551       Synchronized   -                20XX/03/08 10:18:43
>
```

ユニキャストルーティングプロトコルのノンストップルーティングの動作状態は，show nsr unicast コマンドで表示します。

図 22-48　show nsr unicast コマンドの実行結果

```
>show nsr unicast
Date 20XX/04/14 12:00:00 UTC
Status:  Synchronized
Protocol      Total    Asynchronous    Synchronizing   Synchronized
BGP4          5        0               0               5
OSPF          10       0               0               10
BGP4+         5        0               0               5
OSPFv3        10       0               0               10
>
```

22.4.12　グレースフル・リスタートの確認

(1)　運用コマンド一覧

グレースフル・リスタートの運用コマンド一覧を次の表に示します。

表 22-44　運用コマンド一覧

コマンド名	説明
show ip route	ルーティングテーブルで保持する IPv4 経路情報を表示します。
show ip bgp	BGP4 プロトコルに関する情報を表示します。
show ipv6 route	ルーティングテーブルで保持する IPv6 経路情報を表示します。
show ipv6 bgp	BGP4+プロトコルに関する情報を表示します。
show graceful-restart unicast※	ユニキャストルーティングプロトコルのグレースフル・リスタートのリスタートルータの動作状態を表示します。

注※

「運用コマンドレファレンス Vol.3　12. IPv4・IPv6 ルーティングプロトコル共通」を参照してください。

(2) グレースフル・リスタートの確認

グレースフル・リスタートを適用していることは，show ip bgp コマンドまたは show ipv6 bgp コマンドで neighbors パラメータに detail を指定して確認します。

図 22-49　show ip bgp コマンド（neighbors detail パラメータ指定）の実行結果

```
> show ip bgp neighbors detail
Date 20XX/04/17 15:52:14 UTC
BGP Peer: 192.168.2.2       , Remote AS: 65531
Remote Router ID: 192.168.100.2
    BGP Status: Established         HoldTime: 180  , Keepalive: 60
    Established Transitions: 1      Established Date: 20XX/04/17 15:51:00
    BGP Version: 4                  Type: Internal
    Local Address: 192.168.2.1      Local AS: 65531
    Local Router ID: 192.168.1.100
    Next Connect Retry: -           Connect Retry Timer: -
    Last Keep Alive Sent: 15:52:00  Last Keep Alive Received: 15:52:00
    Graceful Restart: Both                                          <-1
      Last Restart Status : Finished    20XX/04/16 18:41:35
      Last Receive Status : Finished    20XX/04/16 19:11:12
       Stalepath-Time: 30

    BGP Message  UpdateIn   UpdateOut  TotalIn    TotalOut
                 0          0          2          4
    BGP Capability Negotiation: <IPv4-Uni Refresh Refresh(v) GracefulRestart ><-2
      Send   : <IPv4-Uni Refresh Refresh(v) GracefulRestart(RestartTime:120s)>
      Receive: <IPv4-Uni Refresh Refresh(v) GracefulRestart(RestartTime:120s, IPv4-uni)>
    Password: UnConfigured
    Track Name: -, Track ID: -, Track State: -
      :
      :
```

1. グレースフル・リスタートのリスタートルータおよびレシーブルータとして動作します。
2. BGP セッション接続時にグレースフル・リスタートのネゴシエーションが成立しています。

グレースフル・リスタートを適用している場合で経路の送信元ルータがリスタート中の経路は，show ip bgp コマンドまたは show ipv6 bgp コマンドで表示します。

図 22-50　show ip bgp コマンドの実行結果

```
> show ip bgp
Date 20XX/01/17 19:12:23 UTC
Local AS: 65531, Local Router ID: 192.168.1.100
Status Codes: d dampened, * valid, > active , S Stale, r RIB failure
Origin Codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop     MED   LocalPref Weight Path
S  10.10/16         172.16.2.2   -     120       20     65532 65528 i    <-1
S  10.20/16         172.16.2.2   -     80        20     65532 65528 i    <-1
*> 172.20/16        192.168.2.2  -     100       10     65530    i
*  172.30/16        192.168.2.2  100   100       10     65530 i
*  192.168.10/24    192.168.2.2  -     100       10     65530 i
*> 192.168.20/24    192.168.2.2  -     100       10           i
*> 192.168.30/24    192.168.2.2  -     100       10           i
```

1. 経路の送信元ルータがリスタート中の経路です。

ユニキャストルーティングプロトコルのグレースフル・リスタートの動作状態は，show graceful-restart unicast コマンドで表示します。

図 22-51　show graceful-restart unicast コマンドの実行結果

```
>show graceful-restart unicast
Date 20XX/04/17 12:00:00 UTC
Status: Completed
```

```
Graceful Restart Time Limit: 180s
Start Time: 20XX/04/08 17:01:23
End Time  : 20XX/04/08 17:01:30
OSPF  : Restart State <Finished>
        Total of Domain: 2 (Succeeded: 2)
BGP   : Restart State <Finished>
        Total of Peer  : 25 (Succeeded: 25)
OSPFv3: Restart State <Finished>
        Total of Domain: 2 (Succeeded: 2)
BGP4+ : Restart State <Finished>
        Total of Peer  : 20 (Succeeded: 20)
```

22.4.13　学習経路数制限の確認

(1)　運用コマンド一覧

学習経路数制限の運用コマンド一覧を次の表に示します。

表 22-45　運用コマンド一覧

コマンド名	説明
show ip route	ルーティングテーブルで保持する IPv4 経路情報を表示します。
show ip bgp	BGP4 プロトコルに関する情報を表示します。
clear ip bgp	学習経路数制限によって切断している BGP4 セッションを再接続します。
show ipv6 route	ルーティングテーブルで保持する IPv6 経路情報を表示します。
show ipv6 bgp	BGP4+プロトコルに関する情報を表示します。
clear ipv6 bgp	学習経路数制限によって切断している BGP4+セッションを再接続します。

(2)　学習経路数制限およびピアから学習している経路数の確認

学習経路数制限およびピアから学習している経路数（アクティブ経路と非アクティブ経路の合計）は，show ip bgp コマンドまたは show ipv6 bgp コマンドで neighbors パラメータに<as>，<peer address>，<host name>，または detail を指定して確認します。

図 22-52　show ip bgp コマンド（neighbors detail パラメータ指定）の実行結果

```
>show ip bgp neighbors detail
 Date 20XX/03/17 18:45:09
 BGP Peer: 172.16.2.2, Remote AS: 65532
 Remote Router ID: 172.16.2.200
     BGP Status: Idle                HoldTime: 90   , Keepalive: 60
     Established Transitions: 1      Established Date: 20XX/03/16 18:42:26<-1
     BGP Version: 4                  Type: External
     Local Address: 172.16.23.214,  Local AS: 65531
     Local Router ID: 172.16.2.100
     Next Connect Retry: -,          Connect Retry Timer: -
     Last Keep Alive Sent: 18:42:20, Last Keep Alive Received: 18:42:20
     NLRI of End-of-RIB Marker: Advertised and Received
     BGP Message  UpdateIn UpdateOut TotalIn TotalOut
                  12       14        36      42
     BGP Peer Last Error: Cease(Over Prefix Limit)                        <-2
     BGP Routes  Accepted     MaximumPrefix RestartTime Threshold         <-3
                 0            10000         60m         80%
     BGP Capability Negotiation: <IPv4-Uni>
       Send   : <IPv4-Uni>
       Receive: <IPv4-Uni>
     Password : Configured
     Fast-external-fallover : Enabled
     Track Name: -, Track ID: -, Track State: -
 BGP Peer: 192.168.2.1, Remote AS: 65531
```

```
Remote Router ID: 192.168.2.200
    BGP Status: Established         HoldTime: 90   , Keepalive: 60
    Established Transitions: 1      Established Date: 20XX/03/16 18:42:31
    BGP Version: 4                  Type: Internal
    Local Address: 192.168.23.214,  Local AS: 65531
    Local Router ID: 192.168.2.100
    Next Connect Retry: 00:32,      Connect Retry Timer: 00:32
    Last Keep Alive Sent: 18:44:31, Last Keep Alive Received: 18:44:31
    NLRI of End-of-RIB Marker: Advertised and Received
    BGP Message  UpdateIn UpdateOut TotalIn TotalOut
                 9        19        51      63
    BGP Routes  Accepted     MaximumPrefix RestartTime Threshold        <-4
                942          1000          none        75%
    BGP Capability Negotiation: <IPv4-Uni>
      Send   : <IPv4-Uni>
      Receive: <IPv4-Uni>
    Password : Configured
    Track Name: -, Track ID: -, Track State: -
```

1. 20XX/03/16 18:42:26 にピアを切断しています。
2. 学習経路数制限によってピアを切断しています。
3. ピアの切断から 60 分後に再接続します。
4. 該当するピアから学習経路数の上限値 1000 に対して 942 の経路を学習しています。

(3)　学習経路数制限によって切断した BGP セッションの再接続

学習経路数制限によって，学習経路数が上限値を超えて切断した BGP セッションは，clear ip bgp コマンドまたは clear ipv6 bgp コマンドで*，<peer address>，または<host name>パラメータを指定して再接続します。

図 22-53　clear ip bgp コマンド（<peer address>パラメータ指定）の実行結果

```
>clear ip bgp 172.16.2.2
>
```

22.4.14　インタフェースダウン時の外部ピア即時切断機能の確認

(1)　運用コマンド一覧

インタフェースダウン時の外部ピア即時切断機能の運用コマンド一覧を次の表に示します。

表 22-46　運用コマンド一覧

コマンド名	説明
show ip bgp	BGP4 プロトコルに関する情報を表示します。
show ipv6 bgp	BGP4+プロトコルに関する情報を表示します。

(2)　インタフェースダウン時の外部ピア即時切断機能の確認

インタフェースダウン時の外部ピア即時切断機能は，show ip bgp コマンドまたは show ipv6 bgp コマンドで neighbors パラメータに<as>，<peer address>，<host name>，または detail を指定して確認します。

図 22-54　show ip bgp コマンド（neighbors detail パラメータ指定）の実行結果

```
>show ip bgp neighbors detail
 Date 20XX/03/17 18:45:09
 BGP Peer: 172.16.2.2, Remote AS: 65532
 Remote Router ID: 172.16.2.200
     BGP Status: Idle               HoldTime: 90
```

```
    Established Transitions: 1      Established Date: 20XX/03/16 18:42:26
    BGP Version: 4                  Type: External
    Local Address: 172.16.23.214,  Local AS: 65531
    Local Router ID: 172.16.2.100
    Next Connect Retry: -,          Connect Retry Timer: -
    Last Keep Alive Sent: 18:42:20, Last Keep Alive Received: 18:42:20
    NLRI of End-of-RIB Marker: Advertised and Received
    BGP Message  UpdateIn UpdateOut TotalIn TotalOut
                 12       14        36      42
    BGP Capability Negotiation: <IPv4-Uni>
      Send   : <IPv4-Uni>
      Receive: <IPv4-Uni>
    Password : Configured
    Fast-external-fallover : Enabled                                    <-1
    Track Name: -, Track ID: -, Track State: -

BGP Peer: 192.168.2.1, Remote AS: 65531
Remote Router ID: 192.168.2.200
    BGP Status: Established         HoldTime: 90
    Established Transitions: 1      Established Date: 20XX/03/16 18:42:31
    BGP Version: 4                  Type: Internal
    Local Address: 192.168.23.214,  Local AS: 65531
    Local Router ID: 192.168.2.100
    Next Connect Retry: 00:32,      Connect Retry Timer: 00:32
    Last Keep Alive Sent: 18:44:31, Last Keep Alive Received: 18:44:31
    NLRI of End-of-RIB Marker: Advertised and Received
    BGP Message  UpdateIn UpdateOut TotalIn TotalOut
                 9        19        51      63
    BGP Capability Negotiation: <IPv4-Uni>
      Send   : <IPv4-Uni>
      Receive: <IPv4-Uni>
    Password : Configured
    Track Name: -, Track ID: -, Track State: -
```

1.インタフェースダウン時の外部ピア即時切断機能が有効です。なお，この項目は内部ピアの場合は表示しません。

23 経路フィルタリング

この章では，IPv4 ユニキャストルーティングおよび IPv6 ユニキャストルーティングの経路を対象とする，経路フィルタリングの解説と操作方法について説明します。

23.1　解説

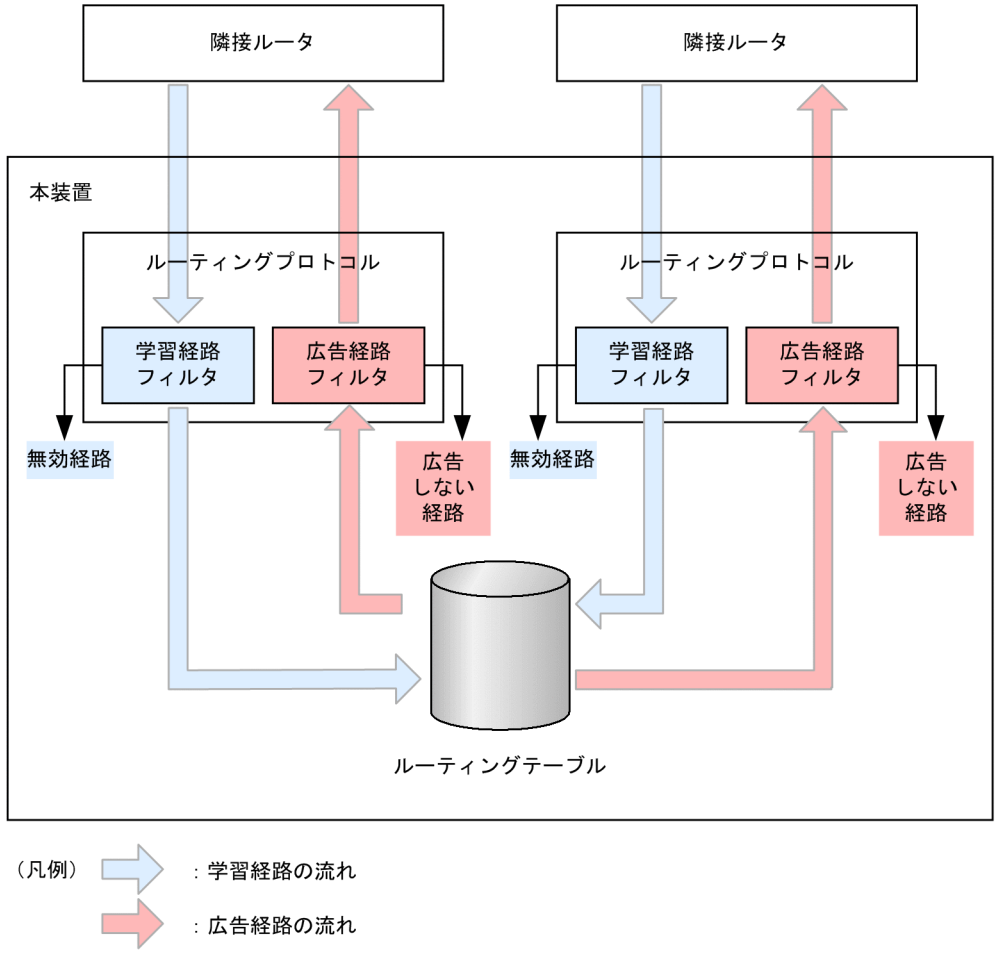
23.1.1　経路フィルタリング概要

経路フィルタリングは，経路をフィルタに通すことで経路を制御する機能です。学習経路フィルタリング，広告経路フィルタリング，およびエクストラネットの経路フィルタリングの３種類があります。

(1)　学習経路と広告経路フィルタリング

学習経路と広告経路の経路フィルタリングの概念を次の図に示します。

図 23–1　経路フィルタリングの概念図



(a)　学習経路フィルタリング

学習経路フィルタリングでは，プロトコルが学習した経路を，プロトコルとルーティングテーブルの間でフィルタします。この機能によって，学習した経路を有効にするかどうかを制御したり，経路の属性値を変更したりできます。

学習経路フィルタリングを設定していない場合，学習した経路はすべて有効経路になります。

(b)　広告経路フィルタリング

広告経路フィルタリングでは，ルーティングテーブルにある経路を，ルーティングテーブルとプロトコルの間でフィルタします。この機能によって，経路を広告するかどうかを制御したり，広告経路の情報を変更したりできます。

広告経路フィルタリングを設定していない場合，プロトコルごとに決まった条件の経路だけを広告します。

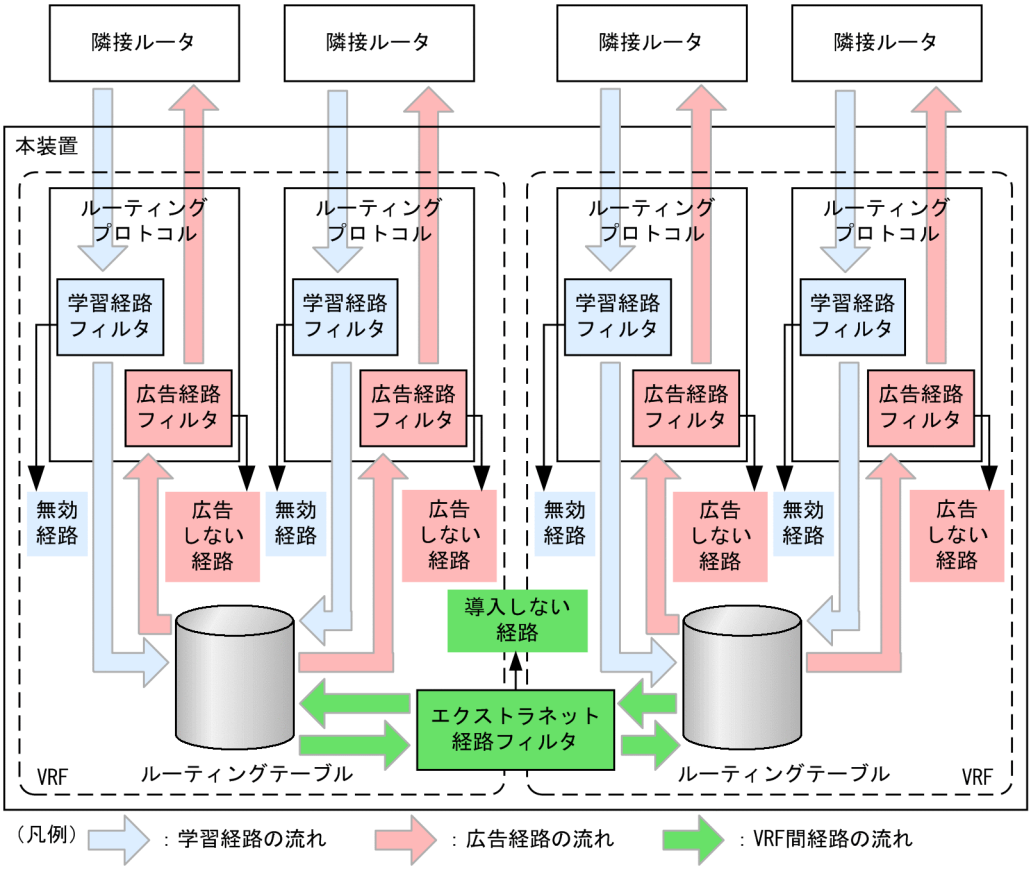
(2)　エクストラネットの経路フィルタリング

エクストラネットを実現するには，異なる VRF 間でアクセスできるような技術が必要です。本装置では，実現の一つの方法として，VRF のルーティングテーブル間で経路情報を交換する方法があります。同時に，エクストラネットの経路フィルタリングをして，交換する経路を VRF のルーティングテーブル間でフィルタします。このフィルタによって，VRF 間で経路を交換するかどうかを制御したり，交換する経路の属性値を変更したりできます。

エクストラネットの経路フィルタリングを設定していない場合，VRF 間で経路を交換しません。

エクストラネットの経路フィルタリングの概念を次の図に示します。

図 23-2　エクストラネットの経路フィルタリングの概念図



なお，エクストラネットの VRF 間で行う経路フィルタリングのことを，VRF 間経路フィルタリングと呼びます。

23.1.2　フィルタ方法

フィルタは，条件を列挙したものです。経路フィルタリング設定にフィルタの識別子を指定することで，学習経路フィルタリングや広告経路フィルタリングにフィルタが適用されます。

本装置で経路フィルタリングに使用できるフィルタには，大きく分けて 2 種類あります。宛先ネットワークだけを条件にするフィルタと，主要な経路属性ほとんどを条件にフィルタして，経路属性も変更できる route-map です。フィルタ方法の概要を次の表に示します。

表 23-1　フィルタ方法の概要

バージョン	フィルタ条件	フィルタの種類
IPv4	宛先ネットワーク	• ip prefix-list • ip access-list
	経路属性	• route-map
	BGP4 経路属性	• ip as-path access-list • ip community-list
IPv6	宛先ネットワーク	• ipv6 prefix-list
	IPv6 アドレス	• ipv6 access-list
	経路属性	• route-map
	BGP4+経路属性	• ip as-path access-list • ip community-list

フィルタの設定では，フィルタの識別子，フィルタ条件，フィルタ条件と一致したときの動作を指定します。動作には，permit（許可）と deny（拒否）のどちらかを選択できます。

一つの識別子に対して，フィルタを複数設定できます。フィルタを評価するときには，指定した識別子のフィルタ設定を設定表示順に評価して，最初に経路とフィルタ条件が一致した設定の動作を採用します。設定表示順は，シーケンス番号を指定できるフィルタではシーケンス番号順，シーケンス番号を指定できないフィルタでは設定順になります。

指定した識別子について経路と動作条件が一致するフィルタ設定がない場合，deny と見なします。これを暗黙の deny といいます。暗黙の deny は，フィルタ条件を設定してあるフィルタの最後にあります。

フィルタ条件の設定が一つもない識別子のフィルタは permit の動作をします。

(1)　宛先ネットワークによるフィルタ

(a)　ip prefix-list，ipv6 prefix-list

ip prefix-list および ipv6 prefix-list は，フィルタ条件としてプレフィックスを指定するフィルタです。これらを経路フィルタリングに使用した場合，経路の宛先ネットワークとプレフィックス条件を比較します。

フィルタ条件として，プレフィックスのほかにマスク長の最大値・最小値を指定できます。経路の宛先ネットワークと比較して，包含し，かつ宛先ネットワークのマスク長が条件に指定したマスク長の範囲内に収まる場合に，一致と見なします。マスク長の範囲を指定しなかった場合，プレフィックス条件のマスク長と完全に一致した場合だけ，一致と見なします。ip prefix-list の比較例および ipv6 prefix-list の比較例をそれぞれ次の表に示します。

表 23-2　ip prefix-list とプレフィックスの比較例

比較対象 プレフィックス	ip prefix-list の条件		
	192.168.0.0/16 マスク長 16 だけ一致	192.168.0.0/16 ge 16 le 24 マスク長 16 以上 24 以下と一致	192.168.0.0/16 ge 8 le 24 マスク長 8 以上 24 以下と一致
0.0.0.0/0	×	×	×
192.0.0.0/8	×	×	○
193.0.0.0/8	×	×	×
192.168.0.0/16	○	○	○
192.169.0.0/16	×	×	×
192.168.43.0/24	×	○	○
192.168.42.3/32	×	×	×

（凡例）○：一致する　×：一致しない

表 23-3　ipv6 prefix-list とプレフィックスの比較例

比較対象 プレフィックス	ipv6 prefix-list の条件		
	2001:db8:f000::/40 マスク長 40 だけ一致	2001:db8:f000::/40 ge 40 le 48 マスク長 40 以上 48 以下と一致	2001:db8:f000::/40 ge 32 le 48 マスク長 32 以上 48 以下と一致
::/0	×	×	×
2001:db8::/32	×	×	○
2001:db8:f000::/36	×	×	○
2001:db8:8000::/36	×	×	×
2001:db8:f000::/40	○	○	○
2001:db8:8000::/48	×	×	×
2001:db8:f000::/48	×	○	○
2001:db8:f000::/64	×	×	×

（凡例）○：一致する　×：一致しない

ip prefix-list を route-map の match ip address から，ipv6 prefix-list を route-map の match ipv6 address から，経路宛先条件として引用した場合，単体で経路フィルタとして使用した場合と同じ方法で比較します。

ip prefix-list を route-map の match ip route-source から経路学習元ルータ条件として引用した場合，経路学習元ルータの IPv4 アドレスにマスク長 32 のマスクを付けたものと条件を比較します。

ipv6 prefix-list を route-map の match ipv6 route-source から経路学習元ルータ条件として引用した場合, 経路学習元ルータの IPv6 アドレスにマスク長 128 のマスクを付けたプレフィックスとプレフィックス宛先を比較します。

(b) ip access-list standard

ip access-list standard のアクセスリスト名は，主にアドレスをフィルタするためのフィルタ設定ですが，経路フィルタリングにも使用できます。経路フィルタリングに使用した場合, 経路の宛先ネットワークのアドレス部分とアドレス条件を比較します。

ip access-list standard を route-map の match ip address から経路宛先条件として引用した場合，単体で経路フィルタとして使用した場合と同じ方法で比較します。

ip access-list standard を route-map の match ip route-source から経路学習元ルータ条件として引用した場合，経路学習元ルータの IPv4 アドレスと条件を比較します。

(c) ip access-list extended

ip access-list extended のアクセスリスト名は，主にパケットをフィルタするためのフィルタ設定ですが，経路フィルタリングにも使用できます。経路フィルタリングに使用した場合, 経路の宛先ネットワークのアドレスと宛先アドレス条件を比較し，経路の宛先ネットワークのマスクと送信元アドレス条件を比較します。上位プロトコル種別やポート番号などのアドレス以外の条件は，すべて無視します。

ip access-list extended を route-map の match ip address から経路宛先条件として引用した場合，単体で経路フィルタとして使用した場合と同じ方法で比較します。

ip access-list extended を route-map の match ip route-source から経路学習元ルータ条件として引用した場合，経路学習元ルータの IPv4 アドレスと宛先アドレス条件を比較して，マスク長 32 のマスク 255.255.255.255 と送信元アドレス条件を比較します。

(d) ipv6 access-list

ipv6 access-list のアクセスリスト名は，主にパケットをフィルタするためのフィルタ設定ですが，経路フィルタリングにも使用できます。

ipv6 access-list を route-map の match ipv6 address から経路宛先条件として引用した場合，経路宛先ネットワークのアドレスと宛先アドレス条件を比較します。送信元アドレス条件，上位プロトコル種別，ポート番号などの宛先アドレス以外の条件は，すべて無視します。

ipv6 access-list を route-map の match ipv6 route-source から経路学習元ルータ条件として引用した場合，経路学習元ルータ IPv6 アドレスと宛先アドレス条件を比較します。送信元アドレス条件，上位プロトコル種別，ポート番号などの宛先アドレス以外の条件は，すべて無視します。

(2) route-map

route-map は，いろいろな種類のフィルタ条件を複数同時に指定できるフィルタです。さらに，条件を満たしたときに経路属性を変更できます。

route-map にはシーケンス番号が付いています。一つのシーケンス番号にフィルタ条件の種類ごとに 1 行ずつフィルタ条件を設定できます。1 行の設定の中には，フィルタ条件を複数指定できます。1 行の中に指定した複数の条件は OR 条件として取り扱われます。シーケンス番号の中に設定した複数の行は AND 条件として取り扱われます。

指定してあるフィルタ条件が，全種類について一つずつ一致すれば，そのシーケンス番号の条件を満たしたことになります。条件を満たした時点で，そのシーケンス番号の動作を採用し，その route-map によってフィルタを終了します。

指定したフィルタ条件のどれもが一致しないようなフィルタ条件の種類が一つでもある場合，そのシーケンス番号の条件は満たさなかったことになります。この場合，次のシーケンス番号を評価します。

route-map のフィルタ条件の種類と route-map で変更できる属性を次の表に示します。

注意

経路に複数の route-map を連続して適用した場合，先に適用した route-map で変更した経路属性が，あとで適用する route-map の経路フィルタリングに影響します。

例えば，redistribute（RIP）でタグ値を変更する route-map を適用して，distribute-list out（RIP）でタグ値を条件とする route-map を適用した場合，まず redistribute でタグ値を変更するため，次に distribute-list out の route-map を適用するときには変更後のタグ値と比較することになります。

表 23–4　route-map のフィルタ条件の種類

条件となる経路属性	説明	コンフィグレーションコマンド
宛先ネットワーク	ip prefix-list，ipv6 prefix-list，ip access-list または ipv6 access-list の識別子を条件として指定して，指定したフィルタで経路の宛先ネットワークをフィルタします。フィルタの動作が permit の場合，一致したと見なします。deny の場合，一致しないと見なします。	ip access-list ipv6 access-list ip prefix-list ipv6 prefix-list match ip address match ipv6 address
プロトコル種別	ルーティングプロトコル名を条件として指定して，経路の学習元プロトコル種別と比較します。	match protocol
隣接ルータ	ip prefix-list，ipv6 prefix-list，ip access-list または ipv6 access-list の識別子を条件として指定して，指定したフィルタで経路の学習元ルータのアドレスをフィルタします。指定したフィルタの動作が permit の場合，一致したと見なします。deny の場合，一致しないと見なします。 学習元隣接ルータのアドレスがあるのは，RIP 経路，BGP4 経路，RIPng 経路および BGP4+経路だけです。そのほかの経路は，隣接ルータ条件と一致しません。	ip access-list ipv6 access-list ip prefix-list ipv6 prefix-list match ip route-source match ipv6 route-source
インタフェース	インタフェースを条件として指定して，経路ネクストホップのインタフェースと比較します。 ネクストホップのない経路は一致しません。 BGP4 および BGP4+学習経路フィルタリングでは，経路はどのインタフェースとも一致しません。	match interface
タグ値	タグ値を条件に指定して，経路のタグ値と比較します。 タグのない経路ではタグ値 0 と見なします。	match tag
AS_PATH 属性	ip as-path access-list の識別子を条件に指定して，経路の AS_PATH 属性を指定した ip as-path access-list でフィルタします。動作が permit の場合，一致したと見なします。deny の場合，一致しないと見なします。 AS_PATH 属性のない経路では，長さ 0 の AS PATH と見なします。	ip as-path access-list match as-path

条件となる経路属性	説明	コンフィグレーションコマンド
COMMUNITIES 属性	ip community-list の識別子を条件に指定して，経路の COMMUNITIES 属性を指定した ip community-list でフィルタします。動作が permit の場合，一致したと見なします。deny の場合，一致しないと見なします。 COMMUNITIES 属性のない経路では，コミュニティなしと見なします。	ip community-list match community
ORIGIN 属性	値 IGP・EGP・INCOMPLETE を条件に指定して，経路の ORIGIN 属性と比較します。 ORIGIN 属性のない経路では，値 IGP と見なします。	match origin
経路種別	OSPF および OSPFv3 の経路種別や local（network（BGP4）および network（BGP4+）の設定による経路であることを示す）をフィルタ条件に指定して，経路のプロトコル依存経路種別と比較します。	match route-type
VRF ID	VRF ID を条件に指定して，経路の VRF ID と比較します。	match vrf

注　インタフェース条件設定に指定した条件が IPv4 にも IPv6 にも使用しないインタフェースだけの場合，そのインタフェース条件設定はどの経路とも一致すると見なします。

表 23-5　route-map で変更できる経路属性

変更できる属性	説明	コンフィグレーションコマンド
ディスタンス値	ルーティングテーブル内での経路優先度，ディスタンス値を変更します。学習経路フィルタリングだけで有効です。	set distance
メトリック値 MED 属性	メトリック値や MED 属性を変更します。値の置き換えのほかに，加算と減算ができます。 BGP4 および BGP4+での経路フィルタリングに限り，BGP NEXT_HOP 属性への経路のメトリックを引き継ぐこともできます。	set metric set metric-type internal（NEXT_HOP 属性宛ての経路のメトリック引き継ぎ）
タグ値	経路のタグ値を変更します。	set tag
LOCAL_PREF 属性	経路の LOCAL_PREF 属性を変更します。値の置き換えのほかに，加算と減算ができます。 BGP4 および BGP4+の経路フィルタリングで使用します。	set local-preference
AS_PATH 属性	経路の AS_PATH 属性を変更します。AS 番号の追加だけできます。ピアの送信側 AS 番号を追加します。 BGP4 および BGP4+の外部ピアで学習・広告した経路の経路フィルタリングで使用します。	set as-path prepend count
COMMUNITIES 属性	経路の COMMUNITIES 属性を変更します。コミュニティの置き換え・追加・削除ができます。 BGP4 および BGP4+の経路フィルタリングで使用します。	set community set community-delete
ORIGIN 属性	経路の ORIGIN 属性を変更します。 BGP4 および BGP4+の経路フィルタリングで使用します。	set origin
OSPF メトリック種別	メトリック種別を変更します。	set metric-type

変更できる属性	説明	コンフィグレーションコマンド
	OSPF および OSPFv3 の広告経路フィルタリングで使用します。	

(3)　そのほかのフィルタ

上記で説明したフィルタのほかに，BGP 経路属性を条件とするフィルタを使用できます。ここで説明するフィルタは，route-map からフィルタ条件として呼び出して使用します。

(a)　ip as-path access-list

AS_PATH 属性専用のフィルタです。正規表現をフィルタ条件として，AS_PATH 属性の文字列表現と比較します。route-map の match as-path から呼び出して使用します。

AS_PATH 属性の文字列表現は，10 進数表記した AS 番号を空白文字で接続したものです。

なお，フィルタ条件として AS_PATH 属性のパスタイプを指定できません。フィルタ条件として指定する AS 番号は，AS_PATH 属性に含まれるすべてのパスタイプがフィルタの評価対象となります。次に示す AS_PATH 属性を持つ経路をフィルタする場合を例として説明します。

[AS_PATH 属性の内容]

```
AS_SEQ: 100 200 300, AS_SET: 1000 2000 3000, AS_CONFED_SEQUENCE: 65001 65002
```

[運用コマンドでの AS_PATH 属性の表示形式]

```
100 200 300 {1000 2000 3000} (65001 65002)
```

このような AS_PATH 属性の場合，次に示すどの AS 番号を指定してもフィルタに一致します。

- "100 200 300"
- "1000 2000 3000"
- "65001 65002"
- "300 1000"

運用コマンドのパスタイプ表記である{}や()は，正規表現の特殊文字のため，パスタイプを表すための文字としては指定できないことに注意してください。

また，AS_SET については BGP4 経路受信時に昇順にソートするため，ソートした結果がフィルタの評価対象となります。

(b)　ip community-list standard

COMMUNITIES 属性専用のフィルタです。複数のコミュニティをフィルタ条件として，経路の COMMUNITIES 属性に条件コミュニティがすべて含まれている場合，一致したと見なします。route-map の match community から呼び出して使用します。

(c)　ip community-list expanded

COMMUNITIES 属性専用のフィルタです。正規表現をフィルタ条件として，COMMUNITIES 属性の文字列表現と比較します。route-map の match community から呼び出して使用します。

COMMUNITIES 属性の文字列表現は，コミュニティ値を文字列に変換して，値の小さいものから順に空白文字で接続したものです。コミュニティ値の文字列表現を次の表に示します。

表 23-6　COMMUNITIES 属性の文字列表現

コミュニティ値	文字列
0xFFFFFF01（16 進）	no-export
0xFFFFFF02（16 進）	no-advertise
0xFFFFFF03（16 進）	local-AS
上記以外	<AS 番号>:<下位 2 オクテット値> <AS 番号>と<下位 2 オクテット値>はともに 10 進表記。

(d)　正規表現

正規表現は文字列のパターンを記述する方法です。正規表現を使用すると，繰り返しなどのパターンを記述できます。正規表現は，AS_PATH 属性や COMMUNITIES 属性のフィルタ条件に使用します。

正規表現で使える文字は，英数字・記号（ただし，ダブルクォート（"）は除く）などの通常文字と，特殊文字です。通常文字，バックスラッシュ（¥）と組み合わせた特殊文字は，文字列中の同じ文字と一致します。特殊文字はそれぞれパターンを示します。特殊文字とそのパターンを次の表に示します。

表 23-7　特殊文字とそのパターン

特殊文字	パターン
.	空白を含むすべての単一文字を意味します。
*	前に置いた文字や文字集合の 0 回以上の繰り返しを意味します。
+	前に置いた文字や文字集合の 1 回以上の繰り返しを意味します。
?	前に置いた文字や文字集合の 0 回または 1 回を意味します（コマンド入力時には［Ctrl］＋［V］キーを入力後［?］キーを入力してください）。
^	文字列の先頭を意味します。
$	文字列の末尾を意味します。
_	文字列の先頭，文字列の末尾，「 」（空白），「_」，「,」，「(」（通常文字），「)」（通常文字），「{」，「}」，「<」，「>」のどれかを意味します。
[ ]	[ ]内の文字範囲のうち単一文字を意味します。[ ]内では，次に示す文字以外は通常文字として扱います（特殊文字としても意味は持ちません）。 ^：文字範囲を示す[ ]の中の先頭に置いた場合，パターンの否定を意味します。 -：[ ]の中で範囲のうち開始と終了を示すために使用します。-の前の文字は-の後の文字よりも文字コードが小さくなるように指定してください。文字コードについては「コンフィグレーションコマンドレファレンス Vol.1　表 1-3 文字コード一覧」を参照してください。 例：[6-8]は 6，7，8 のどれか 1 文字を意味します。[^6-8]は 6，7，8 以外のどれか 1 文字を意味します。
( )	複数文字の集合を意味します。最大で 9 集合までネストできます。
|	OR 条件を意味します。
¥	上記の特殊文字の前に置いた場合，その特殊文字を通常文字として扱います。

正規表現で使用する文字を，結合優先順位が高い順に次に示します。

1. ( )
2. * ＋ ?
3. 通常文字 . [ ] ^ $
4. |

コンフィグレーションコマンドや運用コマンドで正規表現を指定する場合は，正規表現の前後をダブルクォート（"）で囲んで指定してください。

例 1

```
> show ip bgp aspath-regexp "^$"
```

例 2

```
(config)# ip as-path access-list 10 permit "_100_"
```

23.1.3　RIP および RIPng

(1)　学習経路フィルタリング

RIP および RIPng では，学習した経路をすべてフィルタできます。フィルタした結果，学習しないことになった経路はルーティングテーブルに導入されません。

(a)　フィルタの適用方法と適用順

学習した経路を distribute-list in で指定したフィルタでフィルタします。パラメータにインタフェースやルータを指定することによって，特定のインタフェースやルータから学習した経路にだけフィルタを適用できます。学習経路フィルタリングのコンフィグレーションコマンドを次の表に示します。

表 23-8　学習経路フィルタリングのコンフィグレーションコマンド

コマンド名	パラメータ	フィルタ対象経路
distribute-list in（RIP）	gateway <ipv4 address>	指定した隣接ルータから学習した RIP 経路だけ，フィルタを適用します。
	<interface type> <interface number>	指定した IPv4 インタフェースから学習した RIP 経路だけ，フィルタを適用します。
	なし	学習した RIP 経路すべてにフィルタを適用します。
distribute-list in（RIPng）	<interface type> <interface number>	指定した IPv6 インタフェースから学習した RIPng 経路だけ，フィルタを適用します。
	なし	学習した RIPng 経路すべてにフィルタを適用します。

経路の学習後，指定したフィルタを RIP および RIPng それぞれの順番に適用します。適用するフィルタが一つもない場合，またはフィルタを適用した結果がすべて permit である場合，学習経路を有効経路としてルーティングテーブルに導入します。適用した結果が deny であるフィルタが一つでもある場合，その学習経路をルーティングテーブルに導入しません。

(b)　学習経路フィルタリングで変更できる経路属性

RIP および RIPng の学習経路フィルタリングで変更できる属性を次の表に示します。

表 23-9　学習経路フィルタリングで変更できる経路の属性

属性	デフォルト値
ディスタンス値	distance に指定した値。 指定していない場合は 120。
メトリック値	受信経路の属性値。
タグ値	受信経路の属性値。

変更したメトリック値は，RIP および RIPng の優先経路選択に使用します。変更したディスタンス値は，ルーティング種別間の優先経路選択に使用します。

注意

- メトリック値の変更方法に，加算以外の方法を使用しないことをお勧めします。メトリック値を置き換えまたは減算で変更すると，ルーティングループが発生して，パケットを正しく転送できなくなることがあるためです。
- メトリック値を 16 以上に変更するように設定できます。しかし，変更後のメトリック値が 16 以上の RIP 経路および RIPng 経路は無効経路になります。
- コンフィグレーションコマンド metric-offset によるメトリック値の変更は，学習経路フィルタリングしたあとで適用します。経路フィルタで変更したメトリック値を，さらに metric-offset で変更します。metric-offset によって変更した結果，メトリック値が 16 以上になった経路は無効になります。
- タグ値を最大 4294967295 に変更できます。しかし，変更した経路を RIP バージョン 2 で広告するときには，2 進数表現の下位 16 ビットだけを使用して，上位のビットを切り捨てます。RIP の場合，タグ値は，経路を学習した RIP のバージョンに関係なく変更できます。しかし，変更した経路を広告するときに，タグ値を付けて広告するのは RIP バージョン 2 だけです。

(2)　広告経路フィルタリング

RIP および RIPng では，ルーティングテーブルの優先経路だけを広告でき，スプリットホライズンは広告しません。また，RIP では，RIP バージョン 1 の経路広告条件を満たさない経路は広告しません。

広告経路フィルタリングの設定をしていない場合，RIP 経路と RIP インタフェースの直結経路，および RIPng 経路と RIPng インタフェースの直結経路が広告対象になります。

注意

RIP で OSPF 経路や BGP4 経路を広告するとき，または RIPng で OSPFv3 経路や BGP4+経路を広告するときには，広告経路フィルタリングや広告メトリック値を設定することで metric 値を変更してください。上記経路のデフォルト広告メトリック値が 16 なので，そのままでは広告されません。

(a)　広告経路フィルタリングで変更できる経路属性

RIP の広告経路フィルタリングで変更できる属性を次の表に示します。

表 23-10　RIP 広告経路フィルタリングで変更できる経路の属性

属性	経路学習元プロトコル	デフォルト値
メトリック値	直結経路 集約経路	1

属性	経路学習元プロトコル	デフォルト値
	スタティック経路	default-metric で指定した値を使用します。 default-metric 未設定時は 1 を使用します。
	RIP 経路	経路情報のメトリック値を引き継ぎます。
	OSPF 経路 BGP4 経路 他 VRF またはグローバルネットワークからインポートした経路	inherit-metric 設定時は経路情報のメトリック値を引き継ぎます。経路情報にメトリック値がない場合は 16 を使用します。 inherit-metric 未設定時は default-metric で指定した値を使用します。 inherit-metric も default-metric も設定していないときは 16 を使用します。
タグ値	全プロトコル共通	経路情報のタグ値を引き継ぎます。

RIPng の広告経路フィルタリングで変更できる属性を次の表に示します。

表 23-11　RIPng 広告フィルタリングで変更できる経路の属性

属性	経路学習元プロトコル	デフォルト値
メトリック値	直結経路 集約経路	1
	スタティック経路	default-metric で指定した値を使用します。 default-metric 未設定時は 1 を使用します。
	RIPng 経路	経路情報のメトリック値を引き継ぎます。
	OSPFv3 経路 BGP4+経路 他 VRF またはグローバルネットワークからインポートした経路	inherit-metric 設定時は経路情報のメトリック値を引き継ぎます。経路情報にメトリック値がない場合は 16 を使用します。 inherit-metric 未設定時は default-metric で指定した値を使用します。 inherit-metric も default-metric も設定していない場合は 16 を使用します。
タグ値	全プロトコル共通	経路情報のタグ値を引き継ぎます。

注意

- RIP 経路を RIP で広告する場合，または RIPng 経路を RIPng で広告する場合，加算以外のメトリック値変更方法を使用しないことをお勧めします。メトリック値を置き換えまたは減算すると，ルーティングループが発生して，パケットを正しく転送できなくなることがあるためです。
- メトリック値を 16 以上に変更するように経路フィルタを設定できます。しかし，メトリック値が 16 以上の経路は広告されません。
- コンフィグレーションコマンド metric-offset によるメトリック値の変更は，広告経路フィルタリングしたあとで適用します。経路フィルタで変更したメトリック値を，さらに metric-offset で変更します。metric-offset によって変更した結果，メトリック値が 16 以上になった経路は広告されません。
- タグ値を 65535 より大きな値に変更した場合，2 進数表現の下位 16 ビットだけを使用して，上位のビットを切り捨てます。ただし，RIP でタグ値を広告するには，RIP のバージョンが 2 である必要があります。

(b)　フィルタの適用方法と適用順

広告経路フィルタリングでのフィルタの適用方法と適用順を次に示します。

1. RIP または RIPng で広告したい経路を選択します。
   広告したい経路の学習元プロトコルおよび経路種別をコンフィグレーションコマンド redistribute で設定します。このコマンドで指定されたプロトコルの経路だけが広告対象になります。また，route-map を指定すると，route-map でフィルタした結果が permit である経路だけを広告対象にできます。redistribute では，ルーティングテーブル上の経路属性値と条件を比較します。
   RIP 経路および RIP インタフェースの直結経路，または RIPng 経路および RIPng インタフェースの直結経路は，redistribute で指定しなくても広告されます。
   redistribute に経路属性を変更する route-map や経路属性を直接指定すれば，広告する経路の属性も変更できます。
2. メトリック値をプロトコルのデフォルト値に設定します。
   ただし，redistribute でメトリック値を変更した場合は，その値を使用します。
3. redistribute で選択した経路に，distribute-list out の設定に従ってフィルタを適用します。
   distribute-list out では次の設定ができます。
   - インタフェースおよびルータ（RIP だけ）を指定して，その指定先へ広告する場合にだけフィルタを適用。
   - プロトコルを指定して，そのプロトコルで学習した経路にだけフィルタを適用。

   広告経路フィルタリングのコンフィグレーションコマンドを次の表に示します。

表 23-12　広告経路フィルタリングのコンフィグレーションコマンド

コマンド名	パラメータ	フィルタ対象経路
distribute-list out（RIP）	gateway <ipv4 address> <protocol>	指定した隣接ルータへ広告する経路，かつ指定したプロトコルの経路にフィルタを適用します。
	gateway <ipv4 address>	指定した隣接ルータへ広告する経路にフィルタを適用します。
	<interface type> <interface number>	指定した IPv4 インタフェースから広告する経路にフィルタを適用します。
	<protocol>	広告先に関係なく，指定したプロトコルの経路にフィルタを適用します。
	なし	広告先に関係なく，すべての経路にフィルタを適用します。
distribute-list out（RIPng）	<interface type> <interface number>	指定した IPv6 インタフェースから広告する経路にフィルタを適用します。
	<protocol>	広告先に関係なく，指定したプロトコルの経路にフィルタを適用します。
	なし	広告先に関係なく，すべての経路にフィルタを適用します。

経路を RIP インタフェースや特定の隣接ルータへ広告するに当たり，広告先や経路学習元プロトコルに応じてフィルタを選択し，それを表の RIP および RIPng それぞれの順番に適用します。適用するフィルタが一つもない場合，またはフィルタした結果がすべて permit である場合，指定の広告先へ経路を

広告します。適用した結果が deny であるフィルタが一つでもある場合，その広告先へはその経路を広告しません。

distribute-list out に route-map を指定した場合，広告デフォルト属性値や redistribute で変更したあとの属性値に従って経路をフィルタします。

distribute-list out に属性を変更する route-map を指定すれば，広告する経路の属性も変更できます。

23.1.4　OSPF および OSPFv3

(1)　学習経路フィルタリング

OSPF では，SPF 計算で求められた経路の中で，AS 外経路と NSSA 経路だけフィルタできます。また，OSPFv3 では，AS 外経路だけフィルタできます。フィルタした結果，学習しないことになった経路情報は，ルーティングテーブルに無効経路として導入されます。

エリア内経路およびエリア間経路は，フィルタされることなくルーティングテーブルに導入されます。

学習経路フィルタリングで経路を無効にしても，ほかのルータには該当する経路が作成されます。これは，経路の元となる LSA がドメイン内のほかのルータへ伝わるためです。学習経路フィルタリングでは LSA をフィルタできません。

(a)　フィルタの適用方法と適用順

OSPF では AS 外経路と NSSA 経路を，OSPFv3 では AS 外経路を，distribute-list in で指定したフィルタでフィルタします。学習経路フィルタリングに使用するコンフィグレーションコマンドを次の表に示します。

表 23–13　学習経路フィルタリングのコンフィグレーションコマンド

コマンド名	フィルタ対象経路
distribute-list in（OSPF）	設定した OSPF ドメインで求められた AS 外経路と NSSA 経路がフィルタリング対象になります。
distribute-list in（OSPFv3）	設定した OSPFv3 ドメインで求められた AS 外経路がフィルタリング対象になります。

適用するフィルタがない場合，またはフィルタした結果が permit である場合，経路を有効経路としてルーティングテーブルに導入します。フィルタした結果が deny である場合，その経路は無効経路になります。

(b)　学習経路フィルタリングで変更できる経路属性

OSPF および OSPFv3 の学習経路フィルタリングで変更できる属性を次の表に示します。

表 23–14　学習経路フィルタリングで変更できる経路の属性

属性	デフォルト値
ディスタンス値	distance ospf に指定した値。 指定していない場合は 110。

学習経路フィルタリングでは，ディスタンス値だけを変更できます。変更したディスタンス値は，ルーティング種別間の優先経路選択に使用します。

(2)　広告経路フィルタリング

OSPF では OSPF インタフェースの直結経路を，OSPFv3 では OSPFv3 インタフェースの直結経路を，エリア内経路またはエリア間経路として広告します。これらは，広告経路フィルタリングでは制御できません。

また，OSPF 経路および OSPFv3 経路もほかのルータに伝わります。これも，経路フィルタリングでは制御できません。これは，経路フィルタリングとは関係なく，経路の元である LSA は無条件で伝えるためです。

上記以外の優先経路は，広告経路フィルタリングによって広告できます。OSPF へ AS 外経路または NSSA 経路として，OSPFv3 へ AS 外経路として広告します。

広告経路フィルタリングの設定をしていない場合，OSPF では，OSPF インタフェースの直結経路と OSPF 経路のほかは，どの経路も広告しません。また，OSPFv3 も同様です。

(a)　広告経路フィルタリングで変更できる経路属性

OSPF の広告経路フィルタリングで変更できる属性を次の表に示します。

表 23-15　OSPF 広告経路フィルタリングで変更できる OSPF AS 外経路の属性

属性	経路学習元プロトコル	デフォルト値
メトリック値	直結経路	20
	BGP4 経路	default-metric（OSPF）で設定した値。 default-metric 設定がない場合は 1。
	その他	default-metric（OSPF）で設定した値。 default-metric 設定がない場合は 20。
OSPF 経路種別	全プロトコル共通	AS 外経路または NSSA 経路の Type 2
タグ値	全プロトコル共通	経路情報のタグ値を引き継ぎます。

OSPFv3 の広告経路フィルタリングで変更できる属性を次の表に示します。

表 23-16　OSPFv3 広告経路フィルタリングで変更できる OSPFv3 AS 外経路の属性

属性	経路学習元プロトコル	デフォルト値
メトリック値	直結経路	20
	BGP4+経路	default-metric（OSPFv3）で設定した値。 default-metric 設定がない場合は 1。
	その他	default-metric（OSPFv3）で設定した値。 default-metric 設定がない場合は 20。
OSPFv3 経路種別	全プロトコル共通	AS 外経路の Type 2
タグ値	全プロトコル共通	経路情報のタグ値を引き継ぎます。

注意

メトリック値を 16777215 以上に変更するように設定できます。しかし，変更後のメトリック値が 16777215 以上の経路は広告されません。

(b)　フィルタの適用方法と適用順

広告経路フィルタリングでのフィルタの適用方法と適用順を次に示します。

1. OSPF または OSPFv3 で広告したい経路を選択します。

   広告したい経路の学習元プロトコルおよび経路種別をコンフィグレーションコマンド redistribute で設定します。このコマンドで指定されたプロトコルの経路だけが広告対象になります。なお，OSPF または OSPFv3 の該当ドメインを指定しても，そのドメインの経路は再広告しません。また，route-map を指定すると，route-map でフィルタした結果が permit である経路だけを広告対象にできます。redistribute では，ルーティングテーブル上の経路属性値と条件を比較します。

   redistribute に経路属性を変更する route-map や経路属性を直接指定すれば，広告する経路の属性も変更できます。

2. メトリック値と OSPF または OSPFv3 の経路種別をプロトコルのデフォルト値に設定します。

   ただし，redistribute で属性値を変更した場合は，その値を使用します。

3. redistribute で選択した経路に distribute-list out の設定に従ってフィルタを適用します。

   distribute-list out ではパラメータにプロトコルを指定して，指定したプロトコルで学習した経路にだけフィルタを適用します。

   広告経路フィルタリングのコンフィグレーションコマンドを次の表に示します。

表 23-17　広告経路フィルタリングのコンフィグレーションコマンド

コマンド名	パラメータ	フィルタ対象経路
distribute-list out (OSPF)	<protocol>	広告先に関係なく，指定したプロトコルの経路にフィルタを適用します。
	なし	広告先に関係なく，すべての経路にフィルタを適用します。
distribute-list out (OSPFv3)	<protocol>	広告先に関係なく，指定したプロトコルの経路にフィルタを適用します。
	なし	広告先に関係なく，すべての経路にフィルタを適用します。

経路を OSPF または OSPFv3 のドメインへ広告するに当たり，経路の学習元プロトコルに応じてフィルタを選択し，それを表の OSPF または OSPFv3 それぞれの順番に適用します。適用するフィルタが一つもない場合，またはフィルタした結果がすべて permit である場合，その経路を広告します。適用した結果が deny であるフィルタが一つでもある場合，その経路を広告しません。

distribute-list out に route-map を指定した場合，広告属性のデフォルト値や redistribute で変更したあとの属性値に従って経路をフィルタします。

distribute-list out に経路属性を変更する route-map を指定すれば，広告する経路の属性も変更できます。

注意

手順 3 の distribute-list out による広告経路フィルタリング時に match route-type を実行すると，“external”と，“external 1”“external 2”のどちらかに一致するようになります。これは，経路属性の中の OSPF または OSPFv3 の経路種別が，redistribute または広告デフォルト属性値によって外部経路の Type 1 または Type 2 に書き換えられたあとだからです。

23.1.5　BGP4 および BGP4+

(1)　学習経路フィルタリング

BGP4 および BGP4+では，学習した経路をすべてフィルタできます。フィルタした結果学習しないことになった経路はデフォルトではルーティングテーブルに導入されません。

(a)　フィルタの適用方法と適用順

学習した経路を，distribute-list in と neighbor in に従ってフィルタします。neighbor in で指定したフィルタは，指定したピア，またはピアグループに所属するピアから学習した経路にだけ適用します。学習経路フィルタリングに使用するコンフィグレーションコマンドを次の表に示します。

表 23–18　学習経路フィルタリングのコンフィグレーションコマンド

コマンド名	パラメータ	フィルタ対象経路
neighbor in（BGP4） • route-map 指定 • ip access-list 指定 • ip prefix-list 指定	<ipv4 address>（ピアアドレス）	指定したピアから学習した経路だけ，フィルタリング対象になります。
neighbor in（BGP4+） • route-map 指定 • ipv6 prefix-list 指定	<ipv6 address>（ピアアドレス）	
neighbor in（BGP4） • route-map 指定 • ip access-list 指定 • ip prefix-list 指定	<peer group>（ピアグループ）	指定したピアグループに所属するピアから学習した経路だけ，フィルタリング対象になります。
neighbor in（BGP4+） • route-map 指定 • ipv6 prefix-list 指定	<peer group>（ピアグループ）	
distribute-list in（BGP4）	なし	BGP4 または BGP4+で学習した経路すべてがフィルタリング対象になります。
distribute-list in（BGP4+）	なし	

経路の学習後，指定したフィルタを BGP4 および BGP4+それぞれの順番に適用します。適用するフィルタが一つもない場合，またはフィルタを適用した結果がすべて permit である場合，学習経路を有効経路としてルーティングテーブルに導入します。適用した結果が deny であるフィルタが一つでもある場合，その学習経路は無効経路になります。

(b)　学習経路フィルタリングで変更できる経路属性

BGP4 および BGP4+の学習経路フィルタリングで変更できる属性を次の表に示します。

表 23–19　学習経路フィルタリングで変更できる経路の属性

属性	デフォルト値
ディスタンス値	distance bgp で指定した値。 指定していない場合は，次の値を使用します。

属性	デフォルト値
	内部ピア：200 外部ピア：20 メンバー AS 間ピア：200
MED 属性	経路受信時の属性値。
LOCAL_PREF 属性	内部ピア：経路受信時の属性値。 外部ピア：bgp default local-preference で指定した値。未指定時は 100。 メンバー AS 間ピア：経路受信時の属性値
AS_PATH 属性	経路受信時の属性値。
COMMUNITIES 属性	経路受信時の属性値。
ORIGIN 属性値	経路受信時の属性値。

ディスタンス値以外の値は，BGP4 および BGP4+の優先経路選択に使用します。ディスタンス値は，ルーティング種別間の優先経路選択に使用します。

注意

AS_PATH 属性に AS を付け加えられるのは，外部ピアから学習した経路だけです。内部ピアやメンバー AS 間ピアから学習した経路の AS_PATH 属性には AS を加えられません。

(2)　広告経路フィルタリング

BGP4 では，ルーティングテーブルの優先経路のほかに，他ルーティングの経路を優先したために優先でなくなった BGP4 経路，および BGP4 の network 設定による経路を広告できます。また，BGP4+でも同様です。この三種類について宛先ネットワークが同じ経路を広告することになった場合，説明した順で経路を一つ選択し，広告します。

広告経路フィルタリングの設定をしていない場合，BGP4 経路および BGP4+経路だけを広告します。ただし，経路の学習元ピアと同じピアへ広告し戻すことはできません。

(a)　広告経路フィルタリングで変更できる経路属性

BGP4 広告経路フィルタリングで変更できる属性を次の表に示します。

表 23-20　BGP4 広告経路フィルタリングで変更できる BGP4 経路の属性

属性	デフォルト値
MED 属性	広告先ピア種別と経路学習元プロトコルによって異なります。 内部ピアへ広告する場合：BGP4 経路の場合，メトリック値を引き継ぎます。BGP4 以外の経路の場合，default-metric で設定した値を使用します。default-metric で値を指定していない場合，値なしで広告します。 外部ピアへ広告する場合：default-metric で設定した値を使用します。default-metric で値を指定していない場合，値なしで広告します。 メンバー AS 間ピアへ広告する場合：BGP4 経路の場合，メトリック値を引き継ぎます。BGP4 以外の経路の場合，default-metric で設定した値を使用します。default-metric で値を指定していない場合，値なしで広告します。
LOCAL_PREF 属性	BGP4 経路の場合，LOCAL_PREF 属性を引き継ぎます。

属性	デフォルト値
	BGP4 以外の経路の場合，bgp default local-preference で設定した値を使用します。bgp default local-preference を設定していない場合，値 100 を使用します。ただし，広告先ピアが外部ピアの場合，広告に LOCAL_PREF 属性は含まれません。
AS_PATH 属性	ルーティングテーブルの経路の値を引き継ぎます。
ORIGIN 属性	
COMMUNITIES 属性	

BGP4+広告経路フィルタリングで変更できる属性を次の表に示します。

表 23-21　BGP4+広告経路フィルタリングで変更できる BGP4+経路の属性

属性	デフォルト値
MED 属性	広告先ピア種別と経路学習元プロトコルによって異なります。 内部ピアへ広告する場合：BGP4+経路の場合，メトリック値を引き継ぎます。BGP4+以外の経路の場合，default-metric で設定した値を使用します。default-metric で値を指定していない場合，値なしで広告します。 外部ピアへ広告する場合：default-metric で設定した値を使用します。default-metric で値を指定していない場合，値なしで広告します。 メンバー AS 間ピアへ広告する場合：BGP4+経路の場合，メトリック値を引き継ぎます。BGP4+以外の経路の場合，default-metric で設定した値を使用します。default-metric で値を指定していない場合，値なしで広告します。
LOCAL_PREF 属性	BGP4+経路の場合，LOCAL_PREF 属性を引き継ぎます。 BGP4+以外の経路の場合，bgp default local-preference で設定した値を使用します。bgp default local-preference を設定していない場合，値 100 を使用します。ただし，広告先ピアが外部ピアの場合，広告に LOCAL_PREF 属性は含まれません。
AS_PATH 属性	ルーティングテーブルの経路の値を引き継ぎます。
ORIGIN 属性	
COMMUNITIES 属性	

注意

コンフィグレーションコマンド neighbor send-community を設定している場合だけ，COMMUNITIES 属性を広告します。

(b)　フィルタの適用方法と適用順

広告経路フィルタリングでのフィルタの適用方法と適用順を次に示します。

1. BGP4 または BGP4+で広告したい経路を選択します。

   広告したい経路の学習元プロトコルおよび経路種別をコンフィグレーションコマンド redistribute で設定します。このコマンドで指定されたプロトコルの経路だけが広告対象になります。また，route-map を指定すると，route-map でフィルタした結果が permit である経路だけを広告対象にできます。redistribute では，ルーティングテーブル上の経路属性値と条件を比較します。

   BGP4 経路および BGP4+経路は，redistribute で指定しなくても広告されます。

redistribute に経路属性を変更する route-map や経路属性を直接指定すれば，広告する経路の属性も変更できます。

2. MED 属性，LOCAL_PREF 属性をプロトコルのデフォルト値に設定します。
   ただし，redistribute で属性値を変更した場合は，その値を使用します。
3. redistribute で選択した経路に，neighbor out と distribute-list out の設定に従ってフィルタを適用します。
   ピアまたはピアグループを指定して（neighbor out），その所属するピアへ広告する場合にだけフィルタを適用します。また，プロトコルを指定して，そのプロトコルで学習した経路にだけフィルタを適用します。
   広告経路フィルタリングのコンフィグレーションコマンドを次の表に示します。

表 23-22　広告経路フィルタリングのコンフィグレーションコマンド

コマンド名	パラメータ	フィルタ対象経路
neighbor out（BGP4） • route-map 指定 • ip access-list 指定 • ip prefix-list 指定	<ipv4 address>（ピアアドレス） <protocol>	指定したピアへ広告する経路，かつ指定したプロトコルの経路にフィルタを適用します。
neighbor out（BGP4+） • route-map 指定 • ipv6 prefix-list 指定	<ipv6 address>（ピアアドレス） <protocol>	
neighbor out（BGP4） • route-map 指定 • ip access-list 指定 • ip prefix-list 指定	<ipv4 address>（ピアアドレス）	指定したピアへ広告する経路にフィルタを適用します。
neighbor out（BGP4+） • route-map 指定 • ipv6 prefix-list 指定	<ipv6 address>（ピアアドレス）	
neighbor out（BGP4） • route-map 指定 • ip access-list 指定 • ip prefix-list 指定	<peer group>（ピアグループ） <protocol>	指定したピアグループに所属するピアへ広告する経路，かつ指定したプロトコルの経路にフィルタを適用します。
neighbor out（BGP4+） • route-map 指定 • ipv6 prefix-list 指定	<peer group>（ピアグループ） <protocol>	
neighbor out（BGP4） • route-map 指定 • ip access-list 指定 • ip prefix-list 指定	<peer group>（ピアグループ）	指定したピアグループに所属するピアへ広告する経路にフィルタを適用します。
neighbor out（BGP4+） • route-map 指定	<peer group>（ピアグループ）	

コマンド名	パラメータ	フィルタ対象経路
• ipv6 prefix-list 指定		
distribute-list out（BGP4）	<protocol>	広告先に関係なく，指定したプロトコルの経路にフィルタを適用します。
distribute-list out（BGP4+）	<protocol>	
distribute-list out（BGP4）	なし	広告先に関係なく，すべての経路にフィルタを適用します。
distribute-list out（BGP4+）	なし	

経路をピアへ広告するに当たり，広告先や経路学習元プロトコルに応じてフィルタを選択し，それを表の BGP4 および BGP4+それぞれの順番に適用します。適用するフィルタが一つもない場合，またはフィルタした結果がすべて permit である場合，指定ピアへ経路を広告します。適用した結果が deny である経路フィルタが一つでもある場合，そのピアへはその経路を広告しません。

neighbor out や distribute-list out に route-map を指定した場合，広告属性のデフォルト値や redistribute で変更したあとの属性値に従って経路をフィルタします。

neighbor out や distribute-list out に属性を変更する route-map を指定すれば，広告する経路の属性も変更できます。

23.1.6　エクストラネット

(1)　VRF 間経路フィルタリング

VRF 間で導入する経路をフィルタできます。フィルタした結果導入しないことになった経路はルーティングテーブルに導入されません。

(a)　フィルタの適用方法

VRF 間で導入したい経路を，import inter-vrf および ipv6 import inter-vrf に従ってフィルタします。

フィルタした結果が permit である場合，経路をルーティングテーブルに導入します。適用するフィルタがない場合，またはフィルタした結果が deny である場合，経路を導入しません。

VRF 間経路フィルタリングに使用するコンフィグレーションコマンドを次の表に示します。

表 23–23　VRF 間経路フィルタリングのコンフィグレーションコマンド

コマンド名	フィルタ対象経路
import inter-vrf	route-map に指定された VRF の経路がフィルタリング対象になります。
ipv6 import inter-vrf	route-map に指定された VRF の経路がフィルタリング対象になります。

(b)　VRF 間経路フィルタリングで変更できる経路属性

他 VRF またはグローバルネットワークからインポートした経路で変更できる属性を次の表に示します。

表 23–24　VRF 間経路フィルタリングで変更できる経路の属性

属性	デフォルト値
ディスタンス値	210
タグ値	ルーティングテーブルの経路の値を引き継ぎます。

属性	デフォルト値
AS_PATH 属性	

(c)　VRF 間経路の設定

VRF 間経路フィルタを指定します。フィルタ条件に従って，他 VRF またはグローバルネットワークからインポートした経路を自 VRF のルーティングテーブルに導入します。導入した経路の VRF ID は，導入先ルーティングテーブルの VRF ID と同じになります。また，導入した経路のプロトコル種別は extra-vrf になります。

VRF 間経路フィルタにコンフィグレーションコマンド match vrf を指定した場合，導入元ルーティングテーブルの VRF ID と条件比較します。match vrf コマンドを指定しない場合，他 VRF またはグローバルネットワークすべてでフィルタ条件は同じになります。

(d)　プロトコルでの VRF 間経路の広告

各プロトコルで広告フィルタを指定すると，そのプロトコルが動作している VRF のルーティングテーブルから経路を広告します。他 VRF またはグローバルネットワークからインポートした経路を指定する場合，コンフィグレーションコマンド redistribute でプロトコルに extra-vrf を指定します。

23.2　コンフィグレーション（IPv4）

23.2.1　コンフィグレーションコマンド一覧

経路フィルタリングのコンフィグレーションコマンド一覧を次の表に示します。

表 23-25　コンフィグレーションコマンド一覧

コマンド名	説明
distribute-list in (BGP4)	BGP4 で学習した経路をルーティングテーブルに取り込むかどうかをフィルタに従って制御します。
distribute-list in (OSPF)	OSPF で学習した経路をルーティングテーブルに取り込むかどうかをフィルタに従って制御します。
distribute-list in (RIP)	RIP で学習した経路をルーティングテーブルに取り込むかどうかをフィルタに従って制御します。
distribute-list out (BGP4)	BGP4 で広告する経路をフィルタに従って制御します。
distribute-list out (OSPF)	OSPF で広告する経路をフィルタに従って制御します。
distribute-list out (RIP)	RIP で広告する経路をフィルタに従って制御します。
ip as-path access-list	AS_PATH 属性フィルタとして動作する ip as-path access-list を設定します。
ip community-list	COMMUNITIES 属性フィルタとして動作する community-list を設定します。
ip prefix-list	ip prefix-list を設定します。
match as-path	route-map に AS_PATH 属性によるフィルタ条件を設定します。
match community	route-map に COMMUNITIES 属性によるフィルタ条件を設定します。
match interface	route-map にインタフェースによるフィルタ条件を設定します。
match ip address	route-map に IPv4 宛先プレフィックスによるフィルタ条件を設定します。
match ip route-source	route-map に送信元 IPv4 アドレスによるフィルタ条件を設定します。
match origin	route-map に ORIGIN 属性によるフィルタ条件を設定します。
match protocol	route-map にルーティングプロトコルによるフィルタ条件を設定します。
match route-type	route-map に経路種別によるフィルタ条件を設定します。
match tag	route-map にタグによるフィルタ条件を設定します。
match vrf	route-map に VRF によるフィルタ条件を設定します。
neighbor in (BGP4)	BGP4 学習経路フィルタリングに使用するフィルタを設定します。
neighbor out (BGP4)	BGP4 広告経路フィルタリングに使用するフィルタを設定します。
redistribute (BGP4)	BGP4 から広告する経路のプロトコル種別を設定します。
redistribute (OSPF)	OSPF から広告する経路のプロトコル種別を設定します。

コマンド名	説明
redistribute (RIP)	RIP から広告する経路のプロトコル種別を設定します。
route-map	route-map を設定します。
set as-path prepend count	経路情報に追加する AS_PATH 番号の数を設定します。
set community	経路属性の COMMUNITIES 属性を置き換えます。
set community-delete	経路属性の COMMUNITIES 属性の削除を設定します。
set distance	経路情報の優先度を設定します。
set local-preference	経路情報の LOCAL_PREF 属性を設定します。
set metric	経路情報のメトリックを設定します。
set metric-type	経路情報のメトリック種別，またはメトリック値を設定します。
set origin	経路情報の ORIGIN 属性を設定します。
set tag	経路情報のタグを設定します。
deny (ip access-list extended)※1	IPv4 パケットフィルタでのアクセスを拒否する条件を指定します。
deny (ip access-list standard)※1	IPv4 アドレスフィルタでのアクセスを拒否する条件を指定します。
ip access-list extended※1	IPv4 パケットフィルタとして動作するアクセスリストを設定します。
ip access-list resequence※1	IPv4 アドレスフィルタおよび IPv4 パケットフィルタのフィルタ条件適用順序のシーケンス番号を再設定します。
ip access-list standard※1	IPv4 アドレスフィルタとして動作するアクセスリストを設定します。
permit (ip access-list extended)※1	IPv4 パケットフィルタでのアクセスを許可する条件を指定します。
permit (ip access-list standard)※1	IPv4 アドレスフィルタでのアクセスを許可する条件を指定します。
import inter-vrf※2	他 VRF またはグローバルネットワークからインポートする経路をフィルタに従って制御します。
router rip※3	ルーティングプロトコル RIP に関する動作情報を設定します。
router ospf※4	ルーティングプロトコル OSPF に関する動作情報を設定します。
router bgp※5	ルーティングプロトコル BGP（BGP4 および BGP4+）に関する動作情報を設定します。

注※1
「コンフィグレーションコマンドレファレンス Vol.2　7. アクセスリスト」を参照してください。

注※2
「コンフィグレーションコマンドレファレンス Vol.3　5. VRF」を参照してください。

注※3
「コンフィグレーションコマンドレファレンス Vol.3　17. RIP」を参照してください。

注※4
「コンフィグレーションコマンドレファレンス Vol.3　19. OSPF」を参照してください。

注※5
「コンフィグレーションコマンドレファレンス Vol.3　21. BGP4/BGP4+」を参照してください。

23.2.2 RIP 学習経路フィルタリング

(1) 特定宛先ネットワークの経路の学習

192.168.0.0/16 宛ての RIP 経路だけを学習して，ほかの宛先ネットワークへの RIP 経路を学習しないように設定します。

[設定のポイント]

学習経路フィルタリングをするには，distribute-list in を設定してください。経路を宛先ネットワークでフィルタするには，ip prefix-list を使用してください。

まず，192.168.0.0/16 宛ての経路だけ permit になる ip prefix-list を設定します。この ip prefix-list を distribute-list in から参照することで，経路宛先ネットワークによる RIP 学習経路フィルタリングをするように設定します。

[コマンドによる設定]

1. **(config)# ip prefix-list ONLY192168 seq 10 permit 192.168.0.0/16**

   192.168.0.0/16 だけ permit になる ip prefix-list を設定します。ONLY192168 にはほかに条件がないので，宛先アドレスやマスク長の異なる経路は deny になります。

2. **(config)# router rip**

   (config-router)# distribute-list prefix ONLY192168 in

   RIP で学習する経路を ONLY192168 でフィルタするように設定します。

(2) 特定インタフェースについて，特定宛先ネットワークの経路の学習

ポート 1/1 から学習した経路について，192.168.0.0/16 宛ての経路だけを学習して，ほかの宛先ネットワークへの経路を学習しないように設定します。ポート 1/1 以外のインタフェースから学習した経路はフィルタしません。

[設定のポイント]

RIP インタフェース個別に学習経路フィルタリングをするには，distribute-list in に<Interface>を指定してください。

まず，192.168.0.0/16 宛ての経路だけ permit になる ip prefix-list を設定します。この ip prefix-list を distribute-list in gigabitethernet 1/1 から参照することで，ポート 1/1 から学習した経路についてだけ，経路宛先ネットワークによる RIP 学習経路フィルタリングをするように設定します。

[コマンドによる設定]

1. **(config)# ip prefix-list ONLY192168 seq 10 permit 192.168.0.0/16**

   192.168.0.0/16 だけ permit になる ip prefix-list を設定します。ONLY192168 にはほかに条件がないので，宛先アドレスやマスク長の異なる経路は deny になります。

2. **(config)# router rip**

   (config-router)# distribute-list prefix ONLY192168 in gigabitethernet 1/1

   ポート 1/1 から学習した経路だけを，ONLY192168 でフィルタするように設定します。

(3) タグ値と宛先ネットワークの両方による学習経路フィルタリング

宛先ネットワークが 192.168.0.0/16 に含まれていて，かつタグ値が 15 ではない経路を学習しないようにします。それ以外の RIP 経路はすべて学習するようにします。

[設定のポイント]

宛先ネットワーク以外を条件とする場合や経路属性を変更したい場合は，route-map を使用します。この route-map を distribute-list in から参照します。

まず，192.168.0.0/16 に含まれるプレフィックスだけが permit になる ip prefix-list を設定します。次に，この ip prefix-list が permit であり，かつタグ値が 15 でない経路だけが deny になる route-map を設定します。

最後に，この route-map を distribute-list in から参照することで，タグ値と宛先ネットワークの両方による RIP 学習経路フィルタリングを設定します。

タグ値を使用するには RIP バージョン 2 である必要があります。RIP バージョン 1 ではタグ値を使えない点に注意してください。

[コマンドによる設定]

1. **(config)# ip prefix-list PERMIT192168LONGER seq 10 permit 192.168.0.0/16 ge 16 le 32**

   192.168.0.0/16 に含まれる経路だけ permit になる ip prefix-list を設定します。

2. **(config)# route-map TAG permit 10**

   (config-route-map)# match ip address prefix-list PERMIT192168LONGER

   (config-route-map)# match tag 15

   (config-route-map)# exit

   192.168.0.0/16 に含まれて，かつタグ値が 15 の経路が permit になるように設定します。

3. **(config)# route-map TAG deny 20**

   (config-route-map)# match ip address prefix-list PERMIT192168LONGER

   (config-route-map)# exit

   シーケンス番号 10 にマッチしないで，かつ 192.168.0.0/16 に含まれる経路が deny になるように設定します。

4. **(config)# route-map TAG permit 30**

   (config-route-map)# exit

   シーケンス番号 10，20 の両方にマッチしなかった経路が permit になるように設定します。

5. **(config)# router rip**

   (config-router)# distribute-list route-map TAG in

   このフィルタを RIP 学習経路フィルタリングに適用して，192.168.0.0/16 に含まれて，かつタグ値が 15 でない RIP 経路だけを学習しないように設定します。

(4)　宛先ネットワークによるディスタンス値の変更

宛先ネットワークが 192.168.0.0/16 に含まれている RIP 学習経路について，OSPF 経路よりも優先されるように，ディスタンス値を 50 にします。

[設定のポイント]

まず，192.168.0.0/16 を含む経路だけ permit になる ip prefix-list を設定します。次に，この ip prefix-list が permit であればディスタンス値を 50 に変更する route-map を設定します。

最後に，この route-map を distribute-list in から参照することで，宛先ネットワークに基づいてディスタンス値を変更する RIP 学習経路フィルタリングを設定します。

[コマンドによる設定]

1. **(config)# ip prefix-list PERMIT192168LONGER seq 10 permit 192.168.0.0/16 ge 16 le 32**

192.168.0.0/16 に含まれる経路だけ permit になる ip prefix-list を設定します。

2. **(config)# route-map Distance50 permit 10**
   (config-route-map)# match ip address prefix-list PERMIT192168LONGER
   (config-route-map)# set distance 50
   (config-route-map)# exit
   192.168.0.0/16 に含まれる経路を，ディスタンス値を 50 に変更して permit になるように設定します。
3. **(config)# route-map Distance50 permit 20**
   (config-route-map)# exit
   シーケンス番号 10 にマッチしなかった経路を，何も変更しないで permit になるように設定します。
4. **(config)# router rip**
   (config-router)# distribute-list route-map Distance50 in
   このフィルタを RIP 学習経路フィルタリングに適用して，192.168.0.0/16 に含まれる RIP 学習経路だけ，ディスタンス値を 50 に変更するように設定します。

23.2.3　RIP 広告経路フィルタリング

(1)　特定プロトコル経路の広告

スタティック経路と OSPF ドメイン 1 の経路を RIP で広告するように設定します。

[設定のポイント]

デフォルトでは広告しない経路を広告させるには，redistribute を設定します。redistribute には，広告したいプロトコルを指定します。

このとき，OSPF 経路の広告設定にメトリック値も指定してください。OSPF 経路や BGP4 経路は，メトリック値を指定しないと広告されません。

[コマンドによる設定]

1. **(config)# router rip**
   (config-router)# redistribute static
   スタティック経路を RIP へ広告します。
2. **(config-router)# redistribute ospf 1 metric 2**
   OSPF ドメイン 1 の経路を，メトリック値 2 で広告します。

(2)　特定プロトコルの特定宛先ネットワーク経路の広告

スタティック経路と，OSPF 経路の中で宛先ネットワークが 192.168.0.0/16 であるものだけを RIP で広告します。

[設定のポイント]

学習元プロトコル別に広告経路フィルタリングをする場合, redistribute に route-map を指定してください。route-map で宛先ネットワークを条件にするには，ip prefix-list を使用してください。

まず，192.168.0.0/16 宛ての経路だけが permit になる ip prefix-list を設定します。次に，この ip prefix-list を条件とする route-map を設定します。最後に，スタティック経路と OSPF 経路を redistribute で指定します。OSPF 経路の redistribute には，この route-map を指定します。

[コマンドによる設定]

1. **(config)# ip prefix-list ONLY192168 seq 10 permit 192.168.0.0/16**

   192.168.0.0/16 だけ permit になる ip prefix-list を設定します。ONLY192168 にはほかに条件がないので，宛先アドレスやマスク長の異なる経路は deny になります。

2. **(config)# route-map ONLY192168 permit 10**

   (config-route-map)# match ip address prefix-list ONLY192168

   (config-route-map)# exit

   宛先ネットワークが 192.168.0.0/16 の経路だけ permit になる route-map を設定します。

3. **(config)# router rip**

   (config-router)# redistribute static

   スタティック経路を RIP で広告します。

4. **(config-router)# redistribute ospf 1 metric 2 route-map ONLY192168**

   OSPF ドメイン 1 の経路を ONLY192168 でフィルタして，permit になった経路だけを，メトリック値 2 で広告します。

(3)　特定宛先ネットワーク経路の広告抑止

192.168.0.0/16 宛ての経路に限り，RIP では広告しないようにします。

[設定のポイント]

経路の学習元プロトコルと関係なく広告経路フィルタリングする場合，distribute-list out を使用してください。

まず，192.168.0.0/16 宛ての経路だけ deny になる ip prefix-list を設定します。この ip prefix-list を distribute-list out から参照することで，経路宛先ネットワークによる RIP 広告経路フィルタリングをするように設定します。

[コマンドによる設定]

1. **(config)# ip prefix-list OMIT192168 seq 10 deny 192.168.0.0/16**

   192.168.0.0/16 が deny になる ip prefix-list を設定します。

2. **(config)# ip prefix-list OMIT192168 seq 100 permit 0.0.0.0/0 ge 0 le 32**

   任意の宛先アドレスやマスク長に対して permit になる ip prefix-list を設定します。OMIT192168 にはほかに条件がないので，192.168.0.0/16 だけが deny になるフィルタになります。

3. **(config)# router rip**

   (config-router)# distribute-list prefix OMIT192168 out

   RIP で広告する経路すべてを，OMIT192168 でフィルタするように設定します。

(4)　広告先インタフェース個別の広告経路フィルタリング

RIP インタフェースであるポート 1/1 からは，192.168.0.0/16 だけを広告します。RIP インタフェースであるポート 2/1 からは，192.168.0.0/16 以外の経路を広告します。そのほかの RIP インタフェースでは，インタフェース個別のフィルタリングをしません。

[設定のポイント]

RIP インタフェース個別に経路フィルタリングする必要がある場合，distribute-list out に<Interface>を指定してください。

まず，192.168.0.0/16 だけ permit になる ip prefix-list と，192.168.0.0/16 だけ deny になる ip prefix-list を設定します。次に，RIP インタフェースであるポート 1/1 とポート 2/1 に distribute-list

out <Interface>を設定します。distribute-list out <Interface>には，その RIP インタフェースに適切な ip prefix-list を指定します。

[コマンドによる設定]

1. **(config)# ip prefix-list ONLY192168 seq 10 permit 192.168.0.0/16**
   192.168.0.0/16 だけ permit になる ip prefix-list を設定します。ONLY192168 にはほかに条件がないので，宛先アドレスやマスク長の異なる経路は deny になります。
2. **(config)# ip prefix-list OMIT192168 seq 10 deny 192.168.0.0/16**
   192.168.0.0/16 だけ deny になる ip prefix-list を設定します。
3. **(config)# ip prefix-list OMIT192168 seq 100 permit 0.0.0.0/0 ge 0 le 32**
   任意の宛先アドレスやマスク長に対して permit になるように ip prefix-list を設定します。
   OMIT192168 にはほかに条件がないので，192.168.0.0/16 だけが deny になるフィルタになります。
4. **(config)# router rip**
   (config-router)# distribute-list prefix ONLY192168 out gigabitethernet 1/1
   ポート 1/1 から広告する経路を ONLY192168 でフィルタするように設定します。
5. **(config-router)# distribute-list prefix OMIT192168 out gigabitethernet 2/1**
   ポート 2/1 から広告する経路を OMIT192168 でフィルタするように設定します。

(5) タグ値による広告経路の制御

直結経路を，タグ値 210 を付けて広告します。スタティック経路の中で，タグ値が 211 のものだけを広告します。その上で，RIP 経路の中で，タグ値が 210 または 211 の経路を RIP から広告しないようにします。こうすることで，本装置が RIP への広告を始めた経路が，本装置を経由してループしないようにします。

タグ値を使用するには RIP バージョン 2 である必要があります。RIP バージョン 1 ではタグ値を使えない点に注意してください。

[設定のポイント]

宛先ネットワーク以外を条件とする場合，またはメトリック値以外の経路属性を変更したい場合は，route-map を使用します。route-map は，redistribute や distribute-list out で指定できます。

直結経路用のタグ値を 210 にする route-map と，スタティック経路用のタグ値 211 だけが permit になる route-map と，RIP 経路用のタグ値が 210 または 211 の経路が deny になる route-map を，それぞれ設定します。

[コマンドによる設定]

1. **(config)# route-map ConnectedToRIP permit 10**
   (config-route-map)# set tag 210
   (config-route-map)# exit
   タグ値を 210 にする route-map を設定します。
2. **(config)# route-map StaticToRIP permit 10**
   (config-route-map)# match tag 211
   (config-route-map)# exit
   タグ値が 211 の経路だけ permit になる route-map を設定します。
3. **(config)# route-map RIPToRIP deny 10**

