AX6700S・AX6600S・AX6300S 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. 11.7 対応

AX63S-S003-C0

AlaxalA

■対象製品

このマニュアルは AX6700S，AX6600S および AX6300S モデルを対象に記載しています。また，AX6700S，AX6600S および AX6300S のソフトウェア Ver. 11.7 の機能について記載しています。ソフトウェア機能は，基本ソフトウェア OS-SE およびオプションライセンスによってサポートする機能について記載します。

■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。
Internet Explorer は，米国 Microsoft Corporation の米国及びその他の国における登録商標または商標です。
IPX は，Novell,Inc. の商標です。
Microsoft は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
Octpower は，日本電気（株）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。
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。
VitalQIP，VitalQIP Registration Manager は，Lucent technologies の商標です。
VLANaccessClient は，NEC ソフトの商標です。
VLANaccessController，VLANaccessAgent は，NEC の商標です。
Windows は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
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

２０１２年　 1月 （第１３版） ＡＸ６３Ｓ－Ｓ００３－Ｃ０

■著作権

変更履歴

【Ver. 11.7 対応版】

表　変更履歴

章・節・項・タイトル	追加・変更内容
4.1.2　ポリシーベースルーティンググループ	• 本項を追加しました。
14.3　IPv4 マルチキャスト中継機能	•「(5) 系切替時の通信無停止対応機能」を追加しました。
14.6.1　IPv4 マルチキャスト中継	•「(2) PIM-SM の使用」に「(f) 系切替時の通信無停止対応機能使用時の注意事項」および「(g) 系切替時の通信無停止対応機能での IPv4 マルチキャスト中継エントリ再学習時の注意事項」を追加しました。
31.6.1　IPv6 マルチキャスト中継	•「(3) IPv6 PIM-SSM」の「(a) 系切替時の通信無停止対応機能使用時の注意事項」に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. 11.5 対応版】

表　変更履歴

項目	追加・変更内容
ARP	•「(8) アドレス未解決パケットのハードウェア廃棄」を追加しました。
IPv4 マルチキャストルーティングプロトコル概説	• PIM-DM に関する記述を追加しました。また，その他の記述内容を変更しました。
IPv4 PIM-SM	•「(7) PIM-SM の付加機能」を追加しました。
IPv4 PIM-DM	• 本項を追加しました。
VRF での IPv4 マルチキャスト	• PIM-DM に関する記述を追加しました。
IPv4 マルチキャスト中継	• PIM-DM に関する記述を追加しました。
適応ネットワーク構成例	•「(3) PIM-DM を使用する構成」を追加しました。
ネットワーク構成での注意事項	•「(1) PIM-SM および PIM-SSM 共通」の記述を変更しました。 •「(5) PIM-DM」を追加しました。
コンフィグレーションコマンド一覧	• PIM-DM に関する記述を追加しました。
コンフィグレーションの流れ	• PIM-DM に関する記述を追加しました。
IGMP の設定	• PIM-DM に関する記述を追加しました。また，ip igmp router コマンドの有効範囲について記述を追加しました。
IPv4 PIM-DM の設定	• 本項を追加しました。
VRF での IPv4 PIM-SM の設定	• 記述を変更しました。
VRF での IGMP の設定	• 記述を変更しました。
IGMP 情報の確認	• 記述を変更しました。
IPv4 PIM-DM 情報の確認	• 本項を追加しました。

【Ver. 11.4 対応版】

表　変更履歴

項目	追加・変更内容
BGP4	• 経路選択の優先順位を変更しました。 • BGP4 の制限事項を変更しました。
IPv6 DHCP リレー	• 本章を追加しました。
BGP4+	• 経路選択の優先順位を変更しました。 • BGP4+ の制限事項を変更しました。
VRF での IPv6 マルチキャスト	•「(2) IPv6 マルチキャストエクストラネット」を追加しました。 •「(3) PIM-SM VRF ゲートウェイ」を追加しました。 •「(4) IPv6 マルチキャストエクストラネット使用時の注意事項」を追加しました。
ネットワーク構成での注意事項	•「(4) PIM-SM VRF ゲートウェイ」を追加しました。
IPv6 マルチキャストエクストラネットの設定	• 本項を追加しました。
PIM-SM VRF ゲートウェイの設定	• 本項を追加しました。
IPv6 マルチキャスト経路フィルタリング	• 本章を追加しました。

【Ver. 11.3 対応版】

表　変更履歴

項目	追加・変更内容
VRF での IPv6 マルチキャスト	• 本項を追加しました。
コンフィグレーションの流れ	• VRF に関する記述を追加しました。
VRF での IPv6 マルチキャストルーティングの設定	• 本項を追加しました。
VRF での IPv6 PIM-SM の設定	• 本項を追加しました。
VRF での IPv6 PIM-SM ランデブーポイント候補の設定	• 本項を追加しました。
VRF での IPv6 PIM-SM BSR 候補の設定	• 本項を追加しました。
VRF での IPv6 PIM-SM 静的ランデブーポイントの設定	• 本項を追加しました。
VRF での IPv6 PIM-SSM の設定	• 本項を追加しました。
VRF での MLD の設定	• 本項を追加しました。
VRF	•「表 32-3 VRF サポート状況」に IPv6 マルチキャストに関する記述を追加しました。

【Ver. 11.2 対応版】

表　変更履歴

項目	追加・変更内容
ポリシーベースルーティングの注意事項	•「(2) フロー検出拡張モードでのポリシーベースルーティング」を追加しました。
サポート仕様	• エクストラネットの記述を追加しました。
エクストラネット構成での設定	• 本項を追加しました。

項目	追加・変更内容
VRF での IPv4 マルチキャスト	•「(2) IPv4 マルチキャストエクストラネット」を追加しました。 •「(3) PIM-SM VRF ゲートウェイ」を追加しました。 •「(4) IPv4 マルチキャストエクストラネット使用時の注意事項」を追加しました。
ネットワーク構成での注意事項	•「(4) PIM-SM VRF ゲートウェイ」を追加しました。
IPv4 マルチキャストエクストラネットの設定	• 本項を追加しました。
PIM-SM VRF ゲートウェイの設定	• 本項を追加しました。
IPv4 マルチキャスト経路フィルタリング	• 本章を追加しました。
ポリシーベースルーティングの注意事項	•「(2) フロー検出拡張モードでのポリシーベースルーティング」を追加しました。
ポリシーベースルーティングでのエクストラネットの設定	• 本項を追加しました。
RA 送信の間隔時間の目安	• 本項を追加しました。
VRF の解説	• 本節を追加しました。
VRF のコンフィグレーション	• 本節を追加しました。
VRF のオペレーション	• 本節を追加しました。
VRF でのスタティック経路の設定	• 本項を追加しました。
VRF 間にわたるスタティック経路の設定	• 本項を追加しました。
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	• 本項を追加しました。
VRF での RIPng の適用	• 本項を追加しました。
VRF での OSPFv3 の適用	• 本項を追加しました。
VRF での BGP4+ の機能	• 本項を追加しました。
VRF での BGP4+ の設定	• 本項を追加しました。
経路フィルタリング概要	• エクストラネットの記述を追加しました。
エクストラネット	• 本項を追加しました。
エクストラネット	• 本項を追加しました。
エクストラネットの確認	• 本項を追加しました。

【Ver. 11.1 対応版】

表　変更履歴

項目	追加・変更内容
RIP-2	• 認証機能に関する記述を追加しました。
認証の適用	• 本項を追加しました。
パケット制御	• AX6600S の記述を追加しました。
パケット制御	• AX6600S の記述を追加しました。

【Ver. 11.0 対応版】

表　変更履歴

項目	追加・変更内容
ポリシーベースルーティングでのエクストラネットの設定	• 本項を追加しました。
VRF 構成での設定	• 本項を追加しました。
VRF の解説	• 本節を追加しました。
VRF のコンフィグレーション	• 本節を追加しました。
VRF のオペレーション	• 本節を追加しました。
VRF でのスタティック経路の設定	• 本項を追加しました。
VRF 間にわたるスタティック経路の設定	• 本項を追加しました。
VRF での RIP の適用	• 本項を追加しました。
VRF での OSPF の適用	• 本項を追加しました。
BGP4	• コンフィグレーションコマンド neighbor remove-private-as に関する記述を追加しました。
VRF での BGP4 の機能	• 本項を追加しました。
VRF での BGP4 の設定	• 本項を追加しました。
経路フィルタリング概要	• エクストラネットの記述を追加しました。
エクストラネット	• 本項を追加しました。
エクストラネット	• 本項を追加しました。
エクストラネットの確認	• 本項を追加しました。
VRF での IPv4 マルチキャスト	• 本項を追加しました。
VRF での IPv4 マルチキャストルーティングの設定	• 本項を追加しました。
VRF での PIM-SM の設定	• 本項を追加しました。
VRF での IPv4 PIM-SM ランデブーポイント関連の設定	• 本項を追加しました。
VRF での IPv4 PIM-SSM の設定	• 本項を追加しました。
VRF での IGMP の設定	• 本項を追加しました。
BGP4+	• コンフィグレーションコマンド neighbor remove-private-as に関する記述を追加しました。
ネットワーク・パーティション	• 本章を追加しました。

【Ver. 10.6 対応版】

表　変更履歴

項目	追加・変更内容
ARP	•「(4) ローカル ProxyARP」を追加しました。
NSSA	• AS 外経路広告について記述を追加しました。

【Ver. 10.5 対応版】

表　変更履歴

項目	追加・変更内容
経路情報の広告	• RIP 広告経路の自動集約についての記述を追加しました。
IPv4 PIM-SM	• Generation ID の説明を追加しました。
近隣検出	• Generation ID の説明を追加しました。

【Ver. 10.4 対応版】

表　変更履歴

項目	追加・変更内容
BGP4 ピアグループ	• 本項を追加しました。
BGP4 ピアグループのコンフィグレーション	• 本項を追加しました。
BGP4 ピアグループの確認	• 本項を追加しました。
BGP4+ ピアグループ	• 本項を追加しました。
BGP4+ ピアグループのコンフィグレーション	• 本項を追加しました。
BGP4+ ピアグループの確認	• 本項を追加しました。

【Ver. 10.3 対応版】

表　変更履歴

項目	追加・変更内容
ポリシーベースルーティング（IPv4）	• 本章を追加しました。
グレースフル・リスタートの概要	• 本節を追加しました。
高速経路切替機能	• 本節を追加しました。
グレースフル・リスタートの解説	• OSPF のリスタート機能について記述を追加しました。
グレースフル・リスタートのコンフィグレーション	• OSPF のリスタート機能について記述を追加しました。
スタブルータ動作	• OSPF のグレースフル・リスタートについて記述を追加しました。
OSPF 拡張機能のオペレーション	• OSPF のリスタート機能について記述を追加しました。
経路選択	• 相手 BGP 識別子による経路選択について記述を修正しました。 • NEXT_HOP 属性の解決について記述を修正しました。
コンフェデレーション	• 相手 BGP 識別子による経路選択について記述を修正しました。
グレースフル・リスタート	• BGP4 のリスタートルータ機能について記述を追加しました。
グレースフル・リスタートのコンフィグレーション	• BGP4 のリスタートルータ機能について記述を追加しました。
グレースフル・リスタートの確認	• BGP4 のリスタートルータ機能について記述を追加しました。
ポリシーベースルーティング（IPv6）	• 本章を追加しました。
グレースフル・リスタートの概要	• 本節を追加しました。
高速経路切替機能	• 本節を追加しました。
グレースフル・リスタートの解説	• OSPFv3 のリスタート機能について記述を追加しました。
グレースフル・リスタートのコンフィグレーション	• OSPFv3 のリスタート機能について記述を追加しました。
スタブルータ動作	• OSPFv3 のグレースフル・リスタートについて記述を追加しました。

項目	追加・変更内容
OSPFv3 拡張機能のオペレーション	• OSPFv3 のリスタート機能について記述を追加しました。
経路選択	• 相手 BGP 識別子による経路選択について記述を修正しました。 • NEXT_HOP 属性の解決について記述を修正しました。
グレースフル・リスタートのコンフィグレーション	• BGP4+ のリスタートルータ機能について記述を追加しました。
グレースフル・リスタートの確認	• BGP4+ のリスタートルータ機能について記述を追加しました。

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 AX6700S，AX6600S および AX6300S モデルを対象に記載しています。また，AX6700S，AX6600S および AX6300S のソフトウェア Ver. 11.7 の機能について記載しています。ソフトウェア機能は，基本ソフトウェア OS-SE およびオプションライセンスによってサポートする機能について記載します。
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。
なお，このマニュアルでは特に断らないかぎり AX6700S，AX6600S および AX6300S に共通の機能について記載しますが，機種固有の機能については以下のマークで示します。

【AX6700S】：
　AX6700S についての記述です。

【AX6600S】：
　AX6600S についての記述です。

【AX6300S】：
　AX6300S についての記述です。
また，このマニュアルでは特に断らないかぎり基本ソフトウェア OS-SE の機能について記載しますが，オプションライセンスでサポートする機能については以下のマークで示します。

【OP-BGP】：
　オプションライセンス OP-BGP についての記述です。

【OP-DH6R】：
　オプションライセンス OP-DH6R についての記述です。

【OP-MBSE】：
　オプションライセンス OP-MBSE についての記述です。

【OP-NPAR】：
　オプションライセンス OP-NPAR についての記述です。

【OP-VAA】：
　オプションライセンス OP-VAA についての記述です。

■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。
http://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

AX6700S クイックスタートガイド (AX67S-Q001)	AX6600S クイックスタートガイド (AX66S-Q001)	AX6300S クイックスタートガイド (AX63S-Q001)

●ハードウェアの設備条件，取扱方法を調べる

AX6700S ハードウェア取扱説明書 (AX67S-H001)	AX6600S ハードウェア取扱説明書 (AX66S-H001)	AX6300S ハードウェア取扱説明書 (AX63S-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 ・VLAN，スパニングツリー	・フィルタ，QoS ・レイヤ2認証 ・高信頼化機能	・IPv4，IPv6パケット中継 ・IPv4，IPv6ルーティング プロトコル
コンフィグレーションガイド Vol.1 (AX63S-S001)	コンフィグレーションガイド Vol.2 (AX63S-S002)	コンフィグレーションガイド Vol.3 (AX63S-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 (AX63S-S004)	コンフィグレーション コマンドレファレンス Vol.2 (AX63S-S010)	コンフィグレーション コマンドレファレンス Vol.3 (AX63S-S005)
運用コマンドレファレンス Vol.1 (AX63S-S006)	運用コマンドレファレンス Vol.2 (AX63S-S011)	運用コマンドレファレンス Vol.3 (AX63S-S007)

・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 (AX63S-S008)

・MIBについて

MIBレファレンス (AX63S-S009)

●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 (AX36S-T001)

■このマニュアルでの表記

AC	Alternating Current
ACK	ACKnowledge
ADSL	Asymmetric Digital Subscriber Line
ALG	Application Level Gateway
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AS	Autonomous System
AUX	Auxiliary
BCU	Basic Control Unit
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。
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
BSU	Basic Switching Unit
CC	Continuity Check
CDP	Cisco Discovery Protocol
CFM	Connectivity Fault Management
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network System
CONS	Connection Oriented Network System
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNP	Complete Sequence Numbers PDU
CST	Common Spanning Tree
CSU	Control and Switching Unit
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DHCP	Dynamic Host Configuration Protocol
DIS	Draft International Standard/Designated Intermediate System
DNS	Domain Name System
DR	Designated Router
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EFM	Ethernet in the First Mile
ES	End System
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FTTH	Fiber To The Home
GBIC	GigaBit Interface Converter
GSRP	Gigabit Switch Redundancy Protocol
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
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCP	IP Control Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IP Version 6 Control Protocol
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Internal Spanning Tree
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLPQ	Low Latency Priority Queueing
LLQ+3WFQ	Low Latency Queueing + 3 Weighted Fair Queueing
LLRLQ	Low Latency Rate Limited Queueing
LSP	Label Switched Path
LSP	Link State PDU
LSR	Label Switched Router
MA	Maintenance Association
MAC	Media Access Control

MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MEP	Maintenance association End Point
MIB	Management Information Base
MIP	Maintenance domain Intermediate Point
MRU	Maximum Receive Unit
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MSU	Management and Switching Unit
MTU	Maximum Transfer Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NAT	Network Address Translation
NCP	Network Control Protocol
NDP	Neighbor Discovery Protocol
NET	Network Entity Title
NIF	Network Interface
NLA ID	Next-Level Aggregation Identifier
NPDU	Network Protocol Data Unit
NSAP	Network Service Access Point
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OADP	Octpower Auto Discovery Protocol
OAM	Operations,Administration,and Maintenance
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
packet/s	packets per second　　*ppsと表記する場合もあります。
PAD	PADding
PAE	Port Access Entity
PC	Personal Computer
PCI	Protocol Control Information
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PIM-SSM	Protocol Independent Multicast-Source Specific Multicast
PRI	Primary Rate Interface
PS	Power Supply
PSNP	Partial Sequence Numbers PDU
PSP	Packet Switching Processor
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
REJ	REJect
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
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
SD	Secure Digital
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SEL	NSAP SELector
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SOP	System Operational Panel
SPF	Shortest Path First
SSAP	Source Service Access Point
STP	Spanning Tree Protocol
TA	Terminal Adapter

TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
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
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
uRPF	unicast Reverse Path Forwarding
VAA	VLAN Access Agent
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
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queueing
WGQ	Weighted Guaranteed Queueing
WRED	Weighted Random Early Detection
WS	Work Station
WWW	World-Wide Web
XFP	10 gigabit small Form factor Pluggable

■ kB(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　IPv4 パケット中継

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。

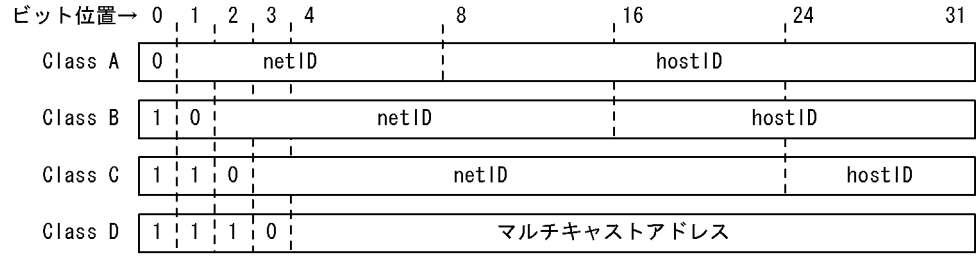
1.1 アドレッシング

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依存しますが，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おり，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，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，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。

1.2 IP レイヤ機能

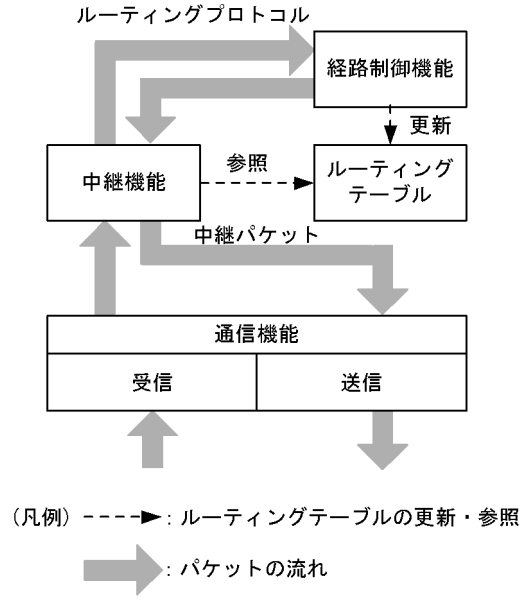
1.2.1 中継機能

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行う機能です。
- 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 VLAN に対して IP アドレスを設定します。一つの VLAN に複数の IP アドレスを設定するマルチホーム接続も可能です。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 のパケット中継で使用する通信プロトコルについて説明します。IPv4 の通信プロトコルとして，次のプロトコルが使用できます。

- 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 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 パケットのヘッダの有効性チェックを行います。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	○	×
ヘッダレングス	ヘッダレングス≧ 5 であること	○	×
TOS	チェックしない	―	―
トータルレングス	トータルレングス≧ 4 ×ヘッダレングスであること	○	×
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	―	―
	フォワーディングするパケットの 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	チェックしない	―	―
宛先アドレス	次の条件をすべて満たすこと 1. クラス A，クラス B，クラス C，クラス D 2. ネットワーク番号が 127(内部ループバックアドレス) でないこと 3. ネットワーク番号が 0 でないこと (ただし，0.0.0.0 を除く)	○	×

(凡例) ○：行う　×：行わない　―：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

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 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 (値は 10 進)

ICMP メッセージ				サポート
タイプ (種別)		コード (詳細種別)		
―	値	―	値	
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	×
		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	×

ICMP メッセージ				サポート
タイプ (種別)		コード (詳細種別)		
―	値	―	値	
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	×
Time Exceeded	11	Time to Live Exceeded in Transit	0	○
		Fragment Reassembly Time Exceeded	1	×
Parameter Problem	12	―	0	○
Echo Request	8	―	0	○
Echo Reply	0	―	0	○
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。

- フォワーディングする受信 IP パケットの TTL が 1
- 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 フレームフォーマット

本装置が送信する ARP フレームのフォーマット，および設定値は RFC826 に従います。

(2) ARP フレーム有効性チェック

本装置は，受信した ARP フレームの有効性をチェックします。ARP フレームのチェック内容を次の表に示します。

表 1-4 ARP フレームのチェック内容

ARP フレームフィールド	チェック内容	フレーム廃棄
ハードウェアタイプ	(イーサネットの場合) 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	チェックしない	―
プロトコルアドレス長	チェックしない	―
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	以下の値ではないこと • マルチキャストアドレス • 自装置プロトコルアドレスと同じ • 0.0.0.0	○
宛先ハードウェアアドレス	• 自宛ハードウェアアドレスであること • ブロードキャストアドレスであること	○
宛先プロトコルアドレス	• 自装置のプロトコルアドレスであること	○

(凡例) ○：チェック異常のときフレームを廃棄する　―：該当しない

注※
「Trailer packet」の自発送信は行いませんが，要求のあった場合は応答を返して学習をします。

(3) ProxyARP

本装置はすべてのインタフェースで ProxyARP を動作させることができます。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

(4) ローカル ProxyARP

本装置はすべてのインタフェースでローカル ProxyARP を動作させることができます。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や，ブロードキャストが禁止されているサブネットで使用します。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，コンフィグレーションコマンド l2-isolation 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，本機能により ICMP リダイレクトが多発しますので，ICMP リダイレクト機能を無効にすることをお勧めします。

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番号が，受信インタフェースのサブネット番号と等しい
- 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

(5) 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。

(6) 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。

(7) ARP 情報の参照

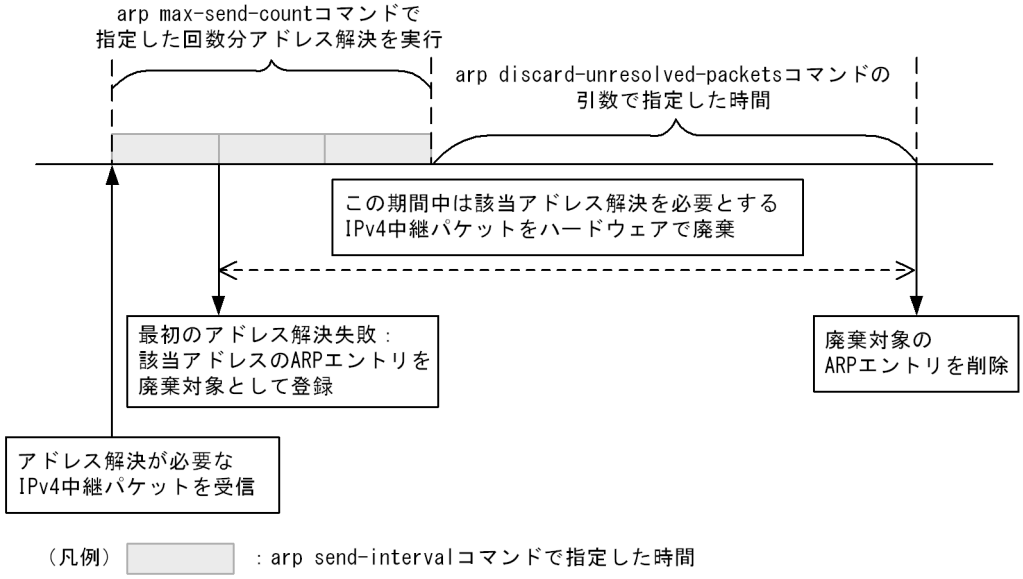
運用端末から show ip arp コマンドで ARP 情報が参照できます。ARP 情報から該当インタフェースの IP アドレスと MAC アドレスの対応がわかります。

(8) アドレス未解決パケットのハードウェア廃棄

ネットワーク構成上の理由で存在しない端末宛ての通信や，存在しないルータを経由する通信を続けると，アドレス解決が必要な中継パケットが CPU に渡され，CPU が高負荷状態となるおそれがあります。このような場合，コンフィグレーションコマンド arp discard-unresolved-packets を設定すると，アドレス解決できない中継パケットをハードウェアで廃棄して，CPU 負荷を軽減できます。

アドレス未解決パケットのハードウェア廃棄の動作を次に示します。

図 1-3 アドレス未解決パケットのハードウェア廃棄の動作



arp discard-unresolved-packets コマンドを設定したインタフェースでは，最初のアドレス解決に失敗したとき，ハードウェアに該当 ARP エントリを廃棄対象エントリとして一時的に登録します。該当 ARP エントリ宛て，および該当 ARP エントリをネクストホップとする中継パケットは，コンフィグレーションコマンド arp max-send-count で指定した回数分のアドレス解決がすべて失敗したあと arp discard-unresolved-packets コマンドで指定した時間が経過するまで，ハードウェアによって廃棄されるため，CPU の負荷が軽減されます。なお，次回のアドレス解決が成功すると，以降は通常どおり通信できます。

本機能はアドレス未解決状態が持続するような特殊な環境でだけ使用してください。

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処理です。

(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おり，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 show ip route コマンドで表示できます。

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，classA なら 8）を表示します。なお，ホストアドレスによる中継を行う場合には 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称です。

Metric：ルートのメトリックです。

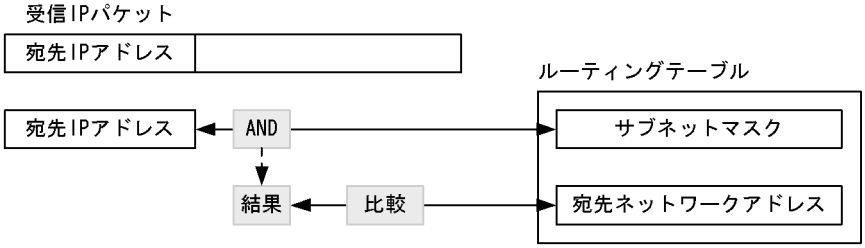
Protocol：学習元プロトコルです。

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 1-4 ルーティングテーブルの検索



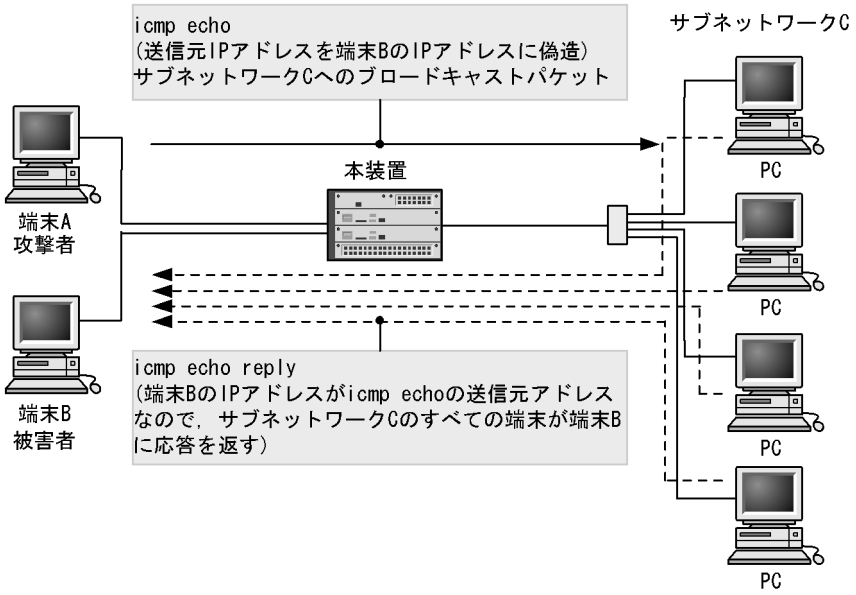
1.4.2 ブロードキャストパケットの中継方法

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コマンドで設定できます。ip subnet-broadcast コマンドは受信側のインタフェースの動作を設定します。また，ip address コマンドの directed-broadcast パラメータでは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コマンド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となります。

図 1-5　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



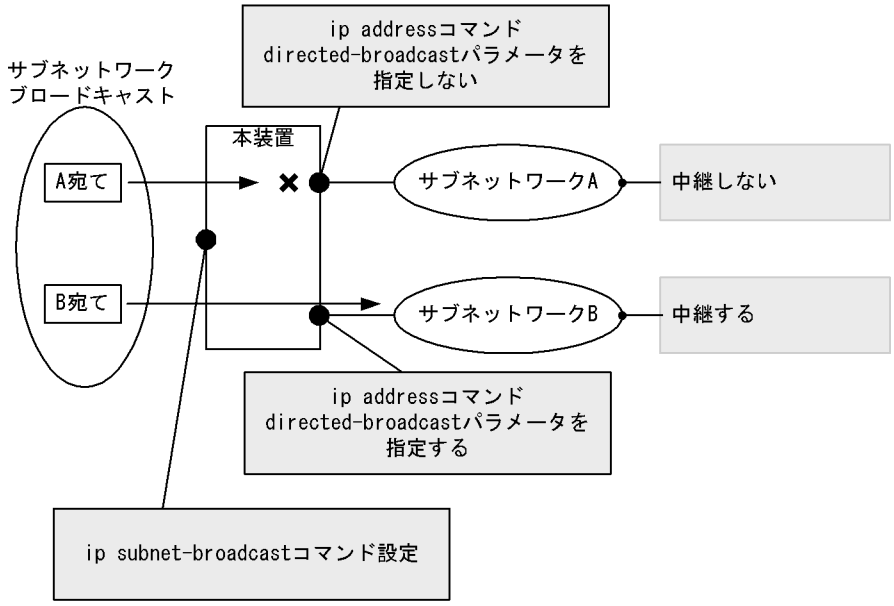
ip subnet-broadcast コマンドが設定され，かつ ip address コマンドの directed-broadcast パラメータが指定された場合に，ダイレクトブロードキャストパケットを中継します。これらのコマンドおよびパラメータの設定と動作の関係を次の表に示します。また，これらのコマンドの設定例を次の図に示します。

表 1-5　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

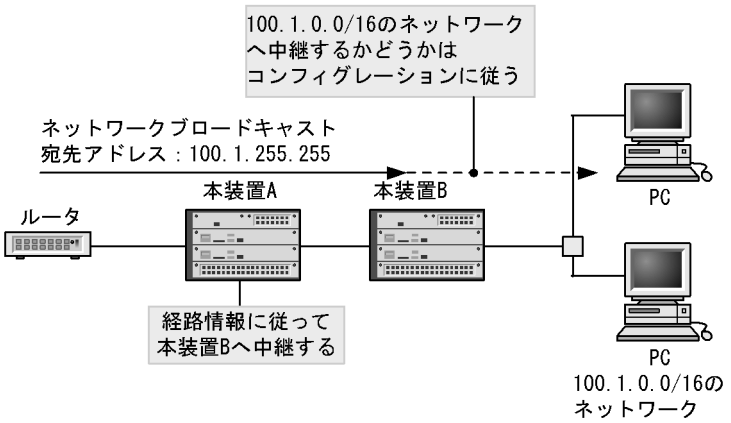
図 1-6 コマンド設定例



(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，100.1.0.0/16 のネットワークに対して，100.1.255.255 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 100.1.0.0/16 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中継スイッチの設定に従い，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 1-7 ネットワークブロードキャスト



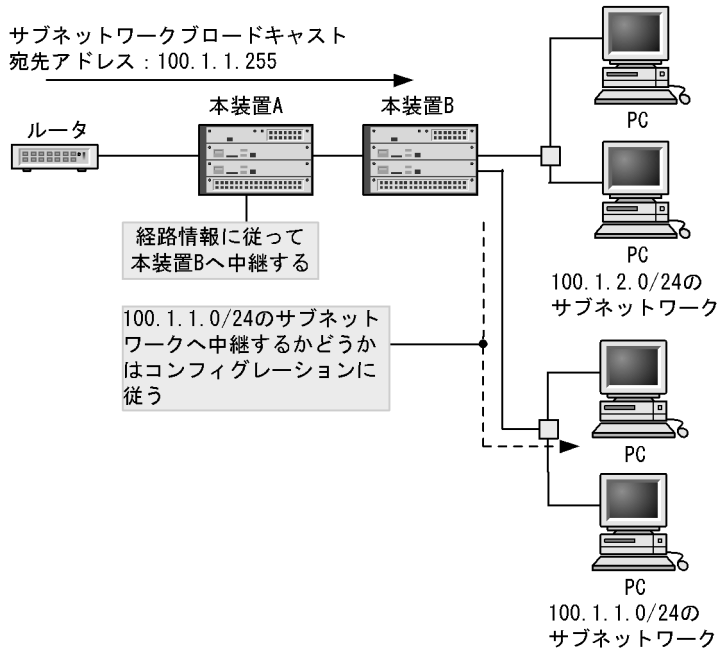
(2) サブネットワークブロードキャスト

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，100.1.0.0/16 のネットワークをサブネットワーク化して，100.1.1.0/24，100.1.2.0/24 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，100.1.1.255 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 100.1.1.0/24 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 100.1.1.0/24 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中継スイッチの設定に従い，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 1-8　サブネットワークブロードキャスト

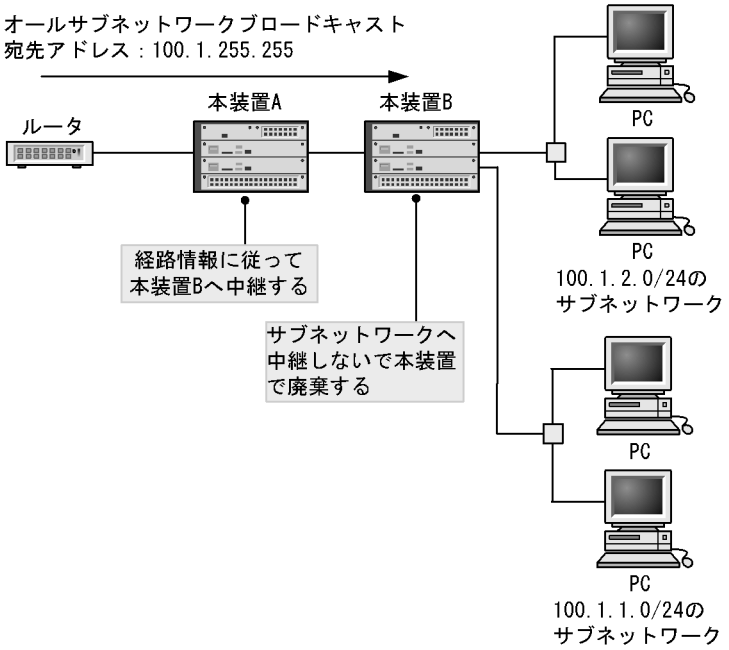


(3) オールサブネットワークブロードキャスト

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，100.1.0.0/16 のネットワークをサブネットワーク化して，100.1.1.0/24 と 100.1.2.0/24 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，100.1.255.255 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，100.1.1.0/24 と 100.1.2.0/24 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 100.1.1.0/24 と 100.1.2.0/24 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 1-9 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）に従い，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。