```
(config-route-map)# match tag 210 211
(config-route-map)# exit
(config)# route-map RIPToRIP permit 20
(config-route-map)# exit
```

タグ値が 210 または 211 の経路が deny になり，そのほかの経路が permit になる route-map を設定します。

4. **(config)# router rip**
   (config-router)# version 2
   (config-router)# redistribute connected route-map ConnectedToRIP
   直結経路を RIP へ広告します。広告条件に ConnectedToRIP を指定します。
5. **(config-router)# redistribute static route-map StaticToRIP**
   スタティック経路を RIP へ広告します。広告条件に StaticToRIP を指定します。
6. **(config-router)# redistribute rip route-map RIPToRIP**
   RIP 経路を RIP へ広告します。広告条件に RIPToRIP を指定します。

23.2.4　OSPF 学習経路フィルタリング

(1)　特定宛先ネットワークの経路の学習

192.168.0.0/16 宛ての経路だけを学習して，ほかの宛先ネットワークへの経路を学習しないように設定します。

[設定のポイント]

学習経路フィルタリングをするには，distribute-list in を設定してください。経路を宛先ネットワークでフィルタするには，ip prefix-list を使用してください。

まず，192.168.0.0/16 宛ての経路だけ permit になる ip prefix-list を設定します。この ip prefix-list を distribute-list in から参照することで，経路宛先ネットワークによる OSPF 学習経路フィルタリングをするように設定します。

[コマンドによる設定]

1. **(config)# ip prefix-list ONLY192168 seq 10 permit 192.168.0.0/16**
   192.168.0.0/16 だけ permit になる ip prefix-list を設定します。ONLY192168 にはほかに条件がないので，宛先アドレスやマスク長の異なる経路は deny になります。
2. **(config)# router ospf 1**
   (config-router)# distribute-list prefix ONLY192168 in
   学習した OSPF の AS 外経路と NSSA 経路を，ONLY192168 でフィルタするように設定します。

(2)　タグ値による学習経路フィルタリング

タグ値が 15 の経路を学習しないようにします。それ以外の経路は学習します。

[設定のポイント]

宛先ネットワーク以外を条件とする場合や経路属性を変更したい場合は，route-map を使用します。この route-map を distribute-list in から参照します。

まず，タグ値が 15 である経路が deny になる route-map を設定します。次に，この route-map を distribute-list in から参照することで，タグ値による OSPF 学習経路フィルタリングを設定します。

[コマンドによる設定]

1. **(config)# route-map TAG15DENY deny 10**
   (config-route-map)# match tag 15
   (config-route-map)# exit
   タグ値が 15 の経路が deny になるように設定します。
2. **(config)# route-map TAG15DENY permit 20**
   (config-route-map)# exit
   シーケンス番号 10 にマッチしない経路が permit になるように設定します。
3. **(config)# router ospf 1**
   (config-router)# distribute-list route-map TAG15DENY in
   このフィルタを OSPF 学習経路フィルタリングに適用して，タグ値が 15 である AS 外経路と NSSA 経路を学習しないように設定します。

(3) 宛先ネットワークによるディスタンス値の変更

宛先ネットワークが 192.168.0.0/16 に含まれている AS 外経路･NSSA 経路よりも RIP 経路の方が優先されるように，ディスタンス値を 150 にします。

[設定のポイント]

宛先ネットワーク以外を条件とする場合や経路属性を変更したい場合は，route-map を使用します。route-map は，distribute-list in で指定して使用します。

まず，192.168.0.0/16 を含む経路が permit になる ip prefix-list を設定します。次に，この ip prefix-list が permit になったらディスタンス値を 150 に変更する route-map を設定します。

最後に，この route-map を distribute-list in から参照することで，宛先ネットワークに基づいてディスタンス値を変更する OSPF 学習経路フィルタリングを設定します。

[コマンドによる設定]

1. **(config)# ip prefix-list PERMIT192168LONGER seq 10 permit 192.168.0.0/16 ge 16 le 32**
   192.168.0.0/16 に含まれる経路だけ permit になる ip prefix-list を設定します。
2. **(config)# route-map Distance150 permit 10**
   (config-route-map)# match ip address prefix-list PERMIT192168LONGER
   (config-route-map)# set distance 150
   (config-route-map)# exit
   192.168.0.0/16 に含まれる経路を，ディスタンス値を 150 に変更して permit になるように設定します。
3. **(config)# route-map Distance150 permit 20**
   (config-route-map)# exit
   シーケンス番号 10 にマッチしなかった経路を，何も変更しないで permit になるように設定します。
4. **(config)# router ospf 1**
   (config-router)# distribute-list route-map Distance150 in
   このフィルタを OSPF 学習経路フィルタリングに適用して，192.168.0.0/16 に含まれる AS 外経路・NSSA 経路だけ，ディスタンス値を 150 に変更するように設定します。

23.2.5　OSPF 広告経路フィルタリング

(1)　特定プロトコル経路の広告

スタティック経路と RIP 経路を OSPF ドメイン 1 へ広告します。

[設定のポイント]

デフォルトでは広告しない経路を広告させるには，redistribute を設定します。redistribute には，広告したいプロトコルを指定します。

[コマンドによる設定]

1. **(config)# router ospf 1**
   (config-router)# redistribute static
   スタティック経路を広告します。
2. **(config-router)# redistribute rip**
   RIP 経路を広告します。

(2)　特定プロトコルの特定宛先ネットワーク経路の広告

スタティック経路と，RIP 経路の中で宛先ネットワークが 192.168.0.0/16 であるものだけを OSPF ドメイン 1 へ広告します。

[設定のポイント]

学習元プロトコル別に広告経路フィルタリングをする場合, redistribute に route-map を指定してください。route-map 中で宛先ネットワーク条件を指定するには，ip prefix-list を設定して，match ip address で参照してください。

まず，192.168.0.0/16 宛ての経路だけが permit になる ip prefix-list を設定します。次に，この ip prefix-list を条件とする route-map を設定します。最後に，スタティック経路と RIP 経路を広告するように，redistribute を設定します。RIP 経路の redistribute には，この route-map を指定します。

[コマンドによる設定]

1. **(config)# ip prefix-list ONLY192168 seq 10 permit 192.168.0.0/16**
   192.168.0.0/16 だけ permit になる ip prefix-list を設定します。ONLY192168 にはほかに条件がないので，宛先アドレスやマスク長の異なる経路は deny になります。
2. **(config)# route-map ONLY192168 permit 10**
   (config-route-map)# match ip address prefix-list ONLY192168
   (config-route-map)# exit
   宛先ネットワークが 192.168.0.0/16 の経路だけ permit になる route-map を設定します。
3. **(config)# router ospf 1**
   (config-router)# redistribute static
   スタティック経路を OSPF ドメイン 1 へ広告します。
4. **(config-router)# redistribute rip route-map ONLY192168**
   RIP 経路を ONLY192168 でフィルタして，permit になった経路だけを広告します。

(3) 特定宛先ネットワーク経路の広告抑止

スタティック経路と RIP 経路を OSPF ドメイン 1 へ広告します。ただし，192.168.0.0/16 宛ての経路に限り，OSPF ドメイン 1 へ広告しないようにします。

[設定のポイント]

経路の学習元プロトコルと関係なく広告経路フィルタリングする場合，distribute-list out を使用してください。

まず，192.168.0.0/16 宛ての経路だけ deny になる ip prefix-list を設定します。この ip prefix-list を distribute-list out から参照することで，経路宛先ネットワークによる広告経路フィルタリングをするように設定します。

最後に，スタティック経路と RIP 経路を広告するよう，redistribute を設定します。

[コマンドによる設定]

1. **(config)# ip prefix-list OMIT192168 seq 10 deny 192.168.0.0/16**
   192.168.0.0/16 が deny になる ip prefix-list を設定します。
2. **(config)# ip prefix-list OMIT192168 seq 100 permit 0.0.0.0/0 ge 0 le 32**
   任意の宛先アドレスやマスク長に対して permit になる ip prefix-list を設定します。OMIT192168 にはほかに条件がないので，192.168.0.0/16 だけが deny になるフィルタになります。
3. **(config)# router ospf 1**
   (config-router)# distribute-list prefix OMIT192168 out
   広告経路を OMIT192168 でフィルタするように設定します。
4. **(config-router)# redistribute static**
   (config-router)# redistribute rip
   スタティック経路と RIP 経路を広告するように設定します。

(4) OSPF ドメイン間の経路広告

OSPF ドメイン 1 と OSPF ドメイン 2 の間で，相互に経路を広告し合います。

OSPF ドメイン 1 の経路に，タグ値 1001 を付けて OSPF ドメイン 2 に広告します。OSPF ドメイン 2 の経路にタグ値 1001 が付いているときは，OSPF ドメイン 1 には広告しません。こうすると，OSPF ドメイン 1 の経路が OSPF ドメイン 2 を経由して OSPF ドメイン 1 に広告し戻すことがなくなるので，ルーティングループを防げます。

同様に，OSPF ドメイン 2 の経路に，タグ値 1002 を付けて OSPF ドメイン 1 に広告します。OSPF ドメイン 1 の経路にタグ値 1002 が付いているときは，OSPF ドメイン 2 には広告しません。

[設定のポイント]

宛先ネットワーク以外を条件とする場合，またはメトリック値以外の経路属性を変更したい場合は，route-map を使用します。route-map は，redistribute や distribute-list out で指定できます。

OSPF ドメイン 1 への広告用に，タグ値 1001 が付いていれば deny，それ以外はタグ値 1002 を付けて permit になる route-map を設定します。これを，OSPF ドメイン 1 の OSPF ドメイン 2 経路を広告する redistribute に指定します。

同様に，OSPF ドメイン 2 への広告用に，タグ値 1002 が付いていれば deny，それ以外はタグ値 1001 を付けて permit になる route-map を設定します。これを，OSPF ドメイン 2 の OSPF ドメイン 1 経路を広告する redistribute に指定します。

[コマンドによる設定]

1. (config)# route-map OSPF2to1 deny 10
   (config-route-map)# match tag 1001
   (config-route-map)# exit
   タグ値が 1001 の経路が deny になるように OSPF2to1 を設定します。
2. (config)# route-map OSPF2to1 permit 20
   (config-route-map)# set tag 1002
   (config-route-map)# exit
   上記を満たさない場合，タグ値を 1002 にするように設定します。
3. (config)# router ospf 1
   (config-router)# redistribute ospf 2 route-map OSPF2to1
   (config-router)# exit
   OSPF ドメイン 2 経路を OSPF ドメイン 1 へ広告します。OSPF2to1 をフィルタとして指定します。
4. (config)# route-map OSPF1to2 deny 10
   (config-route-map)# match tag 1002
   (config-route-map)# exit
   (config)# route-map OSPF1to2 permit 20
   (config-route-map)# set tag 1001
   (config-route-map)# exit
   タグ値が 1002 の場合は deny になり，それ以外はタグ値を 1001 とするように OSPF1to2 を設定します。
5. (config)# router ospf 2
   (config-router)# redistribute ospf 1 route-map OSPF1to2
   (config-router)# exit
   OSPF ドメイン 1 経路を OSPF ドメイン 2 へ広告します。OSPF1to2 をフィルタとして指定します。

23.2.6　BGP4 学習経路フィルタリング

(1)　全ピア共通の条件付き経路の学習

宛先ネットワークが 192.168.0.0/16 に含まれる BGP4 経路を学習しないで，ほかの宛先ネットワークへの BGP4 経路を学習するように設定します。

[設定のポイント]

全ピア共通に学習経路フィルタリングをするには，distribute-list in を設定してください。宛先ネットワークによるフィルタには，ip prefix-list を使用してください。

まず，192.168.0.0/16 に含まれる経路と一致すると deny になる ip prefix-list を設定します。この ip prefix-list を distribute-list in から参照することで，経路宛先ネットワークによる BGP4 学習経路フィルタリングをするように設定します。

[コマンドによる設定]

1. (config)# ip prefix-list DENY192168LONGER seq 10 deny 192.168.0.0/16 ge 16 le 32
   (config)# ip prefix-list DENY192168LONGER seq 20 permit 0.0.0.0/0 ge 0 le 32
   192.168.0.0/16 に含まれるプレフィックスだけ deny になり，それ以外のプレフィックスでは permit になる ip prefix-list を設定します。

2. **(config)# router bgp 65531**
   (config-router)# distribute-list prefix DENY192168LONGER in
   この ip prefix-list をピア共通に学習経路フィルタリングに適用するように設定します。
3. **(config-router)# end**
   # clear ip bgp * in
   学習経路フィルタリング設定の変更を動作に反映します。

(2) ピア個別の条件付き経路の学習

外部ピアについて，宛先ネットワークがプライベートアドレス（10.0.0.0/8，172.16.0.0/12，192.168.0.0/16）の経路を除く，AS_PATH 属性が「65532 65533」の経路を学習します。学習した経路の LOCAL_PREF 属性を 200 に設定します。そのほかの経路は学習しません。

[設定のポイント]

BGP4 ピア個別に学習経路フィルタリングをするには，neighbor in を設定してください。宛先ネットワーク以外の条件比較や属性変更には route-map を使用してください。

まず，プライベートアドレスであれば permit になる ip prefix-list と，AS_PATH 属性が「65532 65533」である場合に permit になる ip as-path access-list を設定します。次に，この二つの条件を組み合わせた route-map を設定します。最後に，この条件でフィルタさせたいピアについて neighbor in を設定します。

[コマンドによる設定]

1. **(config)# ip prefix-list PRIVATE seq 10 permit 10.0.0.0/8 ge 8 le 32**
   (config)# ip prefix-list PRIVATE seq 20 permit 172.16.0.0/12 ge 12 le 32
   (config)# ip prefix-list PRIVATE seq 30 permit 192.168.0.0/16 ge 16 le 32
   プライベートアドレスであれば permit になる ip prefix-list を設定します。
2. **(config)# ip as-path access-list 2 permit "^65532_65533$"**
   AS_PATH 属性が「65532 65533」である場合に permit になる ip as-path access-list を設定します。
3. **(config)# route-map BGP65532IN deny 10**
   (config-route-map)# match ip address prefix-list PRIVATE
   (config-route-map)# exit
   route-map BGP65532IN を，プライベートアドレスだったら deny となるように設定します。
4. **(config)# route-map BGP65532IN permit 20**
   (config-route-map)# match as-path 2
   (config-route-map)# set local-preference 200
   (config-route-map)# exit
   AS_PATH 属性が「65532 65533」と一致したら，LOCAL_PREF 属性を 200 にして permit になるように設定します。BGP65532IN にはほかに条件がないので，ここまでの条件のどれとも一致しない経路は deny になります。
5. **(config)# router bgp 65531**
   (config-router)# neighbor 172.17.1.1 remote-as 65532
   (config-router)# neighbor 172.17.1.1 route-map BGP65532IN in
   外部ピアの受信経路フィルタリングに BGP65532IN を使用するように設定します。
6. **(config-router)# end**

```
# clear ip bgp * in
```

学習経路フィルタリング設定の変更を動作に反映します。

23.2.7　BGP4 広告経路フィルタリング

(1)　他プロトコルの経路を広告する

直結経路とスタティック経路の中で，宛先ネットワークが自 AS のネットワーク（192.168.0.0/16）である経路だけを BGP4 へ広告します。

[設定のポイント]

デフォルトでは広告しない経路を広告させるには，redistribute を設定します。redistribute には，広告したいプロトコルを指定します。

redistribute に，経路広告条件の route-map を指定します。route-map 中の宛先ネットワーク条件の指定には ip prefix-list を使用します。

[コマンドによる設定]

1.
```
(config)# ip prefix-list PERMIT192168LONGER seq 10 permit 192.168.0.0/16 ge 16 le 32
```
192.168.0.0/16 に含まれる経路だけ permit になる ip prefix-list を設定します。

2.
```
(config)# route-map PERMIT192168LONGER permit 10
(config-route-map)# match ip address prefix-list PERMIT192168LONGER
(config-route-map)# exit
```
192.168.0.0/16 に含まれる経路だけ permit になる route-map を設定します。

3.
```
(config)# router bgp 65531
(config-router)# redistribute connected route-map PERMIT192168LONGER
(config-router)# redistribute static route-map PERMIT192168LONGER
```
直結経路とスタティック経路について，route-map PERMIT192168LONGER でフィルタした結果が permit になる経路だけを広告するように，redistribute を設定します。

4.
```
(config-router)# end
# clear ip bgp * out
```
広告経路フィルタリング設定の変更を動作に反映します。

(2)　ピアごとに広告経路を変更する

外部ピアに広告する経路を，AS100 から受信した AS パス長が一つの BGP4 経路，および自 AS のネットワークが宛先である直結経路とスタティック経路（192.168.0.0/16）だけに制限します。広告に当たり，ピア 172.18.1.1 へは AS_PATH の AS 番号を二つ追加します。内部ピアには，BGP4 経路だけを広告します。

[設定のポイント]

ピア個別に経路フィルタリングする必要がある場合，neighbor out を設定してください。

今回の場合，次の四つの route-map を設定します。

- 直結経路およびスタティック経路の redistribute 用

  192.168.0.0/16 に含まれている経路だけ permit になる ip prefix-list を設定して，これを参照する route-map を設定します。
- ピア 172.18.1.1 広告用

経路プロトコルが直結またはスタティックの場合だけ AS を二つ追加する route-map を設定します。

- 172.18.1.1 以外の外部ピア用
  AS が一つの AS_PATH 属性だけ permit になる ip as-path access-list を設定して，これを参照する route-map を設定します。
- 内部ピア用
  BGP4 経路だけ permit，それ以外は deny になる route-map を設定します。

[コマンドによる設定]

1. **(config)# ip prefix-list PERMIT192168LONGER seq 10 permit 192.168.0.0/16 ge 16 le 32**
   (config)# route-map PERMIT192168LONGER permit 10
   (config-route-map)# match ip address prefix-list PERMIT192168LONGER
   (config-route-map)# exit
   192.168.0.0/16 に含まれる経路だけ permit になる route-map を設定します。直結経路およびスタティック経路の redistribute に使用します。
2. **(config)# ip as-path access-list 1 permit "^[0-9]+$"**
   (config)# route-map BGPEXTOUT permit 10
   (config-route-map)# match protocol connected static
   (config-route-map)# exit
   (config)# route-map BGPEXTOUT permit 20
   (config-route-map)# match protocol bgp
   (config-route-map)# match as-path 1
   (config-route-map)# exit
   直結経路，スタティック経路，BGP4 経路の中で AS_PATH 属性の AS 数が一つの経路だけ permit になる route-map を設定します。外部ピアへの広告に使用します。
3. **(config)# route-map BGP17218110UT permit 10**
   (config-route-map)# match protocol connected static
   (config-route-map)# set as-path prepend count 2
   (config-route-map)# exit
   (config)# route-map BGP17218110UT permit 20
   (config-route-map)# match protocol bgp
   (config-route-map)# match as-path 1
   (config-route-map)# set as-path prepend count 2
   (config-route-map)# exit
   直結経路，スタティック経路，BGP4 経路の中で AS_PATH 属性の AS 数が一つの経路だけ permit になり，AS を二つ追加する route-map を設定します。ピア 172.18.1.1 への広告に使用します。
4. **(config)# route-map BGPINTOUT permit 10**
   (config-route-map)# match protocol bgp
   (config-route-map)# exit
   BGP4 経路だけ permit になる route-map を設定します。内部ピアへの広告に使用します。
5. **(config)# router bgp 65531**
   (config-router)# redistribute connected route-map PERMIT192168LONGER

```
(config-router)# redistribute static route-map PERMIT192168LONGER
```

直結経路とスタティック経路について，route-map PERMIT192168LONGER でフィルタした結果が permit になる経路だけを広告するように redistribute を設定します。

6.
```
(config-router)# neighbor 172.17.1.1 remote-as 65532
(config-router)# neighbor 172.17.1.1 route-map BGPEXTOUT out
```

外部ピアへの広告経路のフィルタに BGPEXTOUT を使用します。

7.
```
(config-router)# neighbor 172.18.1.1 remote-as 65533
(config-router)# neighbor 172.18.1.1 route-map BGP17218110UT out
```

外部ピア 172.18.1.1 への広告経路のフィルタに BGP1721811OUT を使用します。

8.
```
(config-router)# neighbor 192.168.1.1 remote-as 65531
(config-router)# neighbor 192.168.1.1 route-map BGPINTOUT out
```

内部ピアへの広告経路のフィルタに BGPINTOUT を使用します。

9.
```
(config-router)# end
# clear ip bgp * out
```

広告経路フィルタリング設定の変更を動作に反映します。

23.2.8　エクストラネット

ある VRF から他 VRF の特定ネットワークに通信する場合, 他 VRF の特定経路を経路フィルタでフィルタリングして，自 VRF へ導入します。

(1)　特定 VRF 経路の導入

VRF 間にわたって通信するために，通信に使用する VRF 2 の経路（172.16.1.0/24）を VRF 3 へ，VRF 3 の経路（172.16.3.0/24）を VRF 2 へインポートするように設定します。

[設定のポイント]

VRF 間経路フィルタリングをするには, import inter-vrf を設定してください。経路を VRF ID でフィルタリングするには，route-map を使用してください。route-map 中の宛先ネットワーク条件の指定には，ip prefix-list を使用してください。

まず，VRF 2 の経路だけ permit になる route-map を設定します。この route-map を VRF 3 の import inter-vrf から参照させます。次に，VRF 3 の経路だけ permit になる route-map を設定します。この route-map を VRF 2 の import inter-vrf から参照させます。

[コマンドによる設定]

1.
```
(config)# ip prefix-list PERMITVRF2 seq 10 permit 172.16.1.0/24
(config)# route-map VRF2PERMIT permit 10
(config-route-map)# match vrf 2
(config-route-map)# match ip address prefix-list PERMITVRF2
(config-route-map)# exit
```

VRF 2 の経路が permit になるように設定します。

2.
```
(config)# vrf definition 3
(config-vrf)# import inter-vrf VRF2PERMIT
(config-vrf)# exit
```

1.のフィルタ設定を VRF 3 のエクストラネットに適用して，VRF 2 の経路を VRF 3 に導入するように設定します。

3.
```
(config)# ip prefix-list PERMITVRF3 seq 10 permit 172.16.3.0/24
(config)# route-map VRF3PERMIT permit 10
(config-route-map)# match vrf 3
(config-route-map)# match ip address prefix-list PERMITVRF3
(config-route-map)# exit
```
VRF 3 の経路が permit になるように設定します。

4.
```
(config)# vrf definition 2
(config-vrf)# import inter-vrf VRF3PERMIT
(config-vrf)# exit
```
3.のフィルタ設定を VRF 2 のエクストラネットに適用して，VRF 3 の経路を VRF 2 に導入するように設定します。

[注意事項]

import inter-vrf から参照される route-map が設定されていない場合，他 VRF またはグローバルネットワークにあるすべての経路をインポートします。意図しない経路をインポートしないように，必ず route-map，import inter-vrf の順に設定してください。

(2) プロトコルによる VRF 間経路の広告

VRF 3 の経路（172.16.3.0/24）を VRF 2 のネットワークへ導入します。導入した VRF 3 の経路を VRF 2 の OSPF で広告します。

[設定のポイント]

VRF 間経路フィルタリングをするには，import inter-vrf を設定してください。経路を VRF でフィルタリングするには，route-map を使用してください。route-map 中の宛先ネットワーク条件の指定には，ip prefix-list を使用してください。OSPF で他 VRF またはグローバルネットワークからインポートした経路を広告するには，redistribute を設定してください。

まず，VRF 3 の経路だけ permit になる route-map を設定します。次に，この route-map を import inter-vrf から参照させて，VRF 3 の経路を VRF 2 へ導入するように設定します。最後に，他 VRF またはグローバルネットワークからインポートした経路を広告するように，VRF 2 の OSPF に redistribute を設定します。

[コマンドによる設定]

1.
```
(config)# ip prefix-list PERMITVRF3 seq 10 permit 172.16.3.0/24
(config)# route-map VRF3TO2 permit 10
(config-route-map)# match vrf 3
(config-route-map)# match ip address prefix-list PERMITVRF3
(config-route-map)# exit
```
VRF 3 の経路が permit になるように設定します。

2.
```
(config)# vrf definition 2
(config-vrf)# import inter-vrf VRF3TO2
(config-vrf)# exit
```
1.のフィルタ設定を VRF 2 のエクストラネットに適用して，VRF 3 の経路を VRF 2 に導入します。

3.
```
(config)# router ospf 1 vrf 2
```

(config-router)# redistribute extra-vrf

他 VRF またはグローバルネットワークからインポートした経路を，VRF 2 の OSPF ドメイン 1 で広告します。

[注意事項]

import inter-vrf から参照される route-map が設定されていない場合，他 VRF またはグローバルネットワークにあるすべての経路をインポートします。意図しない経路をインポートしないように，必ず route-map，import inter-vrf の順に設定してください。

(3)　特定 VRF のディスタンス値の変更

VRF 2 および VRF 3 の経路をグローバルネットワークへ導入します。VRF 2 の経路だけディスタンス値を 150 にします。

[設定のポイント]

VRF 間経路フィルタリングをするには，import inter-vrf を設定してください。経路を VRF でフィルタリングするには，route-map を使用してください。

まず，VRF 2 の経路が permit になり，ディスタンス値を 150 に変更する route-map を設定します。次に，同じ route-map の別シーケンス番号に VRF 3 の経路が permit になるよう設定します。

この route-map を import inter-vrf から参照させて，特定 VRF のディスタンス値を変更するフィルタリングを設定します。

[コマンドによる設定]

1. **(config)# route-map VRF2AND3PERMIT permit 10**
   (config-route-map)# match vrf 2
   (config-route-map)# set distance 150
   (config-route-map)# exit
   VRF 2 の経路が permit になり，ディスタンス値を 150 に変更するように設定します。
2. **(config)# route-map VRF2AND3PERMIT permit 20**
   (config-route-map)# match vrf 3
   (config-route-map)# exit
   VRF 3 の経路が permit になるように設定します。
3. **(config)# vrf definition global**
   (config-vrf)# import inter-vrf VRF2AND3PERMIT
   1.，2.のフィルタ設定をグローバルネットワークのエクストラネットに適用し，VRF 2 および VRF 3 の経路をグローバルネットワークに導入して，VRF 2 の経路のディスタンス値を 150 に変更するように設定します。

[注意事項]

import inter-vrf から参照される route-map が設定されていない場合，他 VRF またはグローバルネットワークにあるすべての経路をインポートします。意図しない経路をインポートしないように，必ず route-map，import inter-vrf の順に設定してください。

23.3　コンフィグレーション（IPv6）

23.3.1　コンフィグレーションコマンド一覧

経路フィルタリングのコンフィグレーションコマンド一覧を次の表に示します。

表 23-26　コンフィグレーションコマンド一覧

コマンド名	説明
distribute-list in (BGP4+)	BGP4+で学習した経路をルーティングテーブルに取り込むかどうかをフィルタに従って制御します。
distribute-list in (OSPFv3)	OSPFv3 で学習した経路をルーティングテーブルに取り込むかどうかをフィルタに従って制御します。
distribute-list in (RIPng)	RIPng で学習した経路をルーティングテーブルに取り込むかどうかをフィルタに従って制御します。
distribute-list out (BGP4+)	BGP4+で広告する経路をフィルタに従って制御します。
distribute-list out (OSPFv3)	OSPFv3 で広告する経路をフィルタに従って制御します。
distribute-list out (RIPng)	RIPng で広告する経路をフィルタに従って制御します。
ip as-path access-list	AS_PATH 属性フィルタとして動作する ip as-path access-list を設定します。
ip community-list	COMMUNITIES 属性フィルタとして動作する community-list を設定します。
ipv6 prefix-list	ipv6 prefix-list を設定します。
match as-path	route-map に AS_PATH 属性によるフィルタ条件を設定します。
match community	route-map に COMMUNITIES 属性によるフィルタ条件を設定します。
match interface	route-map にインタフェースによるフィルタ条件を設定します。
match ipv6 address	route-map に IPv6 宛先プレフィックスによるフィルタ条件を設定します。
match ipv6 route-source	route-map に送信元 IPv6 アドレスによるフィルタ条件を設定します。
match origin	route-map に ORIGIN 属性によるフィルタ条件を設定します。
match protocol	route-map にルーティングプロトコルによるフィルタ条件を設定します。
match route-type	route-map に経路種別によるフィルタ条件を設定します。
match tag	route-map にタグによるフィルタ条件を設定します。
match vrf	route-map に VRF によるフィルタ条件を設定します。
neighbor in (BGP4+)	BGP4+学習経路フィルタリングに使用するフィルタを設定します。
neighbor out (BGP4+)	BGP4+広告経路フィルタリングに使用するフィルタを設定します。
redistribute (BGP4+)	BGP4+から広告する経路のプロトコル種別を設定します。

コマンド名	説明
redistribute (OSPFv3)	OSPFv3 から広告する経路のプロトコル種別を設定します。
redistribute (RIPng)	RIPng から広告する経路のプロトコル種別を設定します。
route-map	route-map を設定します。
set as-path prepend count	経路情報に追加する AS_PATH 番号の数を設定します。
set community	経路属性の COMMUNITIES 属性を置き換えます。
set community-delete	経路属性の COMMUNITIES 属性の削除を設定します。
set distance	経路情報の優先度を設定します。
set local-preference	経路情報の LOCAL_PREF 属性を設定します。
set metric	経路情報のメトリックを設定します。
set metric-type	経路情報のメトリック種別，またはメトリック値を設定します。
set origin	経路情報の ORIGIN 属性を設定します。
set tag	経路情報のタグを設定します。
deny (ipv6 access-list)※1	IPv6 フィルタでのアクセスを拒否する条件を指定します。
ipv6 access-list※1	IPv6 フィルタとして動作するアクセスリストを設定します。
ipv6 access-list resequence※1	IPv6 フィルタのフィルタ条件適用順序のシーケンス番号を再設定します。
permit (ipv6 access-list)※1	IPv6 フィルタでのアクセスを許可する条件を指定します。
ipv6 import inter-vrf※2	他 VRF またはグローバルネットワークからインポートする経路をフィルタに従って制御します。
ipv6 router rip※3	ルーティングプロトコル RIPng に関する動作情報を設定します。
ipv6 router ospf※4	ルーティングプロトコル OSPFv3 に関する動作情報を設定します。
router bgp※5	ルーティングプロトコル BGP（BGP4 および BGP4+）に関する動作情報を設定します。

注※1
「コンフィグレーションコマンドレファレンス Vol.2　7. アクセスリスト」を参照してください。

注※2
「コンフィグレーションコマンドレファレンス Vol.3　5. VRF」を参照してください。

注※3
「コンフィグレーションコマンドレファレンス Vol.3　18. RIPng」を参照してください。

注※4
「コンフィグレーションコマンドレファレンス Vol.3　20. OSPFv3」を参照してください。

注※5
「コンフィグレーションコマンドレファレンス Vol.3　21. BGP4/BGP4+」を参照してください。

23.3.2　RIPng 学習経路フィルタリング

(1)　特定宛先ネットワークの経路の学習

2001:db8:811:ff01::/64 宛ての RIPng 経路だけを学習して，ほかの宛先ネットワークへの RIPng 経路を学習しないように設定します。

[設定のポイント]

学習経路フィルタリングをするには，distribute-list in を設定してください。経路を宛先ネットワークでフィルタするには，ipv6 prefix-list を使用してください。

まず，2001:db8:811:ff01::/64 宛ての経路だけ permit になる ipv6 prefix-list を設定します。この ipv6 prefix-list を distribute-list in から参照することで，経路宛先ネットワークによる RIPng 学習経路フィルタリングをするように設定します。

[コマンドによる設定]

1. **(config)# ipv6 prefix-list ONLY0811ff01 seq 10 permit 2001:db8:811:ff01::/64**

   2001:db8:811:ff01::/64 だけ permit になる ipv6 prefix-list を設定します。ONLY0811ff01 にはほかに条件がないので，宛先アドレスやマスク長の異なる経路は deny になります。

2. **(config)# ipv6 router rip**

   (config-rtr-rip)# distribute-list prefix-list ONLY0811ff01 in

   RIPng で学習する経路を ONLY0811ff01 でフィルタするように設定します。

(2)　特定インタフェースについて，特定宛先ネットワークの経路の学習

ポート 1/1 から学習した経路について，2001:db8:811:ff01::/64 宛ての経路だけを学習して，ほかの宛先ネットワークへの経路を学習しないように設定します。ポート 1/1 以外のインタフェースから学習した経路はフィルタしません。

[設定のポイント]

RIPng インタフェース個別に学習経路フィルタリングをするには，distribute-list in に<Interface>を指定してください。

まず，2001:db8:811:ff01::/64 宛ての経路だけ permit になる ipv6 prefix-list を設定します。この ipv6 prefix-list を distribute-list in gigabitethernet 1/1 から参照することで，ポート 1/1 から学習した経路についてだけ，経路宛先ネットワークによる RIPng 学習経路フィルタリングをするように設定します。

[コマンドによる設定]

1. **(config)# ipv6 prefix-list ONLY0811ff01 seq 10 permit 2001:db8:811:ff01::/64**

   2001:db8:811:ff01::/64 だけ permit になる ipv6 prefix-list を設定します。ONLY0811ff01 にはほかに条件がないので，宛先アドレスやマスク長の異なる経路は deny になります。

2. **(config)# ipv6 router rip**

   (config-rtr-rip)# distribute-list prefix-list ONLY0811ff01 in gigabitethernet 1/1

   ポート 1/1 から学習した経路だけを，ONLY0811ff01 でフィルタするように設定します。

(3)　タグ値と宛先ネットワークの両方による学習経路フィルタリング

宛先ネットワークが 2001:db8::/32 に含まれていて，かつタグ値が 15 ではない経路を学習しないようにします。それ以外の RIPng 経路はすべて学習するようにします。

[設定のポイント]

宛先ネットワーク以外を条件とする場合や経路属性を変更したい場合は，route-map を使用します。この route-map を distribute-list in から参照します。

まず，2001:db8::/32 に含まれるプレフィックスだけが permit になる ipv6 prefix-list を設定します。次に，この ipv6 prefix-list が permit であり，かつタグ値が 15 でない経路だけが deny になる route-map を設定します。

最後に，この route-map を distribute-list in から参照することで，タグ値と宛先ネットワークの両方による RIPng 学習経路フィルタリングを設定します。

[コマンドによる設定]

1. **(config)# ipv6 prefix-list LONGER2001db8 seq 10 permit 2001:db8::/32 ge 32 le 128**

   2001:db8::/32 に含まれる経路だけ permit になる ipv6 prefix-list を設定します。

2. **(config)# route-map TAG permit 10**

   (config-route-map)# match ipv6 address prefix-list LONGER2001db8

   (config-route-map)# match tag 15

   (config-route-map)# exit

   2001:db8::/32 に含まれて，かつタグ値が 15 の経路が permit になるように設定します。

3. **(config)# route-map TAG deny 20**

   (config-route-map)# match ipv6 address prefix-list LONGER2001db8

   (config-route-map)# exit

   シーケンス番号 10 にマッチしないで，かつ 2001:db8::/32 に含まれる経路が deny になるように設定します。

4. **(config)# route-map TAG permit 30**

   (config-route-map)# exit

   シーケンス番号 10，20 の両方にマッチしなかった経路が permit になるように設定します。

5. **(config)# ipv6 router rip**

   (config-rtr-rip)# distribute-list route-map TAG in

   このフィルタを RIPng 学習経路フィルタリングに適用して，2001:db8::/32 に含まれてかつタグ値が 15 でない RIPng 経路だけを学習しないように設定します。

(4)　宛先ネットワークによるディスタンス値の変更

宛先ネットワークが 2001:db8::/32 に含まれている RIPng 学習経路について，OSPFv3 経路よりも優先されるように，ディスタンス値を 50 にします。

[設定のポイント]

まず，2001:db8::/32 を含む経路だけ permit になる ipv6 prefix-list を設定します。次に，この ipv6 prefix-list が permit であればディスタンス値を 50 に変更する route-map を設定します。

最後に，この route-map を distribute-list in から参照することで，宛先ネットワークに基づいてディスタンス値を変更する RIPng 学習経路フィルタリングを設定します。

[コマンドによる設定]

1. **(config)# ipv6 prefix-list LONGER2001db8 seq 10 permit 2001:db8::/32 ge 32 le 128**

   2001:db8::/32 に含まれる経路だけ permit になる ipv6 prefix-list を設定します。

2. **(config)# route-map Distance50 permit 10**

```
(config-route-map)# match ipv6 address prefix-list LONGER2001db8
(config-route-map)# set distance 50
(config-route-map)# exit
```

2001:db8::/32 に含まれる経路を，ディスタンス値を 50 に変更して permit になるように設定します。

3.
```
(config)# route-map Distance50 permit 20
(config-route-map)# exit
```

シーケンス番号 10 にマッチしなかった経路を，何も変更しないで permit になるように設定します。

4.
```
(config)# ipv6 router rip
(config-rtr-rip)# distribute-list route-map Distance50 in
```

このフィルタを RIPng 学習経路フィルタリングに適用して，2001:db8::/32 に含まれる RIPng 学習経路だけ，ディスタンス値を 50 に変更するように設定します。

23.3.3　RIPng 広告経路フィルタリング

(1)　特定プロトコル経路の広告

スタティック経路と OSPFv3 ドメイン 1 の経路を RIPng で広告するように設定します。

[設定のポイント]

デフォルトでは広告しない経路を広告させるには，redistribute を設定します。redistribute には，広告したいプロトコルを指定します。

このとき，OSPFv3 経路の広告設定にメトリック値も指定してください。OSPFv3 経路や BGP4+経路は，メトリック値を指定しないと広告されません。

[コマンドによる設定]

1.
```
(config)# ipv6 router rip
(config-rtr-rip)# redistribute static
```

スタティック経路を RIPng へ広告します。

2.
```
(config-rtr-rip)# redistribute ospf 1 metric 2
```

OSPFv3 ドメイン 1 の経路を，メトリック値 2 で広告します。

(2)　特定プロトコルの特定宛先ネットワーク経路の広告

スタティック経路と，OSPFv3 経路の中で宛先ネットワークが 2001:db8:811:ff01::/64 であるものだけを RIPng で広告します。

[設定のポイント]

学習元プロトコル別に広告経路フィルタリングをする場合，redistribute に route-map を指定してください。route-map で宛先ネットワークを条件にするには，ipv6 prefix-list を使用してください。

まず，2001:db8:811:ff01::/64 宛ての経路だけが permit になる ipv6 prefix-list を設定します。次に，この ipv6 prefix-list を条件とする route-map を設定します。最後に，スタティック経路と OSPFv3 経路を redistribute で指定します。OSPFv3 経路の redistribute には，この route-map を指定します。

[コマンドによる設定]

1.
```
(config)# ipv6 prefix-list ONLY0811ff01 seq 10 permit 2001:db8:811:ff01::/64
```

2001:db8:811:ff01::/64 だけ permit になる ipv6 prefix-list を設定します。ONLY0811ff01 にはほかに条件がないので，宛先アドレスやマスク長の異なる経路は deny になります。

2. (config)# route-map ONLY0811ff01 permit 10
   (config-route-map)# match ipv6 address prefix-list ONLY0811ff01
   (config-route-map)# exit
   宛先ネットワークが 2001:db8:811:ff01::/64 の経路だけ permit になる route-map を設定します。
3. (config)# ipv6 router rip
   (config-rtr-rip)# redistribute static
   スタティック経路を RIPng で広告します。
4. (config-rtr-rip)# redistribute ospf 1 metric 2 route-map ONLY0811ff01
   OSPFv3 ドメイン 1 の経路を ONLY0811ff01 でフィルタして，permit になった経路だけをメトリック値 2 で広告します。

(3)　特定宛先ネットワーク経路の広告抑止

2001:db8:811:ff01::/64 宛ての経路に限り，RIPng では広告しないようにします。

[設定のポイント]

経路の学習元プロトコルと関係なく広告経路フィルタリングする場合，distribute-list out を使用してください。

まず, 2001:db8:811:ff01::/64 宛ての経路だけ deny になる ipv6 prefix-list を設定します。この ipv6 prefix-list を distribute-list out から参照することで，経路宛先ネットワークによる RIPng 広告経路フィルタリングをするように設定します。

[コマンドによる設定]

1. (config)# ipv6 prefix-list OMIT0811ff01 seq 10 deny 2001:db8:811:ff01::/64
   2001:db8:811:ff01::/64 が deny になる ipv6 prefix-list を設定します。
2. (config)# ipv6 prefix-list OMIT0811ff01 seq 100 permit ::/0 ge 0 le 128
   任意の宛先アドレスやマスク長に対して permit になる ipv6 prefix-list を設定します。
   OMIT0811ff01 にはほかに条件がないので，2001:db8:811:ff01::/64 だけが deny になるフィルタになります。
3. (config)# ipv6 router rip
   (config-rtr-rip)# distribute-list prefix-list OMIT0811ff01 out
   RIPng で広告する経路すべてを，OMIT0811ff01 でフィルタするように設定します。

(4)　広告先インタフェース個別の広告経路フィルタリング

RIPng インタフェースであるポート 1/1 からは，2001:db8:811:ff01::/64 だけを広告します。RIPng インタフェースであるポート 1/2 からは，2001:db8:811:ff01::/64 以外の経路を広告します。そのほかの RIPng インタフェースでは，インタフェース個別のフィルタリングをしません。

[設定のポイント]

RIPng インタフェース個別に経路フィルタリングする必要がある場合，distribute-list out に <Interface>を指定してください。

まず，2001:db8:811:ff01::/64 だけ permit になる ipv6 prefix-list と，2001:db8:811:ff01::/64 だけ deny になる ipv6 prefix-list を設定します。次に，RIPng インタフェースであるポート 1/1 とポート 1/2 に distribute-list out <Interface>を設定します。distribute-list out <Interface>には，その RIPng インタフェースに適切な ipv6 prefix-list を指定します。

[コマンドによる設定]

1. **(config)# ipv6 prefix-list ONLY0811ff01 seq 10 permit 2001:db8:811:ff01::/64**
   2001:db8:811:ff01::/64 だけ permit になる ipv6 prefix-list を設定します。ONLY0811ff01 にはほかに条件がないので，宛先アドレスやマスク長の異なる経路は deny になります。
2. **(config)# ipv6 prefix-list OMIT0811ff01 seq 10 deny 2001:db8:811:ff01::/64**
   2001:db8:811:ff01::/64 だけ deny になる ipv6 prefix-list を設定します。
3. **(config)# ipv6 prefix-list OMIT0811ff01 seq 100 permit ::/0 ge 0 le 128**
   任意の宛先アドレスやマスク長に対して permit になる ipv6 prefix-list を設定します。
   OMIT0811ff01 にはほかに条件がないので，2001:db8:811:ff01::/64 だけが deny になるフィルタになります。
4. **(config)# ipv6 router rip**
   (config-rtr-rip)# distribute-list prefix-list ONLY0811ff01 out gigabitethernet 1/1
   ポート 1/1 から広告する経路を ONLY0811ff01 でフィルタするように設定します。
5. **(config-rtr-rip)# distribute-list prefix-list OMIT0811ff01 out gigabitethernet 1/2**
   ポート 1/2 から広告する経路を OMIT0811ff01 でフィルタするように設定します。

(5) タグ値による広告経路の制御

直結経路を，タグ値 210 を付けて広告します。スタティック経路の中で，タグ値が 211 のものだけを広告します。その上で，RIPng 経路の中で，タグ値が 210 または 211 の経路を RIPng から広告しないようにします。こうすることで，本装置が RIPng への広告を始めた経路が，本装置を経由してループしないようにします。

[設定のポイント]

宛先ネットワーク以外を条件とする場合，またはメトリック値以外の経路属性を変更したい場合は，route-map を使用します。route-map は，redistribute や distribute-list out で指定できます。

直結経路用のタグ値を 210 にする route-map と，スタティック経路用のタグ値 211 だけが permit になる route-map と，RIPng 経路用のタグ値が 210 または 211 の経路が deny になる route-map をそれぞれ設定します。

[コマンドによる設定]

1. **(config)# route-map ConnectedToRIPng permit 10**
   (config-route-map)# set tag 210
   (config-route-map)# exit
   タグ値を 210 にする route-map を設定します。
2. **(config)# route-map StaticToRIPng permit 10**
   (config-route-map)# match tag 211
   (config-route-map)# exit
   タグ値が 211 の経路だけ permit になる route-map を設定します。
3. **(config)# route-map RIPngToRIPng deny 10**
   (config-route-map)# match tag 210 211
   (config-route-map)# exit
   (config)# route-map RIPngToRIPng permit 20
   (config-route-map)# exit

タグ値が 210 または 211 の経路が deny になり，そのほかの経路が permit になる route-map を設定します。

4. **(config)# ipv6 router rip**
   (config-rtr-rip)# redistribute connected route-map ConnectedToRIPng
   直結経路を RIPng へ広告します。広告条件に ConnectedToRIPng を指定します。
5. **(config-rtr-rip)# redistribute static route-map StaticToRIPng**
   スタティック経路を RIPng へ広告します。広告条件に StaticToRIPng を指定します。
6. **(config-rtr-rip)# redistribute rip route-map RIPngToRIPng**
   RIPng 経路を RIPng へ広告します。広告条件に RIPngToRIPng を指定します。

23.3.4　OSPFv3 学習経路フィルタリング

(1)　特定宛先ネットワークの経路の学習

2001:db8:811:ff01::/64 宛ての経路だけを学習して，ほかの宛先ネットワークへの経路を学習しないように設定します。

[設定のポイント]

学習経路フィルタリングをするには，distribute-list in を設定してください。経路を宛先ネットワークでフィルタするには，ipv6 prefix-list を使用してください。

まず，2001:db8:811:ff01::/64 宛ての経路だけ permit になる ipv6 prefix-list を設定します。この ipv6 prefix-list を distribute-list in から参照することで，経路宛先ネットワークによる OSPFv3 学習経路フィルタリングをするように設定します。

[コマンドによる設定]

1. **(config)# ipv6 prefix-list ONLY0811ff01 seq 10 permit 2001:db8:811:ff01::/64**
   2001:db8:811:ff01::/64 だけ permit になる ipv6 prefix-list を設定します。ONLY0811ff01 にはほかに条件がないので，宛先アドレスやマスク長の異なる経路は deny になります。
2. **(config)# ipv6 router ospf 1**
   (config-rtr)# distribute-list prefix-list ONLY0811ff01 in
   学習した OSPFv3 の AS 外経路を，ONLY0811ff01 でフィルタするように設定します。

(2)　タグ値による学習経路フィルタリング

タグ値が 15 の経路を学習しないようにします。それ以外の経路は学習します。

[設定のポイント]

宛先ネットワーク以外を条件とする場合や経路属性を変更したい場合は，route-map を使用します。この route-map を distribute-list in から参照します。

まず，タグ値が 15 である経路が deny になる route-map を設定します。次に，この route-map を distribute-list in から参照することで，タグ値による OSPFv3 学習経路フィルタリングを設定します。

[コマンドによる設定]

1. **(config)# route-map TAG15DENY deny 10**
   (config-route-map)# match tag 15
   (config-route-map)# exit

タグ値が 15 の経路が deny になるように設定します。

2. **(config)# route-map TAG15DENY permit 20**
   (config-route-map)# exit
   シーケンス番号 10 にマッチしない経路が permit になるように設定します。
3. **(config)# ipv6 router ospf 1**
   (config-rtr)# distribute-list route-map TAG15DENY in
   このフィルタを OSPFv3 学習経路フィルタリングに適用して，タグ値が 15 である AS 外経路を学習しないように設定します。

(3)　宛先ネットワークによるディスタンス値の変更

宛先ネットワークが 2001:db8::/32 に含まれている AS 外経路よりも RIPng 経路の方が優先されるように，ディスタンス値を 150 にします。

[設定のポイント]

宛先ネットワーク以外を条件とする場合や経路属性を変更したい場合は，route-map を使用します。route-map は，distribute-list in で指定して使用します。

まず，2001:db8::/32 を含む経路が permit になる ipv6 prefix-list を設定します。次に，この ipv6 prefix-list が permit になったらディスタンス値を 150 に変更する route-map を設定します。

最後に，この route-map を distribute-list in から参照することで，宛先ネットワークに基づいてディスタンス値を変更する OSPFv3 学習経路フィルタリングを設定します。

[コマンドによる設定]

1. **(config)# ipv6 prefix-list LONGER2001db8 seq 10 permit 2001:db8::/32 ge 32 le 128**
   2001:db8::/32 に含まれる経路だけ permit になる ipv6 prefix-list を設定します。
2. **(config)# route-map Distance150 permit 10**
   (config-route-map)# match ipv6 address prefix-list LONGER2001db8
   (config-route-map)# set distance 150
   (config-route-map)# exit
   2001:db8::/32 に含まれる経路を，ディスタンス値を 150 に変更して permit になるように設定します。
3. **(config)# route-map Distance150 permit 20**
   (config-route-map)# exit
   シーケンス番号 10 にマッチしなかった経路を，何も変更しないで permit になるように設定します。
4. **(config)# ipv6 router ospf 1**
   (config-rtr)# distribute-list route-map Distance150 in
   このフィルタを OSPFv3 学習経路フィルタリングに適用して，2001:db8::/32 に含まれる AS 外経路だけ，ディスタンス値を 150 に変更するように設定します。

23.3.5　OSPFv3 広告経路フィルタリング

(1)　特定プロトコル経路の広告

スタティック経路と RIPng 経路を OSPFv3 ドメイン 1 へ広告します。

[設定のポイント]

デフォルトでは広告しない経路を広告させるには，redistribute を設定します。redistribute には，広告したいプロトコルを指定します。

[コマンドによる設定]

1. **(config)# ipv6 router ospf 1**
   (config-rtr)# redistribute static
   スタティック経路を広告します。
2. **(config-rtr)# redistribute rip**
   RIPng 経路を広告します。

(2)　特定プロトコルの特定宛先ネットワーク経路の広告

スタティック経路と，RIPng 経路の中で宛先ネットワークが 2001:db8:811:ff01::/64 であるものだけを OSPFv3 ドメイン 1 へ広告します。

[設定のポイント]

学習元プロトコル別に広告経路フィルタリングをする場合, redistribute に route-map を指定してください。route-map 中で宛先ネットワーク条件を指定するには，ipv6 prefix-list を設定して，match ipv6 address で参照してください。

まず，2001:db8:811:ff01::/64 宛ての経路だけが permit になる ipv6 prefix-list を設定します。次に，この ipv6 prefix-list を条件とする route-map を設定します。最後に，スタティック経路と RIPng 経路を広告するように，redistribute を設定します。RIPng 経路の redistribute には，この route-map を指定します。

[コマンドによる設定]

1. **(config)# ipv6 prefix-list ONLY0811ff01 seq 10 permit 2001:db8:811:ff01::/64**
   2001:db8:811:ff01::/64 だけ permit になる ipv6 prefix-list を設定します。ONLY0811ff01 にはほかに条件がないので，宛先アドレスやマスク長の異なる経路は deny になります。
2. **(config)# route-map ONLY0811ff01 permit 10**
   (config-route-map)# match ipv6 address prefix-list ONLY0811ff01
   (config-route-map)# exit
   宛先ネットワークが 2001:db8:811:ff01::/64 の経路だけ permit になる route-map を設定します。
3. **(config)# ipv6 router ospf 1**
   (config-rtr)# redistribute static
   スタティック経路を OSPFv3 ドメイン 1 へ広告します。
4. **(config-rtr)# redistribute rip route-map ONLY0811ff01**
   RIPng 経路を ONLY0811ff01 でフィルタして，permit になった経路だけを広告します。

(3)　特定宛先ネットワーク経路の広告抑止

スタティック経路と RIPng 経路を OSPFv3 ドメイン 1 へ広告します。ただし，2001:db8:811:ff01::/64 宛ての経路に限り，OSPFv3 ドメイン 1 へ広告しないようにします。

[設定のポイント]

経路の学習元プロトコルと関係なく広告経路フィルタリングする場合，distribute-list out を使用してください。

まず，2001:db8:811:ff01::/64 宛ての経路だけ deny になる ipv6 prefix-list を設定します。この ipv6 prefix-list を distribute-list out から参照することで，経路宛先ネットワークによる広告経路フィルタリングをするように設定します。

最後に，スタティック経路と RIPng 経路を広告するように，redistribute を設定します。

[コマンドによる設定]

1. **(config)# ipv6 prefix-list OMIT0811ff01 seq 10 deny 2001:db8:811:ff01::/64**

   2001:db8:811:ff01::/64 が deny になる ipv6 prefix-list を設定します。

2. **(config)# ipv6 prefix-list OMIT0811ff01 seq 100 permit ::/0 ge 0 le 128**

   任意の宛先アドレスやマスク長に対して permit になる ipv6 prefix-list を設定します。
   OMIT0811ff01 にはほかに条件がないので，2001:db8:811:ff01::/64 だけが deny になるフィルタになります。

3. **(config)# ipv6 router ospf 1**

   (config-rtr)# distribute-list prefix-list OMIT0811ff01 out

   広告経路を OMIT0811ff01 でフィルタするように設定します。

4. **(config-rtr)# redistribute static**

   (config-rtr)# redistribute rip

   スタティック経路と RIPng 経路を広告するように設定します。

(4) OSPFv3 ドメイン間の経路広告

OSPFv3 ドメイン 1 と OSPFv3 ドメイン 2 の間で，相互に経路を広告し合います。

OSPFv3 ドメイン 1 の経路に，タグ値 1001 を付けて OSPFv3 ドメイン 2 に広告します。OSPFv3 ドメイン 2 の経路にタグ値 1001 が付いているときは，OSPFv3 ドメイン 1 には広告しません。こうすると，OSPFv3 ドメイン 1 の経路が OSPFv3 ドメイン 2 を経由して OSPFv3 ドメイン 1 に広告し戻すことがなくなるので，ルーティングループを防げます。

同様に，OSPFv3 ドメイン 2 の経路に，タグ値 1002 を付けて OSPFv3 ドメイン 1 に広告します。
OSPFv3 ドメイン 1 の経路にタグ値 1002 が付いているときは，OSPFv3 ドメイン 2 には広告しません。

[設定のポイント]

宛先ネットワーク以外を条件とする場合，またはメトリック値以外の経路属性を変更したい場合は，route-map を使用します。route-map は，redistribute や distribute-list out で指定できます。

OSPFv3 ドメイン 1 への広告用に，タグ値 1001 が付いていれば deny，それ以外はタグ値 1002 を付けて permit になる route-map を設定します。これを，OSPFv3 ドメイン 1 の OSPFv3 ドメイン 2 経路を広告する redistribute に指定します。

同様に，OSPFv3 ドメイン 2 への広告用に，タグ値 1002 が付いていれば deny，それ以外はタグ値 1001 を付けて permit になる route-map を設定します。これを，OSPFv3 ドメイン 2 の OSPFv3 ドメイン 1 経路を広告する redistribute に指定します。

[コマンドによる設定]

1. **(config)# route-map OSPF2to1 deny 10**

   (config-route-map)# match tag 1001

   (config-route-map)# exit

   タグ値が 1001 の経路が deny になるように OSPF2to1 を設定します。

2. **(config)# route-map OSPF2to1 permit 20**

```
(config-route-map)# set tag 1002
(config-route-map)# exit
```

上記を満たさない場合，タグ値を 1002 にするように設定します。

3.
```
(config)# ipv6 router ospf 1
(config-rtr)# redistribute ospf 2 route-map OSPF2to1
(config-rtr)# exit
```

OSPFv3 ドメイン 2 経路を OSPFv3 ドメイン 1 へ広告します。OSPF2to1 をフィルタとして指定します。

4.
```
(config)# route-map OSPF1to2 deny 10
(config-route-map)# match tag 1002
(config-route-map)# exit
(config)# route-map OSPF1to2 permit 20
(config-route-map)# set tag 1001
(config-route-map)# exit
```

タグ値が 1002 の場合は deny になり，そうでない場合はタグ値を 1001 とするように route-map OSPF1to2 を設定します。

5.
```
(config)# ipv6 router ospf 2
(config-rtr)# redistribute ospf 1 route-map OSPF1to2
(config-rtr)# exit
```

OSPFv3 ドメイン 1 経路を OSPFv3 ドメイン 2 へ広告します。OSPF1to2 をフィルタとして指定します。

23.3.6　BGP4+学習経路フィルタリング

(1)　全ピア共通の条件付き経路の学習

宛先ネットワークが 2001:db8::/32 に含まれる BGP4+経路を学習しないで，ほかの宛先ネットワークへの BGP4+経路を学習するように設定します。

[設定のポイント]

全ピア共通に学習経路フィルタリングをするには，distribute-list in を設定してください。宛先ネットワークによるフィルタには，ipv6 prefix-list を使用してください。

まず，2001:db8::/32 に含まれる経路と一致すると deny になる ipv6 prefix-list を設定します。この ipv6 prefix-list を distribute-list in から参照することで，経路宛先ネットワークによる BGP4+学習経路フィルタリングをするように設定します。

[コマンドによる設定]

1.
```
(config)# ipv6 prefix-list LONGER2001db8DENY seq 10 deny 2001:db8::/32 ge 32 le 128
(config)# ipv6 prefix-list LONGER2001db8DENY seq 20 permit ::/0 ge 0 le 128
```

2001:db8::/32 に含まれるプレフィックスだけ deny になり，それ以外のプレフィックスでは permit になる ipv6 prefix-list を設定します。

2.
```
(config)# router bgp 65531
(config-router)# address-family ipv6
(config-router-af)# distribute-list prefix-list LONGER2001db8DENY in
```

この ipv6 prefix-list をピア共通に学習経路フィルタリングに適用するように設定します。

3. **(config-router-af)# end**

   # clear ipv6 bgp * in

   学習経路フィルタリング設定の変更を動作に反映します。

(2) ピア個別の条件付き経路の学習

外部ピアについて，宛先ネットワークが 2001:db8::/32 に含まれる経路を除く，AS_PATH 属性が「65532 65533」の経路を学習します。学習した経路の LOCAL_PREF 属性を 200 に設定します。そのほかの経路は学習しません。

[設定のポイント]

BGP4+ピア個別に学習経路フィルタリングをするには，neighbor in を設定してください。宛先ネットワーク以外の条件比較や属性変更には route-map を使用してください。

まず，2001:db8::/32 に含まれるなら permit になる ipv6 prefix-list と，AS_PATH 属性が「65532 65533」である場合に permit になる ip as-path access-list を設定します。次に，この二つの条件を組み合わせた route-map を設定します。最後に，この条件でフィルタさせたいピアについて neighbor in を設定します。

[コマンドによる設定]

1. **(config)# ipv6 prefix-list LONGER2001db8 seq 10 permit 2001:db8::/32 ge 32 le 128**

   プレフィックスが 2001:db8::/32 に含まれる場合に permit になる ipv6 prefix-list を設定します。

2. **(config)# ip as-path access-list 2 permit "^65532_65533$"**

   AS_PATH 属性が「65532 65533」である場合に permit になる ip as-path access-list を設定します。

3. **(config)# route-map BGP65532IN deny 10**

   (config-route-map)# match ipv6 address prefix-list LONGER2001db8

   (config-route-map)# exit

   route-map BGP65502IN を，宛先ネットワークが 2001:db8::/32 に含まれていたら deny になるように設定します。

4. **(config)# route-map BGP65532IN permit 20**

   (config-route-map)# match as-path 2

   (config-route-map)# set local-preference 200

   (config-route-map)# exit

   AS_PATH 属性が「65532 65533」と一致したら，LOCAL_PREF 属性を 200 にして permit になるように設定します。BGP65532IN にはほかに条件がないので，ここまでの条件のどれとも一致しない経路は deny になります。

5. **(config)# router bgp 65531**

   (config-router)# neighbor 2001:db8:811:1::1 remote-as 65532

   (config-router)# address-family ipv6

   (config-router-af)# neighbor 2001:db8:811:1::1 route-map BGP65532IN in

   外部ピアの受信経路フィルタリングに BGP65532IN を使用するように設定します。

6. **(config-router-af)# end**

   # clear ipv6 bgp * in

   学習経路フィルタリング設定の変更を動作に反映します。

23.3.7　BGP4+広告経路フィルタリング

(1)　他プロトコルの経路を広告する

直結経路とスタティック経路の中で，宛先ネットワークが自 AS のネットワーク（2001:db8::/32）の内部である経路だけを BGP4+へ広告します。

[設定のポイント]

デフォルトでは広告しない経路を広告させるには，redistribute を設定します。redistribute には，広告したいプロトコルを指定します。

redistribute に，経路広告条件の route-map を指定します。route-map 中の宛先ネットワーク条件の指定には ipv6 prefix-list を使用します。

[コマンドによる設定]

1. **(config)# ipv6 prefix-list LONGER2001db8 seq 10 permit 2001:db8::/32 ge 32 le 128**

   2001:db8::/32 に含まれる経路だけ permit になる ipv6 prefix-list を設定します。

2. **(config)# route-map LONGER2001db8PERMIT permit 10**

   (config-route-map)# match ipv6 address prefix-list LONGER2001db8

   (config-route-map)# exit

   2001:db8::/32 に含まれる経路だけ permit になる route-map を設定します。

3. **(config)# router bgp 65531**

   (config-router)# address-family ipv6

   (config-router-af)# redistribute connected route-map LONGER2001db8PERMIT

   (config-router-af)# redistribute static route-map LONGER2001db8PERMIT

   直結経路とスタティック経路について，LONGER2001db8PERMIT でフィルタした結果が permit になる経路だけを広告するように，redistribute を設定します。

4. **(config-router-af)# end**

   # clear ipv6 bgp * out

   広告経路フィルタリング設定の変更を動作に反映します。

(2)　ピアごとに広告経路を変更する

外部ピアに広告する経路を，AS100 から受信した AS パス長が一つの BGP4+経路，および自 AS 内のネットワークが宛先（2001:db8::/32 に含まれる）である直結経路とスタティック経路だけに制限します。広告に当たり，ピア 2001:db8:812:1::1 へは AS_PATH の AS 番号を二つ追加します。内部ピアには，BGP4+経路だけを広告します。

[設定のポイント]

ピア個別に経路フィルタリングする必要がある場合，neighbor out を設定してください。

今回の場合，次の四つの route-map を設定します。

- 直結経路およびスタティック経路の redistribute 用

  2001:db8::/32 に含まれている経路だけ permit になる ipv6 prefix-list を設定して，これを参照する route-map を設定します。

- ピア 2001:db8:812:1::1 広告用

  経路プロトコルが直結またはスタティックの場合だけ AS を二つ追加する route-map を設定します。

- 2001:db8:812:1::1 以外の外部ピア用
  AS が一つの AS_PATH 属性だけ permit になる ip as-path access-list を設定して，これを参照する route-map を設定します。
- 内部ピア用
  BGP4+経路だけ permit，それ以外は deny になる route-map を設定します。

[コマンドによる設定]

1. **(config)# ipv6 prefix-list LONGER2001db8 seq 10 permit 2001:db8::/32 ge 32 le 128**
   (config)# route-map LONGER2001db8PERMIT permit 10
   (config-route-map)# match ipv6 address prefix-list LONGER2001db8
   (config-route-map)# exit
   2001:db8::/32 に含まれる経路だけ permit になる route-map を設定します。直結経路およびスタティック経路の redistribute に使用します。
2. **(config)# ip as-path access-list 1 permit "^[0-9]+$"**
   (config)# route-map BGPEXTOUT permit 10
   (config-route-map)# match protocol connected static
   (config-route-map)# exit
   (config)# route-map BGPEXTOUT permit 20
   (config-route-map)# match protocol bgp
   (config-route-map)# match as-path 1
   (config-route-map)# exit
   直結経路，スタティック経路，BGP4+経路の中で AS_PATH 属性の AS 数が一つの経路だけ permit になる route-map を設定します。外部ピアへの広告に使用します。
3. **(config)# route-map BGP812110UT permit 10**
   (config-route-map)# match protocol connected static
   (config-route-map)# set as-path prepend count 2
   (config-route-map)# exit
   (config)# route-map BGP812110UT permit 20
   (config-route-map)# match protocol bgp
   (config-route-map)# match as-path 1
   (config-route-map)# set as-path prepend count 2
   (config-route-map)# exit
   直結経路，スタティック経路，BGP4+経路の中で AS_PATH 属性の AS 数が一つの経路だけ permit になり，AS を二つ追加する route-map を設定します。ピア 2001:db8:812:1::1 への広告に使用します。
4. **(config)# route-map BGPINTOUT permit 10**
   (config-route-map)# match protocol bgp
   (config-route-map)# exit
   BGP4+経路だけ permit になる route-map を設定します。内部ピアへの広告に使用します。
5. **(config)# router bgp 65531**
   (config-router)# address-family ipv6
   (config-router-af)# redistribute connected route-map LONGER2001db8PERMIT
   (config-router-af)# redistribute static route-map LONGER2001db8PERMIT

```
(config-router-af)# exit
```

直結経路とスタティック経路について，route-map LONGER2001db8PERMIT でフィルタした結果が permit になる経路だけを広告するように，redistribute を設定します。

6.
```
(config-router)# neighbor 2001:db8:811:1::1 remote-as 65532
(config-router)# address-family ipv6
(config-router-af)# neighbor 2001:db8:811:1::1 route-map BGPEXTOUT out
(config-router-af)# exit
```

外部ピアへの広告経路のフィルタに BGPEXTOUT を使用します。

7.
```
(config-router)# neighbor 2001:db8:812:1::1 remote-as 65533
(config-router)# address-family ipv6
(config-router-af)# neighbor 2001:db8:812:1::1 route-map BGP81211OUT out
(config-router-af)# exit
```

外部ピア 2001:db8:812:1::1 への広告経路のフィルタに BGP81211OUT を使用します。

8.
```
(config-router)# neighbor 2001:db8:811:ff01::1 remote-as 65531
(config-router)# address-family ipv6
(config-router-af)# neighbor 2001:db8:811:ff01::1 route-map BGPINTOUT out
```

内部ピアへの広告経路のフィルタに BGPINTOUT を使用します。

9.
```
(config-router-af)# end
# clear ipv6 bgp * out
```

広告経路フィルタリング設定の変更を動作に反映します。

23.3.8　エクストラネット

ある VRF から他 VRF の特定ネットワークに通信する場合, 他 VRF の特定経路を経路フィルタでフィルタリングして，自 VRF へ導入します。

(1)　特定 VRF 経路の導入

VRF 間にわたって通信するために，通信に使用する VRF 2 の経路（2001:db8:1:1::/64）を VRF 3 へ，VRF 3 の経路（2001:db8:1:3::/64）を VRF 2 へインポートするように設定します。

[設定のポイント]

VRF 間経路フィルタリングをするには，ipv6 import inter-vrf を設定してください。経路を VRF ID でフィルタリングするには，route-map を使用してください。route-map 中の宛先ネットワーク条件の指定には，ipv6 prefix-list を使用してください。

まず，VRF 2 の経路だけ permit になる route-map を設定します。この route-map を VRF 3 の ipv6 import inter-vrf から参照させます。次に，VRF 3 の経路だけ permit になる route-map を設定します。この route-map を VRF 2 の ipv6 import inter-vrf から参照させます。

[コマンドによる設定]

1.
```
(config)# ipv6 prefix-list PERMITVRF2 seq 10 permit 2001:db8:1:1::/64
(config)# route-map VRF2PERMIT permit 10
(config-route-map)# match vrf 2
(config-route-map)# match ipv6 address prefix-list PERMITVRF2
(config-route-map)# exit
```

VRF 2 の経路が permit になるように設定します。

2. **(config)# vrf definition 3**
   (config-vrf)# ipv6 import inter-vrf VRF2PERMIT
   (config-vrf)# exit
   1.のフィルタ設定を VRF 3 のエクストラネットに適用して, VRF 2 の経路を VRF 3 に導入するように設定します。
3. **(config)# ipv6 prefix-list PERMITVRF3 seq 10 permit 2001:db8:1:3::/64**
   (config)# route-map VRF3PERMIT permit 10
   (config-route-map)# match vrf 3
   (config-route-map)# match ipv6 address prefix-list PERMITVRF3
   (config-route-map)# exit
   VRF 3 の経路が permit になるように設定します。
4. **(config)# vrf definition 2**
   (config-vrf)# ipv6 import inter-vrf VRF3PERMIT
   (config-vrf)# exit
   3.のフィルタ設定を VRF 2 のエクストラネットに適用して, VRF 3 の経路を VRF 2 に導入するように設定します。

[注意事項]

ipv6 import inter-vrf から参照される route-map が設定されていない場合, 他 VRF またはグローバルネットワークにあるすべての経路をインポートします。意図しない経路をインポートしないように，必ず route-map，ipv6 import inter-vrf の順に設定してください。

(2) プロトコルによる VRF 間経路の広告

VRF 3 の経路（2001:db8:1:3::/64）を VRF 2 のネットワークへ導入します。導入した VRF 3 の経路を VRF 2 の OSPFv3 で広告します。

[設定のポイント]

VRF 間経路フィルタリングをするには，ipv6 import inter-vrf を設定してください。経路を VRF でフィルタリングするには，route-map を使用してください。route-map 中の宛先ネットワーク条件の指定には，ipv6 prefix-list を使用してください。OSPFv3 で他 VRF またはグローバルネットワークからインポートした経路を広告するには，redistribute を設定してください。

まず，VRF 3 の経路だけ permit になる route-map を設定します。次に，この route-map を VRF 2 の ipv6 import inter-vrf から参照させて, VRF 3 の経路を VRF 2 へ導入するように設定します。最後に，他 VRF またはグローバルネットワークからインポートした経路を広告するように，VRF 2 の OSPFv3 に redistribute を設定します。

[コマンドによる設定]

1. **(config)# ipv6 prefix-list PERMITVRF3 seq 10 permit 2001:db8:1:3::/64**
   (config)# route-map VRF3TO2 permit 10
   (config-route-map)# match vrf 3
   (config-route-map)# match ipv6 address prefix-list PERMITVRF3
   (config-route-map)# exit
   VRF 3 の経路が permit になるように設定します。
2. **(config)# vrf definition 2**

```
(config-vrf)# ipv6 import inter-vrf VRF3TO2
(config-vrf)# exit
```

1.のフィルタ設定を VRF 2 のエクストラネットに適用して，VRF 3 の経路を VRF 2 に導入します。

3.
```
(config)# ipv6 router ospf 1 vrf 2
(config-rtr)# redistribute extra-vrf
```

他 VRF またはグローバルネットワークからインポートした経路を，VRF 2 の OSPFv3 ドメイン 1 で広告します。

[注意事項]

ipv6 import inter-vrf から参照される route-map が設定されていない場合, 他 VRF またはグローバルネットワークにあるすべての経路をインポートします。意図しない経路をインポートしないように，必ず route-map，ipv6 import inter-vrf の順に設定してください。

(3)　特定 VRF のディスタンス値の変更

VRF 2 および VRF 3 の経路をグローバルネットワークへ導入します。VRF 2 の経路だけディスタンス値を 150 にします。

[設定のポイント]

VRF 間経路フィルタリングをするには，ipv6 import inter-vrf を設定してください。経路を VRF でフィルタリングするには，route-map を使用してください。

まず，VRF 2 の経路が permit になり，ディスタンス値を 150 に変更する route-map を設定します。次に，同じ route-map の別シーケンス番号に VRF 3 の経路が permit になるよう設定します。

この route-map を ipv6 import inter-vrf から参照させて，特定 VRF のディスタンス値を変更するフィルタリングを設定します。

[コマンドによる設定]

1.
```
(config)# route-map VRF2AND3PERMIT permit 10
(config-route-map)# match vrf 2
(config-route-map)# set distance 150
(config-route-map)# exit
```

VRF 2 の経路が permit になり，ディスタンス値を 150 に変更するように設定します。

2.
```
(config)# route-map VRF2AND3PERMIT permit 20
(config-route-map)# match vrf 3
(config-route-map)# exit
```

VRF 3 の経路が permit になるように設定します。

3.
```
(config)# vrf definition global
(config-vrf)# ipv6 import inter-vrf VRF2AND3PERMIT
```

1.，2.のフィルタ設定をグローバルネットワークのエクストラネットに適用し，VRF 2 および VRF 3 の経路をグローバルネットワークに導入して，VRF 2 の経路のディスタンス値を 150 に変更するように設定します。

[注意事項]

ipv6 import inter-vrf から参照される route-map が設定されていない場合, 他 VRF またはグローバルネットワークにあるすべての経路をインポートします。意図しない経路をインポートしないように，必ず route-map，ipv6 import inter-vrf の順に設定してください。

23.4　オペレーション

23.4.1　運用コマンド一覧

IPv4 ユニキャストルーティングを対象とする経路フィルタリングの運用コマンド一覧を次の表に示します。

表 23-27　運用コマンド一覧（IPv4）

コマンド名	説明
show ip route	IPv4 ユニキャスト経路を一覧表示します。
show ip rip	RIP プロトコルに関する情報を表示します。
show ip ospf	OSPF プロトコルに関する情報を表示します。
show ip bgp	BGP プロトコルに関する情報を表示します。
clear ip bgp	BGP4 セッションもしくは BGP4 プロトコルに関する情報のクリア，または新しい BGP フィルタ情報を使用して受信経路と送信経路のフィルタリングをします。

IPv6 ユニキャストルーティングを対象とする経路フィルタリングの運用コマンド一覧を次の表に示します。

表 23-28　運用コマンド一覧（IPv6）

コマンド名	説明
show ipv6 route	IPv6 ユニキャスト経路を一覧表示します。
show ipv6 rip	RIPng プロトコルに関する情報を表示します。
show ipv6 ospf	OSPFv3 プロトコルに関する情報を表示します。
show ipv6 bgp	BGP4+プロトコルに関する情報を表示します。
clear ipv6 bgp	BGP4+セッションもしくは BGP4+プロトコルに関する情報のクリア，または新しい BGP フィルタ情報を使用して受信経路と送信経路のフィルタリングをします。

23.4.2　学習経路フィルタリング前の確認

(1)　RIP および RIPng が受信した経路の確認

RIP が受信した経路は show ip rip コマンドで，RIPng が受信した経路は show ipv6 rip コマンドで，received-routes パラメータを指定して確認します。

図 23-3　RIP 受信経路表示例

```
> show ip rip received-routes
Date 20XX/03/14 12:00:00 UTC
Status Codes: * valid, > active, r RIB failure

Neighbor Address: 192.168.1.145
   Destination        Next Hop        Interface       Metric   Tag   Timer
*> 172.10.1/24        192.168.1.145   Eth1/7          1        0     23s
```

注意

学習経路フィルタリングで学習しないことになった経路や，RIP 内部または RIPng 内部で優先しないことになった経路は，これらのコマンドでは表示されません。

(2)　OSPF および OSPFv3 の SPF 計算結果の経路確認

OSPF で SPF 計算した AS 外経路と NSSA 経路，OSPFv3 で SPF 計算した AS 外経路は，フィルタで無効になってもルーティングテーブルに無効経路として導入されています。OSPF の AS 外経路と NSSA 経路を show ip route コマンドで，OSPFv3 の AS 外経路を show ipv6 route コマンドで，無効経路を含めて確認できます。コマンド実行時は all-routes パラメータを指定して，さらに-T ospf_external を指定してください。

図 23-4　OSPF AS 外経路・NSSA 経路表示例

```
> show ip route all-routes -T ospf_external
Date 20XX/03/14 12:00:00 UTC
Status Codes: * valid, > active, r RIB failure
Total: 2 routes
   Destination    Next Hop        Interface   Metric   Protocol   Age
*> 172.10.1/24    192.168.1.145   Eth1/7      1/1      OSPF ext2  52s, Tag: 10
*  172.20.1/24    192.168.1.145   Eth1/7      1/1      OSPF ext2  52s, Tag:  0
```

(3)　BGP4 および BGP4+が受信した経路の確認

BGP4 が受信した経路は show ip bgp コマンドで，BGP4+が受信した経路は show ipv6 bgp コマンドで，received-routes パラメータを指定して確認します。

図 23-5　BGP4 受信経路表示例

```
> show ip bgp received-routes
Date 20XX/03/14 12:00:00 UTC
BGP Peer: 177.7.7.145    , Remote AS: 1000
Local AS: 200, Local Router ID: 200.201.202.203
Status Codes: d dampened, * valid, > active, S Stale, r RIB failure
Origin Codes: i - IGP, e - EGP, ? - incomplete
   Network             Next Hop        MED    LocalPref Path
*> 172.10.1/24         192.168.1.145   -      -         1000 i
*  172.20.1/24         192.168.1.145   -      -         1000 i
```

注意

学習経路フィルタリングで学習しないことになった経路や，BGP4 内部または BGP4+内部で優先しないことになった経路は，これらのコマンドでは表示されません。

詳細な経路属性を含めて BGP4 または BGP4+が受信した経路を確認するには，show ip bgp コマンドまたは show ipv6 bgp コマンドで received-routes パラメータを指定して，さらに-F を指定してください。ORIGIN 属性，AS_PATH 属性，MED 属性，LOCAL_PREF 属性，COMMUNITIES 属性を確認できます。

図 23-6　BGP4 受信経路詳細表示例

```
> show ip bgp received-routes -F
Date 20XX/03/14 12:00:00 UTC
BGP Peer: 192.168.1.145    , Remote AS: 1000
Local AS: 200, Local Router ID: 192.168.1.1
Status Codes: d dampened, * valid, > active, S Stale, r RIB failure
Route 172.10.1/24
*> Next Hop 192.168.1.145
     MED: -, LocalPref: -, Type: External route
     Origin: IGP
     Path: 1000
     Next Hop Attribute: 192.168.1.145
     Communities: 120:200
Route 172.20.1/24
*  Next Hop 192.168.1.145
```

```
    MED: -, LocalPref: -, Type: External route
    Origin: IGP
    Path: 1000
    Next Hop Attribute: 192.168.1.145
    Communities: 120:200
```

注意

学習経路フィルタリングで学習しないことになった経路や，BGP4 内部または BGP4+内部で優先しないことになった経路は，これらのコマンドでは表示されません。

23.4.3　学習経路フィルタリング後の確認

(1)　ルーティングテーブルの確認

学習経路フィルタリングした経路は，ルーティングテーブルに導入されています。ルーティングテーブルの経路を表示すると，学習経路フィルタリングした結果がわかります。

ルーティングテーブルの経路を無効経路を含めてすべて表示するには，show ip route コマンドまたは show ipv6 route コマンドで all-routes パラメータを指定してください。

図 23-7　ルーティングテーブルの経路表示例（無効経路を含む）

```
> show ip route all-routes
Date 20XX/03/14 12:00:00 UTC
Status Codes: * valid, > active, r RIB failure
Total: 12 routes
   Destination    Next Hop        Interface     Metric  Protocol   Age
*> 127/8          ----            localhost     0/0     Connected   1h 32s
*> 172.16.1/24    192.168.1.145   Eth1/7        2/0     RIP         12s
*> 192.168.1/24   192.168.1.1     Eth1/7        0/0     Connected   2s
   192.168.1/24   192.168.1.1     Eth1/7        1/-     OSPF intra 48m  3s
*> 192.168.1.1/32 192.168.1.1     Eth1/7        0/0     Connected   1h 31s  <-1
*> 192.168.100/24 192.168.1.145   Eth1/7        -/-     BGP         11m 26s
*> 192.168.110/24 192.168.1.145   Eth1/7        1/1     OSPF ext2  52s
*> 192.168.200/24 192.168.1.145   Eth1/7        0/0     Static      46m 58s
*  192.168.200/24 192.168.1.145   Eth1/7        -/-     BGP         50m 14s
*  192.168.200/24 192.168.1.145   Eth1/7        1/1     OSPF ext2  48m 52s
*  192.168.200/24 192.168.1.145   Eth1/7        2/0     RIP         12s
```

1. 経路行の先頭の「*」および「>」は次の意味を示します。

   *：その経路は有効経路です。*がなければ無効経路です。

   >：その経路は優先経路です。パケット転送には優先経路だけを使用します。

ルーティングテーブルの経路を特定の学習元プロトコルについてだけ確認するには，show ip route コマンドまたは show ipv6 route コマンドで all-routes パラメータを指定して，さらにプロトコルを指定してください。

図 23-8　ルーティングテーブルの経路表示例（RIP だけ，無効経路を含む）

```
> show ip route all-routes rip
Date 20XX/03/14 12:00:00 UTC
Status Codes: * valid, > active, r RIB failure
Total: 2 routes
   Destination        Next Hop        Interface      Metric   Protocol  Age
*> 172.16.1/24        192.168.1.145   Eth1/7         2/0      RIP       12s
*  192.168.200/24     192.168.1.145   Eth1/7         2/0      RIP       12s
```

(2)　ディスタンス値の確認

一つの宛先ネットワークに対していろいろなルーティングプロトコルが経路を学習および導入している場合，優先経路のプロトコルや優先順位を確認する必要があります。優先順位はディスタンス値で決まります。

経路のディスタンス値を表示するには，show ip route コマンドまたは show ipv6 route コマンドで all-routes パラメータを指定して，さらに-P を指定してください。行末にある Distance 項目の一つ目の値がディスタンス値です。

図 23-9　ディスタンス値表示例

```
> show ip route all-routes -P
Date 20XX/03/14 12:00:00 UTC
Status Codes: * valid, > active, r RIB failure
Total: 12 routes
   Destination      Next Hop        Interface   Metric  Protocol   Age
*> 127/8            ----            localhost   0/0     Connected   1h 36m,
 Distance: 0/0/0
*> 172.16.1/24      192.168.1.145   Eth1/7      2/0     RIP        12s,
 Distance: 120/0/0
*> 192.168.1/24     192.168.1.1     Eth1/7      0/0     Connected   0s,
 Distance: 0/0/0
   192.168.1/24     192.168.1.1     Eth1/7      1/-     OSPF intra 52m 32s,
 Distance: -110/1/0
*> 192.168.1.1/32   192.168.1.1     Eth1/7      0/0     Connected   1h 35m,
 Distance: 0/0/0
*> 192.168.100/24   192.168.1.145   Eth1/7      -/-     BGP        12m 37s,
 Distance: 20/0/0
*> 192.168.110/24   192.168.1.145   Eth1/7      1/1     OSPF ext2   6m 11s,
 Distance: 110/1/0
*> 192.168.200/24   192.168.1.145   Eth1/7      0/0     Static     50m 27s,
 Distance: 2/0/0
*  192.168.200/24   192.168.1.145   Eth1/7      -/-     BGP        54m 43s,
 Distance: 20/0/0
*  192.168.200/24   192.168.1.145   Eth1/7      1/1     OSPF ext2  52m 21s,
 Distance: 110/1/0
*  192.168.200/24   192.168.1.145   Eth1/7      2/0     RIP        12s,
 Distance: 120/0/0
```

特定の宛先ネットワークの経路だけディスタンス値を表示するには，show ip route コマンドまたは show ipv6 route コマンドで all-routes パラメータを指定して，さらに宛先ネットワークを指定してください。詳細情報中の Distance 表示行にある一つ目の値がディスタンス値です。

図 23-10　ディスタンス値表示例（特定宛先だけ，無効経路を含む）

```
> show ip route all-routes 192.168.200/24
Date 20XX/03/14 12:00:00 UTC
Route codes: *  = active,   + = changed to active recently
             ' ' = inactive, - = changed to inactive recently
             r  = RIB failure

Route 192.168.200/24
Entries 4 Announced 1 Depth 0 <>

* NextHop 192.168.1.145  , Interface   : Eth1/7
     Protocol <Static>
     Source Gateway ----
     Metric/2    : 0/0
     Distance/2/3: 2/0/0
     Tag : 0, Age : 58m 29s
     AS Path : IGP (Id 1)
     Communities: -
     LocalPref : -
     RT State: <Remote Int Active Gateway>

  NextHop 192.168.1.145  , Interface   : Eth1/7
     Protocol <BGP>
     Source Gateway 192.168.1.145
     Metric/2    : -/-
     Distance/2/3: 20/0/0
     Tag : 0, Age :  1h  2m
     AS Path : 1000 IGP (Id 2)
     Communities: -
     LocalPref : 100
     RT State: <Ext Gateway>
```

(3)　経路属性の確認

ルーティングテーブルの経路の詳細な経路属性を確認するには，show ip route コマンドまたは show ipv6 route コマンドで all-routes パラメータを指定して，さらに-F を指定してください。

図 23-11　経路属性の表示例（詳細表示，無効経路を含む）

```
> show ip route all-routes -F
Date 20XX/03/14 12:00:00 UTC
Status Codes: * valid, > active, r RIB failure
Total: 12 routes
   Destination        Next Hop        Interface     Metric   Protocol  Age
*> 127/8              ----            localhost     0/0      Connected  1h 46m,
 Distance: 0/0/0, Tag: 0, AS-Path: IGP (Id 1), Communities: -, LocalPref: -, <NoAdvise Active R
etain Reject>
*> 172.10.1/24        192.168.1.145   Eth1/7        2/0      RIP       19s,
 Distance: 120/0/0, Tag: 0, AS-Path: IGP (Id 1), Communities: -, LocalPref: -,<Int Active Gatew
ay>
*> 192.168.1/24       192.168.1.1     Eth1/7        0/0      Connected  7s,
 Distance: 0/0/0, Tag: 0, AS-Path: IGP (Id 1), Communities: -, LocalPref: -, <Active Retain>
   192.168.1/24       192.168.1.1     Eth1/7        1/-      OSPF intra 1h  2m,
 Distance: -110/1/0, Tag: 0, AS-Path: IGP (Id 1), Communities: -, LocalPref: -, <NotInstall NoA
dvise Int Hidden Gateway>
*> 192.168.1.1/32     192.168.1.1     Eth1/7        0/0      Connected  1h 45m,
 Distance: 0/0/0, Tag: 0, AS-Path: IGP (Id 1), Communities: -, LocalPref: -, <NoAdvise Active R
etain>
*> 192.168.100/24     192.168.1.145   Eth1/7        -/-      BGP       12m 57s,
 Distance: 20/0/0, Tag: 0, AS-Path: 1000 IGP (Id 3), Communities: 120:200, LocalPref: 100, <Ext
 Active Gateway>
*  192.168.110/24     192.168.1.145   Eth1/7        1/1      OSPF ext2  3m 34s,
 Distance: 110/1/0, Tag: 10, AS-Path: IGP (Id 1), Communities: -, LocalPref: -, <Int Ext Active
 Gateway>
*> 192.168.200/24     192.168.1.145   Eth1/7        0/0      Static     1h  0m,
 Distance: 2/0/0, Tag: 0, AS-Path: IGP (Id 1), Communities: -, LocalPref: -, <Remote Int Active
 Gateway>
*  192.168.200/24     192.168.1.145   Eth1/7        -/-      BGP        1h  5m,
 Distance: 20/0/0, Tag: 0, AS-Path: 1000 IGP (Id 2), Communities: -, LocalPref: 100,
 <Ext Gateway>
*  192.168.200/24     192.168.1.145   Eth1/7        1/1      OSPF ext2  1h  2m,
 Distance: 110/1/0, Tag: 0, AS-Path: IGP (Id 1), Communities: -, LocalPref: -,<Int Ext Gateway>
*  192.168.200/24     192.168.1.145   Eth1/7        2/0      RIP       19s,
 Distance: 120/0/0, Tag: 0, AS-Path: IGP (Id 1), Communities: -, LocalPref: -,<Int Gateway>
```

23.4.4　広告経路フィルタリング前の確認

広告対象となる経路は，基本的にはルーティングテーブルにある優先経路です。広告経路フィルタリングの対象となる経路を確認するには，ルーティングテーブルの経路を表示してください。

IPv4 のルーティングテーブルの優先経路は show ip route コマンドで，IPv6 のルーティングテーブルの優先経路は show ipv6 route コマンドで表示します。

図 23-12　ルーティングテーブルの経路表示例

```
> show ip route
Date 20XX/03/14 12:00:00 UTC
Total: 8 routes
Destination        Next Hop        Interface      Metric   Protocol  Age
172.16.1/24        192.168.1.145   Eth1/7         2/0      RIP       12s
192.168.1/24       192.168.1.1     Eth1/7         0/0      Connected  2s
192.168.1.1/32     192.168.1.1     Eth1/7         0/0      Connected  1h 31s
192.168.100/24     192.168.1.145   Eth1/7         -/-      BGP       11m 26s
192.168.110/24     192.168.1.145   Eth1/7         1/1      OSPF ext2 52s
192.168.200/24     192.168.1.145   Eth1/7         0/0      Static    46m 58s
```

ルーティングテーブルの優先経路を特定の学習元プロトコルだけ表示するには，show ip route コマンドまたは show ipv6 route コマンドでパラメータとしてプロトコルを指定してください。

図 23-13　ルーティングテーブルの経路表示例（RIP だけ）

```
> show ip route rip
Date 20XX/03/14 12:00:00 UTC
Total: 5 routes
Destination        Next Hop        Interface      Metric   Protocol  Age
172.16.1/24        192.168.1.145   Eth1/7         2/0      RIP       12s
```

ルーティングテーブルの優先経路の詳細な経路属性を確認するには，show ip route コマンドまたは show ipv6 route コマンドで-F パラメータを指定してください。

図 23-14　ルーティングテーブルの経路表示例（詳細表示）

```
> show ip route -F
Date 20XX/03/14 12:00:00 UTC
Total: 8 routes
Destination        Next Hop        Interface      Metric   Protocol  Age
172.16.1/24        192.168.1.145   Eth1/7         2/0      RIP       19s,
 Distance: 120/0/0, Tag: 0, AS-Path: IGP (Id 1), Communities: -, LocalPref: -,<Int Active Gatew
ay>
192.168.1/24       192.168.1.1     Eth1/7         0/0      Connected  7s,
 Distance: 0/0/0, Tag: 0, AS-Path: IGP (Id 1), Communities: -, LocalPref: -, <Active Retain>
192.168.1.1/32     192.168.1.1     Eth1/7         0/0      Connected  1h 45m,
 Distance: 0/0/0, Tag: 0, AS-Path: IGP (Id 1), Communities: -, LocalPref: -, <NoAdvise Active R
etain>
192.168.100/24     192.168.1.145   Eth1/7         -/-      BGP       12m 57s,
 Distance: 20/0/0, Tag: 0, AS-Path: 1000 IGP (Id 3), Communities: 120:200, LocalPref: 100, <Ext
 Active Gateway>
192.168.110/24     192.168.1.145   Eth1/7         1/1      OSPF ext2  3m 34s,
 Distance: 110/1/0, Tag: 10, AS-Path: IGP (Id 1), Communities: -, LocalPref: -, <Int Ext Active
 Gateway>
192.168.200/24     192.168.1.145   Eth1/7         0/0      Static     1h  0m,
 Distance: 2/0/0, Tag: 0, AS-Path: IGP (Id 1), Communities: -, LocalPref: -, <Remote Int Active
 Gateway>
```

BGP4 および BGP4+では，ルーティングテーブル上にある BGP4 または BGP4+の優先ではない経路も広告対象になることがあります。優先ではない経路も含めて，ルーティングテーブル上にある BGP4 経路または BGP4+経路を表示するには，show ip route コマンドまたは show ipv6 route コマンドで all-routes パラメータを指定して，さらにパラメータとして bgp を指定してください。

図 23-15　ルーティングテーブルの経路表示例（BGP だけ，無効経路を含む）

```
> show ip route all-routes bgp
Date 20XX/03/14 12:00:00 UTC
Status Codes: * valid, > active, r RIB failure
Total: 12 routes
   Destination     Next Hop        Interface   Metric   Protocol  Age
*> 192.168.100/24  192.168.1.145   Eth1/7      -/-      BGP       11m 26s┐
*  192.168.200/24  192.168.1.145   Eth1/7      -/-      BGP       50m 14s┘ <-1
```

1. 経路行の先頭の「*」および「>」は次の意味を示します。

   *：その経路は有効経路です。*がなければ無効経路です。

   >：その経路は優先経路です。パケット転送には優先経路だけを使用します。

23.4.5　広告経路フィルタリング後の確認

(1)　RIP および RIPng 広告経路の確認

RIP の広告経路を確認するには show ip rip コマンドで，RIPng の広告経路を確認するには show ipv6 rip コマンドで，advertised-routes パラメータを指定してください。RIP の広告先アドレスまたは RIPng の広告先インタフェース名と，そこへ広告している経路および経路属性を表示します。なお，RIP で広告先がインタフェースの場合はブロードキャストアドレスを表示します。

図 23-16 RIP 広告経路表示例

```
> show ip rip advertised-routes
Date 20XX/03/20 16:47:36 UTC

Target Address: 177.7.7.255
Destination        Next Hop        Interface      Metric   Tag   Age
192.168.1/24       192.168.1.1     Eth1/6         1        0      5s
```

(2) OSPF 広告経路の確認

OSPF では，広告経路フィルタリングによって広告した経路は AS-External-LSA と NSSA-External-LSA に含まれています。

AS-External-LSA の中で自装置が生成したものを確認するには，show ip ospf コマンドで database パラメータを指定して，さらに external と self-originate を指定してください。

図 23-17 AS-External-LSA 表示例（自装置生成分だけ）

```
> show ip ospf database external self-originate
Date 20XX/03/14 12:00:00 UTC
Domain: 1
Local Router ID : 192.168.198.197
Area : 0
Address         State Priority Cost  Neighbor   DR           Backup DR
192.168.7.1     BackupDR 1     1     1          192.168.1.1  192.168.198.197

LS Database: AS External Link
Network Address: 192.168.1/24, AS Boundary Router: 192.168.198.197      <-1
    LSID: 192.168.1.0
    Age:  221, Length: 36 , Sequence: 80000001, Checksums: BB9C
     -> Type: 2, Metric: 20, Tag: 00000000, Forward: 0.0.0.0
```

1.Network Address（192.168.1/24）は経路宛先ネットワークを示します。

NSSA-External-LSA の中で自装置が生成したものを確認するには，show ip ospf コマンドで database パラメータを指定して，さらに nssa と self-originate を指定してください。

図 23-18 NSSA-External-LSA 表示例

```
> show ip ospf database nssa self-originate
Date 20XX/03/14 12:00:00 UTC
Domain: 1
Local Router ID : 192.168.198.197
Area : 0
Address         State Priority Cost  Neighbor   DR           Backup DR
192.168.7.1     BackupDR 1     1     1          192.168.1.1  192.168.198.197

LS Database: NSSA AS External Link
Network Address: 192.168.1/24, AS Boundary Router: 192.168.198.197      <-1
    LSID: 192.168.1.0
    Age:   39, Length: 36 , Sequence: 80000001, Checksums: 9FB6
     -> Type: 2, Metric: 20, Tag: 00000000, Forward: 0.0.0.0
```

1.Network Address（192.168.1/24）は経路宛先ネットワークを示します。

(3) OSPFv3 広告経路の確認

OSPFv3 では，広告経路フィルタリングによって広告した経路は AS-External-LSA に含まれています。

AS-External-LSA の中で自装置が生成したものを確認するには，show ipv6 ospf コマンドで database パラメータを指定して，さらに external と self-originate を指定してください。

図 23-19 AS-External-LSA 表示例（自装置生成分だけ）

```
> show ipv6 ospf database external self-originate
Date 20XX/03/14 12:00:00 UTC
```

```
Domain: 1
Local Router ID: 177.7.7.4
LS Database: AS-external-LSA
Advertising Router: 177.7.7.4
    LSID: 0000000a, Age: 298, Length: 36
    Sequence: 80000001, Checksum: 6c76
    Prefix: 2001:db8:7:7::/64                                    <-1
       Prefix Options: <>
       Type: 2, Metric: 20, Tag: 100
```

1. Prefix（2001:db8:7:7::/64）は経路宛先ネットワークを示します。

(4)　BGP4 および BGP4+広告経路の確認

BGP4 の広告経路を確認するには show ip bgp コマンドで，BGP4+の広告経路を確認するには show ipv6 bgp コマンドで，advertised-routes パラメータを指定してください。

図 23-20　BGP4 広告経路表示例

```
> show ip bgp advertised-routes
Date 20XX/03/14 12:00:00 UTC
BGP Peer: 172.16.7.145   , Remote AS: 2000
Local AS: 1000, Local Router ID: 192.168.1.1
Origin Codes: i - IGP, e - EGP, ? - incomplete
Network              Next Hop        MED    LocalPref Path
192.168.100/24       192.168.1.145   0      -         1000 2100 i
192.168.200/24       192.168.1.145   0      -         1000 2100 i
```

BGP4 または BGP4+の広告経路の詳細な経路属性を確認するには，show ip bgp コマンドまたは show ipv6 bgp コマンドで advertised-routes パラメータを指定して，さらに-F を指定してください。ORIGIN 属性，AS_PATH 属性，MED 属性，LOCAL_PREF 属性，COMMUNITIES 属性を確認できます。

図 23-21　BGP4 広告経路表示例（詳細表示）

```
> show ip bgp advertised-routes -F
Date 20XX/03/14 12:00:00 UTC
BGP Peer: 172.16.7.145   , Remote AS: 2000
Local AS: 1000, Local Router ID: 192.168.1.1
Status Codes: d dampened, * valid, > active, S Stale, r RIB failure
Route 192.168.100/24
*> Next Hop 192.168.1.145
     MED:0, LocalPref: -, Type: External route
     Origin: IGP
     Path: 1000 2100
     Next Hop Attribute: 192.168.1.145
     Communities: 1020:1200
Route 192.168.200/24
*> Next Hop 192.168.1.145
     MED: 0, LocalPref: -, Type: External route
     Origin: IGP
     Path: 1000 2100
     Next Hop Attribute: 192.168.1.145
     Communities: 1020:1200
```

23.4.6　エクストラネットの確認

show ip route コマンドまたは show ipv6 route コマンドでプロトコルに extra-vrf を指定して，インポートした経路だけを表示します。

図 23-22　show ip route コマンドの表示例

```
> show ip route vrf 2 extra-vrf
Date 20XX/12/20 12:00:00 UTC
VRF: 2 Total: 1 routes
Destination        Next Hop        Interface      Metric  Protocol   Age
172.16.3.0/24      10.3.1.1        Eth3/1         0/0     Extra-Vrf  365d
>
> show ip route vrf 3 extra-vrf
```