(1) VLAN インタフェースの MTU の決定

VLAN に所属するイーサネットインタフェースの MTU 値，システム MTU 情報，および IP MTU 情報のうち，最小のものを VLAN インタフェースの MTU 値とします。

VLAN インタフェースの MTU 値は，IPv4/IPv6 通信で使用されます。

VLAN インタフェースの MTU 決定マトリクスを次の表に示します。

表 1-6 VLAN インタフェース MTU 値決定マトリクス

設定パターン	1	2	3	4	5	6	7	8
システム MTU 情報	設定あり	設定あり	設定あり	設定あり	省略	省略	省略	省略
IP MTU 情報	設定あり	設定あり	省略	省略	設定あり	設定あり	省略	省略
ポート MTU 情報	設定あり	省略	設定あり	省略	設定あり	省略	設定あり	省略
MTU 値	A2	A1	A4	A1	A2	A3	A4	A5

（凡例）

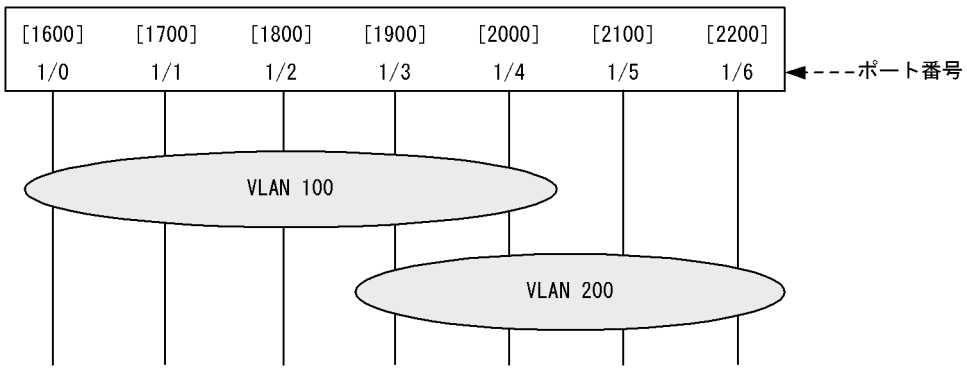
A1：システム MTU 情報の設定値と IP MTU 情報を比較し，小さい方

A2：IP MTU 情報の設定値とポート MTU 情報で指定したポート内の最小値を比較し，小さい方

A3：IP MTU 情報と 1500 を比較し，小さい方
A4：ポート MTU 情報で指定したポート内の最小値（ただし上限値は 9216 になります）
A5：1500

注　回線種別が 10BASE-T（全 / 半二重）または 100BASE-TX（半二重）の場合は，設定内容にかかわらず MTU 値は 1500 になります。

図 1-10　VLAN インタフェースの設定例



- IP 設定なしの場合

  [MTU 決定値]

  VLAN 100 の MTU 値・・・1600
  VLAN 200 の MTU 値・・・1900

- IP 設定ありの場合

  VLAN 100 に ip mtu 1000，VLAN 200 に ip mtu 3000 を設定したとき

  [MTU 決定値]

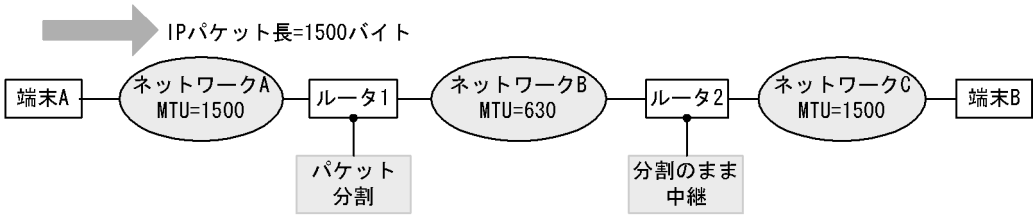
  VLAN 100 の MTU 値・・・1000
  VLAN 200 の MTU 値・・・1900

(2) 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 パケットを，小さな MTU を持つネットワークを通る場合，IP パケットを分割し中継します。

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 に短くなるためにフラグメント化します。

図 1-11　フラグメント化モデル



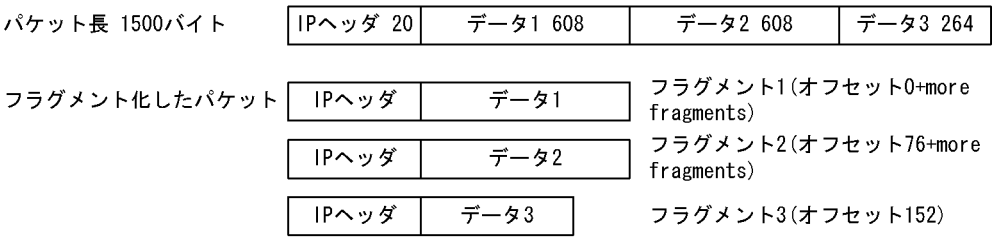
(3) フラグメントの生成

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 ですから，IP ヘッダ長を除くと 610 となり，610 での 8 の倍数長は 608

なので 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 ヘッダを付加します。パケットのフラグメント化を次の図に示します。

図 1-12 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 ヘッダ内のオフセットと more fragments ビットに書き込みます。また，同一の identification を設定して checksum を再計算します。オフセットは，先頭からのデータ長を 8 で割った値を設定します。

(4) 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 identification，オフセット，more fragments を基に再構成します。途中のルータは再構成を行いません。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 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，本装置を介した IPv4 中継が発生することがあります。

この際，ICMP Redirect の送信可否判定を行うため，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 max-send-count	ARP 要求フレームの最大送信回数を指定します。
arp send-interval	ARP 要求フレーム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 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。

2.1.2 インタフェースの設定

［設定のポイント］

VLAN 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 vlan 100**

   VLAN ID 100 のインタフェースコンフィグレーションモードに移行します。

2. **(config-if)# ip address 192.168.1.1 255.255.255.0**

   VLAN ID 100 に IPv4 アドレス 192.168.1.1，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］

VLAN に複数の IPv4 アドレスを設定します。二つ以降の 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 vlan 100**
   VLAN ID 100 のインタフェースコンフィグレーションモードに移行します。

2. **(config-if)# ip address 192.168.1.1 255.255.255.0**
   VLAN ID 100 にプライマリ IPv4 アドレス 192.168.1.1，サブネットマスク 255.255.255.0 を設定します。

3. **(config-if)# ip address 170.1.1.1 255.255.255.0 secondary**
   VLAN ID 100 にセカンダリ IPv4 アドレス 170.1.1.1，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 vlan 100**
   VLAN ID 100 のインタフェース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 170.10.10.1 255.255.255.0 directed-broadcast**
   VLAN ID 100 にプライマリ IP アドレス 170.10.10.1，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 loopback 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。設定可能な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インタフェースコンフィグレーションモードに移行します。

2. **(config-if)# ip address 192.168.1.1**
   ループバックインタフェースに IP アドレス 192.168.1.1 を設定します。

2.1.6 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 123.10.1.1 interface vlan 100 0012.e240.0a00**
   VLAN ID 100 にネクストホップ IPv4 アドレス 123.10.1.1，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。
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。
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。
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，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 「IPv4 インタフェース状態」の表示例

```
> show ip interface summary
vlan100 : UP 158.215.100.1/24
vlan200 : UP 123.10.1.1/24

>
```

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，通信相手となる装置に対して通信できるかどうかを，ping コマンドを実行して確認してください。

図 2-2 ping コマンドの実行結果（通信可の場合）

```
> ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1): 56 data bytes
64 bytes from 192.168.1.51: icmp_seq=0 ttl=255 time=0.286 ms
64 bytes from 192.168.1.51: icmp_seq=1 ttl=255 time=0.271 ms
64 bytes from 192.168.1.51: icmp_seq=2 ttl=255 time=0.266 ms
^C
--- 192.168.0.1 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 192.168.0.1
PING 192.168.0.1 (192.168.0.1): 56 data bytes
^C
--- 192.168.0.1 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 192.168.0.1 numeric
traceroute to 192.168.0.1 (192.168.0.1), 30 hops max, 40 byte packets
1  192.168.2.101  0.612 ms  0.541 ms  0.532 ms
2  192.168.1.51  0.905 ms  0.816 ms  0.807 ms
3  192.168.0.1  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，本装置と隣接装置間のアドレス解決をしているか（ARP エントリ情報があるか）どうか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 vlan 100
Date 2006/03/25 14:00 UTC
Total: 3 entries
 IP Address    Linklayer Address  Netif      Expire    Type
 192.168.2.101 0012.e240.0a00     VLAN0100   Static    arpa
 192.168.1.51  0012.e240.0a01     VLAN0100   Static    arpa
 192.168.0.1   0012.e240.0a02     VLAN0100   3h30m0s   arpa
```

3 Null インタフェース（IPv4）

この章では，IPv4 ネットワークの 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。

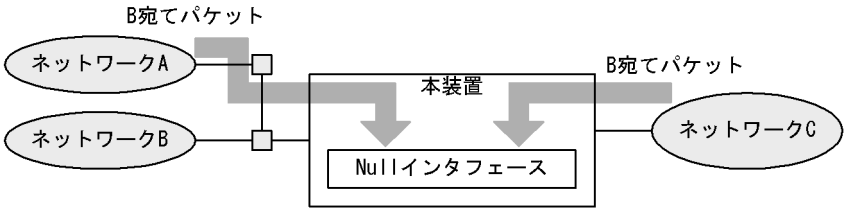
3.1 解説

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行いません。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の廃棄は行いません。

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 3-1 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廃棄を行う場合，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の詳細は「8　スタティックルーティング（IPv4）」～「12　BGP4【OP-BGP】」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廃棄を行え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 3-1 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）
	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

3.2 コンフィグレーション

3.2.1 コンフィグレーションコマンド一覧

Null インタフェース（IPv4）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 3-2 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 ※	IPv4 スタティック経路を生成します。

注※

「コンフィグレーションコマンドレファレンス Vol.3　10. スタティックルーティング（IPv4）」を参照してください。

3.2.2 Null インタフェースの設定

［設定のポイント］

Null インタフェースを設定し，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 10.0.0.0 255.0.0.0 null 0**

   スタティック経路 10.0.0.0/8 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際，パケットは中継されずにすべて Null インタフェースに送信され，廃棄されます。

3.3 オペレーション

3.3.1 運用コマンド一覧

Null インタフェース（IPv4）の運用コマンド一覧を次の表に示します。

表 3-3 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を表示します。
clear counters null-interface ※1	Null インタフェースの IPv4 および IPv6 統計情報をクリアします。
show ip interface ※1	IPv4 インタフェースの状態を表示します。
clear counters ipv4 null-interface ※1	Null インタフェースの IPv4 統計情報をクリアします。
show ip route ※2	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　6. IPv4 ルーティングプロトコル」を参照してください。

3.3.2 Null インタフェースの確認

本装置で Null インタフェースの機能を使用した場合の確認内容には次のものがあります。

(1) コンフィグレーション設定後の確認

(a) 経路情報の確認

show ip route コマンドを実行し，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かどうかを確認してください。

図 3-2 Null インタフェース経路情報表示

```
> show ip route static
Total: 1 routes
Destination        Next Hop        Interface     Metric  Protocol  Age
172.16.251.89/32   ----            null0         0/0     Static     1m  9s
>
```

(2) 運用中の確認

(a) パケット廃棄数の確認

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

図 3-3 Null インタフェースパケット廃棄数表示例

```
> show ip interface delete-packets null-interface
Interface Name:null0
Discard Packets(IPv4) :92(pkts)
>
```

4 ポリシーベースルーティング（IPv4）

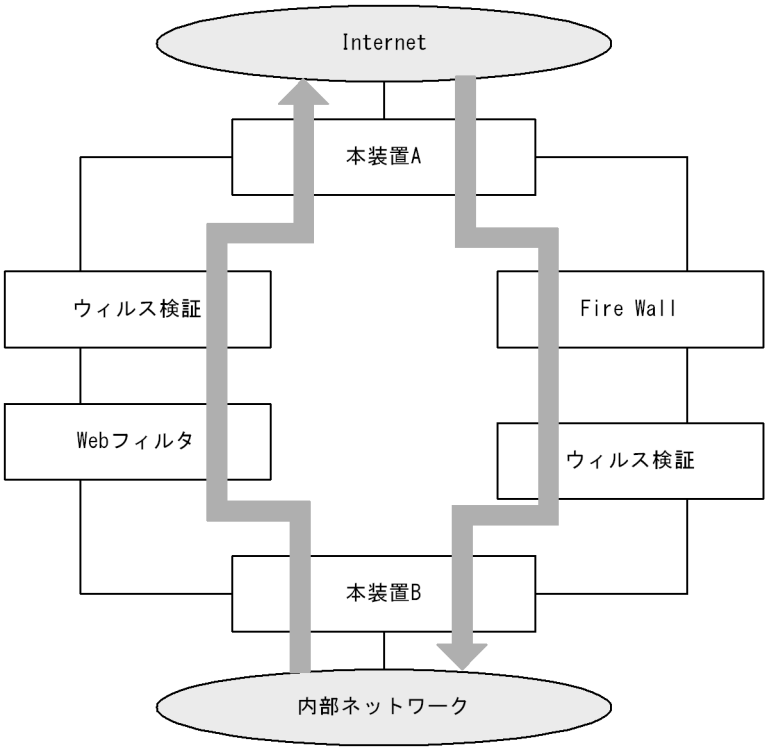
この章では，ポリシーベースルーティング（IPv4）の解説と操作方法について説明します。

4.1 解説

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や，コンフィグレーションコマンドで登録された経路情報に従わないで，ユーザが設定した宛先装置にパケットをレイヤ 3 中継する機能です。

ポリシーベースルーティングの構成例を次の図に示します。

図 4-1 ポリシーベースルーティングの構成例



本装置 A は，Internet から受信したすべてのパケットを Fire Wall およびウィルス検証などのセキュリティ装置に中継します。本装置 B は，内部ネットワークから受信したすべてのパケットを Web フィルタおよびウィルス検証などのフィルタ／セキュリティ装置に中継します。送受信するパケットで異なるセキュリティチェックを実施できます。また，負荷分散や認証などにも適用できます。

このようにポリシーベースルーティングは，経路情報に関係なく，ユーザが指定した経路に従って中継できます。

4.1.1 ポリシーベースルーティングの制御

ポリシーベースルーティングはフィルタの一部機能として動作します。

受信側の VLAN インタフェースに設定したフィルタのフロー検出条件に一致した場合，同フィルタエントリに設定されているポリシーベースルーティングの設定内容に従って，パケットを中継します。

なお，ポリシーベースルーティングの対象となるのはレイヤ 3 中継のパケットだけです。

ポリシーベースルーティングの設定方法には次の二つがあります。

（1） アクセスリストの動作に中継先の経路を指定

アクセスリストの動作に，中継先の経路として送信先インタフェースの VLAN ID およびネクストホップ

アドレスを指定します。

送信先インタフェースが障害などで中継できない場合の動作を**デフォルト動作**といいます。アクセスリストの動作に中継先の経路を指定した場合，デフォルト動作は廃棄です。

なお，送信先インタフェースが障害などから復旧して中継可能になった場合は，該当する中継先の経路から中継を再開します。

(2) アクセスリストの動作にポリシーベースルーティングリスト情報を指定

アクセスリストの動作に，経路情報を登録した**ポリシーベースルーティングリスト情報**を指定します。この指定による機能を**ポリシーベースルーティンググループ**といいます。

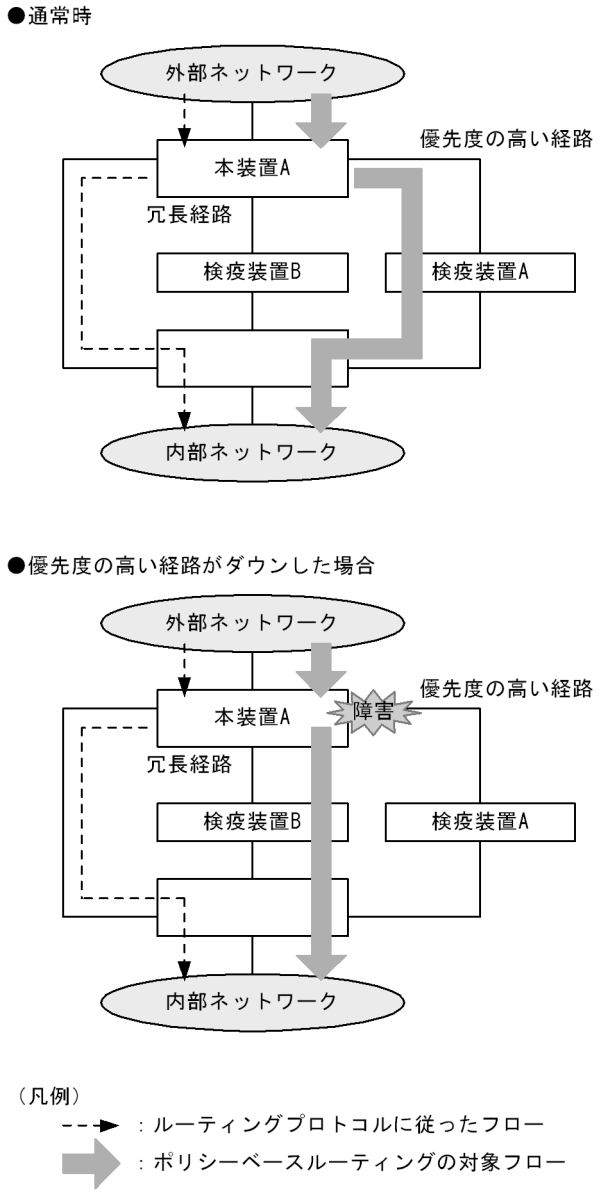
4.1.2 ポリシーベースルーティンググループ

ポリシーベースルーティンググループでは，一つまたは複数の経路をグループ化して設定できます。各経路は設定された適用順序に従って優先度を持ちます。これによって，送信先インタフェースや中継先の経路の状況に合わせて，複数の経路の中から優先度の高い経路を動的に選択します。なお，一つまたは複数の経路をグループ化した情報を**ポリシーベースルーティングリスト情報**といいます。

ポリシーベースルーティングリスト情報に複数の経路を指定することで，経路の冗長化ができます。障害などで優先度の高い経路が中継できなくなった場合，同じポリシーベースルーティングリスト情報に設定している次に優先度の高い経路に切り替えて運用を継続します。

ポリシーベースルーティンググループの構成例を次の図に示します。

図 4-2　ポリシーベースルーティンググループの構成例

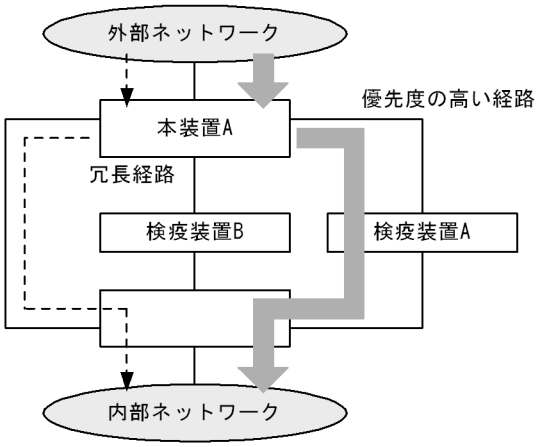


また，ポリシーベースルーティンググループはトラッキング機能のポーリング監視と連携することで，ポーリング監視の対象地点までの経路を監視できます。トラッキング機能のポーリング監視は，ネットワーク上の装置への通信可否を監視します。監視した結果はポリシーベースルーティンググループの経路選択時の判断に使われます。これによって，本装置と隣接装置間で発生した障害だけでなく，それ以外の経路で発生した障害に基づいて，経路の切り替えができます。

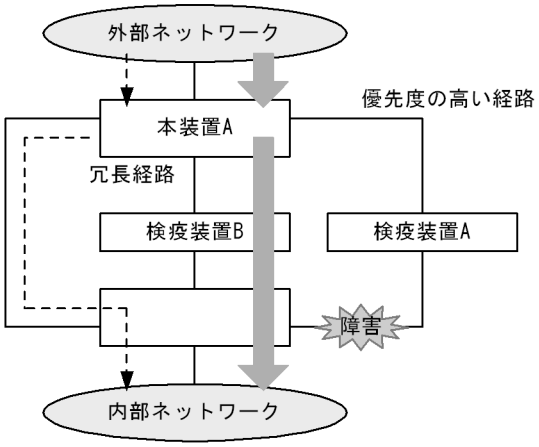
ポリシーベースルーティンググループとトラッキング機能の連携構成例を次の図に示します。

図 4-3 ポリシーベースルーティンググループとトラッキング機能の連携構成例

●通常時



●優先度の高い経路の到達性が保障されなくなった場合



（凡例）
- ：ルーティングプロトコルに従ったフロー
- ：ポリシーベースルーティングの対象フロー

（1） ポリシーベースルーティンググループの経路選択

ポリシーベースルーティンググループでは，ポリシーベースルーティングリスト情報に登録した複数の経路から次の情報を基に経路を選択します。

- 中継可否の監視結果と優先度
- デフォルト動作指定
- 経路切り戻し動作指定

（a） 中継可否の監視結果と優先度

ポリシーベースルーティングリスト情報に登録した経路は，次に示す監視の結果によって中継可否が決定します。

- 送信先インタフェースの VLAN 状態の監視
- トラッキング機能によるポーリング監視

また，中継可能な経路のうち，最も優先度の高い経路を選択します。

● 送信先インタフェースの VLAN 状態の監視

次に示すコンフィグレーションコマンドで中継先の経路を指定したとき，送信先インタフェースの VLAN 状態によって中継可否を判断します。

- policy-interface コマンド
  送信先インタフェースの VLAN ID（vlan パラメータ）およびネクストホップアドレス（next-hop パラメータ）

送信先インタフェースの VLAN が Up のときだけ，中継可能と判断します。

● トラッキング機能によるポーリング監視

次に示すコンフィグレーションコマンドで中継先の経路を指定したとき，送信先インタフェースの VLAN 状態に加えて，トラッキング機能のポーリング監視結果によって中継可否を判断します。

- policy-interface コマンド
  送信先インタフェースの VLAN ID（vlan パラメータ），ネクストホップアドレス（next-hop パラメータ）およびトラック ID（track-object パラメータ）

送信先インタフェースの VLAN およびトラッキング機能のポーリング監視結果が Up のときだけ，中継可能と判断します。

なお，トラッキング機能については，「4.1.5　ポリシーベースルーティングのトラッキング機能」を参照してください。

● 優先度による決定

送信先インタフェースの VLAN 状態の監視またはトラッキング機能によるポーリング監視の結果を基に，ポリシーベースルーティングリスト情報内で中継可能な経路のうち，コンフィグレーションで指定した適用順序で，最も優先度の高い経路を選択します。

(b) デフォルト動作指定

ポリシーベースルーティングリスト情報に登録している経路がすべて中継できない，または経路が登録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コマンド default 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 4-1　デフォルト動作指定

コンフィグレーションでの指定	デフォルト動作	動作説明
permit 指定	通常中継	対象のパケットをルーティングプロトコルに従ってレイヤ 3 中継します
deny 指定	廃棄	対象のパケットを廃棄します
未指定	廃棄	対象のパケットを廃棄します

デフォルト動作によってルーティングプロトコルに従ってパケットをレイヤ 3 中継または廃棄した場合，対象のポリシーベースルーティングリスト情報を指定しているアクセスリストの統計情報にカウントされます。

(c) 経路切り戻し動作指定

ポリシーベースルーティングリスト情報に登録している優先度の高い経路が中継できなくなって優先度の低い経路で中継している状態で，優先度の高い経路が中継可能になった場合の動作を**経路切り戻し動作**と

いいます。経路切り戻し動作はコンフィグレーションコマンド recover で指定できます。経路切り戻し動作指定について次の表に示します。

表 4-2 経路切り戻し動作指定

コンフィグレーションでの指定	経路切り戻し動作	動作説明
on 指定	切り戻す	優先度の高い経路が中継可能になると，経路を切り戻します
off 指定	切り戻さない	優先度の高い経路が中継可能になっても，経路を切り戻しません
未指定	切り戻す	優先度の高い経路が中継可能になると，経路を切り戻します

経路切り戻し動作として「切り戻す」を指定すると，ポリシーベースルーティングリスト情報内で中継可能な経路のうち，常に最も優先度の高い経路を選択します。

経路切り戻し動作として「切り戻さない」を指定すると，選択中の経路より優先度の高い経路が中継可能になっても切り戻しません。選択中の経路が中継できなくなると，常により優先度の低い経路へ切り替えます。ポリシーベースルーティングリスト情報に登録しているすべての経路が中継できない場合，経路を切り戻さないでデフォルト動作になります。ただし，次の場合にはポリシーベースルーティングリスト情報内で中継可能な経路のうち，最も優先度の高い経路を再選択します。

- 運用コマンド reset policy-list の実行
- コンフィグレーションコマンド recover で経路切り戻し動作を「切り戻す」に変更
- ポリシーベースプログラムの再起動
- 系切替後，中継可否の監視を一時的に停止する時間が経過

(2) 起動時のポリシーベースルーティンググループ

本装置では起動時や再起動時など，ポリシーベースプログラムが動作してから一定時間，中継可否の監視および経路の切り替えを停止します。これは，次に示す理由で起動したあとの装置状態を収集し終わるまで，中継可否の監視結果が安定しないためです。

- VLAN インタフェースが Up していない
- トラッキング機能によるポーリング監視結果が Up ではない

ポリシーベースプログラムが動作してからポリシーベースルーティンググループが中継可否の監視を始めるまでの経路の状態を起動中といいます。起動中はポリシーベースルーティングの対象パケットをすべて廃棄します。

なお，起動中に次のコンフィグレーションコマンドでポリシーベースルーティングリスト情報を変更した場合，中継可否の監視を始めた時点で変更が反映されます。

- default（policy-list）
- policy-interface（policy-list）
- policy-list
- recover（policy-list）

ポリシーベースプログラムが動作してから中継可否の監視を始めるまでの時間（中継可否の監視を停止する時間）は，コンフィグレーションコマンド policy-list default-init-interval で変更できます。起動したあとの，中継可否の監視結果が安定するまでに掛かる時間を目安として指定してください。起動中の状態遷移と遷移条件について次の表に示します。

表 4-3 起動中の状態遷移と遷移条件

状態遷移	遷移条件
起動中の終了	中継可否の監視を停止する時間が経過すると起動中を終了します。 また，起動中を中断した場合も同様に起動中を終了します。
起動中を中断	次の場合に起動中を中断します。 • 運用コマンド reset policy-list の実行 • コンフィグレーションで，中継可否の監視を停止する時間を現在の経過時間よりも短く変更 • ポリシーベースプログラムの再起動 • 系切替
起動中の延長	コンフィグレーションで，中継可否の監視を停止する時間をより長く変更すると起動中を延長します。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，中継可否の監視を開始します。

起動中に系切替すると，切替中を終了または中断するまでの間，ポリシーベースルーティングリスト情報の対象パケットはすべて廃棄されます。

起動中を終了または中断すると，ポリシーベースルーティングリスト情報内で中継可能な経路のうち，最も優先度の高い経路を選択します。

（3）系切替時のポリシーベースルーティンググループ

本装置の BCU，CSU または MSU を冗長化している場合，系切替が発生してから一定時間，中継可否の監視および経路の切り替えを停止します。これは，系切替したあとの装置状態を収集し終わるまで，中継可否の監視結果が安定しないためです。

系切替してからポリシーベースルーティンググループが中継可否の監視を始めるまでの経路の状態を切替中といいます。切替中は経路を切り替えないで，系切替前に選択していた経路を引き継ぎます。

なお，切替中に次のコンフィグレーションコマンドでポリシーベースルーティングリスト情報を変更した場合，中継可否の監視を始めた時点で変更が反映されます。

- default（policy-list）
- policy-interface（policy-list）
- policy-list
- recover（policy-list）

ただし，ポリシーベースルーティングリスト情報を設定しているアクセスリストのコンフィグレーションを変更した場合は，ポリシーベースルーティングリスト情報の対象パケットはすべて廃棄されます。

系切替してから中継可否の監視を始めるまでの時間（中継可否の監視を停止する時間）は，コンフィグレーションコマンド policy-list default-aging-interval で変更できます。系切替したあとの，パケットの送受信が安定するまでに掛かる時間を目安として指定してください。切替中の状態遷移と遷移条件について次の表に示します。

表 4-4 切替中の状態遷移と遷移条件

状態遷移	遷移条件
切替中の終了	中継可否の監視を停止する時間が経過すると切替中を終了します。 また，切替中を中断した場合も同様に切替中を終了します。

状態遷移	遷移条件
切替中を中断	次の場合に切替中を中断します。 • 運用コマンド reset policy-list の実行 • コンフィグレーションで，中継可否の監視を停止する時間を現在の経過時間よりも短く変更 • ポリシーベースプログラムの再起動 • 次に示すコンフィグレーションコマンドを実行して，BSU または PSP が再起動 ・fldm prefer ・fwdm prefer ・vrf mode【OP-NPAR】 • 運用コマンド restart vlan の実行 • 運用コマンド activate bsu を実行して，装置内で 1 枚目の BSU を active 状態に変更
切替中の延長	コンフィグレーションで，中継可否の監視を停止する時間をより長く変更すると切替中を延長します。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，中継可否の監視を開始します。 また，BCU，CSU または MSU の系切替が再度発生すると，中継可否の監視を停止する時間をカウントし直すため，切替中を継続します。

切替中を終了または中断すると，ポリシーベースルーティングリスト情報内で中継可能な経路のうち，最も優先度の高い経路を選択して経路を切り替えます。

なお，系切替については，「コンフィグレーションガイド Vol.2　17. BCU/CSU/MSU の冗長化」を参照してください。

4.1.3 ポリシーベースルーティング対象パケット

ポリシーベースルーティングの対象となるパケットについて次の表に示します。

表 4-5　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	アドレス種別	対象可否
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※1	×
	サブネットブロードキャスト	×
	自宛 IP パケット	×※2
	自発 IP パケット	×
IPv4 パケット以外		×

（凡例）○：対象　　×：対象外

注※ 1

IP ブロードキャストアドレスで，255.255.255.255 または 0.0.0.0 の形式を持つ IP アドレスを示します。

注※ 2

ポリシーベースルーティングがデフォルト動作に従っていて，かつデフォルト動作が廃棄のときは廃棄します。その場合，該当するアクセスリストの統計情報にカウントされます。

4.1.4 ネクストホップに設定可能なアドレス種別

ポリシーベースルーティングのネクストホップに設定できる IP アドレス種別を次の表に示します。

表 4-6 ポリシーベースルーティングのネクストホップに設定できる IP アドレス種別

アドレス種別	設定可否
ユニキャスト（受信インタフェース含む）	○※
送信先インタフェースに設定された IP アドレス	×
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	×
内部ループバック（127.0.0.0）	×

（凡例）○：設定できる　　×：設定できない
注※　送信先インタフェースに設定したアドレスと同一ネットワークのアドレスだけが設定できます。

4.1.5 ポリシーベースルーティングのトラッキング機能

ポリシーベースルーティングのトラッキング機能では，ネットワーク上の装置をトラック対象としてポーリングパケットを送信して，通信可能な場合にトラック状態を Up にします。

本装置では，トラック対象の装置へ一定間隔でポーリングパケットを送信して，その応答パケットが戻ってくるかどうかを監視します。応答パケットを受信するとポーリング成功と見なします。ポーリング成功が一定回数続くと，トラック状態を Up にします。応答パケットを受信しないとポーリング失敗と見なします。ポーリング失敗が一定回数続くと，トラック状態を Down にします。

(1) IPv4 ICMP ポーリング監視

IPv4 ICMP **ポーリング監視**では，トラック対象としてネットワーク上の装置を IPv4 アドレスで指定します。ポーリングパケットとして，IPv4 ICMP Echo パケットをトラック対象の IPv4 アドレスへ送信します。ポーリングの応答パケットとして IPv4 ICMP Echo Reply パケットが戻ってくるかどうかを監視します。

(2) ポーリング結果と検証シーケンス

ポーリング監視では，ポーリングパケットを定期的に送信します。送信後，応答待ち時間だけ応答パケットを待ちます。時間内に応答パケットを受信するとポーリングは成功です。パケットを受信しないで応答待ち時間を経過した場合，ポーリングは失敗です。

しかし，ネットワークでは，通信できる状況でも一時的にパケットが廃棄されることがあります。また，通信できない状況でも一時的に通信できることがあります。このようなネットワークにポーリング監視を適用してポーリング結果を直接トラック状態に反映すると，トラック状態が不安定になるおそれがあります。

そのため，本装置のポーリング監視では，ポーリング結果をトラック状態に反映するまでの検証期間があります。検証期間中はそれまでのトラック状態を継続したまま，ポーリング結果によってトラック状態を変更してよいかを検証します。検証期間があることで，通信が安定しない状況でのトラック状態の不用意な切り替えを抑止できます。なお，検証期間はポーリング回数やポーリング間隔を指定して調整できます。また，トラック状態を変更するのに必要なポーリング回数やポーリング間隔は，トラックごとに指定できます。

ポーリング監視トラックに設定できる項目を次の表に示します。各項目はコンフィグレーションコマンドのパラメータで指定します。

表 4-7 ポーリング監視トラックに設定できる項目

項目	説明	デフォルト値
応答待ち時間	ポーリングパケットを送信してから応答パケットを受信するまでの待ち時間	2 秒
ポーリング間隔	検証中以外で動作中のポーリングパケット送信間隔	6 秒
トラック状態を Up と判定するポーリング成功回数	障害回復検証中にトラック状態を Up と判定するために必要なポーリング成功回数	4 回
障害回復検証中のポーリング試行回数	障害回復検証を続けるポーリングの最大回数	5 回
障害回復検証中のポーリング試行間隔	障害回復検証中のポーリングパケット送信間隔	2 秒
トラック状態を Down と判定するポーリング失敗回数	障害発生検証中にトラック状態を Down と判定するために必要なポーリング失敗回数	4 回
障害発生検証中のポーリング試行回数	障害発生検証を続けるポーリングの最大回数	5 回
障害発生検証中のポーリング試行間隔	障害発生検証中のポーリングパケット送信間隔	2 秒

トラックにはトラック状態のほかに，トラック動作状態というトラックの動作状況を示す状態があります。検証期間中のトラック動作状態を検証中，それ以外の状態（装置起動からトラック監視の開始まで，および系切替からトラック監視の開始までの状態を除く）を動作中と呼びます。