```
Date 20XX/12/20 12:00:00 UTC
VRF: 3 Total: 1 routes
Destination        Next Hop        Interface      Metric  Protocol   Age
172.16.1.0/24      10.1.1.1        Eth1/1         0/0     Extra-Vrf  365d
```

24 IPv4 マルチキャストの解説

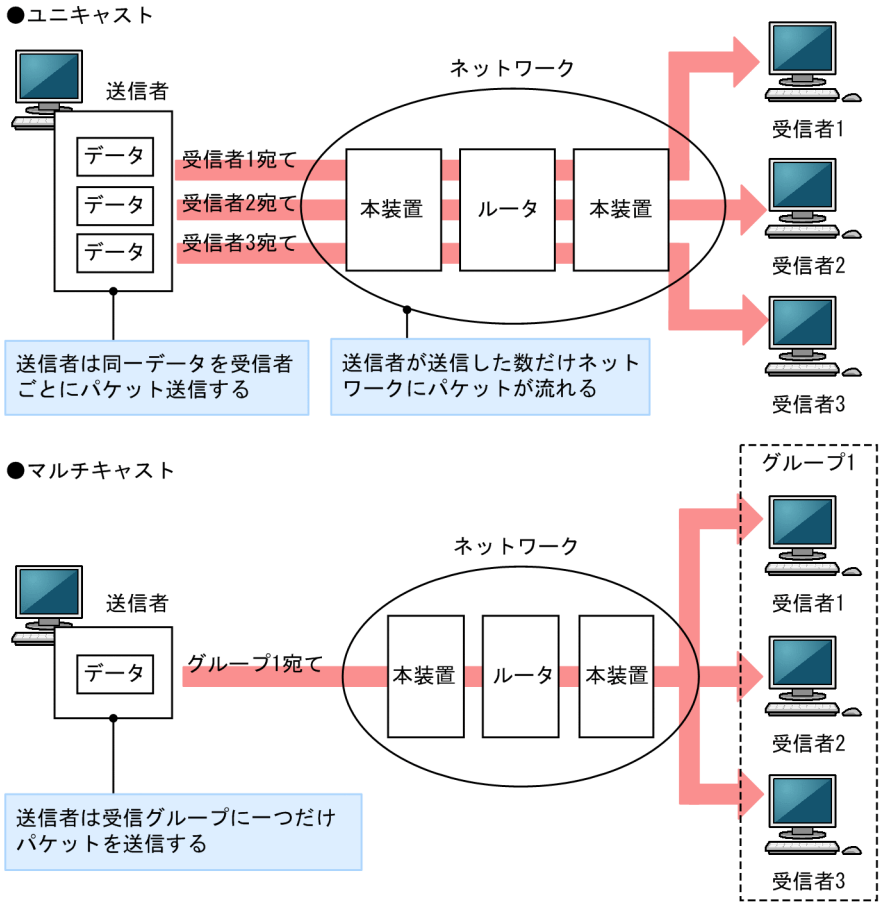
マルチキャストは, ネットワーク内で選択されたグループに対して同一の情報を送信します。この章では IPv4 ネットワークで実現するマルチキャストについて説明します。

24.1　IPv4 マルチキャスト概説

同一の情報を複数のユニキャストで送信すると，送信者とネットワークの負荷が大きくなります。マルチキャストでは，ネットワーク内で選択されたグループに対して同一の情報を送信します。マルチキャストは送信者が受信者ごとにデータを複製する必要がないため，受信者の数に関係なくネットワークの負荷が軽減します。

マルチキャストの概要を次の図に示します。

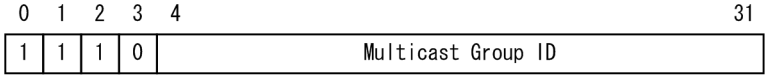
図 24-1　マルチキャストの概要



24.1.1　IPv4 マルチキャストアドレス

IPv4 マルチキャスト通信では IPv4 アドレスの ClassD を使用します。IPv4 マルチキャストアドレスはマルチキャストパケットの送受信に参加しているマルチキャストグループの間だけの，論理的なグループアドレスです。アドレスの範囲は 224.0.0.0 から 239.255.255.255 です。ただし，224.0.0.0 から 224.0.0.255 は予約されたアドレスです。IPv4 マルチキャストアドレスのフォーマットを次の図に示します。

図 24-2　マルチキャストアドレスのフォーマット



24.1.2　IPv4 マルチキャストルーティング機能

本装置は受信したマルチキャストパケットをマルチキャスト中継エントリに従って中継します。マルチキャストルーティング機能は大きく分けて次の三つの機能から構成されます。

- マルチキャストグループマネージメント機能

  グループメンバシップ情報を送受信してマルチキャストグループの存在を学習する機能です。本装置では IGMP（Internet Group Management Protocol）を使用します。

- 経路制御機能

  経路情報を送受信して中継経路を決定して，マルチキャスト経路情報およびマルチキャスト中継エントリを作成する機能です。経路情報の収集には PIM-SM または PIM-SSM を使用します。

- 中継機能

  マルチキャストパケットをマルチキャスト中継エントリに従ってハードウェアおよびソフトウェアで中継する機能です。

24.1.3　IPv4 マルチキャストパケットの受信

マルチキャストルーティング機能を実現するために，本装置では次の表に示す受信要因に該当するマルチキャストパケットをソフトウェアに転送します。

表 24–1　マルチキャストパケットの受信要因

受信要因	内容
wrong-incoming-interface	ハードウェアに登録済みのマルチキャスト中継エントリと一致したマルチキャストパケットを受信インタフェースとは異なるインタフェースから受信した場合に発生する要因
cache-misshit	ハードウェアのマルチキャスト中継エントリに存在しないマルチキャストパケットを受信した場合に発生する要因
register-request	ファーストホップルータが PIM Register メッセージをランデブーポイントへ送信するためのマルチキャストパケットを受信した場合に発生する要因
register-receive	ランデブーポイントで PIM Register メッセージを受信した場合に発生する要因

本装置では，これらのマルチキャストパケットを大量に受信した場合の輻輳を抑止するために，受信要因ごとにパケット数を制限します。なお，この制限はマルチキャストパケットの中継には影響ありません。

24.2　IPv4 マルチキャストグループマネージメント機能

マルチキャストグループマネージメント機能とは，ルーター受信者間でのグループメンバシップ情報の送受信によって，ルータが直接接続したネットワーク上のマルチキャストグループメンバの存在を学習する機能です。本装置ではマルチキャストグループマネージメント機能実現のための管理プロトコルとして IGMP をサポートしています。

24.2.1　IGMP の概要

IGMP はルーター受信者間で使用されるマルチキャストグループ管理プロトコルです。IGMP を使用すると，ルータからのマルチキャストグループの参加問い合わせと受信者からのマルチキャストグループへの参加および離脱要求によって，ルータが受信者のマルチキャストグループへの参加または離脱を認識してマルチキャストパケットを中継したり遮断したりします。

IGMP には IGMPv1，IGMPv2，および IGMPv3 があります。

24.2.2　IGMP メッセージサポート仕様

(1)　IGMPv2 メッセージのサポート仕様

本装置がサポートする IGMPv2 メッセージのサポート仕様を次の表に示します。

表 24-2　IGMPv2 メッセージサポート仕様

タイプ		意味	サポート	
			送信	受信
Membership Query	General Query	マルチキャストグループの参加問い合わせ（全マルチキャストグループ宛て）	○	○
	Group-Specific Query	マルチキャストグループの参加問い合わせ（特定マルチキャストグループ宛て）	○	○
Version1 Membership Report		マルチキャストグループへの参加要求（IGMPv1 対応）	×	○
Version2 Membership Report		マルチキャストグループへの参加要求（IGMPv2 対応）	×	○
Leave Group		マルチキャストグループからの離脱要求	×	○

（凡例）　○：サポートする　×：サポートしない

(2)　IGMPv3 メッセージのサポート仕様

IGMPv3 はフィルタモードと送信元リストを指定することで，送信元フィルタリングを実現します。フィルタモードには次の二つのモードがあります。

INCLUDE モード

　指定された送信元リストからのマルチキャストパケットだけを中継します。

EXCLUDE モード

　指定された送信元リスト以外からのマルチキャストパケットだけを中継します。

本装置がサポートする IGMPv3 メッセージのサポート仕様を次の表に示します。

表 24-3　IGMPv3 メッセージサポート仕様

タイプ		意味	サポート	
			送信	受信
Version 3 Multicast Membership Query	General Query	マルチキャストグループの参加問い合わせ（全マルチキャストグループ宛て）	○	○
	Group-Specific Query	マルチキャストグループの参加問い合わせ（特定マルチキャストグループ宛て）	○	○
	Group-and-Source-Specific Query	マルチキャストグループの参加問い合わせ（特定の送信者およびマルチキャストグループ宛て）	○	○
Version 3 Multicast Membership Report	Current State Report	参加しているマルチキャストグループとフィルタモードの要求	×	○
	State Change Report	参加しているマルチキャストグループとフィルタモードの更新要求	×	○

（凡例）　○：サポートする　×：サポートしない

フィルタモードおよび送信元リストはマルチキャストグループ参加後に変更でき，IGMPv3 Report メッセージに含まれる Group Record で指定します。本装置がサポートする Group Record タイプを次の表に示します。

表 24-4　Group Record タイプ

タイプ		意味	サポート
Current State Report	MODE_IS_INCLUDE	INCLUDE モードであることを示します	○
	MODE_IS_EXCLUDE	EXCLUDE モードであることを示します	○※
State Change Report	CHANGE_TO_INCLUDE_MODE	フィルタモードを INCLUDE モードに変更することを示します	○
	CHANGE_TO_EXCLUDE_MODE	フィルタモードを EXCLUDE モードに変更することを示します	○※
	ALLOW_NEW_SOURCES	マルチキャストパケットの受信を希望する送信者を追加することを示します	○
	BLOCK_OLD_SOURCES	マルチキャストパケットの受信を希望する送信者を削除することを示します	○

（凡例）　○：サポートする

注※　送信元リストは無視します。

24.2.3　IGMP の動作

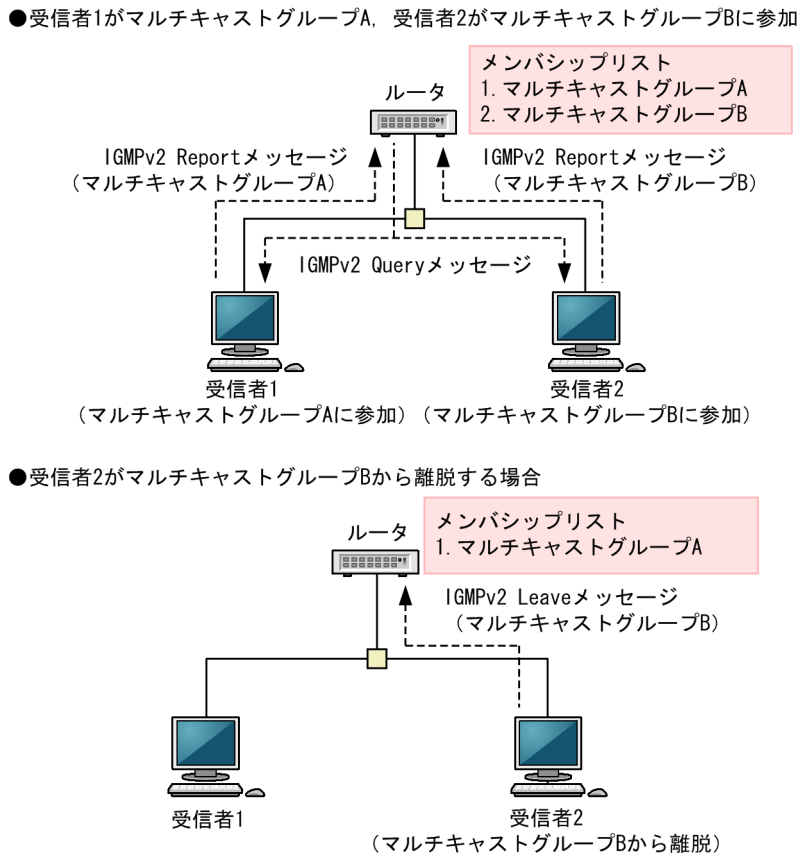
(1)　IGMPv2 の動作

IGMPv2 メッセージを使用した IGMPv2 の動作を次に示します。

- マルチキャストルータは直接接続するインタフェース上にマルチキャストメンバシップの情報を得るため，定期的に IGMPv2 Query（General Query）メッセージを全マルチキャスト受信者（224.0.0.1）宛てに送信します。
- 受信者は IGMPv2 Query（General Query）メッセージを受信すると，IGMPv2 Report メッセージを該当するマルチキャストグループ宛てに送信して，マルチキャストグループへの参加要求をします。
- マルチキャストルータは受信者から IGMPv2 Report メッセージを受信すると，そのグループアドレスをメンバシップリストに追加します。
- マルチキャストルータは受信者から IGMPv2 Leave メッセージを受信すると，そのグループアドレスをメンバシップリストから削除します。

IGMPv2 マルチキャストグループの参加および離脱動作を次の図に示します。

図 24-3　IGMPv2 マルチキャストグループの参加および離脱動作



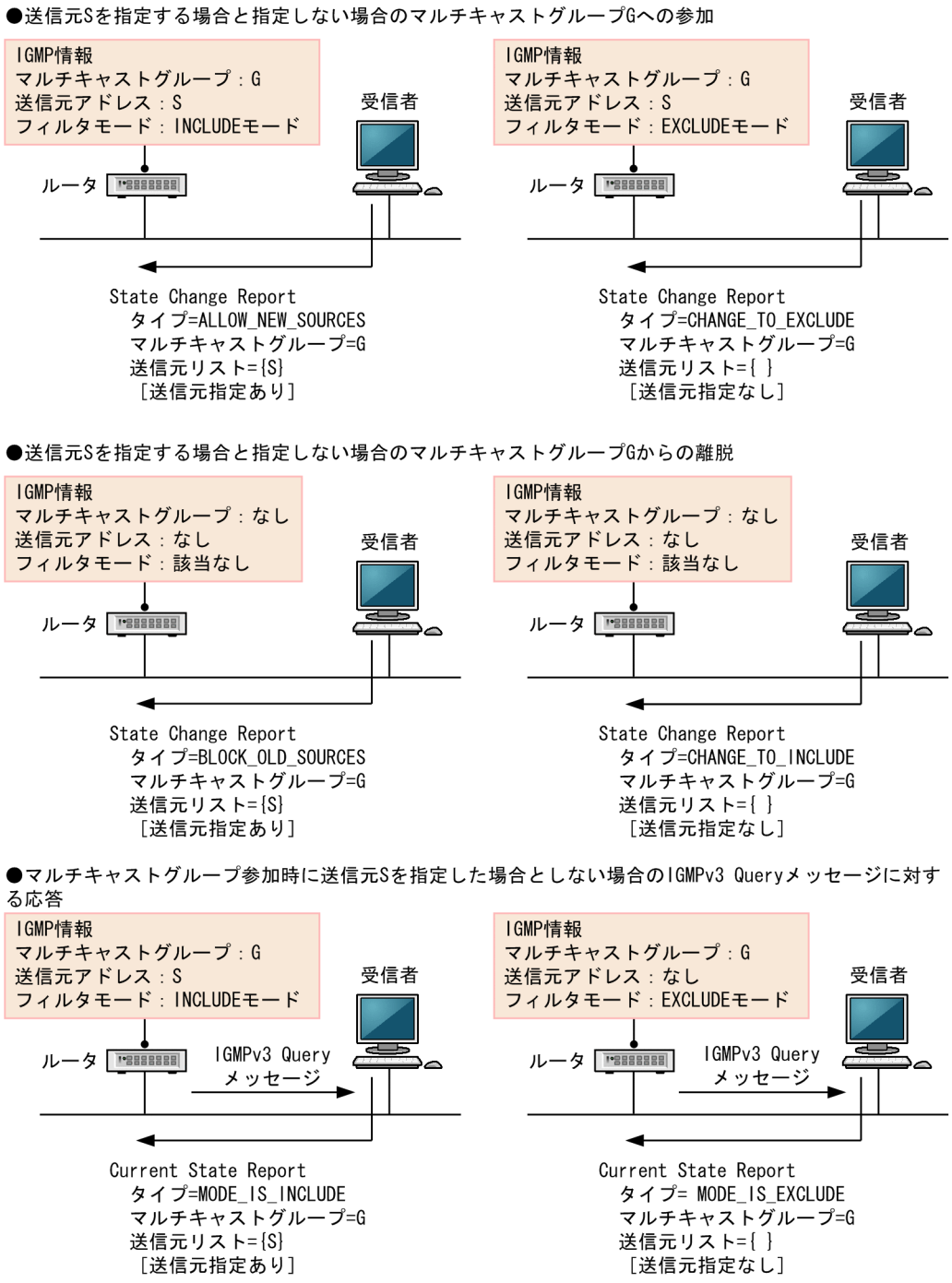
(2)　IGMPv3 の動作

IGMPv3 メッセージを使用した IGMPv3 の動作を次に示します。

- マルチキャストルータは直接接続するインタフェース上にマルチキャストメンバシップの情報を得るため，定期的に IGMPv3 Query（General Query）メッセージを全マルチキャスト受信者（224.0.0.1）宛てに送信します。
- 受信者は IGMPv3 Query（General Query）メッセージを受信すると，IGMPv3 Report（Current State Report）メッセージを 224.0.0.22 宛てに送信して，マルチキャストグループへの参加要求をします。
- マルチキャストルータは受信者から IGMPv3 Report（State Change Report）メッセージを受信すると，Group Record タイプの内容に応じてそのグループアドレスをメンバシップリストに追加，またはメンバシップリストから削除します。

IGMPv3 マルチキャストグループの参加および離脱動作を次の図に示します。

図 24-4　IGMPv3 マルチキャストグループの参加および離脱動作



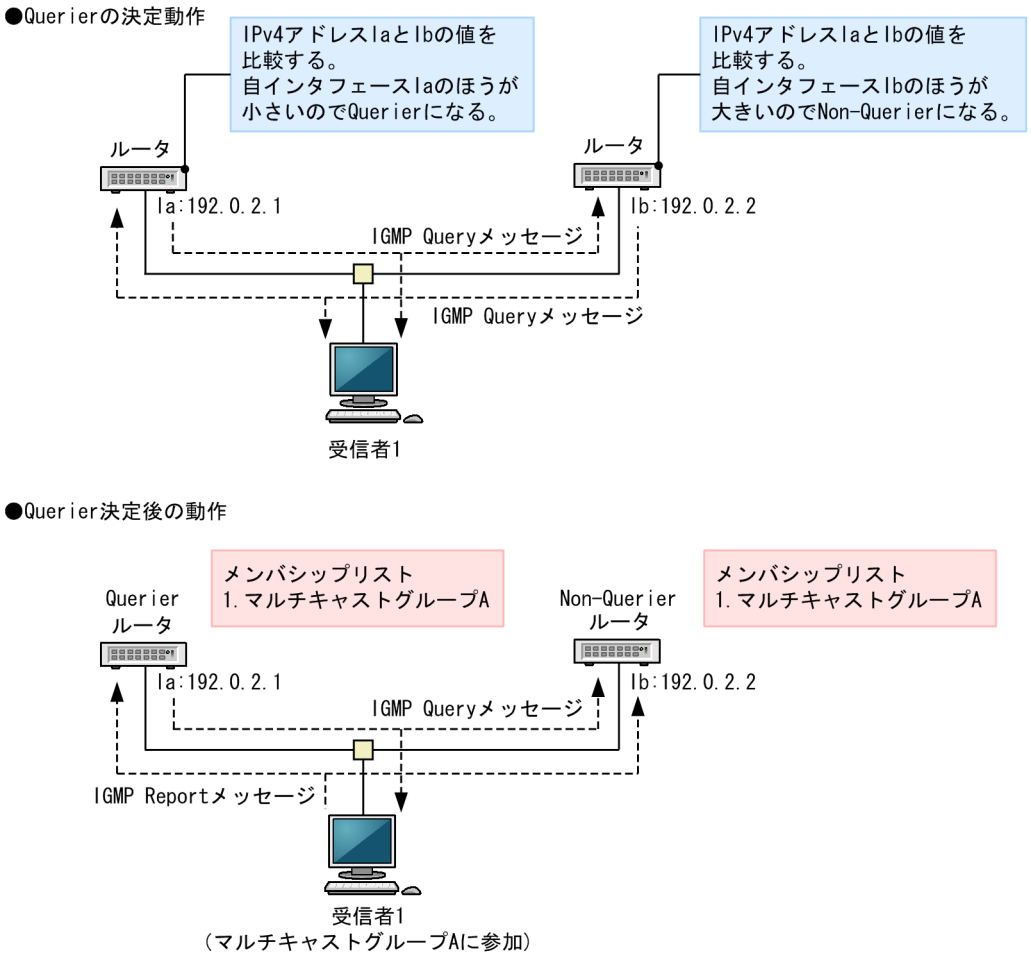
24.2.4　Querier の決定

IGMP ルータは Querier か Non-Querier のどちらか一方の役割を果たします。同一ネットワーク上に複数のルータが存在する場合，そのうちの一つが定期的な IGMP Query メッセージを送信する Querier になります。

Querier を決定するには，同一ネットワーク上に存在する IGMP ルータから受信した IGMP Query メッセージの送信元 IPv4 アドレスと自インタフェースの IPv4 アドレスを比較します。自インタフェースの方

が小さければ Querier として動作します。自インタフェースの方が大きければ Non-Querier となり，IGMP Query メッセージは送信しません。この動作によって同一ネットワーク上には Querier は一つだけ存在することになります。Querier と Non-Querier の決定を次の図に示します。

図 24-5　Querier と Non-Querier の決定



Querier になると，送信元 IPv4 アドレスが自インタフェースより小さい IGMP Query メッセージを受信するまで Querier として動作して，IGMP Query メッセージを定期的（デフォルトでは 125 秒）に送信します。

Non-Querier は IGMP Query メッセージを一定時間（デフォルトでは 255 秒）受信しなかった場合，Querier として動作します。

24.2.5　IPv4 グループメンバの管理

(1)　IGMPv2 使用時の IPv4 グループメンバ管理

IGMPv2 使用時のグループメンバの登録および削除について説明します。

本装置が受信者からの IGMPv2 Report メッセージを受信すると，マルチキャストグループ情報を登録します。Querier，Non-Querier ともに IGMPv2 Report メッセージを受信すると，マルチキャストグループ情報を登録します。

本装置がマルチキャストグループへの離脱要求である IGMPv2 Leave メッセージを受信した場合，該当するマルチキャストグループ情報を削除しますが，Querier と Non-Querier では動作が異なります。

本装置が Querier の場合

IGMPv2 Leave メッセージを受信した時，離脱要求を受信したマルチキャストグループに参加しているほかの受信者の存在を確認するために，IGMPv2 Query（Group-Specific Query）メッセージを 1 秒間隔で 2 回送信します。そのあと，該当するマルチキャストグループ宛ての IGMPv2 Report メッセージを 1 秒間受信しないときに，該当するマルチキャストグループ情報を削除します。

本装置が Non-Querier の場合

受信した IGMPv2 Leave メッセージを無視します。Querier が送信した IGMPv2 Query（Group-Specific Query）メッセージを 2 回受信したあと，該当するマルチキャストグループ宛ての IGMPv2 Report メッセージを 1 秒間受信しないときに，該当するマルチキャストグループ情報を削除します。

(2)　IGMPv3 使用時の IPv4 グループメンバ管理

IGMPv3 使用時のグループメンバの登録および削除について説明します。

本装置が受信者からの IGMPv3 Report（参加要求）メッセージを受信すると，マルチキャストグループ情報を登録します。ここでのマルチキャストグループ情報とは，グループアドレスと，そのグループアドレスに対応する送信元アドレスを指します。Querier，Non-Querier ともに IGMPv3 Report（参加要求）メッセージを受信すると，マルチキャストグループ情報を登録します。

本装置がマルチキャストグループへの離脱要求である IGMPv3 Report（離脱要求）メッセージを受信した場合，該当するマルチキャストグループ情報を削除しますが，Querier と Non-Querier では動作が異なります。

本装置が Querier の場合

IGMPv3 Report（離脱要求）メッセージを受信した時，該当するマルチキャストグループに参加しているほかの受信者の存在を確認するために，送信元リストの指定有無に応じて次に示す IGMPv3 Query メッセージを 1 秒間隔で 2 回送信します。

- 送信元リスト指定なし：Group-Specific Query メッセージ
- 送信元リスト指定あり：Group-and-Source-Specific Query メッセージ

この IGMPv3 Report（離脱要求）メッセージを受信したあと，該当するマルチキャストグループ宛ての IGMPv3 Report（参加要求）メッセージを 2 秒間受信しないときに，該当するマルチキャストグループ情報を削除します。

本装置が Non-Querier の場合

IGMPv3 Report（離脱要求）メッセージを受信したあと，該当するマルチキャストグループ宛ての IGMPv3 Report（参加要求）メッセージを 2 秒間受信しないときに，該当するマルチキャストグループ情報を削除します。

24.2.6　IGMP タイマ値

(1)　IGMPv2 タイマ値

本装置が使用する IGMPv2 タイマ値を次の表に示します。

表 24-5　IGMPv2 タイマ値

タイマ	内容	デフォルト値（秒）	本装置の設定範囲（秒）
Query Interval※1	IGMP General Query メッセージの送信周期時間	125	60～3600
Query Response Interval	IGMP General Query メッセージに対する IGMP Report メッセージの最大応答待ち時間	10	－
Last Member Query Max Response Time※1※2	離脱要求受信後の IGMP Group-Specific Query メッセージに対する IGMP Report メッセージの最大応答待ち時間	1	0.5～25.5
Other Querier Present Interval※3	Querier 監視時間	255	Robustness Variable※4×Query Interval + Query Response Interval / 2
Startup Query Interval※3	Startup 時 IGMP General Query メッセージを送信する時間	31	Query Interval / 4
Last Member Query Interval※1	離脱要求受信後の IGMP Group-Specific Query メッセージの送信周期	1	0.5～25.5
Group Membership Interval※3	参加要求受信時のグループメンバの保持時間	260	Robustness Variable※4×Query Interval + Query Response Interval
Last Member Query Time※3※5	離脱要求受信時のグループメンバの保持時間	2	Last Member Query Interval×（Last Member Query Count※1－1）＋ Last Member Query Max Response Time

（凡例）　－：該当しない

注※1　コンフィグレーションで設定できます。

注※2　本装置独自（RFC2236 未定義）のタイマです。

注※3　計算式で算出されます（コンフィグレーションで設定できません）。

注※4　Robustness Variable は 2 固定です。

注※5　RFC3376（IGMPv3）に定義されている Last Member Query Time 相当のタイマです。

(2)　IGMPv3 タイマ値

本装置が使用する IGMPv3 タイマ値を次の表に示します。

表 24-6　IGMPv3 タイマ値

タイマ	内容	デフォルト値（秒）	本装置の設定範囲（秒）
Query Interval※1	IGMP General Query メッセージの送信周期時間	125	60～3600

タイマ	内容	デフォルト値（秒）	本装置の設定範囲（秒）
Query Response Interval	IGMP General Query メッセージに対する IGMP Report メッセージの最大応答待ち時間	10	－
Last Member Query Max Response Time※1※2	離脱要求受信後の IGMP Group-Specific Query メッセージおよび IGMP Group-and-Source-Specific Query メッセージに対する IGMP Report メッセージの最大応答待ち時間	1	0.5～25.5
Other Querier Present Interval※3	Querier 監視時間	255	Robustness Variable※4×Query Interval ＋ Query Response Interval / 2
Startup Query Interval※3	Startup 時 IGMP General Query メッセージを送信する時間	31	Query Interval / 4
Last Member Query Interval※1	離脱要求受信後の IGMP Group-Specific Query メッセージおよび IGMP Group-and-Source-Specific Query メッセージの送信周期	1	0.5～25.5
Group Membership Interval※3	参加要求受信時のグループメンバの保持時間	260	Robustness Variable※4×Query Interval ＋ Query Response Interval
Last Member Query Time※3	離脱要求受信時のグループメンバの保持時間	2	Last Member Query Interval×（Last Member Query Count※1－1）＋ Last Member Query Max Response Time
Older Host Present Interval※3	IGMPv3 マルチキャストアドレス互換モードへの移行時間	260	Robustness Variable※4×Query Interval ＋ Query Response Interval

（凡例）　－：該当しない

注※1　コンフィグレーションで設定できます。

注※2　本装置独自（RFC3376 未定義）のタイマです。

注※3　計算式で算出されます（コンフィグレーションで設定できません）。

注※4　Robustness Variable は本装置が Querier のときは 2，Non-Querier のときは Querier の Robustness Variable に従います。

24.2.7　IGMPv1/IGMPv2/IGMPv3 装置との接続

本装置は IGMPv2 と IGMPv3 をサポートします。コンフィグレーションコマンド ip igmp version で，インタフェースごとに使用する IGMP バージョンを設定できます。指定するバージョンに応じた動作を次の表に示します。デフォルトは version 3 です。

表 24-7　IGMP バージョン指定時の動作

指定バージョン	バージョン指定時の動作
version 2	IGMPv2 で動作します。 IGMPv1，IGMPv2 それぞれグループアドレス単位で動作します。IGMPv3 メッセージは無視します。
version 3	IGMPv2，IGMPv3 の両方で動作できます。 IGMPv1，IGMPv2，IGMPv3 それぞれグループアドレス単位で動作します。
version 3 only	IGMPv3 で動作します。 IGMPv1 メッセージ，IGMPv2 メッセージは無視します。

(1)　IGMPv2/IGMPv3 ルータとの接続

冗長構成などによって同一ネットワーク上に複数の IGMP ルータが存在する場合，互いの IGMP Query メッセージを受信することで Querier を決定します（「24.2.4　Querier の決定」を参照してください）。本装置は，IGMP バージョンが version 3 または version 3 only に設定されているインタフェースでの IGMPv2 ルータとの接続をサポートしません（IGMPv2 Query メッセージを無視するため，Querier を決定できなくなります）。IGMPv2 ルータと接続する場合は，該当するインタフェースの IGMP バージョンを version 2 に設定してください。

(2)　IGMPv1 ルータとの混在

本装置は IGMPv2, IGMPv3 だけをサポートします。同一ネットワーク上に IGMPv1 ルータを混在させないでください。

(3)　IGMPv1/IGMPv2/IGMPv3 受信者混在時の動作

IGMPv1 受信者，IGMPv2 受信者，および IGMPv3 受信者が混在するネットワークと接続する場合は，該当するインタフェースの IGMP バージョンをデフォルトの状態で使用してください。ただし，IGMPv1 受信者と IGMPv2 受信者が IGMPv3 Query メッセージを IGMPv1/IGMPv2 Query メッセージとして受信できる（RFC 仕様）ことが必要になります。また，該当するインタフェースの IGMP バージョンを version 2 に設定した場合，IGMPv1 受信者と IGMPv2 受信者の混在をサポートしますが，IGMPv3 受信者は無視します。

IGMPv1 受信者，IGMPv2 受信者，および IGMPv3 受信者が混在する場合，グループメンバの登録はマルチキャストグループへの参加を要求する IGMP のバージョンによって異なります。受信者混在時のグループメンバの登録を次の表に示します。

表 24-8　IGMPv1/IGMPv2/IGMPv3 受信者混在時のグループメンバ登録

マルチキャストグループ参加要求	グループメンバの登録
IGMPv1 で受信	IGMPv1 モードでグループメンバを登録
IGMPv2 で受信	IGMPv2 モードでグループメンバを登録
IGMPv3 で受信	IGMPv3 モードでグループメンバを登録
IGMPv1 と IGMPv2 で受信	IGMPv1 モードでグループメンバを登録
IGMPv1 と IGMPv3 で受信	IGMPv1 モードでグループメンバを登録
IGMPv2 と IGMPv3 で受信	IGMPv2 モードでグループメンバを登録

マルチキャストグループ参加要求	グループメンバの登録
IGMPv1 と IGMPv2 と IGMPv3 で受信	IGMPv1 モードでグループメンバを登録

24.2.8　静的グループ参加機能

IGMP に対応する受信者が存在しないネットワークにマルチキャストパケットを中継するために，静的グループ参加機能を設定します。

静的グループ参加機能を設定したインタフェースは，IGMP Report メッセージを受信しなくてもマルチキャストグループに参加したものと同様に動作します。

本機能は IGMPv2 の機能のため，該当するインタフェースの IGMP バージョンを version 3 only に設定している場合は動作しません。また，version 3 に設定している場合は IGMPv2 でマルチキャストグループに参加したものと同様に動作します。

24.2.9　IGMP 使用時の注意事項

- コンフィグレーションの変更によって静的グループ参加機能を設定した場合，PIM-SM の場合は(*,G)マルチキャスト経路情報，PIM-SSM の場合は(S,G)マルチキャスト経路情報が作成されるまで最大 125 秒掛かります。
- コンフィグレーションで設定している PIM-SSM で使用するアドレス範囲外のグループアドレスに対して，送信元指定ありの IGMPv3 Report メッセージ（参加要求）を受信した場合は，全送信者からのマルチキャストパケットを中継します。

24.3　IPv4 マルチキャスト中継機能

マルチキャストパケットの中継処理はマルチキャスト中継エントリに従ってハードウェアおよびソフトウェアで行います。一度中継したマルチキャストパケットの中継情報はハードウェアのマルチキャスト中継エントリに登録されます。マルチキャスト中継エントリに登録されたマルチキャストパケットはハードウェアで中継して, 登録されていないマルチキャストパケットはソフトウェアのマルチキャスト経路情報から生成したマルチキャスト中継エントリに従って中継します。

24.3.1　IPv4 マルチキャスト中継対象外アドレス

マルチキャスト中継処理の対象外となる IPv4 マルチキャストアドレスを次の表に示します。

表 24–9　IPv4 マルチキャスト中継対象外アドレス

中継対象外アドレス	説明
224.0.0.0/24	サブネット内だけで使用するマルチキャストアドレス

24.3.2　IPv4 マルチキャストパケット中継処理

マルチキャストパケットの中継にはハードウェアの中継処理およびソフトウェアの中継処理があります。

(1)　ハードウェアによるマルチキャストパケット中継処理

ハードウェアによるマルチキャストパケットの中継処理には次の機能があります。

- マルチキャスト中継エントリの検索
  マルチキャストグループ宛てのマルチキャストパケットを受信した場合，ハードウェアのマルチキャスト中継エントリから該当するマルチキャスト中継エントリを検索します。
- マルチキャストパケットを受信したインタフェースの正常性チェック
  マルチキャスト中継エントリの検索でマルチキャスト中継エントリが存在した場合，そのマルチキャストパケットが正しいインタフェースから受信されているかどうかをチェックします。
- マルチキャストパケットのフィルタリング
  コンフィグレーションで設定されたフィルタエントリを参照して中継可否を判断します。
- TTL 値に基づいた中継判断と減算
  マルチキャストパケット中の TTL 値を減算して，TTL 値が 0 より大きい場合は中継します。

(2)　ソフトウェアによるマルチキャストパケット中継処理

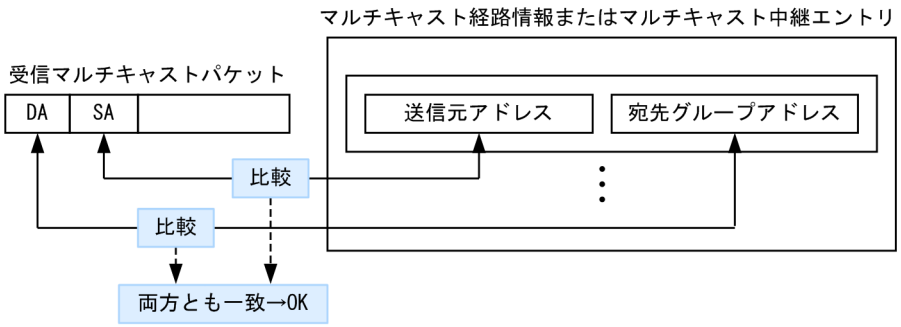
ソフトウェアによるマルチキャストパケット中継処理は次に示す場合ごとに処理が異なります。

- ハードウェアのマルチキャスト中継エントリに登録されていない場合
  最初に受信したマルチキャストパケットをソフトウェアで処理することで，マルチキャスト経路情報からマルチキャスト中継エントリを生成します。生成したマルチキャスト中継エントリをハードウェアに登録するとともに，ソフトウェア処理で使用したマルチキャストパケットを中継します。
- IP カプセル化処理をする場合
  PIM-SM で一時的にランデブーポイント宛てに IP カプセル化して中継します。ランデブーポイントでは各中継先に IP デカプセル化して中継します。

(3)　マルチキャスト経路情報またはマルチキャスト中継エントリの検索

受信したマルチキャストパケットの DA（宛先グループアドレス）と SA（送信元アドレス）に該当するエントリをマルチキャスト経路情報またはマルチキャスト中継エントリから検索します。マルチキャスト経路情報またはマルチキャスト中継エントリの検索方法を次の図に示します。

図 24-6　マルチキャスト経路情報またはマルチキャスト中継エントリの検索方法



(4)　ネガティブキャッシュエントリ

ネガティブキャッシュエントリは，中継できないマルチキャストパケットをハードウェアによって廃棄する機能です。

ネガティブキャッシュエントリは中継先インタフェースの存在しないマルチキャスト中継エントリです。ネガティブキャッシュエントリは，中継できないマルチキャストパケットを受信するとハードウェアに登録します。その後，登録したマルチキャストパケットと同じアドレスのマルチキャストパケットを受信すると，そのマルチキャストパケットをハードウェアによって廃棄します。これによって，大量の中継できないマルチキャストパケットを受信しても，それを原因とする負荷上昇を抑えられます。

(5)　VRF 機能

複数の VRF でマルチキャストを動作させた場合，マルチキャスト中継エントリは VRF ごとに独立して設定できます。異なる VRF では，同じ IPv4 アドレスのマルチキャスト中継エントリを作成できます。また，マルチキャストエクストラネットによって，異なる VRF 間でマルチキャスト通信ができます。

24.4　IPv4 経路制御機能

経路制御機能とは，マルチキャストルーティングプロトコルを使用して収集した隣接情報やマルチキャストグループ情報を基に，マルチキャスト経路情報およびマルチキャスト中継エントリを作成する機能です。

24.4.1　IPv4 マルチキャストルーティングプロトコル概説

マルチキャストルーティングプロトコルは経路制御用のプロトコルです。本装置は次に示すマルチキャストルーティングプロトコルをサポートしています。

- PIM-SM（Protocol Independent Multicast-Sparse Mode）
  ユニキャストの経路機構を利用して，マルチキャストの経路制御を行うプロトコルです。ランデブーポイントへのマルチキャストパケット送信後，最短パスで通信します。
- PIM-SSM（Protocol Independent Multicast-Source Specific Multicast）
  PIM-SSM は PIM-SM の拡張機能です。ランデブーポイントを使用しないで最短パスで通信します。PIM-SM と PIM-SSM は同時に動作できます。ただし，PIM-SM と PIM-SSM で同一のマルチキャストグループを使用できません。

同一ネットワーク内でマルチキャストパケットを中継する場合は，すべてのルータで PIM-SM または PIM-SSM が動作するように設定してください。各プロトコルの適応形態については，「24.5.3　適応ネットワーク構成例」も参照してください。

24.4.2　IPv4 PIM-SM

PIM-SM はルータ間で使用されるマルチキャストルーティングプロトコルです。隣接情報やマルチキャスト配送ツリーへの参加および刈り込み要求などをやり取りすることによって，受信したマルチキャストパケットの中継および廃棄処理を実施します。PIM-SM は最初にランデブーポイント経由でマルチキャストパケットを中継します。そのあと，既存のユニキャストルーティングを利用してマルチキャスト送信者への最短パスに切り替えて，マルチキャストパケットを中継します。

(1)　PIM-SM メッセージサポート仕様

PIM-SM メッセージのサポート仕様を次の表に示します。

表 24-10　PIM-SM メッセージのサポート仕様

メッセージタイプ	機能
PIM Hello	隣接するマルチキャストルータを検出する。
PIM Join/Prune	マルチキャスト配送ツリーの参加および刈り込みをする。
PIM Assert	Forwarder を決定する。
PIM Register	マルチキャストパケットをランデブーポイント宛てに IP カプセル化する。
PIM Register-Stop	PIM Register メッセージを抑止する。
PIM Bootstrap	ブートストラップルータを決定する。また，ランデブーポイントの情報を送信する。
PIM Candidate-RP-Advertisement	ランデブーポイントがブートストラップルータに自ランデブーポイント情報を通知する。

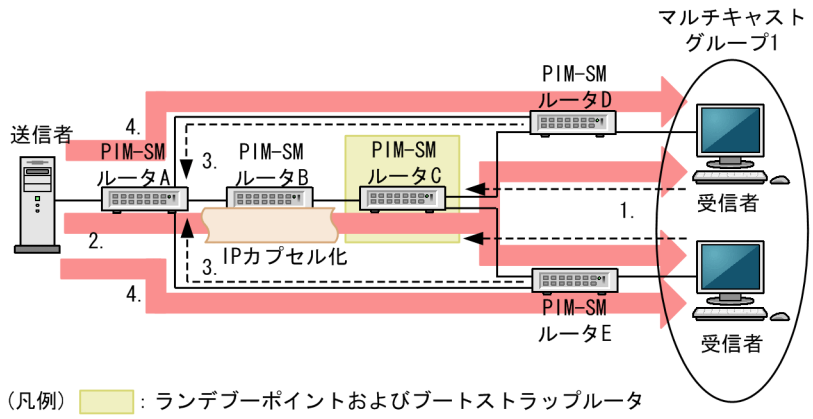
(2)　動作

PIM-SM の動作の流れを次に示します。

1. 各 PIM-SM ルータは IGMP で学習したマルチキャストグループ情報をランデブーポイントに通知します。
2. ランデブーポイントは各 PIM-SM ルータからマルチキャストグループ情報を受信すると，各マルチキャストグループの存在を認識します。
3. PIM-SM は最初にマルチキャストパケットを送信元ネットワークからランデブーポイント経由ですべてのグループメンバに配送するために，送信者を頂点としたランデブーポイント経由配送ツリーを形成します。
4. 送信者から各マルチキャストグループに対して最短パスで到達できるように，既存のユニキャストルーティングを使用して送信者からの最短パス配送ツリーを形成します。
5. 送信者から各グループメンバへ最短パスでマルチキャストパケットを中継します。

PIM-SM の動作概要を次の図に示します。

図 24-7　PIM-SM の動作概要



（凡例）　：ランデブーポイントおよびブートストラップルータ

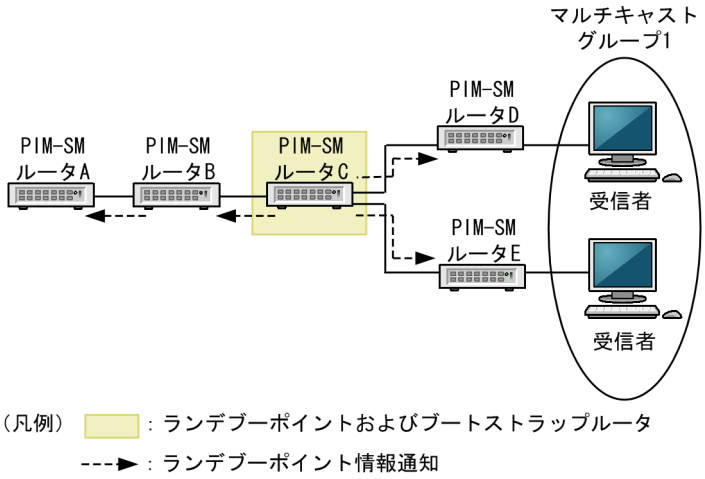
1. マルチキャストグループ参加，およびマルチキャストグループ情報の通知
2. ランデブーポイント経由でマルチキャストパケットの送信
3. 最短パスの決定
4. 最短パスでのマルチキャストパケットの送信

(a)　ランデブーポイントおよびブートストラップルータ

ランデブーポイントルータおよびブートストラップルータはコンフィグレーションで設定します。

ブートストラップルータはランデブーポイントの情報（IPv4 アドレスなど）をすべてのマルチキャストインタフェースに通知します。このとき，ホップバイホップですべてのマルチキャストルータに通知されます。ランデブーポイントおよびブートストラップルータの役割を次の図に示します。

図 24-8　ランデブーポイントおよびブートストラップルータの役割



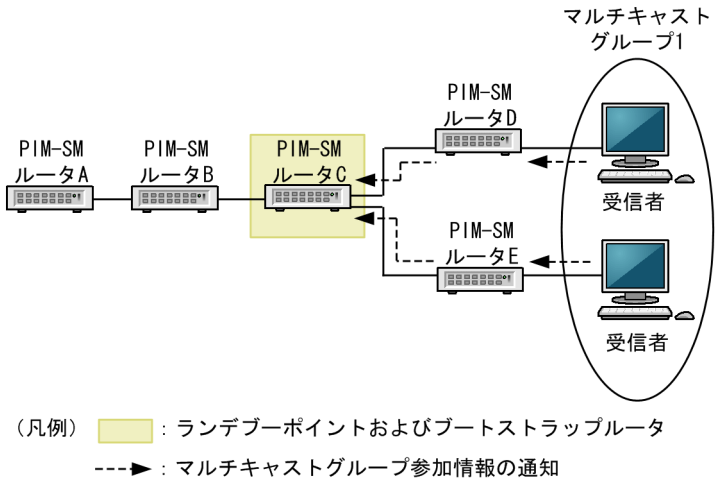
ブートストラップルータ（PIM-SM ルータ C）はランデブーポイント情報をすべてのマルチキャストインタフェースに通知します。ランデブーポイント情報を受信したルータはランデブーポイントの IPv4 アドレスを学習して，受信したインタフェース以外でマルチキャストルータが存在するすべてのインタフェースにランデブーポイント情報を通知します。

ブートストラップルータおよびランデブーポイントのアドレスは，ブートストラップルータおよびランデブーポイントで設定したループバックインタフェースのアドレスとなります。ブートストラップルータ候補とランデブーポイント候補には，同じループバックインタフェースを指定してください。異なるインタフェースを指定した場合，ブートストラップルータ候補の設定が無効になります。

(b)　ランデブーポイントへのマルチキャストグループ参加情報の通知

各ルータは IGMP で学習したマルチキャストグループ参加情報をランデブーポイントに通知します。この通知のときに使用される送信元および宛先 IPv4 アドレスは，それぞれ該当するルータのアドレス（コンフィグレーションコマンド no system-source-address を設定していないループバックインタフェースに設定したアドレス）になります。ランデブーポイントはマルチキャストグループ情報を受信すると，マルチキャストグループの存在をインタフェースごとに認識します。ランデブーポイントへのマルチキャストグループ参加情報の通知を次の図に示します。

図 24-9　ランデブーポイントへのマルチキャストグループ参加情報の通知



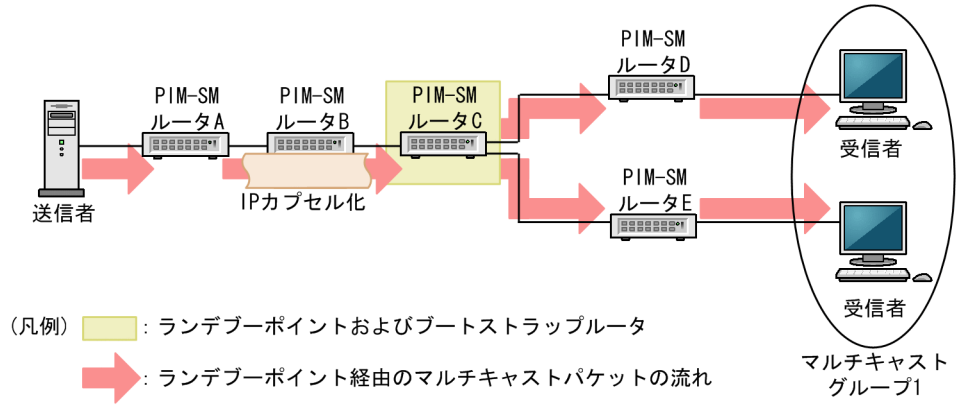
各受信者は IGMP でマルチキャストグループ 1 に参加します。PIM-SM ルータ D および PIM-SM ルータ E はマルチキャストグループ 1 情報を学習して，ランデブーポイント（PIM-SM ルータ C）にマルチキャストグループ 1 情報を通知します。ランデブーポイント（PIM-SM ルータ C）はマルチキャストグループ 1 情報を受信すると，受信したインタフェースにマルチキャストグループ 1 が存在することを学習します。

(c)　ランデブーポイント経由のマルチキャストパケット通信（IP カプセル化）

送信者 S1 がマルチキャストグループ 1 宛てのマルチキャストパケットを送信した場合，PIM-SM ルータ A はそのマルチキャストパケットをランデブーポイント（PIM-SM ルータ C）宛てに IP カプセル化（PIM Register メッセージ）して送信します。

ランデブーポイント（PIM-SM ルータ C）は IP カプセル化したマルチキャストパケットを受信すると，IP デカプセル化してマルチキャストグループ 1 が存在するインタフェースにマルチキャストグループ 1 宛てのマルチキャストパケットを中継します（マルチキャストグループ 1 の存在は「(b)　ランデブーポイントへのマルチキャストグループ参加情報の通知」で学習済み）。PIM-SM ルータ D および PIM-SM ルータ E は，マルチキャストグループ 1 宛てのマルチキャストパケットを受信すると，マルチキャストグループ 1 が存在するインタフェースにマルチキャストパケットを中継します（マルチキャストグループ 1 の存在は「(b)　ランデブーポイントへのマルチキャストグループ参加情報の通知」の IGMP で学習済み）。ランデブーポイント経由のマルチキャストパケット通信（IP カプセル化）を次の図に示します。

図 24-10　ランデブーポイント経由のマルチキャストパケット通信（IP カプセル化）



なお，この通知に使用される送信元 IPv4 アドレスは，次に示す順で選択されます。

1. ランデブーポイント候補として指定したループバックインタフェースの IPv4 アドレス
2. ブートストラップルータ候補として指定したループバックインタフェースの IPv4 アドレス
3. コンフィグレーションコマンド no system-source-address が設定されていないループバックインタフェースに設定した IPv4 アドレス
4. コンフィグレーションコマンド no system-source-address が設定されている，最小のループバックインタフェース ID を持つループバックインタフェースに設定した IPv4 アドレス
5. ランデブーポイント宛て経路の出力インタフェースの IPv4 アドレス

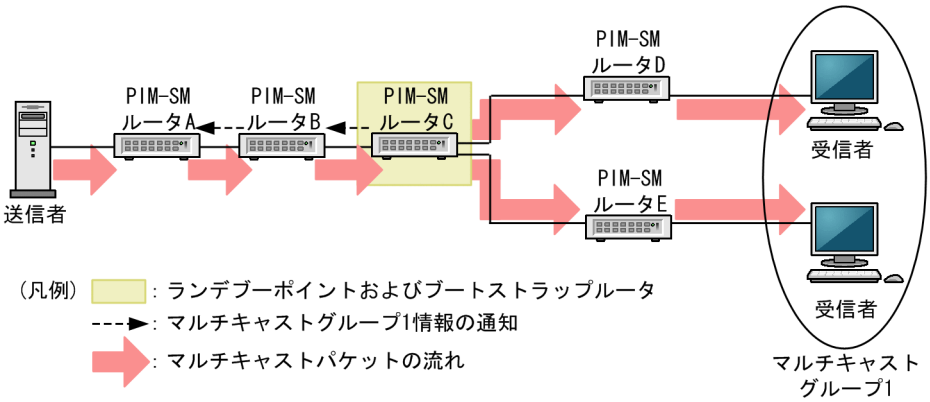
(d)　ランデブーポイント経由のマルチキャストパケット通信（IP デカプセル化）

ランデブーポイント（PIM-SM ルータ C）は IP カプセル化したマルチキャストパケットを受信すると，IP デカプセル化してマルチキャストグループ 1 が存在するインタフェースにマルチキャストグループ 1 宛てのマルチキャストパケットを中継します（「(c)　ランデブーポイント経由のマルチキャストパケット通信（IP カプセル化）」で説明）。

ランデブーポイントはこの処理のあと，既存のユニキャストルーティング情報を基に決定された送信者への最短パス方向にマルチキャストグループ 1 情報を通知します。

マルチキャストグループ 1 情報を受信した PIM-SM ルータ B および PIM-SM ルータ A は受信したインタフェースのマルチキャストグループ 1 の存在を認識（学習）します。PIM-SM ルータ A は送信者が送信したマルチキャストグループ 1 宛てのマルチキャストパケットを IP カプセル化しないで該当するインタフェースに中継します。マルチキャストグループ 1 宛てのマルチキャストパケットを受信した PIM-SM ルータ B，PIM-SM ルータ C，PIM-SM ルータ D および PIM-SM ルータ E はマルチキャストグループ 1 が存在するインタフェースに中継します。ランデブーポイント経由のマルチキャストパケット通信（IP デカプセル化）を次の図に示します。

図 24-11　ランデブーポイント経由のマルチキャストパケット通信（IP デカプセル化）

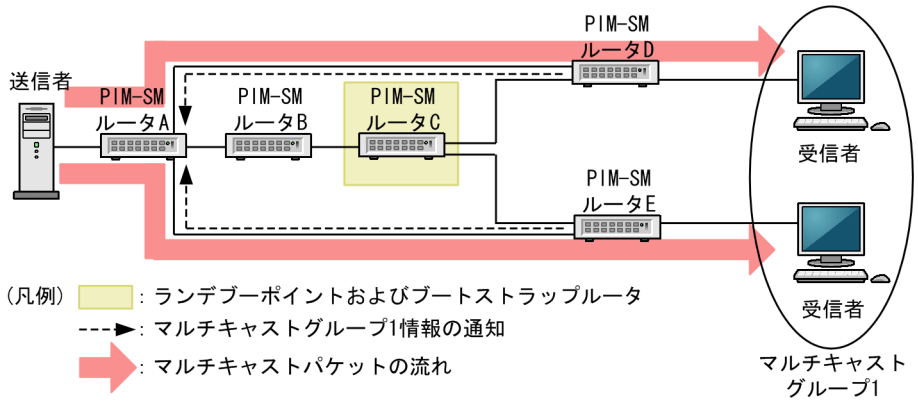


(e)　最短パスのマルチキャストパケット通信

PIM-SM ルータ D および PIM-SM ルータ E が送信者からのマルチキャストグループ 1 宛てマルチキャストパケットを受信した場合（「(d)　ランデブーポイント経由のマルチキャストパケット通信（IP デカプセル化)」で説明)，PIM-SM ルータ D および PIM-SM ルータ E は送信者に対して最短パス（既存のユニキャストルーティング情報）の方向にマルチキャストグループ 1 情報を通知します。

PIM-SM ルータ A は，PIM-SM ルータ D および PIM-SM ルータ E からマルチキャストグループ 1 情報を受信すると，受信したインタフェースにマルチキャストグループ 1 の存在を認識し，送信者のマルチキャストグループ 1 宛てのマルチキャストパケットを受信すると該当するインタフェースに中継します。最短パスのマルチキャストパケット通信を次の図に示します。

図 24-12　最短パスのマルチキャストパケット通信

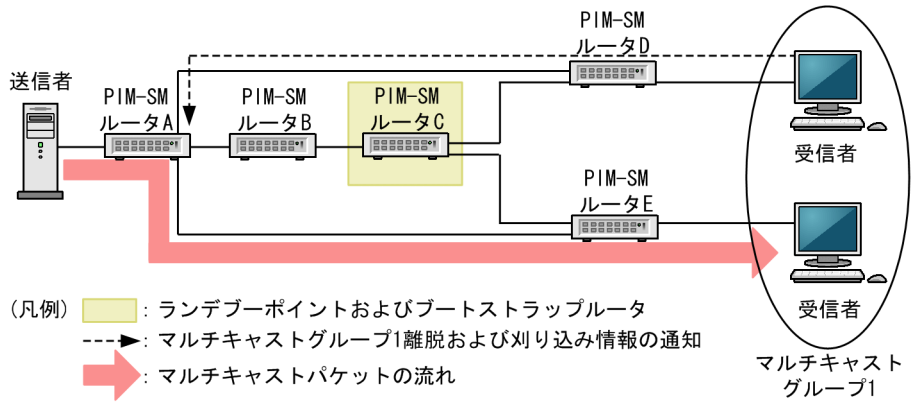


(f)　マルチキャスト配送ツリーの刈り込み

PIM-SM ルータ D は，受信者が IGMP でマルチキャストグループ 1 から離脱した場合，マルチキャストグループ 1 情報を通知していたインタフェースに対してマルチキャストグループ 1 の刈り込み情報を通知します。

PIM-SM ルータ A はマルチキャストグループ 1 の刈り込み通知を受信すると，受信したインタフェースに対してマルチキャストグループ 1 宛てのマルチキャストパケットの中継を中止します。マルチキャスト配送ツリーの刈り込みを次の図に示します。

図 24-13　マルチキャスト配送ツリーの刈り込み



(g)　PIM Bootstrap メッセージの広告範囲制限

IPv4 マルチキャストでは，PIM Bootstrap メッセージの広告範囲を制限する機能をサポートしています。PIM Bootstrap メッセージの広告範囲を制限する場合，広告範囲の境界となるインタフェースにコンフィグレーションコマンド ip pim bsr-border を設定してください。

(3)　近隣検出

PIM-SM ルータは PIM-SM および PIM-SSM を有効にしたすべてのインタフェースに定期的に PIM Hello メッセージを送信します。PIM Hello メッセージは All-PIM-Routers グループアドレス宛て（224.0.0.13）に送信します。このメッセージを受信することで，近隣のマルチキャストルータを動的に検出します。本装置は PIM Hello メッセージの Generation ID オプションをサポートしています。

Generation ID はマルチキャストインタフェースごとに持つ 32 ビットの乱数で，PIM Hello メッセージ送信時に Generation ID を付加して送信します。Generation ID はマルチキャストインタフェースが Up 状態になるたびに再生成します。受信した PIM Hello メッセージに Generation ID オプションが付加されていれば Generation ID を記憶し，Generation ID の変化によって近隣装置のインタフェース障害を検出します。Generation ID の変化を検出すると，近隣装置情報の更新と PIM Hello メッセージ，PIM Bootstrap メッセージおよび PIM Join/Prune メッセージを定期広告のタイミングを待たないで送信します。これによって，マルチキャスト経路情報を速やかに再学習できます。

(4)　Forwarder の決定

同一 LAN 上に複数の PIM-SM ルータを接続している場合，そのネットワークにマルチキャストパケットが重複して中継される可能性があります。

同一 LAN 上に複数の PIM-SM ルータが存在し，二つ以上のルータがその LAN にマルチキャストパケットを中継する場合，PIM-SM ルータは PIM Assert メッセージを使用してそのマルチキャスト経路のプリファ

レンスとメトリックを比較して，送信元ネットワークに対して最適な一つのルータを Forwarder として選択します。

Forwarder となった一つのルータだけが，その LAN でのマルチキャストパケットを中継することで，マルチキャストパケット中継の重複を抑止します。

PIM Assert メッセージによって Forwarder を決定する流れを次に示します。

1. プリファレンスを比較して，プリファレンス値が小さいルータが Forwarder になります。
2. プリファレンス値が等しい場合，メトリックを比較して，メトリック値が小さいルータが Forwarder になります。
3. メトリック値が等しい場合，各ルータの IPv4 アドレスを比較して，IPv4 アドレスが大きいルータが Forwarder になります。

本装置はマルチキャスト経路のプリファレンス値に 101，メトリック値に 1024 を設定して，PIM Assert メッセージを送信します。送信者が本装置と直接接続する場合は，プリファレンス値およびメトリック値に 0 を設定して送信します。また，コンフィグレーションコマンド ip pim assert-preference および ip pim assert-metric を設定することで，ユニキャストルーティングプロトコルから該当するマルチキャスト経路の送信元アドレスへのディスタンス値とメトリック値を取得して，PIM Assert メッセージのプリファレンス値とメトリック値として送信することもできます。

ユニキャストルーティングプロトコルが OSPF の場合，OSPF の経路の学習元によって取得するメトリック値が異なります。OSPF の経路の学習元ごとに取得するメトリック値を次の表に示します。

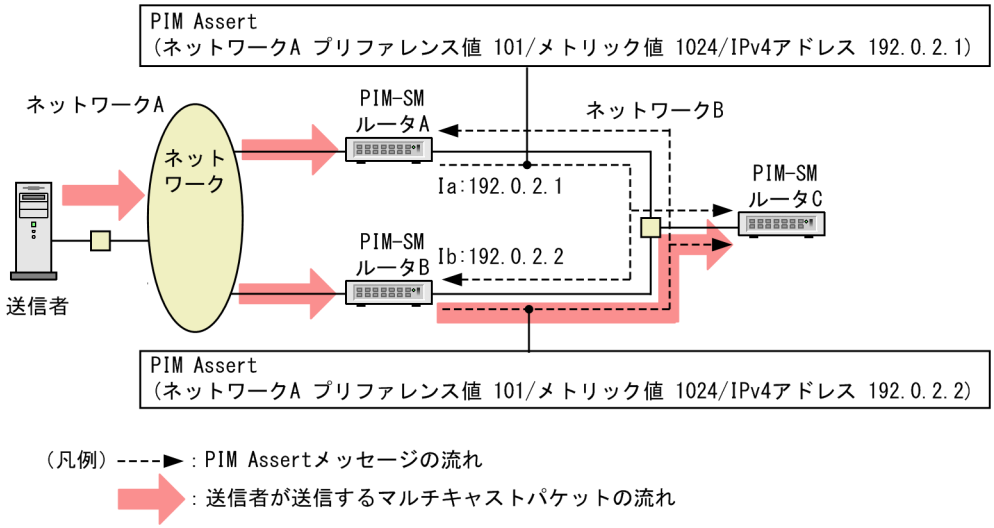
表 24–11　OSPF の経路の学習元ごとに取得するメトリック値

経路の学習元	取得するメトリック値	備考
AS 外経路（TYPE1），NSSA の AS 外経路（TYPE1）	メトリック値＋ Cost 値	第 1 メトリック値
AS 外経路（TYPE2），NSSA の AS 外経路（TYPE2）	メトリック値	
エリア内経路，エリア間経路	Cost 値	

なお，マルチキャストロードバランスと併用した場合，コンフィグレーションコマンド ip pim assert-preference および ip pim assert-metric の設定は無効になります。

Forwarder の決定を次の図に示します。

図 24-14　Forwarder の決定



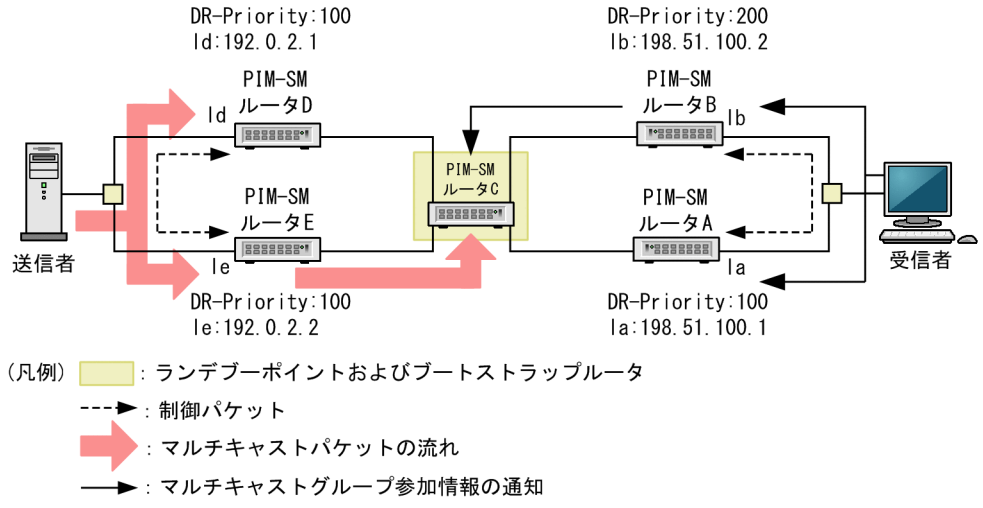
PIM-SM ルータ A の IPv4 アドレス Ia と PIM-SM ルータ B の IPv4 アドレス Ib を比較します。その結果，値の大きい PIM-SM ルータ B が Forwarder になります。

(5)　DR の決定および動作

同一 LAN 上で複数の PIM-SM ルータが存在する場合，PIM-SM ルータ間の制御パケット通信によって中継代表ルータ（DR：Designated Router）を決定します。このとき，同一 LAN 上でいちばん大きい DR-Priority の PIM-SM ルータが DR となります。DR-Priority が等しい場合は，いちばん大きい IPv4 アドレスの PIM-SM ルータが DR となります。また，同一 LAN 上に DR-Priority オプション未サポートの装置が 1 台でも存在する場合は，いちばん大きい IPv4 アドレスの PIM-SM ルータが DR となります。

受信者からのマルチキャストグループ参加情報は DR がランデブーポイント宛てに通知します。送信者が送信したマルチキャストパケットは DR が IP カプセル化してランデブーポイントに送信します。DR の動作を次の図に示します。

図 24-15　DR の動作



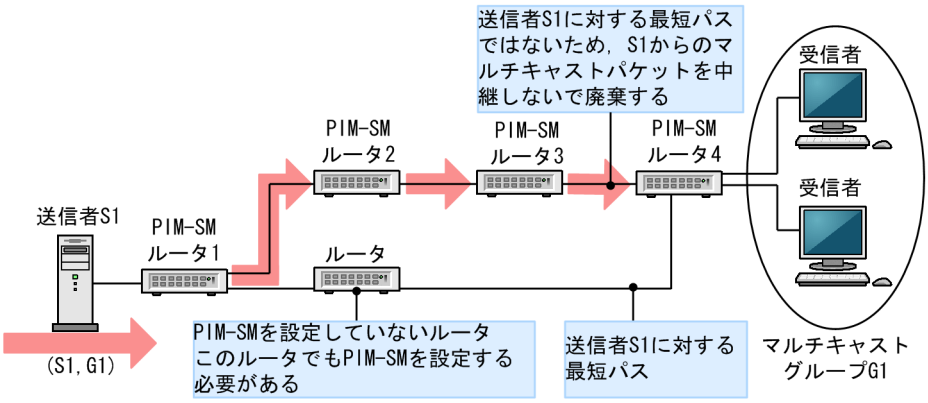
PIM-SM ルータ A と PIM-SM ルータ B の DR-Priority を比較した場合，PIM-SM ルータ B の DR-Priority が大きいため，PIM-SM ルータ B が DR となってランデブーポイントにマルチキャストグループ

参加情報を通知します。PIM-SM ルータ D と PIM-SM ルータ E の DR-Priority を比較した場合，DR-Priority が等しいため，IPv4 アドレスで比較します。その結果，IPv4 アドレスが大きい PIM-SM ルータ E が DR となってランデブーポイントに対して IP カプセル化パケットを中継します。

(6)　冗長経路時の注意事項

次の図に示すような冗長構成の場合，マルチキャストパケットが中継されないので注意してください。冗長経路がある場合は，その経路上のすべてのルータで PIM-SM の設定が必要になります。

図 24-16　冗長経路時の注意



(7)　PIM-SM タイマ仕様

PIM-SM が使用するタイマ値を次の表に示します。

表 24-12　PIM-SM タイマ値

タイマ名	内容	デフォルト値	本装置の設定範囲	備考
Hello_Period※1	PIM Hello メッセージの送信周期	30（秒）	5～3600（秒）	－
Hello_Holdtime※2	隣接関係の保持期間	105（秒）	3.5×Hello_Period（秒）	－
Triggered_Hello_Delay	PIM Hello メッセージの一斉送信を抑止するための調整時間	0～5（秒）	－	起動時の最初の PIM Hello メッセージ送信，または近隣ルータの再起動検出による PIM Hello メッセージ送信時の遅延時間（0～5 秒の間でランダムに決定します）
Assert_Time	PIM Assert メッセージによる中継抑止期間	180（秒）	－	－
Assert_Override_Interval	Assert 制御によるマルチキャスト中継の抑止を更新するための調整時間	3（秒）	－	Assert 敗者がマルチキャスト中継を再開する前（Assert_Time）に Assert 勝者が PIM Assert メッセージを送信して，Assert

タイマ名	内容	デフォルト値	本装置の設定範囲	備考
				敗者の中継抑止時間を更新するための調整時間
t_periodic※1	PIM Join/Prune メッセージの送信周期	60（秒）	1～3600（秒）	－
J/P_HoldTime※2	経路情報および中継先インタフェースの保持期間	210（秒）	3.5×t_periodic（秒）	－
Deletion-Delay-Time※1※3※4	PIM Prune メッセージ受信後のマルチキャスト中継先インタフェースの保持期間	1/3×J/P_HoldTime（秒）	0～300（秒）	－
t_suppressed	PIM Join/Prune メッセージの集中を回避するための送信抑止時間	66～84（秒）	－	－
J/P_Override_Interval	PIM Prune メッセージの受信からマルチキャスト中継停止までの時間	3（秒）	1000～98302（ミリ秒）（Effective_Propagation_Delay ＋ Effective_Override_Interval）	マルチキャスト中継停止までの間にマルチキャスト中継を継続したい下流ルータが PIM Join メッセージを送信すると，マルチキャスト中継は維持されます
Override_Interval※1	Effective_Override_Interval を決定するための本装置の設定時間	2500（ミリ秒）	500～65535（ミリ秒）	－
Effective_Override_Interval	t_override を算出するための LAN 上の決定時間	2500（ミリ秒）	－	LAN 上の全近隣ルータの Override_Interval の最大値※5
t_override	PIM Join/Prune メッセージの一斉送信を抑止するための調整時間	0～2500（ミリ秒）	0～65535（ミリ秒）	調整時間は 0～Effective_Override_Interval の間でランダムに決定します
Propagation_Delay※1	Effective_Propagation_Delay を決定するための本装置の設定時間	500（ミリ秒）	500～32767（ミリ秒）	－
Effective_Propagation_Delay	LAN 上で決定した PIM Join/Prune メッセージが行き渡るまでの遅延時間	500（ミリ秒）	－	LAN 上の全近隣ルータの Propagation_Delay の最大値
Keepalive Timer※1	マルチキャスト中継エントリの保持期間	210（秒）	0（無期限），60～43200（秒）	最大で＋ 90 秒の誤差が発生します
Register_Supression_Time	IP カプセル化送信の抑止期間	60（秒）	－	最大で±30 秒の揺らぎが発生します

タイマ名	内容	デフォルト値	本装置の設定範囲	備考
Register_Probe_Time※1※6※7	IP カプセル化送信の再開確認を送信する時間	5（秒）	5～60（秒）	デフォルトの 5 秒では Register_Supression_Time が満了する 5 秒前に IP カプセル化送信の再開確認（PIM Null-Register メッセージ）を一度だけ送信します
C-RP-Adv-Period	ランデブーポイント候補の通知周期	60（秒）	－	－
RP-Holdtime※2	ランデブーポイント保持期間	150（秒）	2.5×C-RP-Adv-Period（秒）	－
Bootstrap-Period	PIM Bootstrap メッセージの送信周期	60（秒）	－	－
Bootstrap-Timeout※2	PIM Bootstrap メッセージの保持期間	130（秒）	2×Bootstrap-Period ＋ 10（秒）	－
BS_Rand_Override	ブートストラップルータ切り替え調整時間	5～23（秒）	－	本タイマによって優先度の高いブートストラップルータ候補が短時間で選出されます
Negative-Cache-Holdtime※1	ネガティブキャッシュエントリの保持期間	PIM-SM の場合 210（秒），PIM-SSM の場合 3600（秒）	10～3600（秒）	－

（凡例）　－：該当しない

注※1

コンフィグレーションで設定できます。

注※2

計算式で算出されます（コンフィグレーションで設定できません）。

注※3

本タイマ値をコンフィグレーションで設定した場合は設定値を使用しますが，本中継先インタフェースに対して，最後に受信した PIM Join/Prune メッセージに含まれる Join/Prune-Holdtime を超えない値を中継先インタフェースの保持期間として設定します。

注※4

本タイマ値は RFC2362 に準拠した近隣ルータに対して使用するタイマです。コンフィグレーションで設定された値が優先されるため，RFC2362 の規定とは異なった動作をします。なお，コンフィグレーションで値を指定していない場合には RFC2362 の動作に準じます。

注※5

PIM Hello メッセージの LAN Prune Delay オプションを未サポートの近隣ルータが LAN 上に存在する場合，本装置の Override_Interval の設定値によって，次に示す値を適用します。

・Override_Interval≧2500 ミリ秒の場合，2500 ミリ秒

・Override_Interval < 2500 ミリ秒の場合，Override_Interval

注※6

本タイマ値を 10 以上に設定すると，IP カプセル化送信の再開確認を 5 秒おきに複数回送信します。コンフィグレーションで値を指定していない場合には，一度だけ送信します。

注※7

本タイマ値は RFC2362 に準拠しています。

(8)　IPv4 PIM-SM 使用上の注意事項

PIM-SM を使用したネットワークを構成する場合には次に示す制限事項に注意してください。本装置は RFC4601（PIM-SM 仕様）に準拠していますが，一部 RFC との差分があります。RFC との差分を次の表に示します。

表 24–13　RFC との差分

項目	RFC	本装置
パケットフォーマット	RFC にはエンコードグループアドレスおよびエンコードソースアドレスにマスク長を設定するフィールドがある。	エンコードアドレスのマスク長は 32 固定。
	RFC にはエンコードグループアドレスおよびエンコードソースアドレスにアドレスファミリとエンコードタイプを設定するフィールドがある。	エンコードアドレスのアドレスファミリは 1（IPv4），エンコードタイプは 0 固定。IPv4 以外の PIM-SM とは接続できない。
	RFC には PIM メッセージのヘッダに PIM バージョンを設定するフィールドがある。	PIM バージョンは 2 固定。 PIM バージョン 1 と接続できない。
PIM Join/Prune フラグメント	PIM Join/Prune メッセージはネットワークの MTU 長を超えてもフラグメントできる。	送信する PIM Join/Prune メッセージのサイズが大きい場合，8192 オクテットに分割して送信する。さらに，分割して送信する PIM Join/Prune メッセージはネットワークの MTU 長で IP フラグメントによって送信される。
PIM Register メッセージ送信時の IP フラグメント動作	PIM Register ヘッダが付加されることを考慮して，IP フラグメントしたあとにそれぞれのフラグメントパケットを IP カプセル化する。	IP カプセル化したパケットを IP フラグメントする。
IPsec 認証	Authentication Header（AH）を使用する IPsec 転送モードがある。	未サポート。
PMBR との接続	RFC では PMBR（PIM Border Router）との接続および(*，*，RP)マルチキャスト経路情報に関する仕様が記述されている。	PMBR との接続をサポートしていない。また，(*，*，RP)マルチキャスト経路情報もサポートしていない。
最短パスへの切り替え	最短パスへの切り替えタイミングとしてデータレートを基に切り替える方法がある。	ラストホップルータで最初のデータを受信したら，データレートをチェックしないで最短パスへ切り替える。

24.4.3　IPv4 PIM-SSM

PIM-SSM はグループアドレスのアドレス範囲を分離することで，PIM-SM と同時に使用できます。PIM-SSM が使用するグループアドレスは IANA で割り当てられています。本装置では，コンフィグレーション

で PIM-SSM が動作するグループアドレスのアドレス範囲を指定できます。指定したアドレス範囲以外では PIM-SM が動作します。

PIM-SM はマルチキャスト中継エントリの作成にマルチキャストパケットが必要なのに対して，PIM-SSM はマルチキャスト経路情報（PIM Join メッセージ）の交換でマルチキャスト中継エントリを作成して，該当するエントリでマルチキャストパケットを中継します。また，PIM-SSM ではランデブーポイントおよびブートストラップルータは必要ありません。したがって，マルチキャストパケットを中継するときにマルチキャストパケットの IP カプセル化および IP デカプセル化がなくなり，効率の良いマルチキャスト中継が実現できます。

PIM-SSM は IGMPv3（INCLUDE モード）の受信者と接続している場合に動作します。また，本装置には IGMPv2 または IGMPv3（EXCLUDE モード）の受信者が PIM-SSM を利用できるようにする IGMP PIM-SSM 連携機能があります。

(1)　PIM-SSM メッセージサポート仕様

PIM-SSM メッセージのサポート仕様を次の表に示します。

表 24–14　PIM-SSM メッセージのサポート仕様

メッセージタイプ	機能
PIM Hello	隣接するマルチキャストルータを検出する。
PIM Join/Prune	マルチキャスト配送ツリーの参加および刈り込みをする。
PIM Assert	Forwarder を決定する。

(2)　PIM-SSM を動作させる前提条件

本装置のコンフィグレーションで次に示す設定が必要です。

- 各装置の設定
  PIM-SSM が動作するグループアドレスのアドレス範囲を設定します。
- IGMPv3（INCLUDE モード）が動作する受信者が直結している装置
  接続するインタフェースに IGMPv3 を設定します。
- IGMPv2 または IGMPv3（EXCLUDE モード）が動作する受信者が直結している装置
  接続するインタフェースに IGMPv2 または IGMPv3 を設定します。
  使用するグループアドレスに送信元アドレスを設定します。

(3)　PIM-SSM 動作（受信者が IGMPv3（INCLUDE モード）の場合）

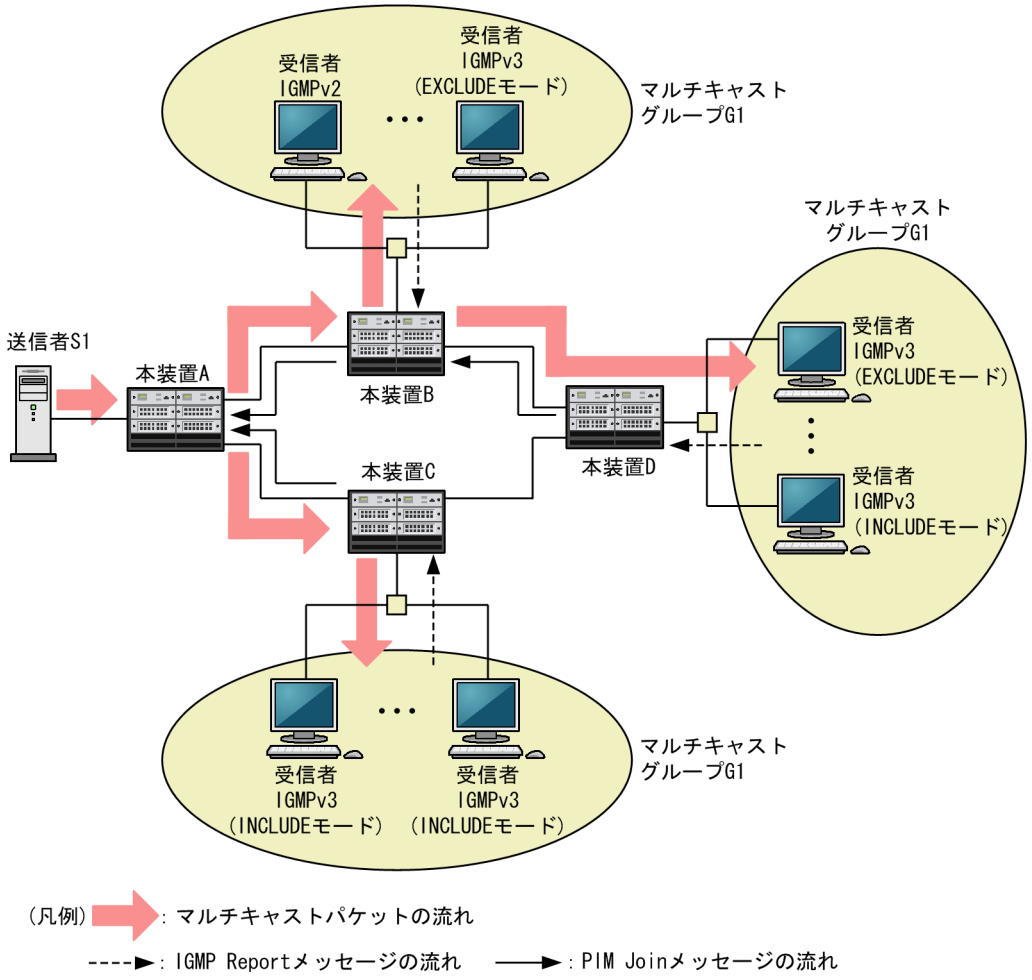
PIM-SSM を使用するためには送信者の情報が必要です。IGMPv3 では，送信者を IGMP Report メッセージで指定すると PIM-SSM を使用できます。マルチキャスト送信者（送信元アドレス：S1）がマルチキャストグループ（グループアドレス：G1）にマルチキャストパケットを送信する場合の動作を次に示します。

1. 受信者からマルチキャストグループに参加するための IGMPv3 Report(G1,S1)メッセージを受信します。
2. IGMPv3 Report(G1,S1)メッセージを受信した装置は，IGMPv3 Report(G1,S1)メッセージで通知された送信元アドレス（S1）の方向（ユニキャストのルーティング情報で決定）に PIM Join メッセージを送信します。この場合，PIM Join メッセージには，送信元アドレス（S1）とグループアドレス（G1）の情報が入ります。

3. PIM Join メッセージを受信した各装置は送信元アドレス（S1）への最短パス方向にホップバイホップで PIM Join メッセージを送信します。PIM Join メッセージを受信した装置は送信元アドレス（S1）とグループアドレス（G1）のマルチキャスト経路情報を学習します。
4. マルチキャスト送信者（送信元アドレス：S1）がマルチキャストグループ（グループアドレス：G1）宛てにマルチキャストパケットを送信します。マルチキャストパケットを受信した装置は学習したマルチキャスト経路情報から生成したマルチキャスト中継エントリに従ってマルチキャストパケットを中継します。

PIM-SSM の動作概要を次の図に示します。

図 24-17　PIM-SSM の動作概要（受信者が IGMPv3（INCLUDE モード）の場合）



(4)　PIM-SSM 動作（受信者が IGMPv2 または IGMPv3（EXCLUDE モード）の場合）

PIM-SSM を使用するためには送信者の情報が必要です。IGMPv2 または IGMPv3（EXCLUDE モード）を使用する場合，本装置で IGMP PIM-SSM 連携機能を設定すると PIM-SSM を使用できます。受信者が IGMPv2 の場合に，マルチキャスト送信者（送信元アドレス：S1）がマルチキャストグループ（グループアドレス：G1）にマルチキャストパケットを送信するときの動作を次に示します。

1. 受信者からマルチキャストグループに参加するための IGMPv2 Report メッセージを受信します。
2. IGMPv2 Report メッセージを受信した装置は，IGMPv2 Report メッセージで通知されたグループアドレス（G1）と IGMP PIM-SSM 連携機能で設定したグループアドレスを比較します。グループアド

レスが一致した場合，IGMP PIM-SSM 連携機能で設定した送信元アドレス（S1）への最短パス方向（ユニキャストのルーティング情報で決定）に PIM Join メッセージを送信します。この場合，PIM Join メッセージには，送信元アドレス（S1）とグループアドレス（G1）の情報が入ります。

3. PIM Join メッセージを受信した各装置は送信元アドレス（S1）への最短パス方向にホップバイホップで PIM Join メッセージを送信します。PIM Join メッセージを受信した装置は送信元アドレス（S1）とグループアドレス（G1）のマルチキャスト経路情報を学習します。
4. マルチキャスト送信者（送信元アドレス：S1）がマルチキャストグループ（グループアドレス：G1）宛てにマルチキャストパケットを送信します。マルチキャストパケットを受信した装置は学習したマルチキャスト経路情報から生成したマルチキャスト中継エントリに従ってマルチキャストパケットを中継します。

PIM-SSM の動作概要については，「図 24–17　PIM-SSM の動作概要（受信者が IGMPv3（INCLUDE モード）の場合）」を参照してください。

(5)　近隣検出

PIM-SM（「24.4.2　IPv4 PIM-SM　(3)　近隣検出」）と同じです。

(6)　Forwarder の決定

PIM-SM（「24.4.2　IPv4 PIM-SM　(4)　Forwarder の決定」）と同じです。

(7)　DR の決定および動作

PIM-SM（「24.4.2　IPv4 PIM-SM　(5)　DR の決定および動作」）と同じです。

(8)　冗長経路時の注意事項

PIM-SM（「24.4.2　IPv4 PIM-SM　(6)　冗長経路時の注意事項」）と同じです。

(9)　PIM-SSM タイマ仕様

PIM-SM（「24.4.2　IPv4 PIM-SM　(7)　PIM-SM タイマ仕様」）を参照してください。

24.4.4　IGMPv3 使用時の IPv4 経路制御動作

(1)　IGMPv3 使用時の IPv4 PIM-SM 動作

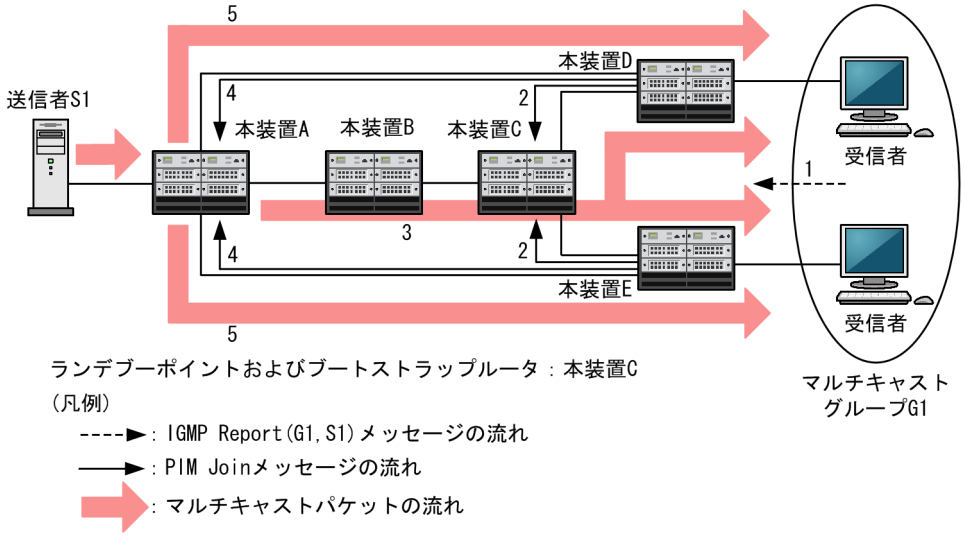
マルチキャスト送信者（送信元アドレス：S1）が PIM-SM で使用するマルチキャストグループ（グループアドレス：G1）にマルチキャストパケットを送信して，受信者が IGMPv3 でマルチキャストグループに参加する場合の動作を次に示します。

1. 受信者からマルチキャストグループに参加するための IGMPv3 Report(G1,S1)メッセージを受信します。
2. IGMPv3 Report(G1,S1)メッセージを受信した装置は，ランデブーポイントへの最短パス方向にグループアドレス（G1）を設定した PIM Join メッセージを送信します。
3. PIM Join メッセージを受信したランデブーポイントは各マルチキャストグループの存在を認識します。マルチキャストパケットを送信元ネットワークからランデブーポイント経由で各グループメンバに配送するために，送信者を頂点としたランデブーポイント経由の配送ツリーを形成します。

4. 送信者から各グループメンバに対して最短パスで到達できるように，既存のユニキャストルーティングを使用して送信者からの最短パスを決定します(PIM Join メッセージを送信者への最短パス方向に送信して，最短パス配送ツリーを形成します)。

5. マルチキャスト送信者（送信元アドレス：S1）がマルチキャストグループ（グループアドレス：G1）宛てに送信したマルチキャストパケットを受信した装置は，最短パス配送ツリーに従ってマルチキャストパケットを中継します。

図 24-18　IGMPv3 使用時の PIM-SM 動作概要



(2)　IGMPv1/IGMPv2 受信者および IGMPv3 受信者混在時の IPv4 経路制御

IGMPv2 で PIM-SSM の設定をしている状態で，IGMPv1 受信者，IGMPv2 受信者と IGMPv3 受信者が混在する場合の経路制御動作について説明します。

コンフィグレーションで設定した PIM-SSM で使用するアドレス範囲に含まれるグループアドレスに対して参加要求を受信した場合，次の表に示すように PIM-SSM が動作します。IGMPv1/IGMPv2 および IGMPv3 受信者混在時の経路制御動作を次の表に示します。

表 24-15　IGMPv1/IGMPv2 および IGMPv3 受信者混在時の経路制御動作

参加グループアドレス	IGMPv1 Report メッセージ IGMPv2 Report メッセージ IGMPv3 Report（EXCLUDE モード）メッセージ	IGMPv3 Report（INCLUDE モード）メッセージ
PIM-SSM で使用するアドレス範囲内	PIM-SSM （IGMP PIM-SSM 連携機能使用時）	PIM-SSM
PIM-SSM で使用するアドレス範囲外	PIM-SM	PIM-SM

IGMPv1 Report メッセージ，IGMPv2 Report メッセージで参加要求を受信した場合，送信元リストには IGMP PIM-SSM 連携機能で設定された送信元アドレスを使用します。IGMPv1 Report メッセージ，IGMPv2 Report メッセージと IGMPv3 Report (EXCLUDE モード) メッセージで同じグループアドレスに対して参加要求を受信した場合，送信元リストには IGMP PIM-SSM 連携機能で設定された送信元アドレスと IGMPv3 Report（INCLUDE モード）メッセージに含まれる送信元リストを合わせたリストを使用します。

24.4.5　系切替時の無停止マルチキャスト中継機能

IPv4 マルチキャストでは，二重化装置による運用で系切替する場合，無停止で PIM-SM および PIM-SSM のマルチキャスト中継を継続する機能をサポートしています。本機能は，コンフィグレーションコマンド ip pim nonstop-forwarding を設定すると有効になります。

本機能では，系切替前に最短パスに切り替わったマルチキャスト中継エントリを無停止中継の対象にしています。そのため，本機能を使用しても，PIM-SM プロトコルの通常処理（ランデブーポイント経由，最短パス切り替えなど）で発生するパケットロスは発生します。

系切替後，再学習時間内は系切替前に設定したハードウェアエントリでマルチキャスト中継を継続します。再学習時間内に新しいマルチキャスト経路情報を学習した場合は，すぐに該当するマルチキャスト中継を開始します。また，学習したエントリに対して離脱要求を受信した場合は，すぐに該当するマルチキャスト中継を停止します。再学習時間内に学習しなかったマルチキャスト中継エントリは，再学習時間終了時に削除します。なお，再学習時間の開始時と終了時にはシステムメッセージを出力します。

再学習時間はデフォルトで 240 秒です。「(2)　再学習時間の算出方法」を参照して，適切な再学習時間を設定してください。

本機能使用時，VRF のインタフェースで IPv4 マルチキャストを使用している場合は，IPv4 マルチキャストを使用した VRF の全インタフェースで本機能が有効になります。

なお，系切替後の IPv4 マルチキャスト中継エントリの再学習状況は，次に示す運用コマンドで確認できます。

- show ip mcache (show ip pim mcache)
- show ip mroute

(1)　無停止マルチキャスト中継機能を使用するための前提条件

(a)　ユニキャストルーティング高可用機能の使用

無停止マルチキャスト中継機能を使用するときは，ユニキャストルーティング高可用機能を有効にしてください。ユニキャストルーティング高可用機能が無効な場合，系切替後に上流のユニキャスト経路が安定しないため，マルチキャスト中継のパケットロスが多発することがあります。

(b)　Generation ID オプションをサポートしている装置の設置

系切替するルータの近隣ルータには，Generation ID オプションをサポート（RFC4601 および RFC5059 に準拠）している装置を設置してください。近隣ルータが Generation ID オプションをサポートしていない場合，系切替後に PIM メッセージの送受信が遅延するため，再学習時間内に再学習が完了しないことがあります。なお，Generation ID オプションについては，「24.4.2　IPv4 PIM-SM」の「(3)　近隣検出」を参照してください。

(2)　再学習時間の算出方法

すべてのマルチキャスト中継エントリの再学習が完了する前に再学習時間が終了すると，未学習のエントリの中継が一時的に停止します。そのため，コンフィグレーションコマンド ip pim nonstop-forwarding の aging-time パラメータには，次の計算式で算出した再学習時間以上の値を設定してください。

再学習時間＝次に示す 1 と 2 のうち最長値＋ 105 秒

1. IGMP のグループメンバ学習時間

各 IGMP インタフェースの IGMP General Query メッセージの送信間隔のうち最長値（デフォルトでは 125 秒）と，IGMP Report メッセージの最大応答待ち時間（本装置が Querier の場合は 10 秒）との合計。

2. PIM Join メッセージの受信時間
各 PIM インタフェースの下流ルータから受信する PIM Join/Prune メッセージの受信間隔のうち最長値（下流ルータが本装置の場合，デフォルトでは 60 秒）。

(3)　無停止マルチキャスト中継機能使用時のタイマ仕様

本機能を有効にした場合，次に示すタイマ仕様を変更します。

- Bootstrap-Period
ブートストラップルータで本機能を使用した場合，再学習時間内は PIM Candidate-RP-Advertisement メッセージの受信と同時に PIM Bootstrap メッセージを送信します（本機能未使用時は 60 秒間隔）。
- RP-Holdtime
ランデブーポイントで本機能を使用した場合，PIM Candidate-RP-Advertisement メッセージの RP-Holdtime をデフォルトでは 260 秒に設定して広告します（本機能未使用時は 150 秒を設定）。
- J/P_HoldTime
上流方向に PIM Join/Prune メッセージを送信する装置で本機能を使用した場合，J/P_HoldTime には次に示す値のうち，長い方の時間を設定して送信します（本機能未使用時は 210 秒を設定）。
  - PIM Join/Prune メッセージの送信間隔（デフォルトで 60 秒）×3.5
  - 再学習時間（デフォルトで 240 秒）＋ 10 秒

(4)　再学習時間内の上流インタフェースの切り替え

再学習時間内にマルチキャスト中継エントリの上流インタフェースのユニキャスト経路が変更された場合，通常と同様に，該当するエントリの上流インタフェースもユニキャスト経路に従って変更します。このとき，一時的にパケットロスが発生します。

このユニキャスト経路の変更を抑止するには，送信元へのユニキャスト経路をスタティック経路で設定してください。また，ユニキャスト経路の変更によって上流インタフェースが該当するエントリの下流インタフェースに変更された場合，この下流インタフェースへの中継を停止します。

(5)　コンフィグレーションコマンド変更時の中継動作

(a)　PIM-SSM で使用するアドレス範囲の変更

再学習時間内にコンフィグレーションコマンドで PIM-SSM で使用するアドレス範囲を変更すると，再学習時間が終了します。この場合，再学習時間内に未学習のマルチキャスト中継エントリの中継を停止します。

(b)　VRF のマルチキャスト中継の停止

再学習時間内にコンフィグレーションコマンドで VRF のマルチキャスト中継を停止すると，再学習時間が終了します。この場合，残りのすべての VRF で，再学習時間内に未学習のマルチキャスト中継エントリの中継を停止します。

(c)　下流インタフェースの IPv4 マルチキャスト設定

再学習時間内にコンフィグレーションコマンドでマルチキャスト中継エントリの下流インタフェースの IPv4 マルチキャストを無効にしても，未学習のエントリの場合は該当するエントリの中継を継続します。ただし，この中継は再学習時間終了時に停止します。

(6)　注意事項

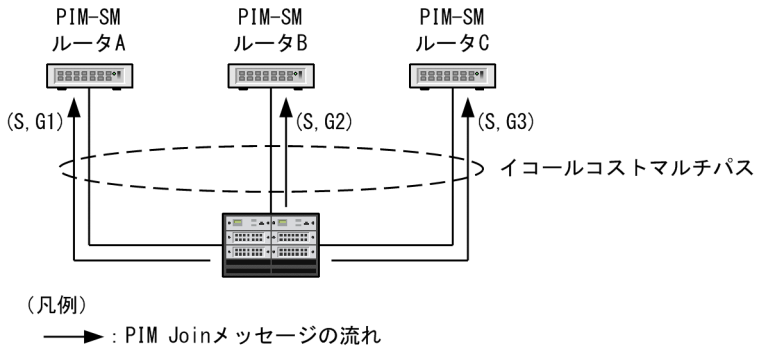
- 本機能を使用する場合，運用系ならびに待機系の BCU および PRU のソフトウェアを本機能対応バージョンにアップデートしてください。

  運用系および待機系の BCU だけが本機能対応バージョンで，PRU が本機能未対応バージョンのまま無停止マルチキャスト中継機能を使用すると，系切替時に IPv4 マルチキャストルーティングプログラムが再起動します。この場合，IPv4 マルチキャストルーティングプログラムがマルチキャスト経路情報を再学習するまで，マルチキャスト中継が停止します。
- 再学習時間の終了時，マルチキャスト中継エントリの無通信を監視しないで，未学習のマルチキャスト中継エントリを削除します。そのため，コンフィグレーションコマンド ip pim keep-alive-time で無通信時のエントリ保持時間を再学習時間より長く設定していても，再学習時間の終了時に該当するマルチキャスト中継エントリは削除されます。
- マルチキャストエクストラネットのマルチキャスト中継エントリは，本機能の対象外です。そのため，系切替が発生すると該当するエントリのマルチキャスト中継を停止します。系切替後，該当するエントリを再学習すると中継を再開します。
- 系切替の直前にマルチキャストパケットの二重中継が発生すると，二重中継の解消に時間が掛かることがあります。この場合，系切替後にマルチキャスト経路情報を再学習すると，PIM Assert メッセージによって二重中継が解消されます。

24.4.6　マルチキャストロードバランス

IPv4 マルチキャストでは，上流経路が複数のイコールコストマルチパスのネットワーク構成で，上流のマルチキャスト経路をイコールコストマルチパス内で分散させることによって，マルチキャスト中継の負荷を軽減させるマルチキャストロードバランスをサポートしています。マルチキャストロードバランスの概要を次の図に示します。

図 24-19　マルチキャストロードバランスの概要



上流経路が複数のイコールコストマルチパスのネットワーク構成で本機能を使用すると，該当するエントリの PIM Join メッセージを，これらの上流経路へイコールコストマルチパス内に分散して送信します。その結果，該当する上流経路から中継されるマルチキャストパケットを分散できます。

本機能では，上流経路を選択するアルゴリズムが複数あります。コンフィグレーションコマンド ip multicast multipath の algorithm パラメータで，ネットワーク構成に適したアルゴリズムを選択してください。

(1)　上流経路分散方式

本機能には，上流経路を自動で分散する方式と，手動で分散する方式があります。

自動分散方式

自動分散方式の設定直後，およびイコールコストマルチパスのユニキャスト経路変更時に，上流経路を自動で分散します。

手動分散方式

手動分散方式の設定直後，およびイコールコストマルチパスのユニキャスト経路変更時には，上流経路を分散しません。運用コマンド rebalance ip mroute を実行すると，上流経路を分散します。ただし，手動分散方式を設定したあとで学習したエントリ，および障害などで上流経路がなくなったエントリは，上流経路を自動で分散します。

コンフィグレーションコマンド ip multicast multipath の rebalance パラメータで，これらの方式を選択してください。なお，手動分散方式で上流経路を分散していない場合は，運用コマンド show ip mroute の rebalance パラメータで分散対象エントリおよび分散先経路を確認できます。

(2)　注意事項

手動分散方式で運用中に, 現在の上流経路と分散後の上流経路が異なるエントリが存在する状態で系切替した場合, 該当するエントリは系切替後の再学習で現在の上流経路から分散後の上流経路に切り替えます。このとき，無停止マルチキャスト中継機能を使用していても，上流経路の切り替え時にパケットロスが発生します。

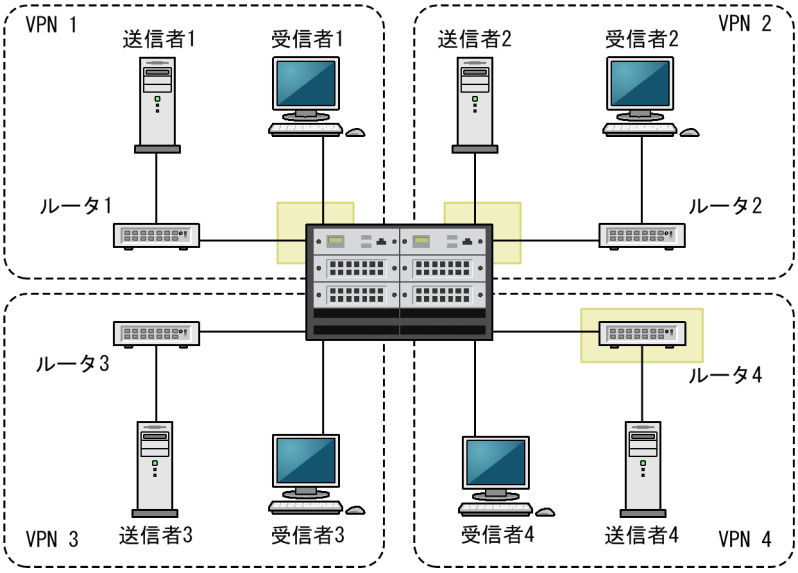
24.4.7　VRF での IPv4 マルチキャスト

(1)　IPv4 マルチキャスト VRF

本装置を複数の VPN に接続して，それぞれの VPN 上でマルチキャストを使用できます。VPN ごとに VRF を設定して，それぞれの VRF でマルチキャストを動作させます。VRF 上のマルチキャストでは，ランデブーポイント，ブートストラップルータ，各種タイマ，PIM-SSM で使用するアドレス範囲などにそれぞれ異なる設定ができます。

本装置を四つの VPN に接続した場合の構成例および本装置での設定情報を次に示します。

図 24-20　VRF でのマルチキャスト



（凡例）　：ランデブーポイントおよびブートストラップルータ

表 24-16　本装置での設定情報

VPN	運用プロトコル	ループバックインタフェースに設定したアドレス	ランデブーポイント () 内はランデブーポイントアドレス	PIM-SSM で使用するアドレス範囲
1	PIM-SM	1.1.1.1	本装置（1.1.1.1）	未使用
2	PIM-SM/ PIM-SSM	2.2.2.2	本装置（2.2.2.2）	232.0.0.0/8
3	PIM-SSM	2.2.2.2	なし	232.10.0.0/16
4	PIM-SM	3.3.3.3	ルータ 4（1.1.1.1）	未使用

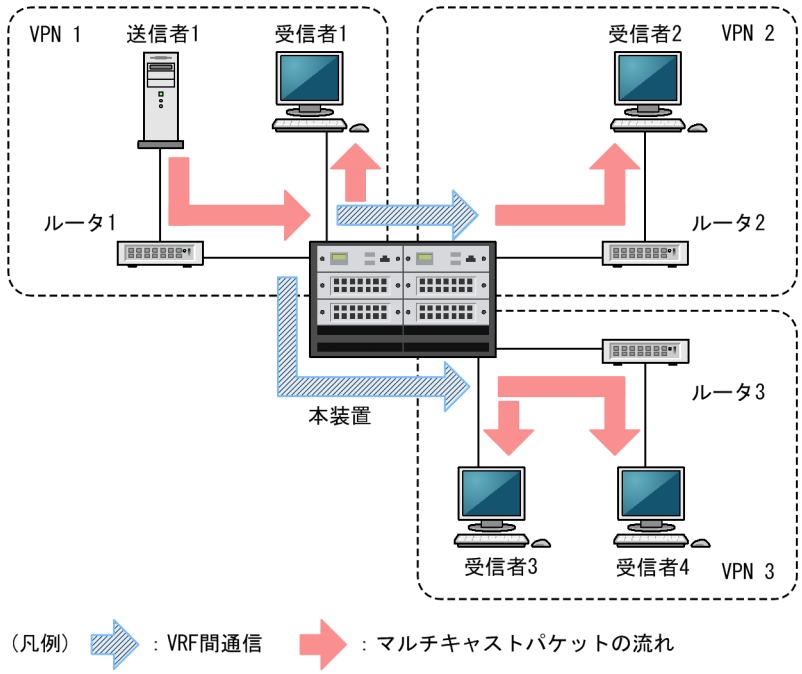
(2)　IPv4 マルチキャストエクストラネット

マルチキャストエクストラネットを使用すると，VRF 間でマルチキャスト中継ができます。また，マルチキャスト経路フィルタリングを使用すると，エクストラネットで使用するグループアドレスの範囲と，下流からの中継要求を許可する VRF を限定できます。マルチキャストエクストラネットは PIM-SSM だけでサポートしています。

なお，ラストホップルータから最短パスを確立するため，ユニキャストエクストラネットによる送信者へのユニキャスト経路が存在する必要があります。

エクストラネットの動作概要を次の図に示します。

図 24-21　マルチキャストエクストラネットの動作概要



(3)　IPv4 マルチキャストエクストラネット使用時の注意事項

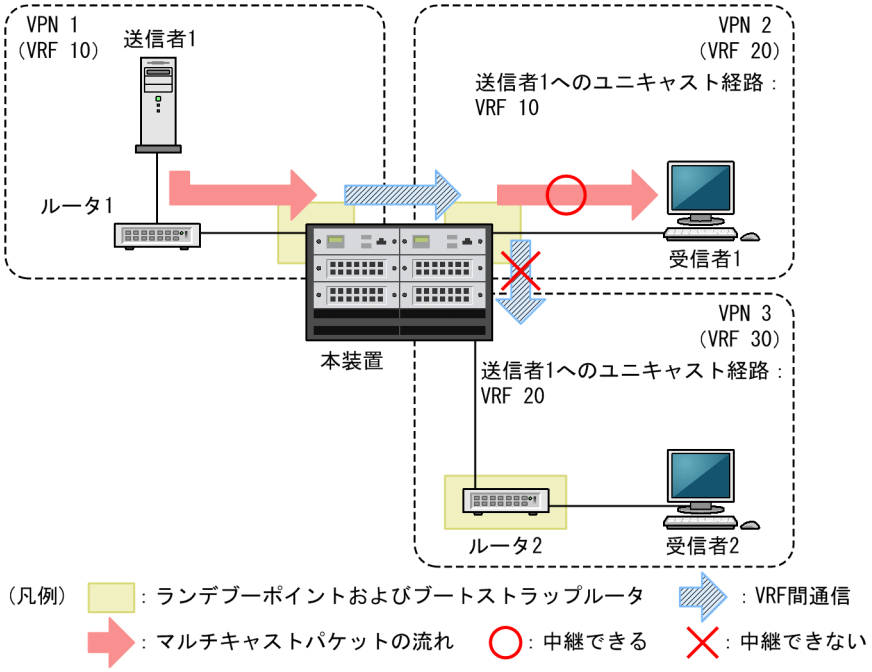
(a)　装置内での 2 段以上の VRF 中継

マルチキャストエクストラネットでは装置内で 2 段以上の VRF 中継を禁止しています。

ある VRF のマルチキャスト経路情報で，上流インタフェースと下流インタフェースの一部にほかの VRF を設定できません。上流インタフェースが異なる VRF のマルチキャスト経路情報は，VRF からの中継要求を無視します。また，下流インタフェースに VRF を持つマルチキャスト経路情報の上流インタフェースが異なる VRF に切り替わった場合，該当マルチキャスト経路情報から VRF の下流インタフェースを切り離します。

次の図に示すように VPN 3 から VPN 1 へのユニキャスト経路が VPN 2 を経由して形成されていた場合，VPN 1 上の送信者 1 が送信するマルチキャストパケットを VPN 2 上の受信者 1 は受信できますが，VPN 3 の受信者 2 は受信できません。

図 24-22　マルチキャストエクストラネット使用時に装置内で VRF 中継を禁止している例



24.5　ネットワーク設計の考え方

24.5.1　IPv4 マルチキャスト中継

本装置でマルチキャストパケットを中継する場合，次の点に注意してください。

(1)　IPv4 PIM-SM/PIM-SSM 共通

(a)　ルーティングプログラムの再起動に伴う中継断

本装置では，運用コマンド restart ipv4-multicast を実行してマルチキャストルーティングプログラムを再起動する場合，マルチキャスト経路情報を再学習するまでマルチキャスト通信が停止するので注意してください。

(b)　動作インタフェース

IP アドレスのマスク長が 8 ビットから 30 ビットのインタフェース上で動作します。

(c)　二重化装置での系切替に伴う中継断

本装置では，二重化装置による運用で系切替する場合，マルチキャスト経路情報を再学習するまでマルチキャスト通信が停止するので注意してください。系切替時に無停止でマルチキャスト通信を継続する場合は，コンフィグレーションコマンド ip pim nonstop-forwarding を設定してください。

(d)　マルチホーム

マルチホームを使用したインタフェースではマルチキャストは動作しません。

(2)　IPv4 PIM-SM

IPv4 で PIM-SM を使用する場合は次の点に注意してください。

(a)　ソフトウェア処理時のパケットロス

本装置では，最初のマルチキャストパケット受信でマルチキャスト通信を行うためのマルチキャスト中継エントリをハードウェアに設定します。マルチキャスト中継エントリを作成するまでの間はソフトウェアでマルチキャストパケットを処理するため，マルチキャスト通信のトラフィック量によっては一時的にマルチキャストパケットをロスする場合があります。

(b)　ソフトウェア処理時のマルチキャストパケットの追い越し

本装置では，ハードウェアへのマルチキャスト中継エントリの設定が完了すると，ハードウェア中継を開始します。そのあと，マルチキャスト中継エントリの生成のためにソフトウェアで処理したマルチキャストパケットを中継します。このときに一部のマルチキャストパケットで追い越しが発生して，マルチキャストパケットの順序が入れ替わる場合があります。

(c)　パス切り替え時の二重中継またはパケットロス

本装置では，ランデブーポイント経由でのマルチキャストパケット中継時およびランデブーポイント経由から最短パス経由への切り替え時，一時的に二重中継またはパケットロスが発生する場合があります。

ランデブーポイント経由のマルチキャストパケットの中継動作およびランデブーポイント経由から最短パス経由への切り替え動作は「24.4.2　IPv4 PIM-SM」を参照してください。

(d)　ループバックインタフェースに設定したアドレスへの到達可能性

本装置をランデブーポイントおよびブートストラップルータとして使用する場合，ループバックインタフェースに設定した IPv4 アドレスがランデブーポイントとブートストラップルータのアドレスになります。このアドレスはマルチキャスト通信する全装置でユニキャストでのルート認識および通信ができる必要があります。

(e)　PIM Register メッセージのチェックサム

本装置以外の装置と混在するシステム構成では，PIM Register メッセージ（IP カプセル化パケット）のチェックサムの計算範囲の相違によってマルチキャスト通信ができない場合があります。ランデブーポイントで PIM Register メッセージがチェックサムエラーによってマルチキャスト中継しない場合は，本装置のコンフィグレーションコマンド ip pim register-checksum で PIM チェックサムを計算する範囲を変更してください。

(f)　静的ランデブーポイント機能

静的ランデブーポイント機能は，ブートストラップルータを使用しないでランデブーポイントを指定する機能です。静的ランデブーポイント機能はコンフィグレーションで設定します。

静的ランデブーポイントはブートストラップルータから PIM Bootstrap メッセージによって広告されたランデブーポイント候補との共存もできます。共存時，静的ランデブーポイントはブートストラップルータから PIM Bootstrap メッセージによって広告されたランデブーポイント候補よりも優先されます。

なお，ランデブーポイント候補のルータは，ランデブーポイントルータアドレスが自アドレスであることを認識することでランデブーポイントとして動作します。したがって，ブートストラップルータを使用しないで静的ランデブーポイント機能を使用してネットワークを設計する場合は，ランデブーポイント候補のルータでも静的ランデブーポイント機能の設定が必要です。

また，静的ランデブーポイント機能を使用する場合，同一ネットワーク上の全ルータに対して同じ設定をする必要があります。

24.5.2　冗長経路（障害などによる経路切り替え）

本装置でマルチキャスト経路が冗長経路になっている場合，次の点に注意してください。

(1)　IPv4 PIM-SM の使用

PIM-SM の場合，次に示す経路切り替えでマルチキャスト通信が再開するまで時間が掛かるので注意してください。なお，時間の表示では送信元のネットワーク情報（ユニキャストルーティング情報）切り替え時間を U と表します。

ここに記述する時間は，本装置が切り替えに掛かる時間です。そのため，実際にマルチキャスト中継が再開するには，本装置が上流ルータに対して PIM Join メッセージを送信してから，上流からマルチキャストパケットが到着するまでの「参加通知時間」が掛かります。

- 優先経路が切り替わった場合，通信再開までに掛かる時間は U 秒です。
  ただし，以降に示す例外があるため，注意してください。
  - 回線障害による優先経路から冗長経路への切り替えに 5 秒以上掛かる（U≧5）場合，通信再開までに U ＋ 0～60 秒掛かることがあります。
  - 回線復旧によって冗長経路から優先経路へ切り替わった場合，優先経路への切り替えには次に示す時間が掛かります。

U ＋（送信者方向の PIM Hello メッセージの送信周期）秒 （デフォルトでは U ＋ 30 秒）

- ランデブーポイントおよびブートストラップルータが本装置に切り替わった（障害やコンフィグレーションなどでランデブーポイントおよびブートストラップルータを本装置にする）場合，通信再開までには次に示す時間が掛かることがあります。

  通信再開までの時間は，ランデブーポイントまたはブートストラップルータで異なります。括弧内はデフォルト値を示します。

  - ランデブーポイント切り替え時：285 秒

    RP-Holdtime（150 秒）＋ Query Interval（125 秒）＋ Query Response Interval（10 秒）
  - ブートストラップルータ切り替え時：最大で 348 秒

    Bootstrap-Timeout（130 秒）＋ BS_Rand_Override（5～23 秒）＋ Bootstrap-Period（60 秒）＋ Query Interval（125 秒）＋ Query Response Interval（10 秒）
- DR（Designated Router）が本装置に切り替わった場合，通信再開までには次に示す時間が掛かることがあります。括弧内はデフォルト値を示します。
  - DR 切り替え時：240 秒

    Hello-Holdtime（105 秒）＋ Query Interval（125 秒）＋ Query Response Interval（10 秒）

障害による冗長経路切り替えだけでなく，構成変更によって意識的に経路を切り替えた場合も，マルチキャスト通信がこれらの時間停止することがあります。システムの構成変更は計画的に実施してください。

(2)　IPv4 PIM-SSM の使用

PIM-SSM の場合，次に示す経路切り替えでマルチキャスト通信が再開するまで時間が掛かるので注意してください。なお，時間の表示では送信元のネットワーク情報（ユニキャストルーティング情報）切り替え時間を U と表します。

ここに記述する時間は，本装置が切り替えに掛かる時間です。そのため，実際にマルチキャスト中継が再開するには，本装置が上流ルータに対して PIM Join メッセージを送信してから，上流からマルチキャストパケットが到着するまでの「参加通知時間」が掛かります。

- 優先経路が切り替わった場合，通信再開までに掛かる時間は U 秒です。

  ただし，以降に示す例外があるため，注意してください。
  - 回線障害による優先経路から冗長経路への切り替えに 5 秒以上掛かる（U≧5）場合，通信再開までに U ＋ 0～60 秒掛かることがあります。
  - 回線復旧によって冗長経路から優先経路へ切り替わった場合，優先経路への切り替えには次に示す時間が掛かります。

    U ＋（送信者方向の PIM Hello メッセージの送信周期）秒 （デフォルトでは U ＋ 30 秒）
- DR（Designated Router）が本装置に切り替わった場合，通信再開までには次に示す時間が掛かることがあります。括弧内はデフォルト値を示します。
  - DR 切り替え時：240 秒

    Hello-Holdtime（105 秒）＋ Query Interval（125 秒）＋ Query Response Interval（10 秒）

24.5.3　適応ネットワーク構成例

(1)　IPv4 PIM-SM を使用する構成

本構成は次の場合に適応します。

- マルチキャスト送信者を限定しない場合
- マルチキャスト送信者が多数存在する場合

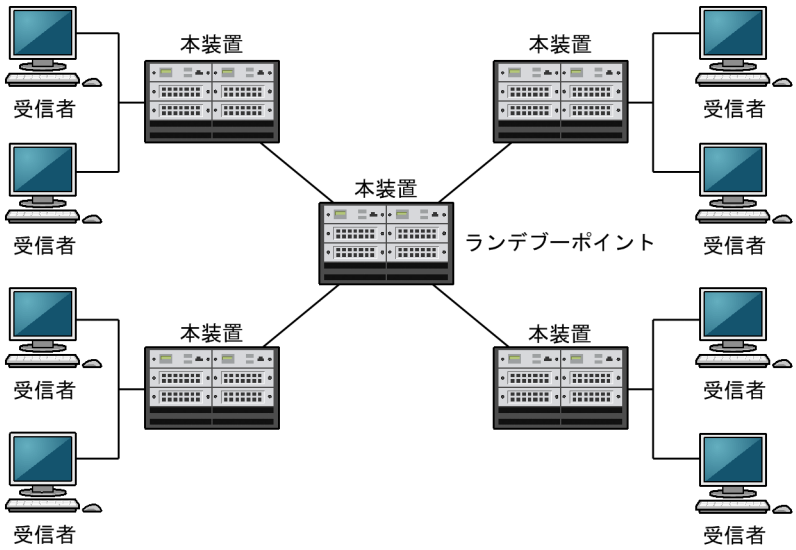
[ネットワークの環境]

1. 前提条件として，すべてのルータでユニキャスト経路が必要です。
2. 本装置間のマルチキャストルーティングプロトコルには PIM-SM を使用します。
3. 各受信者と本装置間のマルチキャストグループ管理制御には IGMP を使用します。
4. 一つの装置をランデブーポイントおよびブートストラップルータとします。
5. ランデブーポイントを静的ランデブーポイントとして指定することもできます。この場合，システム立ち上げ時のランデブーポイント決定までの時間を短縮できます。

[構成図]

構成図を次に示します。

図 24–23　PIM-SM を使用する構成図



(2)　IPv4 PIM-SSM を使用する構成

本構成は次の場合に適応します。

- マルチキャスト送信者を限定する場合（主に配信サーバなど）
- マルチキャスト受信者が IGMPv3 対応で送信する送信者のアドレスを指定できる場合
- ブロードバンドマルチキャスト通信をする場合
- 多チャンネルマルチキャスト通信をする場合

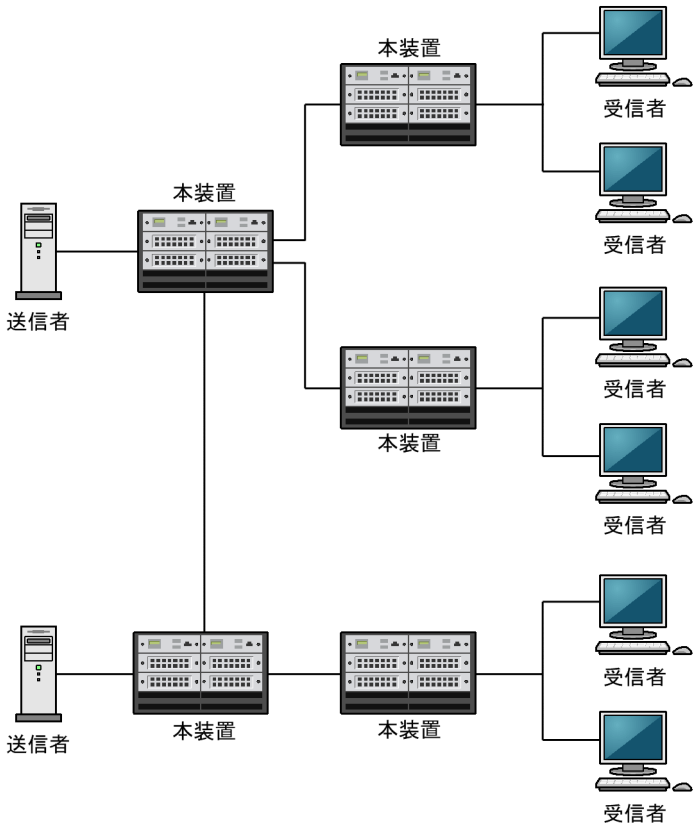
[ネットワークの環境]

1. 前提条件として，すべてのルータでユニキャスト経路が必要です。
2. 本装置間のマルチキャストルーティングプロトコルには PIM-SSM を使用します。
3. 各受信者と本装置間のマルチキャストグループ管理制御には IGMPv2 または IGMPv3 を使用します（IGMPv2 を使用する場合は IGMP PIM-SSM 連携機能の設定が必要です）。

[構成図]

構成図を次に示します。

図 24–24　PIM-SSM を使用する構成図



24.5.4　ネットワーク構成での注意事項

マルチキャストは送信者から各グループメンバ（受信者）にマルチキャストパケットを配信する 1（送信者）：N（受信者）の片方向通信に適します。マルチキャストの適応ネットワーク構成，注意事項を次に示します。

(1)　IPv4 PIM-SM/PIM-SSM 共通

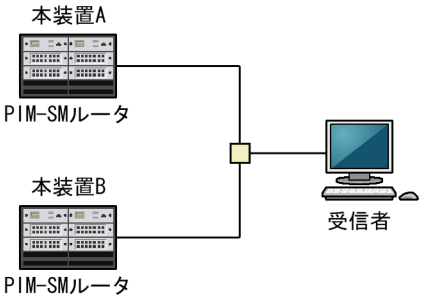
(a)　注意が必要な構成

次に示す構成で PIM-SM または PIM-SSM を使用する場合，注意が必要です。

- 次の図に示す構成のように，受信者と直接接続するルータが同一ネットワーク上に複数存在するインタフェースでは，必ず PIM-SM を動作させてください。

  同一ネットワーク上に複数のルータが存在するインタフェースで PIM-SM を動作させないで IGMP だけを動作させた場合，マルチキャストパケットが二重に中継されることがあります。

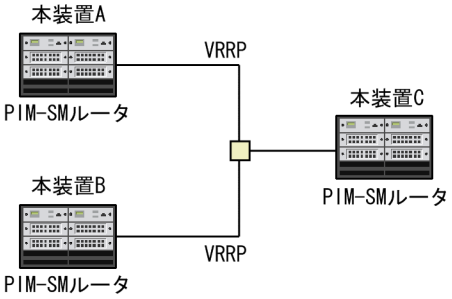
図 24-25　PIM-SM/PIM-SSM で注意が必要な構成（複数ルータと受信者の接続）



- 次の図に示す構成のように，本装置 C が本装置 A と本装置 B に VRRP を設定した仮想インタフェースをゲートウェイとするスタティック経路を設定した環境では，PIM-SM および PIM-SSM が上流ルータを検出できないため，マルチキャスト通信ができません。

  この構成でマルチキャスト通信をする場合は，本装置 C にランデブーポイントアドレス，ブートストラップルータアドレス，およびマルチキャスト送信者アドレスへのゲートウェイアドレスを本装置 A または本装置 B の実アドレスとするスタティック経路を設定する必要があります。

  図 24-26　PIM-SM/PIM-SSM で注意が必要な構成（VRRP を設定した場合）

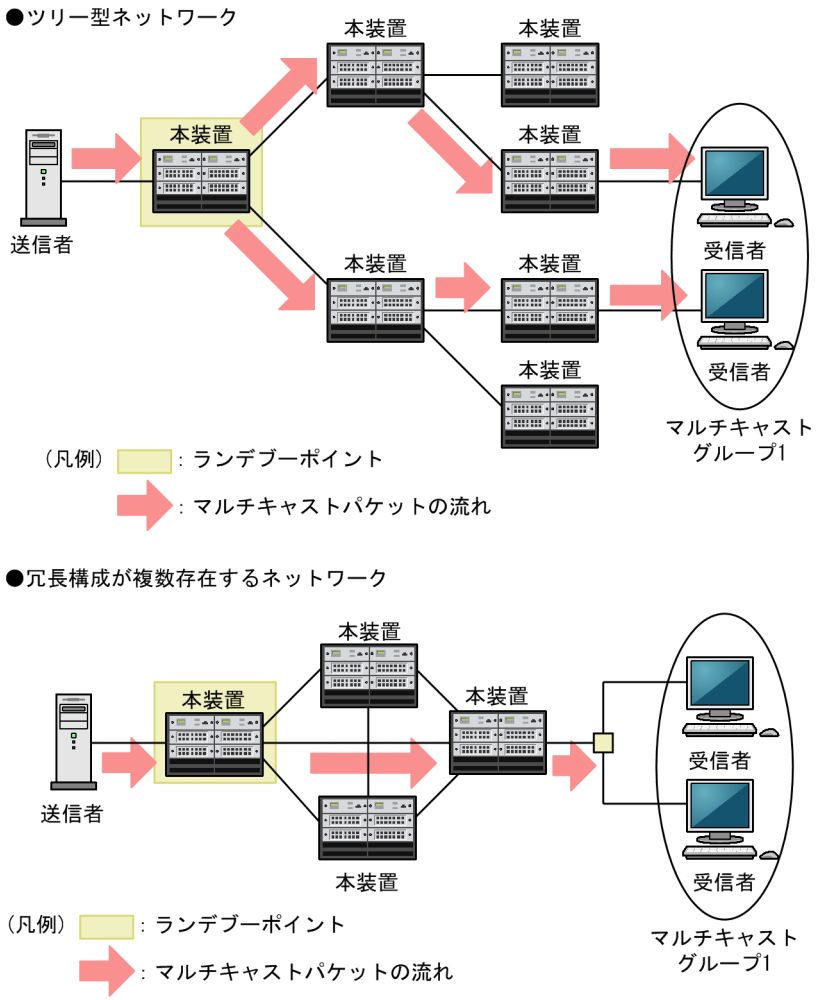


(2)　IPv4 PIM-SM

(a)　推奨構成

PIM-SM では，ツリー型ネットワーク構成および冗長経路が存在するネットワーク構成を推奨します。ただし，ランデブーポイントの配置には十分注意してください。PIM-SM 推奨ネットワーク構成を次の図に示します。

図 24-27　PIM-SM 推奨ネットワーク構成

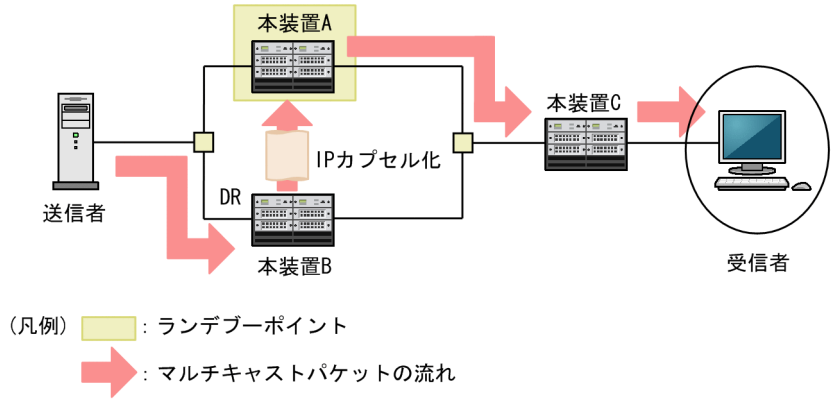


(b)　注意が必要な構成

送信者と直接接続するルータが同一ネットワーク上に 2 台以上存在する構成で PIM-SM を使用する場合は注意が必要です。次の図に示す構成でどれかをランデブーポイントとする場合は，ランデブーポイントが DR（Designated Router）になるようにしてください。

ランデブーポイント以外を DR にした場合，DR からランデブーポイントに対して PIM Register メッセージを送信するため，本装置 A，B に負荷が掛かります。また，PIM Register メッセージ中のマルチキャストパケットを中継するときに，ランデブーポイントでパケットロスが発生するおそれがあります。なお，ランデブーポイントを DR にした場合は，PIM Register メッセージによる IP カプセル化は行いません。

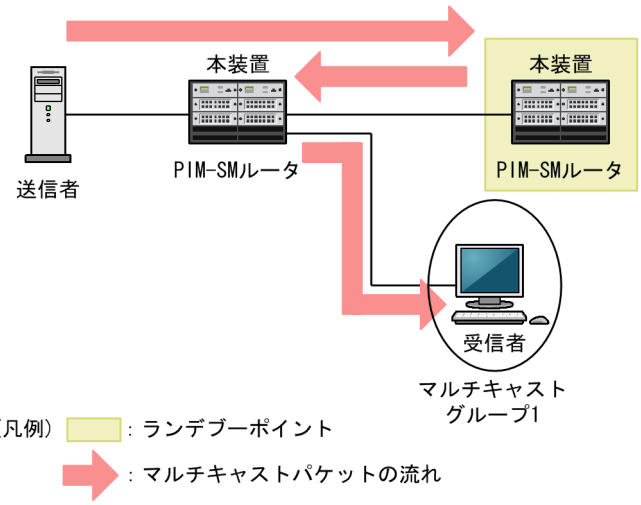
図 24-28　PIM-SM で注意が必要な構成（複数ルータと送信者の接続）



(c)　不適応な構成

送信者とランデブーポイントの間に受信者が存在する構成で PIM-SM は使用しないでください。次の図に示す構成で送信者からマルチキャストグループ 1 へのマルチキャスト通信をする場合，ランデブーポイント経由の中継が効率良く行えません。

図 24-29　PIM-SM で不適応な構成（送信者とランデブーポイントの間に受信者が存在する場合）

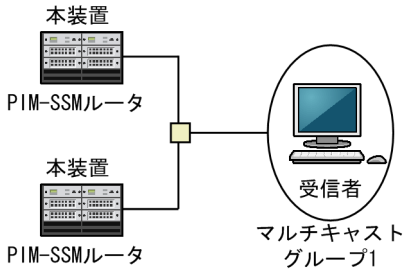


(3)　IPv4 PIM-SSM

(a)　注意が必要な構成

マルチキャスト受信者と同一回線上に複数の PIM-SSM ルータが動作する構成で PIM-SSM を使用する場合は注意が必要です。次の図に示す構成で IGMP PIM-SSM 連携機能を動作させる場合は，同一回線上のすべてのルータにコンフィグレーションコマンド ip pim ssm および ip igmp ssm-map static を設定してください。

図 24-30　PIM-SSM で注意が必要な構成（複数ルータと受信者の接続）



25 IPv4 マルチキャストの設定と運用

この章では，IPv4 マルチキャストのコンフィグレーションの設定方法および状態の確認方法について説明します。

25.1　コンフィグレーション

25.1.1　コンフィグレーションコマンド一覧

IPv4 マルチキャストのコンフィグレーションコマンド一覧を次の表に示します。

表 25-1　コンフィグレーションコマンド一覧

コマンド名	説明
ip igmp group-limit	参加できるマルチキャストグループの最大数を設定します。
ip igmp last-member-query-count	IGMPv2 Leave メッセージまたは IGMPv3 Report（離脱要求）メッセージを受信した際に送信する，IGMP Group-Specific Query メッセージおよび IGMP Group-and-Source-Specific Query メッセージの送信回数を設定します。
ip igmp last-member-query-interval	IGMPv2 Leave メッセージまたは IGMPv3 Report（離脱要求）メッセージを受信した際に送信する，IGMP Group-Specific Query メッセージおよび IGMP Group-and-Source-Specific Query メッセージの送信間隔を設定します。
ip igmp last-member-query-max-response-time	IGMPv2 Leave メッセージまたは IGMPv3 Report（離脱要求）メッセージを受信した際に送信する，IGMP Group-Specific Query メッセージおよび IGMP Group-and-Source-Specific Query メッセージに対する最大応答待ち時間を設定します。
ip igmp query-interval	IGMP Query メッセージの送信間隔を設定します。
ip igmp router	インタフェースで IGMP を動作させます。
ip igmp source-limit	マルチキャストグループ参加時のソースの最大数を設定します。
ip igmp ssm-map enable	IGMP PIM-SSM 連携機能を有効にします。
ip igmp ssm-map static	IGMP PIM-SSM 連携機能でのグループアドレスと送信元アドレスを設定します。
ip igmp static-group	静的グループ参加機能を設定します。
ip igmp version	IGMP バージョンを設定します。
ip multicast multipath	マルチキャストロードバランスを設定します。
ip multicast-routing	IPv4 マルチキャストルーティング機能を有効にします。
ip pim assert-metric	PIM Assert メッセージで使用するメトリック値の取得方法を指定します。
ip pim assert-preference	PIM Assert メッセージで使用するプリファレンス値の取得方法を指定します。
ip pim bsr-border	PIM Bootstrap メッセージの広告範囲を設定します。

コマンド名	説明
ip pim bsr-candidate	ブートストラップルータ候補を設定します。
ip pim deletion-delay-time	PIM Prune メッセージ受信後のマルチキャスト中継先インタフェースの保持期間を設定します。
ip pim dr-priority	DR の優先度を決定するための DR-Priority を設定します。
ip pim keep-alive-time	マルチキャスト中継エントリの無通信時の保持期間を設定します。
ip pim max-interface	IPv4 マルチキャストを設定できるインタフェースの最大数を設定します。
ip pim mcache-limit	マルチキャスト中継エントリの最大数を設定します。
ip pim message-interval	PIM Join/Prune メッセージの送信間隔を設定します。
ip pim mroute-limit	マルチキャスト経路情報の最大数を設定します。
ip pim negative-cache-time	ネガティブキャッシュエントリの保持期間を設定します。
ip pim nonstop-forwarding	無停止マルチキャスト中継機能を設定します。
ip pim override-interval	ほかのルータが送信した PIM Prune メッセージを無効にする PIM Join メッセージが集中するのを回避するための時間を設定します。
ip pim propagation-delay-time	PIM Join/Prune メッセージの転送遅延時間を設定します。
ip pim query-interval	PIM Hello メッセージの送信間隔を設定します。
ip pim register-checksum	PIM Register メッセージのチェックサム範囲を設定します。
ip pim register-probe-time	PIM Register メッセージ送信抑止時間を基に PIM Null-Register メッセージの送信開始時間を設定します。
ip pim rp-address	静的ランデブーポイント機能を設定します。
ip pim rp-candidate	ランデブーポイント候補を設定します。
ip pim rp-mapping-algorithm	ランデブーポイント選出アルゴリズムの種別を設定します。
ip pim sparse-mode	インタフェースで PIM-SM，PIM-SSM および IGMP を動作させます。
ip pim ssm	PIM-SSM で使用するグループアドレスの範囲を設定します。

25.1.2　コンフィグレーションの流れ

使用する構成によって次の設定例を参照してください。

- PIM-SM を使用する場合
  - IPv4 マルチキャストルーティング機能の設定
  - IPv4 PIM-SM/PIM-SSM 動作インタフェースの設定

- IPv4 PIM-SM ランデブーポイント候補の設定（自装置をランデブーポイントにする場合）
- IPv4 PIM-SM ブートストラップルータ候補の設定（自装置をブートストラップルータにする場合）
- IGMP の設定

- PIM-SM（静的ランデブーポイント機能）を使用する場合
  - IPv4 マルチキャストルーティング機能の設定
  - IPv4 PIM-SM/PIM-SSM 動作インタフェースの設定
  - IPv4 PIM-SM 静的ランデブーポイント機能の設定
  - IGMP の設定
- PIM-SSM を使用する場合
  - IPv4 マルチキャストルーティング機能の設定
  - IPv4 PIM-SM/PIM-SSM 動作インタフェースの設定
  - IPv4 PIM-SSM の設定
  - IGMP の設定
- VRF で PIM-SM を使用する場合
  - VRF での IPv4 マルチキャストルーティング機能の設定
  - VRF での IPv4 PIM-SM/PIM-SSM 動作インタフェースの設定
  - VRF での IPv4 PIM-SM ランデブーポイント候補の設定（該当 VPN で自装置をランデブーポイントにする場合）
  - VRF での IPv4 PIM-SM ブートストラップルータ候補の設定（該当 VPN で自装置をブートストラップルータにする場合）
  - VRF での IGMP の設定
- VRF で PIM-SM（静的ランデブーポイント機能）を使用する場合
  - VRF での IPv4 マルチキャストルーティング機能の設定
  - VRF での IPv4 PIM-SM/PIM-SSM 動作インタフェースの設定
  - VRF での IPv4 PIM-SM 静的ランデブーポイント機能の設定
  - VRF での IGMP の設定
- VRF で PIM-SSM を使用する場合
  - VRF での IPv4 マルチキャストルーティング機能の設定
  - VRF での IPv4 PIM-SM/PIM-SSM 動作インタフェースの設定
  - VRF での IPv4 PIM-SSM の設定
  - VRF での IGMP の設定
- VRF（エクストラネット）で PIM-SSM を使用する場合
  - VRF での IPv4 マルチキャストルーティング機能の設定
  - VRF での IPv4 PIM-SM/PIM-SSM 動作インタフェースの設定
  - VRF での IPv4 PIM-SSM の設定
  - IPv4 マルチキャストエクストラネットの設定
  - VRF での IGMP の設定

25.1.3　IPv4 マルチキャストルーティング機能の設定

[設定のポイント]

本装置で IPv4 マルチキャストルーティング機能を動作させるには，ここでの設定のほかに，一つ以上のインタフェースで PIM-SM または PIM-SSM（ip pim sparse-mode コマンド）の設定が必要です。

[コマンドによる設定]

1. **(config)# ip multicast-routing**
   IPv4 マルチキャストルーティング機能を有効にします。

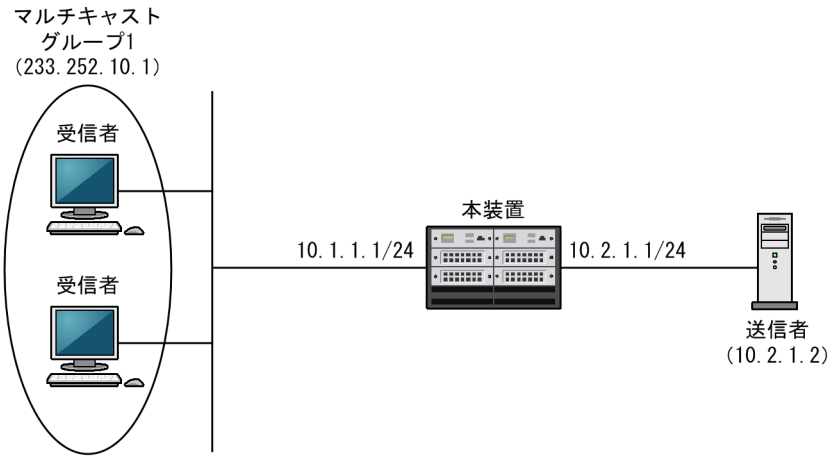
25.1.4　IPv4 PIM-SM/PIM-SSM 動作インタフェースの設定

[設定のポイント]

マルチキャストルーティング機能を動作させるインタフェースには，PIM-SM または PIM-SSM を設定する必要があります。PIM-SM および PIM-SSM はインタフェースコンフィグレーションモードで設定します。

インタフェースの IPv4 アドレスを 10.1.1.1/24 とした場合の PIM-SM および PIM-SSM 構成例を次の図に示します。

図 25-1　PIM-SM/PIM-SSM 構成例



[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   ポート 1/1 のコンフィグレーションモードに移行します。
2. **(config-if)# ip address 10.1.1.1 255.255.255.0**
   ポート 1/1 に IPv4 アドレスを設定します。
3. **(config-if)# ip pim sparse-mode**
   ポート 1/1 に PIM-SM および PIM-SSM を設定します。

25.1.5　IPv4 PIM-SM ランデブーポイント候補の設定

[設定のポイント]

本装置をランデブーポイント候補として使用する場合，ランデブーポイントアドレスとしてループバックインタフェースに IPv4 アドレスを設定します。また，管理するグループアドレスを設定します。

管理するグループアドレスを 233.252.0.0/24，本装置のループバックインタフェース（loopback 0）に設定した IPv4 アドレスを 203.0.113.10 とした場合の設定例を次に示します。

[コマンドによる設定]

1. **(config)# interface loopback 0**
   (config-if)# ip address 203.0.113.10
   (config-if)# exit
   ループバックインタフェース（loopback 0）に IPv4 アドレスを設定します。
2. **(config)# ip access-list standard MLTGROUP1**
   (config-std-nacl)# permit 233.252.0.0 0.0.0.255
   (config-std-nacl)# exit
   (config)# exit
   管理するグループアドレスのアクセスリスト（MLTGROUP1）を作成します。
3. **(config)# ip pim rp-candidate loopback 0 group-list MLTGROUP1**
   本装置をランデブーポイント候補として設定します。管理するグループアドレスにはアクセスリスト（MLTGROUP1）を指定します。

25.1.6　IPv4 PIM-SM ブートストラップルータ候補の設定

[設定のポイント]

本装置をブートストラップルータ候補として使用する場合，ループバックインタフェースに IPv4 アドレスを設定します。また，ブートストラップルータ候補として設定します。

ループバックインタフェース（loopback 0）に設定した IPv4 アドレスを 203.0.113.10 とした場合の設定例を次に示します。

[コマンドによる設定]

1. **(config)# interface loopback 0**
   (config-if)# ip address 203.0.113.10
   (config-if)# exit
   ループバックインタフェース（loopback 0）に IPv4 アドレスを設定します。
2. **(config)# ip pim bsr-candidate loopback 0**
   本装置をブートストラップルータ候補として設定します。

25.1.7　IPv4 PIM-SM 静的ランデブーポイント機能の設定

[設定のポイント]

本装置をランデブーポイントとして使用する場合，ループバックインタフェースに設定した IPv4 アドレスを静的ランデブーポイントの IPv4 アドレスとして設定してください。

静的ランデブーポイントの IPv4 アドレスを 10.10.10.1 とした場合の設定例を次に示します。

[コマンドによる設定]

1. **(config)# ip pim rp-address 10.10.10.1**
   静的ランデブーポイントの IPv4 アドレスに 10.10.10.1 を設定します。

25.1.8　IPv4 PIM-SSM の設定

(1)　IPv4 PIM-SSM で使用するアドレス範囲の設定

[設定のポイント]

PIM-SM が設定されたインタフェースでは，PIM-SSM で使用するアドレス範囲で PIM-SSM が動作します。本装置で設定できるアドレス範囲は一つだけです。

アドレス範囲をデフォルト（232.0.0.0/8）で使用する場合の設定例を次に示します。なお，デフォルト以外のアドレス範囲を指定する場合には，ip pim ssm コマンドの range パラメータで設定してください。

[コマンドによる設定]

1. **(config)# ip pim ssm default**

   PIM-SSM を有効にします。

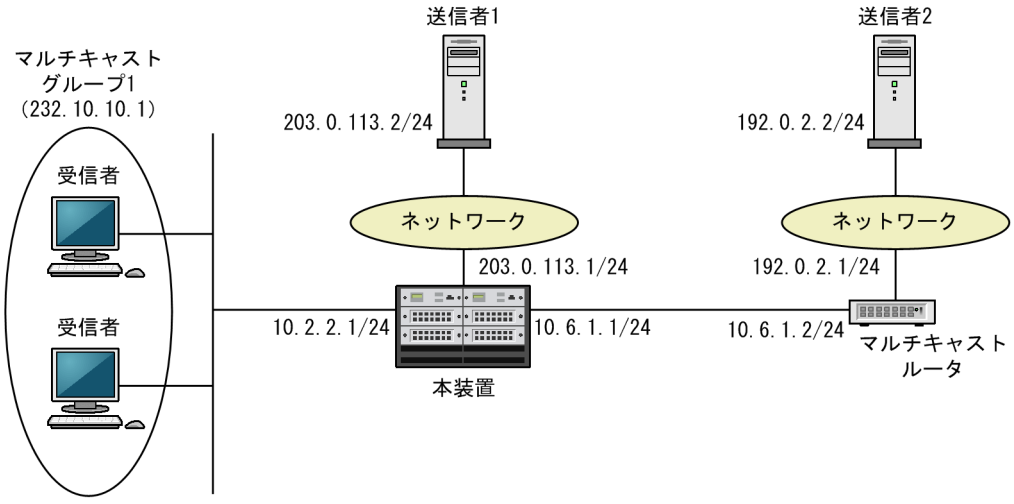
(2)　IGMP PIM-SSM 連携機能の設定

[設定のポイント]

IGMPv2/IGMPv3（EXCLUDE モード）では送信元アドレスを特定できないため，PIM-SSM と連携できません。本装置では，PIM-SSM が動作するグループアドレスと送信元アドレスを設定することで PIM-SSM と連携します。PIM-SSM が動作するグループアドレスは PIM-SSM で使用するアドレス範囲内である必要があります。

グループアドレス 232.10.10.1 を二つの送信者（送信者 1 の送信元アドレスが 203.0.113.2，送信者 2 の送信元アドレスが 192.0.2.2）が使用する場合の PIM-SSM 構成例を次の図に示します。

図 25-2　PIM-SSM 構成例



[コマンドによる設定]

1. **(config)# ip access-list standard MLTGROUP2**
   (config-std-nacl)# permit 232.10.0.0 0.0.255.255
   (config-std-nacl)# exit

   管理するグループアドレスのアクセスリスト（MLTGROUP2）を作成します。

2. **(config)# ip igmp ssm-map static MLTGROUP2 203.0.113.2**
   (config)# ip igmp ssm-map static MLTGROUP2 192.0.2.2

PIM-SSM が動作するグループアドレスと，送信者 1 および送信者 2 の送信元アドレスを設定します。管理するグループアドレスにはアクセスリスト（MLTGROUP2）を指定します。

3. **(config)# ip igmp ssm-map enable**

IGMP PIM-SSM 連携機能を有効にします。

25.1.9　IGMP の設定

[設定のポイント]

IGMP を動作させるインタフェースには，IGMP の設定が必要です。なお，インタフェースに PIM-SM または PIM-SSM（ip pim sparse-mode コマンド）を設定しても IGMP は動作します。

デフォルトでは IGMPv2 および IGMPv3 混在モードです。IGMP バージョンを変更する場合は，ip igmp version コマンドで設定してください。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**

ポート 1/1 のコンフィグレーションモードに移行します。

2. **(config-if)# ip igmp router**

該当インタフェースに IGMP を設定します。

25.1.10　VRF での IPv4 マルチキャストルーティング機能の設定

[設定のポイント]

VRF で IPv4 マルチキャストルーティング機能を動作させるには，VRF ごとに IPv4 マルチキャストルーティング機能の設定が必要です。なお，ここでの設定のほかに，グローバルネットワークまたは VRF ごとに一つ以上のインタフェースで，PIM-SM または PIM-SSM（ip pim sparse-mode コマンド）の設定が必要です。

VRF 10 での IPv4 マルチキャストルーティング機能の設定例を次に示します。

[コマンドによる設定]

1. **(config)# vrf definition 10**
   (config-vrf)# exit

VRF 10 を設定します。

2. **(config)# ip multicast-routing vrf 10**

VRF 10 で IPv4 マルチキャストルーティング機能を有効にします。

25.1.11　VRF での IPv4 PIM-SM/PIM-SSM 動作インタフェースの設定

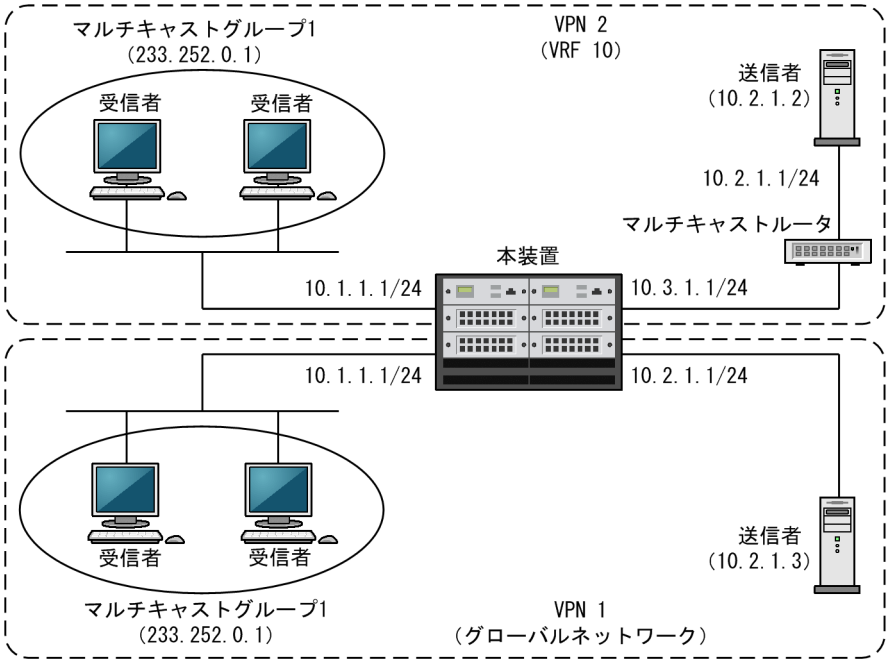
[設定のポイント]

VRF で PIM-SM を使用する場合，VRF に IPv4 マルチキャストルーティング機能を設定して，その VRF の一つ以上のインタフェースに PIM-SM または PIM-SSM を設定します。PIM-SM および PIM-SSM はインタフェースコンフィグレーションモードで設定します。

マルチキャストの送信者と受信者が本装置に直接接続するような，隣接ルータが存在しない VRF でも本設定は必要です。

VPN 2 に VRF 10 を対応させ，VRF 10 のインタフェースの IPv4 アドレスを 10.3.1.1/24 とした場合の PIM-SM および PIM-SSM 構成例を次の図に示します。

図 25-3　VRF での PIM-SM/PIM-SSM 構成例



[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/2**
   ポート 1/2 のコンフィグレーションモードに移行します。
2. **(config-if)# vrf forwarding 10**
   ポート 1/2 に VRF 10 を設定します。
3. **(config-if)# ip address 10.3.1.1 255.255.255.0**
   ポート 1/2 に IPv4 アドレスを設定します。
4. **(config-if)# ip pim sparse-mode**
   (config-if)# exit
   ポート 1/2 に PIM-SM および PIM-SSM を設定します。

25.1.12　VRF での IPv4 PIM-SM ランデブーポイント候補の設定

[設定のポイント]

VRF で本装置をランデブーポイント候補として使用する場合, ランデブーポイントアドレスとして該当 VRF のループバックインタフェースに IPv4 アドレスを設定します。また, 管理するグループアドレスを設定します。

VRF 10 で管理するグループアドレスを 233.252.0.0/24, 該当 VRF のループバックインタフェースを loopback 30, ループバックインタフェースに設定した IPv4 アドレスを 203.0.113.10 とした場合の設定例を次に示します。

[コマンドによる設定]

1. **(config)# interface loopback 30**
   (config-if)# vrf forwarding 10
   (config-if)# ip address 203.0.113.10