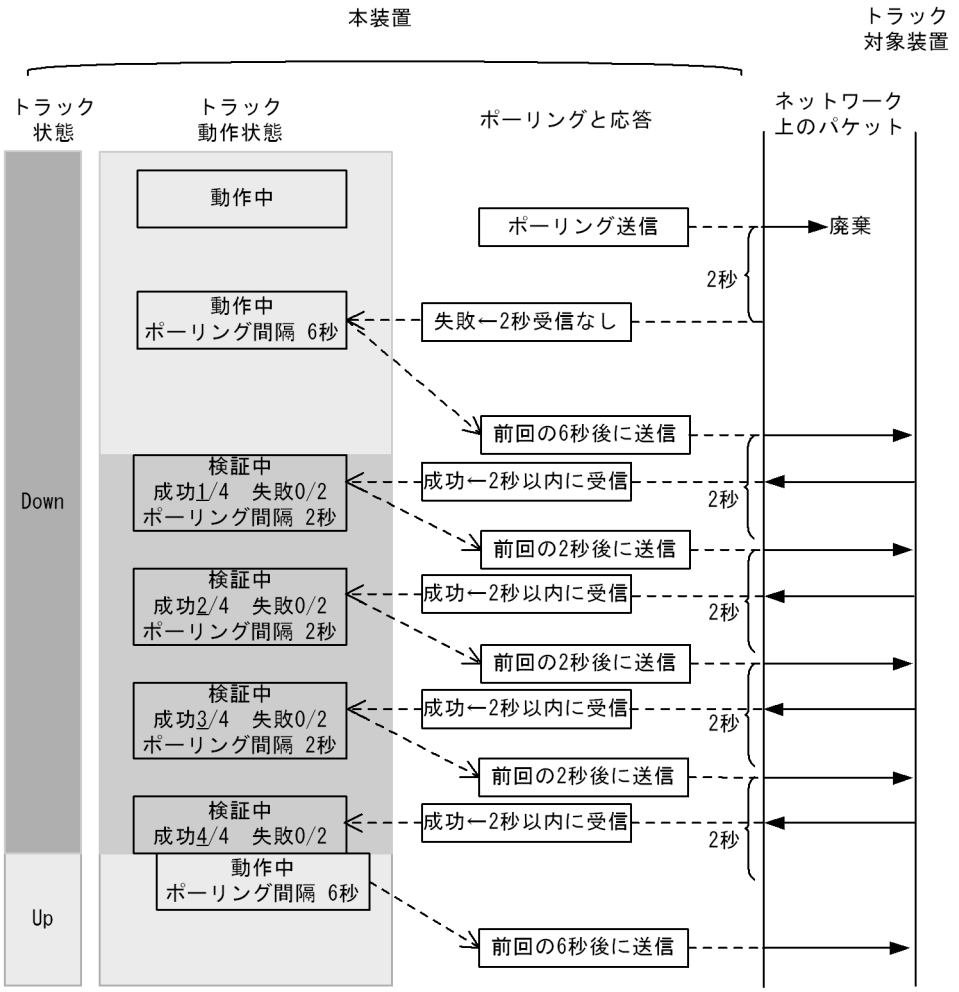
(a) 障害回復検証時

トラック状態が Down のとき，ポーリングの応答結果（失敗）に変化がない状態を継続している間，トラック動作状態は動作中という状態です。動作中は，ポーリング間隔に指定した送信間隔でポーリングパケットが送信されます。

トラック状態が Down のときにポーリングに成功すると，トラック状態を Up へ変更するかどうかの検証を開始します。この検証を**障害回復検証**といいます。

障害回復検証シーケンスを次の図に示します。この図および説明では，各項目の値をすべてデフォルト値を使って説明しています。

図 4-4　障害回復検証シーケンス（検証の結果 Up と判定する例）



まず，トラック状態を Down のままトラック動作状態を検証中にして，障害回復検証を開始します。障害回復検証中のポーリングパケット送信間隔は，障害回復検証中のポーリング試行間隔に指定した時間（2秒）です。

障害回復検証中に，トラック状態を Up と判定するポーリング成功回数（4 回）だけポーリングに成功すると，トラック状態を Up，トラック動作状態を動作中にして，障害回復検証を終了します。なお，ポーリング成功回数には，障害回復検証を開始するきっかけとなったポーリングの成功を含めます。

障害回復検証中に，障害回復検証中のポーリング試行回数（5 回）からトラック状態を Up と判定するポーリング成功回数（4 回）を引いて 1 を足した回数（5 － 4 ＋ 1 ＝ 2 回）だけポーリングに失敗すると，トラック状態を Down のままトラック動作状態を動作中にして，障害回復検証を終了します。

このように，トラック状態の変化に関係なく，障害回復検証中のポーリング試行回数に指定した回数（5回）以内のポーリングで障害回復検証が終了します。

(b) 障害発生検証時

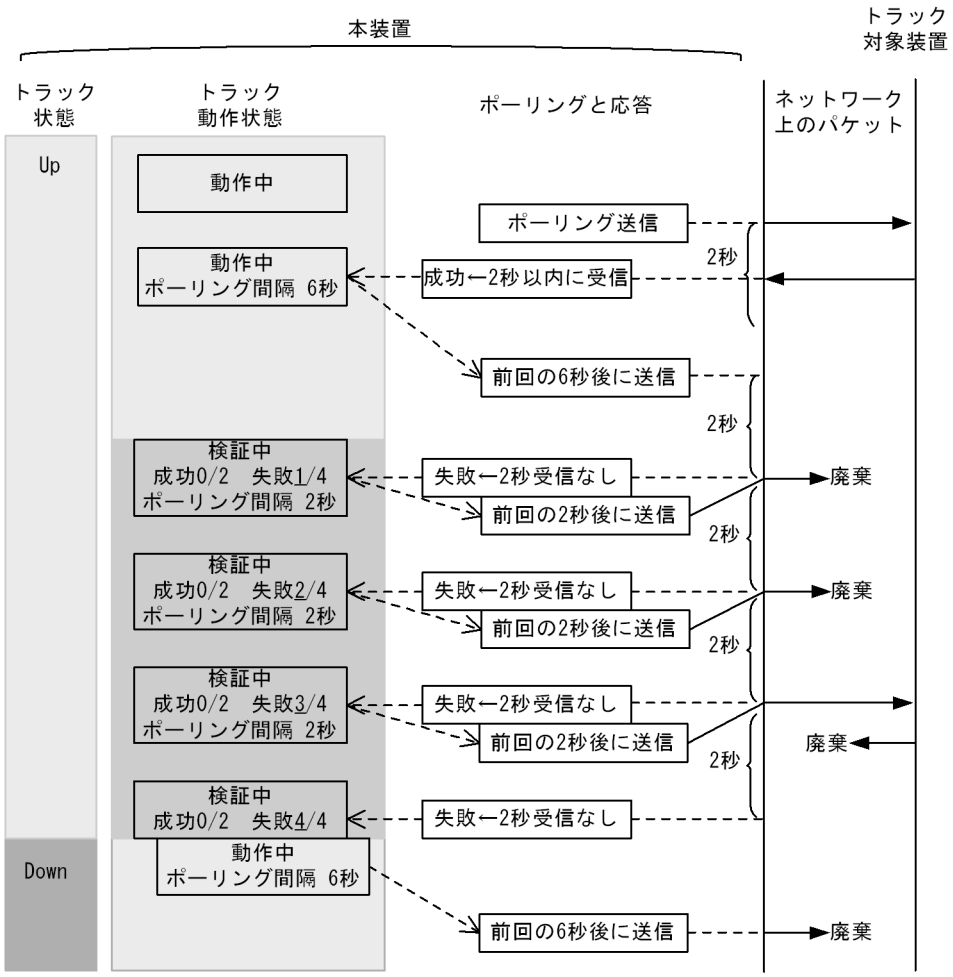
トラック状態が Up のとき，ポーリングの応答結果（成功）に変化がない状態を継続している間，トラック動作状態は動作中という状態です。動作中は，ポーリング間隔に指定した送信間隔でポーリングパケットが送信されます。

トラック状態が Up のときにポーリングに失敗すると，トラック状態を Down へ変更するかどうかの検証

を開始します。この検証を**障害発生検証**といいます。

障害発生検証シーケンスを次の図に示します。この図および説明では，各項目の値をすべてデフォルト値を使って説明しています。

図 4-5　障害発生検証シーケンス（検証の結果 Down と判定する例）



まず，トラック状態を Up のままトラック動作状態を検証中にして，障害発生検証を開始します。障害発生検証中のポーリングパケット送信間隔は，障害発生検証中のポーリング試行間隔に指定した時間（2 秒）です。

障害発生検証中に，トラック状態を Down と判定するポーリング失敗回数（4 回）だけポーリングに失敗すると，トラック状態を Down，トラック動作状態を動作中にして，障害発生検証を終了します。なお，ポーリング失敗回数には，障害発生検証を開始するきっかけとなったポーリングの失敗を含めます。

障害発生検証中に，障害発生検証中のポーリング試行回数（5 回）からトラック状態を Down と判定するポーリング失敗回数（4 回）を引いて 1 を足した回数（5 － 4 ＋ 1 ＝ 2 回）だけポーリングに成功すると，トラック状態を Up のままトラック動作状態を動作中にして，障害発生検証を終了します。

このように，トラック状態の変化に関係なく，障害発生検証中のポーリング試行回数に指定した回数（5 回）以内のポーリングで障害発生検証が終了します。

(3) ポーリング監視の注意事項

- ポリシーベースルーティンググループと連携してトラックを使用する場合は，トラック状態を Down と

判定するポーリング失敗回数を 1 回にしないことを推奨します。これは，ポーリング失敗回数を 1 回にしたトラックと連携させると，ネットワークの状況によっては制御が不安定になるおそれがあるためです。
運用ログやトラップを使用して 1 回のポーリング失敗でもネットワーク管理者に伝えたいという場合にだけ，トラック状態を Down と判定するポーリング失敗回数に 1 回を指定してください。

- ポーリング間隔，障害回復検証中のポーリング試行間隔，および障害発生検証中のポーリング試行間隔には，応答待ち時間よりも長い時間を指定してください。これは，成功と失敗のどちらでも前回のポーリング結果が決まるまで，次のポーリングパケットを送信しないためです。
  ポーリング間隔に応答待ち時間よりも短い時間を指定しても，成功の場合は応答パケットを受信するまで，失敗の場合は応答待ち時間が経過するまで，次のポーリングパケットを送信しません。
- すべてのポーリング監視トラックのポーリングパケットの送信頻度の合計は，最大で 100pps です。トラック動作状態が検証中はポーリング間隔が変わることを考慮したうえで，100pps に収まるように構成して使用してください。
  1 秒当たり 100 パケットを超えるパケットは，次の 1 秒まで送信が持ち越されます。100pps を超える構成では，100pps に収まるようにすべてのトラックのポーリング間隔が広がります。

4.1.6 トラッキング機能のトラック

ポリシーベースルーティングのトラッキング機能では，コンフィグレーションでトラックの動作を停止したり，停止中のトラックのトラック状態を指定したりできます。これによって，トラックのコンフィグレーションを追加または変更する間，連携するポリシーベースルーティンググループの経路選択に影響が少ないようにトラック状態を固定したり，経路選択に影響が少ないタイミングでトラックの動作を開始したりできます。

（1）デフォルトトラック状態

デフォルトトラック状態とは，系切替時を除いて，トラックが停止しているときに適用されるトラック状態です。コンフィグレーションコマンド default-state で，トラックごとに指定できます。コンフィグレーションコマンドで指定していないトラックのデフォルトトラック状態は Down です。

停止中のトラックやコンフィグレーションが完了していないトラックでも，デフォルトトラック状態のコンフィグレーションは有効です。このため，トラックのコンフィグレーションを変更する前にデフォルトトラック状態を指定すると，設定済みの連携するポリシーベースルーティンググループの経路選択に影響を与えないでトラックのコンフィグレーションを変更できます。

（2）コンフィグレーションによるトラックの停止

コンフィグレーションコマンド disable を指定すると，トラックごとに動作を停止できます。停止中のトラックのトラック状態は，デフォルトトラック状態です。

（3）コンフィグレーションが完了していないトラック

コンフィグレーションが完了していないトラックとは，トラック種別を指定していないトラックです。コンフィグレーションコマンド track-object や，コンフィグレーションコマンド type icmp を設定していないトラックが該当します。

コンフィグレーションが完了していないトラックでも，ポリシーベースルーティンググループと連携できます。コンフィグレーションが完了していないトラックをポリシーベースルーティンググループと連携させた場合，該当するトラックのデフォルトトラック状態をトラッキング機能のポーリング監視結果として，経路の中継可否を決定します。

（4） 装置起動時のトラックの動作

ポーリング監視トラックは，本装置の起動時や再起動時に一定時間動作を停止します。これは，次に示す理由などで装置の起動直後はポーリングによる監視ができないためです。

- インタフェースが Up していない
- 経路が安定していない

本装置が起動および再起動してからポーリング監視トラックが動作を始めるまでのトラック動作状態を起動中といいます。起動中のトラック状態はデフォルトトラック状態です。

本装置の起動および再起動後，ポーリング監視トラックが動作を始めるまでの時間は，装置単位にコンフィグレーションコマンド track-object default-init-interval で変更できます。本装置が起動または再起動したあとの，ポーリング監視トラックが使用する通信が安定するまでに掛かる時間を指定してください。デフォルトは 180 秒です。

（5） 系切替時のトラックの動作

本装置の BCU，CSU または MSU を冗長化している場合，ポーリング監視トラックは系切替時に一定時間動作を停止します。これは，系切替したあと現在の装置の状態や経路情報を収集し終わるまで，系切替時の通信無停止を利用していてもポーリングによる監視が安定しないためです。

本装置が系切替してからポーリング監視トラックが動作を始めるまでのトラック動作状態を切替中といいます。切替中のトラック状態は，系切替前のトラック状態を引き継ぎます。このため，連携するポリシーベースルーティンググループでは，系切替前と同じトラック状態を基にして経路を制御できるため，系切替時に通信無停止ができます。

本装置が系切替したあとポーリング監視トラックが動作を始めるまでの時間は，装置単位にコンフィグレーションコマンド track-object default-aging-interval で変更できます。系切替したあとパケットの送受信が安定するまでに掛かる時間を指定してください。デフォルトは 180 秒です。

なお，系切替については「コンフィグレーションガイド Vol.2　17. BCU/CSU/MSU の冗長化」を参照してください。また，系切替時の通信無停止機能については「コンフィグレーションガイド Vol.2　17.1.5 系切替時の通信無停止対応機能一覧」を参照してください。

（6） 系切替時の通信無停止についての注意事項

本装置で系切替が発生すると，次に示す理由で他装置が本装置を監視するポーリングで失敗することがあります。その結果，本装置が障害と判断されて，ネットワーク全体として本装置の系切替による通信無停止が実現できないおそれがあります。

本装置では，通信無停止機能を使用することで，系切替しても本装置を経由する通信を維持します。しかし，本装置が起点または終点となる通信は，系切替すると一時的に停止します。

本装置のポーリング監視トラックは，系切替前のトラック状態を引き継ぐことで状態を維持します。しかし，本装置が系切替すると，一時的に本装置が他装置からのポーリングに応答しません。

4.1.7 ポリシーベースルーティングの注意事項

（1） ポリシーベースルーティングと uRPF 機能の併用について

ポリシーベースルーティングと uRPF 機能が同時に設定された場合，uRPF 機能が優先的に動作します。このため，ポリシーベースルーティング機能は動作しない状態になりますが，対象パケットがフィルタ条件で検出されるため，統計情報はカウントされます。

（2） ポリシーベースルーティングと DHCP snooping の併用について

「コンフィグレーションガイド Vol.2　15.1.7 DHCP snooping 使用時の注意事項」を参照してください。

（3） ポリシーベースルーティングと sFlow 統計機能の併用について

sFlow 統計の対象パケットをポリシーベースルーティングの対象とした場合，sFlow 統計で採取する次の情報はポリシーベースルーティングによる中継先の経路情報ではなく，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

（4） ポリシーベースルーティングとフロー制御の併用について

ポリシーベースルーティングの対象となるパケットを QoS フローリストで検出した場合，ポリシーベースルーティングによる中継と QoS フローリストで設定したフロー制御がどちらも動作します。

（5） フロー検出拡張モードでのポリシーベースルーティング

advance access-list を VLAN インタフェースに適用した場合，そのフィルタエントリはレイヤ 2 中継およびレイヤ 3 中継の両方をフロー検出の対象にします。しかし，動作にポリシーベースルーティングを設定したフィルタエントリは，レイヤ 3 中継だけをフロー検出の対象にします。そのため，レイヤ 2 中継フレームはフロー検出の対象外となり，統計情報はカウントされません。

（6） ポリシーベースルーティングと MTU

ポリシーベースルーティングリスト情報を設定したアクセスリストを適用している受信側インタフェースの MTU が，ポリシーベースルーティングの送信先インタフェースの MTU より大きいと，ポリシーベースルーティングが動作しないことがあります。ポリシーベースルーティングを使用する場合は，受信側インタフェースの MTU を送信側インタフェースの MTU 以下の値で設定してください。

（7） 起動時のポリシーベースルーティンググループ

ポリシーベースプログラムが動作したあと，中継可否の監視を停止する時間が経過して中継可能な経路のうち最も優先度の高い経路を選択した場合，ポリシーベースルーティングリスト情報の運用ログやトラップは出力しません。

（8） 系切替時のポリシーベースルーティンググループ

- 系切替の直前に経路の切り替えが発生すると，経路の設定が装置に反映されないことがあります。未設定の経路は，系切替したあと中継可否の監視を停止する時間が経過すると反映されます。
- 系切替したあと，中継可否の監視を停止する時間が経過して中継可能な経路のうち最も優先度の高い経路を再選択した場合，ポリシーベースルーティングリスト情報の運用ログやトラップは出力しません。

（9） ポリシーベースプログラムの再起動

ポリシーベースルーティンググループとポリシーベーススイッチンググループは，ポリシーベースプログラムで制御しています。そのため，ポリシーベースプログラムが再起動すると，どちらの機能にも影響があります。

4.2 コンフィグレーション

4.2.1 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 4-8 コンフィグレーションコマンド一覧

コマンド名	説明
default	ポリシーベースルーティングリスト情報のデフォルト動作を設定します。
policy-interface	ポリシーベースルーティングリスト情報に経路を設定します。
policy-list	ポリシーベースルーティングリスト情報を設定します。
policy-list default-aging-interval	系切替時にポリシーベースルーティングの中継可否の監視を停止する時間を設定します。
recover	ポリシーベースルーティングリスト情報の経路切り戻し動作を設定します。
access-list ※	IPv4 フィルタとして動作するアクセスリストを設定します。
advance access-group ※	VLAN インタフェースに対して Advance フィルタを適用し，Advance フィルタ機能を有効にします。
advance access-list ※	Advance 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-group ※	VLAN インタフェースに対して IPv4 フィルタを適用し，IPv4 フィルタ機能を有効にします。
ip access-list extended ※	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。
permit ※	フィルタでのアクセス中継する条件を指定します。

注※

「コンフィグレーションコマンドレファレンス Vol.2　4. アクセスリスト」を参照してください。

ポリシーベースルーティングの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 4-9 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トラッキング機能）

コマンド名	説明
default-state	デフォルトトラック状態を設定します。
disable	トラックの動作を停止します。
failure detection	障害発生検証中のポーリング回数やポーリング間隔を設定します。
interval	ポーリング間隔を設定します。
recovery detection	障害回復検証中のポーリング回数やポーリング間隔を設定します。
timeout	ポーリング応答待ち時間を設定します。
track-object	トラッキング機能のトラックを設定します。
type icmp	トラック種別として IPv4 ICMP ポーリング監視を設定します。

4.2.2 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を設定する例を次に示します。

(1) アクセスリストの動作に中継先の経路を指定

IPv4 パケットをフロー検出条件として，IPv4 アドレスをネクストホップとするポリシーベースルーティングを設定する例を次に示します。

[設定のポイント]

アクセスリストを使用してポリシーベースルーティングを設定します。

[コマンドによる設定]

1. **(config)# ip access-list extended FIRE_WALL_POLICY**
   ip access-list（FIRE_WALL_POLICY）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。

2. **(config-ext-nacl)# permit tcp any any action policy interface vlan 100 next-hop 192.168.1.1**
   IPv4 パケットをポリシーベースルーティングする IPv4 パケットフィルタを設定します。ネクストホップ IP アドレスは，192.168.1.1 を設定します。

3. **(config-ext-nacl)# permit ip any any**
   すべてのフレームを中継する IPv4 パケットフィルタを設定します。

4. **(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。

5. **(config)# interface vlan 10**
   VLAN10 のインタフェースモードに移行します。

6. **(config-if)# ip access-group FIRE_WALL_POLICY in layer3-forwarding**
   受信側にレイヤ 3 中継を対象とするポリシーベースルーティングを設定した IPv4 フィルタを有効にします。

(2) ポリシーベースルーティンググループの設定

IPv4 パケットをフロー検出条件として，ポリシーベースルーティングリスト情報を設定する例を次に示します。

[設定のポイント]

アクセスリストを使用してポリシーベースルーティングリスト情報を設定します。

[コマンドによる設定]

1. **(config)# policy-list 10**
   ポリシーベースルーティングリスト情報をリスト番号 10 で設定します。本リストを作成すると，ポリシーベースルーティングリスト情報のモードに移行します。

2. **(config-pol)# policy-interface vlan 100 next-hop 192.168.1.1**
   ポリシーベースルーティングリスト情報に優先度の高い経路として，VLAN100，ネクストホップアドレス 192.168.1.1 を設定します。

3. **(config-pol)# policy-interface vlan 200 next-hop 192.168.2.1**

ポリシーベースルーティングリスト情報に冗長経路として，VLAN200，ネクストホップアドレス 192.168.2.1 を設定します。

4. **(config-pol)# default permit**
   ポリシーベースルーティングリスト情報のデフォルト動作に通常中継を設定します。

5. **(config-pol)# exit**
   ポリシーベースルーティングリスト情報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 POLICY_GROUP**
   ip access-list（POLICY_GROUP）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 tcp any any action policy-list 10**
   IPv4 パケットをポリシーベースルーティングするポリシーベースルーティングリスト情報を設定します。リスト番号には 10 を設定します。

8. **(config-ext-nacl)# permit ip any any**
   すべてのフレームを中継する 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 vlan 10**
    VLAN10 のインタフェースモードに移行します。

11. **(config-if)# ip access-group POLICY_GROUP in layer3-forwarding**
    受信側にレイヤ 3 中継を対象とするポリシーベースルーティングを設定した IPv4 フィルタを有効にします。

（3） 経路切り戻し動作に「切り戻さない」を設定

中継先の経路を設定済みのポリシーベースルーティングリスト情報の経路切り戻し動作として，「切り戻さない」を設定する例を次に示します。

[設定のポイント]

経路切り戻し動作に「切り戻さない」を設定したときは，運用コマンド show ip cache policy で対象のポリシーベースルーティングリスト情報に反映され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)# policy-list 10**
   リスト番号 10 のポリシーベースルーティングリスト情報のモードに移行します。

2. **(config-pol)# recover off**
   経路切り戻し動作に「切り戻さない」を設定します。設定したあとは運用コマンド show ip cache policy 10 を実行してください。

(4) トラッキング機能の設定

IPv4 ICMP ポーリング監視トラックを設定します。

[設定のポイント]

すべてのパラメータを設定したあとでポーリングを開始する場合，次の順序で設定することをお勧めします。

1. track-object コマンドでトラック ID を指定
2. disable コマンドでトラックの動作を停止
3. すべてのパラメータを指定
4. no disable コマンドでトラックの動作停止を解除

なお，IPv4 ICMP ポーリング監視では，送信元 IPv4 アドレスを設定しておくと応答パケットの宛先アドレスが固定されるため，応答パケットの経路が設計しやすくなります。

[コマンドによる設定]

1. **(config)# track-object 1000**
   設定するトラック ID を指定します。

2. **(config-track-object)# disable**
   設定中のトラックの動作を停止します。

3. **(config-track-object)# default-state up**
   トラックのデフォルトトラック状態を Up と指定します。以降，トラックが動作を開始してからトラック状態が Down に変わるまで，トラック状態は Up です。

4. **(config-track-object)# type icmp 192.0.2.2 nexthop 192.168.1.1 source 198.51.100.1**
   (config-track-object)# timeout 5
   (config-track-object)# interval 10
   (config-track-object)# failure detection 4 trial 5 interval 10
   (config-track-object)# recovery detection 4 trial 5 interval 10
   トラックを，192.0.2.2 を監視する IPv4 ICMP ポーリング監視トラックとして指定します。ポーリングパケットの送信元アドレスを 198.51.100.1 と指定します。
   さらに，トラックの応答待ち時間，通常のポーリング間隔，障害発生検証中のポーリング回数とポーリング間隔，障害回復検証中のポーリング回数とポーリング間隔をそれぞれ指定します。

5. **(config-track-object)# no disable**
   トラックの動作を停止するコンフィグレーションを削除します。削除すると，トラックが動作を開始します。

6. **(config-track-object)# exit**
   トラッキング機能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。

7. **(config)# policy-list 10**
   ポリシーベースルーティングリスト情報をリスト番号 10 で設定します。本リストを作成すると，ポリシーベースルーティングリスト情報のモードに移行します。

8. **(config-pol)# policy-interface vlan 100 next-hop 192.168.1.1 track-object 1000**

ポリシーベースルーティングリスト情報の経路として，VLAN100，ネクストホップアドレス 192.168.1.1，トラック ID1000 を設定します。

9. **(config-pol)# default permit**
   ポリシーベースルーティングリスト情報のデフォルト動作に通常中継を設定します。

10. **(config-pol)# exit**
    ポリシーベースルーティングリスト情報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。

11. **(config)# ip access-list extended POLICY_GROUP**
    ip access-list（POLICY_GROUP）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。

12. **(config-ext-nacl)# permit tcp any any action policy-list 10**
    IPv4 パケットをポリシーベースルーティングするポリシーベースルーティングリスト情報を設定します。リスト番号には 10 を設定します。

13. **(config-ext-nacl)# permit ip any any**
    すべてのフレームを中継する IPv4 パケットフィルタを設定します。

14. **(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。

15. **(config)# interface vlan 10**
    VLAN10 のインタフェースモードに移行します。

16. **(config-if)# ip access-group POLICY_GROUP in layer3-forwarding**
    受信側にレイヤ 3 中継を対象とするポリシーベースルーティングを設定した IPv4 フィルタを有効にします。

4.2.3 ポリシーベースルーティングでのエクストラネットの設定【OP-NPAR】

ネットワーク・パーティションのエクストラネットを実現するため，ポリシーベースルーティングを設定します。

VRF 間で通信できるように，二つの VRF を設定したあと，それぞれの VRF（VLAN）にポリシーベースルーティングを設定します。

（1）二つの VRF の設定

[設定のポイント]

二つの VRF を設定し，それぞれ異なる VLAN 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 vlan 20
(config-if)# vrf forwarding 2
(config-if)# ip address 192.168.20.1 255.255.255.0
(config-if)# exit
```
VRF2 を設定して，VLAN20 に VRF2 と IPv4 アドレス 192.168.20.1，サブネットマスク 255.255.255.0 を設定します。

2.
```
(config)# vrf definition 3
(config-vrf)# exit
(config)# interface vlan 30
(config-if)# vrf forwarding 3
(config-if)# ip address 192.168.30.1 255.255.255.0
(config-if)# exit
```
VRF3 を設定して，VLAN30 に VRF3 と IPv4 アドレス 192.168.30.1，サブネットマスク 255.255.255.0 を設定します。

（2）VRF 間のポリシーベースルーティングの設定

［設定のポイント］

VRF の異なる VLAN 間でポリシーベースルーティングを設定します。ポリシーベースルーティングはアクセスリストを使用して設定します。

なお，ポリシーベースルーティングリスト情報に対象の経路を登録すると，ポリシーベースルーティンググループでも同様に運用できます。

［コマンドによる設定］

1.
```
(config)# ip access-list extended EXTRA_NET_POLICY_VLAN_20_TO_30
```
ip access-list（EXTRA_NET_POLICY_VLAN_20_TO_30）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。

2.
```
(config-ext-nacl)# permit ip any 192.168.30.0 0.0.0.255 action policy
interface vlan 30 next-hop 192.168.30.2
```
宛先 IP アドレス 192.168.30.0/24 の IPv4 パケットをポリシーベースルーティングする IPv4 パケットフィルタを設定します。ネクストホップ IP アドレスは，VLAN30 の 192.168.30.2 を設定します。

3.
```
(config-ext-nacl)# permit ip any any
(config-ext-nacl)# exit
```
すべてのフレームを中継する IPv4 パケットフィルタを設定して，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 vlan 20
(config-if)# ip access-group EXTRA_NET_POLICY_VLAN_20_TO_30 in
layer3-forwarding
```
VLAN20 の受信側にレイヤ 3 中継を対象とする ip access-list（EXTRA_NET_POLICY_VLAN_20_TO_30）を有効にします。

5.
```
(config-if)# exit
```
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 EXTRA_NET_POLICY_VLAN_30_TO_20**
   ip access-list（EXTRA_NET_POLICY_VLAN_30_TO_20）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 192.168.20.0 0.0.0.255 action policy interface vlan 20 next-hop 192.168.20.2**
   宛先 IP アドレス 192.168.20.0/24 の IPv4 パケットをポリシーベースルーティングする IPv4 パケットフィルタを設定します。ネクストホップ IP アドレスは，VLAN20 の 192.168.20.2 を設定します。

8. **(config-ext-nacl)# permit ip any any**
   (config-ext-nacl)# exit
   すべてのフレームを中継する IPv4 パケットフィルタを設定して，グローバルコンフィグレーションモードに戻ります。

9. **(config)# interface vlan 30**
   (config-if)# ip access-group EXTRA_NET_POLICY_VLAN_30_TO_20 in layer3-forwarding
   VLAN30 の受信側にレイヤ 3 中継を対象とする ip access-list（EXTRA_NET_POLICY_VLAN_30_TO_20）を有効にします。

4.3 オペレーション

4.3.1 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 4-10 運用コマンド一覧

コマンド名	説明
show ip policy	指定した VLAN インタフェースに設定しているアクセスリスト，およびポリシーベースルーティングリスト情報を表示します。
show ip cache policy	指定したポリシーベースルーティングリスト情報の経路情報と状態を表示します。
reset policy-list	経路情報を再選択します。
restart policy	ポリシーベースプログラムを再起動します。
show access-filter ※	アクセスグループコマンド（ip access-group，advance access-group）で設定したアクセスリスト（access-list，ip access-list，advance access-list）の統計情報を表示します。
clear access-filter ※	アクセスグループコマンド（ip access-group，advance access-group）で設定したアクセスリスト（access-list，ip access-list，advance access-list）の統計情報をクリアします。

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

ポリシーベースルーティングのトラッキング機能の運用コマンド一覧を次の表に示します。

表 4-11 運用コマンド一覧（ポリシーベースルーティングのトラッキング機能）

コマンド名	説明
show track-object	トラッキング機能のトラック情報を表示します。
dump protocols track-object	トラックオブジェクトプログラムが採取しているトレース情報やデバッグ情報をファイルへ出力します。
restart track-object	トラックオブジェクトプログラムを再起動します。

4.3.2 ポリシーベースルーティングの確認

(1) アクセスリストの動作に中継先の経路を指定したポリシーベースルーティングの確認

show access-filter コマンドを実行して，アクセスリストの動作に中継先の経路を指定したポリシーベースルーティングの動作を確認できます。指定した VLAN インタフェースのフィルタに「Extended IP access-list:FIRE_WALL_POLICY layer3-forwarding」および「action policy interface vlan 100 next-hop 192.168.1.1」が表示されること，「matched packets」がカウントされていることを確認します。

図 4-6 show access-filter コマンドの実行結果

```
> show access-filter interface vlan 10 FIRE_WALL_POLICY in
Date 2006/10/01 12:00:00 UTC
Using Interface:vlan 10 in
Extended IP access-list:FIRE_WALL_POLICY layer3-forwarding
      remark "permit Fire Wall policy"
     permit tcp(6) any any action policy interface vlan 100 next-hop 192.168.1.1
        matched packets       :            74699826
      permit ip any any
        matched packets       :              264176
      implicitly denied packets:                   0
```

(2) ポリシーベースルーティンググループの確認

ポリシーベースルーティンググループの動作を確認する方法を示します。

show ip policy コマンドを実行して，VLAN インタフェースの番号からポリシーベースルーティングリスト情報を設定しているアクセスリストの情報が表示されることを確認します。

図 4-7 show ip policy コマンドの実行結果

```
> show ip policy
Date 2012/01/01 12:00:00 UTC
VLAN ID  Access List Name/Number            Sequence  Policy List
     10  POLICY_GROUP                             10           10
```

show access-filter コマンドを実行して，ポリシーベースルーティングリスト情報を設定したアクセスリストの動作を確認できます。指定した VLAN インタフェースのフィルタに「Extended IP access-list:POLICY_GROUP layer3-forwarding」および「action policy-list 10」が表示されること，「matched packets」がカウントされていることを確認します。

図 4-8 show access-filter コマンドの実行結果

```
> show access-filter interface vlan 10 POLICY_GROUP in
Date 2012/01/01 12:00:00 UTC
Using Interface:vlan 10 in
Extended IP access-list:POLICY_GROUP layer3-forwarding
      remark "permit Policy Group policy"
      permit tcp(6) any any action policy-list 10
        matched packets       :            74699826
      permit ip any any
        matched packets       :              264176
      implicitly denied packets:                   0
```

show ip cache policy コマンドを実行して，ポリシーベースルーティングリスト情報内で選択している経路を確認できます。指定したポリシーベースルーティングリスト情報に設定している経路がすべて表示されること，すべての経路のうち選択している経路を示す「*>」が表示されることを確認します。

図 4-9 show ip cache policy コマンドの実行結果（経路の確認）

```
> show ip cache policy 10
Date 2012/01/01 12:00:00 UTC
Policy Base Routing Default Init Interval :  200
   Start Time : 2012/01/01 00:00:00
   End Time   : 2012/01/01 00:03:20
Policy Base Routing Default Aging Interval :  200
   Start Time : 2012/01/01 01:00:00
   End Time   : 2012/01/01 01:03:20
Policy Base Routing List :  10
   Default : Permit
   Recover : On
   Priority    Sequence  VLAN ID  Status  Next Hop         Track Object ID
 *>       1          10      100  Up      192.168.1.1                    -
          2          20      200  Up      192.168.2.1                    -
```

(3) 経路切り戻し動作の確認

show ip cache policy コマンドを実行して，ポリシーベースルーティングリスト情報に設定されている経路切り戻し動作を確認できます。

図 4-10 show ip cache policy コマンドの実行結果（経路切り戻し動作の確認）

```
> show ip cache policy 10
Date 2012/01/01 12:00:00 UTC
Policy Base Routing Default Init Interval :  200
   Start Time : 2012/01/01 00:00:00
   End Time   : 2012/01/01 00:03:20
Policy Base Routing Default Aging Interval :  200
   Start Time : 2012/01/01 01:00:00
   End Time   : 2012/01/01 01:03:20
Policy Base Routing List :  10
   Default : Permit
   Recover : Off                                                          …1
   Priority    Sequence  VLAN ID  Status  Next Hop         Track Object ID
 *>       1          10      100  Up      192.168.1.1                    -
          2          20      200  Up      192.168.2.1                    -
```

1.「Recover：Off」の場合は，経路切り戻し動作として「切り戻さない」が設定されています。

(4) トラッキング機能の確認

トラッキング機能の動作を確認する方法を示します。

show track-object コマンドを実行すると，トラック状態が表示されます。「State」で各トラックのトラック状態を確認できます。

図 4-11 show track-object コマンドの実行結果

```
> show track-object
Date 2012/01/01 12:00:00 UTC
Track State          Type        Target
101   UP(Active)     ICMP        172.16.1.1
102   UP(Transit)    ICMP        172.16.2.1
201   DOWN(Transit)  ICMP        172.16.3.1
>
```

show track-object コマンドでトラック ID を指定すると，指定したトラックのトラック情報が詳細表示されます。「State」でトラック状態を，「Last Change」でトラック状態が遷移した時刻を確認できます。

図 4-12　show track-object コマンドの実行結果（トラック ID 指定）

```
> show track-object 101
Date 2012/01/01 12:00:00 UTC
Track: 101
   State: UP(Active),   Last Change: 2011/12/30 18:11:23
   Type: ICMP
      Destination: 172.16.1.1
      Source: 172.16.1.100, Nexthop: 172.16.1.200
      TOS: max-reliability(2), Precedence: flash(3)
      Interval: 6sec, Timeout: 2sec
>
```

5 DHCP/BOOTP リレーエージェント機能

この章では，DHCP/BOOTP リレーエージェント機能の解説，コンフィグレーション，および確認方法について説明します。

5.1 解説

DHCP/BOOTP リレーエージェント機能とは，DHCP/BOOTP サーバ（以降，サーバという）と DHCP/BOOTP クライアント（以降，クライアントという）が異なるサブネットにある場合，クライアントがブロードキャストする DHCP/BOOTP パケットをサーバに中継する機能です。

DHCP/BOOTP パケットをサーバに中継する際，DHCP/BOOTP パケットの宛先 IP アドレスに，コンフィグレーションで設定したサーバの IP アドレス，またはサーバのサブネットへ中継できるルータの IP アドレスであるヘルパーアドレスを設定します。

5.1.1 サポート仕様

本装置の DHCP/BOOTP リレーエージェント機能のサポート仕様を次の表に示します。

表 5-1 DHCP/BOOTP リレーエージェント機能のサポート仕様

項目	仕様
接続構成	• DHCP リレーエージェント経由で DHCP クライアントを収容 • DHCP リレーエージェント経由で収容
BOOTP 対応	サポート
VRF 対応	同一 VRF，およびエクストラネット※の VLAN 間で中継可能

注※

エクストラネットで DHCP/BOOTP リレーエージェント機能を使用する場合は，VRF 間の経路交換による構成としてください。

5.1.2 DHCP/BOOTP パケットを受信したときのチェック内容

DHCP/BOOTP パケットを受信したときのチェック内容を次の表に示します。

表 5-2 DHCP/BOOTP パケットを受信したときのチェック内容

DHCP/BOOTP パケットヘッダフィールド	チェック内容	チェック異常時のパケットの扱い	
		クライアント→サーバ	サーバ→クライアント
BOOTP REQUEST HOPS	コンフィグレーションの設定値より小さいこと	廃棄する	廃棄しない
リレーエージェントアドレス	本装置宛てであること	廃棄する	廃棄する
IP ヘッダ TTL	1 以上	廃棄する	廃棄する
IP ヘッダ送信元アドレス	ネットワーク番号が 0 でないこと	廃棄しない	廃棄する

5.1.3 中継時の設定内容

DHCP/BOOTP リレーエージェント機能が DHCP/BOOTP パケットを中継するときの設定内容を次の表に示します。

表 5-3 DHCP/BOOTP 中継時の設定内容

パケットヘッダフィールド	設定条件	条件を満たす場合に設定する内容	
		クライアント→サーバ	サーバ→クライアント
DHCP/BOOTP ヘッダリレーエージェントアドレス	0.0.0.0 の時	• 受信インタフェースにマルチホームの設定がない場合，受信インタフェースの IP アドレスを設定します。 • 受信インタフェースにマルチホームの設定がある場合，運用コマンドの show dhcp giaddr コマンドで表示される IP アドレスを設定します。	－
DHCP/BOOTP ヘッダブロードキャストフラグ	1 のとき	－	宛先 IP アドレスを制限付きブロードキャスト※に設定します。
	0 のとき	－	宛先 IP アドレスをクライアント IP アドレスに設定します。 宛先 MAC アドレスをクライアントハードウェアアドレスに設定します。
DHCP/BOOTP ヘッダ BOOTP REQUEST HOPS	DHCP/BOOTP REQUEST パケットを DHCP/BOOTP サーバへ中継するとき	1 増加させます。	－
IP ヘッダ送信元アドレス	DHCP/BOOTP REQUEST パケットを DHCP/BOOTP サーバへ中継するとき	送信インタフェースの IP アドレスを設定します。	－
	DHCP/BOOTP REPLY パケットをクライアントへ中継するとき	－	送信インタフェースの IP アドレスを設定します。
IP ヘッダ宛先アドレス	制限付きブロードキャスト※のとき	ヘルパーアドレスを設定します。	－

（凡例） －：該当しない

注※

IP ブロードキャストアドレスで，255.255.255.255 または 0.0.0.0 の形式を持つ IP アドレスを示します。

5.1.4 DHCP/BOOTP リレーエージェント機能使用時の注意事項

1. DHCP/BOOTP リレーエージェント機能と VRRP 機能を同一インタフェースで同時に運用する場合は，DHCP/BOOTP サーバで，DHCP/BOOTP クライアントゲートウェイアドレス（ルータオプション）を本装置に設定した仮想ルータアドレスに設定する必要があります。
2. 本装置で中継可能なパケットは，IP パケットサイズが 1500 バイト以下で，かつフラグメント化されていないパケットです。

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

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 5-4 コンフィグレーションコマンド一覧

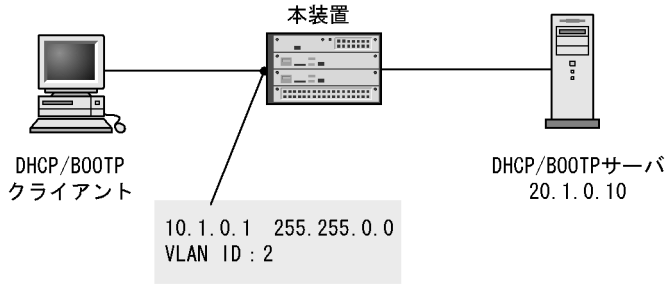
コマンド名	説明
ip bootp-hops	Hops スレッシュホールド値を設定します。
ip helper-address	DHCP リレーエージェントによる転送先アドレスを設定します。「5.2.2 基本構成での設定」，および「5.2.3 マルチホーム構成での設定」では，DHCP/BOOTP サーバの IP アドレスをヘルパーアドレスとして設定するときに使用します。
ip relay-agent-address	DHCP/BOOTP クライアント接続インタフェースのリレーエージェントアドレス（giaddr）を設定します。「5.2.3 マルチホーム構成での設定」では，リレーエージェントアドレスとしてネットワーク A の IP アドレスを設定するときに使用します。

5.2.2 基本構成での設定

[設定のポイント]

DHCP リレーエージェントで，BOOTP REQUEST パケットを中継する転送先アドレスであるヘルパーアドレスを設定します。

図 5-1 基本構成（DHCP/BOOTP サーバと DHCP/BOOTP クライアント間にリレーエージェントが 1 台ある場合）



[コマンドによる設定]

1. **(config)# vlan 2**
   (config-vlan)# exit
   (config)# interface gigabitethernet 1/5
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 2
   (config-if)# exit
   (config)# interface vlan 2
   (config-if)# ip address 10.1.0.1 255.255.0.0
   (config-if)# exit
   あらかじめ VLAN ID，回線，アクセスポート，VLAN インタフェースと IP アドレスを設定しておきます。

2. **(config)# vlan 3**
   (config-vlan)# exit
   (config)# interface gigabitethernet 1/7
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 3
   (config-if)# exit
   (config)# interface vlan 3
   (config-if)# ip address 20.1.0.1 255.255.0.0
   (config-if)# exit
   項番 1 と同様に，DHCP/BOOTP サーバへ中継するインタフェースにもあらかじめ VLAN ID，回線，アクセスポート，IP アドレスの設定をしておきます。

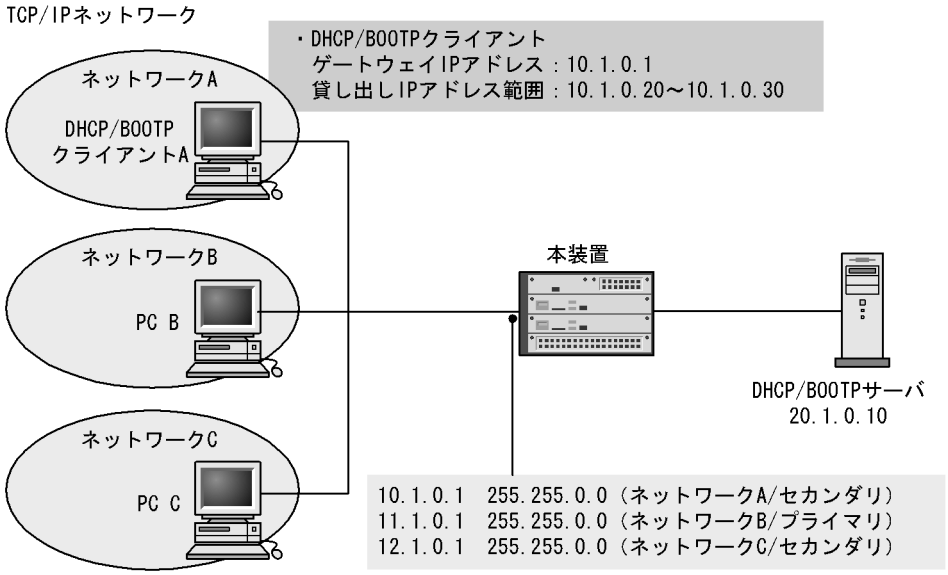
3. **(config)# interface vlan 2**
   (config-if)# ip helper-address 20.1.0.10
   (config-if)# exit
   DHCP/BOOTP サーバの IP アドレスをヘルパーアドレスとして設定します。

5.2.3 マルチホーム構成での設定

[設定のポイント]

マルチホーム構成では，プライマリ IP アドレスを入力インタフェースの IP アドレスとしますが，ip relay-agent-address コマンドで任意の IP アドレスを指定することでセカンダリ IP アドレスを入力インタフェースとして使用できます。
なお，ネットワーク B およびネットワーク C は DHCP/BOOTP 以外のネットワークとします。

図 5-2 マルチホーム構成



[コマンドによる設定]

1. **(config)# vlan 2**
   (config-vlan)# exit

```
(config)# interface gigabitethernet 1/5
(config-if)# switchport mode access
(config-if)# switchport access vlan 2
(config-if)# exit
```

あらかじめ VLAN ID，回線，アクセスポートを設定しておきます。

2.
```
(config)# interface vlan 2
(config-if)# ip address 11.1.0.1 255.255.0.0
(config-if)# ip address 10.1.0.1 255.255.0.0 secondary
(config-if)# ip address 12.1.0.1 255.255.0.0 secondary
(config-if)# exit
```

ネットワーク B の IP アドレスをプライマリ，ネットワーク A および C の IP アドレスをセカンダリとして設定する例です。

3.
```
(config)# vlan 3
(config-vlan)# exit
(config)# interface gigabitethernet 1/7
(config-if)# switchport mode access
(config-if)# switchport access vlan 3
(config-if)# exit
(config)# interface vlan 3
(config-if)# ip address 20.1.0.1 255.255.0.0
(config-if)# exit
```

項番 1，2 と同様に，DHCP/BOOTP サーバへ中継するインタフェースにもあらかじめ VLAN ID，回線，アクセスポート，IP アドレスの設定をしておきます。

4.
```
(config)# interface vlan 2
(config-if)# ip helper-address 20.1.0.10
```

DHCP/BOOTP サーバの IP アドレスをヘルパーアドレスとして設定します。

5.
```
(config-if)# ip relay-agent-address 10.1.0.1
(config-if)# exit
```

リレーエージェントアドレスとしてネットワーク A の IP アドレスを設定します。

[注意事項]

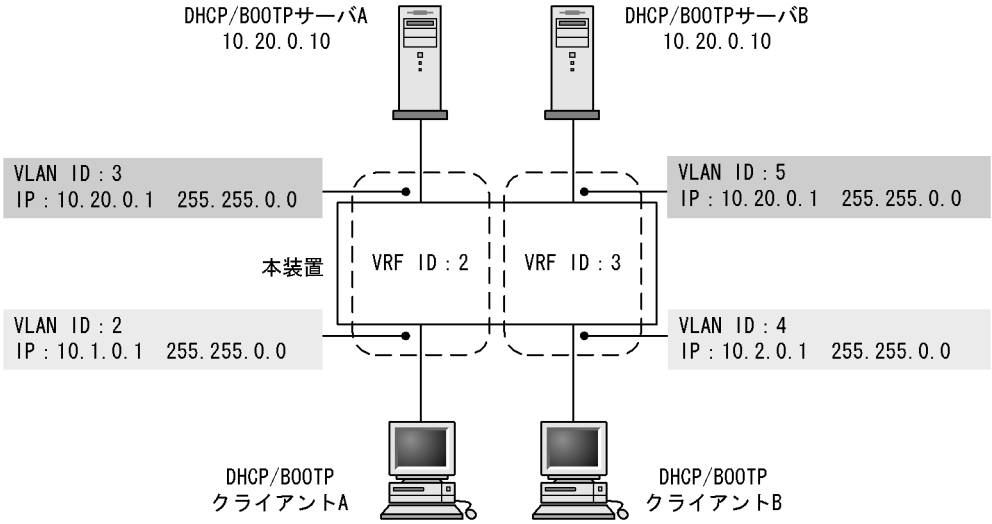
ip relay-agent-address コマンドを省略した場合，リレーエージェントアドレスは，そのインタフェースに設定したプライマリ IP アドレスとなります。

5.2.4 VRF 構成での設定【OP-NPAR】

[設定のポイント]

VRF 構成では，VRF ごとに DHCP/BOOTP サーバを用意します。

図 5-3 VRF 構成



[コマンドによる設定]

1. **(config)# vlan 2**
   (config-vlan)# exit
   (config)# interface gigabitethernet 1/5
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 2
   (config-if)# exit
   (config)# vrf definition 2
   (config-vrf)# exit
   (config)# interface vlan 2
   (config-if)# vrf forwarding 2
   (config-if)# ip address 10.1.0.1 255.255.0.0
   (config-if)# exit
   あらかじめ VLAN ID，回線，アクセスポート，VRF，VLAN インタフェース，VRF ID，IP アドレスを設定しておきます。

2. **(config)# vlan 3**
   (config-vlan)# exit
   (config)# interface gigabitethernet 1/7
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 3
   (config-if)# exit
   (config)# interface vlan 3
   (config-if)# vrf forwarding 2
   (config-if)# ip address 10.20.0.1 255.255.0.0
   (config-if)# exit
   項番 1 と同様に，DHCP/BOOTP サーバへ中継するインタフェースにもあらかじめ VLAN ID，回線，アクセスポート，VRF ID，IP アドレスの設定をしておきます。

3. **(config)# vlan 4**

```
(config-vlan)# exit
(config)# interface gigabitethernet 1/9
(config-if)# switchport mode access
(config-if)# switchport access vlan 4
(config-if)# exit
(config)# vrf definition 3
(config-vrf)# exit
(config)# interface vlan 4
(config-if)# vrf forwarding 3
(config-if)# ip address 10.2.0.1 255.255.0.0
(config-if)# exit
(config)# vlan 5
(config-vlan)# exit
(config)# interface gigabitethernet 1/11
(config-if)# switchport mode access
(config-if)# switchport access vlan 5
(config-if)# exit
(config)# interface vlan 5
(config-if)# vrf forwarding 3
(config-if)# ip address 10.20.0.1 255.255.0.0
(config-if)# exit
```

項番 1，2 と同様に，VRF ID 3 側の各インタフェースにもあらかじめ VLAN ID，回線，アクセスポート，VRF，VRF ID，IP アドレスの設定をしておきます。

4.
```
(config)# interface vlan 2
(config-if)# ip helper-address 10.20.0.10
```
VRF ID 2 側の DHCP/BOOTP サーバの IP アドレスをヘルパーアドレスとして設定します。

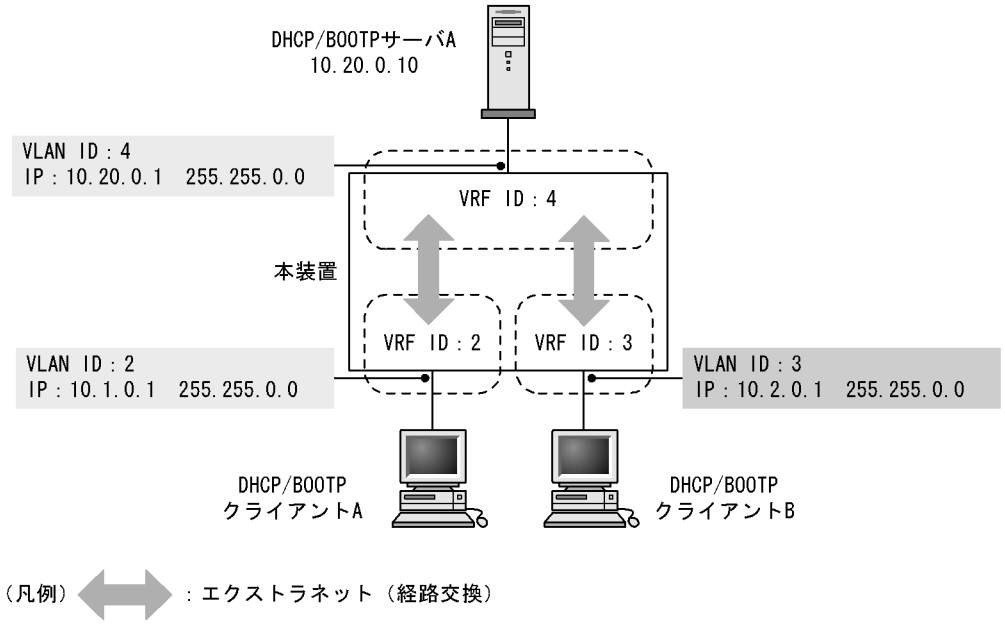
5.
```
(config)# interface vlan 4
(config-if)# ip helper-address 10.20.0.10
```
VRF ID 3 側の DHCP/BOOTP サーバの IP アドレスをヘルパーアドレスとして設定します（VLAN ID 2 とは VRF ID が異なるため，転送先となるヘルパーアドレスは別の宛先として扱われます）。

5.2.5 エクストラネット構成での設定【OP-NPAR】

[設定のポイント]

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。

図 5-4 エクストラネット構成



[コマンドによる設定]

1.
```
(config)# vlan 2
(config-vlan)# exit
(config)# interface gigabitethernet 1/5
(config-if)# switchport mode access
(config-if)# switchport access vlan 2
(config-if)# exit
(config)# vrf definition 2
(config-vrf)# exit
(config)# interface vlan 2
(config-if)# vrf forwarding 2
(config-if)# ip address 10.1.0.1 255.255.0.0
(config-if)# exit
```
あらかじめ VLAN ID，回線，アクセスポート，VRF，VLAN インタフェース，VRF ID，IP アドレスを設定しておきます。

2.
```
(config)# vlan 4
(config-vlan)# exit
(config)# interface gigabitethernet 1/1
(config-if)# switchport mode access
(config-if)# switchport access vlan 4
(config-if)# exit
(config)# vrf definition 4
(config-vrf)# exit
(config)# interface vlan 4
(config-if)# vrf forwarding 4
(config-if)# ip address 10.20.0.1 255.255.0.0
```

```
(config-if)# exit
```
DHCP/BOOTP サーバへ中継するインタフェースにもあらかじめ VLAN ID，回線，アクセスポート，VRF，VRF ID，IP アドレスの設定をしておきます。

3.
```
(config)# vlan 3
(config-vlan)# exit
(config)# interface gigabitethernet 1/7
(config-if)# switchport mode access
(config-if)# switchport access vlan 3
(config-if)# exit
(config)# vrf definition 3
(config-vrf)# exit
(config)# interface vlan 3
(config-if)# vrf forwarding 3
(config-if)# ip address 10.2.0.1 255.255.0.0
(config-if)# exit
```
項番 1 と同様に，VRF ID 3 側のインタフェースにもあらかじめ VLAN ID，回線，アクセスポート，VRF，VRF ID，IP アドレスの設定をしておきます。

4.
```
(config)# route-map VRF4PERMIT permit 10
(config-route-map)# match vrf 4
(config-route-map)# exit
(config)# vrf definition 2
(config-vrf)# import inter-vrf VRF4PERMIT
(config-vrf)# exit
(config)# vrf definition 3
(config-vrf)# import inter-vrf VRF4PERMIT
(config-vrf)# exit
```
VRF ID 4 の経路が permit になるフィルタを作成し，VRF ID 4 の経路を VRF ID 2 と VRF ID 3 に導入するように設定します。

5.
```
(config)# route-map VRF2AND3PERMIT permit 10
(config-route-map)# match vrf 2 3
(config-route-map)# exit
(config)# vrf definition 4
(config-vrf)# import inter-vrf VRF2AND3PERMIT
(config-vrf)# exit
```
VRF ID 2，3 の経路が permit になるフィルタを作成し，VRF ID 2，3 の経路を VRF ID 4 に導入するように設定します。

6.
```
(config)# interface vlan 2
(config-if)# ip helper-address 10.20.0.10
```
VRF ID 4 側の DHCP/BOOTP サーバの IP アドレスをヘルパーアドレスとして設定します。

7.
```
(config)# interface vlan 3
(config-if)# ip helper-address 10.20.0.10
```

VRF ID 4 側の DHCP/BOOTP サーバの IP アドレスをヘルパーアドレスとして設定します。

5.3 オペレーション

5.3.1 運用コマンド一覧

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 5-5 運用コマンド一覧

コマンド名	説明
show dhcp traffic	DHCP/BOOTP リレーエージェントの各種統計情報を表示します。
clear dhcp traffic	リレーエージェント統計情報を 0 クリアします。
show dhcp giaddr	DHCP/BOOTP サーバからの DHCP/BOOTP パケットの受信先 IP アドレスを表示します。

5.3.2 DHCP/BOOTP 受信先 IP アドレスの確認

show dhcp giaddr コマンドを実行し，表示された IP アドレスが DHCP/BOOTP クライアントが接続されている本装置設定のインタフェースの IP アドレスと一致していることを確認してください。

図 5-5 show dhcp giaddr コマンドの実行結果

```
>show dhcp giaddr all
Date 2008/10/15 12:00:00 UTC
DHCP GIADDR <vlan 2>： 10.1.0.1
```

6 DHCP サーバ機能

DHCP サーバ機能は，DHCP クライアントに対して，IP アドレスやオプション情報などを動的に割り当てるための機能です。この章では，DHCP サーバ機能の解説およびコンフィグレーションについて説明します。

6.1 解説

DHCP サーバ機能は，DHCP クライアントに対して，IP アドレスやオプション情報などを動的に割り当てるための機能です。この節では，本装置の DHCP サーバ機能の仕様および動作内容を説明します。

6.1.1 サポート仕様

本装置の DHCP サーバ機能のサポート仕様を次の表に示します。DHCP サーバとクライアント接続は，同一ネットワーク内での直結，および DHCP リレーエージェント経由で行います。

表 6-1 DHCP サーバ機能のサポート仕様

項目	仕様
接続構成	• DHCP クライアントを直接収容 • DHCP リレーエージェント経由で収容
BOOTP サーバ機能	未サポート
ダイナミック DNS 連携	サポート なお，本装置で対応しているのは RFC2136 の DNS UPDATE を使用したダイナミック DNS サーバです。
動的 / 固定 IP アドレス配布機能	サポート

6.1.2 クライアントへの配布情報

本装置でクライアントへ配布可能な情報の一覧を次の表に示します。配布可能な情報の中でオプション扱いの情報については，本装置で配布するオプションを指定した場合でも，クライアント側からオプション要求リストによって要求しない場合は配布データに含めません。

表 6-2 本装置でクライアントに配布する情報の一覧

情報名	概要
IP アドレス	クライアントが使用可能な IP アドレスを設定します。
IP アドレスリース時間	配布する IP アドレスのリース時間を設定します。本装置では default-lease-time/ max-lease-time パラメータとクライアントからの要求によって値が決定されます。(Option No：51)
サブネットマスク	本オプションはコンフィグレーションで指定したネットワーク情報のサブネットマスク長が使用されます。(Option No：1)
ルータオプション	クライアントのサブネット上にあるルータの IP アドレスのリストを指定します。リストは優先度の高いものから順に指定します。このリストがクライアントのゲートウェイアドレスとして使用されます。(Option No：3) なお，本オプションをコンフィグレーションで指定しなかった場合，ルータオプションを含めない代わりに，配布する IP アドレスと同じ値をルータオプションに設定してクライアントに返します。
DNS オプション	クライアントが利用できるドメインネームサーバの IP アドレスのリストを指定します。リストは優先度の高いものから順に指定します。(Option No：6)
ホストネームオプション	サーバでクライアントの名前を指定するときに設定します。名前はローカルドメイン名で制限される可能性があります。指定は文字列で行われます。(Option No：12)
ドメイン名オプション	クライアントがドメインネームシステムによってホスト名を変換するときに使用するドメイン名を指定します。(Option No：15)
NetBIOS over TCP/IP ネームサーバオプション	クライアントが参照する NetBIOS ネームサーバ (WINS サーバ) を IP アドレスのリストで指定します。リストは優先度の高いものから順に指定します。(Option No：44)

情報名	概要
NetBIOS over TCP/IP ノードタイプ指定オプション	NetBIOS オーバー TCP/IP クライアントのノードタイプ (NetBIOS 名前解決方法) を設定します。(Option No：46) • コード 1　B ノード (ブロードキャストノード) • コード 2　P ノード (Peer to Peer ノード (WINS を使用)) • コード 4　M ノード (ミックスノード (ブロードキャストで見つからない場合に WINS を使用する)) • コード 8　H ノード (ハイブリッドノード (WINS で見つからない場合に，ブロードキャストを使用する))

6.1.3 ダイナミック DNS 連携

本装置の DHCP サーバは IP アドレス配布と同時にダイナミック DNS サーバに対してエントリレコードを追加する機能（DNS 更新）に対応しています。この機能を使用するには DHCP サーバで対象とするゾーンと要求先 DNS サーバを指定した上で，DNS サーバ側も本装置からのレコード更新を受け付けるように設定する必要があります。

レコード更新の許可には IP アドレスによる許可と HMAC-MD5 の認証キーを使用する方法があります。IP アドレスによる許可は DNS サーバに接続している IP アドレスまたはネットワークからのアクセスを DNS サーバ側で許可するだけですが，認証キーを使用する場合は DNS サーバで指定されたキーと同じキーを DHCP サーバの DNS 認証キー情報に設定する必要があります。

ダイナミック DNS 連携時の注意事項

- 本装置の DHCP サーバでは動的に割り当てる IP アドレスだけ DNS 更新を行います。固定アドレスで配布を行う場合は事前に DNS サーバにレコードを追加してください。
- DNS 更新を行うには IP アドレス配布時に DHCP クライアントが FQDN を DHCP サーバに返す必要があります。必要な情報がない場合，DHCP サーバはそのリースに対する DNS 更新を行いません。具体的な設定については，クライアントに使用する装置の設定方法を参照してください。
- DNS 更新で認証キーを使用する場合，DNS サーバと本装置の時刻情報が一致している必要があります。多くの場合，時刻情報の誤差は UTC 時間で 5 分以下である必要があるため，NTP による時刻情報の同期を行ってください。

6.1.4 IP アドレスの二重配布防止

本装置の DHCP サーバのサービス（DHCP クライアントにアドレスを割り当てた状態）中に本装置が再起動した場合，本装置上にある割り当て用 IP アドレスのプールはすべて「空き状態」になります。しかし，そのあと本装置が IP アドレスを割り当てる際，事前に割り当てた IP アドレスに対して ICMP エコー要求パケットを送出し，その応答パケットの有無によってすでに使用しているクライアントがいないかを確認し，IP アドレスの二重割り当てを防止します。同時に，以前 IP アドレスを割り当てたクライアントに対しては同じ IP アドレスを割り当てようとするため，クライアントの通信には影響を与えません。

また，ICMP エコー要求パケットの応答が返ってきた（ネットワーク上の端末がすでにその IP アドレスを使っている）場合，show ip dhcp conflict コマンドの実行結果画面に衝突アドレス検出として表示します。

6.1.5 DHCP サーバ機能使用時の注意事項

DHCP サーバ機能使用時の注意事項について説明します。

(1) マルチホーム接続時の入力インタフェースの IP アドレス

マルチホーム接続では，プライマリ IP アドレスを入力インタフェースの IP アドレスとします。このサブネットに設定しているアドレスプールから IP アドレスを DHCP クライアントに割り当てます。

(2) リース時間を短くした場合の同時接続数

リース時間を 10 秒とした場合のクライアント最大接続数は 200 以下となるようにしてください。同様に 20 秒とした場合は 400 以下，30 秒の場合は 600 以下となるように同時接続数を調整してください。

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

DHCP サーバ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 6-3 コンフィグレーションコマンド一覧

コマンド名	説明
client-name	クライアントに配布するホスト名オプションを指定します。ホスト名オプションは，固定 IP アドレス配布でクライアントが使用するホスト名として使われます。
default-router	クライアントに配布するルータオプションを指定します。ルータオプションは，クライアントがサブネット上のルータ IP アドレス（デフォルトルータ）として使用可能な IP アドレスのリストです。「6.2.2 クライアントに IP を配布する設定」のようにクライアントが使用するルータの IP アドレスを設定します。
dns-server	クライアントに配布するドメインネームサーバオプションを指定します。ドメインネームサーバオプションは，クライアントで利用可能な DNS サーバの IP アドレスリストです。「6.2.4 ダイナミック DNS 連携時の設定」のようにクライアントが使用する DNS サーバの IP アドレスを設定します。
domain-name	クライアントに配布するドメインネームオプションを指定します。ドメインネームオプションは，クライアントで配布 IP アドレスに対する名称解決をドメインネームシステムで行う場合に，クライアントが使うべきドメインネームとして使用されます。「6.2.4 ダイナミック DNS 連携時の設定」のようにクライアントがホスト名解決に使用するドメインネームを設定します。
hardware-address	クライアント装置に固定の IP アドレスを配布する際に，対象となる装置の MAC アドレスを指定します。本コマンドはホストコマンドとセットで使用します。「6.2.3 クライアントに固定 IP を配布する設定」のようにクライアントの MAC アドレスを設定します。
host	クライアント装置に固定の IP アドレスを配布する際に，割り当てる IP アドレスを指定します。本コマンドはハードウェアアドレスコマンドとセットで使用します。「6.2.3 クライアントに固定 IP を配布する設定」のようにクライアントが使用する IP アドレスを設定します。
ip dhcp dynamic-dns-update	IP アドレス配布時，ダイナミック DNS 連携を有効にするかどうかを設定します。「6.2.4 ダイナミック DNS 連携時の設定」のようにダイナミック DNS 連携を有効にするために設定します。
ip dhcp excluded-address	network コマンドで指定した IP アドレスプールのうち，配布対象から除外とする IP アドレスの範囲を指定します。「6.2.2 クライアントに IP を配布する設定」のようにネットワークのアドレス範囲のうち，クライアントへの配布から除外する IP アドレスを設定します。
ip dhcp key	ダイナミック DNS 使用時，DNS サーバとの認証で使用する認証キーを設定します。
ip dhcp pool	DHCP アドレスプール情報を設定します。
ip dhcp zone	ダイナミック DNS 使用時，DNS 更新を行うゾーンの情報を設定します。「6.2.4 ダイナミック DNS 連携時の設定」ように連携を行うドメインのゾーン情報を設定します。
lease	クライアントに配布する IP アドレスのデフォルトリース時間を指定します。「6.2.2 クライアントに IP を配布する設定」のようにクライアントが使用する IP アドレスのリース時間を設定します。

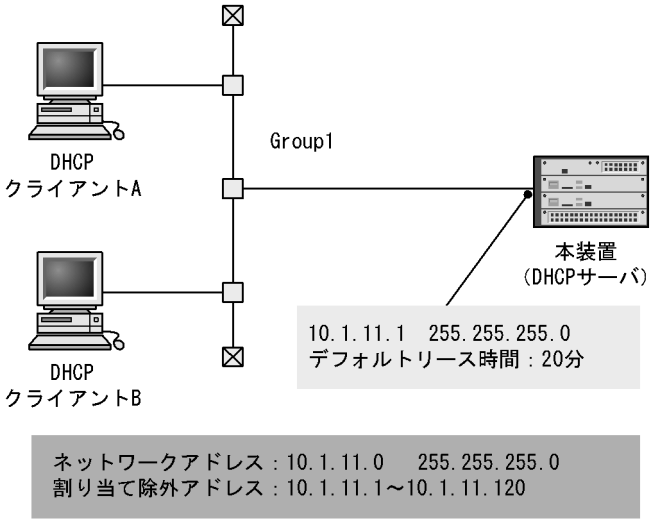
コマンド名	説明
max-lease	クライアントがリース時間を指定して IP アドレスを要求した際に，許容する最大リース時間を指定します。
netbios-name-server	クライアントに配布する NetBIOS ネームサーバオプションを指定します。NetBIOS ネームサーバオプションは，クライアントで利用可能な NetBIOS ネームサーバ（NBNS//WINS サーバ）の IP アドレスリストです。
netbios-node-type	クライアントに配布する NetBIOS ノードタイプオプションを指定します。NetBIOS ノードタイプオプションは，クライアントが NetBIOS オーバー TCP/IP での名前解決を行う方法を指定します。
network	DHCP によって動的に IP アドレスを配布するネットワークのサブネットを指定します。実際に DHCP アドレスプールとして登録されるのはサブネットのうち，IP アドレスホスト部のビットがすべて 0，およびすべて 1 のアドレスを除いたものです。「6.2.2　クライアントに IP を配布する設定」のように DHCP によって IP アドレスを配布するネットワークを設定します。
service dhcp	DHCP サーバを有効にするインタフェースを指定します。 本設定を行ったインタフェースでだけ DHCP パケットを受信します。「6.2.2　クライアントに IP を配布する設定」のように DHCP クライアントが接続されている VLAN インタフェースを設定します。

6.2.2 クライアントに IP を配布する設定

[設定のポイント]

DHCP クライアントへ割り当てをしたくない IP アドレスを割り当て除外アドレスに設定します。また，DHCP クライアントに対して IP アドレスを動的に配布するための DHCP アドレスプールを設定します。

図 6-1　クライアントーサーバ構成（動的 IP アドレス配布時）



[コマンドによる設定]

1. **(config)# interface vlan 10**
   (config-if)# ip address 10.1.11.1 255.255.255.0
   (config-if)# exit
   あらかじめ VLAN インタフェースと IP アドレスを設定しておきます。

2. **(config)# service dhcp vlan 10**
   DHCP サーバを有効にする VLAN インタフェース名称を指定します。

3. **(config)# ip dhcp excluded-address 10.1.11.1 10.1.11.120**
   DHCP サーバが DHCP クライアントに割り当てから除外する IP アドレスを設定します。