```
(config-if)# exit
```

VRF 10 のループバックインタフェース（loopback 30）に IPv4 アドレスを設定します。

2.
```
(config)# ip access-list standard MLTGROUP1
(config-std-nacl)# permit 233.252.0.0 0.0.0.255
(config-std-nacl)# exit
```

VRF 10 で管理するグループアドレスのアクセスリスト（MLTGROUP1）を作成します。

3.
```
(config)# ip pim vrf 10 rp-candidate loopback 30 group-list MLTGROUP1
```

本装置を VRF 10 のランデブーポイント候補として設定します。管理するグループアドレスにはアクセスリスト（MLTGROUP1）を指定します。

25.1.13　VRF での IPv4 PIM-SM ブートストラップルータ候補の設定

[設定のポイント]

VRF で本装置をブートストラップルータ候補として使用する場合，ループバックインタフェースに IPv4 アドレスを設定します。また，ブートストラップルータ候補として設定します。

本装置のループバックインタフェース（loopback 30）に設定した IPv4 アドレスを 203.0.113.10 とした場合の設定例を次に示します。

[コマンドによる設定]

1.
```
(config)# interface loopback 30
(config-if)# vrf forwarding 10
(config-if)# ip address 203.0.113.10
(config-if)# exit
```

VRF 10 のループバックインタフェース（loopback 30）に IPv4 アドレスを設定します。

2.
```
(config)# ip pim vrf 10 bsr-candidate loopback 30
```

本装置を VRF 10 のブートストラップルータ候補として設定します。

25.1.14　VRF での IPv4 PIM-SM 静的ランデブーポイント機能の設定

[設定のポイント]

本装置をランデブーポイントとして使用する場合，同じ VRF のループバックインタフェースに設定した IPv4 アドレスを静的ランデブーポイントの IPv4 アドレスとして設定してください。

VRF 10 の静的ランデブーポイントの IPv4 アドレスを 10.10.10.1 とした場合の設定例を次に示します。

[コマンドによる設定]

1.
```
(config)# ip pim vrf 10 rp-address 10.10.10.1
```

VRF 10 で静的ランデブーポイントの IPv4 アドレスに 10.10.10.1 を設定します。

25.1.15　VRF での IPv4 PIM-SSM の設定

(1)　IPv4 PIM-SSM で使用するアドレス範囲の設定

[設定のポイント]

PIM-SM が設定された該当 VRF のインタフェースでは，PIM-SSM で使用するアドレス範囲で PIM-SSM が動作します。本装置で設定できるアドレス範囲は VRF ごとに一つだけです。

VRF 10 でアドレス範囲をデフォルト（232.0.0.0/8）で使用する場合の設定例を次に示します。なお，デフォルト以外のアドレス範囲を指定する場合には，ip pim ssm コマンドの range パラメータで設定してください。

[コマンドによる設定]

1. **(config)# ip pim vrf 10 ssm default**
   VRF 10 で PIM-SSM を有効にします。

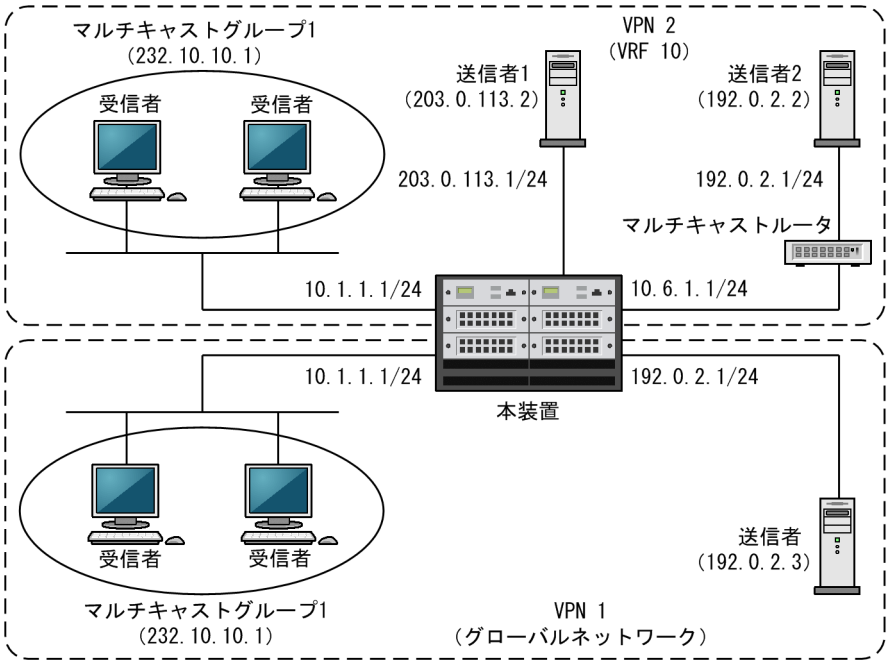
(2)　IGMP PIM-SSM 連携機能の設定

[設定のポイント]

IGMPv2/IGMPv3（EXCLUDE モード）では送信元アドレスを特定できないため，PIM-SSM と連携できません。本装置では，PIM-SSM が動作するグループアドレスと送信元アドレスを設定することで PIM-SSM と連携します。PIM-SSM が動作するグループアドレスは PIM-SSM で使用するアドレス範囲内である必要があります。なお，本機能は VRF ごとに設定します。

VPN 2 に VRF 10 を対応させ，VPN 2 で使用するグループアドレス 232.10.10.1 を同一 VPN 内で二つの送信者（送信者 1 の送信元アドレスが 203.0.113.2，送信者 2 の送信元アドレスが 192.0.2.2）が使用する場合の PIM-SSM 構成例を次の図に示します。

図 25-4　VRF での PIM-SSM 構成例



[コマンドによる設定]

1. **(config)# ip access-list standard MLTGROUP2**

```
(config-std-nacl)# permit 232.10.0.0 0.0.255.255
(config-std-nacl)# exit
```

VRF 10 で管理するグループアドレスのアクセスリスト（MLTGROUP2）を作成します。

2. `(config)# ip igmp ssm-map vrf 10 static MLTGROUP2 203.0.113.2`
   `(config)# ip igmp ssm-map vrf 10 static MLTGROUP2 192.0.2.2`
   VPN 2 で PIM-SSM が動作するグループアドレスと，送信者 1 および送信者 2 の送信元アドレスを VRF 10 に設定します。管理するグループアドレスにはアクセスリスト（MLTGROUP2）を指定します。
3. `(config)# ip igmp vrf 10 ssm-map enable`
   VRF 10 で IGMP PIM-SSM 連携機能を有効にします。

25.1.16　VRF での IGMP の設定

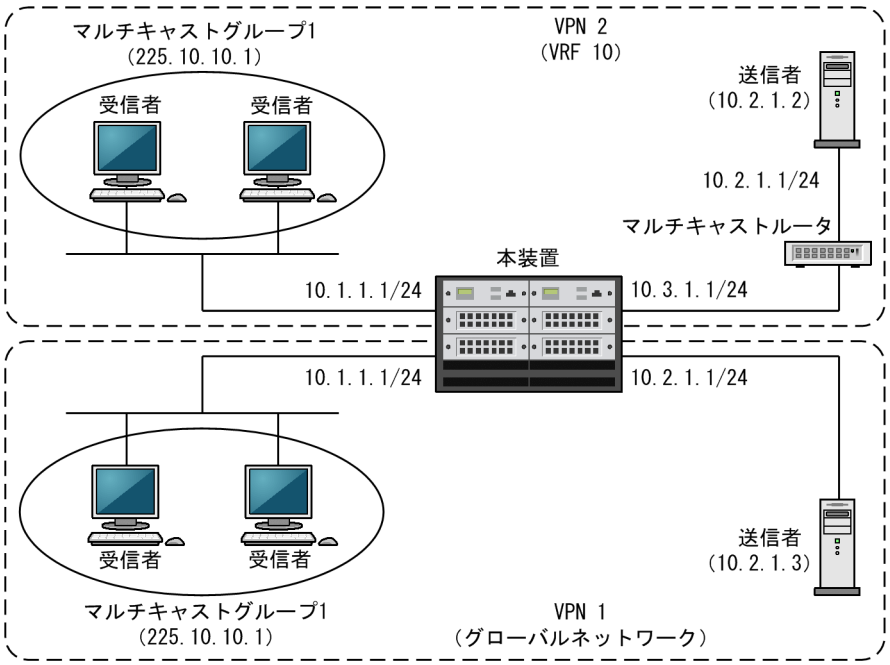
[設定のポイント]

VRF で IGMP を動作させるには，該当 VRF のインタフェースに IGMP を設定します。なお，該当 VRF のインタフェースに PIM-SM または PIM-SSM（ip pim sparse-mode コマンド）を設定しても IGMP は動作します。

デフォルトでは IGMPv2 および IGMPv3 混在モードです。IGMP バージョンを変更する場合は，ip igmp version コマンドで設定してください。

VPN 2 に VRF 10 を対応させ，VRF 10 のインタフェースの IPv4 アドレスを 10.1.1.1/24 とした場合の IGMP 構成例を次の図に示します。

図 25-5　VRF での IGMP 構成例



[コマンドによる設定]

1. `(config)# interface gigabitethernet 1/1`
   ポート 1/1 のコンフィグレーションモードに移行します。
2. `(config-if)# vrf forwarding 10`

ポート 1/1 に VRF 10 を設定します。

3. **(config-if)# ip address 10.1.1.1 255.255.255.0**

   ポート 1/1 に IPv4 アドレスを設定します。

4. **(config-if)# ip igmp router**

   (config-if)# exit

   ポート 1/1 に IGMP を設定します。

25.1.17　IPv4 マルチキャストエクストラネットの設定

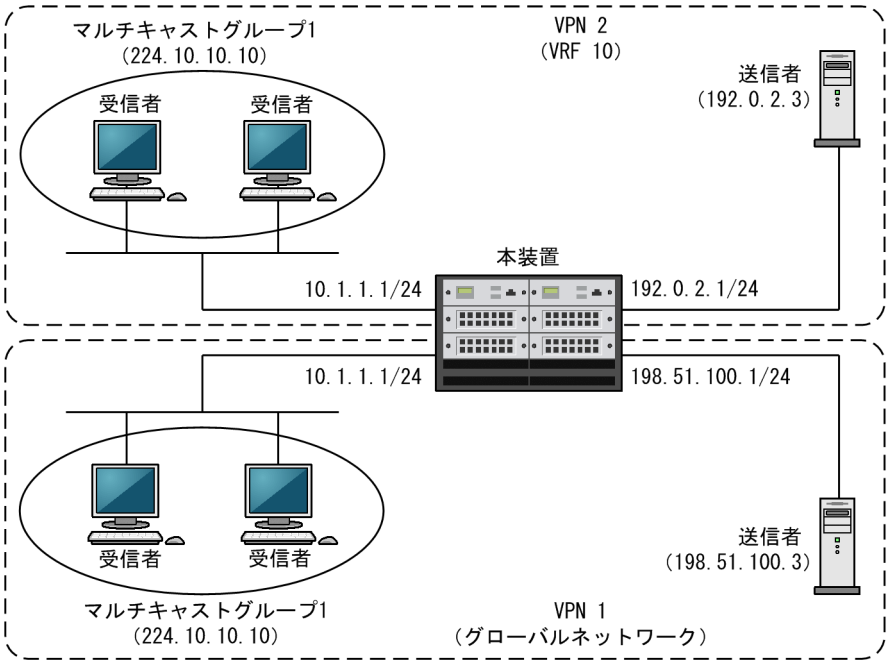
[設定のポイント]

マルチキャストエクストラネットでは，中継先 VRF に送信者へのユニキャストエクストラネットの設定があり，ユニキャスト経路が存在する必要があります。

送信者が存在する VRF にマルチキャスト経路フィルタリングを設定します。経路フィルタリングに条件を指定しない場合は，すべてのグループアドレスをマルチキャストが動作するすべての VRF へ中継できます。マルチキャスト経路フィルタリングはグローバルコンフィグレーションモードで設定します。

VPN 2 に VRF 10 を対応させ，VRF 10 のインタフェースの IPv4 アドレスを 10.1.1.1/24，198.51.100.1/24 とした場合の PIM-SSM 構成例を次の図に示します。この場合，VPN 1（グローバルネットワーク）に，VPN 2（VRF 10）上の送信者（198.51.100.3）へのユニキャスト経路が存在する必要があります。

図 25-6　VRF での PIM-SSM 構成例（エクストラネット）



[コマンドによる設定]

1. **(config)# route-map MLTEXNET permit 10**

   (config-route-map)# exit

   すべてのマルチキャスト中継要求を許可する route-map を作成します。

2. **(config)# vrf definition 10**

```
(config-vrf)# import multicast inter-vrf MLTEXNET
(config-vrf)# exit
```

VRF 10 にすべての VRF からのマルチキャスト中継要求を許可する設定をします。

25.2　オペレーション

25.2.1　運用コマンド一覧

IPv4 マルチキャストの運用コマンド一覧を次の表に示します。

表 25-2　運用コマンド一覧

コマンド名	説明
show ip mcache (show ip pim mcache)	IPv4 マルチキャスト中継エントリを表示します。
show ip mroute	IPv4 マルチキャスト経路情報を表示します。
show ip pim interface	IPv4 PIM のインタフェース情報を表示します。
show ip pim neighbor	IPv4 マルチキャストインタフェースの隣接情報を表示します。
show ip pim bsr	IPv4 PIM-SM ブートストラップルータ情報を表示します。
show ip pim rp-mapping	IPv4 PIM-SM ランデブーポイント情報を表示します。
show ip pim rp-hash	個別の IPv4 グループアドレスに対するランデブーポイント情報を表示します。
show ip igmp interface	IGMP のインタフェース情報を表示します。
show ip igmp group	IGMP のマルチキャストグループ情報を表示します。
show ip rpf	IPv4 PIM の RPF 情報を表示します。
rebalance ip mroute	マルチキャストロードバランス使用時に，回線障害などで偏ったマルチキャスト経路を分散します。
show ip multicast statistics	IPv4 マルチキャストの統計情報を表示します。
clear ip multicast statistics	IPv4 マルチキャストの統計情報をクリアします。
show ip multicast resources	IPv4 マルチキャストルーティング機能で使用している各種エントリ数を表示します。
restart ipv4-multicast	IPv4 マルチキャストルーティングプログラムを再起動します。
dump protocols ipv4-multicast	IPv4 マルチキャストルーティング機能のイベントトレース情報および制御テーブル情報のダンプを採取します。
erase protocol-dump ipv4-multicast	IPv4 マルチキャストルーティング機能のイベントトレース情報，制御テーブル情報およびコアファイルを削除します。

25.2.2　IPv4 PIM-SM 情報の確認

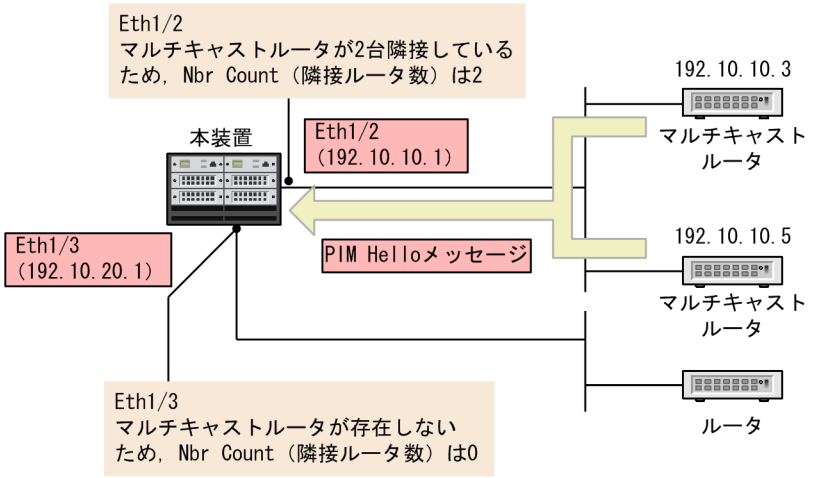
本装置の IPv4 マルチキャストルーティング機能で，PIM-SM を設定した場合の確認内容には次のものがあります。

(1)　インタフェース情報

本装置で PIM-SM および PIM-SSM のインタフェース情報を確認する場合は，show ip pim interface コマンドを実行して，PIM-SM または PIM-SSM を設定したインタフェースが表示されることを確認してください。コマンドの実行結果を次の図に示します。

図 25-7　show ip pim interface コマンドの実行結果

```
> show ip pim interface
Date 20XX/12/10 15:08:10 UTC
Total: 2 interfaces
Interface        Mode    Hello  Nbr    DR
                         Intvl  Count  Address
Eth1/2           sparse     30      2  192.10.10.5
Eth1/3           sparse     30      0  This system
>
```

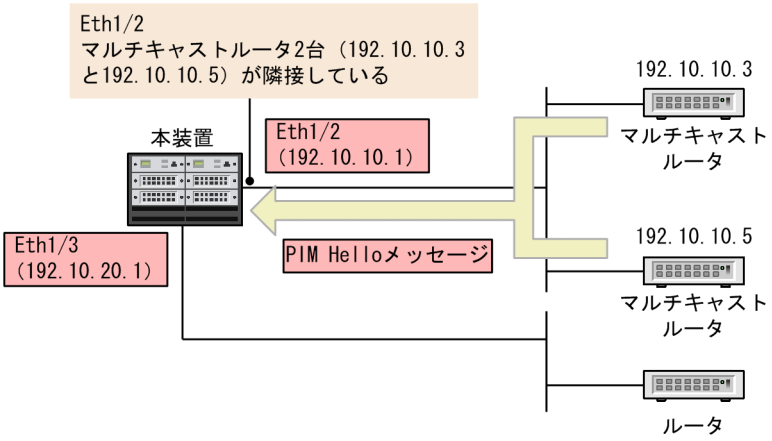


(2)　隣接情報

本装置でマルチキャストインタフェースの隣接情報を確認する場合は，show ip pim neighbor コマンドを実行して，該当インタフェースの隣接ルータを確認してください。コマンドの実行結果を次の図に示します。

図 25-8　show ip pim neighbor コマンドの実行結果

```
> show ip pim neighbor
Date 20XX/01/13 10:01:00 UTC
Total: 2 neighbors
Interface        Neighbor Address  Uptime   Expires
Eth1/2           192.10.10.3         01:10    00:35
                 192.10.10.5         01:10    01:35
>
```



(3)　マルチキャスト経路情報

本装置でマルチキャスト経路情報を確認する場合は，show ip mroute コマンドを実行して，該当するマルチキャスト経路情報が存在することを確認してください。コマンドの実行結果を次の図に示します。

図 25-9　show ip mroute コマンドの実行結果

```
> show ip mroute
Date 20XX/01/13 10:01:00 UTC
Total: 2 routes, 2 groups, 1 source
(S,G) 2 routes ------------------------------------------------------------
Group Address    Source Address   Flags  Protocol  Uptime   Expires  Assert
232.1.1.1        192.0.2.1        FLT    SSM        25:47    --:--    00:00
    incoming:Eth1/2            upstream:Direct
    outgoing:Eth1/3            uptime: 24:10   expires: --:--
             Eth1/4            uptime: 24:10   expires: --:--
             Eth1/5            uptime: 24:10   expires: --:--

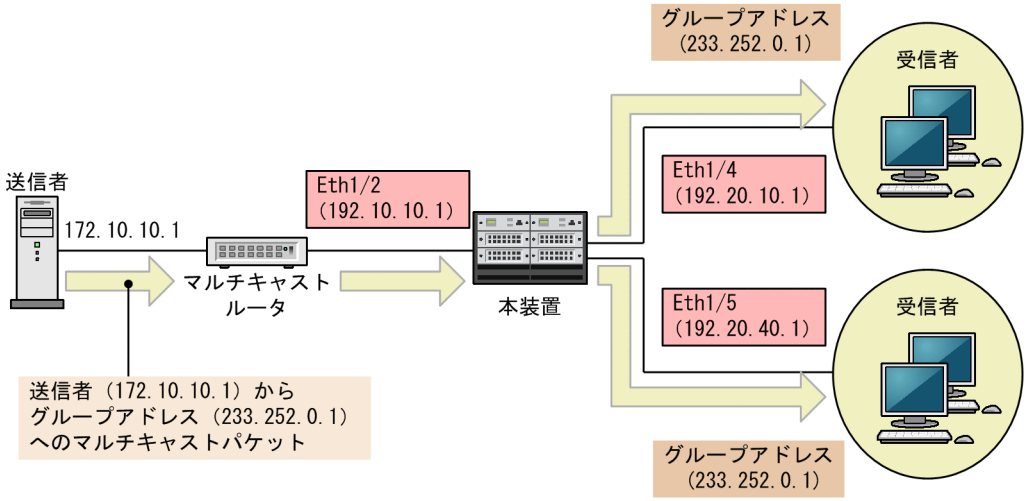
232.1.1.2        192.0.2.1        FLT    SSM        24:10    --:--    00:00
    incoming:Eth1/2            upstream:Direct
    outgoing:Eth1/4            uptime: 24:10   expires: --:--
>
```

(4)　マルチキャスト中継エントリ情報

本装置でマルチキャスト中継エントリを確認する場合は，show ip mcache コマンドを実行して，グループアドレスへの経路が存在していることを確認してください。コマンドの実行結果を次の図に示します。

図 25-10　show ip mcache コマンドの実行結果

```
> show ip mcache
Date 20XX/12/10 16:40:59 UTC
Total: 1 route
- Forwarding entry ----------------------------------------------------------
Group Address    Source Address  Flags  Protocol  Uptime   Expires
233.252.0.1      172.10.10.100   -      SSM        01:00    02:00
     incoming:Eth1/2
     outgoing:Eth1/4
              Eth1/5
>
```

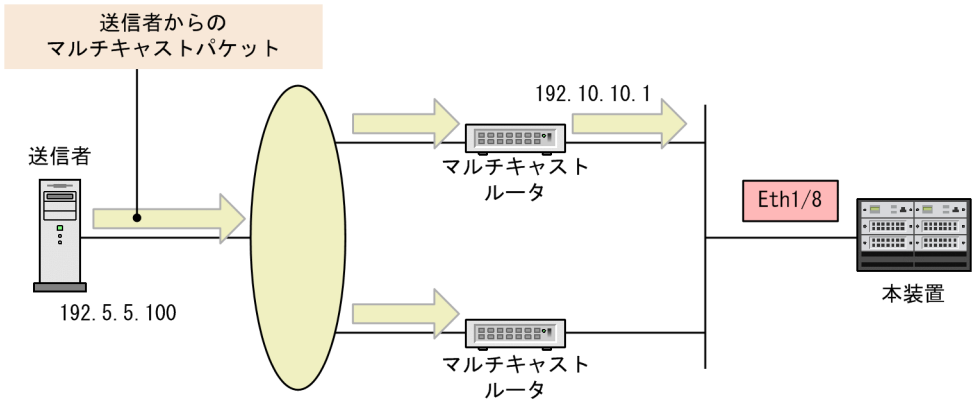


(5)　RPF 情報

本装置で PIM-SM および PIM-SSM の RPF 情報を確認する場合は，show ip rpf コマンドを実行して，RPF 情報を確認してください。コマンドの実行結果を次の図に示します。

図 25-11　show ip rpf コマンドの実行結果

```
> show ip rpf 192.5.5.100
Date 20XX/01/13 10:01:00 UTC
Incoming:Eth1/8    Upstream: 192.10.10.1
>
```



(6)　PIM-SM ブートストラップルータ情報

本装置で IPv4 PIM-SM ブートストラップルータ情報を確認する場合は，show ip pim bsr コマンドを実行して，ブートストラップルータアドレスが表示されていることを確認してください。コマンドの実行結果を次の図に示します。

図 25-12　show ip pim bsr コマンドの実行結果

```
> show ip pim bsr
Date 20XX/01/13 10:01:00 UTC
Status:Not Candidate Bootstrap Router
BSR Address : 192.10.10.10
    Priority: 100    Hash mask length: 30
    Uptime  : 03:00
    Bootstrap Timeout : 130 seconds
>
```

(7)　PIM-SM ランデブーポイント情報

本装置で IPv4 PIM-SM ランデブーポイント情報を確認する場合は，show ip pim rp-mapping コマンドを実行して，該当のグループアドレスに対するランデブーポイントアドレスが表示されていることを確認してください。コマンドの実行結果を次の図に示します。

図 25-13　show ip pim rp-mapping コマンドの実行結果

```
> show ip pim rp-mapping
Date 20XX/01/13 10:01:00 UTC
Status:Not Candidate Rendezvous Point
Total: 2 routes, 2 groups, 1 RP
Group/Masklen       C-RP Address Priority Uptime  Expires
233.250.0.2/32      192.1.1.1         100  02:00   02:30
233.250.0.1/32      192.1.1.1         100  02:00   02:30
>
```

25.2.3　IGMP 情報の確認

本装置の IPv4 マルチキャストルーティング機能で IGMP を設定した場合の確認内容には次のものがあります。

(1)　インタフェース情報

本装置で IGMP のインタフェース情報を確認する場合は，show ip igmp interface コマンドを実行して，IGMP を設定したインタフェースが表示されることを確認してください。コマンドの実行結果を次の図に示します。

図 25-14　show ip igmp interface コマンドの実行結果

```
> show ip igmp interface
Date 20XX/01/13 10:01:00 UTC
Total: 3 Interfaces
Interface     Version  Querier         Expires  Group Count  Notice
Eth1/2           2     This System        -              2
Eth1/3           3     192.20.2.1       02:30            0
Eth1/4          (3)    192.30.3.1       00:50            2   Q
>
```

(2)　グループアドレス情報

本装置で IGMP のグループアドレス情報を確認する場合は，show ip igmp group コマンドを実行して，Group Address 欄のグループアドレスを確認してください。コマンドの実行結果を次の図に示します。

図 25-15　show ip igmp group コマンドの実行結果