4. **(config)# ip dhcp pool Group1**
   DHCP アドレスプールを設定します。
   DHCP コンフィグレーションモードへ移行します。

5. **(dhcp-config)# network 10.1.11.0 255.255.255.0**
   DHCP アドレスプールのネットワークアドレスを設定します。

6. **(dhcp-config)# lease 0 0 20**
   DHCP アドレスプールのデフォルトリース時間に 20 分を設定します。

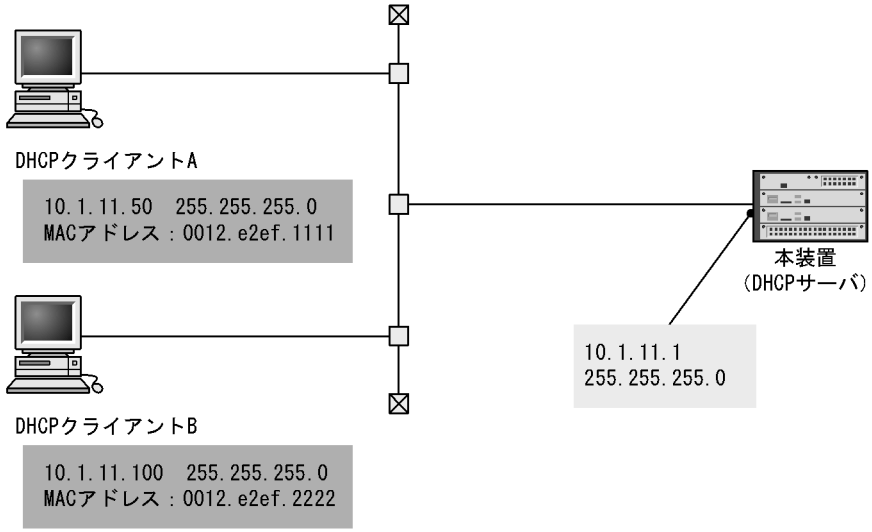
7. **(dhcp-config)# default-router 10.1.11.1**
   サブネット上にあるルータの IP アドレスを設定します。

6.2.3 クライアントに固定 IP を配布する設定

[設定のポイント]

DHCP クライアントごとに IP アドレスを固定で配布するために，クライアントごとに IP アドレスと MAC アドレスを設定します。

図 6-2 クライアントーサーバ構成（固定 IP アドレス配布時）



[コマンドによる設定]

1. **(config)# interface vlan 10**
   (config-if)# ip address 10.1.11.1 255.255.255.0
   (config-if)# exit

あらかじめ VLAN インタフェースと IP アドレスを設定しておきます。

2. **(config)# service dhcp vlan 10**
   DHCP サーバを有効にする VLAN インタフェース名称を指定します。

3. **(config)# ip dhcp pool Client1**
   DHCP クライアント A のアドレスプール名称を設定します。
   DHCP コンフィグレーションモードへ移行します。

4. **(dhcp-config)# host 10.1.11.50 255.255.255.0**
   DHCP クライアント A のアドレスプールに対する固定 IP アドレスを設定します。

5. **(dhcp-config)# hardware-address 0012.e2ef.1111 ethernet**
   DHCP クライアント A の DHCP アドレスプールに対する MAC アドレスを設定します。

6. **(dhcp-config)# default-router 10.1.11.1**
   (dhcp-config)# exit
   サブネット上のルータ IP アドレスを設定します。

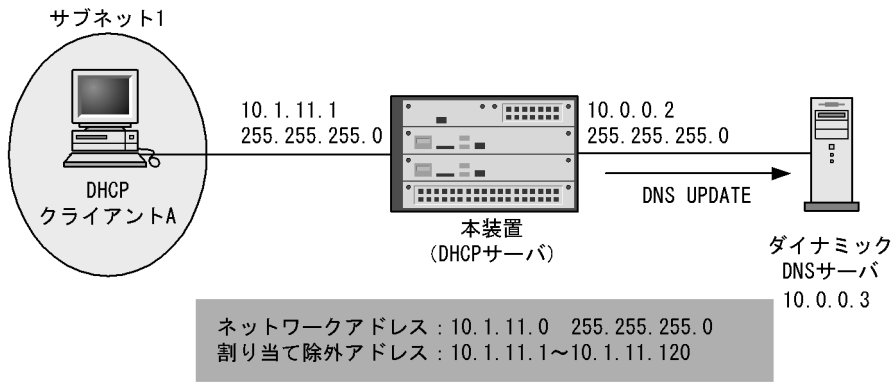
7. **(config)# ip dhcp pool Client2**
   (dhcp-config)# host 10.1.11.100 255.255.255.0
   (dhcp-config)# hardware-address 0012.e2ef.2222 ethernet
   (dhcp-config)# default-router 10.1.11.1
   項番 3 から 6 と同様に，DHCP クライアント B にもアドレスプール名称，固定 IP アドレス，MAC アドレスを設定します。

6.2.4 ダイナミック DNS 連携時の設定

[設定のポイント]

クライアントに対して IP アドレスを配布した際に，クライアントに対応する DNS レコードをダイナミック DNS サーバに通知できるように，ゾーン情報の設定とダイナミック DNS サーバ連携を有効にします。

図 6-3 ダイナミック DNS 連携をする場合の接続構成



[コマンドによる設定]

1. **(config)# interface vlan 10**
   (config-if)# ip address 10.1.11.1 255.255.255.0
   (config-if)# exit
   あらかじめサブネット 1 の VLAN インタフェースと IP アドレスを設定しておきます。

2. **(config)# interface vlan 20**
   (config-if)# ip address 10.0.0.2 255.255.255.0
   (config-if)# exit
   項番 1 と同様に，あらかじめダイナミック DNS サーバの VLAN インタフェースと IP アドレスを設定しておきます。

3. **(config)# service dhcp vlan 10**
   (config)# ip dhcp excluded-address 10.1.11.1 10.1.11.120
   (config)# ip dhcp pool Group1
   (dhcp-config)# network 10.1.11.0 255.255.255.0
   (dhcp-config)# default-router 10.1.11.1
   「6.2.2　クライアントに IP を配布する設定」と同様に IP アドレスを設定します。

4. **(dhcp-config)# domain-name example.net**
   ドメインネームシステムでホスト名称を解決しているときに，クライアントが使うべきドメインネームを設定します。

5. **(dhcp-config)# dns-server 10.0.0.3**
   クライアントが利用可能な DNS サーバの IP アドレスを設定します。

6. **(dhcp-config)# exit**
   DHCP コンフィグレーションモードからグローバルコンフィグレーションモードへ移行します。

7. **(config)# ip dhcp zone example.net. primary 10.0.0.3**
   正引きドメイン example.net. に対するゾーン情報を設定し，ダイナミック DNS サーバに 10.0.0.3 を設定します。

8. **(config)# ip dhcp zone 11.1.10.in-addr.arpa. primary 10.0.0.3**
   逆引きドメイン 11.1.10.in-addr.arpa. に対するゾーン情報を設定し，ダイナミック DNS サーバに 10.0.0.3 を設定します。

9. **(config)# ip dhcp dynamic-dns-update**
   ダイナミック DNS 連携を有効にします。

6.3 オペレーション

6.3.1 運用コマンド一覧

DHCP サーバの運用コマンド一覧を次の表に示します。

表 6-4 運用コマンド一覧

コマンド名	説明
show ip dhcp binding	DHCP サーバ上の結合情報を表示します。
clear ip dhcp binding	DHCP サーバのデータベースから結合情報を削除します。
show ip dhcp import	DHCP サーバのコンフィグレーションで設定されたオプション / パラメータ値を表示します。
show ip dhcp conflict	DHCP サーバによって検出した衝突 IP アドレス情報を表示します。衝突 IP アドレスとは，DHCP サーバのプール IP アドレスでは空きとなっていますが，すでにネットワーク上の端末に割り当てられている IP アドレスを指します。衝突 IP アドレスは，DHCP サーバが DHCP クライアントに対して IP アドレスを割り当てる前に ICMP パケット送出の応答有無によって検出します。
clear ip dhcp conflict	DHCP サーバから衝突 IP アドレス情報を取り除きます。
show ip dhcp server statistics	DHCP サーバの統計情報を表示します。
clear ip dhcp server statistics	DHCP サーバの統計情報をリセットします。
restart dhcp	DHCP サーバデーモンプロセスを再起動します。
dump protocols dhcp	DHCP サーバプログラムで採取しているサーバのログおよびパケットの送受信ログをファイルへ出力します。
dhcp server monitor	DHCP サーバで送受信するパケットの送受信ログの採取を開始します。
no dhcp server monitor	DHCP サーバプログラムでのパケットの送受信ログの採取を停止します。

6.3.2 割り当て可能な IP アドレス数の確認

クライアントに割り当て可能な IP アドレスの個数は，show ip dhcp server statistics コマンドの実行結果「address pools」で示されます。この数がクライアントに割り当てたい数よりも多いことを確認してください。

図 6-4 show ip dhcp server statistics コマンドの実行結果

```
> show ip dhcp server statistics
Date 2008/10/15 12:00:00 UTC
   < DHCP Server use statistics >
     address pools           :19
     automatic bindings      :170
     manual bindings         :1
     expired bindings        :3
     over pools request      :0
     discard packets         :0
   < Receive Packets >
     BOOTREQUEST             :0
     DHCPDISCOVER            :178
     DHCPREQUEST             :178
     DHCPDECLINE             :0
     DHCPRELEASE             :1
     DHCPINFORM              :0
   < Send Packets >
     BOOTREPLY               :0
     DHCPOFFER               :178
     DHCPACK                 :172
     DHCPNAK                 :6
>
```

6.3.3 配布した IP アドレスの確認

実際に DHCP クライアントへ割り当てられた IP アドレスについては，show ip dhcp binding コマンドを実行して確認してください。リースを満了していない IP アドレスが表示されます。

図 6-5 show ip dhcp binding コマンドの実行結果

```
> show ip dhcp binding
Date 2008/10/15 12:00:00 UTC
<IP address>      <MAC address>       <Lease expiration>   <Type>
10.1.11.1         0012.e2ef.1111      08/10/15 19:39:20    Automatic
10.1.11.50        0012.e2ef.2222                           Manual
>
```

7 IPv4 ルーティングプロトコル概要

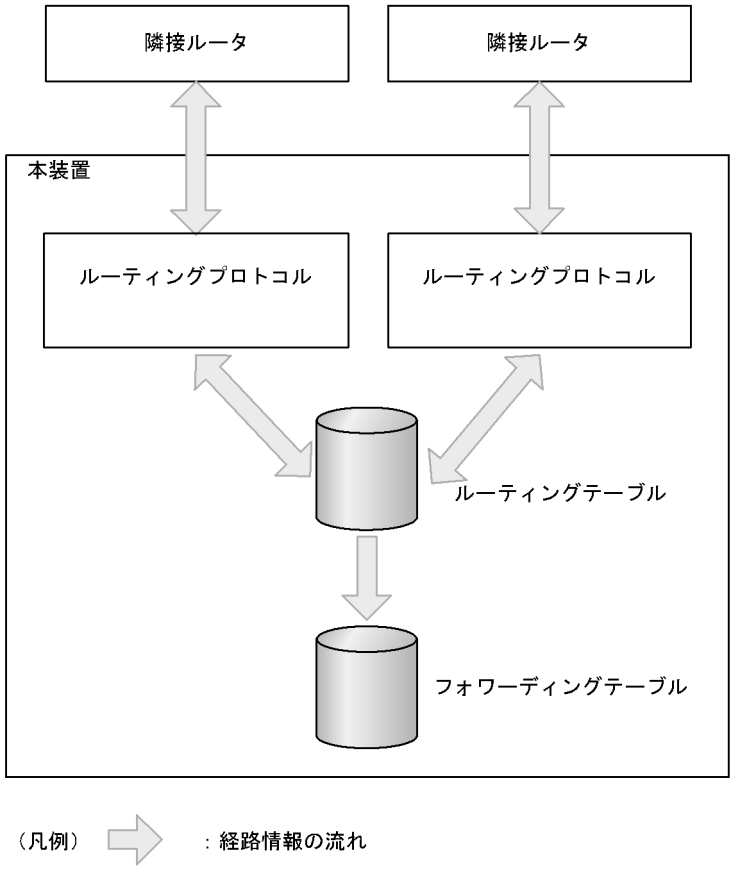
この章では，IPv4 のルーティングプロトコルの概要について説明します。

7.1 IPv4 ルーティング共通の解説

7.1.1 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 7-1 ルーティングの概要



7.1.2 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 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）をサポートしています。

7.1.3 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）を次の表に示します。

表 7-1 経路情報

経路情報		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。

7.1.4 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の表に示します。

表 7-2 ルーティングプロトコルごとの適用範囲

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	○	○	○	○	○

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
	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

7.1.5 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の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 7-3 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 の外部ピア学習経路	20
OSPF の AS 内経路	110
OSPF の AS 外経路	110

経路	デフォルトディスタンス値
RIP 経路	120
集約経路	130
BGP4 の内部ピア学習経路	200
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

(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，「13　経路フィルタリング（IPv4)」を参照してください。

(a) RIP 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。

(b) OSPF での経路広告

OSPF 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 OSPF ドメインに由来する複数の OSPF AS 内経路，または OSPF AS 外経路が存在することがあります。OSPF 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。OSPF AS 外経路および OSPF 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 OSPF ドメイン間で互いに経路を広告することはありません。OSPF AS 内経路や OSPF AS 外経路をほかの OSPF ドメインに AS 外経路として広告したい場合には，経路フィルタリングを設定してください。

(c) 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 BGP4 経路はほかの AS に広告されます。この場合，BGP4 以外のルーティングプロトコルで BGP4 経路と同一宛先経路が存在しても BGP4 で選択された最適な 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。

7.1.6 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 ClassA，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 ClassA，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。この項では 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

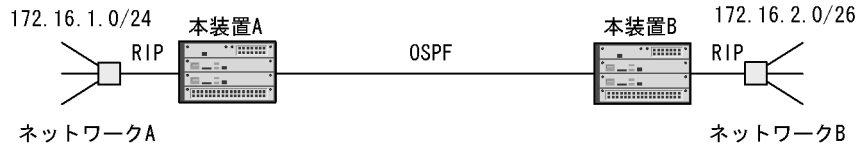
サブネッティングされたネットワークへの経路は次に示すどちらかの条件に当てはまる場合，該当する経路を RIP-1 で広告しないので注意してください。

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 7-2 異なるサブネットマスク長のサブネット間の接続

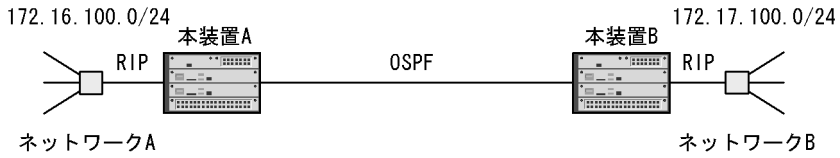


「図 7-5 サブネット間の接続の例」の本装置 A の場合，ネットワーク A とネットワーク B は同一ネットワーク内の同一サブネット長のサブネットのために経路を広告します。

● 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 7-3 異なるネットワークアドレスのサブネット間の接続



「図 7-5 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。

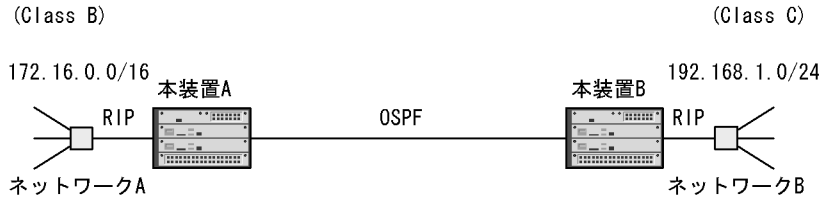
(b) OSPF による RIP のネットワーク間接続

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 7-4 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。

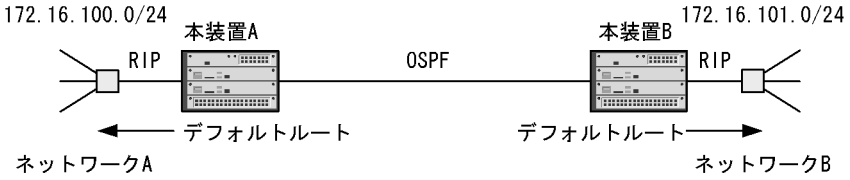
図 7-5 サブネット間の接続の例

● 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，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，OSPF 経路経由で相手のネットワークに配送されます。

図 7-6 デフォルトルートの広告の例

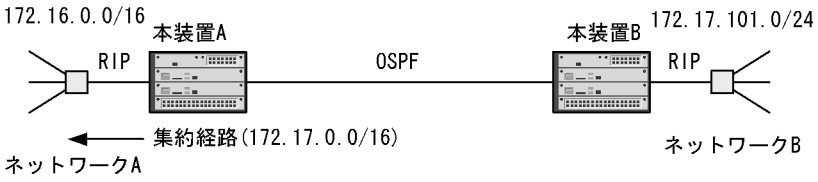


● 集約経路を広告する。

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，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，OSPF/OSPFASE 経路経由で相手のネットワークに配送されます。

図 7-7 集約経路の広告の例

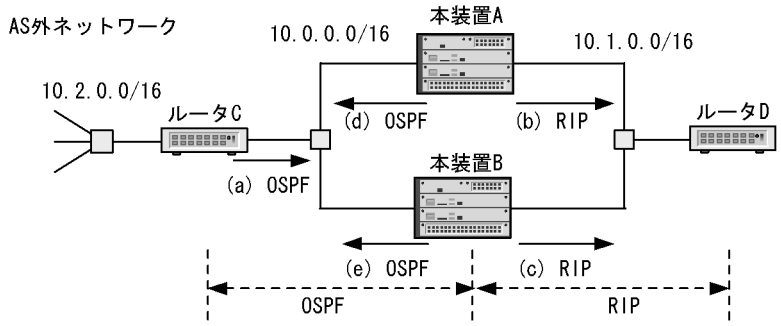


(2) 複数のプロトコルで同じ宛先の経路を学習する場合の注意事項

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，10.1.0.0 のネットワークでは RIP を使用しています。

図 7-8 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。

7.1.7 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・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 取得に時間がかかる場合があります。

7.2 IPv4 ルーティング共通のオペレーション

7.2.1 運用コマンド一覧

IPv4 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 7-4 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 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 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)(IPv4) ※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，通信可能であ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 processes cpu unicast ※3	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 ※3	ユニキャストルーティングプログラムを再起動します。
debug protocols unicast ※3	ユニキャストルーティングプログラムが出力するイベントログ情報の運用メッセージ表示を開始します。
no debug protocols unicast ※3	ユニキャストルーティングプログラムが出力するイベントログ情報の運用メッセージ表示を停止します。
dump protocols unicast ※3	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 ※3	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 9. ソフトウェアバージョンと装置状態の確認」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 8. IPv4・IPv6 ルーティングプロトコル共通」を参照してください。

7.2.2 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。

図 7-9 show ip route コマンドの表示例

```
> show ip route
Date 2006/03/14 12:00:00 UTC
Total: 13 routes
Destination        Next Hop        Interface      Metric   Protocol  Age
172.16/16          192.168.1.100   VLAN0010       2/0      RIP        8s …1
192.168.1/24       192.168.1.1     VLAN0010       0/0      Connected  8s
     :
     :
>
```

1. 宛先アドレスに対する経路が存在するかどうか確認してください。

7.3 ネットワーク設計の考え方

この節では，IPv4 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。

7.3.1 アドレス設計

ローカルアドレスを使用するときで IP 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（ClassA または ClassB）をサブネット化して使用し，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）。

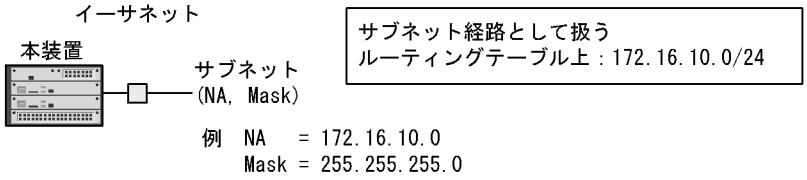
1. および 2. のアドレッシング条件に合わないで RIP-1 によるルーティングを行う場合は，経路広告条件に注意が必要です。

7.3.2 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。

直結経路の取り扱いについて次の図に示します。

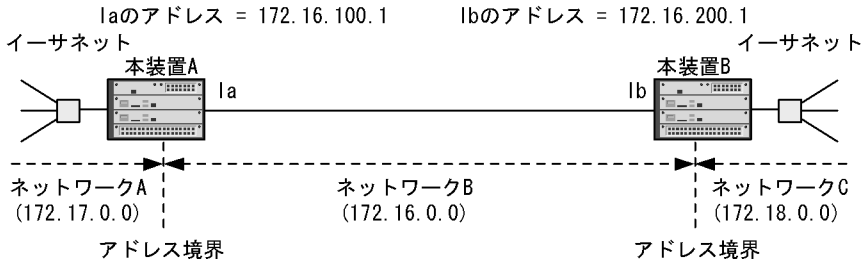
図 7-10 直結経路の取り扱い



7.3.3 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 7-11 通常のアドレス境界設計例



7.4　ロードバランスの解説

7.4.1　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 7-12　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）

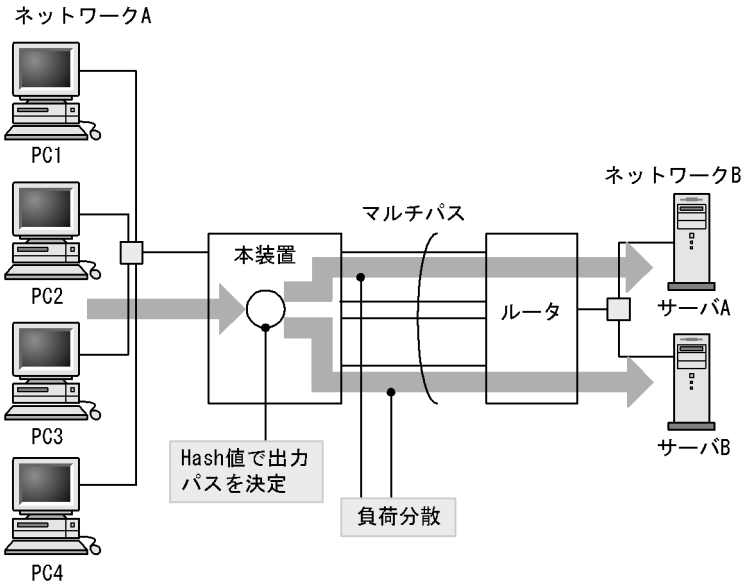
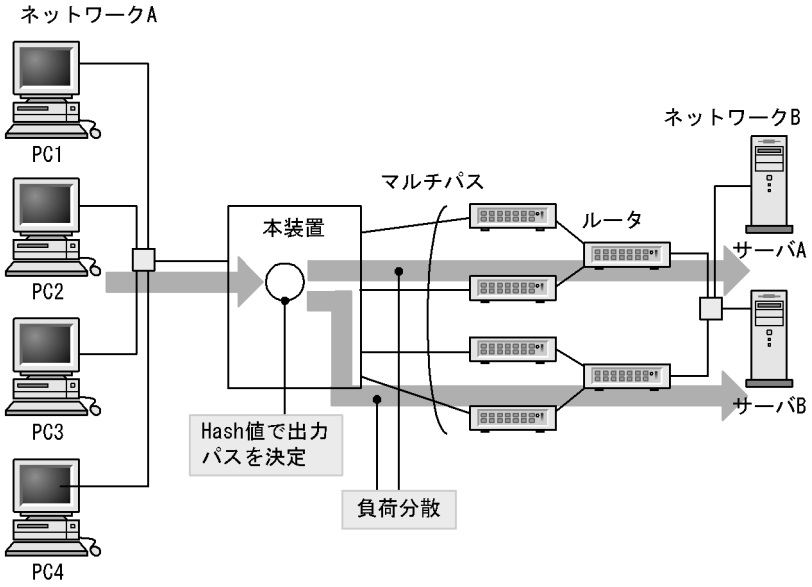


図 7-13　マルチパスを使用した負荷分散（隣接ルータが複数の場合）



7.4.2　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 7-5　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可能な最大マルチパス数	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。
マルチパスで生成できるルーティングプロトコル	• スタティック (IPv4) • OSPF • 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（IPv4）：6 • OSPF：4 • BGP4：1（マルチパスを生成しません）	－
接続構成	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 7-6 ロードバランス仕様

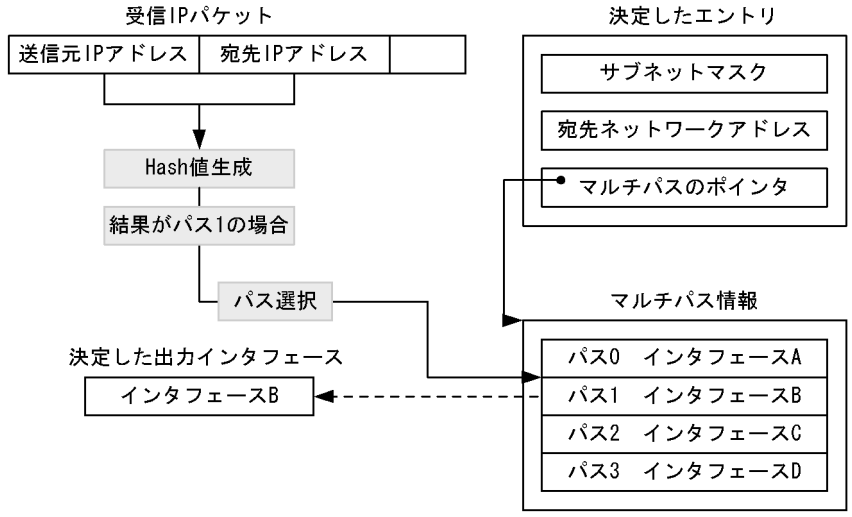
項目	仕様	備考
マルチパスの振り分け方法	宛先 IP アドレスと送信元 IP アドレスから 16 パスに振り分ける値（Hash 値）を算出し，決定した出力パスに振り分けます。宛先 IP アドレスと送信元 IP アドレスが同一のパケットは，同一出力パスを選択します。これによって，送信の順序性を保証します。	－
ルーティングテーブル内のマルチパス情報	ルーティングテーブルに設定する各出力インタフェースの hash の割り当て比率は，ほぼ均等になります。	「7.4.4 ロードバランス使用時の注意事項」の 1 および 2 を参照
各パスの重み付け	できません。	「7.4.4 ロードバランス使用時の注意事項」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

7.4.3 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，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 7-14 出力インタフェースの決定



7.4.4 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 16 パスの内 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，回線速度の速い回線に重み付けをするには，マルチホーム接続によってできますが，障害の発生などを考慮し，冗長構成と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出しようとした場合，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ないので，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。そのような場合，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 を設定してください。
6. 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 経路のマルチパスに Null インタフェースを含む場合，該当経路を使用して中継されないことがあります。そのような場合，BGP 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 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。**【OP-NPAR】**

7.5 ロードバランスのコンフィグレーション

7.5.1 スタティック経路を使用したロードバランス

「8.2.4 マルチパス経路の設定」を参照してください。

7.5.2 OSPF でのロードバランス

「10.2.6 マルチパスの設定」を参照してください。

7.5.3 BGP4 でのロードバランス【OP-BGP】

「12.5.3 BGP4 マルチパスのコンフィグレーション （2）BGP4 マルチパスの設定」を参照してください。

7.6 ロードバランスのオペレーション

7.6.1 選択パスの確認

(1) 経路情報の確認

show ip route コマンドを実行し，マルチパス経路の設定内容が正しく反映されているかどうかを確認してください。

図 7-15 マルチパスの経路情報表示

```
> show ip route
Date 2006/03/14 12:00:00 UTC
Total: 13 routes
Destination        Next Hop        Interface      Metric   Protocol  Age
192.168.1/24       192.168.1.1     VLAN0010       0/0      Connected 19m 46s
192.168.1.1/32     192.168.1.1     VLAN0010       0/0      Connected 19m 46s
192.168.2/24       192.168.2.1     VLAN0020       0/0      Connected 19m 46s
192.168.2.1/32     192.168.2.1     VLAN0020       0/0      Connected 19m 46s
192.168.3/24       192.168.3.1     VLAN0030       0/0      Connected 19m 46s
192.168.3.1/32     192.168.3.1     VLAN0030       0/0      Connected 19m 46s
172.16/16          192.168.1.200   VLAN0010       0/0      Static     9s
                   192.168.2.200   VLAN0020       -        -         -
                   192.168.3.200   VLAN0030       -        -         -
     :
     :
>
```

(2) 当該宛先アドレスとの通信可否を確認する

ロードバランスで使用する本装置のインタフェースについて，通信相手となる装置に対して通信できるかどうかを，ping <IPv4 Address> specific-route source <Source Address> コマンドを実行して確認してください。ping コマンドの <Source Address> には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IPv4 アドレスを指定してください。

7.7 経路集約の解説

7.7.1 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，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するなどです。

経路集約の指定はコンフィグレーションコマンド ip 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。

7.7.2 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無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。

7.7.3 AS_PATH 属性の集約

BGP4 経路が集約元経路に含まれる場合は集約した経路に BGP4 経路のパス属性を付加します。集約元の 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 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

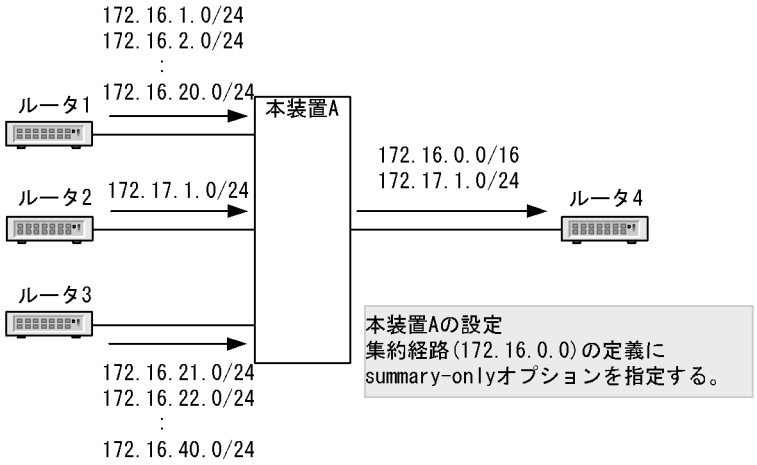
集約元となる BGP4 経路が持つすべてコミュニティを，集約した経路の COMMUNITIES 属性に設定します。

7.7.4 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。

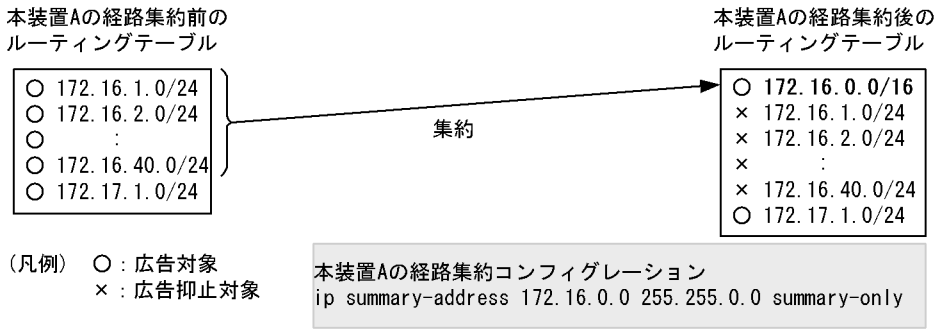
集約元経路の広告抑止は集約経路単位または全集約経路に対して指定できます。集約経路単位に指定する場合は，コンフィグレーションコマンド ip summary-address の summary-only パラメータで指定します。集約元経路の広告抑止の適用例を次の図に示します。

図 7-16 集約元経路の広告抑止の適用例



本装置 A は，ルータ 1 より 172.16.1.0/24，172.16.2.0/24，…，172.16.20.0/24 を受信し，ルータ 2 より 172.17.1.0/24 を受信し，ルータ 3 より 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 7-17 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



7.8 経路集約のコンフィグレーション

7.8.1 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 7-7 コンフィグレーションコマンド一覧

コマンド名	説明
ip summary-address	IPv4 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（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（RIP）※	RIP から広告する経路のプロトコル種別を設定します。

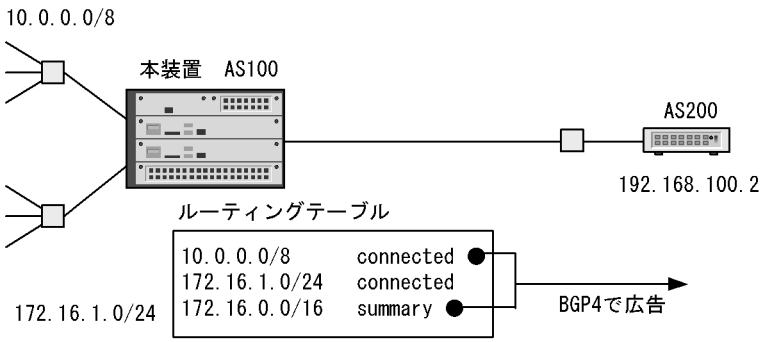
注※

「コンフィグレーションコマンドレファレンス Vol.3　14. 経路フィルタリング（IPv4 ／ IPv6 共通）」を参照してください。

7.8.2 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 7-18 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 を生成する設定を行います。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 接続を行う設定をします。

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。

7.9 経路集約のオペレーション

7.9.1 運用コマンド一覧

経路集約の運用コマンド一覧〔IPv4〕を次の表に示します。

表 7-8 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	BGP プロトコルに関する情報を表示します。
restart unicast ※	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 ※	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 ※	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※

「運用コマンドレファレンス Vol.3 8. IPv4・IPv6 ルーティングプロトコル共通」を参照してください。

7.9.2 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。集約経路の表示例を次の図に示します。

図 7-19 集約経路の表示例

```
> show ip route summary_routes
Date 2006/03/14 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。アクティブ経路の表示例を次の図に示します。

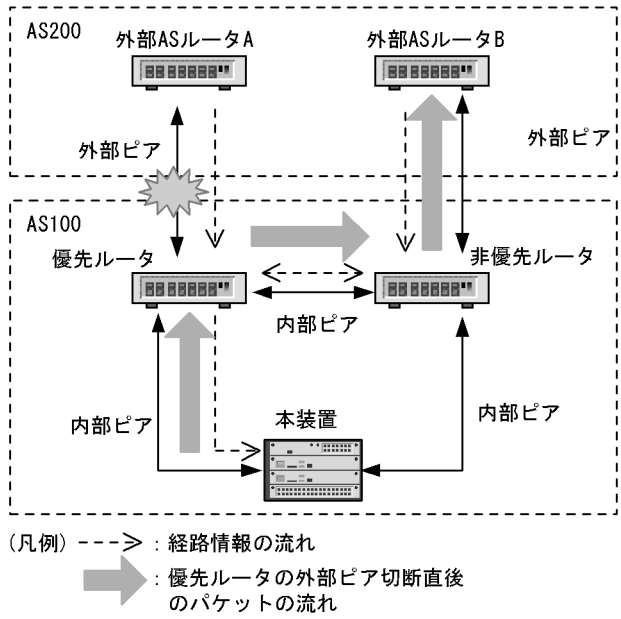
図 7-20 アクティブ経路の表示例

```
> show ip route 172.16.0.0/16 longer-prefixes
Date 2006/03/14 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      VLAN0010       0/0      Connected 365d
172.16.1.1/32      172.16.1.1      VLAN0010       0/0      Connected 365d
```

7.10　経路削除保留機能

経路削除保留機能は，ルーティングプロトコルが無効にした経路を，ルーティングテーブルから一定時間削除しないようにすることで，新しく代替経路が生成されるまでの間，既存経路によってフォワーディングを維持する機能です。経路削除保留機能の適用例を次の図に示します。

図 7-21　経路削除保留機能の適用例



上図で優先ルータと外部 AS ルータ A 間のピア切断によって，本装置の BGP4 経路は非優先ルータから再学習するまでの間，一時的に無効となりますが，経路削除保留機能を適用しているためルーティングテーブルからは経路情報が削除されず，次の経路でパケットフォワーディングが維持されます。

[優先ルータ→非優先ルータ→外部 AS ルータ B]

コンフィグレーションコマンド routing options delete-delay で設定する経路削除保留タイマ値として，5 ～ 4294967295（秒）の範囲の数値を指定した場合に，本機能が適用されます。

7.11 グレースフル・リスタートの概要

7.11.1 概要

グレースフル・リスタートは，装置が系切替したときや，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停止時間を短縮するための機能です。

7.11.2 グレースフル・リスタートを使用しない場合の問題

本装置では，装置が系切替したときや，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，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。

7.11.3 グレースフル・リスタートによる解決方法

グレースフル・リスタートは，上記問題を解決することによってルーティングプログラム交替時の通信停止時間を短縮する機能です。次に具体的な解決方法を示します。

- 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・経路広告の処理順序を固定します。グレースフル・リスタートをするに当たり，まず隣接ルータから経路情報を学習し，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。

次の図と表に，本装置のグレースフル・リスタート動作手順を示します

図 7-22 グレースフル・リスタート手順

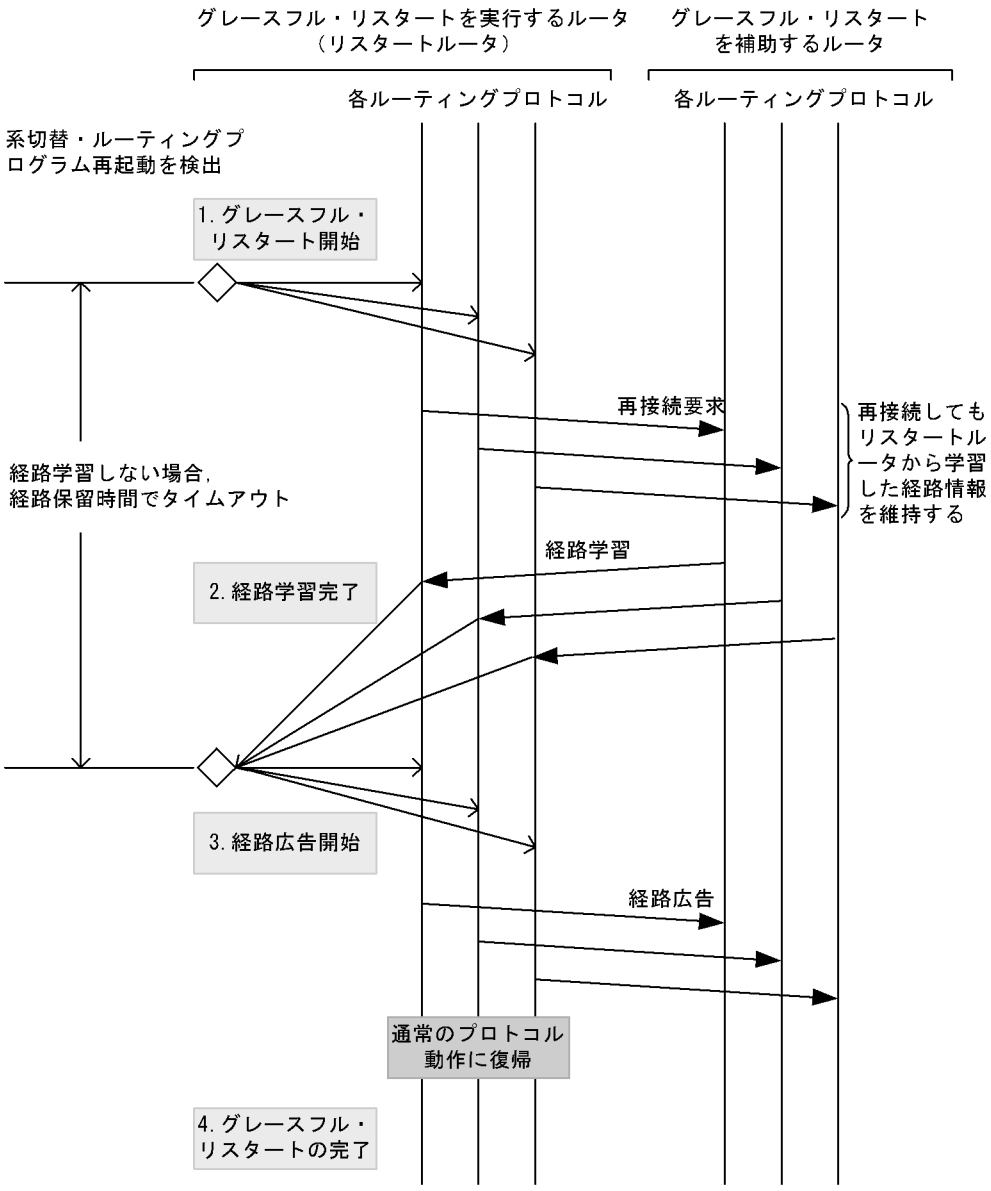


表 7-9 グレースフル・リスタート手順

手順	動作
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・リスタートによる再接続を行い，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。**【OP-NPAR】** • 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

手順	動作
4	各プロトコルは，経路広告を完了したら通常のプロトコル動作に復帰します。 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。

7.11.4 グレースフル・リスタートのサポート範囲

グレースフル・リスタート機能のサポート範囲を次の表に示します。

表 7-10 グレースフル・リスタート機能のサポート範囲

項目		サポート
対象イベント	装置再起動	×
	装置系切替	○※1
	ユニキャストルーティングプログラム再起動	○※1
対象インタフェース	VLAN インタフェース	○※2※3
	マネージメントポート	×
対象フォワーディング・パケット	IPv4 ユニキャスト	○※4※5
	IPv6 ユニキャスト	○※4※5
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

注※1

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には，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。

注※2

スパニングツリーを使用する VLAN を除きます。

注※3

LACP を使用するリンクアグリゲーションを使用する場合を除きます。

注※4

ソフトウェアによるフォワーディング・パケットを除きます。

・装置内でフラグメント化が必要なパケット

・オプション付きパケット

注※5

グレースフル・リスタート以外のサービス機能の中断により中継不可となるケースを除きます。例えば，次のケースがあります。

・DHCP のサービス中断

・ARP/NDP の応答中断

7.11.5 設定可能なコンフィグレーション

本装置では，装置全体で設定するグレースフル・リスタート時の経路保留時間と，各プロトコルで設定するグレースフル・リスタート機能およびグレースフル・リスタート補助機能があります。また，グレースフル・リスタート機能とグレースフル・リスタート補助機能を同時に設定することもできます。

7.11.6 関連するマニュアル記載事項

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ご確認ください。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 ：「11.5 グレースフル・リスタートの解説」
- BGP4 ：「12.4.11 グレースフル・リスタート」
- OSPFv3 ：「28.3 グレースフル・リスタートの解説」
- BGP4+ ：「29.4.11 グレースフル・リスタート」

7.11.7 使用上の注意事項

1. 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を，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，OSPFv3：25 秒
   BGP4，BGP4+ ：100 秒
2. 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 7-11 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）
250	55
1000	80
2000	145
3000	205
4000	300

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，DHCP サーバ，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。

3. 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。
4. OSPF・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和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。
5. BGP4・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かかる時間の和よりも長くしてください。これは，BGP4・BGP4+ ピアのコネクションを確立するためには，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，BGP4+ で直接接続されていない内部ピア接続により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，BGP4・BGP4+ のリスタート時間を，OSPF・OSPFv3 のリスタート時間とピアのコネクション確立にかかる時間の和よりも長くしてください。これは，BGP4・BGP4+ ピアのコネクションを確立するためには，ピアアドレスを解決する IGP がグレースフル・リスタートにより経路を学習しておく必要があるためです。
6. 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，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）の削除が実行されるので，通信が停止します。また，BGP4 と BGP4+ では，リスタート時間が BGP コネクションの再確立を待つ時間の上限となるので，再確立が最も遅い場合は，リスタート時間後に BGP4 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 と 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 BGP4 ピア数に依存します。

7. 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。
8. 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。
9. 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。
10. 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。

7.12 高速経路切替機能

7.12.1 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 7-12 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 経路の NextHop 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 経路の NextHop 変更	第 2 優先経路への切り替え
	マルチパス経路の縮退

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 7-13 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					
		BGP4	OSPF	RIP	スタティック※	集約経路	直結経路
第 2 優先経路	BGP4	○	○	○	○	×	×
	OSPF	○	－	○	○	×	×
	RIP	○	○	○	○	×	×
	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 のパラメータとして次を指定した場合
   - reject
   - noinstall
2. コンフィグレーションコマンド ip route のインタフェースとして次を指定した場合
   - Null インタフェース
   - ループバックインタフェース

・マネージメントポート

7.12.2 使用上の注意事項

第 2 優先経路のネクストホップが ARP 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 BGP4 や OSPF など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 によって動的にアドレス解決が行わ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，ネクストホップの動的なアドレス解決が行われないため，スタティック ARP の設定などの措置が必要となります。

7.13 VRF の解説【OP-NPAR】

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，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。

7.13.1 サポート範囲

VRF でサポートする IPv4 ルーティングプロトコルの機能を次の表に示します。

表 7-14 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	○
	OSPF	○
	BGP4	○
マルチパス／ロードバランス		○※
経路集約		○
経路削除保留機能		○
グレースフル・リスタート		○
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	○
	ポリシーベースルーティング	○

（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。

7.13.2 経路数の制限

VRF 単位で，収容する経路数を制限できます。

(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，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) 警告メッセージの出力

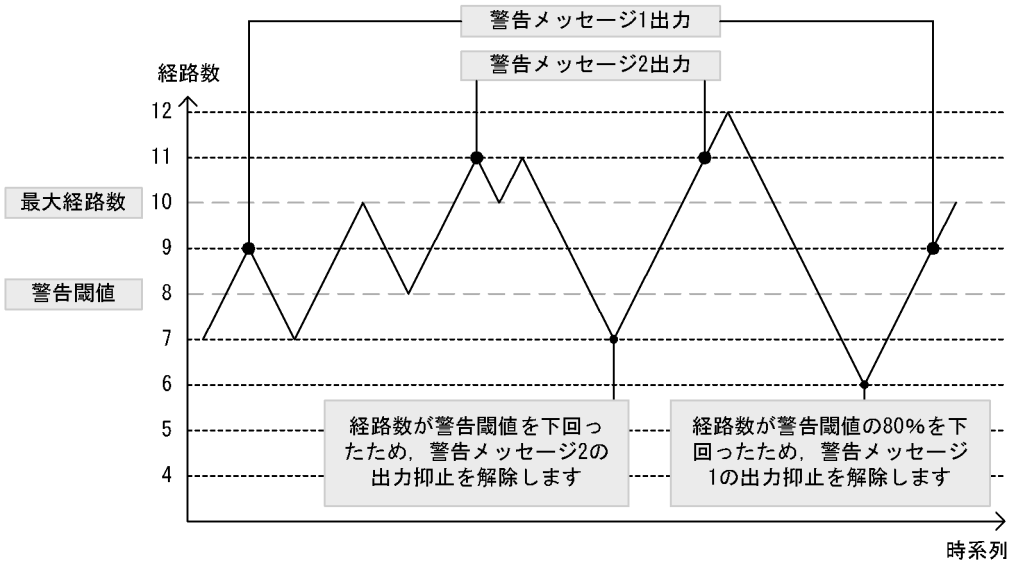
VRF ごとの経路数が指定した警告閾値および最大経路数を超過した場合，警告メッセージを出力します。

警告閾値を超過したときの警告メッセージ（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警告メッセージ（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。

経路数と警告メッセージ出力の関係を次の図に示します。

図 7-23　経路数と警告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 を実行してください。

7.13.3　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三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
- ポリシーベースルーティング

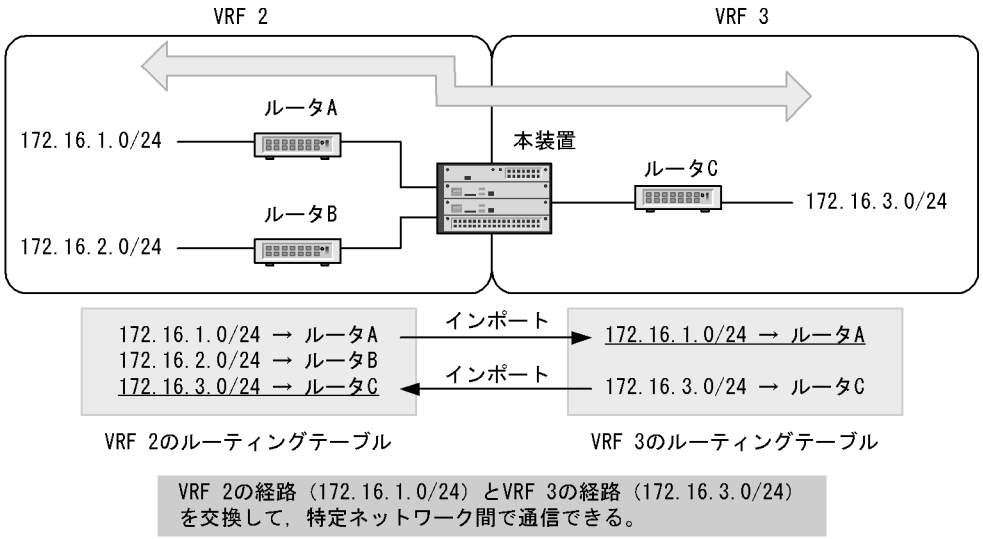
ここでは，ルーティングテーブルを操作する VRF 間の経路交換，および VRF 間にわたるスタティックルーティングについて説明します。また，VRF 間でインポートできる経路について説明します。

（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 7-24 VRF 間の経路交換

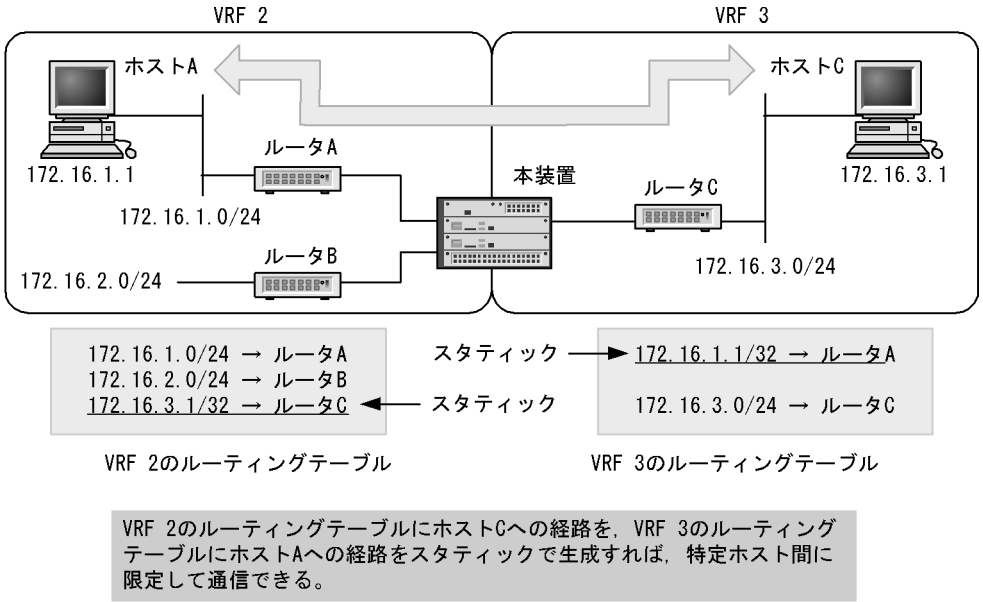


(2) VRF 間にわたるスタティックルーティング

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 7-25 VRF 間にわたるスタティックルーティング



(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。

表 7-15 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

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	○
loopback インタフェースで設定した IPv4 装置アドレスの経路	○
VLAN 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 VLAN インタフェースとなる経路	○
出力インタフェースが loopback 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	×
出力インタフェースが Null 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

なお，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。

7.14 VRF のコンフィグレーション【OP-NPAR】

7.14.1 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 7-16 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 ※1	IPv4 スタティック経路を生成します。
match vrf ※2	route-map に VRF によるフィルタ条件を設定します。
route-map ※2	route-map を設定します。
import inter-vrf ※3	他 VRF またはグローバルネットワークからの経路インポートをフィルタに従って制御します。
maximum routes ※3	VRF の最大経路数と警告の運用メッセージ出力閾値を設定します。
vrf definition ※3	VRF 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 10. 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 14. 経路フィルタリング（IPv4 ／ IPv6 共通）」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 30. VRF【OP-NPAR】」を参照してください。

7.14.2 最大経路数の設定

VRF の最大経路数と警告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，最大経路数と警告メッセージ出力の閾値を設定します。

[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 で収容できる最大経路数として 1000 を設定します。また，警告メッセージを出力する閾値を 80%に設定します。

7.14.3 エクストラネットの設定

エクストラネットの設定については，「8.2.7 VRF 間にわたるスタティック経路の設定【OP-NPAR】」，および「13.2.8 エクストラネット【OP-NPAR】」を参照してください。

7.15 VRF のオペレーション【OP-NPAR】

7.15.1 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 7-17 運用コマンド一覧

コマンド名	説明
show ip vrf	VRF の IPv4 情報を表示します。
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 static	スタティック経路に関する情報を表示します。

7.15.2 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。

図 7-26 show ip vrf コマンドの実行結果

```
> show ip vrf 2
Date 2008/12/20 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 7-27 show ip vrf detail コマンドの実行結果

```
> show ip vrf 2 detail
Date 2008/12/20 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
VLAN0010       192.168.10.1/24    192.168.10.255  Up
loopback2      2.2.2.2/32         2.2.2.2         Up
loopback2      127.0.0.1/8        127.0.0.1       Up
>
```

1. 最大経路数，警告メッセージ出力の閾値，現在の経路数の順に表示します。

7.15.3 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，「13.3.10 エクストラネットの確認【OP-NPAR】」を参照してください。

8 スタティックルーティング（IPv4）

この章では，IPv4 のスタティックルーティングについて説明します。

8.1 解説

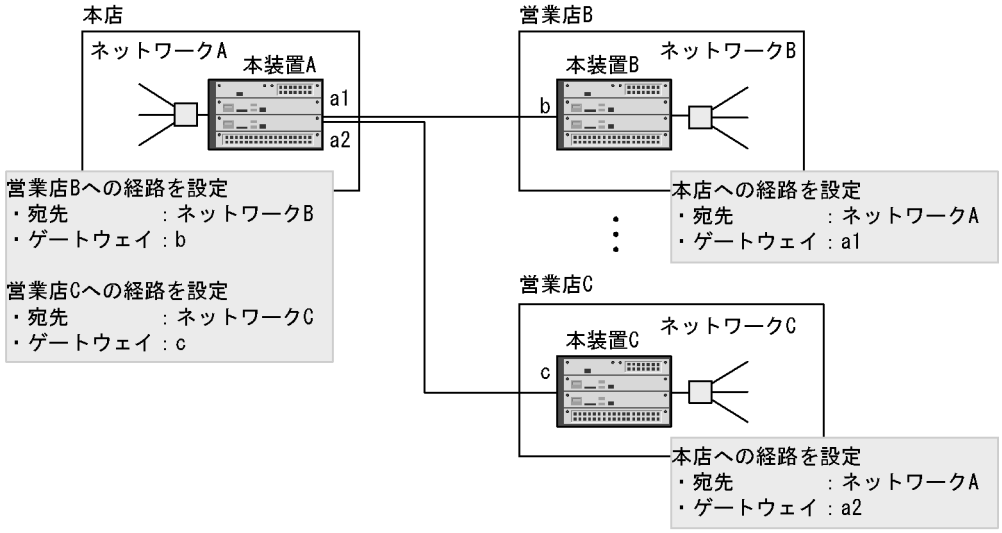
8.1.1 概要

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，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の通信はできません。

図 8-1 スタティックルーティングのネットワーク構成例



8.1.2 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分けし，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い，複数の経路が選択され，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 6 ですが，コンフィグレーションコマンドの ip route static maximum-paths で変更できます。

表 8-1 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。

8.1.3 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，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・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・削除を制御します。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 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ぶことができます。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せずに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）により，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せずに 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違い，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「3　Null インタフェース（IPv4）」を参照してください。

8.1.4 動的監視機能

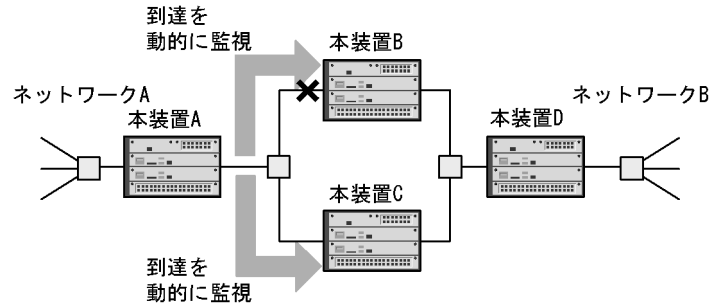
スタティック経路は，ゲートウェイと直接接続されたインタフェースの状態またはゲートウェイへの経路の有無によって，経路の生成・削除を制御します。したがって，経路が生成されている場合でも，該当するゲートウェイへの到達保証はありません。本装置は，生成されたスタティック経路のゲートウェイに対する，ICMPv4 のエコー要求およびエコー応答メッセージを使用した周期的なポーリングによって，到達性を動的に監視する機能を持ちます。この機能を使用することによって，「8.1.3　スタティック経路の中継経路指定」の経路生成・削除条件に加え，該当するゲートウェイへの到達性が確保できている場合だけ，スタティック経路を生成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 8-2 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。動的監視を行っていない状態で，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。これによって，本装置 C 経由のスタティック経路への切り替えが行われないで，本装置 A －ネットワーク B 間の通信が停止します。

動的監視を行っていると，本装置 A 側のインタフェースが正常である場合でも，動的監視機能によって本装置 B への到達不可を検知し，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の切り替えが行われ，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

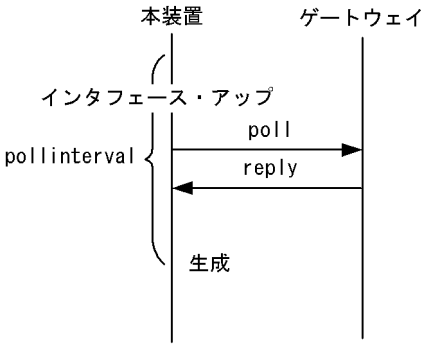
スタティック経路の動的監視による経路の生成，削除および再生成タイミングはコンフィグレーションコマンドの ip route static poll-interval および ip route static poll-multiplier の設定値に依存します。

以降，ip route static poll-interval の設定値を pollinterval，および ip 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 8-3 スタティック経路の動的監視による経路生成

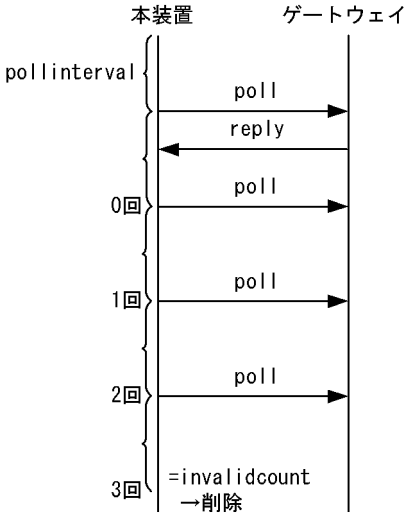


(b) 経路削除タイミング

pollinterval 周期でのポーリングに対し，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。

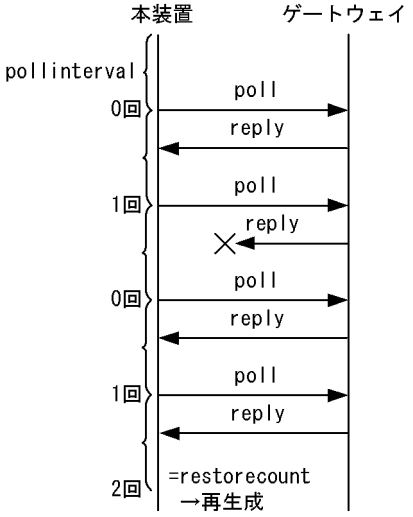
図 8-4 スタティック経路の動的監視による経路削除（invalidcount=3 の場合）



(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，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 8-5 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）



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

スタティックルーティング（IPv4）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 8-2 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	ポーリング間隔時間を指定します。
ip route static poll-multiplier	ポーリング回数，連続応答回数を指定します。

8.2.2 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。

[設定のポイント]

スタティック経路の設定は 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。

8.2.3 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。

[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。本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。

8.2.4 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。

[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ことで，マルチパスを構築できます。

[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。

8.2.5 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・生成のタイミングを調整したあとに，スタティック経路に動的監視機能を適用します。

[設定のポイント]

ポーリング間隔と回数の設定は 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。

8.2.6 VRF でのスタティック経路の設定【OP-NPAR】

VRF でスタティック経路を設定します。

[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。

8.2.7 VRF 間にわたるスタティック経路の設定【OP-NPAR】

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］

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。

8.3 オペレーション

8.3.1 運用コマンド一覧

スタティックルーティング（IPv4）の運用コマンド一覧を次の表に示します。

表 8-3 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 static	スタティック経路に関する情報を表示します。
clear ip static-gateway	スタティック経路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ポーリングをし，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。
restart unicast ※	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 ※	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 ※	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※

「運用コマンドレファレンス Vol.3　8. IPv4・IPv6 ルーティングプロトコル共通」を参照してください。

8.3.2 経路情報の確認

スタティック経路情報を確認します。

図 8-6 show ip static route の実行結果

```
> show ip static route
Date 2006/03/14 12:00:00 UTC
Status Codes: * valid, > active
   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]

1. 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。
2. 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 として「>」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。
3. Status Codes として「*」および「>」が表示されていない無効経路は，Status に何らかの障害要因が示されます。「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表し

ます。また，「UnReach」は，動的監視機能によって，到達性が確認されていないことを表します。

8.3.3 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確認します。

図 8-7 show ip static gateway の実行結果

```
> show ip static gateway
Date 2006/03/14 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］

1. 動的監視を行っ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。
2. 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。上記実行結果において，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。

9 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。

9.1 解説

9.1.1 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 9-1 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，ほかのルータからのリクエストに応答する場合と，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，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，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，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，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，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

なお，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。

9.1.2 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。経路選択の優先順位を次の表に示します。

表 9-2 経路選択の優先順位

優先順位	内容
高	メトリック値が最も小さい経路を選択します。
↑	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)。
	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。
↓	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。※
低	そのほかの場合，新しく学習した経路を無視します。

注※ 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。

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 9-3 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，次の表に従って同じ宛先への経路情報の優先度を決定します。

表 9-4　第 2 優先経路の登録を指定した場合の経路選択の優先順位

優先順位	内容
高	メトリック値が小さい経路を選択します。
↑	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）。
	ネクストホップアドレスが小さい経路を選択します。※ 1
	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。※ 2
↓	今まで第 1 優先であった経路を選択します。
低	そのほかの場合，新しく学習した経路を無視します。

注

ネクストホップアドレスが同じ場合は第 1 優先経路だけ生成します。

注※ 1

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。

注※ 2

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。

9.1.3　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 9-5　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 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

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
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

次の表に RIP で広告対象のアドレス種別を示します。

表 9-6 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
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「9.1.5　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，経路情報の広告が行われます。また，コンフィグレーションコマンドneighborの設定によって，特定の隣接ルータにだけ広告を限定することができます。次の表にRIPにおける経路情報の広告先を示します。

表9-7　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，広告が抑止されます。
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。

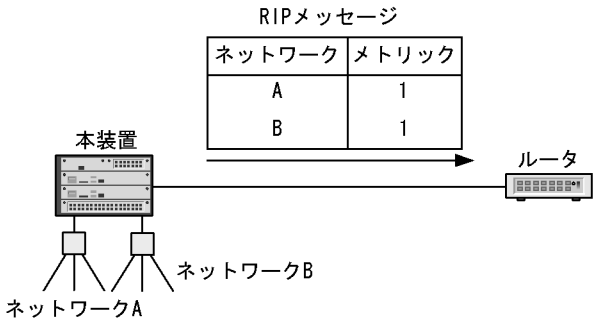
表9-8　経路広告タイミング

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

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 9-1　周期的な経路情報広告

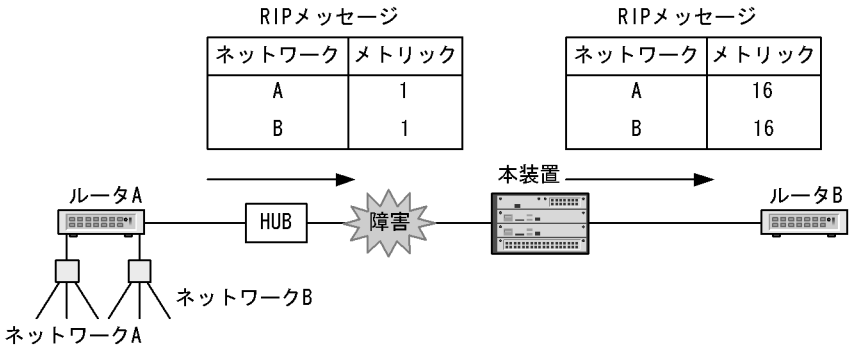


本装置は，ネットワークAおよびBに関する経路情報を30秒周期（周期広告タイマ）でルータに広告する。

(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 9-2　triggered update による経路情報の広告

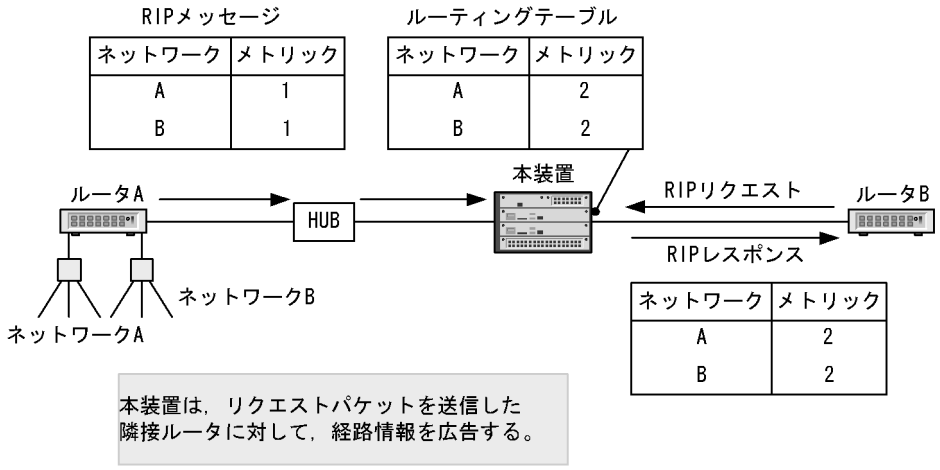


本装置はHUBと本装置間の障害を検出するとルーティングテーブルからネットワークAおよびBの経路情報を削除する。
同時にルータBに対してネットワークAおよびBの経路情報をメトリック16（到達不可）で広告する。

(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した際に，本パケットを送信した隣接ルータに対して経路情報を通知します。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 9-3　リクエストパケット受信による経路情報の広告

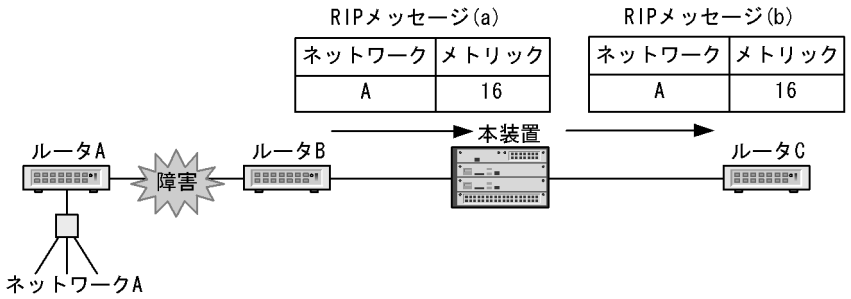


本装置は，リクエストパケットを送信した
隣接ルータに対して，経路情報を広告する。

(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。

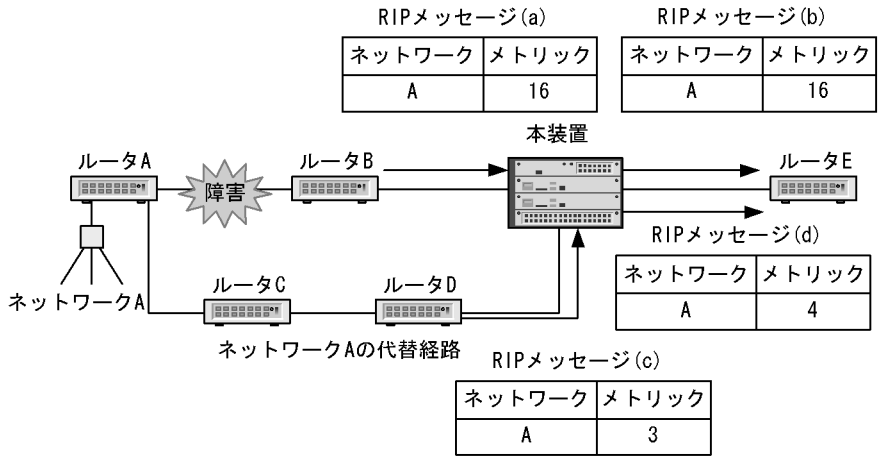
図 9-4　ルートポイズニング



(a) 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，ルーティングテーブルからネットワークAの経路情報を削除する。
(b) (a)を受信して即時に，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の経路情報を広告する。本装置は代替経路が存在しない場合は該当経路をメトリック16(到達不可)でルータCに広告する。

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 9-5　ルートポイズニング期間中の再学習



(a) 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，ルーティングテーブルからネットワークAの経路情報を削除する。
(b) 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の経路情報を広告する。
(c) 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，ルーティングテーブルに追加する(切り替え時間はルータDの周期広告時間による)。
(d) 本装置は，ルータEに対してネットワークAの経路情報を広告する。