```
> show ip igmp group brief
Date 20XX/01/13 10:01:00 UTC
Total: 7 groups
Group Address   Interface       Version  Mode      Source Count
224.1.1.1       Eth1/1             2     EXCLUDE              0
232.1.1.2       Eth1/2             2     EXCLUDE              2
234.1.1.1       Eth1/3             2     EXCLUDE              1
234.1.1.2       Eth1/4             3     INCLUDE              1
232.1.1.1       Eth1/5             3     INCLUDE              1
232.1.1.3       Eth1/5             3     INCLUDE              2
235.1.1.1       Eth1/5             3     EXCLUDE              3
>
```

26 IPv6 マルチキャストの解説

マルチキャストは, ネットワーク内で選択されたグループに対して同一の情報を送信します。この章では，IPv6 ネットワークで実現するマルチキャストについて説明します。

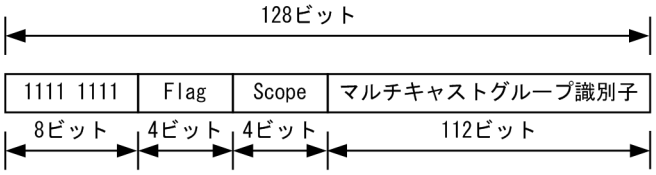
26.1　IPv6 マルチキャスト概説

IPv6 マルチキャストは IPv4 マルチキャストと同様の機能を IPv6 で実現します。IPv4 マルチキャストについては，「24.1　IPv4 マルチキャスト概説」を参照してください。IPv4 マルチキャストと IPv6 マルチキャストとは完全に独立に動作します。そのため，同一ルータ内でも IPv4 マルチキャストと IPv6 マルチキャストとはまったく独立なものとして設定できます。

26.1.1　IPv6 マルチキャストアドレス

IPv6 マルチキャスト通信では上位 8 ビットが FF（16 進数）となる IPv6 アドレスを宛先アドレスとして使用します。IPv6 マルチキャストアドレスはマルチキャストパケットの送受信に参加しているマルチキャストグループの間だけの，論理的なグループアドレスです。IPv6 マルチキャストアドレスのフォーマットを次の図に示します。

図 26–1　マルチキャストアドレスのフォーマット



26.1.2　IPv6 マルチキャストルーティング機能

本装置は受信したマルチキャストパケットをマルチキャスト中継エントリに従って中継します。マルチキャストルーティング機能は大きく分けて次の三つの機能から構成されます。

- マルチキャストグループマネージメント機能

  グループメンバシップ情報を送受信してマルチキャストグループの存在を学習する機能です。本装置では MLD（Multicast Listener Discovery）プロトコルを使用します。
- 経路制御機能

  経路情報を送受信して中継経路を決定して，マルチキャスト経路情報およびマルチキャスト中継エントリを作成する機能です。経路情報の収集には PIM-SM または PIM-SSM を使用します。
- 中継機能

  マルチキャストパケットをマルチキャスト中継エントリに従ってハードウェアおよびソフトウェアで中継する機能です。

26.1.3　IPv6 マルチキャストパケットの受信

マルチキャストルーティング機能を実現するために，本装置では次の表に示す受信要因に該当するマルチキャストパケットをソフトウェアに転送します。

表 26–1　マルチキャストパケットの受信要因

受信要因	内容
wrong-incoming-interface	ハードウェアに登録済みのマルチキャスト中継エントリと一致したマルチキャストパケットを受信インタフェースとは異なるインタフェースから受信した場合に発生する要因

受信要因	内容
cache-misshit	ハードウェアのマルチキャスト中継エントリに存在しないマルチキャストパケットを受信した場合に発生する要因
register-request	ファーストホップルータが PIM Register メッセージをランデブーポイントへ送信するためのマルチキャストパケットを受信した場合に発生する要因
register-receive	ランデブーポイントで PIM Register メッセージを受信した場合に発生する要因

本装置では，これらのマルチキャストパケットを大量に受信した場合の輻輳を抑止するために，受信要因ごとにパケット数を制限します。なお，この制限はマルチキャストパケットの中継には影響ありません。

26.2　IPv6 マルチキャストグループマネージメント機能

マルチキャストグループマネージメント機能とは, ルーター受信者間でのグループメンバシップ情報の送受信によって, ルータが直接接続したネットワーク上のマルチキャストグループメンバの存在を学習する機能です。本装置ではマルチキャストグループマネージメント機能実現のための管理プロトコルとして MLD をサポートしています。

26.2.1　MLD の概要

MLD はルーター受信者間で使用されるマルチキャストグループ管理プロトコルです。MLD を使用すると, ルータからのマルチキャストグループの参加問い合わせと受信者からのマルチキャストグループへの参加および離脱要求によって, ルータが受信者のマルチキャストグループへの参加または離脱を認識してマルチキャストパケットを中継したり遮断したりします。

MLD には MLDv1 および MLDv2 があります。

26.2.2　MLD メッセージサポート仕様

(1)　MLDv1 メッセージのサポート仕様

本装置がサポートする MLDv1 メッセージのサポート仕様を次の表に示します。

表 26-2　MLDv1 メッセージサポート仕様

タイプ		意味	サポート	
			送信	受信
Multicast Listener Query	General Query	マルチキャストグループの参加問い合わせ（全マルチキャストグループ宛て）	○	○
	Multicast-Address-Specific Query	マルチキャストグループの参加問い合わせ（特定マルチキャストグループ宛て）	○	○
Multicast Listener Report		マルチキャストグループへの参加要求	×※	○
Multicast Listener Done		マルチキャストグループからの離脱要求	×※	○

（凡例）　○：サポートする　×：サポートしない

注※

ルーティングプロトコルなどの制御用に使用しているマルチキャストグループ宛てに送信することがあります。

(2)　MLDv2 メッセージのサポート仕様

MLDv2 はフィルタモードと送信元リストを指定することで, 送信元フィルタリングを実現します。フィルタモードには次の二つのモードがあります。

INCLUDE モード

指定された送信元リストからのマルチキャストパケットだけを中継します。

EXCLUDE モード

指定された送信元リスト以外からのマルチキャストパケットだけを中継します。

本装置がサポートする MLDv2 メッセージのサポート仕様を次の表に示します。

表 26-3　MLDv2 メッセージサポート仕様

タイプ		意味	サポート	
			送信	受信
Version 2 Multicast Listener Query	General Query	マルチキャストグループの参加問い合わせ（全マルチキャストグループ宛て）	○	○
	Multicast Address Specific Query	マルチキャストグループの参加問い合わせ（特定マルチキャストグループ宛て）	○	○
	Multicast Address and Source Specific Query	マルチキャストグループの参加問い合わせ（特定の送信者およびマルチキャストグループ宛て）	○	○
Version 2 Multicast Listener Report	Current State Report	参加しているマルチキャストグループとフィルタモードの要求	×	○
	State Change Report	参加しているマルチキャストグループとフィルタモードの更新要求	×	○

（凡例）　○：サポートする　×：サポートしない

フィルタモードおよび送信元リストはマルチキャストグループ参加後に変更でき，MLDv2 Report メッセージに含まれる Multicast Address Record で指定します。本装置がサポートする Multicast Address Record タイプを次の表に示します。

表 26-4　Multicast Address Record タイプ

タイプ		意味	サポート
Current State Report	MODE_IS_INCLUDE	INCLUDE モードであることを示します	○
	MODE_IS_EXCLUDE	EXCLUDE モードであることを示します	○※
State Change Report	CHANGE_TO_INCLUDE_MODE	フィルタモードを INCLUDE モードに変更することを示します	○
	CHANGE_TO_EXCLUDE_MODE	フィルタモードを EXCLUDE モードに変更することを示します	○※
	ALLOW_NEW_SOURCES	マルチキャストパケットの受信を希望する送信者を追加することを示します	○
	BLOCK_OLD_SOURCES	マルチキャストパケットの受信を希望する送信者を削除することを示します	○

（凡例）　○：サポートする

注※　送信元リストは無視します。

26.2.3　MLD の動作

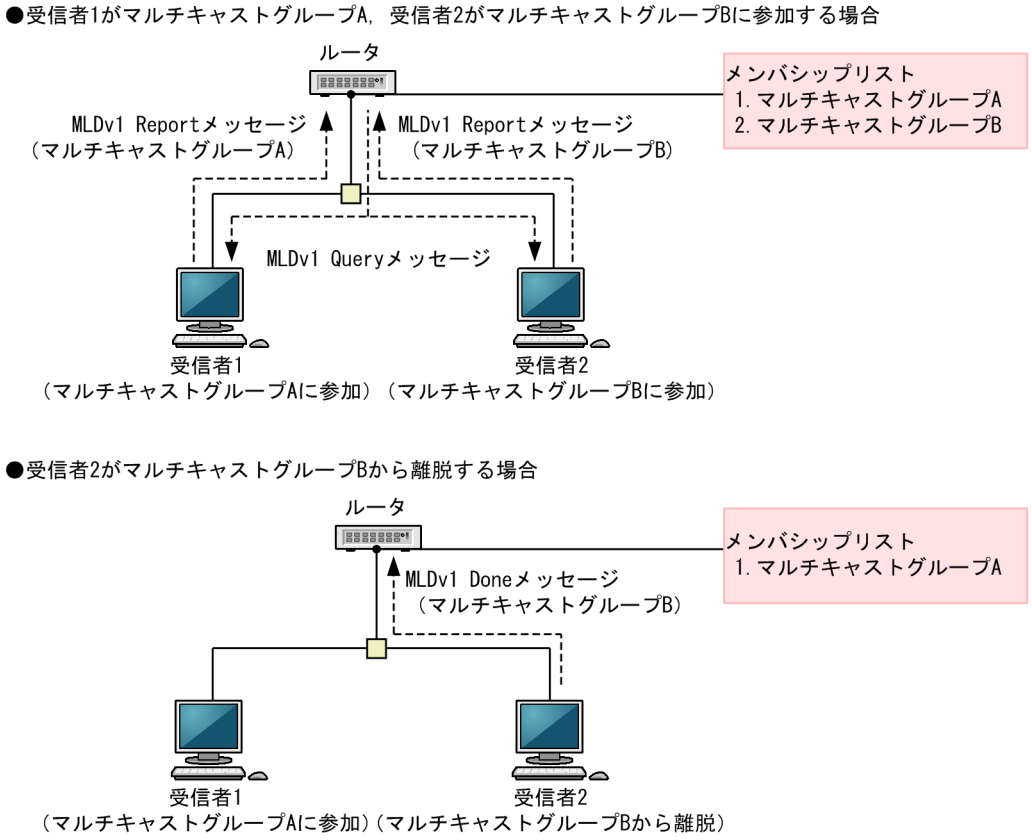
(1)　MLDv1 の動作

MLDv1 メッセージを使用した MLDv1 の動作を次に示します。

- マルチキャストルータは直接接続するインタフェース上にマルチキャストメンバシップの情報を得るため，定期的に MLDv1 Query（General Query）メッセージをリンクローカル・全ノードアドレス（ff02::1）宛てに送信します。
- 受信者は MLDv1 Query（General Query）メッセージを受信すると，MLDv1 Report メッセージを該当するマルチキャストグループ宛てに送信して，マルチキャストグループへの参加要求をします。
- マルチキャストルータは受信者から MLDv1 Report メッセージを受信すると，そのグループアドレスをメンバシップリストに追加します。
- マルチキャストルータは受信者から MLDv1 Done メッセージを受信すると，そのグループアドレスをメンバシップリストから削除します。

MLDv1 マルチキャストグループの参加および離脱動作を次の図に示します。

図 26-2　MLDv1 マルチキャストグループの参加および離脱動作



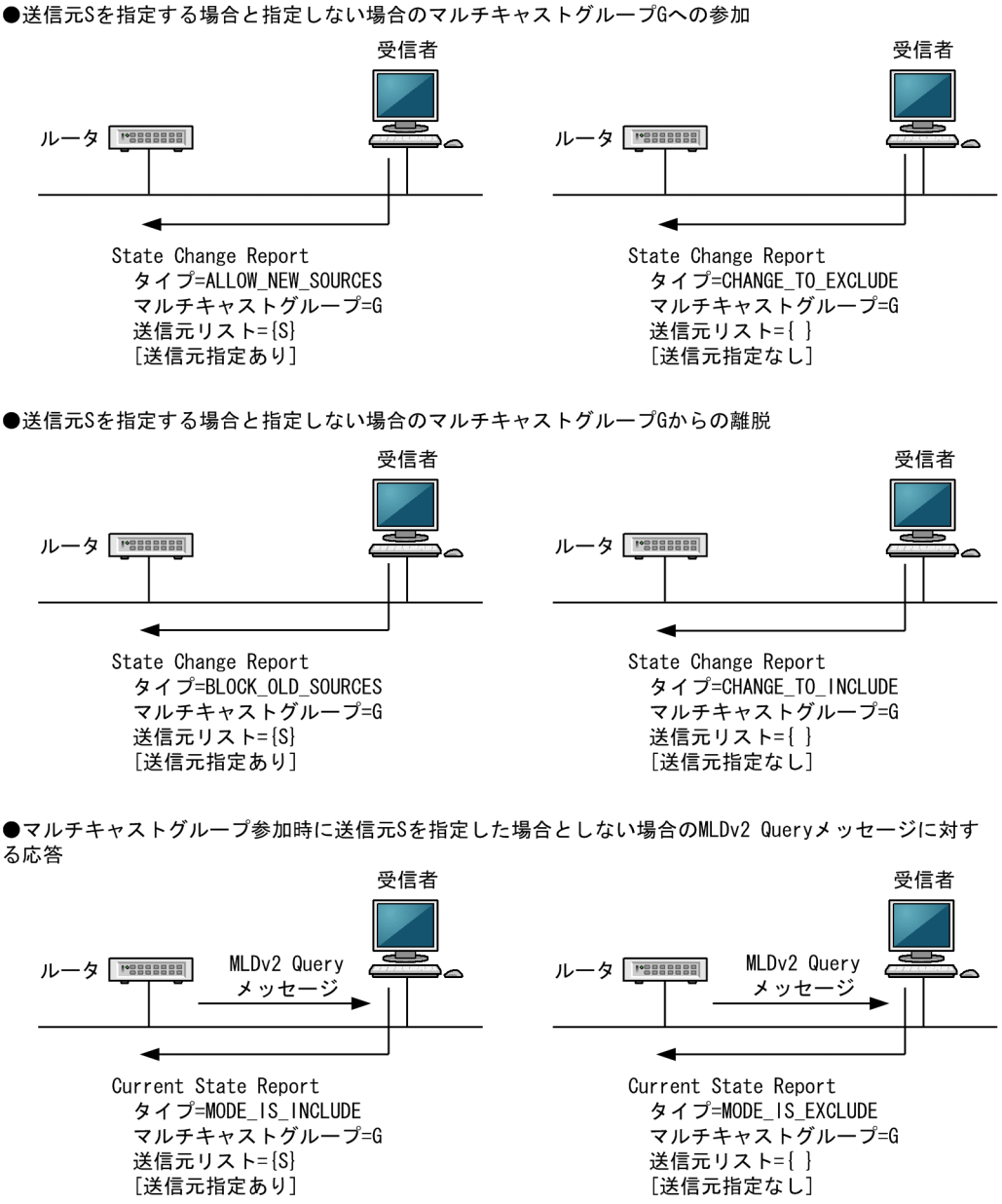
(2)　MLDv2 の動作

MLDv2 メッセージを使用した MLDv2 の動作を次に示します。

- マルチキャストルータは直接接続するインタフェース上にマルチキャストメンバシップの情報を得るため，定期的に MLDv2 Query（General Query）メッセージをリンクローカル・全ノードアドレス（ff02::1）宛てに送信します。
- 受信者は MLDv2 Query（General Query）メッセージを受信すると，MLDv2 Report（Current State Report）メッセージを ff02::16 宛てに送信して，マルチキャストグループへの参加要求をします。
- マルチキャストルータは受信者から MLDv2 Report（State Change Report）メッセージを受信すると，Multicast Address Record タイプの内容に応じてそのグループアドレスをメンバシップリストに追加，またはメンバシップリストから削除します。

MLDv2 マルチキャストグループの参加および離脱動作を次の図に示します。

図 26-3　MLDv2 マルチキャストグループの参加および離脱動作

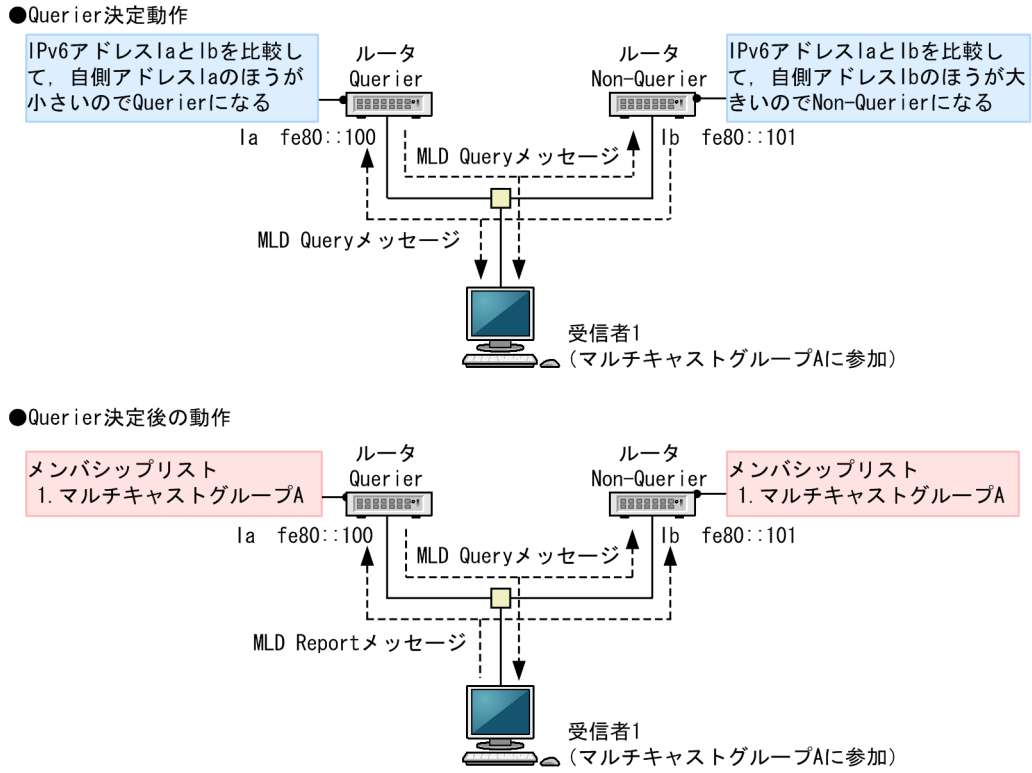


26.2.4　Querier の決定

MLD ルータは Querier か Non-Querier のどちらか一方の役割を果たします。同一ネットワーク上に複数のルータが存在する場合，そのうちの一つが定期的な MLD Query メッセージを送信する Querier になります。

Querier を決定するには，同一ネットワーク上に存在する MLD ルータから受信した MLD Query メッセージの送信元 IPv6 リンクローカルアドレスと自インタフェースの IPv6 リンクローカルアドレスを比較します。自インタフェースの方が小さければ Querier として動作します。自インタフェースの方が大きければ Non-Querier となり，MLD Query メッセージは送信しません。この動作によって同一ネットワーク上には Querier は一つだけ存在することになります。Querier と Non-Querier の決定を次の図に示します。

図 26-4　Querier と Non-Querier の決定



Querier になると，送信元 IPv6 アドレスが自インタフェースより小さい MLD Query メッセージを受信するまで Querier として動作して，MLD Query メッセージを定期的（デフォルトでは 125 秒）に送信します。

Non-Querier は MLD Query メッセージを一定時間（デフォルトでは 255 秒）受信しなかった場合，Querier として動作します。

なお，インタフェースに設定された IPv6 リンクローカルアドレス以外のアドレスは，Querier の決定には影響しません。

26.2.5　IPv6 グループメンバの管理

(1)　MLDv1 使用時の IPv6 グループメンバ管理

MLDv1 使用時のグループメンバの登録および削除について説明します。

本装置が受信者からの MLDv1 Report メッセージを受信すると，マルチキャストグループ情報を登録します。Querier，Non-Querier ともに MLDv1 Report メッセージを受信すると，マルチキャストグループ情報を登録します。

本装置がマルチキャストグループへの離脱要求である MLDv1 Done メッセージを受信した場合，該当するマルチキャストグループ情報を削除しますが，MLD 即時離脱機能およびホストトラッキング機能の有効または無効によって動作が異なります。

MLD 即時離脱機能およびホストトラッキング機能が無効のとき

本装置が Querier の場合

MLDv1 Done メッセージを受信した時, 離脱要求を受信したマルチキャストグループに参加しているほかの受信者の存在を確認するために，MLDv1 Query（Multicast-Address-Specific Query）メッセージを 1 秒間隔で 2 回送信します。そのあと，該当するマルチキャストグループ宛ての MLDv1 Report メッセージを 1 秒間受信しないときに，該当するマルチキャストグループ情報を削除します。

本装置が Non-Querier の場合

受信した MLDv1 Done メッセージを無視します。Querier が送信した MLDv1 Query（Multicast-Address-Specific Query）メッセージを 2 回受信したあと，該当するマルチキャストグループ宛ての MLDv1 Report メッセージを 1 秒間受信しないときに, 該当するマルチキャストグループ情報を削除します。

MLD 即時離脱機能が有効のとき

本装置が Querier，Non-Querier に関係なく，MLDv1 Done メッセージ受信時に該当するマルチキャストグループ情報を削除します。

ホストトラッキング機能が有効のとき

本装置が Querier，Non-Querier に関係なく，MLDv1 Done メッセージ受信時に該当するマルチキャストグループ情報を削除します。このとき，管理しているほかの受信者が存在する場合は削除しません。

なお，ホストトラッキング機能は，MLDv1 と MLDv2 混在時だけ有効です。

(2)　MLDv2 使用時の IPv6 グループメンバ管理

MLDv2 使用時のグループメンバの登録および削除について説明します。

本装置が受信者からの MLDv2 Report（参加要求）メッセージを受信すると，マルチキャストグループ情報を登録します。ここでのマルチキャストグループ情報とは，グループアドレスと，そのグループアドレスに対応する送信元アドレスを指します。Querier，Non-Querier ともに MLDv2 Report（参加要求）メッセージを受信すると，マルチキャストグループ情報を登録します。

本装置がマルチキャストグループへの離脱要求である MLDv2 Report（離脱要求）メッセージを受信した場合，該当するマルチキャストグループ情報を削除しますが，MLD 即時離脱機能およびホストトラッキング機能の有効または無効によって動作が異なります。

MLD 即時離脱機能およびホストトラッキング機能が無効のとき

本装置が Querier の場合

MLDv2 Report（離脱要求）メッセージを受信した時，該当するマルチキャストグループに参加しているほかの受信者の存在を確認するために，送信元リストの指定有無に応じて次に示す MLDv2 Query メッセージを 1 秒間隔で 2 回送信します。

- 送信元リスト指定なし：Multicast Address Specific Query メッセージ
- 送信元リスト指定あり：Multicast Address and Source Specific Query メッセージ

この MLDv2 Report（離脱要求）メッセージを受信したあと，該当するマルチキャストグループ宛ての MLDv2 Report（参加要求）メッセージを 2 秒間受信しないときに，該当するマルチキャストグループ情報を削除します。

本装置が Non-Querier の場合

MLDv2 Report（離脱要求）メッセージを受信したあと，該当するマルチキャストグループ宛ての MLDv2 Report（参加要求）メッセージを 2 秒間受信しないときに，該当するマルチキャストグループ情報を削除します。

MLD 即時離脱機能が有効のとき

本装置が Querier，Non-Querier に関係なく，MLDv2 Report（離脱要求）メッセージ受信時に該当するマルチキャストグループ情報を削除します。

ホストトラッキング機能が有効のとき

本装置が Querier，Non-Querier に関係なく，マルチキャストグループに参加している最後の受信者からの MLDv2 Report（離脱要求）メッセージ受信時に，該当するマルチキャストグループ情報を削除します。

26.2.6　MLD タイマ値

(1)　MLDv1 タイマ値

本装置が使用する MLDv1 タイマ値を次の表に示します。

表 26-5　MLDv1 タイマ値

タイマ	内容	デフォルト値（秒）	本装置の設定範囲（秒）
Query Interval※1	MLD General Query メッセージの送信周期時間	125	60～3600
Query Response Interval	MLD Report メッセージの最大応答待ち時間	10	－
Other Querier Present Interval※2	Querier 監視時間	255	Robustness Variable※3× Query Interval + Query Response Interval / 2
Startup Query Interval※2	Startup 時 MLD General Query メッセージを送信する時間	31	Query Interval / 4
Last Member Query Interval	離脱要求受信後の MLD Multicast-Address-Specific Query メッセージの送信周期	1	－

タイマ	内容	デフォルト値（秒）	本装置の設定範囲（秒）
Multicast Listener Interval※2	グループメンバの保持時間	260	Robustness Variable※3× Query Interval + Query Response Interval

（凡例）　－：該当しない

注※1　コンフィグレーションで設定できます。

注※2　計算式で算出されます（コンフィグレーションで設定できません）。

注※3　Robustness Variable は 2 固定です。

(2)　MLDv2 タイマ値

本装置が使用する MLDv2 タイマ値を次の表に示します。

表 26-6　MLDv2 タイマ値

タイマ	内容	デフォルト値（秒）	本装置の設定範囲（秒）
Query Interval※1	MLD General Query メッセージの送信周期時間	125	60～3600
Query Response Interval	MLD Report メッセージの最大応答待ち時間	10	－
Other Querier Present Interval※2	Querier 監視時間	255	Robustness Variable※3× Query Interval + Query Response Interval/2
Startup Query Interval※2	Startup 時 MLD General Query メッセージを送信する時間	31	Query Interval / 4
Last Listener Query Interval	離脱要求受信後の MLD Multicast Address Specific Query メッセージおよび MLD Multicast Address and Source Specific Query メッセージの送信周期	1	－
Multicast Address Listening Interval※2	グループメンバの保持時間	260	Robustness Variable※3× Query Interval + Query Response Interval
Older Version Host Present Interval※2	MLDv2 マルチキャストアドレス互換モードへの移行時間	260	Robustness Variable※3× Query Interval + Query Response Interval

（凡例）　－：該当しない

注※1　コンフィグレーションで設定できます。

注※2　計算式で算出されます（コンフィグレーションで設定できません）。

注※3　Robustness Variable は本装置が Querier のときは 2，Non-Querier のときは Querier の Robustness Variable に従います。

26.2.7　MLDv1/MLDv2 装置との接続

本装置は MLDv1 と MLDv2 をサポートします。コンフィグレーションコマンド ipv6 mld version で，インタフェースごとに使用する MLD バージョンを設定できます。指定するバージョンに応じた動作を次の表に示します。デフォルトは version 2 です。

表 26-7　MLD バージョン指定時の動作

指定バージョン	バージョン指定時の動作
version 1	MLDv1 で動作します。 MLDv2 メッセージは無視します。
version 2	MLDv1，MLDv2 の両方で動作できます。 MLDv1，MLDv2 それぞれグループアドレス単位で動作します。
version 2 only	MLDv2 で動作します。 MLDv1 メッセージは無視します。

(1)　MLDv1/MLDv2 ルータとの接続

冗長構成などによって同一ネットワーク上に複数の MLD ルータが存在する場合，互いの MLD Query メッセージを受信することで Querier を決定します（「26.2.4　Querier の決定」を参照してください）。本装置は，MLD バージョンが version 2 または version 2 only に設定されているインタフェースでの MLDv1 ルータとの接続をサポートしません（MLDv1 Query メッセージを無視するため，Querier を決定できなくなります）。MLDv1 ルータと接続する場合は，該当するインタフェースの MLD バージョンを version 1 に設定してください。

(2)　MLDv1/MLDv2 受信者混在時の動作

MLDv1 受信者と MLDv2 受信者が混在するネットワークと接続する場合は，該当するインタフェースの MLD バージョンをデフォルトの状態で使用してください。ただし，MLDv1 受信者が MLDv2 Query メッセージを MLDv1 Query メッセージとして受信できる（RFC 仕様）ことが必要になります。

MLDv1 受信者と MLDv2 受信者が混在する場合，グループメンバの登録はマルチキャストグループへの参加を要求する MLD のバージョンによって異なります。受信者混在時のグループメンバの登録を次の表に示します。

表 26-8　MLDv1/MLDv2 受信者混在時のグループメンバ登録

マルチキャストグループ参加要求	グループメンバの登録
MLDv1 で受信	MLDv1 モードでグループメンバを登録
MLDv2 で受信	MLDv2 モードでグループメンバを登録
MLDv1 と MLDv2 で受信	MLDv1 モードでグループメンバを登録

26.2.8　静的グループ参加機能

MLD に対応する受信者が存在しないネットワークにマルチキャストパケットを中継するために，静的グループ参加機能を設定します。

静的グループ参加機能を設定したインタフェースは，MLD Report メッセージを受信しなくてもマルチキャストグループに参加したものと同様に動作します。

本機能は MLDv1 の機能のため，該当するインタフェースの MLD バージョンを version 2 only に設定している場合は動作しません。また，version 2 に設定している場合は MLDv1 でマルチキャストグループに参加したものと同様に動作します。

通常，静的グループ参加機能を設定すると，本装置が DR のときだけ該当するマルチキャストグループのマルチキャスト中継を開始します。しかし，コンフィグレーションコマンド ipv6 mld static-group で ignore-dr パラメータを設定した場合，本装置が DR でなくてもマルチキャスト中継を開始します。なお，本装置が DR でない状態で静的グループ参加機能を設定したあと，ignore-dr パラメータを追加で設定した場合，該当するマルチキャストグループのマルチキャスト中継を最大 125 秒後に開始します。

26.2.9　MLD 使用時の注意事項

- コンフィグレーションの変更によって静的グループ参加機能を設定した場合, PIM-SM の場合は(*,G)マルチキャスト経路情報，PIM-SSM の場合は(S,G)マルチキャスト経路情報が作成されるまで最大 125 秒掛かります。
- コンフィグレーションで設定している PIM-SSM で使用するアドレス範囲外のグループアドレスに対して，送信元指定ありの MLDv2 Report メッセージ（参加要求）を受信した場合は，全送信者からのマルチキャストパケットを中継します。

26.3　IPv6 マルチキャスト中継機能

マルチキャストパケットの中継処理はマルチキャスト中継エントリに従ってハードウェアおよびソフトウェアで行います。一度中継したマルチキャストパケットの中継情報はハードウェアのマルチキャスト中継エントリに登録されます。マルチキャスト中継エントリに登録されたマルチキャストパケットはハードウェアで中継して，登録されていないマルチキャストパケットはソフトウェアのマルチキャスト経路情報から生成したマルチキャスト中継エントリに従って中継します。

26.3.1　IPv6 マルチキャスト中継対象外アドレス

マルチキャスト中継処理の対象外となる IPv6 マルチキャストアドレスを次の表に示します。

表 26–9　IPv6 マルチキャスト中継対象外アドレス

中継対象外アドレス	説明
ffx0::/16	予約マルチキャストアドレス
ffx1::/16	ノードローカル・マルチキャストアドレス
ffx2::/16	リンクローカル・マルチキャストアドレス

注　x には 0～f までの値が入ります。

IPv6 マルチキャストアドレスについては，「3.1.5　マルチキャストアドレス」を参照してください。

26.3.2　IPv6 マルチキャストパケット中継処理

マルチキャストパケットの中継にはハードウェアの中継処理およびソフトウェアの中継処理があります。

(1)　ハードウェアによるマルチキャストパケット中継処理

ハードウェアによるマルチキャストパケットの中継処理には次の機能があります。

- マルチキャスト中継エントリの検索
  マルチキャストグループ宛てのマルチキャストパケットを受信した場合，ハードウェアのマルチキャスト中継エントリから該当するマルチキャスト中継エントリを検索します。
- マルチキャストパケットを受信したインタフェースの正常性チェック
  マルチキャスト中継エントリの検索でマルチキャスト中継エントリが存在した場合，そのマルチキャストパケットが正しいインタフェースから受信されているかどうかをチェックします。
- マルチキャストパケットのフィルタリング
  コンフィグレーションで設定されたフィルタエントリを参照して中継可否を判断します。
- ホップリミット値に基づいた中継判断と減算
  マルチキャストパケット中のホップリミット値を減算して，ホップリミット値が 0 より大きい場合は中継します。

(2)　ソフトウェアによるマルチキャストパケット中継処理

ソフトウェアによるマルチキャストパケット中継処理は次に示す場合ごとに処理が異なります。

- ハードウェアのマルチキャスト中継エントリに登録されていない場合

最初に受信したマルチキャストパケットをソフトウェアで処理することで，マルチキャスト経路情報からマルチキャスト中継エントリを生成します。生成したマルチキャスト中継エントリをハードウェアに登録するとともに，ソフトウェア処理で使用したマルチキャストパケットを中継します。

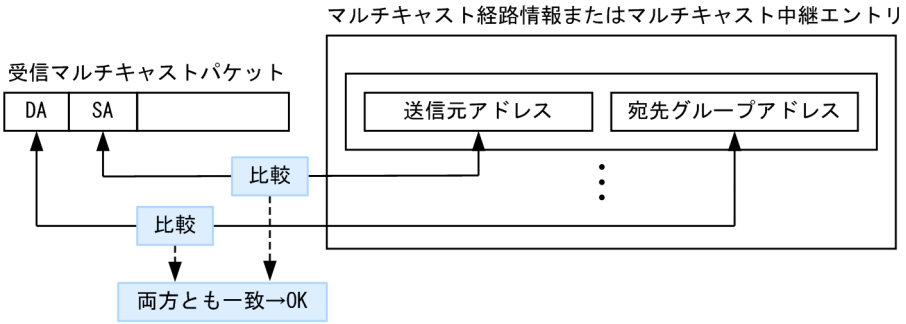
- IP カプセル化処理をする場合

  PIM-SM で一時的にランデブーポイント宛てに IP カプセル化して中継します。ランデブーポイントでは各中継先に IP デカプセル化して中継します。

(3)　マルチキャスト経路情報またはマルチキャスト中継エントリの検索

受信したマルチキャストパケットの DA（宛先グループアドレス）と SA（送信元アドレス）に該当するエントリをマルチキャスト経路情報またはマルチキャスト中継エントリから検索します。マルチキャスト経路情報またはマルチキャスト中継エントリの検索方法を次の図に示します。

図 26-5　マルチキャスト経路情報またはマルチキャスト中継エントリの検索方法



(4)　ネガティブキャッシュエントリ

ネガティブキャッシュエントリは，中継できないマルチキャストパケットをハードウェアによって廃棄する機能です。

ネガティブキャッシュエントリは中継先インタフェースの存在しないマルチキャスト中継エントリです。ネガティブキャッシュエントリは，中継できないマルチキャストパケットを受信するとハードウェアに登録します。その後，登録したマルチキャストパケットと同じアドレスのマルチキャストパケットを受信すると，そのマルチキャストパケットをハードウェアによって廃棄します。これによって，大量の中継できないマルチキャストパケットを受信しても，それを原因とする負荷上昇を抑えられます。

(5)　VRF 機能

複数の VRF でマルチキャストを動作させた場合，マルチキャスト中継エントリは VRF ごとに独立して設定できます。異なる VRF では，同じ IPv6 アドレスのマルチキャスト中継エントリを作成できます。また，マルチキャストエクストラネットによって，異なる VRF 間でマルチキャスト通信ができます。

26.4　IPv6 経路制御機能

経路制御機能とは, マルチキャストルーティングプロトコルを使用して収集した隣接情報やマルチキャストグループ情報を基に，マルチキャスト経路情報およびマルチキャスト中継エントリを作成する機能です。

26.4.1　IPv6 マルチキャストルーティングプロトコル概説

マルチキャストルーティングプロトコルは経路制御用のプロトコルです。本装置は次に示すマルチキャストルーティングプロトコルをサポートしています。

- PIM-SM（Protocol Independent Multicast-Sparse Mode）
  ユニキャストの経路機構を利用して，マルチキャストの経路制御を行うプロトコルです。ランデブーポイントへのマルチキャストパケット送信後，最短パスで通信します。
- PIM-SSM（Protocol Independent Multicast-Source Specific Multicast）
  PIM-SSM は PIM-SM の拡張機能です。ランデブーポイントを使用しないで最短パスで通信します。PIM-SM と PIM-SSM は同時に動作できます。ただし, PIM-SM と PIM-SSM で同一のマルチキャストグループを使用できません。

同一ネットワーク内でマルチキャストパケットを中継する場合は, すべてのルータで PIM-SM または PIM-SSM が動作するように設定してください。各プロトコルの適応形態については,「26.5.3　適応ネットワーク構成例」も参照してください。

26.4.2　IPv6 PIM-SM

PIM-SM はルータ間で使用されるマルチキャストルーティングプロトコルです。隣接情報やマルチキャスト配送ツリーへの参加および刈り込み要求などをやり取りすることによって，受信したマルチキャストパケットの中継および廃棄処理を実施します。PIM-SM は最初にランデブーポイント経由でマルチキャストパケットを中継します。そのあと, 既存のユニキャストルーティングを利用してマルチキャスト送信者への最短パスに切り替えて，マルチキャストパケットを中継します。

(1)　PIM-SM メッセージサポート仕様

PIM-SM メッセージのサポート仕様を次の表に示します。

表 26–10　PIM-SM メッセージのサポート仕様

メッセージタイプ	機能
PIM Hello	隣接するマルチキャストルータを検出する。
PIM Join/Prune	マルチキャスト配送ツリーの参加および刈り込みをする。
PIM Assert	Forwarder を決定する。
PIM Register	マルチキャストパケットをランデブーポイント宛てに IP カプセル化する。
PIM Register-Stop	PIM Register メッセージを抑止する。
PIM Bootstrap	ブートストラップルータを決定する。また，ランデブーポイントの情報を送信する。
PIM Candidate-RP-Advertisement	ランデブーポイントがブートストラップルータに自ランデブーポイント情報を通知する。

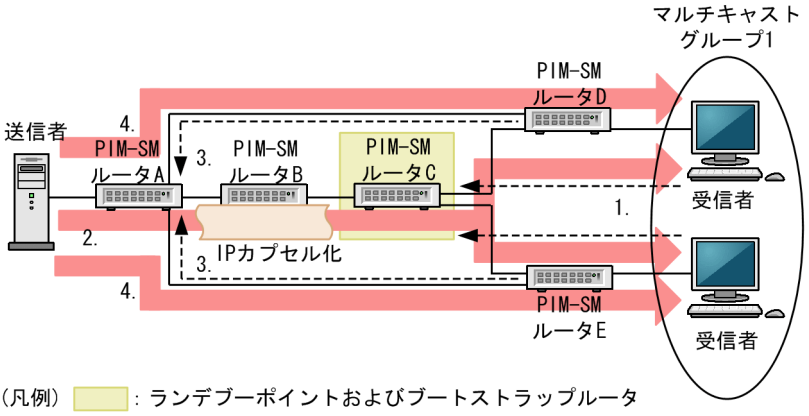
(2)　動作

PIM-SM の動作の流れを次に示します。

1. 各 PIM-SM ルータは MLD で学習したマルチキャストグループ情報をランデブーポイントに通知します。
2. ランデブーポイントは各 PIM-SM ルータからマルチキャストグループ情報を受信すると，各マルチキャストグループの存在を認識します。
3. PIM-SM は最初にマルチキャストパケットを送信元ネットワークからランデブーポイント経由ですべてのグループメンバに配送するために，送信者を頂点としたランデブーポイント経由配送ツリーを形成します。
4. 送信者から各マルチキャストグループに対して最短パスで到達できるように，既存のユニキャストルーティングを使用して送信者からの最短パス配送ツリーを形成します。
5. 送信者から各グループメンバへ最短パスでマルチキャストパケットを中継します。

PIM-SM の動作概要を次の図に示します。

図 26-6　PIM-SM の動作概要



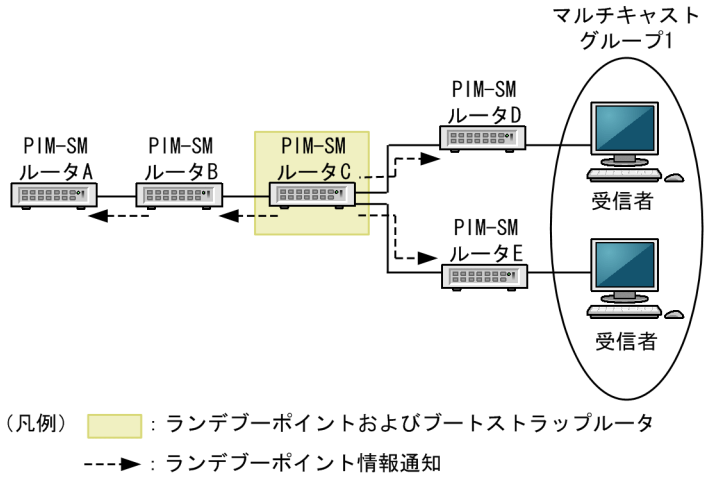
1. マルチキャストグループ参加，およびマルチキャストグループ情報の通知
2. ランデブーポイント経由でマルチキャストパケットの送信
3. 最短パスの決定
4. 最短パスでのマルチキャストパケットの送信

(a)　ランデブーポイントおよびブートストラップルータ

ランデブーポイントルータおよびブートストラップルータはコンフィグレーションで設定します。IPv4 の PIM-SM と IPv6 の PIM-SM とで，ランデブーポイントおよびブートストラップルータを設定するルータを別にすることもできます。

ブートストラップルータはランデブーポイントの情報（IPv6 アドレスなど）をすべてのマルチキャストインタフェースに通知します。このとき，ホップバイホップで全マルチキャストルータリンクローカル・グループアドレス（ff02::d）宛てに通知されます。ランデブーポイントおよびブートストラップルータの役割を次の図に示します。

図 26-7　ランデブーポイントおよびブートストラップルータの役割



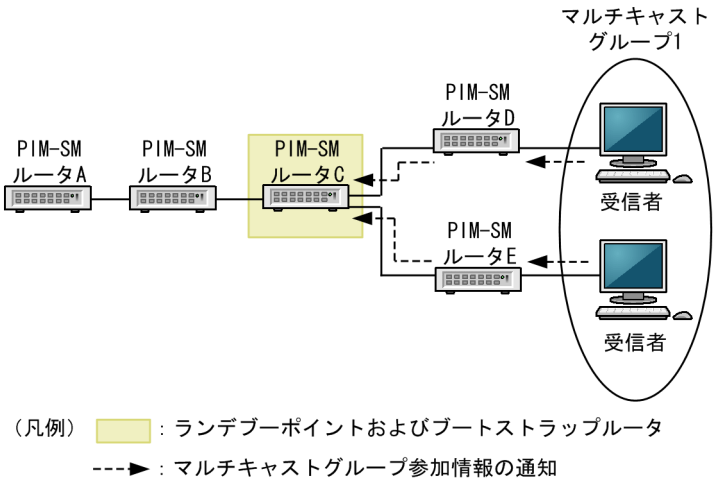
ブートストラップルータ（PIM-SM ルータ C）はランデブーポイント情報をすべてのマルチキャストインタフェースに通知します。ランデブーポイント情報を受信したルータはランデブーポイントの IPv6 アドレスを学習して，受信したインタフェース以外でマルチキャストルータが存在するすべてのインタフェースにランデブーポイント情報を通知します。

ブートストラップルータおよびランデブーポイントのアドレスは，ブートストラップルータおよびランデブーポイントで設定したループバックインタフェースのアドレスとなります。ブートストラップルータ候補とランデブーポイント候補には，同じ IPv6 アドレスを指定してください。異なる IPv6 アドレスを指定した場合，ブートストラップルータ候補の設定が無効になります。

(b)　ランデブーポイントへのマルチキャストグループ参加情報の通知

各ルータは MLD で学習したマルチキャストグループ参加情報をランデブーポイントに通知します。この通知のときに使用される送信元および宛先 IPv6 アドレスは，それぞれ該当するルータのアドレス（コンフィグレーションコマンド no system-source-address を設定していないループバックインタフェースに設定したアドレス）になります。ランデブーポイントはマルチキャストグループ情報を受信すると，マルチキャストグループの存在をインタフェースごとに認識します。ランデブーポイントへのマルチキャストグループ参加情報の通知を次の図に示します。

図 26-8　ランデブーポイントへのマルチキャストグループ参加情報の通知



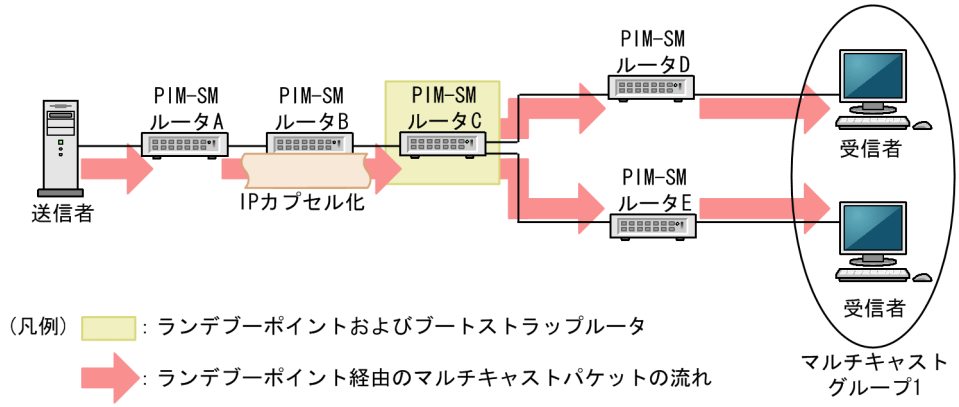
各受信者は MLD でマルチキャストグループ 1 に参加します。PIM-SM ルータ D および PIM-SM ルータ E はマルチキャストグループ 1 情報を学習して，ランデブーポイント（PIM-SM ルータ C）にマルチキャストグループ 1 情報を通知します。ランデブーポイント（PIM-SM ルータ C）はマルチキャストグループ 1 情報を受信すると，受信したインタフェースにマルチキャストグループ 1 が存在することを学習します。

(c)　ランデブーポイント経由のマルチキャストパケット通信（IP カプセル化）

送信者 S1 がマルチキャストグループ 1 宛てのマルチキャストパケットを送信した場合，PIM-SM ルータ A はそのマルチキャストパケットをランデブーポイント（PIM-SM ルータ C）宛てに IP カプセル化（PIM Register メッセージ）して送信します。

ランデブーポイント（PIM-SM ルータ C）は IP カプセル化したマルチキャストパケットを受信すると，IP デカプセル化してマルチキャストグループ 1 が存在するインタフェースにマルチキャストグループ 1 宛てのマルチキャストパケットを中継します（マルチキャストグループ 1 の存在は「(b)　ランデブーポイントへのマルチキャストグループ参加情報の通知」で学習済み）。PIM-SM ルータ D および PIM-SM ルータ E は，マルチキャストグループ 1 宛てのマルチキャストパケットを受信すると，マルチキャストグループ 1 が存在するインタフェースにマルチキャストパケットを中継します（マルチキャストグループ 1 の存在は「(b)　ランデブーポイントへのマルチキャストグループ参加情報の通知」の MLD で学習済み）。ランデブーポイント経由のマルチキャストパケット通信（IP カプセル化）を次の図に示します。

図 26-9　ランデブーポイント経由のマルチキャストパケット通信（IP カプセル化）



なお，この通知に使用される送信元 IPv6 アドレスは，次に示す順で選択されます。

1. ランデブーポイント候補として指定したループバックインタフェースの IPv6 アドレス
2. ブートストラップルータ候補として指定したループバックインタフェースの IPv6 アドレス
3. コンフィグレーションコマンド no system-source-address が設定されていないループバックインタフェースに設定した IPv6 アドレス
4. コンフィグレーションコマンド no system-source-address が設定されている，最小のループバックインタフェース ID を持つループバックインタフェースに設定した IPv6 アドレス

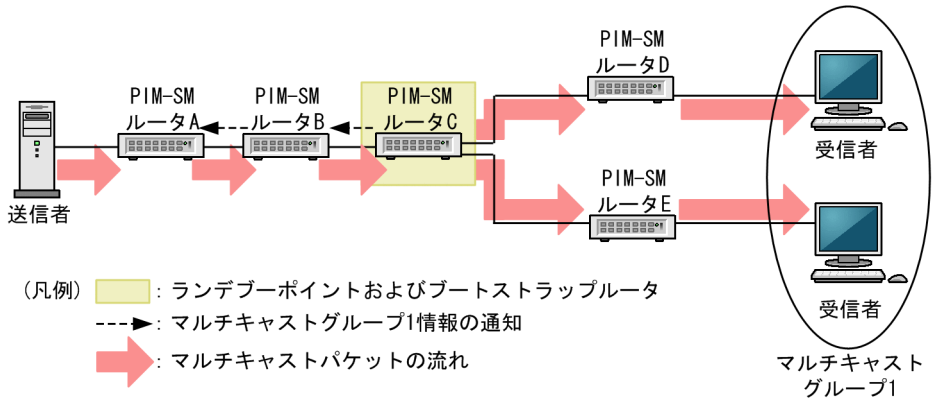
(d)　ランデブーポイント経由のマルチキャストパケット通信（IP デカプセル化）

ランデブーポイント（PIM-SM ルータ C）は IP カプセル化したマルチキャストパケットを受信すると，IP デカプセル化してマルチキャストグループ 1 が存在するインタフェースにマルチキャストグループ 1 宛てのマルチキャストパケットを中継します（「(c)　ランデブーポイント経由のマルチキャストパケット通信（IP カプセル化）」で説明）。

ランデブーポイントはこの処理のあと，既存のユニキャストルーティング情報を基に決定された送信者への最短パス方向にマルチキャストグループ 1 情報を通知します。この通知のときに使用される宛先アドレスは全マルチキャストルータリンクローカル・グループアドレス（ff02::d）です。

マルチキャストグループ 1 情報を受信した PIM-SM ルータ B および PIM-SM ルータ A は受信したインタフェースのマルチキャストグループ 1 の存在を認識（学習）します。PIM-SM ルータ A は送信者が送信したマルチキャストグループ 1 宛てのマルチキャストパケットを IP カプセル化しないで該当するインタフェースに中継します。マルチキャストグループ 1 宛てのマルチキャストパケットを受信した PIM-SM ルータ B，PIM-SM ルータ C，PIM-SM ルータ D および PIM-SM ルータ E はマルチキャストグループ 1 が存在するインタフェースに中継します。ランデブーポイント経由のマルチキャストパケット通信（IP デカプセル化）を次の図に示します。

図 26-10　ランデブーポイント経由のマルチキャストパケット通信（IP デカプセル化）

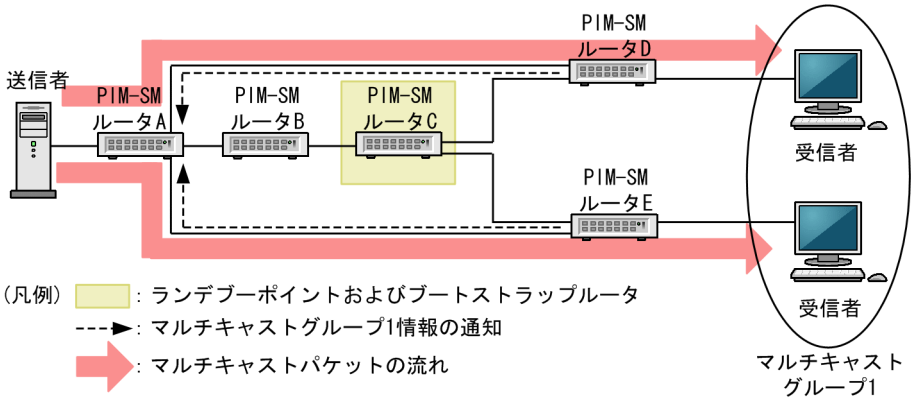


(e)　最短パスのマルチキャストパケット通信

PIM-SM ルータ D および PIM-SM ルータ E が送信者からのマルチキャストグループ 1 宛てマルチキャストパケットを受信した場合（「(d)　ランデブーポイント経由のマルチキャストパケット通信（IP デカプセル化）」で説明），PIM-SM ルータ D および PIM-SM ルータ E は送信者に対して最短パス（既存のユニキャストルーティング情報）の方向にマルチキャストグループ 1 情報を通知します。この通知のときに使用される宛先アドレスは全マルチキャストルータリンクローカル・グループアドレス（ff02::d）です。

PIM-SM ルータ A は，PIM-SM ルータ D および PIM-SM ルータ E からマルチキャストグループ 1 情報を受信すると，受信したインタフェースにマルチキャストグループ 1 の存在を認識し，送信者のマルチキャストグループ 1 宛てのマルチキャストパケットを受信すると該当するインタフェースに中継します。最短パスのマルチキャストパケット通信を次の図に示します。

図 26-11　最短パスのマルチキャストパケット通信

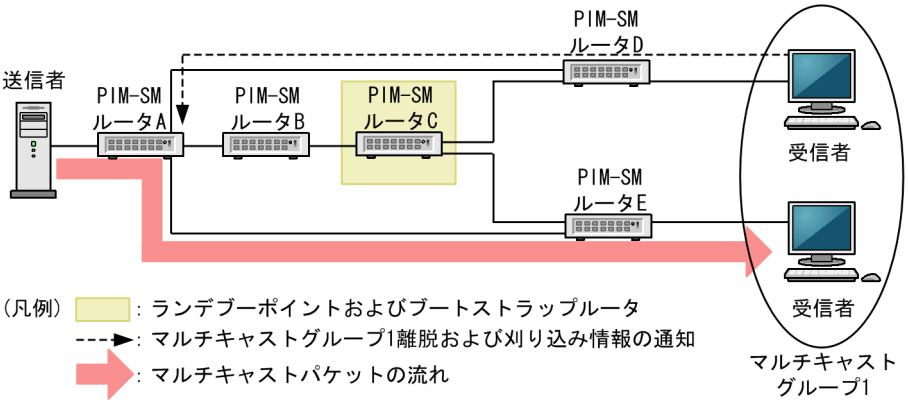


(f)　マルチキャスト配送ツリーの刈り込み

PIM-SM ルータ D は，受信者が MLD でマルチキャストグループ 1 から離脱した場合，マルチキャストグループ 1 情報を通知していたインタフェースに対してマルチキャストグループ 1 の刈り込み情報を通知します。この通知のときに使用される宛先アドレスは全マルチキャストルータリンクローカル・グループアドレス（ff02::d）です。

PIM-SM ルータ A はマルチキャストグループ 1 の刈り込み通知を受信すると，受信したインタフェースに対してマルチキャストグループ 1 宛てのマルチキャストパケットの中継を中止します。マルチキャスト配送ツリーの刈り込みを次の図に示します。

図 26-12　マルチキャスト配送ツリーの刈り込み



(3)　近隣検出

PIM-SM ルータは PIM-SM および PIM-SSM を有効にしたすべてのインタフェースに定期的に PIM Hello メッセージを送信します。PIM Hello メッセージは全マルチキャストルータリンクローカル・グループアドレス宛て（ff02::d）に送信します。このメッセージを受信することで，近隣のマルチキャストルータを動的に検出します。本装置は PIM Hello メッセージの Generation ID オプションをサポートしています。

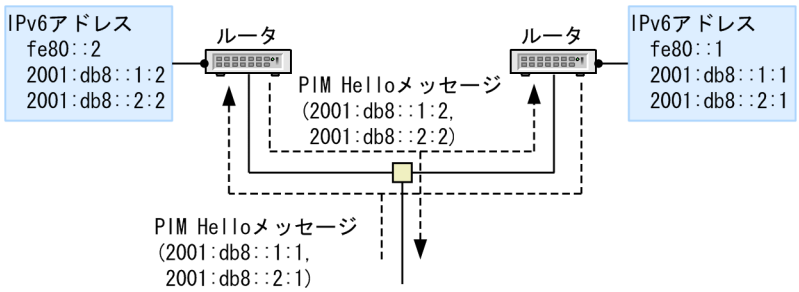
Generation ID はマルチキャストインタフェースごとに持つ 32 ビットの乱数で，PIM Hello メッセージ送信時に Generation ID を付加して送信します。Generation ID はマルチキャストインタフェースが Up 状態になるたびに再生成します。受信した PIM Hello メッセージに Generation ID オプションが付加されていれば Generation ID を記憶し，Generation ID の変化によって近隣装置のインタフェース障害を検出します。Generation ID の変化を検出すると，近隣装置情報の更新と PIM Hello メッセージ，PIM

Bootstrap メッセージ，および PIM Join/Prune メッセージを定期広告のタイミングを待たないで送信します。これによって，マルチキャスト経路情報を速やかに再学習できます。

本装置から送信される PIM Hello メッセージには，送信元インタフェースに設定されているリンクローカルアドレス以外のアドレスリストが PIM Hello メッセージのオプションデータ（タイプ 24）として含まれています。このオプションデータを受信すると，本装置は隣接するマルチキャストルータのリンクローカルアドレス以外のアドレスを認識できます。

本装置からマルチキャスト送信者へ到達するためのネクストホップがリンクローカルアドレス以外の場合にも，このアドレスリストを参照することで本装置は送信者へ到達するためのマルチキャストルータを検出できます。隣接するマルチキャストルータのアドレス受信例を次の図に示します。

図 26-13　PIM Hello メッセージによる隣接マルチキャストルータのアドレス受信



(4)　Forwarder の決定

同一 LAN 上に複数の PIM-SM ルータを接続している場合，そのネットワークにマルチキャストパケットが重複して中継される可能性があります。

同一 LAN 上に複数の PIM-SM ルータが存在し，二つ以上のルータがその LAN にマルチキャストパケットを中継する場合，PIM-SM ルータは PIM Assert メッセージを使用してそのマルチキャスト経路のプリファレンスとメトリックを比較して，送信元ネットワークに対して最適な一つのルータを Forwarder として選択します。

Forwarder となった一つのルータだけが，その LAN でのマルチキャストパケットを中継することで，マルチキャストパケット中継の重複を抑止します。

PIM Assert メッセージによって Forwarder を決定する流れを次に示します。

1. プリファレンスを比較して，プリファレンス値が小さいルータが Forwarder になります。
2. プリファレンス値が等しい場合，メトリックを比較して，メトリック値が小さいルータが Forwarder になります。
3. メトリック値が等しい場合，各ルータの IPv6 アドレスを比較して，IPv6 アドレスが大きいルータが Forwarder になります。

本装置はマルチキャスト経路のプリファレンス値に 101，メトリック値に 1024 を設定して，PIM Assert メッセージを送信します。送信者が本装置と直接接続する場合は，プリファレンス値およびメトリック値に 0 を設定して送信します。また，コンフィグレーションコマンド ipv6 pim assert-preference および ipv6 pim assert-metric を設定することで，任意の値またはユニキャストルーティングプロトコルから該当するマルチキャスト経路の送信元アドレスへのディスタンス値とメトリック値を取得して，PIM Assert メッセージのプリファレンス値とメトリック値として送信することもできます。

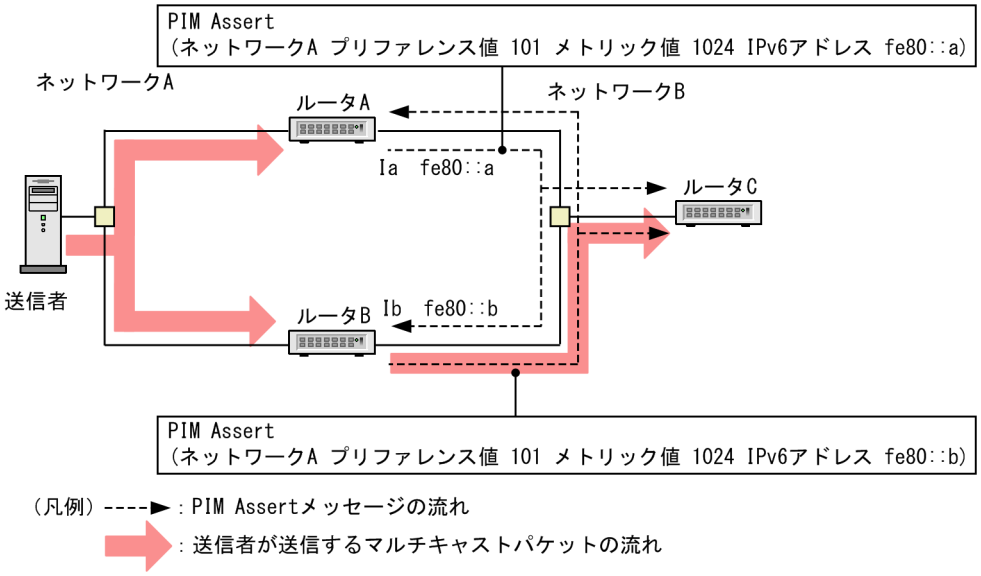
ユニキャストルーティングプロトコルが OSPFv3 の場合，OSPFv3 の経路の学習元によって取得するメトリック値が異なります。OSPFv3 の経路の学習元ごとに取得するメトリック値を次の表に示します。

表 26-11　OSPFv3 の経路の学習元ごとに取得するメトリック値

経路の学習元	取得するメトリック値	備考
AS 外経路（TYPE1）	メトリック値＋ Cost 値	第 1 メトリック値
AS 外経路（TYPE2）	メトリック値	
エリア内経路，エリア間経路	Cost 値	

Forwarder の決定を次の図に示します。

図 26-14　Forwarder の決定



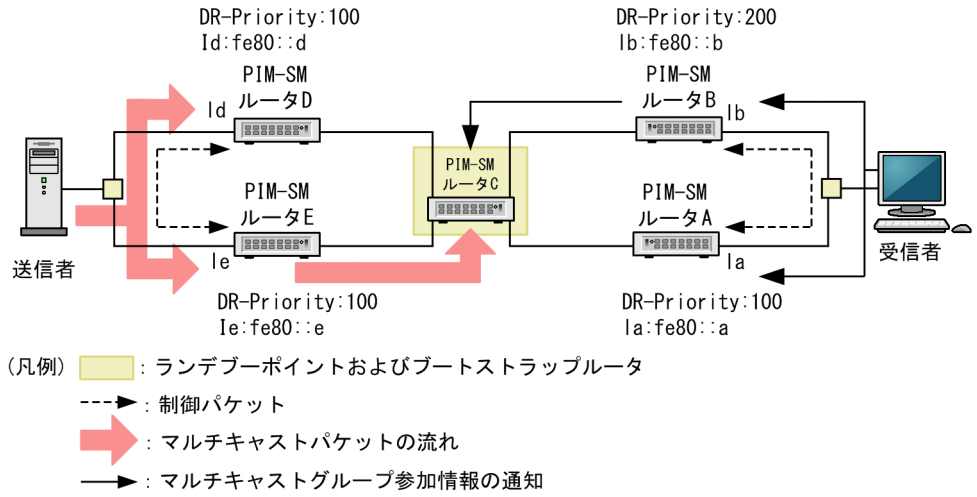
PIM-SM ルータ A の IPv6 アドレス Ia と PIM-SM ルータ B の IPv6 アドレス Ib を比較します。その結果，値の大きい PIM-SM ルータ B が Forwarder になります。

(5)　DR の決定および動作

同一 LAN 上で複数の PIM-SM ルータが存在する場合，PIM-SM ルータ間の制御パケット通信によって中継代表ルータ（DR：Designated Router）を決定します。このとき，同一 LAN 上でいちばん大きい DR-Priority の PIM-SM ルータが DR となります。DR-Priority が等しい場合は，いちばん大きい IPv6 リンクローカルアドレスの PIM-SM ルータが DR となります。また，同一 LAN 上に DR-Priority オプション未サポートの装置が 1 台でも存在する場合は，いちばん大きい IPv6 リンクローカルアドレスの PIM-SM ルータが DR となります。

受信者からのマルチキャストグループ参加情報は DR がランデブーポイント宛てに通知します。送信者が送信したマルチキャストパケットは DR が IP カプセル化してランデブーポイントに送信します。DR の動作を次の図に示します。

図 26-15　DR の動作

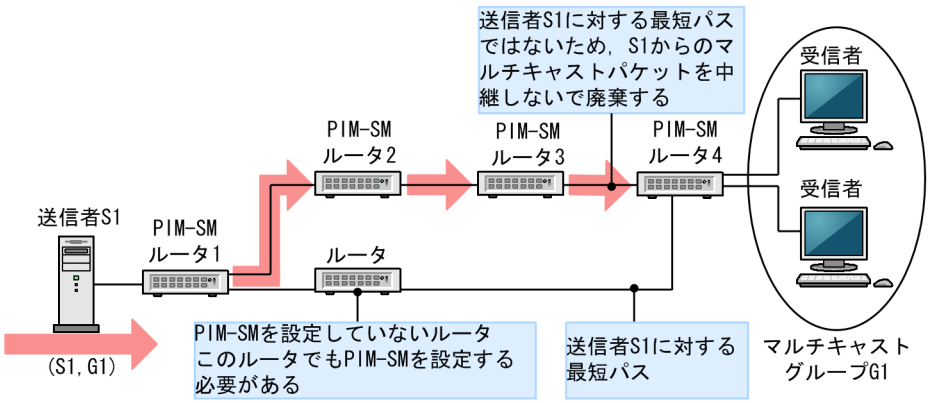


PIM-SM ルータ A と PIM-SM ルータ B の DR-Priority を比較した場合，PIM-SM ルータ B の DR-Priority が大きいため，PIM-SM ルータ B が DR となってランデブーポイントにマルチキャストグループ参加情報を通知します。PIM-SM ルータ D と PIM-SM ルータ E の DR-Priority を比較した場合，DR-Priority が等しいため，IPv6 アドレスで比較します。その結果，IPv6 アドレスが大きい PIM-SM ルータ E が DR となってランデブーポイントに対して IP カプセル化パケットを中継します。

(6)　冗長経路時の注意事項

次に示す図のような冗長構成の場合，マルチキャストパケットが中継されないので注意してください。冗長経路がある場合は，その経路上のすべてのルータで PIM-SM の設定が必要になります。

図 26-16　冗長経路時の注意事項



(7)　IPv6 PIM-SM タイマ仕様

PIM-SM が使用するタイマ値を次の表に示します。

表 26-12　PIM-SM タイマ値

タイマ名	内容	デフォルト値	本装置の設定範囲	備考
Hello_Period※1	PIM Hello メッセージの送信周期	30（秒）	5～3600（秒）	－

タイマ名	内容	デフォルト値	本装置の設定範囲	備考
Hello_Holdtime※2	隣接関係の保持期間	105（秒）	3.5×Hello_Period（秒）	－
Triggered_Hello_Delay	PIM Hello メッセージの一斉送信を抑止するための調整時間	0～5（秒）	－	起動時の最初の PIM Hello メッセージ送信，または近隣ルータの再起動検出による PIM Hello メッセージ送信時の遅延時間（0～5 秒の間でランダムに決定します）
Assert_Time	PIM Assert メッセージによる中継抑止期間	180（秒）	－	－
Assert_Override_Interval	Assert 制御によるマルチキャスト中継の抑止を更新するための調整時間	3（秒）	－	Assert 敗者がマルチキャスト中継を再開する前（Assert_Time）に Assert 勝者が PIM Assert メッセージを送信して，Assert 敗者の中継抑止時間を更新するための調整時間
t_periodic※1	PIM Join/Prune メッセージの送信周期	60（秒）	30～3600（秒）	最大で＋ 50%の揺らぎが発生します
J/P_HoldTime※2	経路情報および中継先インタフェースの保持期間	210（秒）	3.5×t_periodic（秒）	－
Deletion-Delay-Time※1※3※4	PIM Prune メッセージ受信後のマルチキャスト中継先インタフェースの保持期間	1/3×J/P_HoldTime（秒）	0～300（秒）	－
t_suppressed	PIM Join/Prune メッセージの集中を回避するための送信抑止時間	66～84（秒）	－	－
J/P_Override_Interval	PIM Prune メッセージの受信からマルチキャスト中継停止までの時間	3（秒）	1000～98302（ミリ秒）（Effective_Propagation_Delay ＋ Effective_Override_Interval）	マルチキャスト中継停止までの間にマルチキャスト中継を継続したい下流ルータが PIM Join メッセージを送信すると，マルチキャスト中継は維持されます
Override_Interval※1	Effective_Override_Interval を決定するための本装置の設定時間	2500（ミリ秒）	500～65535（ミリ秒）	－
Effective_Override_Interval	t_override を算出するための LAN 上の決定時間	2500（ミリ秒）	－	LAN 上の全近隣ルータの Override_Interval の最大値

タイマ名	内容	デフォルト値	本装置の設定範囲	備考
t_override	PIM Join/Prune メッセージの一斉送信を抑止するための調整時間	0～2500（ミリ秒）	0～65535（ミリ秒）	調整時間は 0～Effective_Override_Interval の間でランダムに決定します
Propagation_Delay※1	Effective_Propagation_Delay を決定するための本装置の設定時間	500（ミリ秒）	500～32767（ミリ秒）	－
Effective_Propagation_Delay	LAN 上で決定した PIM Join/Prune メッセージが行き渡るまでの遅延時間	500（ミリ秒）	－	LAN 上の全近隣ルータの Propagation_Delay の最大値
Keepalive Timer※1	マルチキャスト中継エントリの保持期間	210（秒）	0（無期限），60～43200（秒）	最大で＋ 90 秒の誤差が発生します
Register_Supression_Time	IP カプセル化送信の抑止期間	60（秒）	－	最大で±30 秒の揺らぎが発生します
Register_Probe_Time※1※5※6	IP カプセル化送信の再開確認を送信する時間	5（秒）	5～60（秒）	デフォルトの 5 秒では Register_Supression_Time が満了する 5 秒前に IP カプセル化送信の再開確認（PIM Null-Register メッセージ）を一度だけ送信します
C-RP-Adv-Period	ランデブーポイント候補の通知周期	60（秒）	－	－
RP-Holdtime※2	ランデブーポイント保持期間	150（秒）	2.5×C-RP-Adv-Period（秒）	－
Bootstrap-Period	PIM Bootstrap メッセージの送信周期	60（秒）	－	－
Bootstrap-Timeout※2	PIM Bootstrap メッセージの保持期間	130（秒）	2×Bootstrap-Period ＋ 10（秒）	－
Negative-Cache-Holdtime※1（PIM-SM）	ネガティブキャッシュエントリの保持期間	210（秒）	10～3600（秒）	PIM-SSM の場合は 3600 秒の固定。

（凡例）　－：該当しない

注※1

　コンフィグレーションで設定できます。

注※2

　計算式で算出されます（コンフィグレーションで設定できません）。

注※3

本タイマ値をコンフィグレーションで設定した場合は設定値を使用しますが，本中継先インタフェースに対して，最後に受信した PIM Join/Prune メッセージに含まれる Join/Prune-Holdtime を超えない値を中継先インタフェースの保持期間として設定します。

注※4

本タイマ値は RFC2362 に準拠した近隣ルータに対して使用するタイマです。コンフィグレーションで設定された値が優先されるため，RFC2362 の規定とは異なった動作をします。なお，コンフィグレーションで値を指定していない場合には RFC2362 の動作に準じます。

注※5

本タイマ値を 10 以上に設定すると，IP カプセル化送信の再開確認を 5 秒おきに複数回送信します。コンフィグレーションで値を指定していない場合には，一度だけ送信します。

注※6

本タイマ値は RFC2362 に準拠しています。

(8)　IPv6 PIM-SM 使用時の注意事項

PIM-SM を使用したネットワークを構成する場合には次に示す制限事項に注意してください。本装置は RFC4601（PIM-SM 仕様）に準拠していますが，一部 RFC との差分があります。RFC との差分を次の表に示します。

表 26-13　RFC との差分

項目	RFC	本装置
パケットフォーマット	RFC にはエンコードグループアドレスおよびエンコードソースアドレスにマスク長を設定するフィールドがある。	エンコードアドレスのマスク長は 128 固定。
	RFC にはエンコードグループアドレスおよびエンコードソースアドレスにアドレスファミリとエンコードタイプを設定するフィールドがある。	エンコードアドレスのアドレスファミリは 2(IPv6)，エンコードタイプは 0 固定。IPv6 以外の PIM-SM とは接続できない。
	RFC には PIM メッセージのヘッダに PIM バージョンを設定するフィールドがある。	PIM バージョンは 2 固定。 PIM バージョン 1 と接続できない。
PIM Join/Prune フラグメント	PIM Join/Prune メッセージはネットワークの MTU 長を超えてもフラグメントできる。	送信する PIM Join/Prune メッセージのサイズが大きい場合，8192 オクテットに分割して送信する。さらに，分割して送信する PIM Join/Prune メッセージはネットワークの MTU 長で IP フラグメントによって送信される。
PIM Register メッセージ送信時の IP フラグメント動作	PIM Register ヘッダが付加されることを考慮して，IP フラグメントしたあとにそれぞれのフラグメントパケットを IP カプセル化する。	IP カプセル化したパケットを IP フラグメントする。
IPsec 認証	Authentication Header（AH）を使用する IPsec 転送モードがある。	未サポート。
PMBR との接続	RFC では PMBR（PIM Border Router）との接続および(*，*，RP)マルチキャスト経路情報に関する仕様が記述されている。	PMBR との接続をサポートしていない。また，(*，*，RP)マルチキャスト経路情報もサポートしていない。

項目	RFC	本装置
最短パスへの切り替え	最短パスへの切り替えタイミングとしてデータレートを基に切り替える方法がある。	ラストホップルータで最初のデータを受信したら，データレートをチェックしないで最短パスへ切り替える。

26.4.3　IPv6 PIM-SSM

PIM-SSM はグループアドレスのアドレス範囲を分離することで，PIM-SM と同時に使用できます。PIM-SSM が使用するグループアドレスは IANA で割り当てられています。本装置では，コンフィグレーションで PIM-SSM が動作するグループアドレスのアドレス範囲を指定できます。指定したアドレス範囲以外では PIM-SM が動作します。

PIM-SM はマルチキャスト中継エントリの作成にマルチキャストパケットが必要なのに対して，PIM-SSM はマルチキャスト経路情報（PIM Join メッセージ）の交換でマルチキャスト中継エントリを作成して，該当するエントリでマルチキャストパケットを中継します。また，PIM-SSM ではランデブーポイントおよびブートストラップルータは必要ありません。したがって，マルチキャストパケットを中継するときにマルチキャストパケットの IP カプセル化および IP デカプセル化がなくなり，効率の良いマルチキャスト中継が実現できます。

PIM-SSM は MLDv2（INCLUDE モード）の受信者と接続している場合に動作します。また，本装置には MLDv1 または MLDv2（EXCLUDE モード）の受信者が PIM-SSM を利用できるようにする MLD PIM-SSM 連携機能があります。

(1)　IPv6 PIM-SSM メッセージサポート仕様

PIM-SSM メッセージのサポート仕様を次の表に示します。

表 26–14　PIM-SSM メッセージのサポート仕様

メッセージタイプ	機能
PIM Hello	隣接するマルチキャストルータを検出する。
PIM Join/Prune	マルチキャスト配送ツリーの参加および刈り込みをする。
PIM Assert	Forwarder を決定する。

(2)　IPv6 PIM-SSM を動作させる前提条件

本装置のコンフィグレーションで次に示す設定が必要です。

- 各装置の設定
  PIM-SSM が動作するグループアドレスのアドレス範囲を設定します。
- MLDv2（INCLUDE モード）が動作する受信者が直結している装置
  接続するインタフェースに MLDv2 を設定します。
- MLDv1 または MLDv2（EXCLUDE モード）が動作する受信者が直結している装置
  接続するインタフェースに MLDv1 または MLDv2 を設定します。
  使用するグループアドレスに送信元アドレスを設定します。

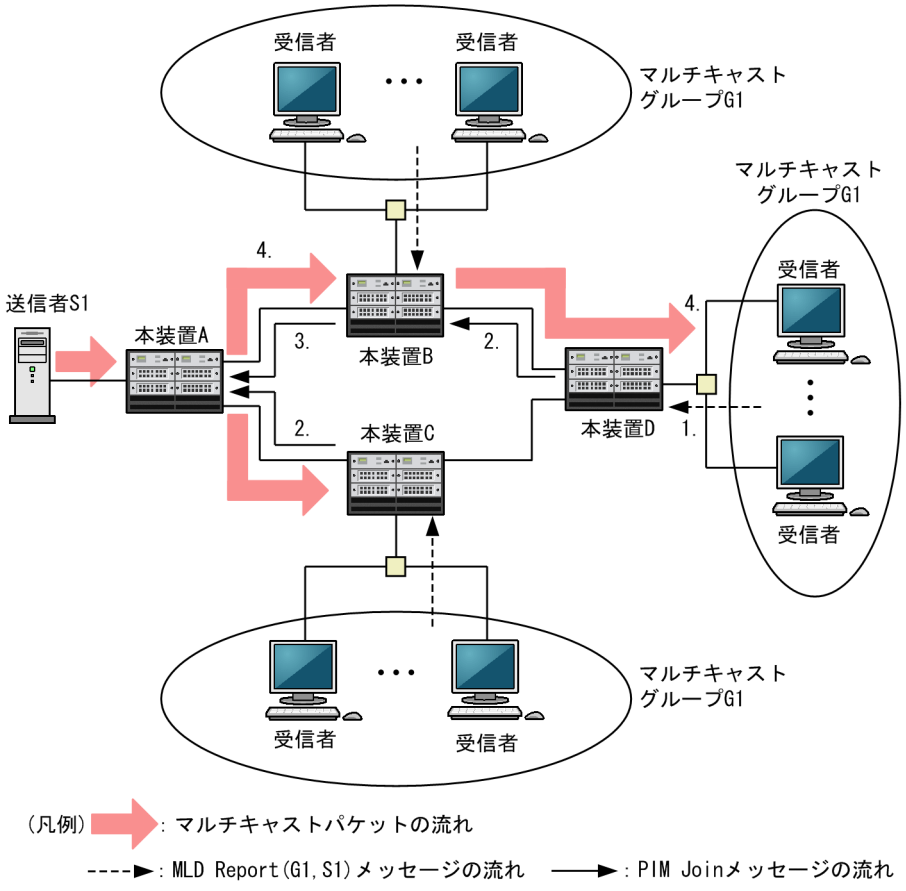
(3)　IPv6 PIM-SSM 動作（受信者が MLDv2（INCLUDE モード）の場合）

PIM-SSM を使用するためには送信者の情報が必要です。MLDv2 では，送信者を MLD Report メッセージで指定すると PIM-SSM を使用できます。マルチキャスト送信者（送信元アドレス：S1）がマルチキャストグループ（グループアドレス：G1）にマルチキャストパケットを送信する場合の動作を次に示します。

1. 受信者からマルチキャストグループに参加するための MLDv2 Report(G1,S1)メッセージを受信します。
2. MLDv2 Report(G1,S1)メッセージを受信した装置は，MLDv2 Report(G1,S1)メッセージで通知された送信元アドレス（S1）の方向（ユニキャストのルーティング情報で決定）に PIM Join メッセージを送信します。この場合，PIM Join メッセージには，送信元アドレス（S1）とグループアドレス（G1）の情報が入ります。
3. PIM Join メッセージを受信した各装置は，送信元アドレス（S1）への最短パス方向にホップバイホップで PIM Join メッセージを送信します。PIM Join メッセージを受信した装置は送信元アドレス（S1）とグループアドレス（G1）のマルチキャスト経路情報を学習します。
4. マルチキャスト送信者（送信元アドレス：S1）がマルチキャストグループ（グループアドレス：G1）宛てにマルチキャストパケットを送信します。マルチキャストパケットを受信した装置は学習したマルチキャスト経路情報から生成したマルチキャスト中継エントリに従ってマルチキャストパケットを中継します。

PIM-SSM の動作概要を次の図に示します。

図 26-17　PIM-SSM 動作概要（受信者が MLDv2（INCLUDE モード）の場合）



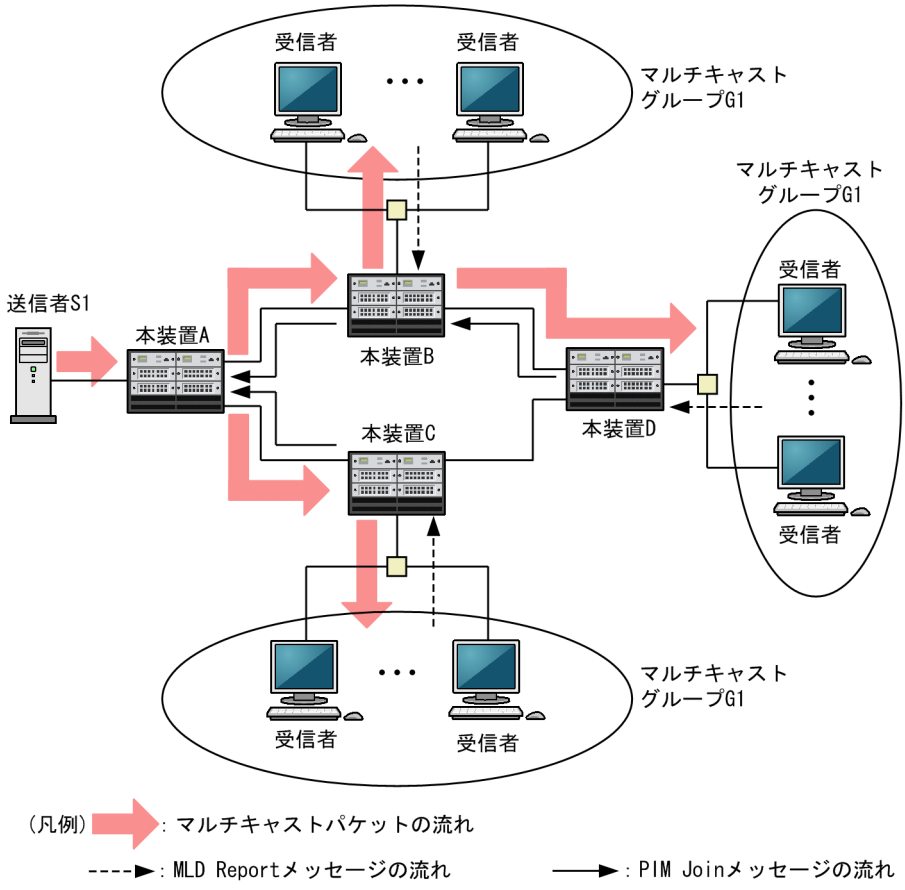
(4)　IPv6 PIM-SSM 動作（受信者が MLDv1 または MLDv2（EXCLUDE モード）の場合）

PIM-SSM を使用するためには送信者の情報が必要です。MLDv1 または MLDv2（EXCLUDE モード）を使用する場合，本装置で MLD PIM-SSM 連携機能を設定すると PIM-SSM を使用できます。受信者が MLDv1 の場合に，マルチキャスト送信者（送信元アドレス：S1）がマルチキャストグループ（グループアドレス：G1）にマルチキャストパケットを送信するときの動作を次に示します。

1. 受信者からマルチキャストグループに参加するための MLDv1 Report メッセージを受信します。
2. MLDv1 Report メッセージを受信した装置は，MLDv1 Report メッセージで通知されたグループアドレス（G1）と MLD PIM-SSM 連携機能で設定したグループアドレスを比較します。グループアドレスが一致した場合，MLD PIM-SSM 連携機能で設定した送信元アドレス（S1）への最短パス方向（ユニキャストのルーティング情報で決定）に PIM Join メッセージを送信します。この場合，PIM Join メッセージには，送信元アドレス（S1）とグループアドレス（G1）の情報が入ります。
3. PIM Join メッセージを受信した各装置は送信元アドレス（S1）への最短パス方向にホップバイホップで PIM Join メッセージを送信します。PIM Join メッセージを受信した装置は送信元アドレス（S1）とグループアドレス（G1）のマルチキャスト経路情報を学習します。
4. マルチキャスト送信者（送信元アドレス：S1）がマルチキャストグループ（グループアドレス：G1）宛てにマルチキャストパケットを送信します。マルチキャストパケットを受信した装置は学習したマルチキャスト経路情報から生成したマルチキャスト中継エントリに従ってマルチキャストパケットを中継します。

PIM-SSM の動作概要を次の図に示します。

図 26-18　PIM-SSM の動作概要（受信者が MLDv1 または MLDv2（EXCLUDE モード）の場合）



(5)　近隣検出

PIM-SM（「26.4.2　IPv6 PIM-SM　(3)　近隣検出」）と同じです。

(6)　Forwarder の決定

PIM-SM（「26.4.2　IPv6 PIM-SM　(4)　Forwarder の決定」）と同じです。

(7)　DR の決定および動作

PIM-SM（「26.4.2　IPv6 PIM-SM　(5)　DR の決定および動作」）と同じです。

(8)　冗長経路時の注意事項

PIM-SM（「26.4.2　IPv6 PIM-SM　(6)　冗長経路時の注意事項」）と同じです。

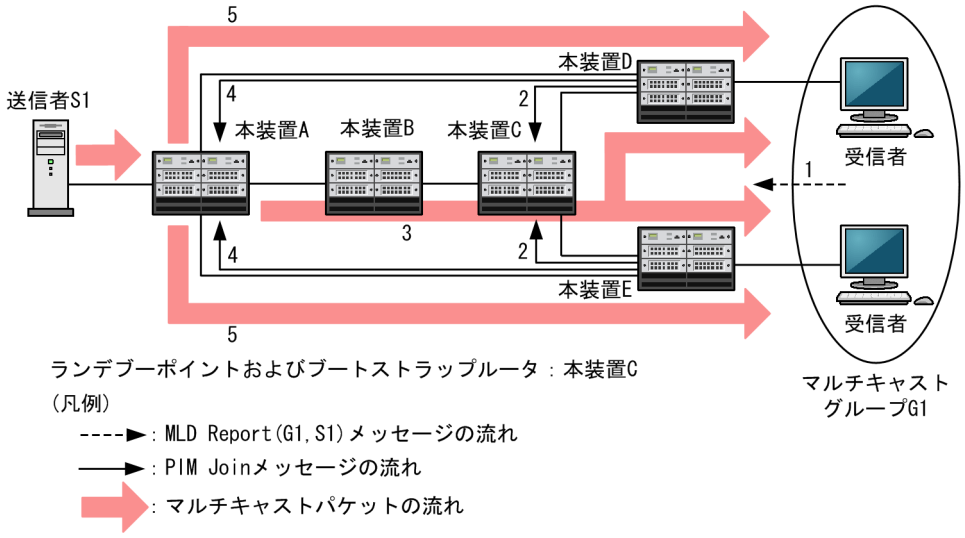
26.4.4　MLDv2 使用時の IPv6 経路制御動作

(1)　MLDv2 使用時の IPv6 PIM-SM 動作

マルチキャスト送信者（送信元アドレス：S1）が PIM-SM で使用するマルチキャストグループ（グループアドレス：G1）にマルチキャストパケットを送信して，受信者が MLDv2 でマルチキャストグループに参加する場合の動作を次に示します。

1. 受信者からマルチキャストグループに参加するための MLDv2 Report(G1,S1)メッセージを受信します。
2. MLDv2 Report(G1,S1)メッセージを受信した装置は，ランデブーポイントへの最短パス方向にグループアドレス（G1）を設定した PIM Join メッセージを送信します。
3. PIM Join メッセージを受信したランデブーポイントは各マルチキャストグループの存在を認識します。マルチキャストパケットを送信元ネットワークからランデブーポイント経由で各グループメンバに配送するために，送信者を頂点としたランデブーポイント経由の配送ツリーを形成します。
4. 送信者から各グループメンバに対して最短パスで到達できるように，既存のユニキャストルーティングを使用して送信者からの最短パスを決定します(PIM Join メッセージを送信者への最短パス方向に送信して，最短パス配送ツリーを形成します)。
5. マルチキャスト送信者（送信元アドレス：S1）がマルチキャストグループ（グループアドレス：G1）宛てに送信したマルチキャストパケットを受信した装置は，最短パス配送ツリーに従ってマルチキャストパケットを中継します。

図 26-19　MLDv2 使用時の PIM-SM 動作概要



(2)　MLDv1/MLDv2 受信者混在時の IPv6 経路制御

MLDv1 で PIM-SSM の設定をしている状態で，MLDv1 受信者と MLDv2 受信者が混在する場合の経路制御動作について説明します。

コンフィグレーションで設定した PIM-SSM で使用するアドレス範囲に含まれるグループアドレスに対して参加要求を受信した場合，次の表に示すように PIM-SSM が動作します。MLDv1/MLDv2 受信者混在時の経路制御動作を次の表に示します。

表 26-15　MLDv1/MLDv2 受信者混在時の経路制御動作

参加グループアドレス	MLDv1 Report メッセージ MLDv2 Report（EXCLUDE モード）メッセージ	MLDv2 Report（INCLUDE モード）メッセージ
PIM-SSM で使用するアドレス範囲内	PIM-SSM （MLD PIM-SSM 連携機能使用時）	PIM-SSM
PIM-SSM で使用するアドレス範囲外	PIM-SM	PIM-SM

MLDv1 Report メッセージで参加要求を受信した場合，送信元リストには MLD PIM-SSM 連携機能で設定された送信元アドレスを使用します。MLDv1 Report メッセージと MLDv2 Report（EXCLUDE モード）メッセージで同じグループアドレスに対して参加要求を受信した場合，送信元リストには MLD PIM-SSM 連携機能で設定された送信元アドレスと MLDv2 Report（INCLUDE モード）メッセージに含まれる送信元リストを合わせたリストを使用します。

26.4.5　系切替時の無停止マルチキャスト中継機能

IPv6 マルチキャストでは，二重化構成での運用で系切替する場合，無停止で PIM-SSM のマルチキャスト中継を継続する機能をサポートしています。本機能は，コンフィグレーションコマンド ipv6 pim nonstop-forwarding を設定すると有効になります。

系切替後，再学習時間内は系切替前に設定したハードウェアエントリでマルチキャスト中継を継続します。再学習時間内に新しいマルチキャスト経路情報を学習した場合は，すぐに該当するマルチキャスト中継を開

始します。また，学習した中継先に対して離脱要求を受信した場合は，すぐに該当するマルチキャスト中継を停止します。再学習時間内に学習しなかったマルチキャスト中継エントリは，再学習時間終了時に削除します。なお，再学習時間の開始時と終了時にはシステムメッセージを出力します。

再学習時間はデフォルトで 240 秒です。「(2)　再学習時間の算出方法」を参照して，適切な再学習時間を設定してください。

本機能使用時，VRF のインタフェースで IPv6 マルチキャストを使用している場合は，IPv6 マルチキャストを使用した VRF の全インタフェースで本機能が有効になります。

なお，系切替後の IPv6 マルチキャスト中継エントリの再学習状況は，次に示す運用コマンドで確認できます。

- show ipv6 mcache (show ipv6 pim mcache)
- show ipv6 mroute

(1)　無停止マルチキャスト中継機能を使用するための前提条件

(a)　ユニキャストルーティング高可用機能の使用

無停止マルチキャスト中継機能を使用するときは，ユニキャストルーティング高可用機能を有効にしてください。ユニキャストルーティング高可用機能が無効な場合，系切替後に上流のユニキャスト経路が安定しないため，マルチキャスト中継のパケットロスが多発することがあります。

(b)　Generation ID オプションをサポートしている装置の設置

系切替するルータの近隣ルータには，Generation ID オプションをサポート（RFC4601 および RFC5059 に準拠）している装置を設置してください。近隣ルータが Generation ID オプションをサポートしていない場合，系切替後に PIM メッセージの送受信が遅延するため，再学習時間内に再学習が完了しないことがあります。なお，Generation ID オプションについては，「26.4.2　IPv6 PIM-SM」の「(3)　近隣検出」を参照してください。

(2)　再学習時間の算出方法

すべてのマルチキャスト中継エントリの再学習が完了する前に再学習時間が終了すると，未学習のエントリの中継が一時的に停止します。そのため，コンフィグレーションコマンド ipv6 pim nonstop-forwarding の aging-time パラメータには，次の計算式で算出した再学習時間以上の値を設定してください。

再学習時間＝次に示す 1 と 2 のうち最長値＋ 105 秒

1. MLD のグループメンバ学習時間
   各 MLD インタフェースの MLD General Query メッセージの送信間隔のうち最長値（デフォルトでは 125 秒）と，MLD Report メッセージの最大応答待ち時間（本装置が Querier の場合は 10 秒）との合計。
2. PIM Join メッセージの受信時間
   各 PIM インタフェースの下流ルータから受信する PIM Join/Prune メッセージの受信間隔のうち最長値（下流ルータが本装置の場合，デフォルトでは 60 秒）。

(3)　無停止マルチキャスト中継機能使用時のタイマ仕様

本機能を有効にした場合，次に示すタイマ仕様を変更します。

- J/P_HoldTime

上流方向に PIM Join/Prune メッセージを送信する装置で本機能を使用した場合，J/P_HoldTime には次に示す値のうち，長い方の時間を設定して送信します（本機能未使用時は 210 秒を設定）。

- PIM Join/Prune メッセージの送信間隔（デフォルトで 60 秒）×3.5
- 再学習時間（デフォルトで 240 秒）＋ 10 秒

(4)　再学習時間内の上流インタフェースの切り替え

再学習時間内にマルチキャスト中継エントリの上流インタフェースのユニキャスト経路が変更された場合，通常と同様に，該当するエントリの上流インタフェースもユニキャスト経路に従って変更します。このとき，一時的にパケットロスが発生します。

このユニキャスト経路の変更を抑止するには，送信元へのユニキャスト経路をスタティック経路で設定するか，コンフィグレーションコマンド ipv6 pim nonstop-forwarding で keep-incoming パラメータを設定してください。また，ユニキャスト経路の変更によって上流インタフェースが該当するエントリの下流インタフェースに変更された場合，この下流インタフェースへの中継を停止します。

(5)　コンフィグレーションコマンド変更時の中継動作

(a)　PIM-SSM で使用するアドレス範囲の変更

再学習時間内にコンフィグレーションコマンドで PIM-SSM で使用するアドレス範囲を変更すると，再学習時間が終了します。この場合，再学習時間内に未学習のマルチキャスト中継エントリの中継を停止します。

(b)　VRF のマルチキャスト中継の停止

再学習時間内にコンフィグレーションコマンドで VRF のマルチキャスト中継を停止すると，再学習時間が終了します。この場合，残りのすべての VRF で，再学習時間内に未学習のマルチキャスト中継エントリの中継を停止します。

(c)　下流インタフェースの IPv6 マルチキャスト設定

再学習時間内にコンフィグレーションコマンドでマルチキャスト中継エントリの下流インタフェースの IPv6 マルチキャストを無効にしても，未学習のエントリの場合は該当するエントリの中継を継続することがあります。ただし，この中継は再学習時間終了時に停止します。

(6)　注意事項

- 本機能を使用する場合，運用系ならびに待機系の BCU および PRU のソフトウェアを本機能対応バージョンにアップデートしてください。

  運用系および待機系の BCU だけが本機能対応バージョンで，PRU が本機能未対応バージョンのまま無停止マルチキャスト中継機能を使用すると，系切替時に IPv6 マルチキャストルーティングプログラムが再起動します。この場合，IPv6 マルチキャストルーティングプログラムがマルチキャスト経路情報を再学習するまで，マルチキャスト中継が停止します。
- エクストラネットのマルチキャスト中継エントリは本機能の対象外です。そのため，系切替が発生すると該当するエントリのマルチキャスト中継は停止します。系切替後，該当するエントリを再学習することで中継が再開します。
- 系切替の直前にマルチキャストパケットの二重中継が発生すると，二重中継の解消に時間が掛かることがあります。この場合，系切替後にマルチキャスト経路情報を再学習すると，PIM Assert メッセージによって二重中継が解消されます。

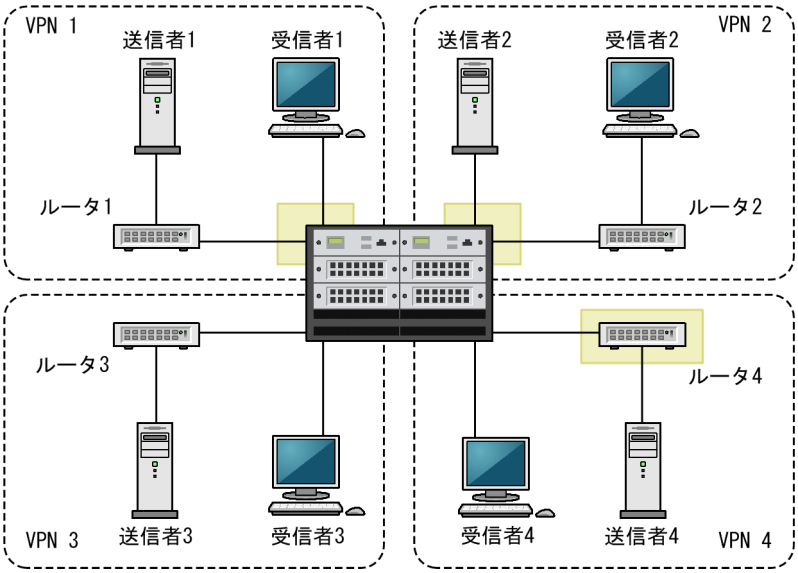
26.4.6　VRF での IPv6 マルチキャスト

(1)　IPv6 マルチキャスト VRF

本装置を複数の VPN に接続して，それぞれの VPN 上でマルチキャストを使用できます。VPN ごとに VRF を設定して，それぞれの VRF でマルチキャストを動作させます。VRF 上のマルチキャストでは，ランデブーポイント，ブートストラップルータ，各種タイマ，PIM-SSM で使用するアドレス範囲などにそれぞれ異なる設定ができます。

本装置を四つの VPN に接続した場合の構成例および本装置での設定情報を次に示します。

図 26-20　VRF でのマルチキャスト



（凡例）　：ランデブーポイントおよびブートストラップルータ

表 26-16　本装置での設定情報

VPN	運用プロトコル	ループバックインタフェースに設定したアドレス	ランデブーポイント () 内はランデブーポイントアドレス	PIM-SSM で使用するアドレス範囲
1	PIM-SM	2001:db8::1	本装置（2001:db8::1）	未使用
2	PIM-SM/ PIM-SSM	2001:db8::2	本装置（2001:db8::2）	ff30::/12
3	PIM-SSM	2001:db8::2	なし	ff35:100::/32
4	PIM-SM	2001:db8::3	ルータ 4（2001:db8::1）	未使用

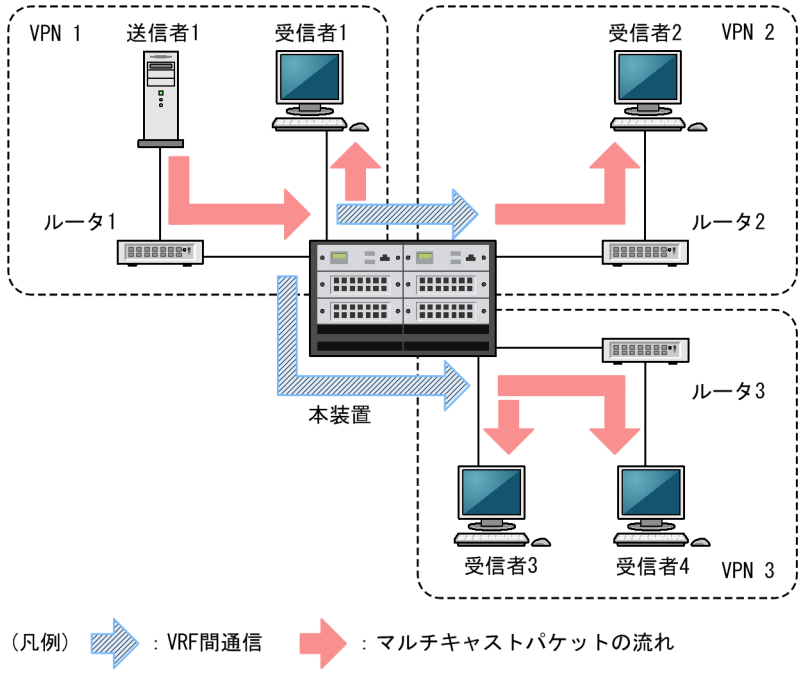
(2)　IPv6 マルチキャストエクストラネット

マルチキャストエクストラネットを使用すると，VRF 間でマルチキャスト中継ができます。また，マルチキャスト経路フィルタリングを使用すると，エクストラネットで使用するグループアドレスの範囲と，下流からの中継要求を許可する VRF を限定できます。マルチキャストエクストラネットは PIM-SSM だけでサポートしています。

なお，ラストホップルータから最短パスを確立するため，ユニキャストエクストラネットによる送信者へのユニキャスト経路が存在する必要があります。

エクストラネットの動作概要を次の図に示します。

図 26-21　マルチキャストエクストラネットの動作概要



(3)　IPv6 マルチキャストエクストラネット使用時の注意事項

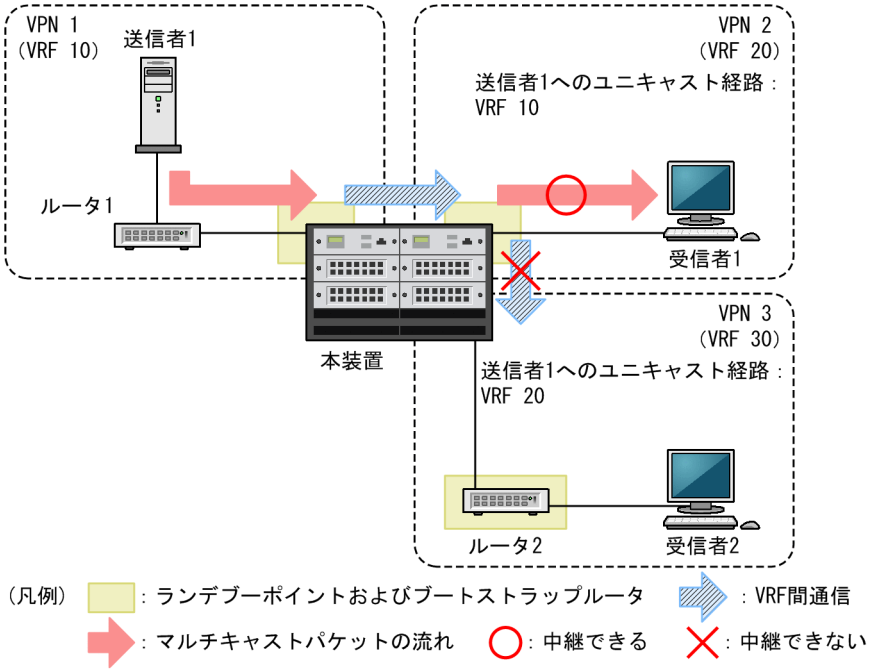
(a)　装置内での 2 段以上の VRF 中継

マルチキャストエクストラネットでは装置内で 2 段以上の VRF 中継を禁止しています。

ある VRF のマルチキャスト経路情報で，上流インタフェースと下流インタフェースの一部にほかの VRF を設定できません。上流インタフェースが異なる VRF のマルチキャスト経路情報は，VRF からの中継要求を無視します。また，下流インタフェースに VRF を持つマルチキャスト経路情報の上流インタフェースが異なる VRF に切り替わった場合，該当マルチキャスト経路情報から VRF の下流インタフェースを切り離します。

次の図に示すように VPN 3 から VPN 1 へのユニキャスト経路が VPN 2 を経由して形成されていた場合，VPN 1 上の送信者 1 が送信するマルチキャストパケットを VPN 2 上の受信者 1 は受信できますが，VPN 3 の受信者 2 は受信できません。

図 26-22　マルチキャストエクストラネット使用時に装置内で VRF 中継を禁止している例



(b)　下流インタフェースを追加または削除した場合のシステムメッセージ出力

IPv6 マルチキャスト中継エントリの下流インタフェースがマルチキャストエクストラネットの場合，コンフィグレーションコマンド ipv6 multicast join-prune-event logging enable を設定していても，メッセージ種別 MULTI-INFO のシステムメッセージを出力しません。

26.5　ネットワーク設計の考え方

26.5.1　IPv6 マルチキャスト中継

本装置でマルチキャストパケットを中継する場合，次の点に注意してください。

(1)　IPv6 PIM-SM/PIM-SSM 共通

(a)　ルーティングプログラムの再起動に伴う中継断

本装置では，運用コマンド restart ipv6-multicast を実行してマルチキャストルーティングプログラムを再起動する場合，マルチキャスト経路情報を再学習するまでマルチキャスト通信が停止するので注意してください。

(b)　動作インタフェース

IP アドレスのマスク長が 8 ビットから 30 ビットのインタフェース上で動作します。

(c)　BCU 二重化構成での系切替に伴う中継断

本装置を二重化構成で運用している場合，コンフィグレーションコマンド ipv6 pim nonstop-forwarding を設定すると，系切替時に無停止でマルチキャスト中継を継続できます。ipv6 pim nonstop-forwarding コマンドを設定しないと，系切替後にマルチキャスト経路情報を再学習するまでマルチキャスト通信が停止します。

(2)　IPv6 PIM-SM

IPv6 で PIM-SM を使用する場合は次の点に注意してください。

(a)　ソフトウェア処理時のパケットロス

本装置では，最初のマルチキャストパケット受信でマルチキャスト通信を行うためのマルチキャスト中継エントリをハードウェアに設定します。マルチキャスト中継エントリを作成するまでの間はソフトウェアでマルチキャストパケットを処理するため，マルチキャスト通信のトラフィック量によっては一時的にマルチキャストパケットをロスする場合があります。

(b)　ソフトウェア処理時のマルチキャストパケットの追い越し

本装置では，ハードウェアへのマルチキャスト中継エントリの設定が完了すると，ハードウェア中継を開始します。そのあと，マルチキャスト中継エントリの生成のためにソフトウェアで処理したマルチキャストパケットを中継します。このときに一部のマルチキャストパケットで追い越しが発生して，マルチキャストパケットの順序が入れ替わる場合があります。

(c)　パス切り替え時の二重中継またはパケットロス

本装置では，ランデブーポイント経由でのマルチキャストパケット中継時およびランデブーポイント経由から最短パス経由への切り替え時，一時的に二重中継またはパケットロスが発生する場合があります。

ランデブーポイント経由のマルチキャストパケットの中継動作およびランデブーポイント経由から最短パス経由への切り替え動作は「26.4.2　IPv6 PIM-SM」を参照してください。

(d)　ループバックインタフェースへのアドレス設定必須

本装置をファーストホップルータとして使用する場合，ランデブーポイントへの通信にはループバックインタフェースに設定した IPv6 アドレスが使用されます。そのため IPv6 の PIM-SM では，ランデブーポイントやブートストラップルータでない場合にもループバックインタフェースへのアドレス設定が必須です。

(e)　ループバックインタフェースに設定したアドレスへの到達可能性

本装置をランデブーポイントおよびブートストラップルータとして使用する場合，ループバックインタフェースに設定した IPv6 アドレスがランデブーポイントとブートストラップルータのアドレスになります。このアドレスはマルチキャスト通信する全装置でユニキャストでのルート認識および通信ができる必要があります。

(f)　静的ランデブーポイント機能

静的ランデブーポイント機能は，ブートストラップルータを使用しないでランデブーポイントを指定する機能です。静的ランデブーポイント機能はコンフィグレーションで設定します。

静的ランデブーポイントはブートストラップルータから PIM Bootstrap メッセージによって広告されたランデブーポイント候補との共存もできます。共存時，静的ランデブーポイントはブートストラップルータから PIM Bootstrap メッセージによって広告されたランデブーポイント候補よりも優先されます。

なお，ランデブーポイント候補のルータは，ランデブーポイントルータアドレスが自アドレスであることを認識することでランデブーポイントとして動作します。したがって，ブートストラップルータを使用しないで静的ランデブーポイント機能を使用してネットワークを設計する場合は，ランデブーポイント候補のルータでも静的ランデブーポイント機能の設定が必要です。

また，静的ランデブーポイント機能を使用する場合，同一ネットワーク上の全ルータに対して同じ設定をする必要があります。

26.5.2　冗長経路（障害などによる経路切り替え）

本装置でマルチキャスト経路が冗長経路になっている場合，次の点に注意してください。

(1)　IPv6 PIM-SM の使用

PIM-SM の場合，次に示す経路切り替えでマルチキャスト通信が再開するまで時間が掛かるので注意してください。なお，時間の表示では送信元のネットワーク情報（ユニキャストルーティング情報）切り替え時間を U と表します。

ここに記述する時間は，本装置が切り替えに掛かる時間です。そのため，実際にマルチキャスト中継が再開するには，本装置が上流ルータに対して PIM Join メッセージを送信してから，上流からマルチキャストパケットが到着するまでの「参加通知時間」が掛かります。

- 優先経路が切り替わった場合，通信再開までには次に示す時間が掛かることがあります。
  U ＋ 20 秒
- 回線障害によって優先経路から冗長経路へ切り替わった場合，通信再開までには次に示す時間が掛かることがあります。
  U ＜ 5 の時：5～10 秒
  U≧5 の時：U ＋ 0～60 秒
- 回線復旧によって冗長経路から優先経路へ切り替わった場合，優先経路による通信への切り替えまでには次に示す時間が掛かることがあります。

0 秒

ただし，切り戻りには次に示す時間が掛かります。

U ＋（送信者方向の PIM Hello メッセージの送信周期＋ 20）秒 （デフォルトでは U ＋ 30 ＋ 20 ＝ U ＋ 50 秒）

- ランデブーポイントおよびブートストラップルータが本装置に切り替わった（障害やコンフィグレーションなどでランデブーポイントおよびブートストラップルータを本装置にする）場合，通信再開までには次に示す時間が掛かることがあります。

  通信再開までの時間は，ランデブーポイントまたはブートストラップルータで異なります。括弧内はデフォルト値を示します。

  - ランデブーポイント切り替え時：285 秒

    RP-Holdtime（150 秒）＋ Query Interval（125 秒）＋ Query Response Interval（10 秒）

  - ブートストラップルータ切り替え時：最大で 385 秒

    Bootstrap-Timeout（130 秒）＋ BS_Rand_Override（0～60 秒）＋ Bootstrap-Period（60 秒）＋ Query Interval（125 秒）＋ Query Response Interval（10 秒）

- DR（Designated Router）が本装置に切り替わった場合，通信再開までには次に示す時間が掛かることがあります。括弧内はデフォルト値を示します。

  - DR 切り替え時：240 秒

    Hello-Holdtime（105 秒）＋ Query Interval（125 秒）＋ Query Response Interval（10 秒）

障害による冗長経路切り替えだけでなく，構成変更によって意識的に経路を切り替えた場合も，マルチキャスト通信がこれらの時間停止することがあります。システムの構成変更は計画的に実施してください。

(2)　IPv6 PIM-SSM の使用

PIM-SSM の場合，次に示す経路切り替えでマルチキャスト通信が再開するまで時間が掛かるので注意してください。なお，時間の表示では送信元のネットワーク情報（ユニキャストルーティング情報）切り替え時間を U と表します。

ここに記述する時間は，本装置が切り替えに掛かる時間です。そのため，実際にマルチキャスト中継が再開するには，本装置が上流ルータに対して PIM Join メッセージを送信してから，上流からマルチキャストパケットが到着するまでの「参加通知時間」が掛かります。

- 優先経路が切り替わった場合，通信再開までには次に示す時間が掛かることがあります。

  U ＋ 20 秒

- 回線障害によって優先経路から冗長経路へ切り替わった場合，通信再開までには次に示す時間が掛かることがあります。

  U ＜ 5 の時：5～10 秒

  U≧5 の時：U ＋ 0～135 秒

- 回線復旧によって冗長経路から優先経路へ切り替わった場合，優先経路による通信への切り替えまでには次に示す時間が掛かることがあります。

  0 秒

  ただし，切り戻りには次に示す時間が掛かります。

  U ＋（送信者方向の PIM Hello メッセージの送信周期＋ 20）秒 （デフォルトでは U ＋ 30 ＋ 20 ＝ U ＋ 50 秒）

- DR（Designated Router）が本装置に切り替わった場合，通信再開までには次に示す時間が掛かることがあります。括弧内はデフォルト値を示します。

- DR 切り替え時：240 秒
  Hello-Holdtime（105 秒）＋ Query Interval（125 秒）＋ Query Response Interval（10 秒）

26.5.3　適応ネットワーク構成例

(1)　IPv6 PIM-SM を使用する構成

本構成は次の場合に適応します。

- マルチキャスト送信者を限定しない場合
- マルチキャスト送信者が多数存在する場合

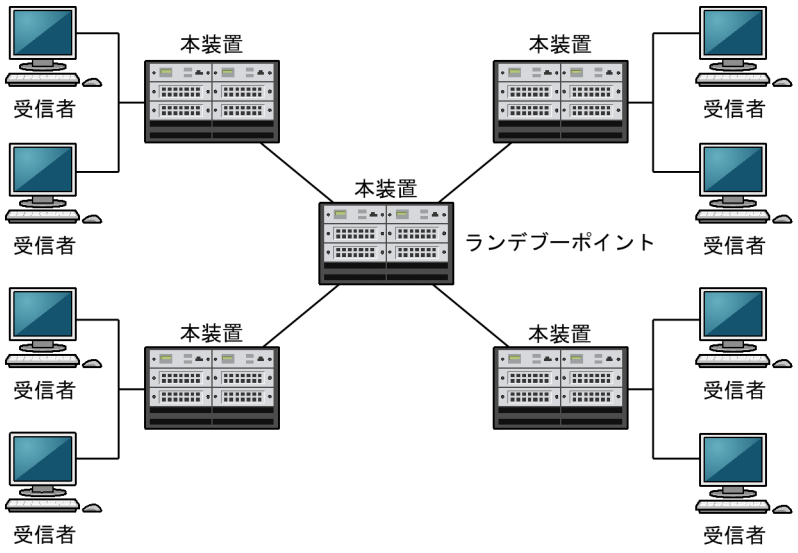
[ネットワークの環境]

1. 前提条件として，すべてのルータでユニキャスト経路が必要です。
2. 本装置間のマルチキャストルーティングプロトコルには PIM-SM を使用します。
3. 各受信者と本装置間のマルチキャストグループ管理制御には MLD を使用します。
4. 一つの装置をランデブーポイントおよびブートストラップルータとします。
5. ランデブーポイントを静的ランデブーポイントとして指定することもできます。この場合，システム立ち上げ時のランデブーポイント決定までの時間を短縮できます。

[構成図]

構成図を次に示します。

図 26–23　PIM-SM を使用する構成図



(2)　IPv6 PIM-SSM を使用する構成

本構成は次の場合に適応します。

- マルチキャスト送信者を限定する場合（主に配信サーバなど）
- マルチキャスト受信者が MLDv2 対応で送信する送信者のアドレスを指定できる場合
- ブロードバンドマルチキャスト通信をする場合
- 多チャンネルマルチキャスト通信をする場合

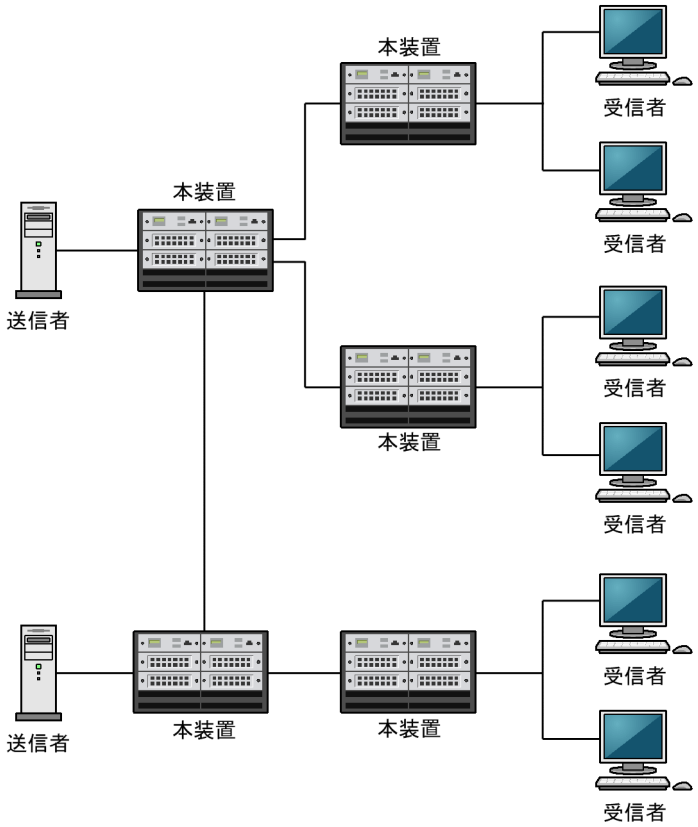
［ネットワークの環境］

1. 前提条件として，すべてのルータでユニキャスト経路が必要です。
2. 本装置間のマルチキャストルーティングプロトコルには PIM-SSM を使用します。
3. 各受信者と本装置間のマルチキャストグループ管理制御には MLD を使用します（MLDv1 を使用する場合は MLD PIM-SSM 連携機能の設定が必要です）。

［構成図］

構成図を次に示します。

図 26–24　PIM-SSM を使用する構成図



26.5.4　ネットワーク構成での注意事項

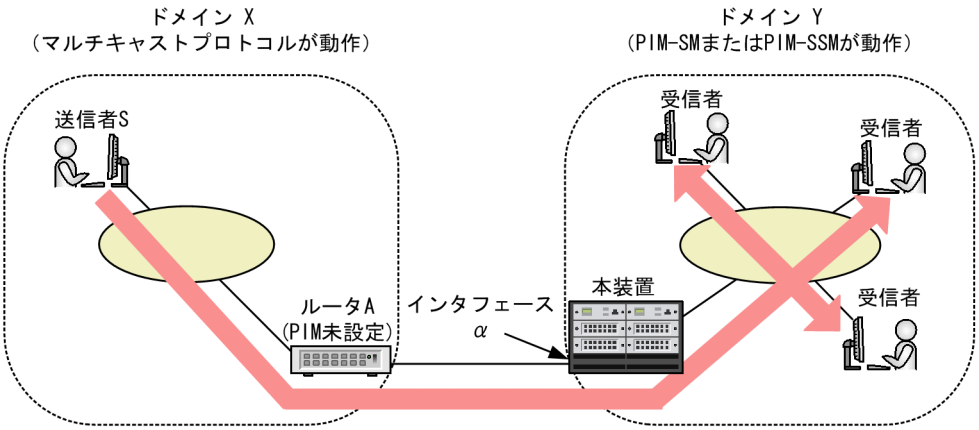
マルチキャストは送信者から各グループメンバ（受信者）にマルチキャストパケットを配信する 1（送信者）：N（受信者）の片方向通信に適します。マルチキャストの適応ネットワーク構成，注意事項を次に示します。

(1)　IPv6 PIM-SM/PIM-SSM 共通

(a)　隣接ルータが PIM-SM/PIM-SSM を設定していない場合の構成

PIM-SM または PIM-SSM（以下，PIM と略します）では送信者から受信者に至る経路上のすべてのルータで PIM の設定が必要となります。そのため，途中で PIM を設定していないルータがあると，マルチキャストパケットが中継できません。隣接ルータが PIM を設定していない場合には，マルチキャストサーバ仮想接続機能を使用するとマルチキャストパケットの中継ができるようになります。マルチキャストサーバ仮想接続機能を使用する場合の適応例を次の図に示します。

図 26-25　マルチキャストサーバ仮想接続機能を使用する場合の適応例



ルータ A と本装置は異なるマルチキャストドメインに属しているため，これらの間には PIM が設定されていません。一方，ドメイン X にいる送信者からドメイン Y にいる受信者にマルチキャストパケットを送信したいという要求があります。ルータ A と本装置の間で PIM が動作していないので，送信者 S から送られたマルチキャストパケットは本装置で廃棄されます。ここで本装置のインタフェース α にマルチキャストサーバ仮想接続機能で送信者 S を設定すると，ドメイン Y 内へマルチキャストパケットを転送できるようになります。ただし，静的グループ参加機能などを使用して，ルータ A が本装置のインタフェース α に対してマルチキャストパケットを送信し続ける設定が必要です。

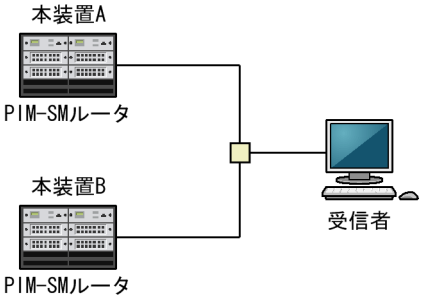
(b)　注意が必要な構成

次に示す構成で PIM-SM または PIM-SSM を使用する場合，注意が必要です。

- 次の図に示す構成のように，受信者と直接接続するルータが同一ネットワーク上に複数存在するインタフェースでは，必ず PIM-SM を動作させてください。

  同一ネットワーク上に複数のルータが存在するインタフェースで PIM-SM を動作させないで MLD だけを動作させた場合，マルチキャストパケットが二重に中継されることがあります。

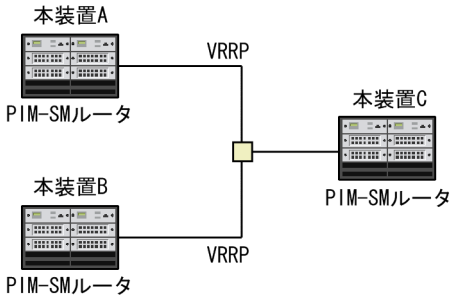
  図 26-26　PIM-SM/PIM-SSM で注意が必要な構成（複数ルータと受信者の接続）



- 次の図に示す構成のように，本装置 C が本装置 A と本装置 B に VRRP を設定した仮想インタフェースをゲートウェイとするスタティック経路を設定した環境では，PIM-SM および PIM-SSM が上流ルータを検出できないため，マルチキャスト通信ができません。

  この構成でマルチキャスト通信をする場合は，本装置 C にランデブーポイントアドレス，ブートストラップルータアドレス，およびマルチキャスト送信者アドレスへのゲートウェイアドレスを本装置 A または本装置 B の実アドレスとするスタティック経路を設定する必要があります。

図 26-27　PIM-SM/PIM-SSM で注意が必要な構成（VRRP を設定した場合）

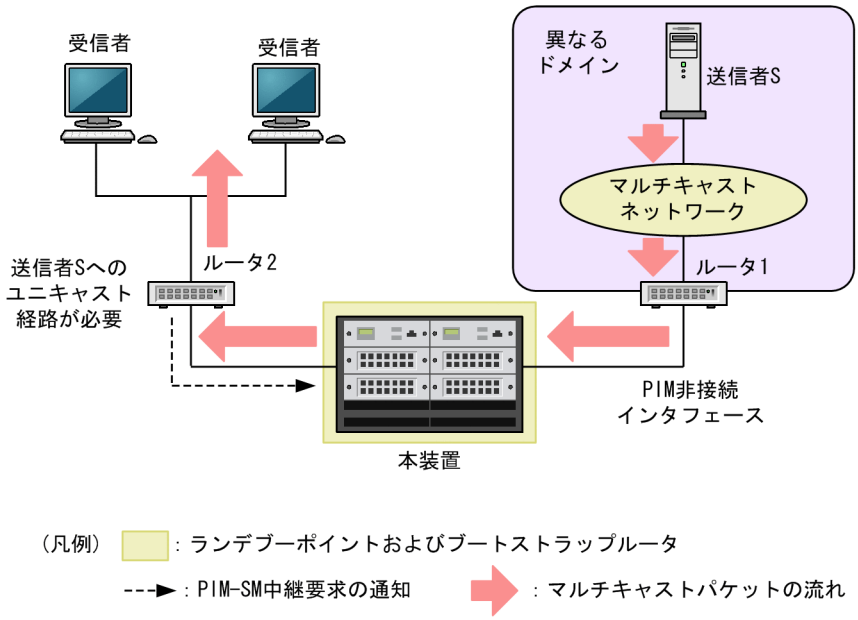


- 異なるドメイン上のルータと PIM-SM および PIM-SSM プロトコルを使用しないでマルチキャスト中継をする場合，そのルータとのインタフェースを PIM 非接続インタフェースと呼びます。

  次の図に示す構成のように，異なるドメイン上の送信者 S から送信されるマルチキャストパケットを PIM 非接続インタフェースを経由してマルチキャスト中継する場合，次の設定が必要です。

  - 本装置の下流ルータ（ルータ 2）に，送信者 S へのユニキャスト経路を設定する。
  - 本装置の PIM 非接続インタフェースに，マルチキャストサーバ仮想接続機能を設定する。

  図 26-28　PIM-SM/PIM-SSM で注意が必要な構成（PIM 非接続インタフェース経由の中継）

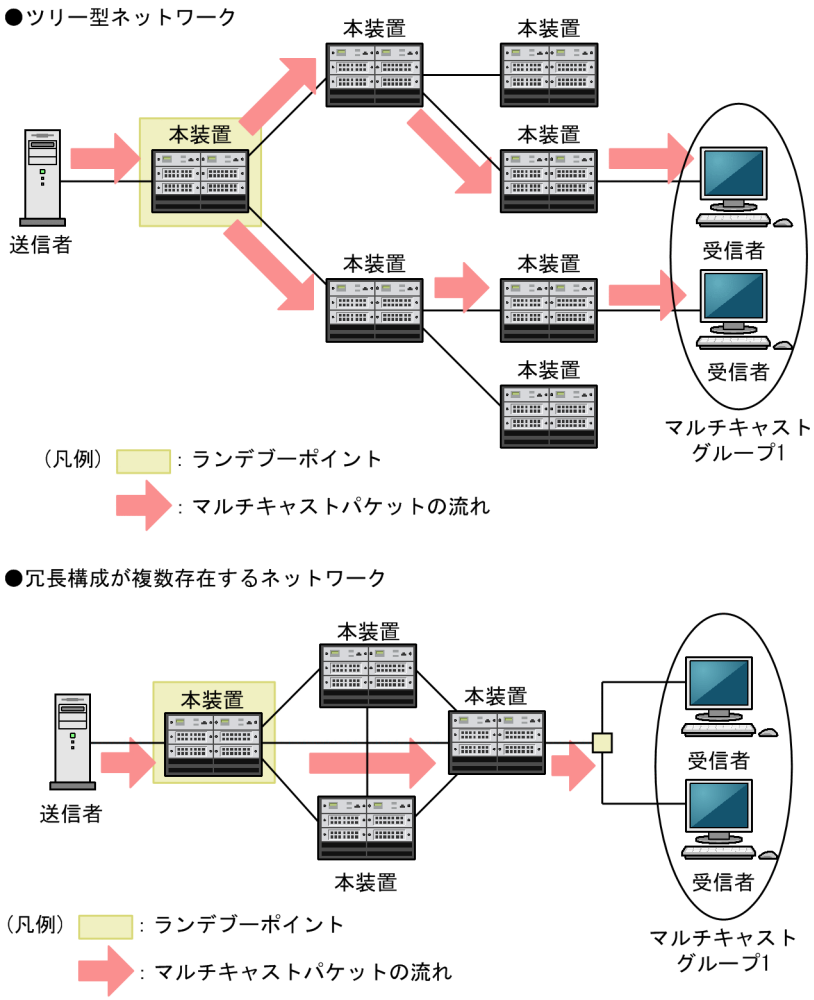


(2)　IPv6 PIM-SM

(a)　推奨構成

PIM-SM では，ツリー型ネットワーク構成および冗長経路が存在するネットワーク構成を推奨します。ただし，ランデブーポイントの配置には十分注意してください。PIM-SM 推奨ネットワーク構成を次の図に示します。

図 26-29　PIM-SM 推奨ネットワーク構成

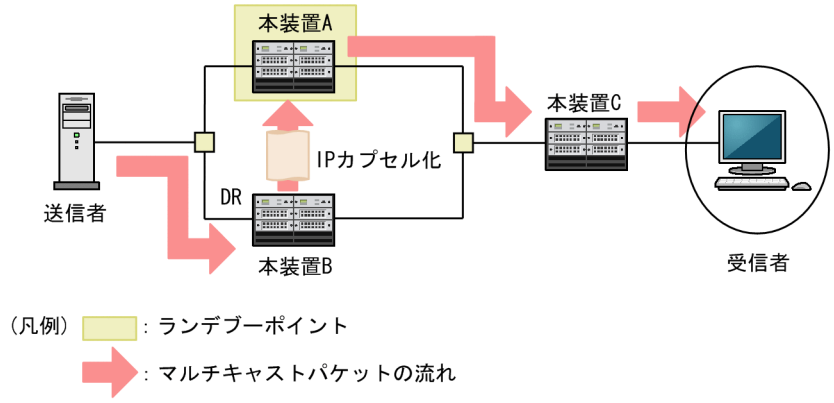


(b)　注意が必要な構成

送信者と直接接続するルータが同一ネットワーク上に 2 台以上存在する構成で PIM-SM を使用する場合は注意が必要です。次の図に示す構成でどれかをランデブーポイントとする場合は，ランデブーポイントが DR（Designated Router）になるようにしてください。

ランデブーポイント以外を DR にした場合，DR からランデブーポイントに対して PIM Register メッセージを送信するため，本装置 A，B に負荷が掛かります。また，PIM Register メッセージ中のマルチキャストパケットを中継するときに，ランデブーポイントでパケットロスが発生するおそれがあります。なお，ランデブーポイントを DR にした場合は，PIM Register メッセージによる IP カプセル化は行いません。

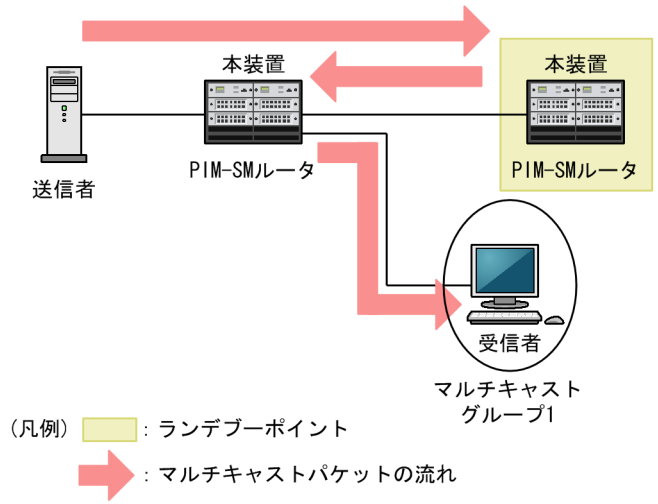
図 26-30　PIM-SM で注意が必要な構成（複数ルータと送信者の接続）



(c)　不適応な構成

送信者とランデブーポイントの間に受信者が存在する構成で PIM-SM は使用しないでください。次の図に示す構成で送信者からマルチキャストグループ 1 へのマルチキャスト通信をする場合，ランデブーポイント経由の中継が効率良く行えません。

図 26-31　PIM-SM で不適応な構成（送信者とランデブーポイントの間に受信者が存在する場合）



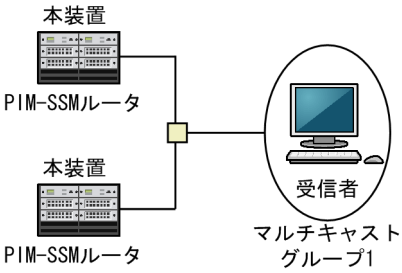
(3)　IPv6 PIM-SSM

(a)　注意が必要な構成

次に示す構成で PIM-SSM を使用する場合，注意が必要です。

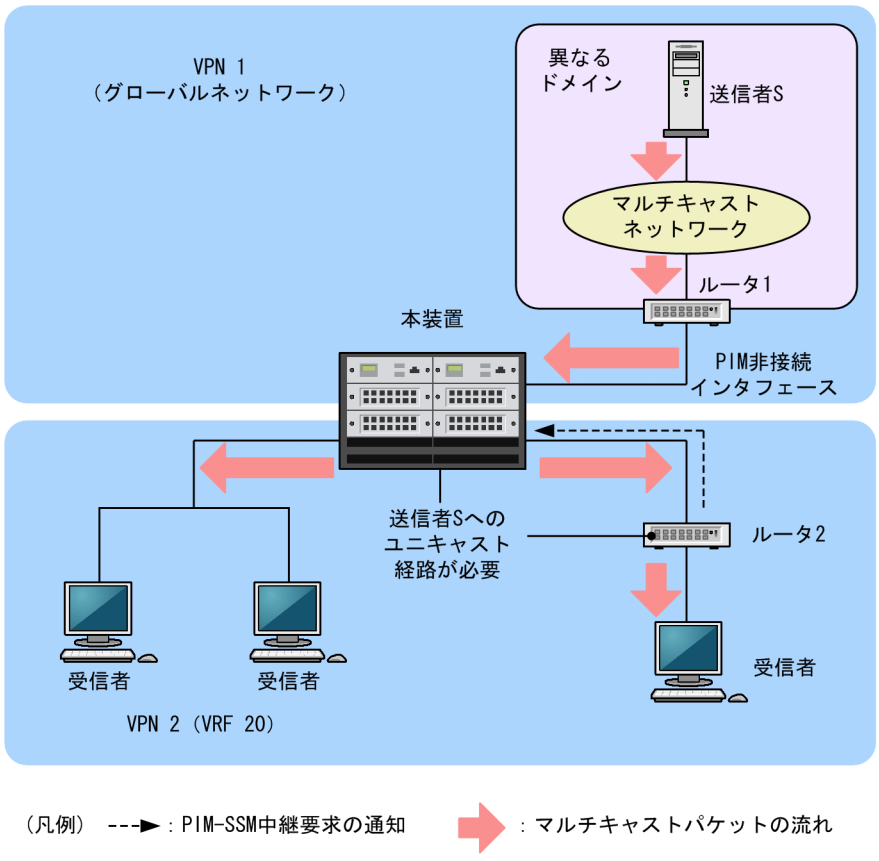
- マルチキャスト受信者と同一回線上に複数の PIM-SSM ルータが動作する構成で PIM-SSM を使用する場合は注意が必要です。次の図に示す構成で MLD PIM-SSM 連携機能を動作させる場合は，同一回線上のすべてのルータにコンフィグレーションコマンド ipv6 pim ssm および ipv6 mld ssm-map static を設定してください。

図 26-32　PIM-SSM で注意が必要な構成（複数ルータと受信者の接続）



- 次の図に示す構成のように，上流となる VPN 1（グローバルネットワーク）で異なるドメイン上の送信者 S から送信されるマルチキャストパケットを PIM 非接続インタフェースを経由して VPN 2（VRF 20）にマルチキャスト中継する場合，次の設定が必要です。
  - 本装置では，上流となる VRF の PIM 非接続インタフェースにマルチキャストサーバ仮想接続機能を設定する。また，マルチキャストエクストラネットの設定とともに，本装置の中継先 VRF に送信者 S へのユニキャスト経路を設定する。
  - 中継先 VPN 上の下流ルータ（ルータ 2）に，送信者 S へのユニキャスト経路を設定する。

図 26-33　PIM-SSM で注意が必要な構成（エクストラネットでの PIM 非接続インタフェース経由の中継）



(b)　送信者に複数のアドレスを設定したときの注意事項

PIM-SSM 使用時マルチキャスト送信者に複数の IPv6 アドレスを付与して運用する場合，送信されるマルチキャストパケットの送信元アドレスが本装置にコンフィグレーションコマンド ipv6 mld ssm-map static で設定した送信元アドレスと一致するようにしてください。特に，RA（Router Advertisement）な

どのアドレス自動設定機能を使用した場合は, マルチキャスト送信者が自動設定されたアドレスを使用して通信することがあります。

27 IPv6 マルチキャストの設定と運用

この章では，IPv6 マルチキャストのコンフィグレーションの設定方法および状態の確認方法について説明します。

27.1　コンフィグレーション

27.1.1　コンフィグレーションコマンド一覧

IPv6 マルチキャストのコンフィグレーションコマンド一覧を次の表に示します。

表 27-1　コンフィグレーションコマンド一覧

コマンド名	説明
ipv6 mld fast-leave	インタフェースで MLD 即時離脱機能を有効にします。
ipv6 mld group-limit	参加できるマルチキャストグループの最大数を設定します。
ipv6 mld query-interval	MLD Query メッセージの送信間隔を設定します。
ipv6 mld router	インタフェースで MLD を動作させます。
ipv6 mld source-limit	マルチキャストグループ参加時のソースの最大数を設定します。
ipv6 mld ssm-map enable	MLD PIM-SSM 連携機能を有効にします。
ipv6 mld ssm-map static	MLD PIM-SSM 連携機能でのグループアドレスと送信元アドレスを設定します。
ipv6 mld static-group	静的グループ参加機能を設定します。
ipv6 mld version	MLD バージョンを設定します。
ipv6 multicast-routing	IPv6 マルチキャストルーティング機能を有効にします。
ipv6 multicast join-prune-event logging enable	IPv6 マルチキャスト運用中に IPv6 PIM または MLD の出力インタフェースを変更した場合に，システムメッセージを出力します。
ipv6 pim	インタフェースで PIM-SM，PIM-SSM および MLD を動作させます。
ipv6 pim assert-metric	PIM Assert メッセージで使用するメトリック値を設定します。
ipv6 pim assert-preference	PIM Assert メッセージで使用するプリファレンス値を設定します。
ipv6 pim bsr candidate bsr	ブートストラップルータ候補を設定します。
ipv6 pim bsr candidate rp	ランデブーポイント候補を設定します。
ipv6 pim deletion-delay-time	PIM Prune メッセージ受信後のマルチキャスト中継先インタフェースの保持期間を設定します。
ipv6 pim direct	マルチキャストサーバ仮想接続機能を設定します。
ipv6 pim dr-priority	DR の優先度を決定するための DR-Priority を設定します。
ipv6 pim hello-interval	PIM Hello メッセージの送信間隔を設定します。
ipv6 pim join-prune-interval	PIM Join/Prune メッセージの送信間隔を設定します。
ipv6 pim keep-alive-time	マルチキャスト中継エントリの無通信時の保持期間を設定します。
ipv6 pim max-interface	IPv6 マルチキャストを設定できるインタフェースの最大数を設定します。
ipv6 pim mcache-limit	マルチキャスト中継エントリの最大数を設定します。

コマンド名	説明
ipv6 pim mroute-limit	マルチキャスト経路情報の最大数を設定します。
ipv6 pim negative-cache-time	ネガティブキャッシュエントリの保持期間を設定します。
ipv6 pim nonstop-forwarding	無停止マルチキャスト中継機能を設定します。
ipv6 pim override-interval	ほかのルータが送信した PIM Prune メッセージを無効にする PIM Join メッセージが集中するのを回避するための時間を設定します。
ipv6 pim propagation-delay-time	PIM Join/Prune メッセージの転送遅延時間を設定します。
ipv6 pim register-probe-time	PIM Register メッセージ送信抑止時間を基に PIM Null-Register メッセージの送信開始時間を設定します。
ipv6 pim rp-address	静的ランデブーポイント機能を設定します。
ipv6 pim rp-mapping-algorithm	ランデブーポイント選出アルゴリズムの種別を設定します。
ipv6 pim ssm	PIM-SSM で使用するグループアドレスの範囲を設定します。

27.1.2　コンフィグレーションの流れ

使用する構成によって次の設定例を参照してください。

- **PIM-SM を使用する場合**
  - IPv6 マルチキャストルーティング機能の設定
  - IPv6 PIM-SM/PIM-SSM 動作インタフェースの設定
  - IPv6 PIM-SM ランデブーポイント候補の設定（自装置をランデブーポイントにする場合）
  - IPv6 PIM-SM ブートストラップルータ候補の設定（自装置をブートストラップルータにする場合）
  - MLD の設定
- **PIM-SM（静的ランデブーポイント機能）を使用する場合**
  - IPv6 マルチキャストルーティング機能の設定
  - IPv6 PIM-SM/PIM-SSM 動作インタフェースの設定
  - IPv6 PIM-SM 静的ランデブーポイント機能の設定
  - MLD の設定
- **PIM-SSM を使用する場合**
  - IPv6 マルチキャストルーティング機能の設定
  - IPv6 PIM-SM/PIM-SSM 動作インタフェースの設定
  - IPv6 PIM-SSM の設定
  - MLD の設定
- **VRF で PIM-SM を使用する場合**
  - VRF での IPv6 マルチキャストルーティング機能の設定
  - VRF での IPv6 PIM-SM/PIM-SSM 動作インタフェースの設定
  - VRF での IPv6 PIM-SM ランデブーポイント候補の設定（該当 VPN で自装置をランデブーポイントにする場合）

- VRF での IPv6 PIM-SM ブートストラップルータ候補の設定（該当 VPN で自装置をブートストラップルータにする場合）
- VRF での MLD の設定

- VRF で PIM-SM（静的ランデブーポイント機能）を使用する場合
  - VRF での IPv6 マルチキャストルーティング機能の設定
  - VRF での IPv6 PIM-SM/PIM-SSM 動作インタフェースの設定
  - VRF での IPv6 PIM-SM 静的ランデブーポイント機能の設定
  - VRF での MLD の設定
- VRF で PIM-SSM を使用する場合
  - VRF での IPv6 マルチキャストルーティング機能の設定
  - VRF での IPv6 PIM-SM/PIM-SSM 動作インタフェースの設定
  - VRF での IPv6 PIM-SSM の設定
  - VRF での MLD の設定
- VRF（エクストラネット）で PIM-SSM を使用する場合
  - VRF での IPv6 マルチキャストルーティング機能の設定
  - VRF での IPv6 PIM-SM/PIM-SSM 動作インタフェースの設定
  - VRF での IPv6 PIM-SSM の設定
  - IPv6 マルチキャストエクストラネットの設定

27.1.3　IPv6 マルチキャストルーティング機能の設定

[設定のポイント]

本装置で IPv6 マルチキャストルーティング機能を動作させるには，ここでの設定のほかに，一つ以上のインタフェースで PIM-SM または PIM-SSM（ipv6 pim コマンド）の設定が必要です。

本装置のループバックインタフェース（loopback 0）に設定した IPv6 アドレスを 2001:db8:1::2 とした場合の設定例を次に示します。

[コマンドによる設定]

1. **(config)# interface loopback 0**
   (config-if)# ipv6 address 2001:db8:1::2
   (config-if)# exit
   ループバックインタフェース（loopback 0）に IPv6 アドレスを設定します。
2. **(config)# ipv6 multicast-routing**
   IPv6 マルチキャストルーティング機能を有効にします。

27.1.4　IPv6 PIM-SM/PIM-SSM 動作インタフェースの設定

[設定のポイント]

マルチキャストルーティング機能を動作させるインタフェースには，PIM-SM または PIM-SSM を設定する必要があります。PIM-SM および PIM-SSM はインタフェースコンフィグレーションモードで設定します。

インタフェースの IPv6 アドレスを 2001:db8:10::/64 とした場合の設定例を次に示します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   ポート 1/1 のコンフィグレーションモードに移行します。
2. **(config-if)# ipv6 address 2001:db8:10::/64**
   (config-if)# ipv6 enable
   ポート 1/1 に IPv6 アドレスを設定します。
3. **(config-if)# ipv6 pim**
   ポート 1/1 に PIM-SM および PIM-SSM を設定します。

27.1.5　IPv6 PIM-SM ランデブーポイント候補の設定

[設定のポイント]

本装置をランデブーポイント候補として使用する場合，ランデブーポイントアドレスとしてループバックインタフェースに IPv6 アドレスを設定します。また，管理するグループアドレスを設定します。

管理するグループアドレスを ff00::/8，本装置のループバックインタフェース（loopback 0）に設定した IPv6 アドレスを 2001:db8:1::2 とした場合の設定例を次に示します。

[コマンドによる設定]

1. **(config)# interface loopback 0**
   (config-if)# ipv6 address 2001:db8:1::2
   (config-if)# exit
   ループバックインタフェース（loopback 0）に IPv6 アドレスを設定します。
2. **(config)# ipv6 access-list GROUP1**
   (config-ipv6-acl)# permit ipv6 any ff00::/8
   (config-ipv6-acl)# exit
   管理するグループアドレスのアクセスリスト（GROUP1）を作成します。
3. **(config)# ipv6 pim bsr candidate rp 2001:db8:1::2 group-list GROUP1**
   本装置をランデブーポイント候補として設定します。管理するグループアドレスにはアクセスリスト（GROUP1）を指定します。

27.1.6　IPv6 PIM-SM ブートストラップルータ候補の設定

[設定のポイント]

本装置をブートストラップルータ候補として使用する場合，ループバックインタフェースに IPv6 アドレスを設定します。また，ブートストラップルータ候補として設定します。

ループバックインタフェース（loopback 0）に設定した IPv6 アドレスを 2001:db8:1::2 とした場合の設定例を次に示します。

[コマンドによる設定]

1. **(config)# interface loopback 0**
   (config-if)# ipv6 address 2001:db8:1::2
   (config-if)# exit
   ループバックインタフェース（loopback 0）に IPv6 アドレスを設定します。

2.(config)# ipv6 pim bsr candidate bsr 2001:db8:1::2

本装置をブートストラップルータ候補として設定します。

27.1.7　IPv6 PIM-SM 静的ランデブーポイント機能の設定

[設定のポイント]

本装置をランデブーポイントとして使用する場合，ループバックインタフェースに設定した IPv6 アドレスを静的ランデブーポイントの IPv6 アドレスとして設定してください。

静的ランデブーポイントの IPv6 アドレスを 2001:db8:1::5 とした場合の設定例を次に示します。

[コマンドによる設定]

1.(config)# ipv6 pim rp-address 2001:db8:1::5

静的ランデブーポイントの IPv6 アドレスに 2001:db8:1::5 を設定します。

27.1.8　IPv6 PIM-SSM の設定

(1)　IPv6 PIM-SSM で使用するアドレス範囲の設定

[設定のポイント]

PIM-SM が設定されたインタフェースでは，PIM-SSM で使用するアドレス範囲で PIM-SSM が動作します。本装置で設定できるアドレス範囲は一つだけです。

アドレス範囲をデフォルト（ff30::/12）で使用する場合の設定例を次に示します。なお，デフォルト以外のアドレス範囲を指定する場合には，ipv6 pim ssm コマンドの range パラメータで設定してください。

[コマンドによる設定]

1.(config)# ipv6 pim ssm default

PIM-SSM を有効にします。

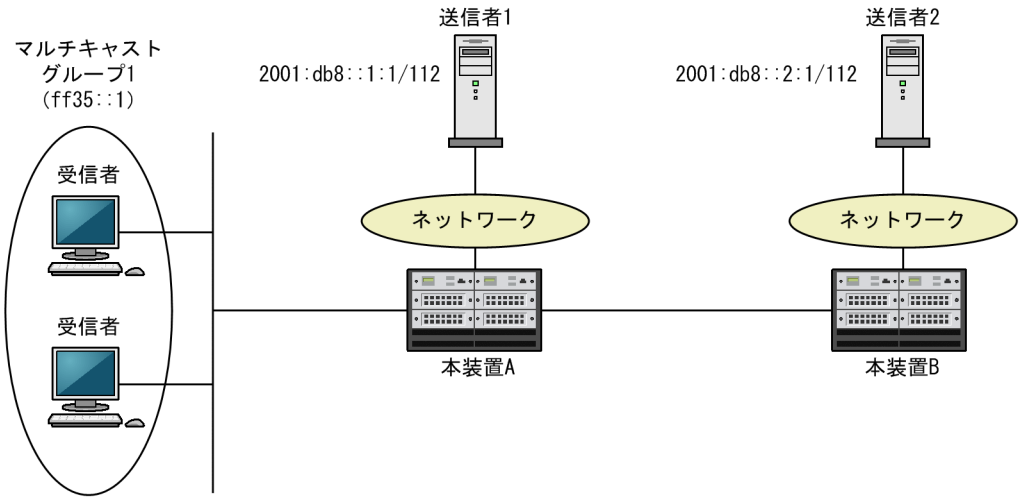
(2)　MLD PIM-SSM 連携機能の設定

[設定のポイント]

MLDv1/MLDv2（EXCLUDE モード）では送信元アドレスが特定できないため PIM-SSM と連携できません。本装置では, PIM-SSM が動作するグループアドレスと送信元アドレスを設定することで PIM-SSM と連携します。PIM-SSM が動作するグループアドレスは PIM-SSM で使用するアドレス範囲内である必要があります。

グループアドレス ff35::1 を二つの送信者（送信者 1 の送信元アドレスが 2001:db8::1:1，送信者 2 の送信元アドレスが 2001:db8::2:1）が使用する場合の PIM-SSM 構成例を次の図に示します。

図 27-1　PIM-SSM 構成例



[コマンドによる設定]

1. **(config)# ipv6 access-list GROUP3**
   (config-ipv6-acl)# permit ipv6 any ff35::/16
   (config-ipv6-acl)# exit
   管理するグループアドレスのアクセスリスト（GROUP3）を作成します。
2. **(config)# ipv6 mld ssm-map static GROUP3 2001:db8::1:1**
   (config)# ipv6 mld ssm-map static GROUP3 2001:db8::2:1
   PIM-SSM が動作するグループアドレスと，送信者 1 および送信者 2 の送信元アドレスを設定します。
   管理するグループアドレスにはアクセスリスト（GROUP3）を指定します。
3. **(config)# ipv6 mld ssm-map enable**
   MLD PIM-SSM 連携機能を有効にします。

27.1.9　MLD の設定

[設定のポイント]

MLD を動作させるインタフェースには，MLD の設定が必要です。なお，インタフェースに PIM-SM または PIM-SSM（ipv6 pim コマンド）を設定しても MLD は動作します。

デフォルトでは MLDv1 および MLDv2 混在モードです。MLD バージョンを変更する場合は，ipv6 mld version コマンドで設定してください。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   ポート 1/1 のコンフィグレーションモードに移行します。
2. **(config-if)# ipv6 mld router**
   該当インタフェースに MLD を設定します。

27.1.10　VRF での IPv6 マルチキャストルーティング機能の設定

[設定のポイント]

VRF で IPv6 マルチキャストルーティング機能を動作させるには，VRF ごとにループバックインタフェースへのアドレス設定，および IPv6 マルチキャストルーティング機能の設定が必要です。なお，ここでの設定のほかに，グローバルネットワークまたは VRF ごとに一つ以上のインタフェースで，PIM-SM または PIM-SSM（ipv6 pim コマンド）の設定が必要です。

VRF 10 での IPv6 マルチキャストルーティング機能の設定例を次に示します。

[コマンドによる設定]

1. **(config)# vrf definition 10**
   (config-vrf)# exit
   VRF 10 を設定します。
2. **(config)# interface loopback 30**
   (config-if)# vrf forwarding 10
   (config-if)# ipv6 address 2001:db8:1::10
   (config-if)# exit
   VRF 10 のループバックインタフェース（loopback 30）に IPv6 アドレスを設定します。
3. **(config)# ipv6 multicast-routing vrf 10**
   VRF 10 で IPv6 マルチキャストルーティング機能を有効にします。

27.1.11　VRF での IPv6 PIM-SM/PIM-SSM 動作インタフェースの設定

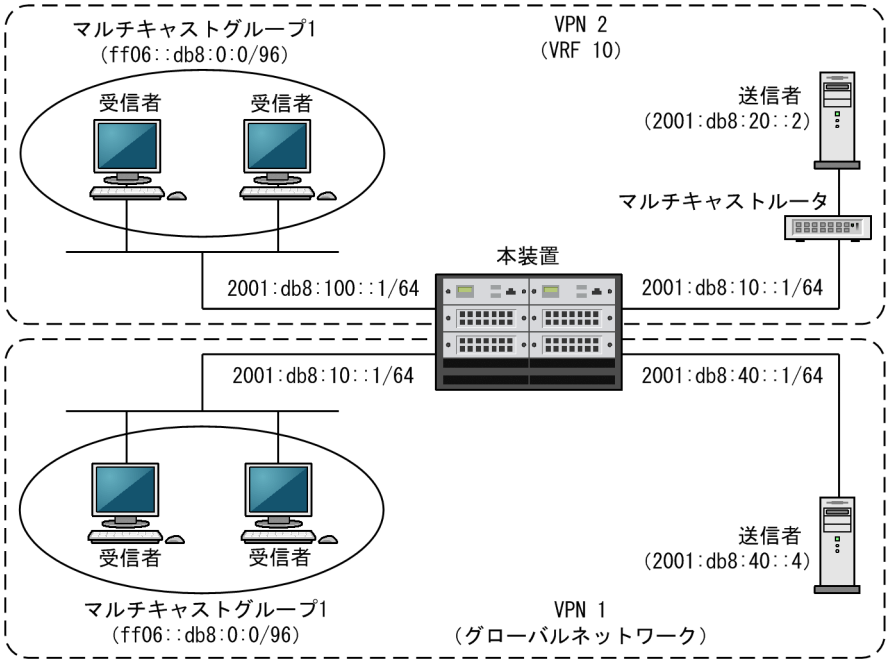
[設定のポイント]

VRF で PIM-SM を使用する場合，VRF に IPv6 マルチキャストルーティング機能を設定して，その VRF の一つ以上のインタフェースに PIM-SM または PIM-SSM を設定します。PIM-SM および PIM-SSM はインタフェースコンフィグレーションモードで設定します。

マルチキャストの送信者と受信者が本装置に直接接続するような，隣接ルータが存在しない VRF でも本設定は必要です。

VPN 2 に VRF 10 を対応させ，VRF 10 のインタフェースの IPv6 アドレスを 2001:db8:10::1/64 とした場合の PIM-SM および PIM-SSM 構成例を次の図に示します。

図 27-2　VRF での PIM-SM/PIM-SSM 構成例



[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   ポート 1/1 のコンフィグレーションモードに移行します。
2. **(config-if)# vrf forwarding 10**
   ポート 1/1 に VRF 10 を設定します。
3. **(config-if)# ipv6 address 2001:db8:10::/64**
   (config-if)# ipv6 enable
   ポート 1/1 に IPv6 アドレスを設定します。
4. **(config-if)# ipv6 pim**
   (config-if)# exit
   ポート 1/1 に PIM-SM および PIM-SSM を設定します。

27.1.12　VRF での IPv6 PIM-SM ランデブーポイント候補の設定

[設定のポイント]

VRF で本装置をランデブーポイント候補として使用する場合, ランデブーポイントアドレスとして該当 VRF のループバックインタフェースに IPv6 アドレスを設定します。また，管理するグループアドレスを設定します。

VRF 10 で管理するグループアドレスを ff06::db8:0:0/96，該当 VRF のループバックインタフェースを loopback 30，ループバックインタフェースに設定した IPv6 アドレスを 2001:db8:1::10 とした場合の設定例を次に示します。

[コマンドによる設定]

1. **(config)# interface loopback 30**
   (config-if)# vrf forwarding 10