(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。

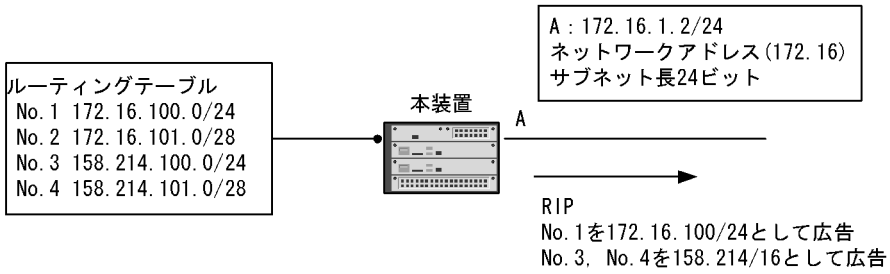
表 9-9　広告経路の自動集約対象となるアドレス種別

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，自動集約を行わず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 9-6　RIP-1 使用時の広告経路自動集約化」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，自動集約を行わず，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 9-7　RIP-2 使用時の広告経路自動集約化」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化を次の図に示します。

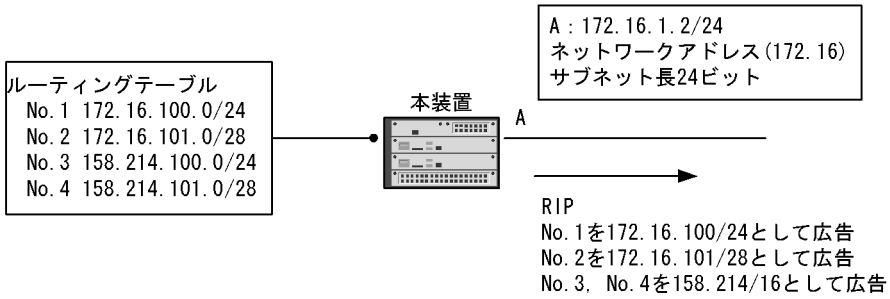
図 9-6 RIP-1 使用時の広告経路自動集約化



●ルーティングテーブル上の各経路情報の取り扱い
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，サブネット長も一致するため集約せずに広告する
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されない
No.3/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広告される

RIP-2 使用時のサブネット経路の自動集約化を次の図に示します。

図 9-7 RIP-2 使用時の広告経路自動集約化



●ルーティングテーブル上の各経路情報の取り扱い
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せずに広告する
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せずに広告する
No.3/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広告される

(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，一番小さなメトリック値を用いて広告されます。

(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。

9.1.4 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の 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。

(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。

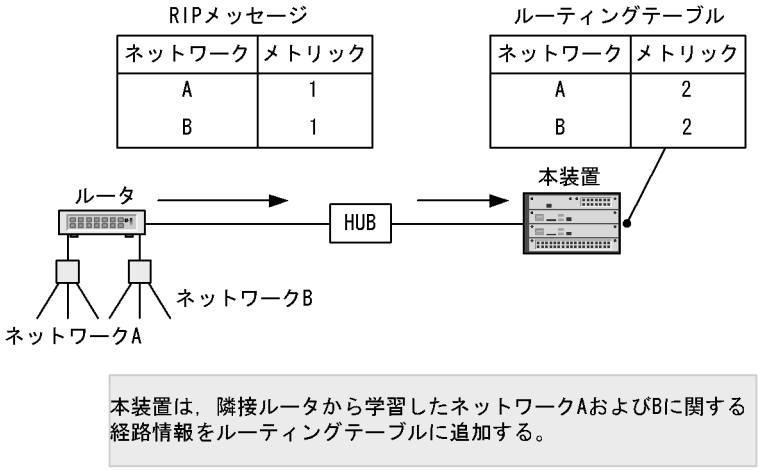
表 9-10　経路情報の学習・切り替えのタイミング

機能	内容
隣接ルータからのレスポンスパケット受信	隣接ルータから通知に従い，経路情報を追加，変更または削除を行います。
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，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。

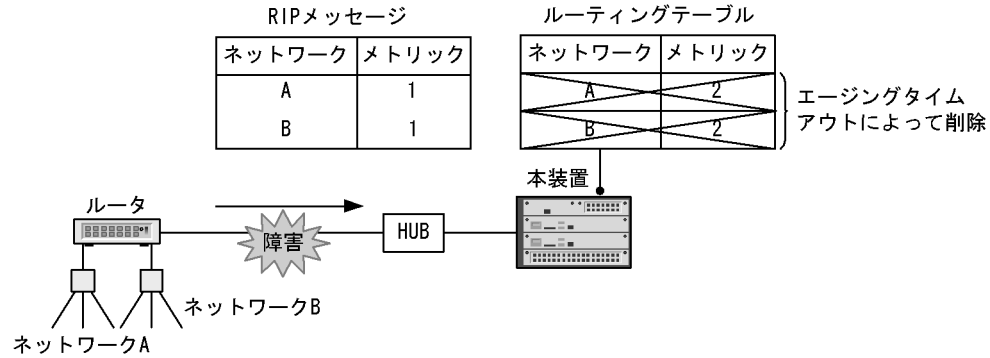
図 9-8　レスポンスパケット受信による経路情報の生成



(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り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）します。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 9-9　エージングタイムアウトによる経路情報の削除

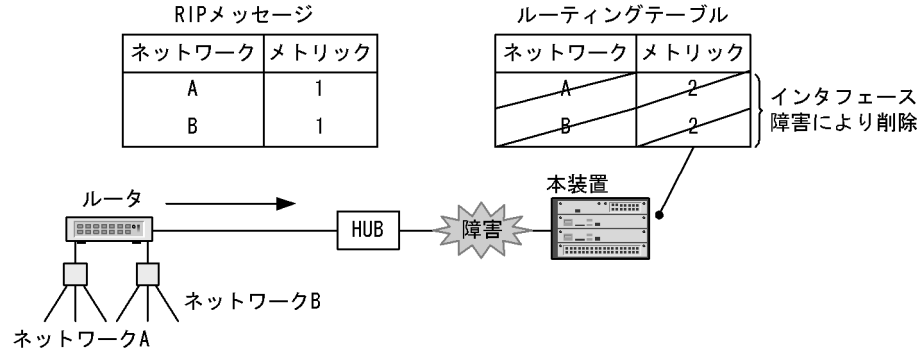


ルータとHUB間で障害が発生すると，本装置にネットワークAおよびBの経路情報が広告されない。
本装置は180秒(エージングタイムアウト値)間広告のない経路情報をルーティングテーブルから削除する。

(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した際に，当該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 9-10　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，当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する。

9.1.5　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 9-11　RIP-1 の経路情報の広告条件

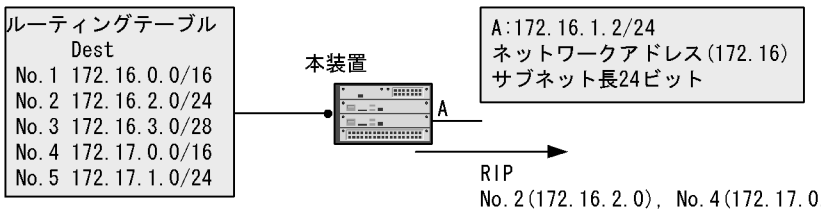
広告する経路情報	広告条件
デフォルト経路情報	無条件に広告します。ただし，RIP 以外で学習したデフォルト経路情報は広告経路フィルタの設定が必要です。
ナチュラルマスク経路情報	本装置が保持しているナチュラルマスク経路情報とインタフェースのネットワークアドレス（アドレスクラスに対応したネットワークアドレス）が異なるとき。
サブネット経路情報※	本装置が保持しているサブネット経路情報のネットワークアドレス（アドレスクラスに対応したネットワークアドレス）とインタフェースのネットワークアドレスが一致し，該当するサブネット経路情報のサブネット長とインタフェースアドレスのサブネット長が一致したとき。
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 9-11　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



●ルーティングテーブル上の各経路情報の取り扱い
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・マスク経路情報なので広告されない。
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，サブネット長も一致するサブネット経路情報なので広告される。
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なので広告されない。
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・マスク経路情報なので広告される。
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なので広告されない。

また，この図での広告条件を次の表に示します。

表 9-12　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

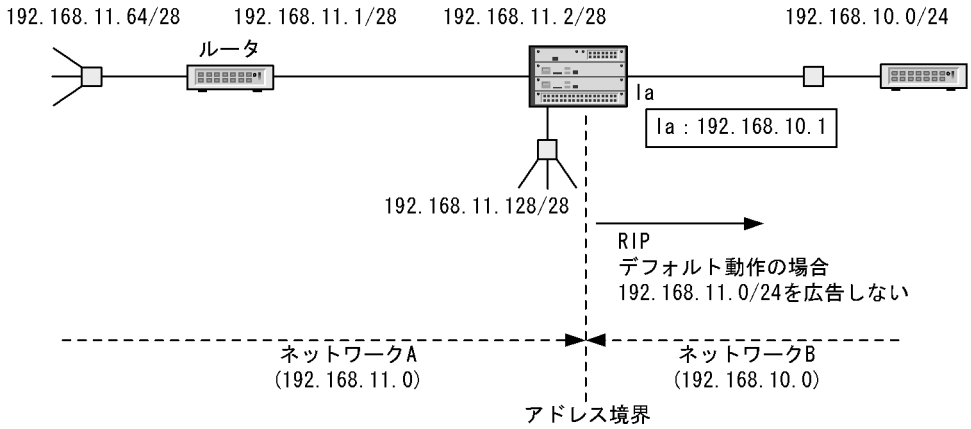
経路情報の種類	ルーティングテーブル上の経路情報	広告条件		広告の有無
		インタフェース D のネットワークアドレスとの一致／不一致	インタフェース D のサブネット長との一致／不一致	
ナチュラルマスク経路	172.16.0.0/16(No.1)	一致	－	×
	172.17.0.0/16(No.4)	不一致	－	○
サブネット経路	172.17.1.0/24(No.5)	不一致	一致	×
	172.16.2.0/24(No.2)	一致	一致	○
	172.16.3.0/28(No.3)	一致	不一致	×

（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。アドレス境界をまたがる場合，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 9-12　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 9-13 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，サブネットの中で一番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。

9.1.6 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インタフェース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

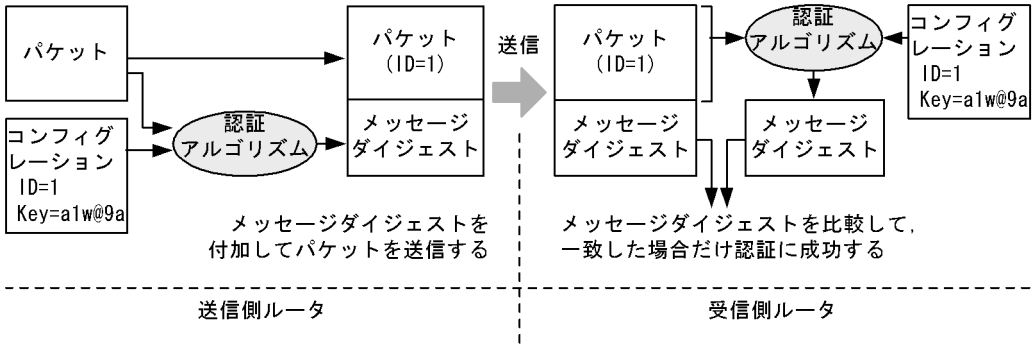
平文パスワード認証では，メッセージにコンフィグレーションで設定した認証キーをそのままパスワードとして埋め込んで送信します。コンフィグレーションで複数の認証キーが設定されている場合は，すべての認証キーごとにメッセージを複製して送信します。

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，認証に成功したとみなします。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 9-13　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，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，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，認証に成功したとみなします。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 9-14 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。

9.2 コンフィグレーション

9.2.1 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 9-15 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 RIP パケットで経路情報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 ※	IPv4 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　14. 経路フィルタリング（IPv4 ／ IPv6 共通）」を参照してください。

9.2.2 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。

9.2.3 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において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 vlan 10 out
   インタフェース vlan 10 から送信する RIP パケットのメトリック値に 2 を加算します。

2. **(config-router)# metric-offset 2 vlan 20 in**
   インタフェース vlan 20 から受信する RIP パケットのメトリック値に 2 を加算します。

9.2.4 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。

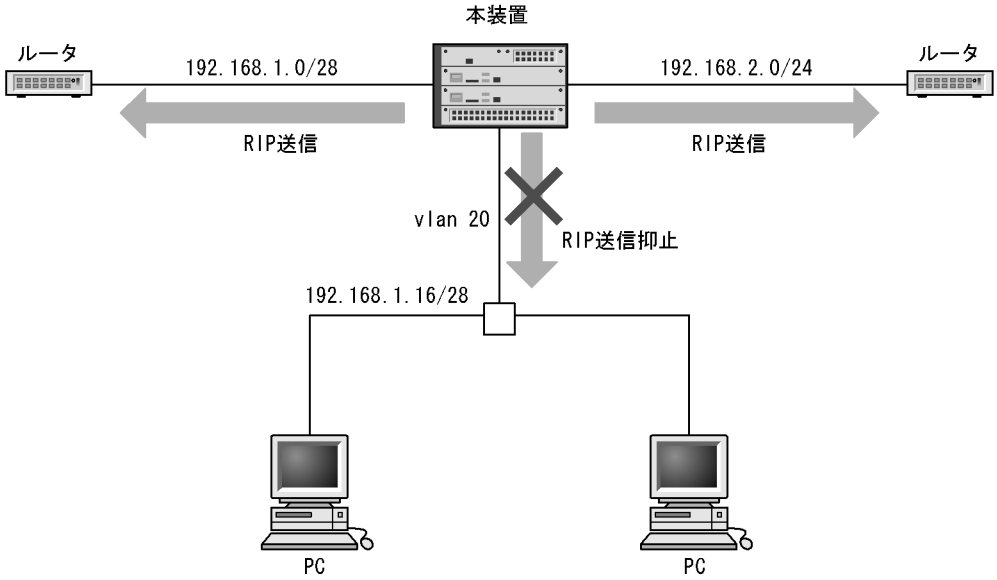
9.2.5 RIP パケットの送信抑止

RIP 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で RIP の送信を抑止する設定には passive-interface コマンドを使用します。

図 9-14　RIP パケットの送信抑止



［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 vlan 20
   インタフェース vlan 20 に対する RIP パケットの送信を抑止します。

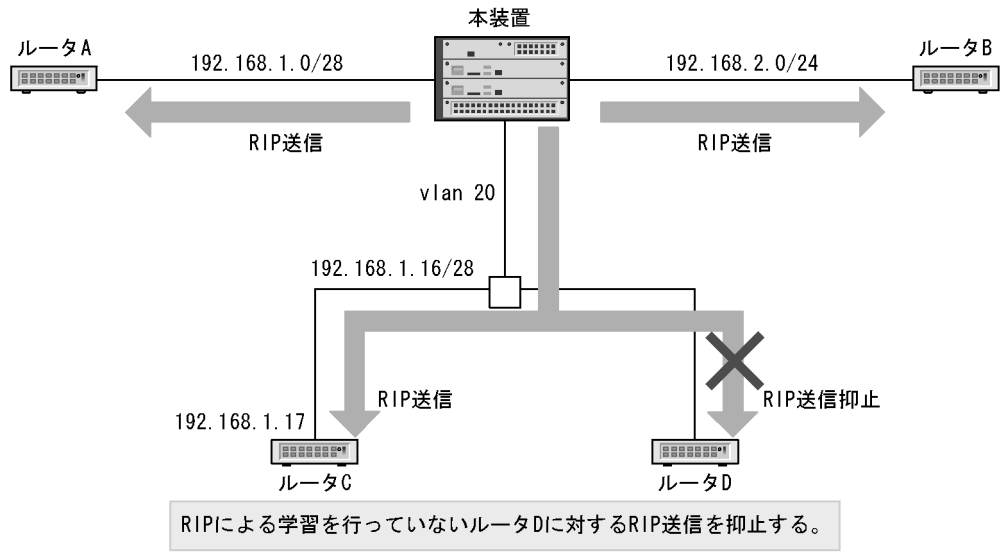
9.2.6　RIP パケット送信相手の限定

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 9-15 RIP パケット送信相手の限定



[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 vlan 20
   インタフェース vlan 20 に対する RIP パケットの送信を抑止します。

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により経路広告を行うことを設定します。

9.2.7 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 vlan 1**
   (config-if)# ip rip authentication key 1 md5 a1w@9a
   (config-if)# ip rip version 2
   インタフェース vlan 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。

9.2.8 VRF での RIP の適用【OP-NPAR】

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，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。

9.3 オペレーション

9.3.1 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 9-16 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。
show processes cpu unicast ※	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。
debug protocols unicast ※	ユニキャストルーティングプログラムが出力するイベントログ情報の運用メッセージ表示を開始します。
no debug protocols unicast ※	ユニキャストルーティングプログラムが出力するイベントログ情報の運用メッセージ表示を停止します。
dump protocols unicast ※	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 ※	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※

「運用コマンドレファレンス Vol.3　8. IPv4・IPv6 ルーティングプロトコル共通」を参照してください。

9.3.2 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 9-16 show ip rip の実行結果

```
> show ip rip
Date 2006/03/14 12:00:00 UTC
RIP Flags: <ON>
Default Metric: 1, Distance: 120
Timers (seconds)
  Update              : 30
  Aging               : 180
  Garbage-Collection  : 60
```

9.3.3 送信先情報の確認

RIP の送信先情報を表示します。

図 9-17 show ip rip target の実行結果

```
> show ip rip target
Date 2006/03/14 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>
```

9.3.4 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 9-18 show ip rip route の実行結果

```
> show ip rip route 172.0.0.0/8
Date 2006/03/14 12:00:00 UTC
Status Codes: * valid, > active
   Destination        Next Hop        Interface       Metric Tag   Timer
*> 172.16/16          192.168.1.100   VLAN0010        3      0      4s
*> 172.17/16          192.168.2.2     VLAN0020        4      0     10s
*> 172.18/16          192.168.2.2     VLAN0020        3      0     10s
*> 172.19/16          192.168.1.200   VLAN0010        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 9-19 show ip rip received-routes の実行結果

```
> show ip rip received-routes 192.168.2.2
Date 2006/03/14 12:00:00 UTC
Status Codes: * valid, > active

Neighbor Address: 192.168.2.2
   Destination        Next Hop        Interface       Metric Tag   Timer
*> 172.17/16          192.168.2.2     VLAN0020        4      0     15s
*> 172.18/16          192.168.2.2     VLAN0020        3      0     15s
*> 192.168.3/24       192.168.2.2     VLAN0020        2      0     15s
*> 192.168.5/24       192.168.2.2     VLAN0020        4      0     15s
```

9.3.5 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 9-20 show ip rip advertised-routes の実行結果 (1)

```
> show ip rip advertised-routes 192.168.2.255
Date 2006/03/14 12:00:00 UTC
Target Address: 192.168.2.255
Destination        Next Hop        Interface       Metric Tag   Age
172.16/16          192.168.1.100   VLAN0010        4      0     19s
172.19/16          192.168.1.200   VLAN0010        6      0      2s
192.168.4/24       192.168.1.200   VLAN0010        3      0      2s
192.168.6/24       192.168.1.100   VLAN0010        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 9-21 show ip rip advertised-routes の実行結果 (2)

```
> show ip rip advertised-routes 172.0.0.0/8
Date 2006/03/14 12:00:00 UTC
Target Address: 192.168.1.100
Destination        Next Hop         Interface       Metric Tag   Age
172.17/16          192.168.2.2      VLAN0020        5      0      1s
172.18/16          192.168.2.2      VLAN0020        4      0      1s
172.19/16          192.168.1.200    VLAN0010        6      0      7s
Target Address: 192.168.1.200
Destination        Next Hop         Interface       Metric Tag   Age
172.16/16          192.168.1.100    VLAN0010        4      0     24s
172.17/16          192.168.2.2      VLAN0020        5      0      1s
172.18/16          192.168.2.2      VLAN0020        4      0      1s
Target Address: 192.168.2.255
Destination        Next Hop         Interface       Metric Tag   Age
172.16/16          192.168.1.100    VLAN0010        4      0     24s
172.19/16          192.168.1.200    VLAN0010        6      0      7s
```

10 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。

10.1 OSPF 基本機能の解説

OSPF（Open Shortest Path First）は，ルータ間の接続の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。

10.1.1 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，接続状態の情報を他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，宛先に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。

使用プロトコルの選択についての注意事項

RIP-2 でも，RIP-1 とは異なり，サブネットマスクの情報を含めることによって，サブネット分割したネットワークを宛先として扱えます。単にサブネットを扱うことが目的で，すべてのルータが RIP-2 を使用可能なら，RIP-2 をお勧めします。

10.1.2 OSPF の機能

OSPF の機能を次の表に示します。本装置では，1 台のルータ上で AS を最大四つの OSPF ネットワークに分割し，OSPF ネットワークごとに別個に経路の交換，計算，生成を行えます。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。

なお，VRF で OSPF を使用した場合，各 VRF を最大四つのドメインに分割できます。

表 10-1 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	○
仮想リンク	○
マルチバックボーン	○
グレースフル・リスタート	○
スタブルータ	○

(凡例) ○：取り扱う

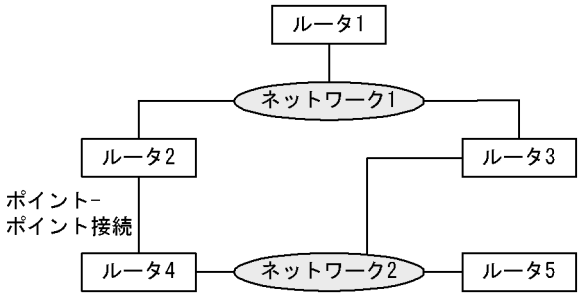
10.1.3 経路選択アルゴリズム

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，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，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。

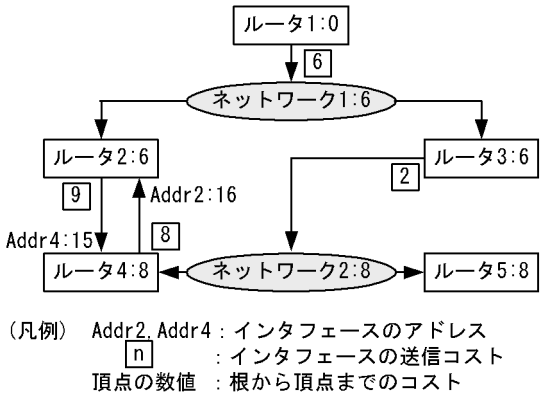
図 10-1 ネットワーク構成例



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 ーネットワーク 1)+0(ネットワーク 1 ールータ 3)+2(ルータ 3 ーネットワーク 2)=8 となります。

図 10-2 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。

10.1.4 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。OSPF を使用し，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，以下の情報を付加して 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

Type 1 と Type 2 の 2 種類があります。Type 1 と Type 2 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 で到達可能なアドレスです。OSPF で到達可能でない場合 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，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ることはありません。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。

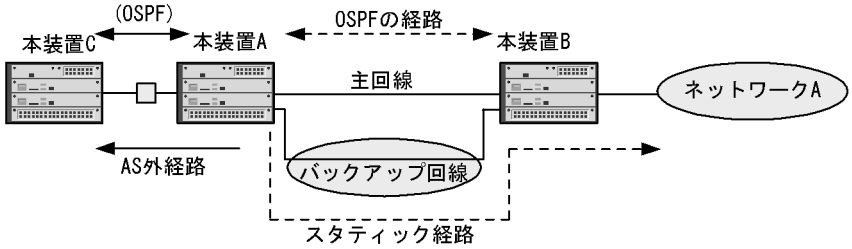
表 10-2 別ドメインの経路を再配布する場合のフィルタ属性

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 Type 2。	
タグ値	経路のタグ値を引き継ぎます。	0

10.1.5 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 10-3 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。

10.1.6 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選択を行います。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，それぞれ別個に SPF アルゴリズムに基づいて経路選択を行います。

OSPF における経路選択の優先順位を次の表に示します。なお，この優先順位は変更できません。

表 10-3 経路選択の優先順位

優先順位	選択項目	詳細
高	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）は，AS 外経路より優先します。
↑	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。
	経路の宛先タイプ	• AS 内経路：エリア内経路は，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が，別エリアの AS 境界ルータが広告している経路よりも優先します。
	AS 外経路タイプ	メトリックタイプが Type1 の AS 外経路は，Type 2 の AS 外経路より優先します。
	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。
	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。
↓ 低	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。

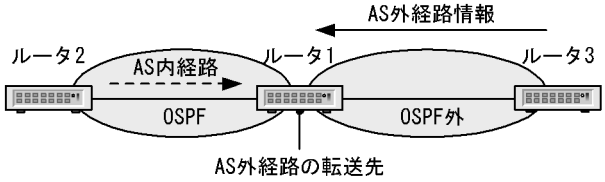
(2) AS 外経路のネクストホップ選択

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 より学習した経路を AS 外経路として導入するに当たって，転送先をルータ 1 とします。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。

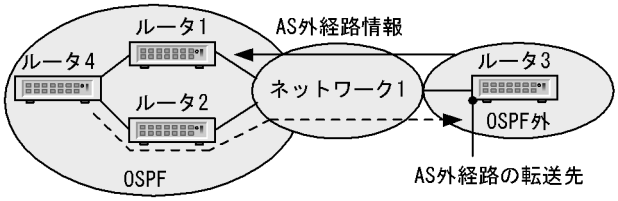
図 10-4　システム構成例（AS 境界ルータを目標とする場合）



(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 より学習した経路を AS 外経路として導入する当たって，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）とします。ルータ 4 からネットワーク 1 に転送する場合，ルータ 2 経由の経路の方がコストが少ない場合は，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。

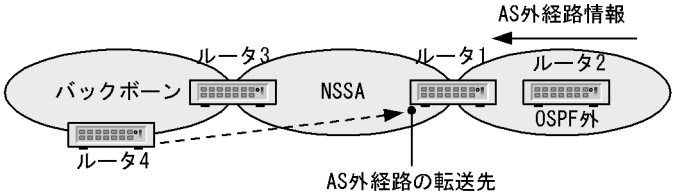
図 10-5　システム構成例（フォワーディングアドレスを目標とする場合）



(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 10-6　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。

10.1.7 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，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。

10.1.8 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に当たって，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ことになり，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

各ルータのルータ ID の決定に当たり，該当するルータにある OSPF が動作しているインタフェースに割り当ててある IP アドレスの中からどれか一つを選択して，これをルータ ID として使用してください。ルータ ID は，基本的には任意の 32 ビットの数値ですが，この方法を使用することで OSPF ネットワーク設計時のミスなどによるルータ ID の重複を防ぐことができます。
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することはできません。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行っても，同一ドメイン内での LSA 広告は抑止されません。

また，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

装置アドレスを複数の 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 ドメインに設定することはできません。

10.2 OSPF 基本機能の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

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 10-4 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 10-5 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として，固定の値を設定します。
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 外経路広告を行う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　14. 経路フィルタリング（IPv4 ／ IPv6 共通）」を参照してください。

表 10-6 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　14. 経路フィルタリング（IPv4 ／ IPv6 共通）」を参照してください。

10.2.2 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，必ず設定が必要です。
   また，マルチバックボーン機能を使用しドメイン間で経路を再配布する場合，必ず設定が必要です。
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。

10.2.3 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 の交換を行います。
- エリア分割しない場合，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。

10.2.4 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。
- 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を制御することはできません。
- 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。

10.2.5 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，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。

[コマンドによる設定]

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。

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 vlan 1**
   (config-if)# ip ospf cost 10
   (config-if)# exit
   コストを 10 に設定します。

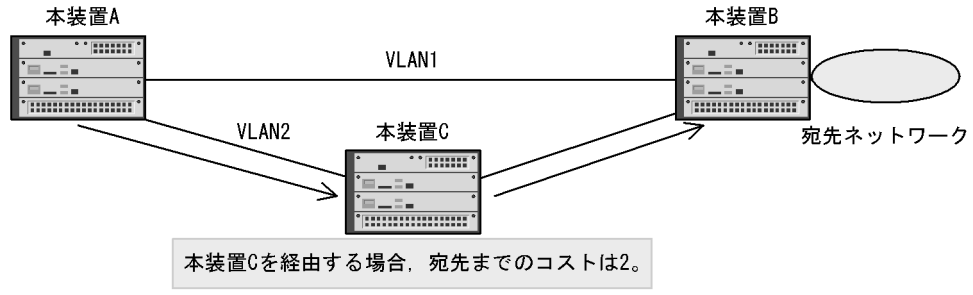
4. **(config)# interface vlan 2**
   (config-if)# ip ospf cost 2
   コストを 2 に設定します。VLAN2 のコスト値を VLAN1 のコスト値よりも小さくすることによって，VLAN2 を経由する経路が優先されます。

10.2.6 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 10-7 マルチパスの構成



[コマンドによる設定]

本装置 A で，イコールコストマルチパスを構築します。

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 vlan 1
(config-if)# ip ospf cost 2
```
VLAN1 のコスト値を 2 とすることで，VLAN2 を経由する経路とコストを等しくします。

10.2.7 VRF での OSPF の適用【OP-NPAR】

[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。

[コマンドによる設定]

ループバックアドレスをルータ ID として使用し，VRF 2 で OSPF を適用します。

1.
```
(config)# interface loopback 2
```
インタフェースモードへ移行し，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 100.1.1.1
```
VRF 2 を指定し，IP アドレスを 100.1.1.1 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，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。

10.3 インタフェースの解説

10.3.1 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。このような構成において，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達されるため，ルータやネットワークに不要な負荷が掛かることになります。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 インタフェースとしてください。

(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。

10.3.2 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。

(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について，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。

10.3.3 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 パケットによって当該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は，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 と設定すると，このルータはインタフェースが接続しているエリアについて，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。

10.3.4 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。LSA は，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，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。

10.3.5 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 パケットの送受信を行いません。

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。

10.4 インタフェースのコンフィグレーション

10.4.1 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 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 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－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。
neighbor（ospf モード）	隣接ルータのアドレスを設定します。
passive-interface（ospf モード）	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 状態変更のトラップを送信することができます。

表 10-8 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
system mtu ※1	装置の MTU を設定します。
snmp-server host ※2	トラップを送信するネットワーク管理装置を設定します。
ip mtu ※3	インタフェースでの送信 IP MTU 長を指定します。
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　12. 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.2　24. SNMP」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　3. ループバックインタフェース（IPv4）」を参照してください。

10.4.2 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行います。
   詳細は，「10.2 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. **インタフェースの設定を行います。**
   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行います。
   詳細は，「10.2 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. **インタフェースの設定を行います。**
   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。

10.4.3 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 vlan 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。また，同時に隣接ルータの priority を 2 に設定します。

10.4.4 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行います。priority や passive-interface コマンドを設定することで，動作を変えることができます。

(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 vlan 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 vlan 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 vlan 2
   VLAN2 をパッシブインタフェースに設定します。

10.5 OSPF のオペレーション

10.5.1 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 10-9 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。
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 processes cpu unicast ※	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 ※	ユニキャストルーティングプログラムを再起動します。
debug protocols unicast ※	ユニキャストルーティングプログラムが出力するイベントログ情報の運用メッセージ表示を開始します。
no debug protocols unicast ※	ユニキャストルーティングプログラムが出力するイベントログ情報の運用メッセージ表示を停止します。
dump protocols unicast ※	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 ※	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※

「運用コマンドレファレンス Vol.3　8. IPv4・IPv6 ルーティングプロトコル共通」を参照してください。

10.5.2 ドメインの確認

OSPF が動作中である場合，ルータ ID やディスタンス値などの設定内容の確認は，運用コマンド show ip ospf で行います。

図 10-8 show ip ospf コマンドの実行結果

```
>show ip ospf
Date 2006/03/14 12:00:00 UTC
OSPF protocol: ON

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
```

10.5.3 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 の確認は，運用コマンド show ip ospf neighbor で行います。

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。

隣接関係が確立された場合，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，運用コマンド show ip ospf interface または show ip ospf neighbor detail 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 内より 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，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 10-9 show ip ospf neighbor コマンドの実行結果

```
>show ip ospf neighbor
Date 2006/03/14 12:00:00 UTC
Domain: 1
Area: 0
Address         State                RouterID      Priority Interface
172.16.10.11    Full/BackupDR        172.16.1.1           1  172.16.10.10
172.16.10.12    Full/DR Other        172.16.1.2           1  172.16.10.10
172.126.110.111 Exch Start/BackupDR  172.126.123.111      1  172.126.120.130
```

図 10-10　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 2009/05/30 12:00:00 UTC
Domain: 1
Index: 2, Name: VLAN0010, Address: 192.168.50.1, State: P to P
Auth Type: Simple
MTU: 1436, DDinPacket: 70, LSRinPacket: 117, ACKinPacket: 70
Router ID: 192.168.50.1, Network Type: P to P
Area: 0, DR: none, Backup DR: none
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 10-11　show ip ospf neighbor コマンド（detail）の実行結果

```
>show ip ospf neighbor detail
Date 2009/05/30 12:00:00 UTC
Domain: 1
Area: 0
Interface Address: 172.16.10.10, Interface State: BackupDR
    Interface Name: VLAN0020
    Neighbor Router ID: 172.16.1.1, Neighbor State: Full/DR
    Neighbor Address: 172.16.10.11, Priority: 1, Poll Interval: 0s
    Last Hello: 6s, Last Exchange: 45d 12h
    DR: 172.16.10.11, Backup DR: 172.16.10.10
    DS: 0, LSR: 0, Retrans: 0, <Master>

    Neighbor Router ID: 172.16.1.2, Neighbor State: Full/DR Other
    Neighbor Address: 172.16.10.12, Priority: 1, Poll Interval: 0s
    Last Hello:  3s, Last Exchange:  1s
    DR: 172.16.10.11, Backup DR: 172.16.10.10
    DS: 0, LSR: 0, Retrans: 0, <>
>
```

10.5.4　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）などの設定確認は，運用コマンド show ip ospf interface で行います。

なお，IP インタフェースが Down 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 10-12　show ip ospf interface コマンドの実行結果

```
>show ip ospf interface
Date 2006/03/14 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
```

10.5.5 LSA の確認

(1) LSA の数の確認

OSPF で保持している LSA の数の確認は，運用コマンド show ip ospf database database-summary で行います。

図 10-13 show ip ospf database database-summary コマンドの実行結果

```
>show ip ospf database database-summary
Date 2006/03/14 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

LSA の種別ごとの，LSA の広告情報や Age の確認は，運用コマンド show ip ospf database で行います。

LSA の種別として，” Router Link ”,“ Network Link ” などがあります。show ip ospf database を実行して，本装置が，以下の LSA を広告していることを確認してください。

(a) ” Router Link ” を広告していること
　表示される LSID は，ルータ ID です。

(b) 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。

(c) 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 10-14 show ip ospf database コマンドの実行結果