```
(config-if)# ipv6 address 2001:db8:1::10
(config-if)# exit
```

VRF 10 のループバックインタフェース（loopback 30）に IPv6 アドレスを設定します。

2.
```
(config)# ipv6 access-list GROUP1
(config-ipv6-acl)# permit ipv6 any ff06::db8:0:0/96
(config-ipv6-acl)# exit
```

VRF 10 で管理するグループアドレスのアクセスリスト（GROUP1）を作成します。

3.
```
(config)# ipv6 pim vrf 10 bsr candidate rp 2001:db8:1::10 group-list GROUP1
```

本装置を VRF 10 のランデブーポイント候補として設定します。管理するグループアドレスにはアクセスリスト（GROUP1）を指定します。

27.1.13　VRF での IPv6 PIM-SM ブートストラップルータ候補の設定

[設定のポイント]

VRF で本装置をブートストラップルータ候補として使用する場合，ループバックインタフェースに IPv6 アドレスを設定します。また，ブートストラップルータ候補として設定します。

本装置のループバックインタフェース（loopback 30）に設定した IPv6 アドレスを 2001:db8:1::10 とした場合の設定例を次に示します。

[コマンドによる設定]

1.
```
(config)# interface loopback 30
(config-if)# vrf forwarding 10
(config-if)# ipv6 address 2001:db8:1::10
(config-if)# exit
```

VRF 10 のループバックインタフェース（loopback 30）に IPv6 アドレスを設定します。

2.
```
(config)# ipv6 pim vrf 10 bsr candidate bsr 2001:db8:1::10
```

本装置を VRF 10 のブートストラップルータ候補として設定します。

27.1.14　VRF での IPv6 PIM-SM 静的ランデブーポイント機能の設定

[設定のポイント]

本装置をランデブーポイントとして使用する場合，同じ VRF のループバックインタフェースに設定した IPv6 アドレスを静的ランデブーポイントの IPv6 アドレスとして設定してください。

VRF 10 の静的ランデブーポイントの IPv6 アドレスを 2001:db8:1::10 とした場合の設定例を次に示します。

[コマンドによる設定]

1.
```
(config)# ipv6 pim vrf 10 rp-address 2001:db8:1::10
```

VRF 10 で静的ランデブーポイントの IPv6 アドレスに 2001:db8:1::10 を設定します。

27.1.15　VRF での IPv6 PIM-SSM の設定

(1)　IPv6 PIM-SSM で使用するアドレス範囲の設定

[設定のポイント]

PIM-SM が設定された該当 VRF のインタフェースでは，PIM-SSM で使用するアドレス範囲で PIM-SSM が動作します。本装置で設定できるアドレス範囲は VRF ごとに一つだけです。

VRF 10 でアドレス範囲をデフォルト（ff30::/12）で使用する場合の設定例を次に示します。なお，デフォルト以外のアドレス範囲を指定する場合には，ipv6 pim ssm コマンドの range パラメータで設定してください。

[コマンドによる設定]

1.**(config)# ipv6 pim vrf 10 ssm default**

VRF 10 で PIM-SSM を有効にします。

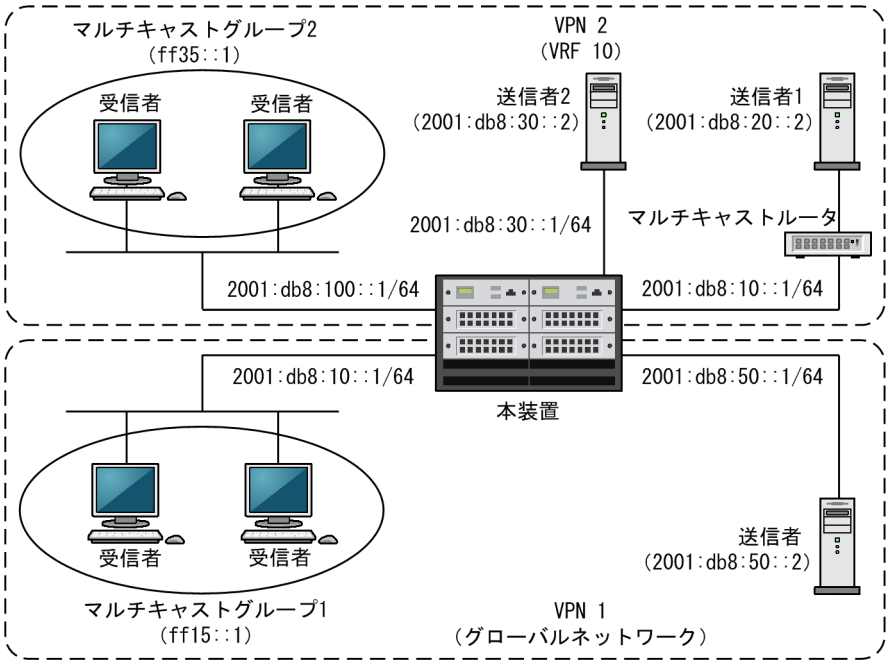
(2)　MLD PIM-SSM 連携機能の設定

[設定のポイント]

MLDv1/MLDv2（EXCLUDE モード）では送信元アドレスを特定できないため，PIM-SSM と連携できません。本装置では，PIM-SSM が動作するグループアドレスと送信元アドレスを設定することで PIM-SSM と連携します。PIM-SSM が動作するグループアドレスは PIM-SSM で使用するアドレス範囲内である必要があります。なお，本機能は VRF ごとに設定します。

VPN 2 に VRF 10 を対応させ，VPN 2 で使用するグループアドレス ff35::1 を同一 VPN 内で二つの送信者（送信者 1 の送信元アドレスが 2001:db8:20::2，送信者 2 の送信元アドレスが 2001:db8:30::2）が使用する場合の PIM-SSM 構成例を次の図に示します。

図 27-3　VRF での PIM-SSM 構成例



[コマンドによる設定]

1.**(config)# ipv6 access-list GROUP2**

```
(config-ipv6-acl)# permit ipv6 any ff35::/16
(config-ipv6-acl)# exit
```

VRF 10 で管理するグループアドレスのアクセスリスト（GROUP2）を作成します。

2. `(config)# ipv6 mld ssm-map vrf 10 static GROUP2 2001:db8:20::2`
   `(config)# ipv6 mld ssm-map vrf 10 static GROUP2 2001:db8:30::2`
   VPN 2 で PIM-SSM が動作するグループアドレスと，送信者 1 および送信者 2 の送信元アドレスを VRF 10 に設定します。管理するグループアドレスにはアクセスリスト（GROUP2）を指定します。
3. `(config)# ipv6 mld vrf 10 ssm-map enable`
   VRF 10 で MLD PIM-SSM 連携機能を有効にします。

27.1.16　VRF での MLD の設定

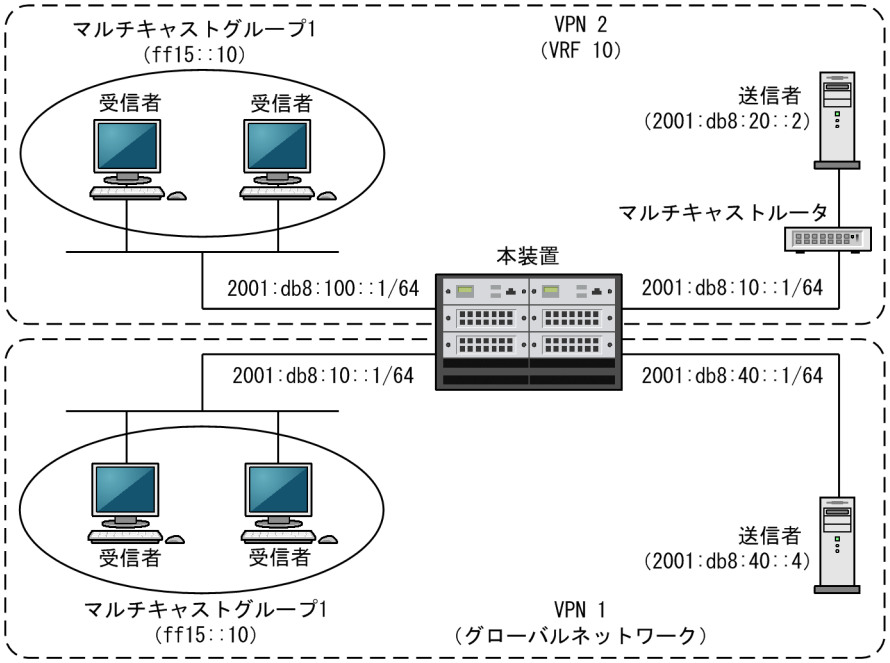
[設定のポイント]

VRF で MLD を動作させるには，該当 VRF のインタフェースに MLD を設定します。なお，該当 VRF のインタフェースに PIM-SM または PIM-SSM（ipv6 pim コマンド）を設定しても MLD は動作します。

デフォルトでは MLDv1 および MLDv2 混在モードです。MLD バージョンを変更する場合は，ipv6 mld version コマンドで設定してください。

VPN 2 に VRF 10 を対応させ，VRF 10 のインタフェースの IPv6 アドレスを 2001:db8:100::1/64 とした場合の MLD 構成例を次の図に示します。

図 27-4　VRF での MLD 構成例



[コマンドによる設定]

1. `(config)# interface gigabitethernet 1/1`
   ポート 1/1 のコンフィグレーションモードに移行します。
2. `(config-if)# vrf forwarding 10`
   ポート 1/1 に VRF 10 を設定します。

3. **(config-if)# ipv6 address 2001:db8:100::1/64**
   (config-if)# ipv6 enable
   ポート 1/1 に IPv6 アドレスを設定します。
4. **(config-if)# ipv6 mld router**
   (config-if)# exit
   ポート 1/1 に MLD を設定します。

27.1.17　IPv6 マルチキャストエクストラネットの設定

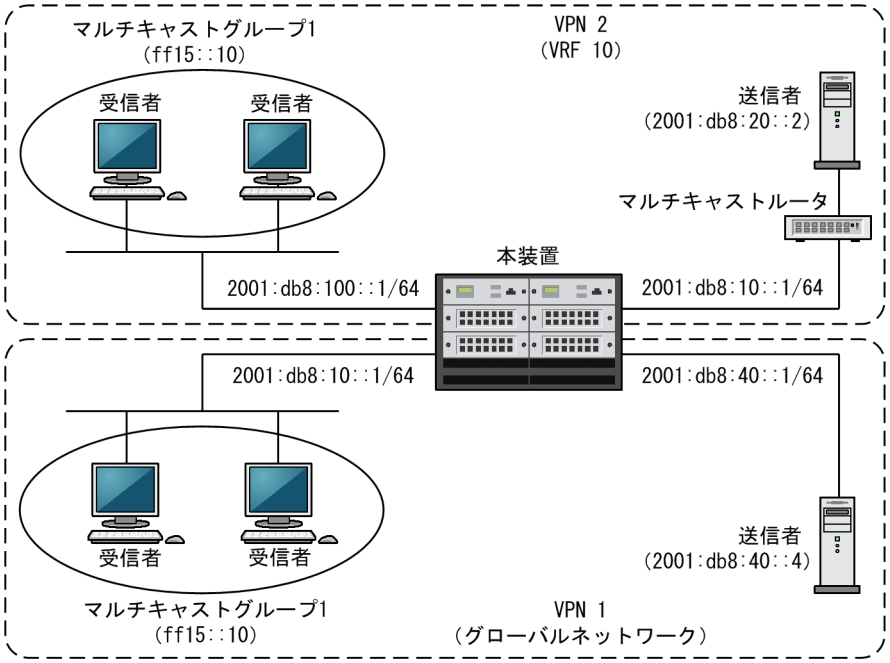
[設定のポイント]

マルチキャストエクストラネットでは，中継先 VRF に送信者へのユニキャストエクストラネットの設定があり，ユニキャスト経路が存在する必要があります。

送信者が存在する VRF にマルチキャスト経路フィルタリングを設定します。経路フィルタリングに条件を指定しない場合は，すべてのグループアドレスをマルチキャストが動作するすべての VRF へ中継できます。マルチキャスト経路フィルタリングはグローバルコンフィグレーションモードで設定します。

VPN 2 に VRF 10 を対応させ，VRF 10 のインタフェースの IPv6 アドレスを 2001:db8:100::1/64，2001:db8:10::1/64 とした場合の PIM-SSM 構成例を次の図に示します。この場合，VPN 1（グローバルネットワーク）に，VPN 2（VRF 10）上の送信者（2001:db8:20::2）へのユニキャスト経路が存在する必要があります。

図 27-5　VRF での PIM-SSM 構成例（エクストラネット）



[コマンドによる設定]

1. **(config)# route-map MLT6EXNET permit 10**
   (config-route-map)# exit
   すべてのマルチキャスト中継要求を許可する route-map を作成します。
2. **(config)# vrf definition 10**

```
(config-vrf)# ipv6 import multicast inter-vrf MLT6EXNET
(config-vrf)# exit
```

VRF 10 にすべての VRF からの IPv6 マルチキャスト中継要求を許可する設定をします。

27.2　オペレーション

27.2.1　運用コマンド一覧

IPv6 マルチキャストの運用コマンド一覧を次の表に示します。

表 27-2　運用コマンド一覧

コマンド名	説明
show ipv6 mcache (show ipv6 pim mcache)	IPv6 マルチキャスト中継エントリを表示します。
show ipv6 mroute	IPv6 マルチキャスト経路情報を表示します。
show ipv6 pim interface	IPv6 PIM のインタフェース情報を表示します。
show ipv6 pim neighbor	IPv6 マルチキャストインタフェースの隣接情報を表示します。
show ipv6 pim bsr	IPv6 PIM-SM ブートストラップルータ情報を表示します。
show ipv6 pim rp-mapping	IPv6 PIM-SM ランデブーポイント情報を表示します。
show ipv6 pim rp-hash	個別の IPv6 グループアドレスに対するランデブーポイント情報を表示します。
show ipv6 mld interface	MLD のインタフェース情報を表示します。
show ipv6 mld group	MLD のマルチキャストグループ情報を表示します。
clear ipv6 mld standby	待機系の IPv6 マルチキャスト同期情報をいったんクリアして，運用系の MLD マルチキャストグループ情報を待機系へ再同期します。
show ipv6 rpf	IPv6 PIM の RPF 情報を表示します。
show ipv6 multicast statistics	IPv6 マルチキャストの統計情報を表示します。
clear ipv6 multicast statistics	IPv6 マルチキャストの統計情報をクリアします。
show ipv6 multicast resources	IPv6 マルチキャストルーティング機能で使用している各種エントリ数を表示します。
restart ipv6-multicast	IPv6 マルチキャストルーティングプログラムを再起動します。
dump protocols ipv6-multicast	IPv6 マルチキャストルーティング機能のイベントトレース情報および制御テーブル情報のダンプを採取します。
erase protocol-dump ipv6-multicast	IPv6 マルチキャストルーティング機能のイベントトレース情報，制御テーブル情報およびコアファイルを削除します。

27.2.2　IPv6 PIM-SM 情報の確認

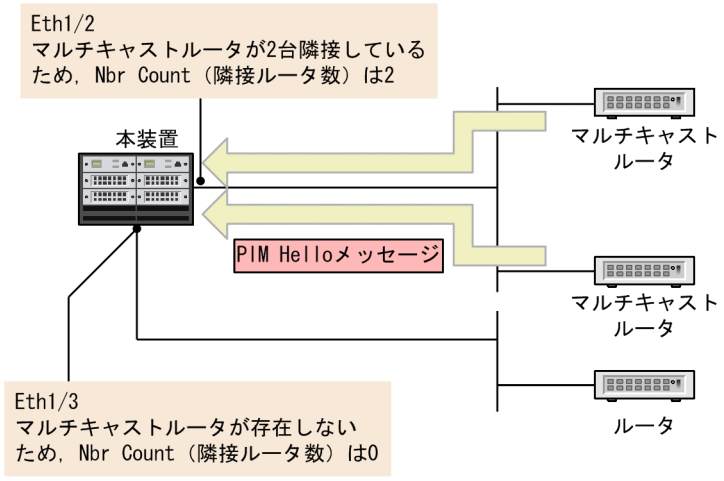
本装置の IPv6 マルチキャストルーティング機能で，PIM-SM を設定した場合の確認内容には次のものがあります。

(1)　インタフェース情報

本装置で PIM-SM および PIM-SSM のインタフェース情報を確認する場合は，show ipv6 pim interface コマンドを実行して，PIM-SM または PIM-SSM を設定したインタフェースが表示されることを確認してください。コマンドの実行結果を次の図に示します。

図 27-6　show ipv6 pim interface コマンドの実行結果

```
> show ipv6 pim interface
Date 20XX/01/13 10:01:00 UTC
Total: 2 interfaces
Interface  Mode   Hello  Nbr    DR
                  Intvl  Count  Address
Eth1/2     sparse    30      2  fe80::212:e2ff:fe08:6401
Eth1/3     sparse    30      0  This system
>
```

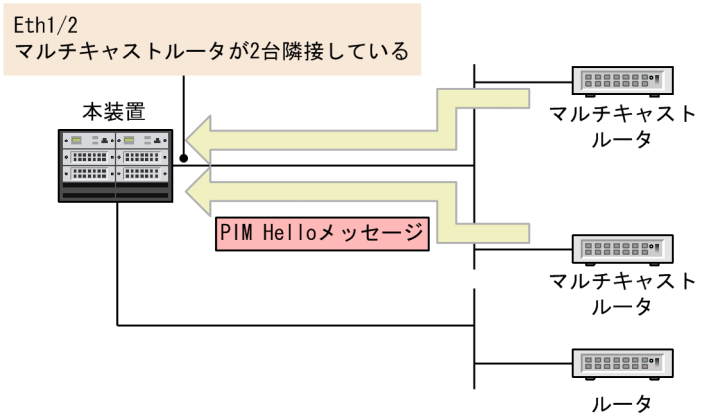


(2)　隣接情報

本装置でマルチキャストインタフェースの隣接情報を確認する場合は，show ipv6 pim neighbor コマンドを実行して，該当インタフェースの隣接ルータを確認してください。コマンドの実行結果を次の図に示します。

図 27-7　show ipv6 pim neighbor コマンドの実行結果

```
> show ipv6 pim neighbor
Date 20XX/12/10 17:16:12 UTC
Total: 2 neighbors
Interface  Neighbor Address          Uptime  Expires
Eth1/2     fe80::212:e2ff:fe08:6401   00:15   01:30
           fe80::212:e2ff:fe08:6402   00:05   01:40
>
```



(3)　マルチキャスト経路情報

本装置でマルチキャスト経路情報を確認する場合は，show ipv6 mroute コマンドを実行して，該当するマルチキャスト経路情報が存在することを確認してください。コマンドの実行結果を次の図に示します。

図 27-8　show ipv6 mroute コマンドの実行結果

```
> show ipv6 mroute
Date 20XX/01/13 10:01:00 UTC
Total: 2 routes, 2 groups, 1 source
(S,G) 2 routes ------------------------------------------------
Group Address                           Source Address
ff35::1                                 2001:db8::100
    flags:FLT  protocol:SSM  uptime: 08:18    expires: --:--    assert: 00:00
    incoming:Eth1/2           upstream:Direct
    outgoing:Eth1/3           uptime: 06:17    expires: --:--
             Eth1/4           uptime: 06:45    expires: --:--

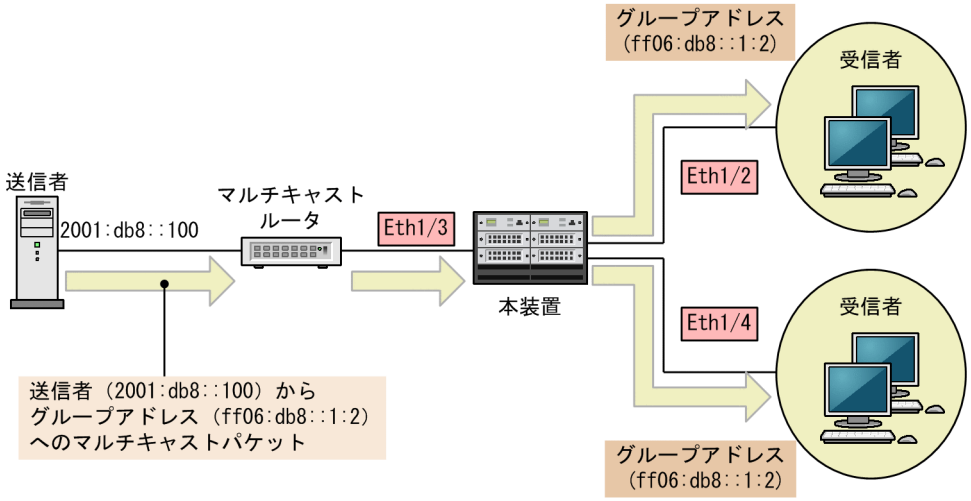
ff35::2                                 2001:db8::100
    flags:FLT  protocol:SSM  uptime: 08:18    expires: --:--    assert: 00:00
    incoming:Eth1/2           upstream:Direct
    outgoing:Eth1/3           uptime: 06:17    expires: --:--
             Eth1/4           uptime: 06:45    expires: --:--
>
```

(4)　マルチキャスト中継エントリ情報

本装置でマルチキャスト中継エントリを確認する場合は，show ipv6 mcache コマンドを実行して，グループアドレスへの経路が存在していることを確認してください。コマンドの実行結果を次の図に示します。

図 27-9　show ipv6 mcache コマンドの実行結果

```
> show ipv6 mcache
Date 20XX/01/13 10:01:00 UTC
Total: 1 route
- Forwarding entry  ---------------------------------------------------------
Group Address                            Source Address
ff06::db8:1:2                            2001:db8::100
    flags:-   protocol:SSM  uptime: 00:20  expires: --:--
    incoming:Eth1/3
    outgoing:Eth1/2
             Eth1/4
>
```

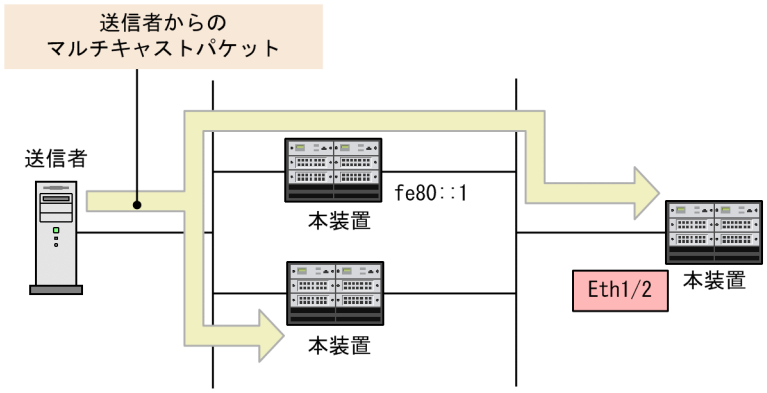


(5)　RPF 情報

本装置で PIM-SM および PIM-SSM の RPF 情報を確認する場合は，show ipv6 rpf コマンドを実行して，RPF 情報を確認してください。コマンドの実行結果を次の図に示します。

図 27-10　show ipv6 rpf コマンドの実行結果

```
> show ipv6 rpf 2001:db8::100
Date 20XX/01/13 10:01:00 UTC
Incoming:Eth1/2    Upstream: fe80::1
>
```



(6)　PIM-SM ブートストラップルータ情報

本装置で IPv6 PIM-SM ブートストラップルータ情報を確認する場合は，show ipv6 pim bsr コマンドを実行して，ブートストラップルータアドレスが表示されていることを確認してください。コマンドの実行結果を次の図に示します。

図 27-11　show ipv6 pim bsr コマンドの実行結果

```
> show ipv6 pim bsr
Date 20XX/01/13 10:01:00 UTC
Status:Not Candidate Bootstrap Router
BSR Address : 2001:db8:1::1
    Priority: 100    Hash mask length: 96
    Uptime  : 03:00
    Bootstrap Timeout : 130 seconds
>
```

(7)　PIM-SM ランデブーポイント情報

本装置で IPv6 PIM-SM ランデブーポイント情報を確認する場合は，show ipv6 pim rp-mapping コマンドを実行して，該当のグループアドレスに対するランデブーポイントアドレスが表示されていることを確認してください。コマンドの実行結果を次の図に示します。

図 27-12　show ipv6 pim rp-mapping コマンドの実行結果

```
> show ipv6 pim rp-mapping brief
Date 20XX/01/13 10:01:00 UTC
Status:Not Candidate Rendezvous Point
Total: 2 routes, 2 groups, 1 RP
Group/Masklen                C-RP Address
ff06:db8:2::/128             2001:db8:1::1
ff06:db8:1::/128             2001:db8:1::1
>
```

27.2.3　MLD 情報の確認

本装置の IPv6 マルチキャストルーティング機能で MLD を設定した場合の確認内容には次のものがあります。

(1)　インタフェース情報

本装置で MLD のインタフェース情報を確認する場合は，show ipv6 mld interface コマンドを実行して，MLD を設定したインタフェースが表示されることを確認してください。コマンドの実行結果を次の図に示します。

図 27-13　show ipv6 mld interface コマンドの実行結果

```
> show ipv6 mld interface
Date 20XX/01/13 10:01:00 UTC
Total: 5 Interfaces
Interface   Version   Querier                   Expires  Group Count  Notice
Eth1/1          1     fe80::212:e2ff:fe08:6401   02:30             4  L
Eth1/3          2     fe80::212:e2ff:fe08:6401   01:30             2
Eth1/4        (2)     This System                  -               5  QR
Eth1/5          1     fe80::212:e2ff:fe08:6401   01:00             3  Q
Eth1/6          1     fe80::212:e2ff:fe08:6401   02:30             6
>
```

(2)　グループアドレス情報

本装置で MLD のグループアドレス情報を確認する場合は，show ipv6 mld group コマンドを実行して，Group Address 欄のグループアドレスを確認してください。コマンドの実行結果を次の図に示します。

図 27-14　show ipv6 mld group コマンドの実行結果

```
> show ipv6 mld group brief
Date 20XX/01/13 10:01:00 UTC
Total: 4 groups
Group Address       Interface    Version  Mode  Source Count
ff15:100::50        Eth1/1           1    EXCLUDE          9
ff15:100::60        Eth1/3           2    INCLUDE          2
ff15:200::1         Eth1/3           1    EXCLUDE          0
ff15:200::2         Eth1/4           2    EXCLUDE          1
>
```

28 IPv6 マルチキャスト拡張機能

この章では，IPv6 マルチキャストの拡張機能について説明します。

28.1　マルチキャストチャネル参加制限機能の解説

28.1.1　概要

マルチキャストチャネル参加制限機能は，MLD を使用しているインタフェースでマルチキャストチャネル（グループアドレスおよび送信元アドレス）への参加条件を設定して，条件を超える参加を制限する機能です。マルチキャストチャネル参加制限機能の一覧を次の表に示します。

表 28–1　マルチキャストチャネル参加制限機能の一覧

機能名	制限する値
マルチキャストチャネルフィルタ機能	指定したマルチキャストチャネルだけ参加を許可
ソース数制限機能	ソース（送信元）数
マルチキャストグループ数制限機能	マルチキャストグループ数
マルチキャストチャネル数制限機能	指定したマルチキャストチャネルリスト内でのマルチキャストチャネル数
マルチキャストチャネル受信者数制限機能	マルチキャストチャネルの総受信者数
帯域管理機能	MLD インタフェースでの使用帯域

マルチキャストチャネル参加制限機能の共通動作を次に示します。

(1)　静的グループ参加機能の扱い

静的グループ参加機能で設定したエントリは，マルチキャストチャネル参加制限機能の対象外です。制限に関係なく，マルチキャストグループに参加できます。

(2)　MLD PIM-SSM 連携機能の扱い

MLD PIM-SSM 連携機能で設定したエントリは，マルチキャストチャネル参加制限機能の対象です。

MLD Report（参加要求）メッセージを受信して，MLD PIM-SSM 連携機能で複数の送信元アドレスと連携している場合，送信元アドレス数の上限値まではマルチキャストグループへの参加を許可して，上限値を超えると参加を拒否します。マルチキャストグループへの参加可否は，コンフィグレーションコマンド ipv6 mld ssm-map static の設定順に判定します。

静的グループ参加機能を設定しているマルチキャストグループに MLD PIM-SSM 連携機能を設定している場合は，制限に関係なくすべての送信元アドレスに対してマルチキャストグループへの参加を許可します。

(3)　コンフィグレーション変更時の動作

マルチキャストチャネルフィルタ機能の場合

コンフィグレーションの変更によって学習済みのマルチキャストチャネルがフィルタ条件に一致しなくなった場合，そのマルチキャストチャネルはタイムアウトするまで維持されます。この状態で離脱すると，該当するマルチキャストチャネルは参加できません。

マルチキャストチャネルフィルタ機能以外の場合

コンフィグレーションの変更によって学習済みのマルチキャストチャネルがフィルタ条件に一致しなくなった，または各機能で制限している値の使用数が上限値を超えた場合，学習済みのマルチキャスト

グループは離脱するまで維持されます。この状態で離脱すると，各機能で制限している値の使用数が上限値を下回るまで参加できません。

(4)　マルチキャストグループへの参加拒否時の動作

マルチキャストチャネルフィルタ機能の場合

参加が許可されていないマルチキャストチャネル宛ての MLD Report（参加要求）メッセージを受信した場合，マルチキャストグループへの参加を拒否します。このとき，該当する MLD Report（参加要求）メッセージを廃棄します。

マルチキャストチャネルフィルタ機能以外の場合

各機能で制限している値の使用数が上限値を超えた場合，マルチキャストグループへの参加を拒否します。このとき，該当する MLD Report（参加要求）メッセージを廃棄します。

MLD Report（参加要求）メッセージ廃棄時，および MLD Report（参加要求）メッセージ廃棄状態から回復時には，システムメッセージを出力します。

28.1.2　マルチキャストチャネルリストでのフィルタリング

マルチキャストチャネルフィルタ機能，マルチキャストチャネル数制限機能，および帯域管理機能では，マルチキャストチャネルリストを使用してマルチキャストチャネルの中継に関するマルチキャストグループへの参加をフィルタリングします。マルチキャストチャネルリストには，これらの機能の対象となるマルチキャストチャネルを設定します。マルチキャストチャネルリストについては，「(1)　マルチキャストチャネルリストの設定方法」を参照してください。

なお，使用するプロトコルによってフィルタリングの対象が異なります。

PIM-SM の場合

フィルタリングの対象は，グループアドレスだけです。

PIM-SSM の場合

フィルタリングの対象は，グループアドレスと送信元アドレスの組み合わせです。MLDv1 Report メッセージおよび MLDv2 Report（EXCLUDE モード）メッセージは送信元アドレスが不定なため，対象外になります。ただし，MLD PIM-SSM 連携機能を使用するとフィルタリングの対象になります。このときのフィルタリングの対象は，グループアドレスと送信元アドレスの組み合わせです。

(1)　マルチキャストチャネルリストの設定方法

マルチキャストチャネルリストは，コンフィグレーションコマンド ipv6 access-list を使用してアクセスリストで設定します。アクセスリストに設定する条件を次の表に示します。

表 28–2　アクセスリストに設定する条件

パラメータ	内容
アクセス可否条件	permit または deny を設定します。 permit の場合フィルタ条件が有効に，deny の場合フィルタ条件が無効になります。
シーケンス番号	シーケンス番号を設定します。シーケンス番号がフィルタリングの順番※1 になります。
フィルタ条件	• IPv6 パケットの上位プロトコル条件には，ipv6 を設定します。 • 送信元 IPv6 アドレスには，送信元アドレス※2 または any を設定します。 • 宛先 IPv6 アドレスには，グループアドレス※2 または any を設定します。

注※1

シーケンス番号順にフィルタリングします。そのため，アクセスリスト内に同一の(S,G)を設定している場合，シーケンス番号の小さいフィルタ条件に従ってフィルタリングします。

注※2

プレフィックスを指定できます。

(2)　MLD Report メッセージ受信時のフィルタリング

受信した MLD Report メッセージおよび使用するプロトコル（PIM-SM または PIM-SSM）によって，適用するフィルタ条件が異なります。MLDv1 Report メッセージおよび MLDv2 Report（EXCLUDE モード）メッセージで適用するフィルタ条件と，その判定方法を次の表に示します。

表 28-3　MLDv1 Report メッセージおよび MLDv2 Report（EXCLUDE モード）メッセージで適用するフィルタ条件と判定方法

プロトコル	MLD PIM-SSM 連携機能の設定	適用するフィルタ条件		判定方法
		送信元アドレス	宛先アドレス	
PIM-SM	なし	送信元アドレス	グループアドレス	一致しない※1
		any	グループアドレス	次のどちらも満たすと一致 • アクセス可否条件が permit • MLD Report メッセージのグループアドレスと一致
		送信元アドレス	any	一致しない※1
		any	any	アクセス可否条件が permit で一致
	あり	－	－	一致しない※2
PIM-SSM	なし	－	－	一致しない※3
	あり	送信元アドレス	グループアドレス	次のどちらも満たすと一致 • アクセス可否条件が permit • MLD PIM-SSM 連携機能の送信元アドレスおよび MLD Report メッセージのグループアドレスと一致
		any	グループアドレス	次のどちらも満たすと一致 • アクセス可否条件が permit • MLD Report メッセージのグループアドレスと一致
		送信元アドレス	any	次のどちらも満たすと一致 • アクセス可否条件が permit • MLD PIM-SSM 連携機能の送信元アドレスと一致
		any	any	アクセス可否条件が permit で一致

（凡例）　－：該当しない

注※1

MLDv1 Report メッセージおよび MLDv2 Report（EXCLUDE モード）メッセージでは送信元アドレスが不明なため，一致しません。

注※2

PIM-SM アドレスには MLD PIM-SSM 連携機能が設定できないため，一致しません。

注※3

MLD PIM-SSM 連携機能の設定がないため，一致しません。

MLDv2 Report（INCLUDE モード）メッセージで適用するフィルタ条件と，その判定方法を次の表に示します。

表 28-4　MLDv2 Report（INCLUDE モード）メッセージで適用するフィルタ条件と判定方法

プロトコル	適用するフィルタ条件		判定方法
	送信元アドレス	宛先アドレス	
PIM-SM	送信元アドレス	グループアドレス	一致しない※
	any	グループアドレス	次のどちらも満たすと一致 • アクセス可否条件が permit • MLD Report メッセージのグループアドレスと一致
	送信元アドレス	any	一致しない※
	any	any	アクセス可否条件が permit で一致
PIM-SSM	送信元アドレス	グループアドレス	次のどちらも満たすと一致 • アクセス可否条件が permit • MLD Report メッセージの送信元アドレスおよびグループアドレスと一致
	any	グループアドレス	次のどちらも満たすと一致 • アクセス可否条件が permit • MLD Report メッセージのグループアドレスと一致
	送信元アドレス	any	次のどちらも満たすと一致 • アクセス可否条件が permit • MLD Report メッセージの送信元アドレスと一致
	any	any	アクセス可否条件が permit で一致

注

CHANGE_TO_INCLUDE_MODE で送信元アドレス指定なし，および BLOCK_OLD_SOURCES は対象外です。

注※

PIM-SM ではフィルタ条件の送信元アドレスが any だけ対象のため，一致しません。

判定の結果，フィルタ条件に一致したと見なす場合，各機能で制限している値の使用数をカウントします。マルチキャストチャネルフィルタ機能の場合は参加を許可します。

(3)　MLD PIM-SSM 連携機能での送信元アドレス追加時のフィルタリング

MLD PIM-SSM 連携機能で送信元アドレスを追加した場合も，フィルタリングの対象になります。MLD PIM-SSM 連携機能で適用するフィルタ条件と，その判定方法を次の表に示します。

表 28–5　MLD PIM-SSM 連携機能で適用するフィルタ条件と判定方法

プロトコル	適用するフィルタ条件		判定方法
	送信元アドレス	宛先アドレス	
PIM-SM	－	－	一致しない※
PIM-SSM	送信元アドレス	グループアドレス	次のどちらも満たすと一致 • アクセス可否条件が permit • MLD PIM-SSM 連携機能で追加した送信元アドレスおよび連携しているグループアドレスと一致
	any	グループアドレス	次のどちらも満たすと一致 • アクセス可否条件が permit • 連携しているグループアドレスと一致
	送信元アドレス	any	次のどちらも満たすと一致 • アクセス可否条件が permit • MLD PIM-SSM 連携機能で追加した送信元アドレスと一致
	any	any	アクセス可否条件が permit で一致

（凡例）　－：該当しない

注※

PIM-SM アドレスには MLD PIM-SSM 連携機能が設定できないため，一致しません。

判定の結果，フィルタ条件に一致したと見なす場合，各機能で制限している値の使用数をカウントします。マルチキャストチャネルフィルタ機能の場合は参加を許可します。

(4)　マルチキャストチャネルリスト不一致時の動作

マルチキャストチャネルフィルタ機能の場合

参加対象のマルチキャストチャネルが，設定したすべてのマルチキャストチャネルリストに一致しない場合，マルチキャストグループへの参加を拒否します。

マルチキャストチャネルフィルタ機能以外の場合

参加対象のマルチキャストチャネルが，設定したすべてのマルチキャストチャネルリストに一致しない場合，該当する機能の対象外になります。

28.1.3　マルチキャストチャネルフィルタ機能

マルチキャストチャネルフィルタ機能は，MLD インタフェース単位でマルチキャストチャネルリストに設定したマルチキャストチャネルだけにマルチキャストグループへの参加を許可する機能です。

(1)　マルチキャストグループへの参加判定

コンフィグレーションコマンド ipv6 mld access-group で設定したマルチキャストチャネルリストと，受信した MLD Report（参加要求）メッセージを比較します。このとき，参加を要求したマルチキャストチャネルがマルチキャストチャネルリストに設定されている場合だけ，マルチキャストグループへの参加を許可します。

(2)　統計情報

本機能では，フィルタ条件に一致，またはすべてのフィルタ条件に不一致となった MLD Report（参加要求）メッセージの統計を収集します。収集した統計情報は運用コマンド show ipv6 mld access-group で確認できます。

28.1.4　ソース数・マルチキャストグループ数制限機能

ソース数・マルチキャストグループ数制限機能は，ソース（送信元）数またはマルチキャストグループ数の上限値を設定して，MLD インタフェース単位でマルチキャストグループへの参加を制限する機能です。

(1)　マルチキャストグループへの参加判定

MLD Report（参加要求）メッセージを受信すると，そこに含まれるすべてのソース参加要求とマルチキャストグループ参加要求を対象として，ソース登録数およびマルチキャストグループ登録数をカウントします。このとき，カウントした数が上限値以下の場合だけ，マルチキャストグループへの参加を許可します。

28.1.5　マルチキャストチャネル数制限機能

マルチキャストチャネル数制限機能は，MLD インタフェース単位でマルチキャストチャネルリストを設定して，設定したマルチキャストチャネルリスト内でマルチキャストグループに参加できるマルチキャストチャネル数を制限する機能です。

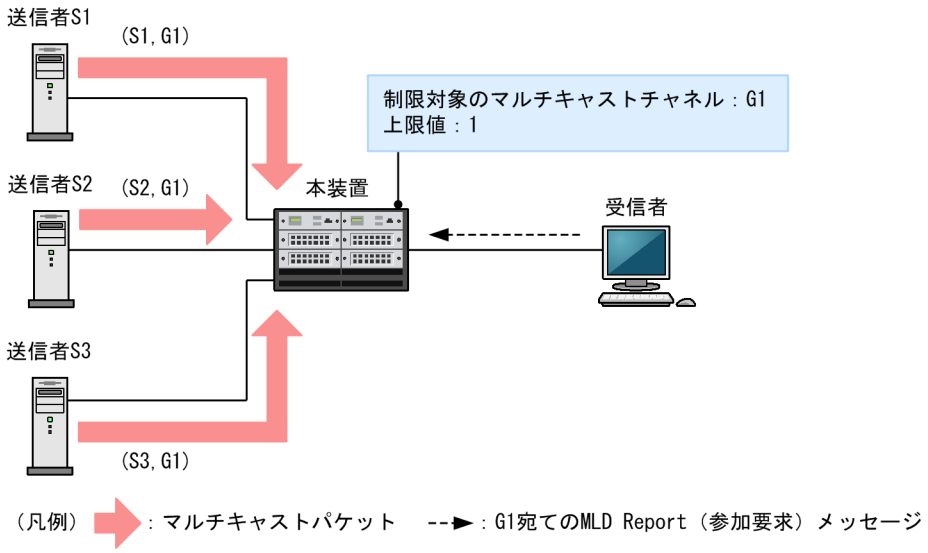
(1)　マルチキャストグループへの参加判定

コンフィグレーションコマンド ipv6 mld channel-limit で設定したマルチキャストチャネル数の上限値と，MLD Report（参加要求）メッセージの受信によってカウントした参加数を比較します。このとき，参加数が上限値以下の場合だけ，マルチキャストグループへの参加を許可します。

(2)　注意事項

本機能は MLD のマルチキャストグループ情報生成時に制限する機能です。そのため，PIM-SM で使用しているマルチキャストグループでは，マルチキャストグループへの参加が許可されたあとマルチキャストパケットの送信者が追加されると，上限値に関係なくマルチキャストチャネルの参加が許可されます。PIM-SM 使用時にマルチキャストチャネル数の上限値を超える例を次の図に示します。

図 28-1　PIM-SM 使用時にマルチキャストチャネル数の上限値を超える例



この例では，グループアドレス G1 を対象として，マルチキャストチャネル数の上限値を 1 に設定しています。受信者から G1 宛ての MLD Report（参加要求）メッセージを受信すると，上限値を超えないため G1 の参加が許可されます。その後，G1 の送信者 S1，S2，S3 が追加されると，上限値を超えた(S1,G1)，(S2,G1)，(S3,G1)の 3 チャネルも参加が許可されます。このように，PIM-SM では，送信者が追加されると上限値を超過して中継されます。

28.1.6　マルチキャストチャネル受信者数制限機能

マルチキャストチャネル受信者数制限機能は，マルチキャストチャネルの総受信者数の上限値を設定して，VRF，グローバルネットワーク，または MLD インタフェース単位でマルチキャストチャネルに参加する受信者数を制限する機能です。

本機能は，コンフィグレーションコマンド ipv6 mld explicit-tracking で limit パラメータまたは total-limit パラメータを設定すると有効になります。limit パラメータでは MLD インタフェース単位，total-limit パラメータでは VRF またはグローバルネットワーク単位で制限します。

(1)　MLD Report（参加要求）メッセージ受信時のマルチキャストチャネル受信者数のカウント方法

コンフィグレーションコマンド ipv6 mld explicit-tracking を設定したインタフェースで MLD Report（参加要求）メッセージを受信すると，マルチキャストチャネル単位で受信者情報を保持します。このとき，MLD インタフェース単位のマルチキャストチャネル受信者数，および VRF またはグローバルネットワーク当たりのマルチキャストチャネル受信者数をカウントします。MLD Report（参加要求）メッセージごとのマルチキャストチャネル受信者数のカウント方法を次の表に示します。

表 28-6　MLD Report（参加要求）メッセージごとのマルチキャストチャネル受信者数のカウント方法

MLD バージョン	Record タイプ	カウント方法
MLDv1	−	グループアドレスだけで 1 カウント
MLDv2	MODE_IS_INCLUDE	送信元アドレスとグループアドレスの組で 1 カウント

MLD バージョン	Record タイプ	カウント方法
	MODE_IS_EXCLUDE	グループアドレスだけで 1 カウント
	CHANGE_TO_INCLUDE_MODE	送信元アドレスとグループアドレスの組で 1 カウント※1
	CHANGE_TO_EXCLUDE_MODE	グループアドレスだけで 1 カウント
	ALLOW_NEW_SOURCES	送信元アドレスとグループアドレスの組で 1 カウント
	BLOCK_OLD_SOURCES	―※2

（凡例）　―：該当しない

注※1

送信元アドレスの指定がない場合は対象外です。

注※2

対象外です。

(2)　マルチキャストチャネル受信者の追加判定

MLD インタフェースに設定した上限値，および VRF またはグローバルネットワークに設定した上限値と，MLD Report（参加要求）メッセージの受信によってカウントしたマルチキャストチャネル受信者数を比較します。このとき，マルチキャストチャネル受信者数が上限値以下の場合だけ，マルチキャストチャネル受信者の追加を許可します。

(3)　MLDv1 での動作

コンフィグレーションコマンド ipv6 mld version で MLD バージョンを version 1 に設定しているインタフェースでは，本機能は無効になります。

28.1.7　帯域管理機能

帯域管理機能は，対象となるマルチキャストチャネルリストに帯域値を設定して，該当するマルチキャストチャネルの学習時に帯域値を集計することで，MLD インタフェース単位で帯域上限値を超えるマルチキャストグループへの参加を制限する機能です。

(1)　マルチキャストチャネルリストへの帯域値の割り当て

マルチキャストチャネルが使用する帯域値は，マルチキャストチャネルリストに設定した帯域値によって決定します。マルチキャストチャネルリストの帯域値は，コンフィグレーションコマンド ipv6 multicast bandwidth で VRF またはグローバルネットワーク単位に設定します。

同じマルチキャストチャネルを複数のマルチキャストチャネルリストに設定している場合，ipv6 multicast bandwidth コマンド設定時のシーケンス番号が小さい帯域値を優先します。

(2)　帯域管理対象のマルチキャストチャネルリストの設定

帯域管理対象のマルチキャストチャネルリストは，コンフィグレーションコマンド ipv6 mld bandwidth-limit-filter で指定します。マルチキャストチャネルリストを指定しない場合，該当する VRF またはグローバルネットワークに設定したすべての帯域管理対象のマルチキャストチャネルリストが対象になります。

(3)　マルチキャストグループへの参加判定

設定した帯域上限値と，MLD Report（参加要求）メッセージの受信によって集計した使用中の帯域値を比較します。このとき，使用中の帯域値が帯域上限値以下の場合だけ，マルチキャストグループへの参加を許可します。

(4)　注意事項

- 本機能は，コンフィグレーションでマルチキャストチャネルに設定した帯域値に基づいて，マルチキャストグループへの参加可否を判断する機能です。実際のマルチキャストパケットのトラフィック量を確認する機能ではありません。
- PIM-SM では，MLD Report（参加要求）メッセージの受信時に今後生成される経路を認識できません。そのため，本機能を PIM-SM で使用する場合は，該当するマルチキャストグループに対して何台の送信者からマルチキャストパケットが配信されるかを予測して，予測した帯域の合計値をマルチキャストチャネルの帯域値に設定してください。
- BCU を二重化構成で運用している場合，警告閾値を超えたためにシステムメッセージが出力されたあと，警告閾値は下回ったが回復閾値を下回っていない状態で BCU が系切替したときは，そのあとに回復閾値を下回っても回復のシステムメッセージは出力されません。

28.1.8　マルチキャストチャネル参加制限機能の処理順序

マルチキャストチャネル参加制限機能の処理順序を，優先順位が高い順に次に示します。

1. マルチキャストチャネルフィルタ機能
2. マルチキャストグループ数制限機能
3. ソース数制限機能
4. マルチキャストチャネル数制限機能
5. 帯域管理機能
6. MLD インタフェース単位のマルチキャストチャネル受信者数制限機能
7. VRF またはグローバルネットワーク単位のマルチキャストチャネル受信者数制限機能

この優先順で各機能の上限値と比較します。制限を超えた場合，以降の機能については比較しません。

28.1.9　系切替時の参加制限状態の維持

BCU 二重化構成で IPv6 マルチキャストの無停止マルチキャスト中継機能を使用している場合，マルチキャストチャネル参加制限機能で管理する情報を運用系 BCU と待機系 BCU で同期します。そのため，マルチキャストチャネル参加制限機能でマルチキャストグループへの参加を制限している状態で系切替が発生した場合でも，旧運用系 BCU での参加制限状態を新運用系 BCU で維持します。

なお，MLD プロトコル自体は運用系 BCU と待機系 BCU で同期しないため，系切替後には MLD マルチキャストグループを再学習します。

28.2　マルチキャストチャネル参加制限機能のコンフィグレーション

28.2.1　コンフィグレーションコマンド一覧

マルチキャストチャネル参加制限機能のコンフィグレーションコマンド一覧を次の表に示します。

表 28–7　コンフィグレーションコマンド一覧

コマンド名	説明
ipv6 mld access-group	マルチキャストチャネルフィルタ機能で参加を許可するマルチキャストチャネルを設定します。
ipv6 mld bandwidth-limit	帯域管理機能の上限値を設定します。
ipv6 mld bandwidth-limit-filter	帯域管理対象のマルチキャストチャネルを設定します。
ipv6 mld channel-limit	マルチキャストチャネル数制限機能の上限値を設定します。
ipv6 mld channel-limit-filter	マルチキャストチャネル数制限機能の対象となるマルチキャストチャネルを設定します。
ipv6 mld explicit-tracking	マルチキャストチャネル受信者数制限機能の上限値を設定します。
ipv6 multicast bandwidth	帯域管理対象のマルチキャストチャネルに帯域値を設定します。

28.2.2　コンフィグレーションの流れ

使用する機能によって次の設定例を参照してください。

- **マルチキャストチャネルフィルタ機能を使用する場合**
  - マルチキャストチャネルリストの設定
  - マルチキャストチャネルフィルタ機能の設定
- **ソース数制限機能を使用する場合**
  - ソース数制限機能の設定
- **マルチキャストグループ数制限機能を使用する場合**
  - マルチキャストグループ数制限機能の設定
- **マルチキャストチャネル数制限機能を使用する場合**
  - マルチキャストチャネルリストの設定
  - マルチキャストチャネル数制限機能の設定
- **マルチキャストチャネル受信者数制限機能を使用する場合**
  - マルチキャストチャネル受信者数制限機能の設定
- **帯域管理機能を使用する場合**
  - マルチキャストチャネルリストの設定
  - マルチキャストチャネルへの帯域値の設定
  - 帯域管理機能の設定

28.2.3　マルチキャストチャネルリストの設定

[設定のポイント]

マルチキャストチャネルリストをアクセスリストで設定します。

[コマンドによる設定]

1. **(config)# ipv6 access-list MOVIE1**
   (config-ipv6-acl)# permit ipv6 host 2001:db8:20::100 host ff35::100
   (config-ipv6-acl)# permit ipv6 host 2001:db8:20::200 host ff35::200
   (config-ipv6-acl)# deny ipv6 host 2001:db8:20::300 host ff35::300
   (config-ipv6-acl)# exit
   マルチキャストチャネルリスト（MOVIE1）に，送信元アドレスおよびグループアドレスを設定します。送信元アドレス 2001:db8:20::300，グループアドレス ff35::300 のフィルタ条件は deny 指定のため，無効になります。

28.2.4　マルチキャストチャネルへの帯域値の設定

[設定のポイント]

マルチキャストチャネルに帯域値を設定します。設定した帯域値は，マルチキャストチャネルリストに設定したすべてのマルチキャストチャネルに適用されます。

[コマンドによる設定]

1. **(config)# ipv6 multicast bandwidth MOVIE1 1M 10**
   グローバルネットワークで使用するマルチキャストチャネルリスト（MOVIE1）の帯域値を 1Mbit/s に設定します。この設定によって，MOVIE1 に設定したマルチキャストチャネルには帯域値 1Mbit/s が適用されます。
2. **(config)# ipv6 multicast vrf 10 bandwidth MOVIE1 1M 10**
   VRF 10 で使用するマルチキャストチャネルリスト（MOVIE1）の帯域値を 1Mbit/s に設定します。この設定によって, MOVIE1 に設定したマルチキャストチャネルには帯域値 1Mbit/s が適用されます。

28.2.5　マルチキャストチャネルフィルタ機能の設定

[設定のポイント]

MLD インタフェースにマルチキャストチャネルリストを設定して，設定したマルチキャストチャネル以外のマルチキャストグループへの参加を制限します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   MLD を使用しているポート 1/1 のコンフィグレーションモードに移行します。
2. **(config-if)# ipv6 mld access-group MOVIE1**
   ポート 1/1 でマルチキャストグループへの参加を許可するマルチキャストチャネルリスト（MOVIE1）を設定します。この設定によって，ポート 1/1 では MOVIE1 に設定したマルチキャストチャネルだけにマルチキャストグループへの参加を許可します。

28.2.6　ソース数制限機能の設定

[設定のポイント]

MLD インタフェースにソース（送信元）数の上限値を設定して，上限値を超えるマルチキャストグループへの参加を制限します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   MLD を使用しているポート 1/1 のコンフィグレーションモードに移行します。
2. **(config-if)# ipv6 mld source-limit 50**
   ポート 1/1 でソース数の上限値を 50 に設定します。

28.2.7　マルチキャストグループ数制限機能の設定

[設定のポイント]

MLD インタフェースにマルチキャストグループ数の上限値を設定して，上限値を超えるマルチキャストグループへの参加を制限します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   MLD を使用しているポート 1/1 のコンフィグレーションモードに移行します。
2. **(config-if)# ipv6 mld group-limit 50**
   ポート 1/1 でマルチキャストグループ数の上限値を 50 に設定します。

28.2.8　マルチキャストチャネル数制限機能の設定

[設定のポイント]

MLD インタフェースにマルチキャストチャネルリスト，およびマルチキャストグループに参加できるマルチキャストチャネル数の上限値を設定して，設定したマルチキャストチャネルリスト内で上限値を超えるマルチキャストグループへの参加を制限します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   MLD を使用しているポート 1/1 のコンフィグレーションモードに移行します。
2. **(config-if)# ipv6 mld channel-limit 1**
   ポート 1/1 でマルチキャストチャネル数の上限値を 1 に設定します。
3. **(config-if)# ipv6 mld channel-limit-filter MOVIE1**
   ポート 1/1 でマルチキャストチャネル数制限の対象となるマルチキャストチャネルリスト（MOVIE1）を設定します。この設定によって，マルチキャストチャネル数制限の対象は MOVIE1 で設定したマルチキャストチャネルになります。また，MOVIE1 に設定したマルチキャストチャネル内で 1 チャネルまで，マルチキャストグループへの参加を許可します。

28.2.9　マルチキャストチャネル受信者数制限機能の設定

[設定のポイント]

VRF，グローバルネットワーク，または MLD インタフェース単位でマルチキャストチャネル受信者数の上限値を設定して，上限値を超える受信者の参加を制限します。

[コマンドによる設定]

1. **(config)# ipv6 mld vrf 10 explicit-tracking total-limit 500**
   VRF 10 のマルチキャストチャネル受信者数の上限値を 500 に設定します。
2. **(config)# interface gigabitethernet 1/1**
   MLD を使用しているポート 1/1 のコンフィグレーションモードに移行します。
3. **(config-if)# ipv6 mld explicit-tracking limit 50**
   ポート 1/1 でマルチキャストチャネル受信者数の上限値を 50 に設定します。

28.2.10　帯域管理機能の設定

[設定のポイント]

MLD インタフェースに帯域上限値を設定して，帯域値を設定したマルチキャストチャネルについて，帯域上限値を超えるマルチキャストグループへの参加を制限します。

MLD インタフェースでは，帯域管理機能の対象となるマルチキャストチャネルリストを指定できます。マルチキャストチャネルリストを指定しない場合，該当するグローバルネットワークで帯域値を設定したすべてのマルチキャストチャネルリストが帯域管理の対象になります。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   MLD を使用しているポート 1/1 のコンフィグレーションモードに移行します。
2. **(config-if)# ipv6 mld bandwidth-limit 1500**
   ポート 1/1 で帯域上限値を 1500kbit/s に設定します。
3. **(config-if)# ipv6 mld bandwidth-limit-filter MOVIE1**
   ポート 1/1 で帯域管理の対象となるマルチキャストチャネルリスト（MOVIE1）を設定します。この設定によって，帯域管理の対象は MOVIE1 で設定したマルチキャストチャネルになります。また，使用帯域値の合計が 1500kbit/s になるまで，マルチキャストグループへの参加を許可します。
   なお，MOVIE1 以外のマルチキャストチャネルは 0kbit/s と見なすため帯域管理の対象外となり，上限値に関係なくマルチキャストグループへの参加を許可します。

28.3　ホストトラッキング機能の解説

28.3.1　概要

ホストトラッキング機能は，MLD 即時離脱機能の拡張機能です。

本機能を使用すると，本装置が Querier，Non-Querier に関係なく，マルチキャストグループに参加している最後の受信者からの MLDv2 Report（離脱要求）メッセージ受信時に，該当するマルチキャストグループ情報を削除します。MLDv2 Report（離脱要求）メッセージ受信時に，最後の受信者からであることを確認してマルチキャストグループ情報を削除するため，複数の受信者が存在する場合でもほかの受信者へのマルチキャスト中継が停止することなく，即時離脱処理ができます。

ホストトラッキング機能を使用する場合は，コンフィグレーションコマンド ipv6 mld version で該当するインタフェースの MLD バージョンを version 2 または version 2 only に設定してください。

28.3.2　注意事項

- ホストトラッキング機能と MLD 即時離脱機能を同時に設定した場合，ホストトラッキング機能が優先されます。
- ホストトラッキング機能を設定したあと，Multicast Address Listening Interval が経過する（すべての受信者情報を収集する）までの間は，即時離脱処理をしません。
- ホストトラッキング機能を設定したあと，Multicast Address Listening Interval が経過するまでに系切替した場合，新運用系では受信者情報の収集を終了して，即時離脱処理を開始します。そのため，系切替直後のマルチキャストグループ離脱時に，該当するマルチキャストグループに参加している受信者へのマルチキャスト通信が停止するおそれがあります。

28.4　ホストトラッキング機能のコンフィグレーション

28.4.1　コンフィグレーションコマンド一覧

ホストトラッキング機能のコンフィグレーションコマンド一覧を次の表に示します。

表 28-8　コンフィグレーションコマンド一覧

コマンド名	説明
ipv6 mld explicit-tracking	インタフェースでホストトラッキング機能を有効にします。

28.4.2　ホストトラッキング機能の設定

[設定のポイント]

ホストトラッキング機能を使用する場合は，MLD インタフェースにホストトラッキング機能を設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   MLD を使用しているポート 1/1 のコンフィグレーションモードに移行します。
2. **(config-if)# ipv6 mld explicit-tracking**
   ポート 1/1 にホストトラッキング機能を設定します。

28.5　IPv6 マルチキャスト拡張機能のオペレーション

28.5.1　運用コマンド一覧

IPv6 マルチキャスト拡張機能の運用コマンド一覧を次の表に示します。

表 28-9　運用コマンド一覧

コマンド名	説明
show ipv6 mld group	explicit パラメータを指定して，ホストトラッキング機能の受信者情報を表示します。
show ipv6 mld bandwidth	帯域管理機能の情報を表示します。
show ipv6 mld access-group	マルチキャストチャネルフィルタ機能の統計情報を表示します。
clear ipv6 mld access-group	マルチキャストチャネルフィルタ機能の統計情報をクリアします。

28.5.2　マルチキャストチャネルフィルタの統計情報の確認

show ipv6 mld access-group コマンドで，マルチキャストチャネルフィルタの統計情報を確認します。

図 28-2　show ipv6 mld access-group コマンドの実行結果

```
> show ipv6 mld access-group
Date 20XX/01/13 10:01:00 UTC
Total: 2 Interfaces
Interface Name: Eth1/1
    Multicast Channel List     Sequence    Hit Counts
    MOVIE1                           10          1827
    MOVIE2                           20            51
    Discards (mismatch)                            30

Interface Name: Eth1/2
    Multicast Channel List     Sequence    Hit Counts
    MOVIE1                           10            15
    MOVIE2                           20           223
    Discards (mismatch)                           123
>
```

28.5.3　帯域管理情報の確認

show ipv6 mld bandwidth コマンドで interface パラメータを指定して，MLD インタフェース単位の帯域管理情報を確認します。

図 28-3　show ipv6 mld bandwidth コマンド（interface パラメータ指定）の実行結果

```
> show ipv6 mld bandwidth interface
Date 20XX/01/13 10:01:00 UTC
Total: 2 Interfaces
Interface Name: Eth1/1
    Max Rate     :   10000000 kbit/s
    Current Rate :    1256024 kbit/s
Interface Name: Eth1/2
    Max Rate     :   12000000 kbit/s
    Current Rate :      54226 kbit/s
>
```

28.5.4　ホストトラッキング機能の受信者情報の確認

show ipv6 mld group コマンドで explicit パラメータを指定して，ホストトラッキング機能の受信者情報を確認します。

図 28-4　show ipv6 mld group コマンド（explicit パラメータ指定）の実行結果

```
>show ipv6 mld group explicit
Date 20XX/04/20 12:10:10 UTC
Total: 3 groups, 7 host-channels
Group Address/Source Address/Host Address Interface Flags Uptime Expires
ff15::1                                   Eth1/11   1E     05:05   04:25
    *fe80::1                               -        2E     00:20   04:25
    *fe80::4                               -        1E     00:20   04:25
  2001:db8::4                              -                05:15   04:25
    *fe80::2                               -        2I     00:20   04:05
    *fe80::3                               -        2I     00:20   04:25
  2001:db8::5                              -                05:05   04:15
    *fe80::2                               -        2I     00:20   04:15
    *fe80::3                               -        2I     00:20   04:10
ff15::2                                   Eth1/12   2E H   00:20   00:20
    *fe80::2                               -        2E     00:20   04:25
ff15::4                                   Eth1/13   1ES    05:15   --:--
  2001:db8::1                              -          S    05:15   --:--
>
```

29 マルチキャスト経路フィルタリング

この章では，IPv4 マルチキャストルーティングおよび IPv6 マルチキャストルーティングの経路を対象とする経路フィルタリングの解説と操作方法について説明します。

29.1　解説

29.1.1　マルチキャスト経路フィルタリング概説

マルチキャスト経路フィルタリングは, マルチキャスト経路をフィルタに通すことで経路を制御する機能です。本機能はマルチキャストエクストラネットだけで使用します。

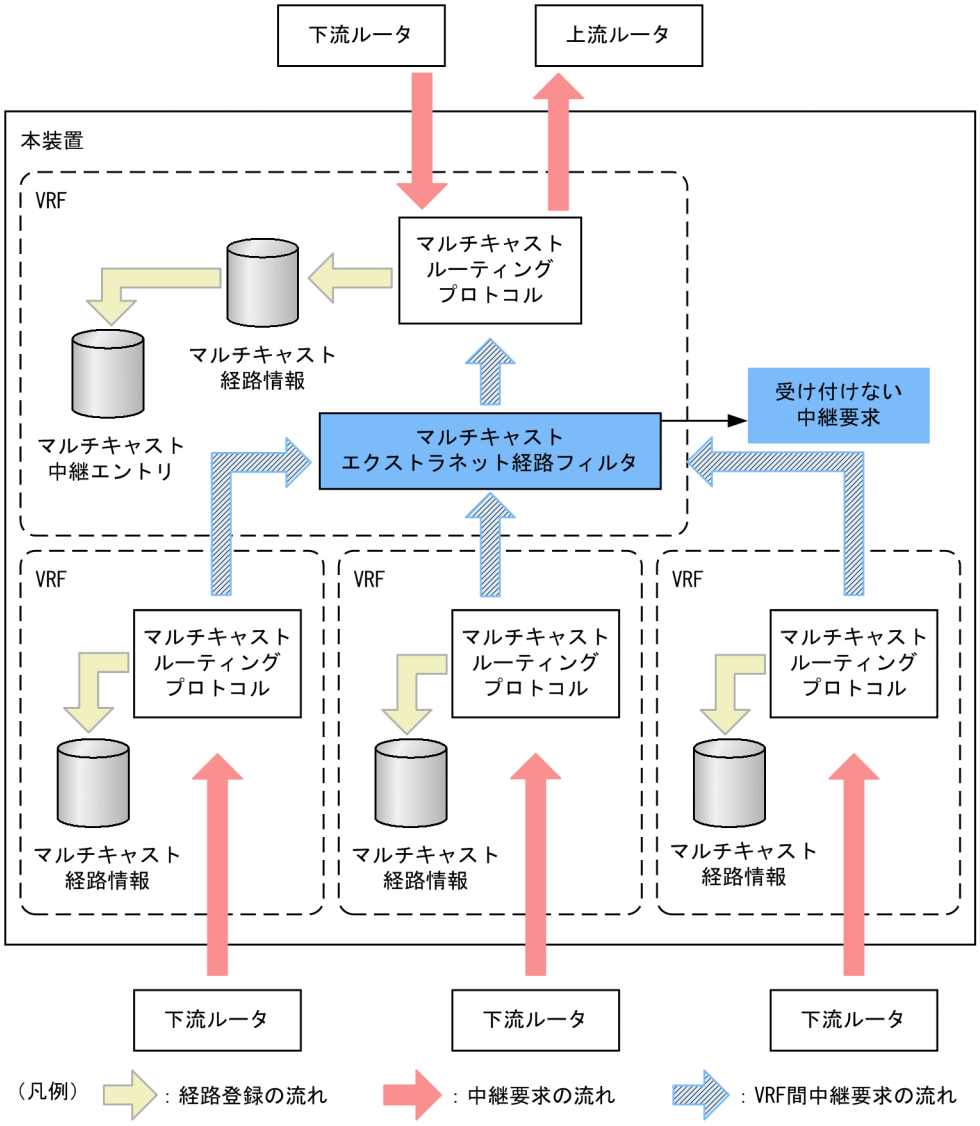
(1)　マルチキャストエクストラネットの経路フィルタリング

マルチキャストエクストラネットを実現するには，異なる VRF 間で中継要求を受け渡す必要があります。本装置では，VRF のルーティングプロトコル間で中継要求を交換する方法を使用します。マルチキャストエクストラネットの経路フィルタリングでは，中継要求を VRF のルーティングプロトコル間でフィルタします。この機能によって，VRF 間でマルチキャストパケットのグループアドレスごとに中継要求を受け付けるかどうか制御できます。なお, マルチキャストルーティングプロトコルは送信元アドレスについてユニキャストエクストラネットのルーティング情報を参照するため, ユニキャストエクストラネット経路フィルタに従います。

エクストラネットの経路フィルタリングを設定していない場合，VRF 間の中継要求をすべて廃棄します。

エクストラネットの経路フィルタリングの概念を次の図に示します。

図 29-1　マルチキャストエクストラネットの経路フィルタリングの概念図



29.1.2　マルチキャストフィルタ方法

マルチキャストフィルタ方法については「23.1.2　フィルタ方法」を参照してください。

マルチキャストフィルタでのコンフィグレーションコマンドに対する動作を次の表に示します。

表 29-1　マルチキャストフィルタでのコンフィグレーションコマンドに対する動作

コンフィグレーションコマンド	説明
ip access-list standard	permit だけを使用します。 deny を指定した IPv4 アドレスは無視します。
ipv6 access-list	permit だけを使用します。 deny を指定した IPv6 アドレスは無視します。
route-map	permit だけを使用します。 deny を指定した route-map は無視します。

経路フィルタリングのコンフィグレーションコマンドのうち，サポートしているのはこの表に記載しているコマンドだけです。その他のコマンドを指定した場合は無視します。

29.1.3　マルチキャストエクストラネット

(1)　VRF 間経路フィルタリング

VRF 間で導入する経路をフィルタできます。フィルタした結果，導入しないことになった経路はマルチキャスト経路情報を生成しません。

(a)　フィルタの適用方法

上流側 VRF に設定します。中継先 VRF からの経路通知に対して，許可するグループアドレスをコンフィグレーションコマンドの設定に従ってフィルタします。フィルタした結果が permit である場合，経路をマルチキャスト経路情報に導入します。適用するフィルタがない場合，経路を導入しません。

マルチキャスト VRF 間経路フィルタリングに使うコンフィグレーションコマンドを次の表に示します。

表 29–2　マルチキャスト VRF 間経路フィルタリングのコンフィグレーションコマンド

コマンド名	フィルタ対象経路
import multicast inter-vrf	route-map に指定された VRF からの中継要求がフィルタリング対象になります。
ipv6 import multicast inter-vrf	route-map に指定された VRF からの中継要求がフィルタリング対象になります。

マルチキャストエクストラネットでの route-map のフィルタ条件を次の表に示します。これ以外の条件は無視します。

表 29–3　マルチキャストエクストラネットでの route-map のフィルタ条件

条件となる経路属性	説明	コンフィグレーションコマンド
グループアドレス	指定したアクセスリストを条件として，指定したフィルタでグループアドレスをフィルタします。 フィルタの動作が permit の場合，一致したと見なします。 本条件を設定しない場合，すべてのグループアドレスが許可対象になります。	match ip address ip access-list standard match ipv6 address ipv6 access-list
VRF ID	VRF ID を条件として指定して，経路の VRF ID と比較します。これで指定した VRF からの中継要求を許可します。 本コマンドを設定した VRF と同じ ID を指定した場合，その ID だけ無視します。これによって，複数の VRF をグループ化して共通の route-map を使用できます。 本条件を設定しない場合，すべての VRF からの中継要求を許可します。	match vrf

(b)　VRF 間経路の設定

VRF 間経路フィルタを指定します。フィルタ条件に従って，他 VRF またはグローバルネットワークから中継要求のあった経路を自 VRF のマルチキャスト経路情報に導入します。導入した経路は導入先マルチ

キャスト経路情報の中継先インタフェースに追加されます。マルチキャスト VRF 間経路フィルタにコンフィグレーションコマンド match vrf を指定した場合，中継要求元の VRF ID と条件比較します。match vrf コマンドを指定しない場合，他 VRF またはグローバルネットワークすべてでフィルタ条件は同じになります。

(c)　プロトコルでの VRF 間経路の広告

VRF に経路フィルタを設定すると，他 VRF またはグローバルネットワークからの中継要求を許可できます。他 VRF またはグローバルネットワークから中継要求を受けてフィルタした結果許可された場合，マルチキャスト経路情報を生成して，上流ルータがあれば上流ルータに中継要求を送信します。

他 VRF またはグローバルネットワークが自 VRF に中継要求を送信するためには，ユニキャストエクストラネットで，中継要求元となる VRF に送信元アドレスへの経路を自 VRF となるように設定します。

29.2　コンフィグレーション

29.2.1　コンフィグレーションコマンド一覧

マルチキャスト経路フィルタリングのコンフィグレーションコマンド一覧を次の表に示します。

表 29-4　コンフィグレーションコマンド一覧

コマンド名	説明
ip access-list standard※1	IPv4 アドレスフィルタとして動作するアクセスリストを設定します。
ipv6 access-list※1	IPv6 アドレスフィルタとして動作するアクセスリストを設定します。
import multicast inter-vrf※2	他 VRF またはグローバルネットワークからのマルチキャスト中継要求をフィルタに従って制御します。
ipv6 import multicast inter-vrf※2	他 VRF またはグローバルネットワークからのマルチキャスト中継要求をフィルタに従って制御します。
match ip address※3	route-map にグループアドレスによるフィルタ条件を設定します。
match ipv6 address※3	route-map にグループアドレスによるフィルタ条件を設定します。
match vrf※3	route-map に VRF によるフィルタ条件を設定します。

注※1

「コンフィグレーションコマンドレファレンス Vol.2　7. アクセスリスト」を参照してください。

注※2

「コンフィグレーションコマンドレファレンス Vol.3　5. VRF」を参照してください。

注※3

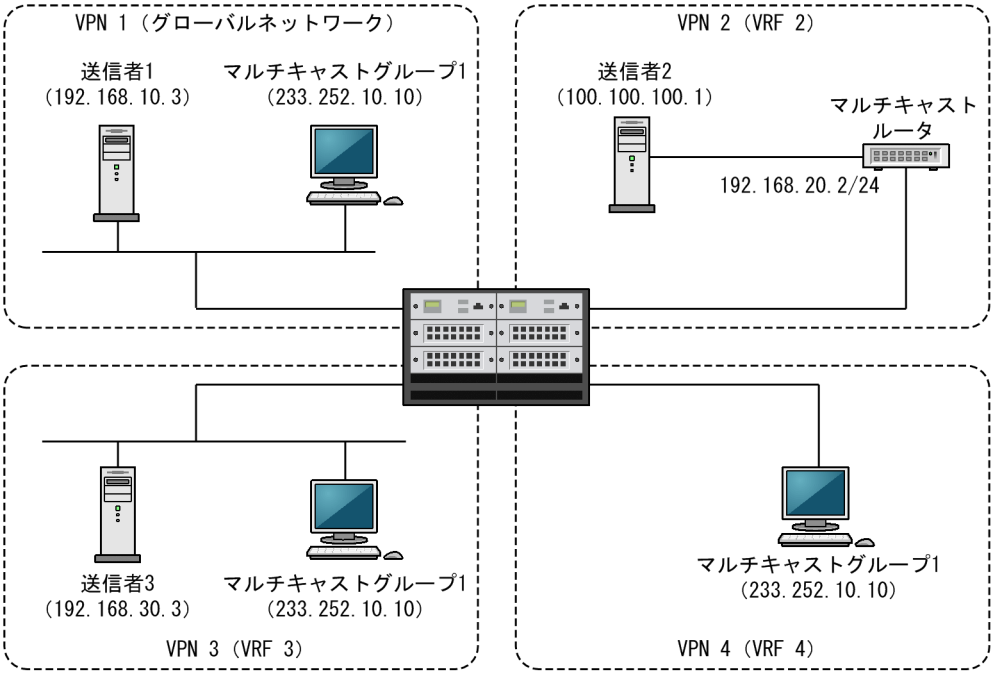
「コンフィグレーションコマンドレファレンス Vol.3　22. 経路フィルタリング」を参照してください。

29.2.2　IPv4 マルチキャストエクストラネットの設定

次の図のようなネットワーク構成で，マルチキャストエクストラネットを設定します。

マルチキャストエクストラネット経路フィルタリングを使用して，いくつかの制限を掛けることができます。

図 29-2　マルチキャストエクストラネットの構成例（IPv4）



(1)　すべての VRF からの要求を許可する設定

VRF 2 に，すべての VRF およびグローバルネットワークからのマルチキャスト中継要求を許可する設定をします。

事前にユニキャストのエクストラネットを設定して，中継先 VRF およびグローバルネットワークから送信者への経路が VRF 2 になるように設定してください。

[設定のポイント]

route-map はフィルタ条件を設定しない場合，すべての条件が許可になります。

[コマンドによる設定]

1. **(config)# route-map MLTEXNET permit 10**
   (config-route-map)# exit
   すべてのフィルタ条件を許可にします。
2. **(config)# vrf definition 2**
   (config-vrf)# import multicast inter-vrf MLTEXNET
   (config-vrf)# exit
   1.のフィルタ設定を VRF 2 のエクストラネットに適用して，すべての VRF およびグローバルネットワークからのマルチキャスト中継要求を許可する設定をします。

(2)　特定の VRF だけ許可する設定

VRF 2 に，VRF 3 および VRF 4 からのマルチキャスト中継要求を許可する設定をします。

事前にユニキャストのエクストラネットを設定して，VRF 3 および VRF 4 から送信者への経路が VRF 2 になるように設定してください。

[設定のポイント]

この設定をしない場合，すべての VRF からのマルチキャスト中継要求を受け付けます。

[コマンドによる設定]

1. **(config)# route-map MLTEXNET permit 10**
   (config-route-map)# match vrf 3 4
   (config-route-map)# exit
   VRF 3 および VRF 4 からのマルチキャスト中継要求だけを許可します。
2. **(config)# vrf definition 2**
   (config-vrf)# import multicast inter-vrf MLTEXNET
   (config-vrf)# exit
   1.のフィルタ設定を VRF 2 のエクストラネットに適用して，VRF 3 および VRF 4 からのマルチキャスト中継要求を許可する設定をします。

(3)　特定のグループアドレスだけ許可する設定

233.252.0.0/16 の範囲内のグループアドレスだけマルチキャスト中継要求を許可する設定をします。

事前にユニキャストのエクストラネットを設定して，中継先 VRF およびグローバルネットワークから送信者への経路が VRF 2 になるように設定してください。

[設定のポイント]

エクストラネットで使用するグループアドレスの範囲を設定すると，そのアドレス以外のグループアドレスを他 VRF と独立して，VRF 内通信に割り当てられます。ローカルで使用するグループアドレスは，VRF ごとに異なる用途に使用できます。

この設定をしない場合，すべてのグループアドレス（224.0.0.0/4）をエクストラネットで使用します。

[コマンドによる設定]

1. **(config)# ip access-list standard MLTGROUP**
   (config-std-nacl)# permit 233.252.0.0 0.0.255.255
   (config-std-nacl)# exit
   (config)# route-map MLTEXNET permit 10
   (config-route-map)# match ip address MLTGROUP
   (config-route-map)# exit
   エクストラネットで使用するグループアドレスに 233.252.0.0/16 を設定します。
2. **(config)# vrf definition 2**
   (config-vrf)# import multicast inter-vrf MLTEXNET
   (config-vrf)# exit
   1.のフィルタ設定を VRF 2 のエクストラネットに適用して，VRF 2 が受け付ける他 VRF からの中継要求を 233.252.0.0/16 に限定します。

(4)　双方向 IPv4 マルチキャストエクストラネットの設定

グローバルネットワーク，VRF 2，VRF 3 および VRF 4 で，マルチキャストエクストラネットによって相互に通信できるように設定します。

事前にユニキャストのエクストラネットを設定して，グローバルネットワーク，VRF 2，VRF 3 および VRF 4 から送信者への経路が，接続したい VRF またはグローバルネットワークになるように設定してください。

[設定のポイント]

route-map の match vrf コマンドで設定した VRF は，共通のフィルタを指定できます。

[コマンドによる設定]

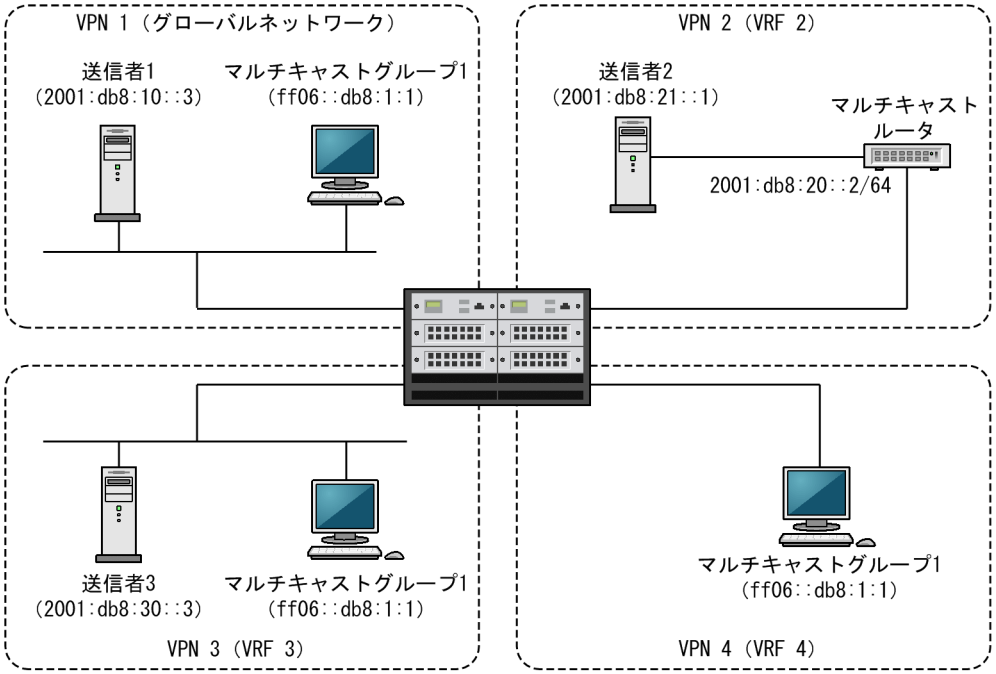
1. **(config)# ip access-list standard MLTGROUP**
   (config-std-nacl)# permit 233.252.0.0 0.0.255.255
   (config-std-nacl)# exit
   (config)# route-map MLTEXNET permit 10
   (config-route-map)# match vrf global 2 3 4
   (config-route-map)# match ip address MLTGROUP
   (config-route-map)# exit
   グローバルネットワーク，VRF 2，VRF 3 および VRF 4 からのグループアドレス 233.252.0.0/16 に対するマルチキャスト中継要求を許可する設定をします。
2. **(config)# vrf definition global**
   (config-vrf)# import multicast inter-vrf MLTEXNET
   (config-vrf)# exit
   (config)# vrf definition 2
   (config-vrf)# import multicast inter-vrf MLTEXNET
   (config-vrf)# exit
   (config)# vrf definition 3
   (config-vrf)# import multicast inter-vrf MLTEXNET
   (config-vrf)# exit
   (config)# vrf definition 4
   (config-vrf)# import multicast inter-vrf MLTEXNET
   (config-vrf)# exit
   1.のフィルタ設定をグローバルネットワーク，VRF 2，VRF 3 および VRF 4 のエクストラネットに適用して，相互にマルチキャスト中継要求を許可する設定をします。

29.2.3　IPv6 マルチキャストエクストラネットの設定

次の図のようなネットワーク構成で，マルチキャストエクストラネットを設定します。

マルチキャストエクストラネット経路フィルタリングを使用して，いくつかの制限を掛けることができます。

図 29-3　マルチキャストエクストラネットの構成例（IPv6）



(1)　すべての VRF からの要求を許可する設定

VRF 2 に，すべての VRF およびグローバルネットワークからのマルチキャスト中継要求を許可する設定をします。

事前にユニキャストのエクストラネットを設定して，中継先 VRF およびグローバルネットワークから送信者への経路が VRF 2 になるように設定してください。

[設定のポイント]

route-map はフィルタ条件を設定しない場合，すべての条件が許可になります。

[コマンドによる設定]

1. **(config)# route-map MLT6EXNET permit 10**
   (config-route-map)# exit
   すべてのフィルタ条件を許可にします。
2. **(config)# vrf definition 2**
   (config-vrf)# ipv6 import multicast inter-vrf MLT6EXNET
   (config-vrf)# exit
   1.のフィルタ設定を VRF 2 のエクストラネットに適用して，すべての VRF およびグローバルネットワークからのマルチキャスト中継要求を許可する設定をします。

(2)　特定の VRF だけ許可する設定

VRF 2 に，VRF 3 および VRF 4 からのマルチキャスト中継要求を許可する設定をします。

事前にユニキャストのエクストラネットを設定して，VRF 3 および VRF 4 から送信者への経路が VRF 2 になるように設定してください。

[設定のポイント]

この設定をしない場合，すべての VRF からのマルチキャスト中継要求を受け付けます。

[コマンドによる設定]

1. **(config)# route-map MLT6EXNET permit 10**
   (config-route-map)# match vrf 3 4
   (config-route-map)# exit
   VRF 3 および VRF 4 からのマルチキャスト中継要求だけを許可します。
2. **(config)# vrf definition 2**
   (config-vrf)# ipv6 import multicast inter-vrf MLT6EXNET
   (config-vrf)# exit
   1.のフィルタ設定を VRF 2 のエクストラネットに適用して，VRF 3 および VRF 4 からのマルチキャスト中継要求を許可する設定をします。

(3)　特定のグループアドレスだけ許可する設定

ff06::db8:0:0/96 の範囲内のグループアドレスだけマルチキャスト中継要求を許可する設定をします。

事前にユニキャストのエクストラネットを設定して，中継先 VRF およびグローバルネットワークから送信者への経路が VRF 2 になるように設定してください。

[設定のポイント]

エクストラネットで使用するグループアドレスの範囲を設定すると，そのアドレス以外のグループアドレスを他 VRF と独立して，VRF 内通信に割り当てられます。ローカルで使用するグループアドレスは，VRF ごとに異なる用途に使用できます。

この設定をしない場合，すべてのグループアドレス（ff00::/8）をエクストラネットで使用します。

[コマンドによる設定]

1. **(config)# ipv6 access-list MLT6GROUP**
   (config-ipv6-acl)# permit ipv6 ff06::db8:0:0/96 any
   (config-ipv6-acl)# exit
   (config)# route-map MLT6EXNET permit 10
   (config-route-map)# match ipv6 address MLT6GROUP
   (config-route-map)# exit
   エクストラネットで使用するグループアドレスに ff06::db8:0:0/96 を設定します。
2. **(config)# vrf definition 2**
   (config-vrf)# ipv6 import multicast inter-vrf MLT6EXNET
   (config-vrf)# exit
   1.のフィルタ設定を VRF 2 のエクストラネットに適用して，VRF 2 が受け付ける他 VRF からの中継要求を ff06::db8:0:0/96 に限定します。

(4)　双方向 IPv6 マルチキャストエクストラネットの設定

グローバルネットワーク，VRF 2，VRF 3 および VRF 4 で，マルチキャストエクストラネットによって相互に通信できるように設定します。

事前にユニキャストのエクストラネットを設定して，グローバルネットワーク，VRF 2，VRF 3 および VRF 4 から送信者への経路が，接続したい VRF またはグローバルネットワークになるように設定してください。

[設定のポイント]

route-map の match vrf コマンドで設定した VRF は，import した VRF と同じ VRF ID は無視して登録します。そのため，双方向通信するすべての VRF を一つの route-map に記述することで，それぞれの VRF の import に対し共通に指定できます。

[コマンドによる設定]

1.
```
(config)# ipv6 access-list MLT6GROUP
(config-ipv6-acl)# permit ipv6 ff06::db8:0:0/96 any
(config-ipv6-acl)# exit
(config)# route-map MLT6EXNET permit 10
(config-route-map)# match vrf global 2 3 4
(config-route-map)# match ipv6 address MLT6GROUP
(config-route-map)# exit
```

グローバルネットワーク，VRF 2，VRF 3 および VRF 4 からのグループアドレス ff06::db8:0:0/96 に対するマルチキャスト中継要求を許可する設定をします。

2.
```
(config)# vrf definition global
(config-vrf)# ipv6 import multicast inter-vrf MLT6EXNET
(config-vrf)# exit
(config)# vrf definition 2
(config-vrf)# ipv6 import multicast inter-vrf MLT6EXNET
(config-vrf)# exit
(config)# vrf definition 3
(config-vrf)# ipv6 import multicast inter-vrf MLT6EXNET
(config-vrf)# exit
(config)# vrf definition 4
(config-vrf)# ipv6 import multicast inter-vrf MLT6EXNET
(config-vrf)# exit
```

1.のフィルタ設定をグローバルネットワーク，VRF 2，VRF 3 および VRF 4 のエクストラネットに適用して，相互にマルチキャスト中継要求を許可する設定をします。

29.3　オペレーション

29.3.1　運用コマンド一覧

マルチキャスト経路フィルタリングの運用コマンド一覧を次の表に示します。

表 29-5　運用コマンド一覧

コマンド名	説明
show ip mcache※1	マルチキャスト中継エントリを一覧表示します。
show ip mroute※1	マルチキャスト経路情報を一覧表示します。
show ip multicast resources※1	IPv4 マルチキャストルーティング機能で使用している各種エントリ数を表示します。
show ipv6 mcache※2	マルチキャスト中継エントリを一覧表示します。
show ipv6 mroute※2	マルチキャスト経路情報を一覧表示します。
show ipv6 multicast resources※2	IPv6 マルチキャストルーティング機能で使用している各種エントリ数を表示します。

注※1

「運用コマンドレファレンス Vol.3　13. IPv4 マルチキャストルーティングプロトコル」を参照してください。

注※2

「運用コマンドレファレンス Vol.3　14. IPv6 マルチキャストルーティングプロトコル」を参照してください。

29.3.2　マルチキャストエクストラネットの確認

show ip mroute コマンドおよび show ip mcache コマンドで，IPv4 マルチキャストエクストラネットによって VRF 間中継するエントリを確認できます。異なる VRF に中継要求を発行しているエントリは incoming に中継要求先 VRF ID が表示されます。また，異なる VRF からの中継要求を許可したエントリは outgoing に VRF ID が表示されます。

なお，show ipv6 mroute コマンドおよび show ipv6 mcache コマンドで，IPv6 マルチキャストエクストラネットの確認ができます。

図 29-4　show ip mroute コマンドの実行結果

```
> show ip mroute vrf all
Date 20XX/01/13 10:01:00 UTC
Total: 4 routes
VRF: 1  Total: 1 route , 1 group , 1 source
(S,G) 1 route  ------------------------------------------------------------
Group Address    Source Address   Flags  Protocol  Uptime   Expires  Assert
232.1.1.1        192.0.2.10       FT     SSM        53:05    02:55    00:00
    incoming:Eth1/1.1          upstream:Direct
    outgoing:VRF 2             uptime:  53:05
             VRF 10            uptime:  53:05
             VRF 11            uptime:  53:05

VRF: 2  Total: 1 route , 1 group , 1 source
(S,G) 1 route  ------------------------------------------------------------
Group Address    Source Address   Flags  Protocol  Uptime   Expires  Assert
232.1.1.1        192.0.2.10       LT     SSM        53:05    --:--    00:00
    incoming:VRF 1             upstream:Extra
    outgoing:Eth1/1.2          uptime:  53:05    expires:  --:--
```

```
VRF: 10  Total: 1 route , 1 group , 1 source
(S,G) 3 routes ------------------------------------------------------------
Group Address    Source Address   Flags  Protocol  Uptime   Expires  Assert
232.1.1.1        192.0.2.10       LT     SSM        53:05    --:--    00:00
    incoming:VRF 1             upstream:Extra
    outgoing:Eth1/1.10         uptime:  53:05    expires:  --:--

VRF: 11  Total: 1 route , 1 group , 1 source
(S,G) 3 routes ------------------------------------------------------------
Group Address    Source Address   Flags  Protocol  Uptime   Expires  Assert
232.1.1.1        192.0.2.10       LT     SSM        53:05    --:--    00:00
    incoming:VRF 1             upstream:Extra
    outgoing:Eth1/1.11         uptime:  53:05    expires:  --:--
```

図 29-5　show ip mcache コマンドの実行結果

```
> show ip mcache vrf all
Date 20XX/01/13 10:01:00 UTC
Total: 4 routes
VRF: 1  Total: 1 route
- Forwarding entry ----------------------------------------------------------
Group Address   Source Address  Flags  Protocol  Uptime   Expires
232.1.1.1       192.0.2.10      U      SSM        53:30    --:--
    incoming:Eth1/1.1
    outgoing:Eth1/1.2          VRF 2
             Eth1/1.10         VRF 10
             Eth1/1.11         VRF 11

VRF: 2  Total: 1 route
- Forwarding entry ----------------------------------------------------------
Group Address   Source Address  Flags  Protocol  Uptime   Expires
232.1.1.1       192.0.2.10      D      SSM        53:30    --:--
    incoming:VRF 1
    outgoing:Eth1/1.2

VRF: 10  Total: 1 route
- Forwarding entry ----------------------------------------------------------
Group Address   Source Address  Flags  Protocol  Uptime   Expires
232.1.1.1       192.0.2.10      D      SSM        53:30    --:--
    incoming:VRF 1
    outgoing:Eth1/1.10

VRF: 11  Total: 1 route
- Forwarding entry ----------------------------------------------------------
Group Address   Source Address  Flags  Protocol  Uptime   Expires
232.1.1.1       192.0.2.10      D      SSM        53:30    --:--
    incoming:VRF 1
    outgoing:Eth1/1.11
```

30 BFD

BFD は，二つの装置間の転送機能障害を高速で検出する機能です。この章では，BFD の解説と操作方法について説明します。

30.1 解説

30.1.1 概要

BFD は二つの装置間の経路の到達性を継続的に監視する機能です。両装置は定期的に BFD パケットを送受信して，一定時間以上 BFD パケットを受信しない場合に対向装置との経路に障害が発生したと見なします。この二つの装置の組み合わせを BFD セッションと呼びます。

BFD は，他プロトコルと BFD セッションを連携させる形式で設定します。障害を検出すると連携するプロトコルに通知するため，通知されたプロトコルでは速やかに障害対策ができます。BFD セッションは，連携するプロトコルの性質に依存しないで，必要に応じて設定できます。

なお，BFD は迅速な代替経路の確立などを目的とした，通信障害の高速な検出に特化したプロトコルであり，障害の原因や発生個所の特定には不向きです。

30.1.2 サポート機能一覧

本装置の BFD がサポートする機能の一覧を次の表に示します。

表 30-1 BFD サポート状況

機能		サポート
BFD バージョン	1	○
動作モード	非同期モード	○
	要求モード	×
エコー機能		×
認証		×
マルチホップ		○
グレースフル・リスタートとの連携		○
インタフェース	イーサネットインタフェース	○
	イーサネットサブインタフェース	○
	ポートチャネルインタフェース	○
	ポートチャネルサブインタフェース	○
	VLAN インタフェース	○
	マネージメントポート	×
	シリアル接続ポート（AUX）	×
	ループバックインタフェース	×
	Null インタフェース	×
連携プロトコル	スタティックルーティング	○
	RIP，RIPng	×

機能		サポート
	OSPF	○
	OSPFv3	○
	BGP4	○
	BGP4+	○

（凡例） ○：サポートする　×：サポートしない

本装置は BFD のバージョン 1 をサポートします。それ以外のバージョンの BFD パケットを受信した場合は，該当パケットを廃棄します。要求モードの使用を要求する BFD パケットを受信した場合は，要求モードをサポートしない旨を応答して非同期モードで動作します。エコー機能および認証を利用した BFD パケットを受信した場合は，該当パケットを廃棄して BFD セッションを確立しません。

BFD は，自装置がグレースフル・リスタートに対応しているかを，BFD パケットで対向装置に広告します。これによって，グレースフル・リスタート中に発生した BFD セッションのダウンが障害によるものか，グレースフル・リスタートによるものかを識別できるようになります。なお，グレースフル・リスタートの影響によるダウンは，障害として扱いません。本装置はグレースフル・リスタートに対応していて，BFD 監視を継続できるとして広告します。また，対向装置がグレースフル・リスタート中でも，障害を検出できます。

なお，サポートしていないインタフェースをネクストホップにすると，BFD セッションはダウンします。BFD を使用する場合は，マネージメントポートをネクストホップに設定しないでください。

30.1.3 BFD セッション

対向装置を BFD による監視対象としてコンフィグレーションに設定することで，本装置と対向装置の間に BFD セッションを生成します。ここでの監視対象とは，次の組み合わせによって一意に決定される接続対象を指します。

- 宛先 IP アドレス
- BFD パケットの送信インタフェース（シングルホップの場合だけ）

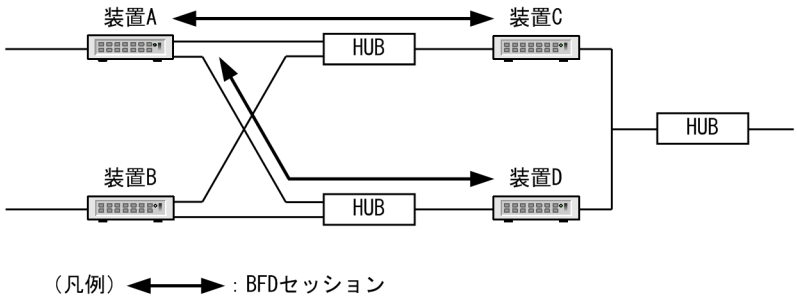
本装置に BFD が設定されていない場合は，対向装置からの BFD パケットを受信しても応答しないため，BFD セッションは確立しません。BFD セッションを生成するには，本装置と対向装置で双方向の設定が必要です。

(1) 基本動作

本装置の BFD は，連携するプロトコルからの要求に基づいて動作します。プロトコルの監視機能として BFD をコンフィグレーションに設定して，かつ監視対象となる対向装置が決定した時点で，新しい BFD セッションの生成と確立を開始します。対向装置の決定方法はプロトコルに依存します。コンフィグレーションが変更されると，動作に反映します。また，コンフィグレーションが削除されると，BFD セッションも削除します。

BFD の基本動作を次の図に示します。

図 30-1 BFD の基本動作



装置 A では，装置 C と装置 D を BFD 監視対象として設定します。装置 C では装置 A を，装置 D でも装置 A を BFD 監視対象として設定します。このとき，装置 A と装置 C，装置 A と装置 D の間に，それぞれ BFD セッションが生成されます。

(2) BFD セッションの状態

生成された BFD セッションは，状態に従って監視を開始します。BFD セッションの状態を次の表に示します。

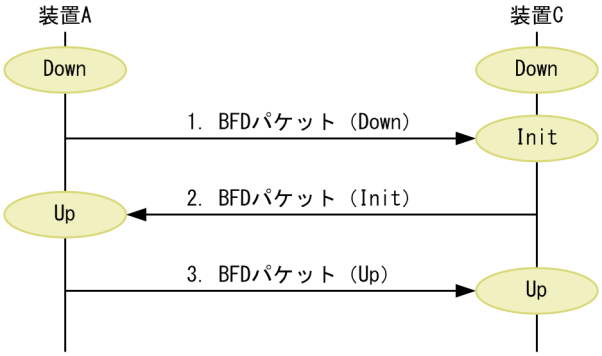
表 30-2 BFD セッションの状態

状態	内容	説明
Down	ダウン	生成された BFD セッションの初期状態，または対向装置を認識していない状態です。
Init	応答中	対向装置から Down 状態の BFD パケットを受信して，自装置だけが監視対象を認識した過渡状態です。Init 状態を経由しないで，直接 Up 状態になることもあります。
Up	確立	Init または Up 状態の BFD パケットを受信して，互いに監視対象を認識した状態です。セッションが確立されて，BFD 監視が有効になります。
AdminDown	管理的ダウン	ユーザまたはシステムによって，意図的に BFD セッションをダウンさせた状態です。BFD セッションの確立は抑止されていて，対向装置から AdminDown 状態を通知されると BFD セッションがダウンします。

BFD パケットには，送信側の装置の状態が含まれています。BFD パケット上の状態と受信側の装置の状態によって，BFD セッションの状態が決定します。

装置 A と装置 C 間の BFD セッションでの，状態遷移の例を次の図に示します。

図 30-2　BFD の状態遷移



1. 装置 A および C はコンフィグレーションに従って BFD セッションを Down 状態で作成して，BFD 監視対象となったシステムに BFD パケット（Down）を一定の周期で送信します。
2. BFD パケット（Down）を受信した装置 C は，装置 A を認識したため Init 状態へ遷移して，BFD パケット（Init）を一定の周期で送信します。BFD パケット（Init）を受信した装置 A は，Up 状態へ遷移します。
3. 装置 A は BFD パケット（Up）を一定の周期で送信します。BFD パケット（Up）を受信した Init 状態の装置 C は，Up 状態へ遷移します。

このように，両装置が Up 状態となることで BFD セッションが確立したと見なされて，BFD 監視が有効になります。

確立しているセッションでどちらかの装置が Down 状態または AdminDown 状態になると，BFD パケットの受信によって対向装置も Down 状態となって，BFD セッションはダウンします。

(3)　BFD セッションの共有

一つの監視対象に対して，生成される BFD セッションは最大で一つです。同じ監視対象に対して複数の BFD 監視が設定された場合，一つの BFD セッションを共有して監視します。

BFD セッションを共有する場合，監視間隔は次のように算出します。

- 最小送信間隔は最も短いものを選択します。
- 最小受信間隔は最も短いものを選択します。
- 検出乗数は最も小さいものを選択します。

なお，監視対象が同じ対向装置でも，宛先 IP アドレスや送信インタフェースが一致しないときは共有しません。

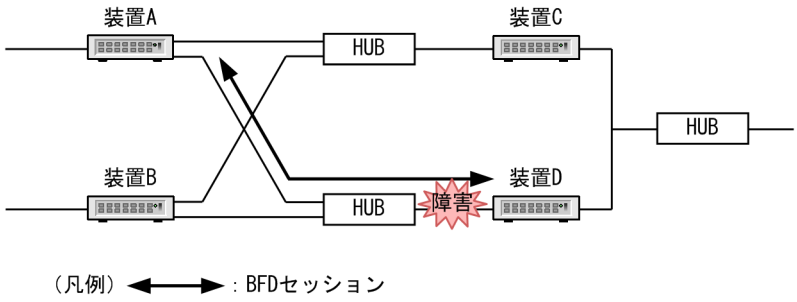
30.1.4　BFD による障害検出

(1)　障害検出の仕組み

BFD セッションの確立後，障害検出時間のうちに BFD パケットを受信しなかった場合，BFD セッションはダウンします。

装置 D と HUB の間に障害が発生した例を次の図に示します。

図 30-3　BFD セッションでの障害発生



装置 A と装置 D の間に HUB があるため，装置 A ではリンク障害を検出できないでリンクアップしたままになります。しかし，BFD パケットを受信しなくなることによって，障害検出時間の経過後に BFD セッションでは障害を検出できます。このように，システム間に L2 スイッチなどが存在して対向装置の障害が伝わらないときなどに BFD は有効です。

(2)　障害検出時間の設定

障害検出時間は，コンフィグレーションで設定する本装置の監視間隔，および対向装置で設定されている監視間隔によって決定します。本装置での，各監視間隔の設定と障害検出時間の算出方法を次の表に示します。

表 30-3　監視間隔の設定および算出方法

決定者	監視間隔	説明
本装置	最小送信間隔	本装置が要求する BFD パケットの最小送信間隔です。本装置が対向装置へ送信する BFD パケットの間隔の算出に使用します。 コンフィグレーションで設定できます。1 秒未満の値を設定した場合，セッションが確立するまでは 1 秒となります。
	最小受信間隔	本装置が要求する BFD パケットの最小受信間隔です。対向装置が本装置へ送信する BFD パケットの間隔の算出に使用します。 コンフィグレーションで設定できます。
	検出乗数	本装置が要求する検出乗数です。障害として扱う連続パケットロスの回数を示します。 コンフィグレーションで設定できます。
対向装置	最小送信間隔	対向装置が要求する最小送信間隔です。 対向装置が送信する BFD パケットで本装置に通知されます。
	最小受信間隔	対向装置が要求する最小受信間隔です。 対向装置が送信する BFD パケットで本装置に通知されます。
	検出乗数	対向装置が要求する検出乗数です。 対向装置が送信する BFD パケットで本装置に通知されます。
本装置	送信間隔	本装置の BFD パケット送信間隔です。 本装置の最小送信間隔と対向装置の最小受信間隔を比較して，値の大きい方を採用します。
	受信間隔	本装置の BFD パケット受信間隔です。 本装置の最小受信間隔と対向装置の最小送信間隔を比較して，値の大きい方を採用します。

決定者	監視間隔	説明
	障害検出時間	障害検出時間のうちに BFD パケットを受信できないときに，障害と見なして BFD セッションをダウンさせます。 本装置の受信間隔に，対向装置が要求する検出乗数を乗算した値です。

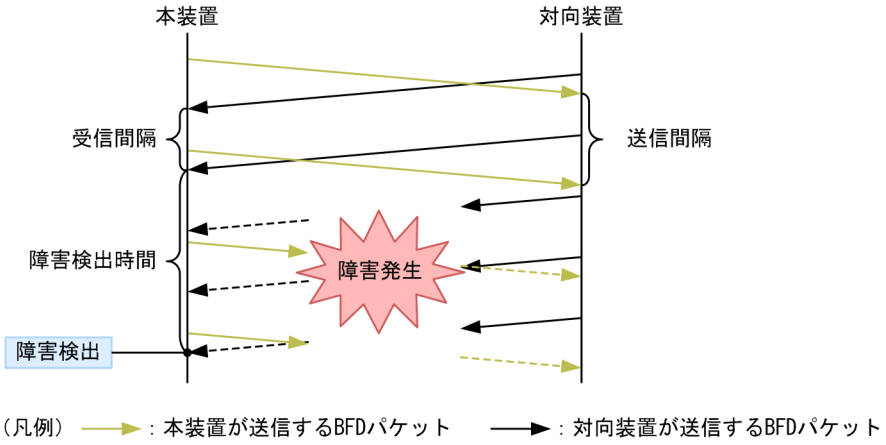
送信間隔と受信間隔は，同じ値である必要はありません。また，パケットの送受信間隔は，通信方向ごとに独立して決定します。

本装置の障害検出時間が 300 秒を超えない範囲で指定してください。

(3)　障害検出動作

本装置から見た，BFD セッションでの障害検出例を次の図に示します。なお，検出乗数は 3 とします。

図 30-4　BFD セッションでの障害検出



障害を検出すると，連携するプロトコルに BFD セッションのダウンを通知して，BFD パケットの送信を停止します。監視対象を動的に決定するプロトコルの場合は，プロトコルによって該当の BFD セッションは削除されて，監視対象を再選出します。

30.1.5　マルチホップの監視

監視対象の IP アドレスが本装置に直接接続されたネットワークのアドレスではない場合は，コンフィグレーションコマンド type bfd で multihop パラメータを指定して，マルチホップの監視を有効にしてください。

multihop パラメータを指定した BFD セッションでは，BFD パケットの送信元アドレスとしてループバックアドレスを使用します。本装置のループバックインタフェースに IP アドレスを設定してください。対向装置への経路に VRF を使用している場合，ループバックインタフェースにも VRF の設定が必要です。

監視対象の IP アドレスが本装置に直接接続されたネットワークのアドレスではないのに multihop パラメータを指定しない場合や，ループバックインタフェースにアドレスを設定しない場合，BFD セッションは確立しません。

なお，運用中の BFD セッションが使用するループバックアドレスを変更または削除した場合，対象の BFD セッションをダウンさせて，再確立します。対象の BFD セッションは一度削除されるため，統計情報などは引き継がれません。このとき，BFD を使用して監視している経路の通信が，一時的に停止することがあります。

30.1.6 BFD とプロトコルの連携

BFD セッションの状態と他プロトコルを連携させると，連携するプロトコルでは速やかな障害対策ができます。

BFD による障害検出で経路を切り替えたい場合，経路の学習元となるすべての隣接ルータ間で BFD 監視を設定してください。また，ネットワーク内の各装置で同一装置に対する障害検出時間のずれを少なくするため，各装置のコンフィグレーションで BFD セッションの障害検出時間（最小送信間隔，最小受信間隔，および検出乗数）を統一してください。

(1) スタティックルーティングのゲートウェイ監視

ゲートウェイを BFD で監視している場合，BFD によって障害を検出すると，すぐにスタティック経路を削除します。

スタティックルーティングのゲートウェイ監視は隣接ゲートウェイに対して設定してください。

隣接ゲートウェイに対して直接接続されたインタフェースがアップすると BFD による監視を開始します。BFD でゲートウェイを監視しているスタティック経路は，BFD セッションが確立しているときだけ生成します。

(2) OSPF および OSPFv3 の隣接ルータ監視

隣接ルータを BFD で監視している場合，隣接ルータの障害を検出すると，すぐに OSPF の隣接関係を切断して LSA の再生成と広告をします。その後，SPF 計算の遅延時間が経過したあとで経路計算をして，代替経路へ切り替えます。

OSPF または OSPFv3 の隣接関係の確立と BFD セッションの確立は，独立して動作します。

なお，ブロードキャスト型ネットワークでは，すべての隣接ルータで BFD を使用してください。BFD を使用していないルータと隣接関係を確立できますが，BFD を使用していないルータが指定ルータになると，該当ルータが Hello パケットによって障害を認識するまでそのネットワークを経由する通信が停止します。

(3) BGP4 および BGP4+のピア監視

ピアを BFD で監視している場合，BFD によって障害を検出すると，すぐに BGP ピアの隣接関係を切断して経路を切り替えます。

BGP ピアの隣接関係の確立と BFD セッションの確立は，独立して動作します。

30.1.7 BCU 二重化構成での動作

BFD の各機能について，系切替時の動作を次の表に示します。

表 30–4 系切替時の BFD セッションの動作

項目	説明
監視状態	継続して監視できます。
統計情報	クリアされます。

項目	説明
運用コマンドおよび MIB	系切替後，連携プロトコルが隣接ルータを再認識するまで，BFD セッションの情報を確認できません。連携プロトコルが隣接ルータを再認識したあと，運用コマンド show bfd session または MIB で確認できます。

30.1.8 BFD 使用時の注意事項

(1) ポートチャネルインタフェースでの使用条件

ポートチャネルインタフェース上で BFD を動作させる場合，BFD の障害検出時間がリンクアグリゲーションでの障害検出時間より長くなるように設定してください。BFD の障害検出時間の方が短い場合，一部の回線のダウンを BFD が障害として検出するおそれがあります。

(2) トラックのコンフィグレーション削除

BFD を設定したトラック（コンフィグレーションコマンド track name または type bfd）を削除するときは，ルーティングプロトコルのコンフィグレーションから連携するトラックの設定を削除したあと，該当するトラックを削除してください。BFD を設定したトラックを先に削除した場合，連携するルーティングプロトコルは隣接関係を切断します。

(3) BFD セッション数

BFD を使用しても各プロトコルの収容条件には影響しませんが，BFD セッション数が装置当たりの収容条件を超えないようにしてください。BFD セッション数が収容条件を超えても各プロトコルは動作しますが，BFD による障害検出ができません。

(4) 同一装置に対する BFD の設定

同一装置に対する BFD セッションは一つのセッションになるように，ネットワークを設計してください。

同一ネットワーク上に存在する装置とループバックインタフェースに設定したアドレスを使用してピアリングしている場合，BGP ピアのアドレスを解決しているルーティングプロトコルか，BGP ピアのどちらか一方に BFD と連携する設定をしてください。なお，BGP ピアのアドレスを解決しているルーティングプロトコルに BFD と連携する設定をすると，より早く障害を検出できます。

30.2 コンフィグレーション

30.2.1 コンフィグレーションコマンド一覧

BFD および連携するプロトコルのコンフィグレーションコマンド一覧を次の表に示します。

表 30-5 コンフィグレーションコマンド一覧

コマンド名	説明
bfd interval	トラックに BFD セッションの監視間隔を設定します。
bfd multiplier	トラックに BFD セッションの検出乗数を設定します。
track name	動的監視トラックを設定します。
type bfd	トラックに監視種別として BFD 監視を設定します。
ip route※1	IPv4 スタティック経路をトラックと連携させます。
ipv6 route※2	IPv6 スタティック経路をトラックと連携させます。
ip ospf track※3	OSPF をトラックと連携させます。
ipv6 ospf track※4	OSPFv3 をトラックと連携させます。
neighbor track※5	BGP をトラックと連携させます。

注※1
「コンフィグレーションコマンドレファレンス Vol.3　15. スタティックルーティング（IPv4)」を参照してください。

注※2
「コンフィグレーションコマンドレファレンス Vol.3　16. スタティックルーティング（IPv6)」を参照してください。

注※3
「コンフィグレーションコマンドレファレンス Vol.3　19. OSPF」を参照してください。

注※4
「コンフィグレーションコマンドレファレンス Vol.3　20. OSPFv3」を参照してください。

注※5
「コンフィグレーションコマンドレファレンス Vol.3　21. BGP4/BGP4+」を参照してください。

30.2.2 BFD の設定

BFD 監視の設定例を次に示します。

[設定のポイント]
BFD 監視のためのトラックを設定します。

[コマンドによる設定]

1. **(config)# track name BFD001**
   トラックを設定します。トラック名（BFD001）を指定すると，トラックの入力モードに移行します。
2. **(config-track)# type bfd**

監視方法として BFD を指定します。

3. **(config-track)# bfd interval min-rx 150**
   (config-track)# bfd multiplier 5
   BFD セッションの最小受信間隔を 150，検出乗数を 5 に設定します。

30.2.3 スタティックルーティングのゲートウェイ監視の設定

IPv4 スタティック経路のゲートウェイを対象とした BFD 監視の設定例を次に示します。

[設定のポイント]

BFD 監視のトラックを，スタティック経路の設定時に指定します。

[コマンドによる設定]

1. **(config)# ip route 192.168.1.0 255.255.255.0 172.16.1.100 noresolve track BFD001**
   スタティック経路（192.168.1.0/24）のネクストホップとして，隣接ゲートウェイ（172.16.1.100）を指定します。隣接ゲートウェイに BFD 監視を設定します。

30.2.4 OSPF および OSPFv3 の隣接ルータ監視の設定

OSPF の隣接ルータを対象とした BFD 監視の設定例を次に示します。

[設定のポイント]

BFD 監視のトラックを，OSPF の設定時に指定します。

[コマンドによる設定]

1. **(config)# router ospf 1**
   ospf モードへ移行します。ドメイン番号を 1 にします。
2. **(config-router)# router-id 100.1.1.1**
   ルータ ID として 100.1.1.1 を設定します。
3. **(config-router)# top**
   グローバルコンフィグレーションモードに戻ります。
4. **(config)# interface gigabitethernet 1/1**
   (config-if)# ip ospf 1 area 0
   OSPF を適用します。
5. **(config-if)# ip ospf track BFD001**
   OSPF が動作するインタフェースに BFD 監視を適用します。

30.2.5 BGP4 および BGP4+のピア監視の設定

BGP のピアを対象とした BFD 監視の設定例を次に示します。

[設定のポイント]

BFD 監視のトラックを，BGP ピアの設定時に指定します。

直接接続されたインタフェースのアドレスを使用していない BGP ピアを BFD で監視する場合，ループバックインタフェースに IP アドレスと，type bfd コマンドで multihop パラメータを設定してください。

[コマンドによる設定]

1. **(config)# router bgp 65531**
   ルーティングプロトコルに BGP4 および BGP4+を適用します。パラメータに自ルータが所属する AS 番号（65531）を指定します。
2. **(config-router)# bgp router-id 192.168.1.100**
   自ルータ識別子（192.168.1.100）を設定します。
3. **(config-router)# neighbor 172.16.2.2 remote-as 65532**
   外部ピア（相手側アドレス：172.16.2.2, AS 番号：65532）を設定します。
4. **(config-router)# neighbor 172.16.2.2 track BFD001**
   ピア（相手側アドレス：172.16.2.2）に BFD 監視を設定します。

30.3 オペレーション

30.3.1 運用コマンド一覧

BFD の運用コマンド一覧を次の表に示します。

表 30-6 運用コマンド一覧

コマンド名	説明
show bfd session	BFD セッションの情報と状態を表示します。
show bfd discard-packets	BFD パケットの廃棄情報を表示します。
clear bfd session	BFD セッションを一時的にダウンさせて，再確立します。
clear bfd statistics	BFD セッションの統計情報をクリアします。
restart bfd	BFD プログラムを再起動します。
dump protocols bfd	BFD プログラムで採取している制御情報をファイルへ出力します。
show track※1	トラック情報を表示します。
show ip ospf※2	OSPF プロトコルに関する情報を表示します。
show ip bgp※2	BGP4 プロトコルに関する情報を表示します。
show ip static※2	IPv4 スタティック経路に関する情報を表示します。
show ipv6 ospf※3	OSPFv3 プロトコルに関する情報を表示します。
show ipv6 bgp※3	BGP4+プロトコルに関する情報を表示します。
show ipv6 static※3	IPv6 スタティック経路に関する情報を表示します。

注※1

「運用コマンドレファレンス Vol.2　13. トラッキング機能」を参照してください。

注※2

「運用コマンドレファレンス Vol.3　10. IPv4 ルーティングプロトコル」を参照してください。

注※3

「運用コマンドレファレンス Vol.3　11. IPv6 ルーティングプロトコル」を参照してください。

30.3.2 BFD セッションの確認

(1) BFD セッション情報の確認

show bfd session コマンドで，BFD セッション情報を表示します。IP アドレスを指定するか，detail パラメータを指定すると，詳細情報を表示します。

図 30-5 show bfd session コマンドの実行結果

```
> show bfd session
Date 20XX/07/10 18:37:50 UTC
Total: 3 sessions
RemoteAddress                       VRF Index State  DetectTime TrackName
172.16.10.11                          -     2 Down            - Network2
192.168.16.5                          2     1 Up            440 Network1
```

```
192.168.22.1                            2     3 AdminDown       - BGP0100
>
```

図 30-6　show bfd session コマンドの実行結果（詳細表示）

```
> show bfd session vrf 2 ip 192.168.16.5
Date 20XX/05/22 15:55:33 UTC
Session Index 1
  State : Up
    Remote System    : 192.168.16.5  VRF:2
    Local System     : 192.168.16.1  VRF:2
    Discriminator    : Hex                    Decimal
      Remote         : 0xbce20002             3168927746
      Local          : 0xe0430001             3762487297
    Detection Time   : 440
    Diagnostic       : -
    Operating Mode   : Asynchronous (Echo off)
  Track : Network1
    Path             : Singlehop
    Parameter        :   TxInterval     RxInterval     Multiplier
    Remote System    :          150            200              2
    Local System     :          160            220              3
    Current          :          200            220              2
  Statistics
    Packets Counter  :                   Tx                   Rx
      Since Last Up  :                 2194                 3291
      Since Boot     :                 2195                 3292
    Up Count         : 1
    Last Up Time     : 20XX/05/22 15:37:20 UTC
    Last Down Time   : -
      Diagnostic     : -
>
```

(2)　廃棄パケットの確認

show bfd discard-packets コマンドで，廃棄された BFD パケットを表示します。BFD パケットの送信元は，Remote Address で確認できます。

図 30-7　show bfd discard-packets コマンドの実行結果

```
> show bfd discard-packets
Date 20XX/07/10 18:37:50 UTC
15 packets discard
    10 packets: Unknown Session (Discriminator=0xd1ef0023)
        Remote Address: 172.16.10.11 VRF:2
    1 packet: Authentication Failure
        Remote Address: 192.168.22.1
        Local Address: 192.168.22.4
    4 packets: Invalid Desired Min TX Interval (Interval=0)
        Remote Address: 192.168.22.1
        Local Address: 192.168.22.4
>
```

30.3.3　プロトコルの確認

(1)　スタティックルーティングの確認

show ip static コマンドまたは show ipv6 static コマンドで gateway パラメータを指定して，連携するトラック情報を表示します。ゲートウェイに対応する BFD セッションは，show bfd session コマンドでゲートウェイの IP アドレスを指定して確認してください。

図 30-8　show ip static gateway コマンドの実行結果

```
> show ip static gateway
Date 20XX/03/14 12:00:00 UTC
Gateway         Status  Success     Failure     Transition
10.1.1.50       IFdown  -           -           -
10.1.1.100      -       -           -           -
10.2.1.100      Reach   -           0/4         13m 39s
```

```
10.2.1.101      UnReach 1/2         -           21s
172.16.1.100    -       -           -           -
172.16.2.100    -       -           -           -

Track gateway
Gateway         Name                            ID   Status   Transition
172.16.1.100    BFD001                          3    Up       53s
>
```

(2) OSPF 隣接情報の確認

show ip ospf コマンドまたは show ipv6 ospf コマンドで neighbor detail パラメータを指定して，連携するトラック情報を表示します。対応する BFD セッションは，show bfd session コマンドで隣接ルータの IP アドレスを指定して確認してください。

図 30-9　show ip ospf neighbor detail コマンドの実行結果

```
> show ip ospf neighbor detail
Date 20XX/07/10 18:37:50 UTC

Domain: 1
Area: 0
Interface Address: 172.16.10.10, Interface State: BackupDR
    Interface Name: Eth1/2
    Neighbor Router ID: 172.16.1.1, Neighbor State: Full/DR
    Neighbor Address: 172.16.10.11, Priority: 1, Poll Interval: 0s
    DeadTime: 6s, Up: 1d 12h, Adjacent: 1d 12h
    DR: 172.16.10.11, Backup DR: 172.16.10.10
    DS: 0, LSR: 0, Retrans: 0, <Master>
    Track Name: BFD001, Track ID: 1, Track State: Up
>
```

(3) BGP 隣接情報の確認

show ip bgp コマンドまたは show ipv6 bgp コマンドで neighbors detail パラメータを指定して，連携するトラック情報を表示します。ピアに対応する BFD セッションは，show bfd session コマンドでピアの IP アドレスを指定して確認してください。

図 30-10　show ip bgp neighbors detail コマンドの実行結果

```
> show ip bgp neighbors detail
Date 20XX/07/10 18:37:50 UTC
BGP Peer: 172.16.2.2, Remote AS: 65531
Remote Router ID: 172.16.2.20, Peer Group: INTERNAL-GROUP
    BGP Status:Established          HoldTime: 90   , Keepalive: 30
    Established Transitions: 1      Established Date: 20XX/07/16 18:42:26
    BGP Version: 4                  Type: Internal
    Local Address: 172.16.2.214,  Local AS: 65531
    Local Router ID: 172.16.2.100
    Next Connect Retry: -,          Connect Retry Timer: -
    Last Keep Alive Sent: 18:42:20, Last Keep Alive Received: 18:42:20
    BGP Message  UpdateIn UpdateOut TotalIn TotalOut
                 12       14        36      42
    BGP Capability Negotiation: <IPv4-Uni Refresh Refresh(v)>
      Send   : <IPv4-Uni Refresh Refresh(v)>
      Receive: <IPv4-Uni Refresh Refresh(v)>
    Password : UnConfigured
    Track Name: BFD001, Track ID: 2, Track State: Up
>
```

付録

付録 A　準拠規格

付録 A.1　IP・ARP・ICMP

表 A–1　IPv4・ARP・ICMP の準拠規格および勧告

規格番号(発行年月)	規格名
RFC768(1980 年 8 月)	User Datagram Protocol
RFC791(1981 年 9 月)	Internet Protocol
RFC792(1981 年 9 月)	Internet Control Message Protocol
RFC793(1981 年 9 月)	Transmission Control Protocol
RFC813(1982 年 7 月)	Window and Acknowledgement Strategy in TCP
RFC826(1982 年 11 月)	An Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware
RFC896(1984 年 1 月)	Congestion Control in IP/TCP Internetworks
RFC922(1984 年 10 月)	Broadcasting Internet datagrams in the presence of subnets
RFC950(1985 年 8 月)	Internet Standard Subnetting Procedure
RFC1027(1987 年 10 月)	Using ARP to implement transparent subnet gateways
RFC1122(1989 年 10 月)	Requirements for Internet hosts-communication layers
RFC1191(1990 年 12 月)	Path MTU discovery
RFC1323(1992 年 5 月)	TCP Extensions for High Performance
RFC1519(1993 年 9 月)	Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy
RFC1812(1995 年 6 月)	Requirements for IP Version 4 Routers
RFC2018(1996 年 10 月)	TCP Selective Acknowledgment Options
RFC2474(1998 年 12 月)	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
RFC2644(1999 年 8 月)	Changing the Default for Directed Broadcasts in Routers
RFC2883(2000 年 7 月)	An Extension to the Selective Acknowledgement (SACK) Option for TCP
RFC3021(2000 年 12 月)	Using 31-Bit Prefixes on IPv4 Point-to-Point Links
RFC3168(2001 年 9 月)	The Addition of Explicit Congestion Notification (ECN) to IP
RFC3782(2004 年 4 月)	The NewReno Modification to TCP's Fast Recovery Algorithm
RFC4632(2006 年 8 月)	Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan
RFC5227(2008 年 7 月)	IPv4 Address Conflict Detection

規格番号(発行年月)	規格名
RFC5494(2009 年 4 月)	IANA Allocation Guidelines for the Address Resolution Protocol (ARP)
RFC5681(2009 年 9 月)	TCP Congestion Control
RFC5927(2010 年 7 月)	ICMP Attacks against TCP
RFC6056(2011 年 1 月)	Recommendations for Transport-Protocol Port Randomization

付録 A.2　IPv6・NDP・ICMPv6

表 A–2　IPv6・NDP・ICMPv6 の準拠規格および勧告

規格番号(発行年月)	規格名
RFC768(1980 年 8 月)	User Datagram Protocol
RFC793(1981 年 9 月)	Transmission Control Protocol
RFC813(1982 年 7 月)	Window and Acknowledgement Strategy in TCP
RFC896(1984 年 1 月)	Congestion Control in IP/TCP Internetworks
RFC1323(1992 年 5 月)	TCP Extensions for High Performance
RFC1981(1996 年 8 月)	Path MTU Discovery for IP version 6
RFC2018(1996 年 10 月)	TCP Selective Acknowledgment Options
RFC2460(1998 年 12 月)	Internet Protocol, Version 6 (IPv6) Specification
RFC2474(1998 年 12 月)	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
RFC2710(1999 年 10 月)	Multicast Listener Discovery for IPv6
RFC2883(2000 年 7 月)	An Extension to the Selective Acknowledgement (SACK) Option for TCP
RFC3168(2001 年 9 月)	The Addition of Explicit Congestion Notification (ECN) to IP
RFC3587(2003 年 8 月)	IPv6 Global Unicast Address Format
RFC3782(2004 年 4 月)	The NewReno Modification to TCP's Fast Recovery Algorithm
RFC3879(2004 年 9 月)	Deprecating Site Local Addresses
RFC4291(2006 年 2 月)	IP Version 6 Addressing Architecture
RFC4311(2005 年 11 月)	IPv6 Host-to-Router Load Sharing
RFC4443(2006 年 3 月)	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
RFC4861(2007 年 9 月)	Neighbor Discovery for IP version 6 (IPv6)
RFC4862(2007 年 9 月)	IPv6 Stateless Address Autoconfiguration
RFC5095(2007 年 12 月)	Deprecation of Type 0 Routing Headers in IPv6

規格番号(発行年月)	規格名
RFC5681(2009 年 9 月)	TCP Congestion Control
RFC5722(2009 年 12 月)	Handling of Overlapping IPv6 Fragments
RFC5927(2010 年 7 月)	ICMP Attacks against TCP
RFC5942(2010 年 7 月)	IPv6 Subnet Model: The Relationship between Links and Subnet Prefixes
RFC5952(2010 年 8 月)	A Recommendation for IPv6 Address Text Representation
RFC6056(2011 年 1 月)	Recommendations for Transport-Protocol Port Randomization
RFC6085(2011 年 1 月)	Address Mapping of IPv6 Multicast Packets on Ethernet

付録 A.3　uRPF

表 A-3　uRPF の準拠規格および勧告

規格番号(発行年月)	規格名
RFC3704(2004 年 3 月)	Ingress Filtering for Multihomed Networks

付録 A.4　RA

表 A-4　RA の準拠規格および勧告

規格番号(発行年月)	規格名
RFC4862(2007 年 9 月)	IPv6 Stateless Address Autoconfiguration
RFC8106(2017 年 3 月)	IPv6 Router Advertisement Options for DNS Configuration

付録 A.5　DHCP/BOOTP リレーエージェント

表 A-5　DHCP/BOOTP リレーエージェントの準拠規格および勧告

規格番号(発行年月)	規格名
RFC1542(1993 年 10 月)	Clarifications and Extensions for the Bootstrap Protocol
RFC2131(1997 年 3 月)	Dynamic Host Configuration Protocol
RFC3046(2001 年 1 月)	DHCP Relay Agent Information Option
RFC3527(2003 年 4 月)	Link Selection sub-option for the Relay Agent Information Option for DHCPv4
RFC5107(2008 年 2 月)	DHCP Server Identifier Override Suboption

付録 A.6　DHCPv6 リレーエージェント

表 A–6　DHCPv6 リレーエージェントの準拠規格および勧告

規格番号(発行年月)	規格名
RFC3315(2003 年 7 月)	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
RFC3633(2003 年 12 月)	IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6

付録 A.7　VRRP

表 A–7　VRRP の準拠規格および勧告

規格番号(発行年月)	規格名
RFC3768(2004 年 4 月)	Virtual Router Redundancy Protocol
RFC5798(2010 年 3 月)	Virtual Router Redundancy Protocol Version 3 for IPv4 and IPv6
draft-ietf-vrrp-ipv6-spec-02 (2002 年 3 月)	Virtual Router Redundancy Protocol for IPv6
draft-ietf-vrrp-ipv6-spec-07 (2004 年 10 月)	Virtual Router Redundancy Protocol for IPv6
draft-ietf-vrrp-unified-spec-02 (2008 年 4 月)	Virtual Router Redundancy Protocol Version 3 for IPv4 and IPv6

付録 A.8　RIP

表 A–8　RIP の準拠規格および勧告

規格番号(発行年月)	規格名
RFC1058(1988 年 6 月)	Routing Information Protocol
RFC1519(1993 年 9 月)	Classless Inter-Domain Routing(CIDR): an Address Assignment and Aggregation Strategy
RFC2453(1998 年 11 月)	RIP Version 2
RFC4822(2007 年 2 月)	RIPv2 Cryptographic Authentication

付録 A.9　RIPng

表 A–9　RIPng の準拠規格および勧告

規格番号(発行年月)	規格名
RFC2080(1997 年 1 月)	RIPng for IPv6

付録 A.10　OSPF

表 A–10　OSPF の準拠規格および勧告

規格番号(発行年月)	規格名
RFC1519(1993 年 9 月)	Classless Inter-Domain Routing(CIDR): an Address Assignment and Aggregation Strategy
RFC2328(1998 年 4 月)	OSPF Version 2
RFC3101(2003 年 1 月)	The OSPF Not-So-Stubby Area (NSSA) Option
RFC3137(2001 年 6 月)	OSPF Stub Router Advertisement
RFC3623(2003 年 11 月)	Graceful OSPF Restart
RFC5250(2008 年 7 月)	The OSPF Opaque LSA Option
RFC5309(2008 年 10 月)	Point-to-Point Operation over LAN in Link State Routing Protocols

付録 A.11　OSPFv3

表 A–11　OSPFv3 の準拠規格および勧告

規格番号(発行年月)	規格名
RFC3137(2001 年 6 月)	OSPF Stub Router Advertisement
RFC5187(2008 年 6 月)	OSPFv3 Graceful Restart
RFC5309(2008 年 10 月)	Point-to-Point Operation over LAN in Link State Routing Protocols
RFC5340(2008 年 7 月)	OSPF for IPv6
draft-kompella-ospf-opaquev2-00 (2002 年 10 月)	OSPFv2 Opaque LSAs in OSPFv3

付録 A.12　BGP4

表 A–12　BGP4 の準拠規格および勧告

規格番号(発行年月)	規格名
RFC1519(1993 年 9 月)	Classless Inter-Domain Routing(CIDR): an Address Assignment and Aggregation Strategy
RFC1997(1996 年 8 月)	BGP Communities Attribute
RFC2385(1998 年 8 月)	Protection of BGP Sessions via the TCP MD5 Signature Option
RFC2439(1998 年 11 月)	BGP Route Flap Damping
RFC2918(2000 年 9 月)	Route Refresh Capability for BGP-4
RFC4271(2006 年 1 月)	A Border Gateway Protocol 4 (BGP-4)

規格番号(発行年月)	規格名
RFC4456(2006 年 8 月)	BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)
RFC4724(2007 年 1 月)	Graceful Restart Mechanism for BGP
RFC5004(2007 年 9 月)	Avoid BGP Best Path Transitions from One External to Another
RFC5065(2007 年 8 月)	Autonomous System Confederations for BGP
RFC5492(2009 年 2 月)	Capabilities Advertisement with BGP-4
RFC6793(2012 年 12 月)	BGP Support for Four-Octet Autonomous System (AS) Number Space
RFC6996(2013 年 7 月)	Autonomous System (AS) Reservation for Private Use
RFC7705(2015 年 11 月)	Autonomous System Migration Mechanisms and Their Effects on the BGP AS_PATH Attribute

付録 A.13　BGP4+

表 A-13　BGP4+の準拠規格および勧告

規格番号(発行年月)	規格名
RFC1997(1996 年 8 月)	BGP Communities Attribute
RFC2385(1998 年 8 月)	Protection of BGP Sessions via the TCP MD5 Signature Option
RFC2439(1998 年 11 月)	BGP Route Flap Damping
RFC2545(1999 年 3 月)	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
RFC2918(2000 年 9 月)	Route Refresh Capability for BGP-4
RFC4271(2006 年 1 月)	A Border Gateway Protocol 4 (BGP-4)
RFC4456(2006 年 8 月)	BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)
RFC4724(2007 年 1 月)	Graceful Restart Mechanism for BGP
RFC4760(2007 年 1 月)	Multiprotocol Extensions for BGP-4
RFC5004(2007 年 9 月)	Avoid BGP Best Path Transitions from One External to Another
RFC5065(2007 年 8 月)	Autonomous System Confederations for BGP
RFC5492(2009 年 2 月)	Capabilities Advertisement with BGP-4
RFC6793(2012 年 12 月)	BGP Support for Four-Octet Autonomous System (AS) Number Space
RFC6996(2013 年 7 月)	Autonomous System (AS) Reservation for Private Use
RFC7705(2015 年 11 月)	Autonomous System Migration Mechanisms and Their Effects on the BGP AS_PATH Attribute

付録 A.14　IPv4 マルチキャスト

表 A-14　IP マルチキャストの準拠規格および勧告

規格番号(発行年月)	規格名
RFC2236(1997 年 11 月)	Internet Group Management Protocol,Version2
RFC2362(1998 年 6 月)※1	Protocol Independent Multicast-Sparse Mode (PIM-SM) : Protocol Specification
RFC2934(2000 年 10 月)	Protocol Independent Multicast MIB for IPv4
RFC3376(2002 年 10 月)	Internet Group Management Protocol, Version 3
RFC4601(2006 年 8 月)	Protocol Independent Multicast-Sparse Mode (PIM-SM) : Protocol Specification (Revised)
RFC4604(2006 年 8 月)	Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast
RFC4607(2006 年 8 月)	Source-Specific Multicast for IP
RFC4608(2006 年 8 月)	Source-Specific Protocol Independent Multicast in 232/8
RFC5059(2008 年 1 月)※2	Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)

注※1　この規格はブートストラップルータ，タイマ値の Oif-Deletion-Delay および Probe-Time だけ準拠しています。

注※2　この規格は PIM Hello オプションの Generation ID 関連部およびブートストラップメッセージのフラグメント機能だけ準拠しています。

付録 A.15　IPv6 マルチキャスト

表 A-15　IPv6 マルチキャストの準拠規格および勧告

規格番号(発行年月)	規格名
RFC2362(1998 年 6 月)※1	Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification
RFC2710(1999 年 10 月)	Multicast Listener Discovery (MLD) for IPv6
RFC3590(2003 年 9 月)	Source Address Selection for the Multicast Listener Discovery (MLD) Protocol
RFC3810(2004 年 6 月)	Multicast Listener Discovery Version 2 (MLDv2) for IPv6
RFC4601(2006 年 8 月)	Protocol Independent Multicast-Sparse Mode (PIM-SM) : Protocol Specification (Revised)
RFC4604(2006 年 8 月)	Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast
RFC4607(2006 年 8 月)	Source-Specific Multicast for IP

規格番号(発行年月)	規格名
RFC5059(2008 年 1 月)※2	Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)

注※1　この規格はブートストラップルータ，タイマ値の Oif-Deletion-Delay および Probe-Time だけ準拠しています。

注※2　この規格は PIM Hello オプションの Generation ID 関連部およびブートストラップメッセージのフラグメント機能だけ準拠しています。

付録 A.16　BFD

表 A-16　BFD の準拠規格および勧告

規格番号(発行年月)	規格名
RFC5880(2010 年 6 月)	Bidirectional Forwarding Detection (BFD)
RFC5881(2010 年 6 月)	Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)
RFC5882(2010 年 6 月)	Generic Application of Bidirectional Forwarding Detection (BFD)
RFC5883(2010 年 6 月)	Bidirectional Forwarding Detection (BFD) for Multihop Paths

索引

数字

6to4 アドレス　34

A

Address Conflict Detection　11
ADVERTISEMENT パケットの送信　146
ADVERTISEMENT パケットの認証　147
ARP　9
ARP 情報の確認　26
ARP 情報の参照　11
ARP 情報の設定　11
ARP パケットのチェック内容　9
ARP パケットフォーマット　9
ARP パケット有効性チェック　9
AS 外経路　274
AS 外経路の広告　275

B

BFD　709
BFD および連携するプロトコルのコンフィグレーションコマンド一覧　718
BFD セッション　710
BFD の運用コマンド一覧　721
BGP4　367
BGP4+　367
BGP4+学習経路数制限のコンフィグレーションコマンド一覧　454
BGP4+拡張機能　403
BGP4+広告用経路生成のコンフィグレーションコマンド一覧　446
BGP4+の運用コマンド一覧　399
BGP4+のコンフィグレーションコマンド一覧　391
BGP4+ピアグループのコンフィグレーションコマンド一覧　441
BGP4+マルチパスのコンフィグレーションコマンド一覧　444
BGP4 学習経路数制限のコンフィグレーションコマンド一覧　439
BGP4 拡張機能　403
BGP4 広告用経路生成のコンフィグレーションコマンド一覧　431
BGP4 の運用コマンド一覧　399
BGP4 のコンフィグレーションコマンド一覧　383
BGP4 ピアグループのコンフィグレーションコマンド一覧　427
BGP4 マルチパスのコンフィグレーションコマンド一覧　430
BGP スピーカ　369

D

DHCP/BOOTP パケット転送時の設定内容116, 117
DHCP/BOOTP プロトコル　115
DHCP/BOOTP リレーエージェント　113
DHCP/BOOTP リレーエージェント使用時の注意事項　121
DHCP/BOOTP リレーエージェントの運用コマンド一覧　128
DHCP/BOOTP リレーエージェントのコンフィグレーションコマンド一覧　122
DHCP Option82　119
DHCPv6 パケット転送時の設定内容　132
DHCPv6 リレーエージェント　129
DHCPv6 リレーエージェントの運用コマンド一覧　141
DHCPv6 リレーエージェントのコンフィグレーションコマンド一覧　136
DR の決定および動作　631
DR の決定および動作〔PIM-SM〕　564
DR の動作　564
Duplicate Address Detection　46

F

Forwarder の決定〔IPv6 経路制御機能〕　630
Forwarder の決定〔PIM-SM〕　562

I

ICMP　6
ICMP Redirect の送信仕様　8
ICMP Time Exceeded の送信仕様　8
ICMPv6　44
ICMPv6 Redirect の送信仕様　45
ICMPv6 Time Exceeded の送信仕様　45
ICMPv6 メッセージサポート仕様　44
ICMP メッセージサポート仕様　7
ICMP メッセージフォーマット　6
IGMPv2 使用時の IPv4 グループメンバ管理　549

IGMPv2 マルチキャストグループの参加および離脱動作　546
IGMPv3 使用時の IPv4 グループメンバ管理　550
IGMPv3 マルチキャストグループの参加および離脱動作　548
IGMP の動作　546
IGMP メッセージサポート仕様　544
IPv4 PIM-SM　557
IPv4 PIM-SM 使用上の注意事項　568
IPv4 PIM-SSM　568
IPv4 インタフェースの up/down 確認　25
IPv4 埋め込み IPv6 アドレス　34
IPv4 グループメンバの管理　549
IPv4 経路集約の運用コマンド一覧　195
IPv4 経路制御機能　557
IPv4 互換アドレス　33
IPv4 コンフィグレーションコマンド一覧　22
IPv4 射影アドレス　33
IPv4 使用時の注意事項　19
IPv4 スタティックルーティングの運用コマンド一覧　224
IPv4 で使用する通信プロトコル　5
IPv4 マルチキャストアドレス　542
IPv4 マルチキャスト概説　542
IPv4 マルチキャストグループマネージメント機能　544
IPv4 マルチキャスト中継　580
IPv4 マルチキャスト中継機能　555
IPv4 マルチキャスト中継対象外アドレス　555
IPv4 マルチキャストの運用コマンド一覧　603
IPv4 マルチキャストの解説　541
IPv4 マルチキャストのコンフィグレーションコマンド一覧　590
IPv4 マルチキャストの設定と運用　589
IPv4 マルチキャストルーティング機能　543
IPv4 マルチキャストルーティングプロトコル概説　557
IPv4 ルーティング機能の概要　4
IPv6 PIM-SM　624
IPv6 PIM-SM 使用時の注意事項　635
IPv6 PIM-SM タイマ仕様　632
IPv6 PIM-SSM　636
IPv6 アドレス　28
IPv6 アドレス付与単位　40
IPv6 インタフェースの up/down 確認　55
IPv6 拡張ヘッダサポート仕様　43
IPv6 拡張ヘッダの項目　43
IPv6 グループメンバの管理　617
IPv6 グローバルアドレス　32
IPv6 経路集約の運用コマンド一覧　195
IPv6 経路制御機能　624
IPv6 コンフィグレーションコマンド一覧　52
IPv6 サイトローカルアドレス　32
IPv6 使用時の注意事項　49
IPv6 スタティックルーティングの運用コマンド一覧　224
IPv6 中継回線の MTU 長の変更　49
IPv6 で使用する通信プロトコル　41
IPv6 パケットフォーマット　41
IPv6 パケットヘッダのチェック内容　42
IPv6 パケットヘッダ有効性チェック　41
IPv6 ヘッダ形式　42
IPv6 マルチキャストアドレス　36, 610
IPv6 マルチキャスト概説　610
IPv6 マルチキャスト拡張機能　677
IPv6 マルチキャスト拡張機能の運用コマンド一覧　693
IPv6 マルチキャストグループマネージメント機能　612
IPv6 マルチキャスト中継　646
IPv6 マルチキャスト中継機能　622
IPv6 マルチキャスト中継対象外アドレス　622
IPv6 マルチキャストの運用コマンド一覧　671
IPv6 マルチキャストの解説　609
IPv6 マルチキャストのコンフィグレーションコマンド一覧　658
IPv6 マルチキャストの設定と運用　657
IPv6 マルチキャストパケット中継処理　622
IPv6 マルチキャストルーティング機能　610
IPv6 リンクローカルアドレス　32
IPv6 ルーティング機能の概要　40
IPv6 レイヤ機能　40
IPv6・NDP・ICMPv6 の運用コマンド一覧　55
IPv6・NDP・ICMPv6 の解説　27
IPv6・NDP・ICMPv6 の設定と運用　51
IPX 互換アドレス　34
IP アドレス　2
IP アドレスフォーマット　2
IP アドレス付与単位　4
IP オプションサポート仕様　6
IP パケットの中継方法　12
IP パケットフォーマット　5
IP パケットヘッダのチェック内容　5
IP パケットヘッダ有効性チェック　5
IP レイヤ機能　4
IP・ARP・ICMP の運用コマンド一覧　25
IP・ARP・ICMP の解説　1
IP・ARP・ICMP の設定と運用　21

M

MLDv1/MLDv2 装置との接続　620
MLDv1 マルチキャストグループの参加および離脱動作　614
MLD 使用時の注意事項　621
MLD タイマ値　618
MLD の概要　612
MLD の動作　614
MLD メッセージサポート仕様　612
MTU　16
MTU とフラグメント　16
MTU とフラグメント〔中継機能〕　16

N

NDP　45
NDP エントリの削除条件　45
NDP 情報の確認　56
NDP 情報の参照　45
NSAP 互換アドレス　34
Null インタフェース　69
Null インタフェースの運用コマンド一覧　74
Null インタフェースのコンフィグレーションコマンド一覧　72
Null インタフェースの設定　72

O

OSPF　271
OSPFv3　321
OSPFv3 インタフェースのコンフィグレーションコマンド一覧　336
OSPFv3 拡張機能　343
OSPFv3 拡張機能の運用コマンド一覧　363
OSPFv3 基本機能のコンフィグレーションコマンド一覧　329
OSPFv3 の運用コマンド一覧　338
OSPF 拡張機能　295
OSPF 拡張機能の運用コマンド一覧　318
OSPF 基本機能のコンフィグレーションコマンド一覧　280
OSPF の運用コマンド一覧　290
OSPF パケット, NBMA 設定に関するコンフィグレーションコマンド一覧　287

P

PIM 非接続インタフェース　652
PIM-SM タイマ仕様　565
PIM-SM の動作概要〔IPv4 マルチキャスト〕　558
PIM-SM の動作概要〔IPv6 マルチキャスト〕　625
PIM-SM メッセージサポート仕様　557
PIM-SM メッセージのサポート仕様　624
PIM-SM〔マルチキャストルーティングプロトコル概説〕　557
PIM-SSM〔マルチキャストルーティングプロトコル概説〕　557
ProxyARP　10
ProxyNDP　45

Q

Querier と Non-Querier の決定〔IPv4〕　549
Querier と Non-Querier の決定〔IPv6〕　616
Querier の決定〔IPv4 マルチキャスト〕　548
Querier の決定〔IPv6 マルチキャスト〕　616

R

RA　103
RA の運用コマンド一覧　112
RA のコンフィグレーションコマンド一覧　110
RFC との差分〔PIM-SM 使用上の注意事項〕 568, 635
RIP　227
RIPng　253
RIPng の運用コマンド一覧　269
RIPng のコンフィグレーションコマンド一覧　265
RIP の運用コマンド一覧　251
RIP のコンフィグレーションコマンド一覧　245

T

TCP MD5 認証の運用コマンド一覧　462
TCP MD5 認証のコンフィグレーションコマンド一覧〔BGP4+〕　445
TCP MD5 認証のコンフィグレーションコマンド一覧〔BGP4〕　431
Teredo IPv6 アドレス　35

U

uRPF　77
uRPF の運用コマンド一覧　82
uRPF のコンフィグレーションコマンド一覧　81

V

VRF　57, 58, 204
VRF インスタンス　58
VRF の運用コマンド一覧　67, 211
VRF のコンフィグレーションコマンド一覧　65, 209
VRRP　143

VRRP における障害検出の仕組み　146
VRRP の運用コマンド一覧　166
VRRP のコンフィグレーションコマンド一覧　155
VRRP のコンフィグレーションの流れ　155

あ

アクセプトモード　148
宛先アドレスとの通信可否の確認〔IPv4〕　25
宛先アドレスとの通信可否の確認〔IPv6〕　55
宛先アドレスまでの経路確認〔IPv4〕　26
宛先アドレスまでの経路確認〔IPv6〕　56
アドレス自動生成例　39
アドレス表記方法　30
アドレスフォーマットプレフィックス　30
アドレスフォーマットプレフィックスの種類　31
アドレッシング〔IPv4〕　2
アドレッシング〔IPv6〕　28
暗号認証使用時の注意事項〔RIP-2〕　243
暗号認証の認証手順〔RIP-2〕　243

い

イコールコストマルチパス　278
インターネットプロトコル（IP）　5
インターネットプロトコル　バージョン 6（IPv6）41
インタフェース ID 省略時のアドレス自動生成　38
インタフェースダウン時の外部ピア即時切断機能の運用コマンド一覧　471
インタフェースダウン時の外部ピア即時切断機能のコンフィグレーションコマンド一覧〔BGP4+〕　455
インタフェースダウン時の外部ピア即時切断機能のコンフィグレーションコマンド一覧〔BGP4〕　439
インタフェースの設定〔IPv4〕　22
インタフェースの設定〔IPv6〕　52
インタフェースへの複数グローバルアドレスの設定　49

え

エージングタイマ　11
エクストラネット　63
エニキャストアドレス　28
エニキャストアドレス通信　29
エリアとエリア分割機能の解説　296
エリアのバックボーンへの接続　299
エリア分割についての注意事項　296
エリア分割を使用した OSPF ネットワークトポロジの例　296
エリアボーダルータでの経路の集約　297
エリアボーダルータについての注意事項　296

お

オールサブネットワークブロードキャスト　15
オペレーション　166
オペレーション〔IPv6・NDP・ICMPv6〕　55
オペレーション〔IP・ARP・ICMP〕　25

か

学習経路数制限の運用コマンド一覧　470
仮想 MAC 宛てフレームの受信　145
仮想 MAC アドレスによる ARP 応答および NDP 応答　145
仮想リンク　299
仮想リンクの動作　300
仮想ルータの MAC アドレスと IP アドレス　144

き

近隣検出〔IPv6 マルチキャスト〕　629
近隣検出〔PIM-SM〕　562

く

グレースフル・リスタートの運用コマンド一覧　468
グレースフル・リスタートのコンフィグレーションコマンド一覧〔BGP4+〕　453
グレースフル・リスタートのコンフィグレーションコマンド一覧〔BGP4〕　438
グレースフル・リスタートのコンフィグレーションコマンド一覧〔OSPFv3〕　358
グレースフル・リスタートのコンフィグレーションコマンド一覧〔OSPF〕　313
グローバルアドレス　32

け

経路集約のコンフィグレーションコマンド一覧　192
経路選択アルゴリズム　273
経路選択の基準　276
経路の集約および抑止とエリア外への要約　297
経路フィルタリング　473
経路フィルタリングの運用コマンド一覧（IPv4）532
経路フィルタリングの運用コマンド一覧（IPv6）532
経路フィルタリングのコンフィグレーションコマンド一覧（IPv4）　496
経路フィルタリングのコンフィグレーションコマンド一覧（IPv6）　514

こ

広告用経路生成の運用コマンド一覧　463
コミュニティの運用コマンド一覧　457

コミュニティのコンフィグレーションコマンド一覧〔BGP4+〕　442
コミュニティのコンフィグレーションコマンド一覧〔BGP4〕　428
コンフィグレーション〔IPv6・NDP・ICMPv6〕　52
コンフィグレーション〔IP・ARP・ICMP〕　22
コンフィグレーション〔VRRP〕　155
コンフェデレーションの運用コマンド一覧　466
コンフェデレーションのコンフィグレーションコマンド一覧〔BGP4+〕　451
コンフェデレーションのコンフィグレーションコマンド一覧〔BGP4〕　436

さ

最短パスのマルチキャストパケット通信〔PIM-SM〕　561, 628
サイトローカルアドレス　32
サブネットマスク　2
サブネットワークブロードキャスト　14
サブネットワークへのブロードキャストパケットを使った攻撃例　13
サポート機能のネゴシエーションの運用コマンド一覧　459
サポート範囲〔DHCP/BOOTP リレーエージェント〕　114
サポート範囲〔DHCPv6 リレーエージェント〕　130

し

システム構成例（AS 境界ルータを目標とする場合）　277
システム構成例（任意のインタフェースを目標とする場合）　278
システム構成例（フォワーディングアドレスを目標とする場合）　277
自動切り戻しおよび自動切り戻しの抑止　147
冗長経路（障害などによる経路切り替え）〔IPv4 マルチキャスト〕　581
冗長経路（障害などによる経路切り替え）〔IPv6 マルチキャスト〕　647
冗長経路時の注意事項〔IPv4 マルチキャスト(PIM-SM)〕　565
冗長経路時の注意事項〔IPv6 マルチキャスト〕　632

す

スタティック ARP の設定　24
スタティック NDP 情報の設定　45
スタティック NDP の設定　54
スタティックルーティング　170, 213
スタティックルーティングのコンフィグレーションコマンド一覧　219
スタブエリア，NSSA を使用する場合と，エリアボーダルータとして動作する場合のコンフィグレーションコマンド一覧　302
スタブエリアを使用する場合と，エリアボーダルータとして動作する場合のコンフィグレーションコマンド一覧　349
スタブルータのコンフィグレーションコマンド一覧〔OSPFv3〕　362
スタブルータのコンフィグレーションコマンド一覧〔OSPF〕　317
ステートレスアドレス自動設定機能　39

せ

静的グループ参加機能　620
設定できないアドレス〔IPv6〕　38
設定できるアドレス〔IPv6〕　38
全ノードアドレス　37
全ルータアドレス　37

そ

ソフトウェアによるマルチキャストパケット中継処理　555

た

ダイナミックルーティング　170
ダイレクトブロードキャスト中継の設定　23

ち

中継機能〔IPv4 パケット中継〕　12
中継機能〔IPv4 レイヤ機能〕　4
中継機能〔IPv6 パケット中継〕　47
中継機能〔IPv6 レイヤ機能〕　40

つ

通信機能〔IPv4〕　5
通信機能〔IPv6〕　41

て

適応ネットワーク構成例〔IPv4 マルチキャスト〕582
適応ネットワーク構成例〔IPv6 マルチキャスト〕649
デフォルト動作　90

と

動作〔PIM-SM〕　558

に

認証キーの変更手順〔RIP-2〕　243

ね

ネガティブキャッシュエントリ〔IPv4〕　556
ネガティブキャッシュエントリ〔IPv6〕　623
ネットワーク構成での注意事項〔IPv4 マルチキャスト〕　584
ネットワーク構成での注意事項〔IPv6 マルチキャスト〕　650
ネットワーク設計の考え方〔IPv4 マルチキャスト〕　580
ネットワーク設計の考え方〔IPv6 マルチキャスト〕　646
ネットワークブロードキャスト　14

の

ノンストップルーティングの運用コマンド一覧　467
ノンストップルーティングのコンフィグレーションコマンド一覧〔BGP4+〕　452
ノンストップルーティングのコンフィグレーションコマンド一覧〔BGP4〕　437
ノンストップルーティングのコンフィグレーションコマンド一覧〔OSPFv3〕　353
ノンストップルーティングのコンフィグレーションコマンド一覧〔OSPF〕　309

は

ハードウェアによるマルチキャストパケット中継処理　555
廃棄プレフィックスアドレス　35
バインディング（IA_PD）　134
パケットのフラグメント化　17
バックボーン　296
バックボーン間の接続　300
バックボーン分断に対する予備経路　300

ひ

ピアグループの運用コマンド一覧　456
平文パスワード認証の認証手順〔RIP-2〕　243

ふ

フォロー仮想ルータ　152
プライマリ仮想ルータ　151
フラグメント化　16
フラグメント化モデル　16
フラグメントの再構成　17
フラグメントの生成　16
プレフィックス長で設定できる具体例　39
ブロードキャストパケットの中継方法　13

ほ

ホストトラッキング機能の解説　691
ホストトラッキング機能のコンフィグレーションコマンド一覧　692
ポリシーベースルーティング　85
ポリシーベースルーティングの運用コマンド一覧 100
ポリシーベースルーティングのコンフィグレーションコマンド一覧　94
本装置で使用する IPv6 アドレスの扱い　38

ま

マスタの選出方法　146
マルチキャストアドレス通信　30
マルチキャストアドレスのスコープフィールド値　37
マルチキャストアドレスのフォーマット〔IPv4〕 542
マルチキャストアドレスのフォーマット〔IPv6〕 610
マルチキャストアドレス〔IPv6〕　29, 36
マルチキャスト経路情報またはマルチキャスト中継エントリの検索　623
マルチキャスト経路情報またはマルチキャスト中継エントリの検索方法　556
マルチキャスト経路情報またはマルチキャスト中継エントリの検索〔IPv4 マルチキャスト〕　556
マルチキャスト経路フィルタリング　695
マルチキャスト経路フィルタリングの運用コマンド一覧　707
マルチキャスト経路フィルタリングのコンフィグレーションコマンド一覧　700
マルチキャストチャネル参加制限機能の解説　678
マルチキャストチャネル参加制限機能のコンフィグレーションコマンド一覧　687
マルチキャスト配送ツリーの刈り込み　629
マルチキャスト配送ツリーの刈り込み〔PIM-SM〕 562
マルチパスの運用コマンド一覧　458
マルチホームの設定　23

み

未指定アドレス　32

ゆ

優先度　146
ユニキャストアドレス　32
ユニキャストアドレス通信　28
ユニキャストアドレス〔IPv6〕　28

ユニキャストルーティング　169
ユニキャストルーティング共通の運用コマンド一覧　179

よ

要請ノードアドレス　38

ら

ランデブーポイントおよびブートストラップルータ　625
ランデブーポイントおよびブートストラップルータの役割　559
ランデブーポイント経由のマルチキャストパケット通信（IP カプセル化）　560, 627
ランデブーポイント経由のマルチキャストパケット通信（IP デカプセル化）　561, 627
ランデブーポイントへのマルチキャストグループ参加情報の通知　559

り

リレーエージェント情報オプション　119
リンクローカルアドレス　32
リンクローカルアドレスの手動設定　53
隣接ルータ認証のコンフィグレーションコマンド一覧　306

る

ルーティングテーブルの検索〔IPv4 パケット中継〕12
ルーティングテーブルの検索〔IPv6 パケット中継〕47
ルーティングテーブルの内容〔IPv4 パケット中継〕12
ルーティングテーブルの内容〔IPv6 パケット中継〕47
ルート・フラップ・ダンプニングの運用コマンド一覧　464
ルート･フラップ･ダンプニングのコンフィグレーションコマンド一覧〔BGP4+〕　448
ルート･フラップ･ダンプニングのコンフィグレーションコマンド一覧〔BGP4〕　434
ルート・リフレクションの運用コマンド一覧　465
ルート・リフレクションのコンフィグレーションコマンド一覧〔BGP4+〕　449
ルート・リフレクションのコンフィグレーションコマンド一覧〔BGP4〕　435
ルート・リフレッシュの運用コマンド一覧　460
ループバックアドレス　33
ループバックインタフェースの設定〔IPv4〕　23
ループバックインタフェースの設定〔IPv6〕　53

ろ

ローカル ProxyARP　10