```
>show ip ospf database
Date 2006/03/14 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
```

11 OSPF 拡張機能

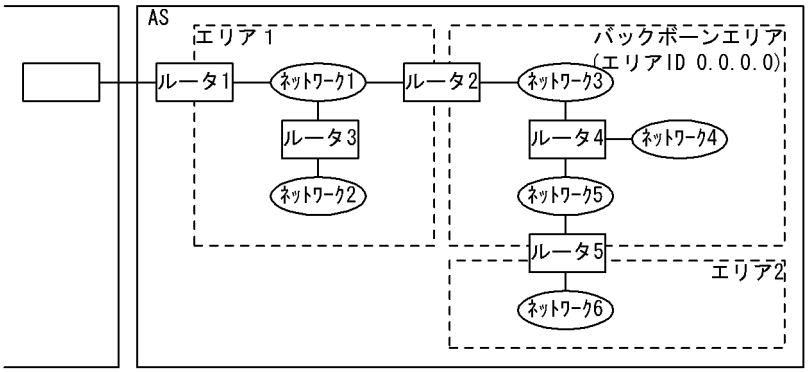
この章では，OSPF の拡張機能について説明します。

11.1 エリアとエリア分割機能の解説

11.1.1 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 11-1 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しているルータを，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の交換を行うため，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

エリア分割を行うと，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，エリア分割を行わ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，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，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，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。

11.1.2 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 11-1 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り，アドレスの範囲をコンフィグレーションで設定することによって，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，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。

11.1.3 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，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）。

11.1.4 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，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，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。

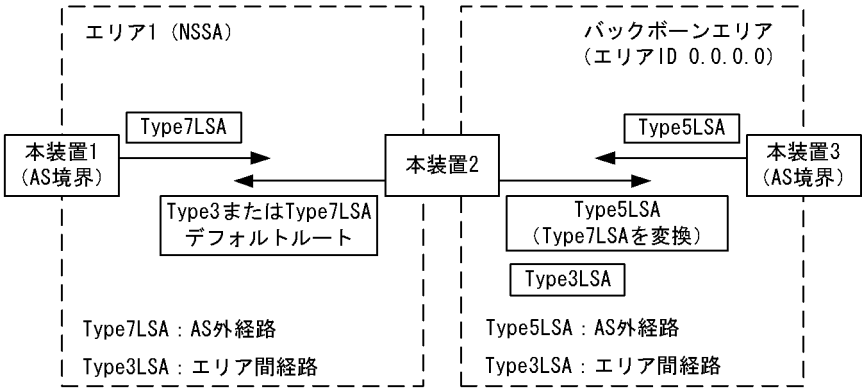
(1) AS 外経路広告

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 11-2 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。

11.1.5 仮想リンク

OSPF では，スタブエリア，または NSSA として設定しておらず，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。

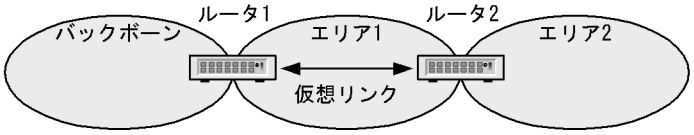
仮想リンクの使い方として，次に示す三つの例を挙げます。

- 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ことによって，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り，エリア 2 をバックボーンに接続しているとみなせるようになります。

図 11-3 エリアのバックボーンへの接続

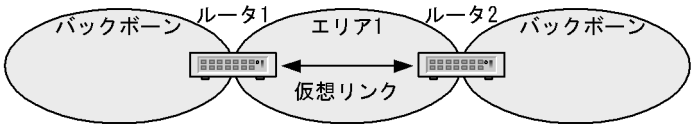


(b) 複数のバックボーンの結合

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ことによって，バックボーンが結合されることになり，この障害を回避できます。

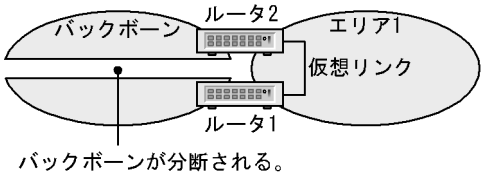
図 11-4 バックボーン間の接続



(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，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 11-5 バックボーン分断に対する予備経路



11.1.6 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 パケットの送受信を行い，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，以下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。

11.2 エリアの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

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，「10 OSPF」で解説している機能のコマンドは，「表 10-5 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 10-6 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 10-7 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 11-2 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 11-3 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。

11.2.2 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。**

11.2.3 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 100.1.1.1**
   ルータ ID として 100.1.1.1 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。

11.2.4 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り，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。

[コマンドによる設定]

エリア 0 とエリア 1 に属するエリアボーダルータにおける，経路集約の設定例を示します。

1. **(config)# router ospf 1**
   (config-router)# area 0 range 10.0.0.0 255.255.254.0
   エリア 0 において，ネットワーク 10.0.0.0 でマスク 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 において，ネットワーク 10.0.2.0 でマスク 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。

11.2.5 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。

11.3 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ことで，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，認証を行いません。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，認証を行いません。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。

11.3.1 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

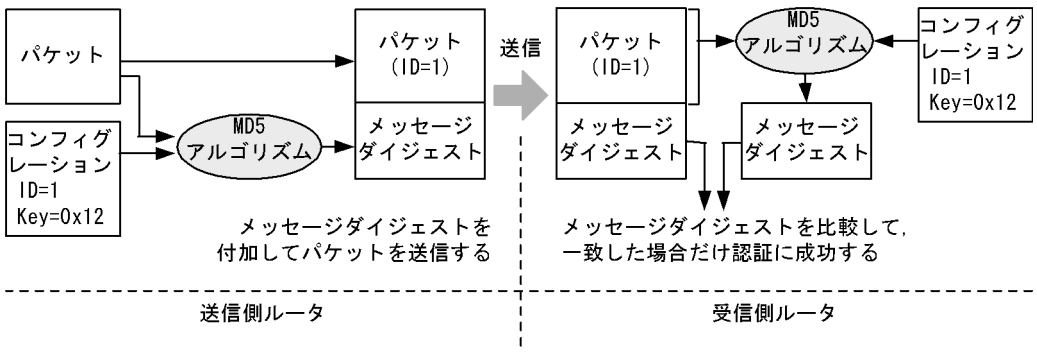
平文パスワード認証では，経路情報の送信時は，コンフィグレーションで設定した認証鍵をそのままパスワードとして埋め込んで送信します。

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，認証に成功したとみなします。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することで，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 11-6 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，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，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，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，認証に成功したとみなします。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ものとみなします。認証に失敗した情報は破棄されます。

11.4 隣接ルータ認証のコンフィグレーション

11.4.1 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トラップを送信できます。

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
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 ※	トラップを送信する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.2　24. SNMP」を参照してください。

11.4.2 MD5 認証キーの変更

認証キーの移行を行うために，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。**

11.4.3 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行うことを設定します。

2. **(config)# interface vlan 1**
   (config-if)# ip ospf authentication-key a1w@9a
   認証鍵を a1w@9a に設定します。
   VLAN1 がエリア 1 に設定されている場合，VLAN1 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。

11.4.4 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 認証を行うことを設定します。

2. **(config)# interface vlan 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。VLAN1 がエリア 1 に設定されている場合，VLAN1 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。

11.5 グレースフル・リスタートの解説

11.5.1 概要

グレースフル・リスタートは，装置が系切替したときや，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停止時間を短縮する機能です。

OSPF では，グレースフル・リスタートによって OSPF の再起動を行う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。

11.5.2 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・リスタートを行っている間，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以下に示します。

- 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インタフェースすべてでヘルパールータとして動作を行います。
- 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，以下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可能性があるため，ヘルパー機能を中断し，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，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の削除を実施し，ヘルパー機能を削除した場合。

11.5.3 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。

- 装置が系切替したとき。
- 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

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 Opaque LSA を広告します。
Opaque LSA について，次の制限事項があります。

- Type9 の Opaque LSA 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。
- Type10，Type11 の Opaque LSA の学習，広告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 11-7　OSPF グレースフル・リスタート手順

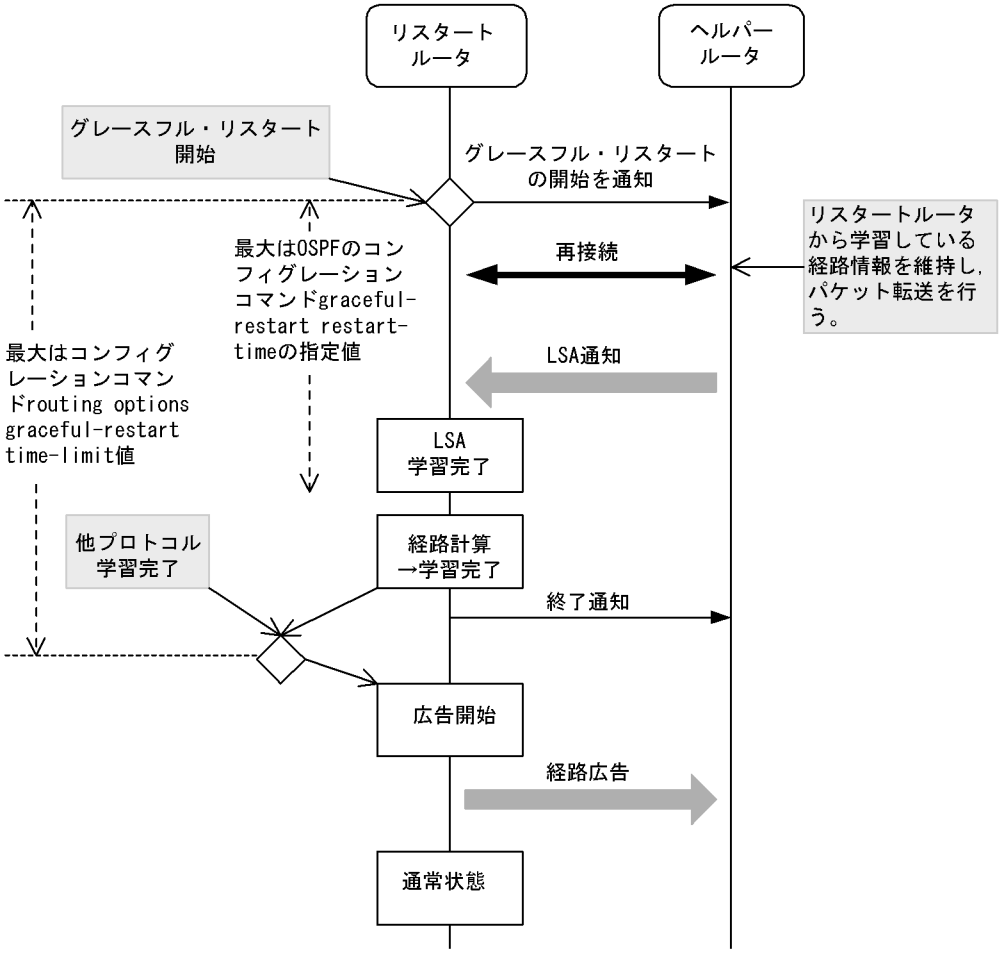


表 11-5　OSPF グレースフル・リスタート手順

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	装置が系切替したとき。	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 情報のパケット交換を行います。
		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 OSPF インタフェースについて再接続完了し，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行い，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行います。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，経路計算を行います。
3	広告開始	OSPF の経路学習が完了し，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

次に OSPF のグレースフル・リスタートが失敗するケースを示します。

- 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。
- 再接続を行っ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の graceful-restart mode を変更し，リスタートルータ機能を削除した場合。

(4) 注意事項

1. 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。
2. 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。
3. 本装置の系切替時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ルーティングエントリが削除されることがあります。
4. 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することができず，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。

11.6 グレースフル・リスタートのコンフィグレーション

11.6.1 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 11-6 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　8. ルーティングオプション（IPv4）」を参照してください。

11.6.2 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)# 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。

11.6.3 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)# router ospf 1**
   (config-router)# graceful-restart mode helper
   ヘルパー機能を使用します。

11.7 スタブルータの解説

11.7.1 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。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，このような通知を行っているルータを，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ぐことができます。

(1) マックスメトリック

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，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装置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。

11.7.2 スタブルータ動作

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。

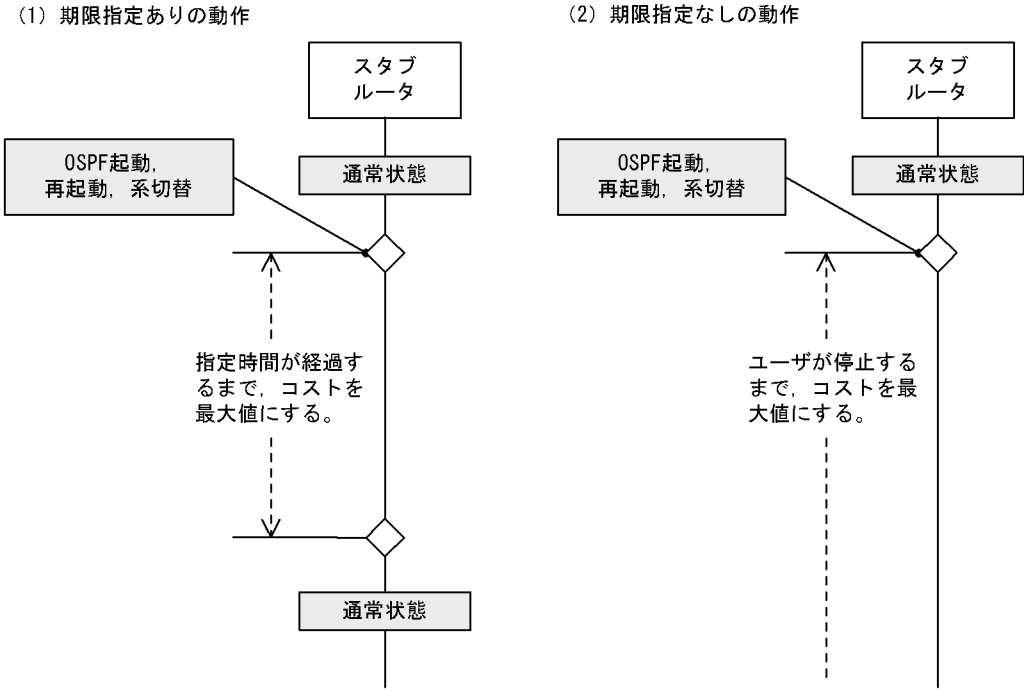
(2) 起動後にスタブルータとして動作する場合

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。

- 装置の系切替後（グレースフル・リスタート成功時を除く）
- ユニキャストルーティングプログラムの再起動後（グレースフル・リスタート成功時を除く）
- グレースフル・リスタートが発生し，本装置がリスタートルータとしての経路学習に失敗した後
- 装置起動

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 11-8 スタブルータの動作



（3）注意事項

1. 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。
2. 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。
3. 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，仮想ネーバはその仮想リンクを到達不能とみなします。
4. 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。

11.8 スタブルータのコンフィグレーション

11.8.1 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 11-7 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。

11.8.2 スタブルータ機能

[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，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。

11.9 OSPF 拡張機能のオペレーション

11.9.1 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 11-8 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 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 8. IPv4・IPv6 ルーティングプロトコル共通」を参照してください。

11.9.2 エリアボーダの確認

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，運用コマンド show ip ospf を実行し，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かどうかを確認してください。

図 11-9 show ip ospf コマンドの実行結果

```
>show ip ospf
Date 2006/03/14 12:00:00 UTC
OSPF protocol: ON

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
  Helper Status : Finished  2006/02/15 14:12:22
Area            Interfaces  Network Range      State
0               1           -                  -
10              1           192.168.1.1/24     Advertise
                            172.19/18          DoNotAdvertise
```

11.9.3 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かどうかを確認してください。運用コマンド show ip ospf に area パラメータを指定した場合，エリアの一覧を表示します。

図 11-10 show ip ospf area コマンドの実行結果

```
>show ip ospf area
Date 2006/03/14 12:00:00 UTC
Domain: 1
ID              Neighbor   SPFcount   Flags
0               2          14         <ASBoundary>
1               2          8          <NSSA>
>
```

11.9.4 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

グレースフル・リスタートの状態を，show ip ospf コマンドを実行し，確認してください。

図 11-11 show ip ospf コマンドの実行結果

```
>show ip ospf
Date 2006/03/14 12:00:00 UTC
OSPF protocol: ON

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
  Helper Status : Finished  2006/02/15 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

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，show graceful-restart unicast コマンドを実行し，確認してください。

図 11-12 show graceful-restart unicast コマンドの実行結果

```
>show graceful-restart unicast
Date 2006/04/14 12:00:00 UTC
Status: Completed
Graceful Restart Time Limit: 180s
Start Time: 2006/04/08 17:01:23
End Time  : 2006/04/08 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)
```

12 BGP4【OP-BGP】

この章では，IPv4 のルーティングプロトコル BGP4 の解説と操作方法について説明します。

12.1 基本機能の解説

12.1.1 概要

BGP4（Border Gateway Protocol 4）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。

BGP4 の機能を次の表に示します。

表 12-1 BGP4(IPv4) の機能

機能	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	○
グレースフル・リスタート	○
学習経路数制限	○

（凡例） ○：取り扱う
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
注※ 2 VRF では取り扱いません

12.1.2 ピアの種別と接続形態

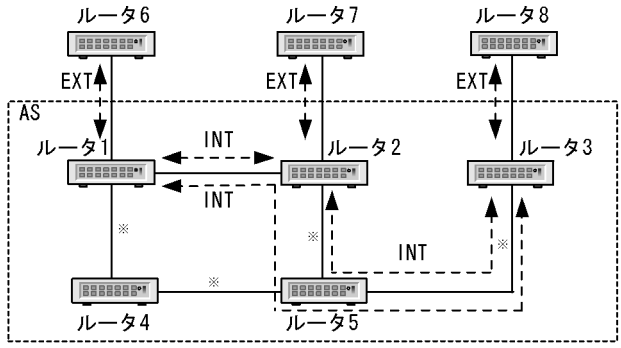
BGP4 は AS 間のルーティングプロトコルなので，扱う経路情報は宛先ネットワークへの AS パス情報（パケットが宛先のネットワークに到達するまでに通過する AS の列）で構成されます。BGP4 が動作するルータを BGP スピーカと呼びます。この BGP スピーカはそのほかの BGP スピーカと経路情報を交換するためにピアを形成します。

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。なお，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，メンバー AS 間ピアが追加されます。メンバー AS 間ピアについては，

「12.4.10　コンフェデレーション」を参照してください。

ネットワーク構成に合わせてピアを使用してください。外部ピアと内部ピアを次の図に示します。

図 12-1　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BGP4スピーカ
　　ルータ6，ルータ7，ルータ8：外部BGP4スピーカ
　　ルータ4，ルータ5　　：内部非BGP4スピーカ
　　INT　：内部ピア
　　EXT　：外部ピア
注※　IGPが動作する。

(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 アドレスは，直接接続されたインタフェースのインタフェース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の neighbor ebgp-multihop を使用することによって，直接接続されたインタフェースのインタフェースアドレス以外のアドレス（例えば装置アドレス）で接続できます。

「図 12-1　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

内部の同じ AS に属する BGP スピーカ間に形成するピアです。BGP4 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なければなりません。これは，内部ピアで受信した経路情報は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 12-1　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) 装置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の IP アドレス（これを装置アドレスと呼びます）を外部ピアや内部ピアの IP アドレスとして使用することによって，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 12-1　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 間の内部ピアは確立できません。しかし，内部ピアの IP アドレスとして装置アドレスを使用

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。

[装置アドレス使用上の注意事項]

装置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）でお互いに学習していなければなりません。なお，本装置は装置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なければなりません。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 12-1　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。

12.1.3　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学習した同じ宛先への複数の経路情報から次の表に示す優先順位で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。

なお，コンフェデレーション構成での経路選択は，「12.4.10　コンフェデレーション」を参照してください。

表 12-2　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。
↑	LOCAL_PREF 属性の値が最も大きい経路を選択します。
	AS_PATH 属性の AS 数が最も短い経路を選択します。※ 1
	ORIGIN 属性の値で IGP，EGP，Incomplete の順で選択します。
	MED 属性の値が最も小さい経路を選択します。※ 2
	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。
	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。
	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。※ 3
↓	CLUSTER_LIST 属性長が最も短い経路を選択します。※ 4
低	学習元ピアのアドレスが小さい経路を選択します。※ 3

注※ 1

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。

注※ 2

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 を指定することによって，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。

注※ 3

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 を指定することによって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。

注※ 4

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。

経路選択に関連する経路情報に含まれる BGP 属性（weight 値，LOCAL_PREF 属性，AS_PATH 属性，ORIGIN 属性，MED 属性，NEXT_HOP 属性）の概念を次に説明します。

（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 の範囲で指定します。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 の範囲で指定します。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 を設定して，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。

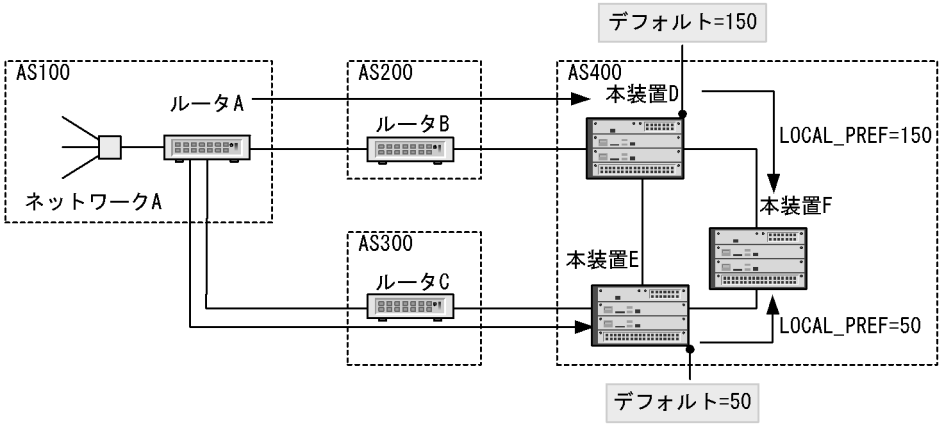
（b） LOCAL_PREF 属性のフィルタ単位での変更

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 を組み合わせることによって，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 12-2 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け取ります。本装置 D の LOCAL_PREF 値を 150 に，本装置 E の LOCAL_PREF 値を 50 に設定するとします。それによって，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 に設定し，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。本装置 F でのネットワーク A への経路情報は，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 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 12-3 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。
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 を組み合わせることによって，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。

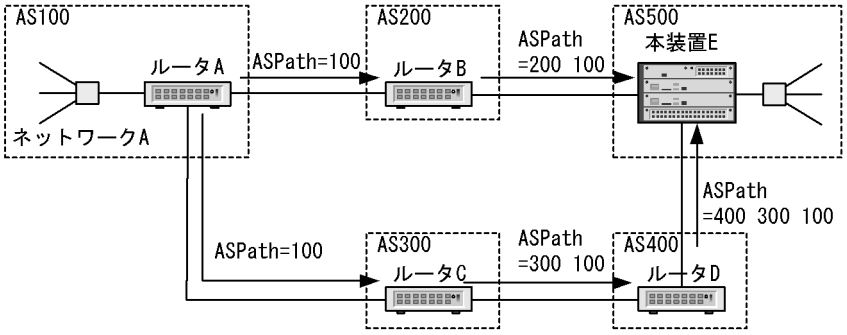
(4) AS_PATH 属性

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 との組み合わせによって複数の自 AS 番号を AS_PATH 属性に追加することもできます。これはある宛先ネットワークへの複数の経路が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 12-3　AS_PATH 属性による経路選択

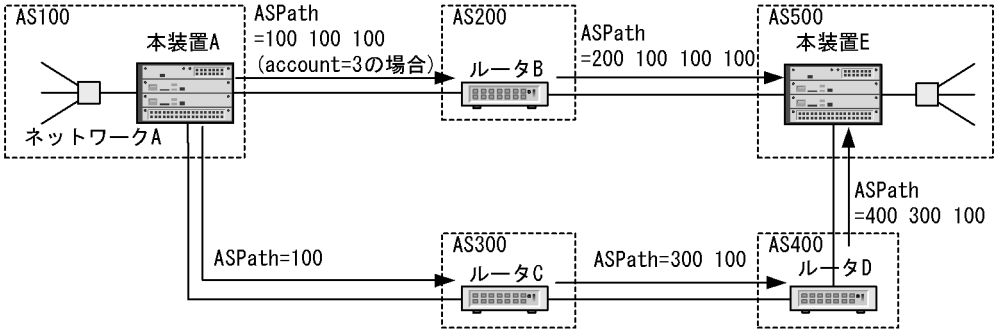


ルータ A が自 AS に存在するネットワーク A を AS200 経由で通知するとき，AS500 に到達する経路情報の AS_PATH 属性は「200 100」を持ちます。ルータ A が自 AS 内のネットワーク A を AS300，AS400 経由で通知するとき，AS500 に到達する経路情報の AS_PATH 属性は「400 300 100」を持ちます。したがって，AS500 の本装置 E は最も短い AS_PATH 属性を持つ AS200 経由で到達した経路を選択します。

(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 の例を次の図に示します。

図 12-4　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 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」を持ち，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。

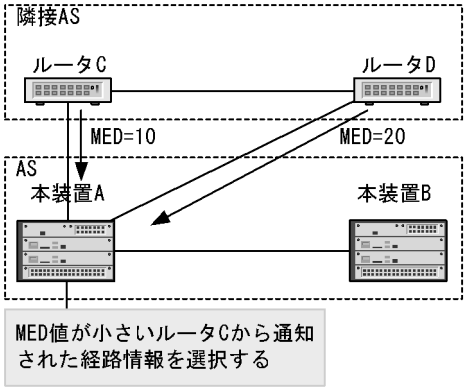
(5) MED 属性

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 BGP4 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 を指定して，異なる隣接 AS から学習した BGP4 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 12-5 MED 属性による経路選択



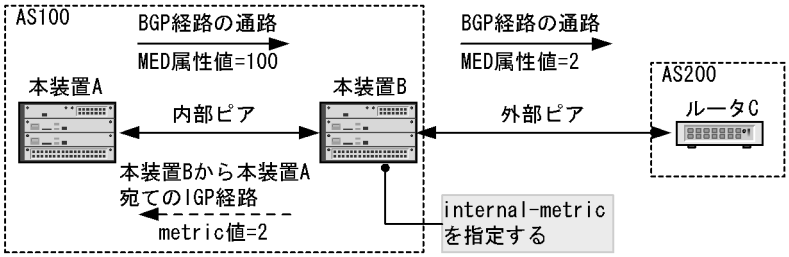
ある宛先ネットワークに対する経路情報をルータ C は MED 属性値 10 で，ルータ D は MED 属性値 20 で本装置 A に通知しているものとします。この場合，本装置 A はルータ C から通知された経路情報を該当する宛先ネットワークへの経路として選択します。

(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 を組み合わせることによって，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，set metric-type に internal 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 BGP4 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 12-6 set metric-type internal の使用例



この図では本装置 A，本装置 B の間で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 BGP4 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 属性値に設定したい場合，本装置 B でコンフィグレーションコマンド set metric-type internal を指定します。

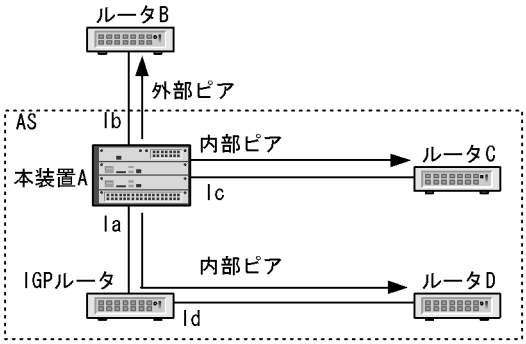
(6) NEXT_HOP 属性

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。

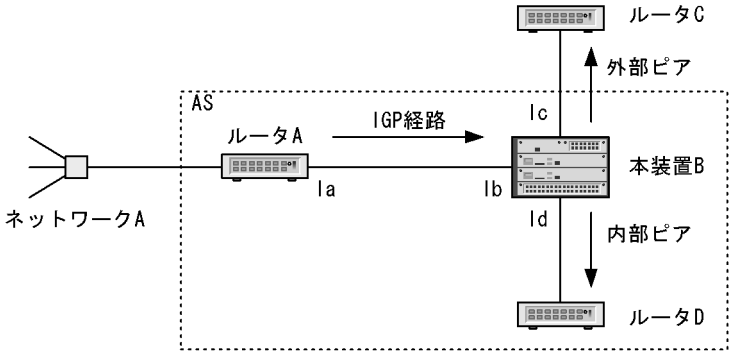
図 12-7　BGP4 ピアから学習した経路を広告する場合に通知する経路情報の NEXT_HOP 属性の設定例



- **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 12-8　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って，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。BGP4 経路のネクストホップへ到達可能な経路の中から，宛先のマスク長が最も長い経路を選択し，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，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，かつ noinstall パラメータの指定がある場合，当該 BGP4 経路を抑止します。

12.1.4 VRF での BGP4 の機能【OP-NPAR】

(1) 概要

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。なお，異なる VRF 間のピア接続はできません。

(2) VRF で 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 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 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りますので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・リフレクション機能）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。

12.1.5 BGP4 使用時の注意事項

BGP4 を使用したネットワークを構成する場合は次の制限事項に注意してください。

(1) BGP4 の制限事項

本装置は 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 12-4 RFC との差分

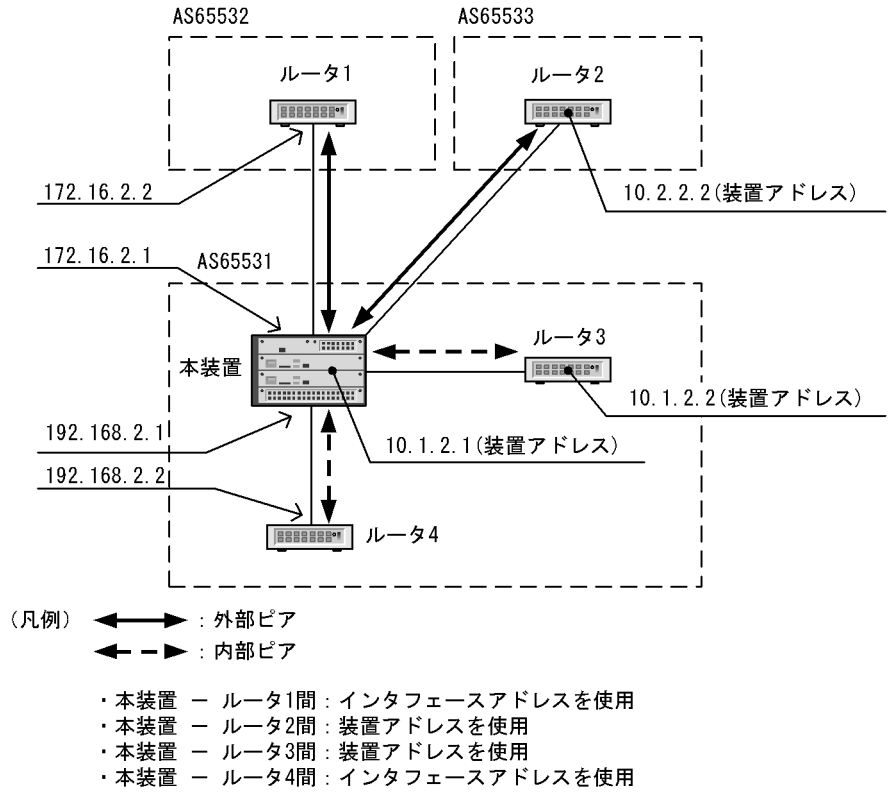
RFC 番号	RFC		本装置
RFC4271	パス属性：NEXT_HOP	経路を広告される外部ピアが，広告している BGP スピーカのインタフェースの一つとサブネットを共有している場合，スピーカはそのようなインタフェースに関連した IP アドレスを，NEXT_HOP 属性に使用することができます。これは“ファーストパーティ”NEXT_HOP 属性として知られています。	“ファーストパーティ”NEXT_HOP 属性はサポートしません。
		外部ピアへメッセージを送信する場合で，かつ，ピアがスピーカから複数 IP ホップはなれている場合（別名“マルチホップ EBGP”）BGP スピーカは，NEXT_HOP 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。	Idle 状態から start までの間の最初のタイマは 16 ～ 36 秒です。
	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，初期設定を完了します。その後，そのピアへ OPEN メッセージを送信してその Hold タイマをセットし，状態を Open Sent に変更します。Hold タイマの値は 4 分が提案されています。	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。

RFC 番号	RFC		本装置
	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。このレート制限は宛先ごとに処理されます。しかし，Min Route Advertisement Interval の値は，BGP4 ピアごとに設定されます。	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。	Min AS Origination Interval はサポートしていません。
	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，Keepalive，Min Route Advertisement Interval に関係したタイマにジッタを適用すべきです。	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。	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 秒になります。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 タイマが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。
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。

12.2 基本機能のコンフィグレーション

次の構成例を基にコンフィグレーションを説明します。

図 12-9 接続構成例



12.2.1 コンフィグレーションコマンド一覧

基本機能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以下に示します。

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
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。
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/BGP4+ の動作を抑止します。

コマンド名	説明
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 間ピア接続を許容することを設定します。
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/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アドレスに装置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/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。
distribute-list in（BGP4）※2	BGP4 の学習経路フィルタリングの条件として用いる経路フィルタを指定します。
distribute-list out（BGP4）※2	BGP4 の広告経路フィルタリングの条件として用いる経路フィルタを指定します。
neighbor in（BGP4）※2	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用いる経路フィルタを指定します。
neighbor out（BGP4）※2	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用いる経路フィルタを指定します。
redistribute（BGP4）※2	BGP4 で広告する経路のプロトコルを指定します。

注※ 1

BGP4+（IPv6）ピアと共用コマンドです。

注※ 2

「コンフィグレーションコマンドレファレンス Vol.3　14. 経路フィルタリング（IPv4 ／ IPv6 共通）」を参照してください。

表 12-6 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	1. 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リング設定を適用します。 ・全 BGP4 ピアに BGP4 経路の再広告要求を行います。 2. パラメータに * out を指定した場合 ・BGP4 広告用経路フィルタリングに最新の経路フィルタリング設定を適用します。 ・neighbor remove-private-as の設定を運用に反映します。 ・全 BGP4 ピアに BGP4 経路の再広告を行います。 3. 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リング設定を適用します。 ・neighbor remove-private-as 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行います。 4. パラメータに * を指定した場合 全 BGP4 ピアを切断します。

12.2.2 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自装置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. **フィルタ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行います。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，コンフィグレーションコマンド neighbor remote-as の設定前に，コンフィグレーションコマンド disable 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コンフィグレーションコマンド disable を削除してください。

12.2.3 BGP4 ピアの設定

[設定のポイント]

ピアの設定は最初に neighbor remote-as コマンドでピアの相手側アドレスと相手側の AS 番号を設定した後，当該ピアの他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/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直接接続されたインタフェースのインタフェース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に装置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に装置アドレスを指定します。

12.2.4 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。

12.2.5 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。

12.2.6 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，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。

12.2.7 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，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 192.169.10.0/24**
   (config)# ip prefix-list MY_NET_2 seq 10 permit 192.169.20.0/24
   (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 192.169.10.0/24 の場合，MED 属性値に 120 を設定します。
   宛先ネットワークが 192.169.20.0/24 も広告対象にします。

12.2.8 学習経路フィルタリングの条件の設定

[設定のポイント]

ピアごとに学習フィルタを適用する場合は neighbor in 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，他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，他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，他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。

12.2.9 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経路フィルタを適用する場合は distribute-list out 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 192.169.10.0/24 と 192.169.20.0/24 の経路を広告します。

12.2.10 フィルタ設定の運用への反映

[設定のポイント]

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させるには，運用コマンド clear ip bgp を使用します。

[コマンドによる設定]

1. **# clear ip bgp * both**
   学習経路フィルタと広告経路フィルタを運用に反映させます。

[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・リフレッシュ機能（「12.4.5 ルート・リフレッシュ」参照）の両方を実行します。ルート・リフレッシュ機能の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・リフレッシュ要求は行いませんが経路フィルタの変更は反映します。

12.2.11 VRF での BGP4 の設定【OP-NPAR】

[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。

12.3 基本機能のオペレーション

12.3.1 運用コマンド一覧

基本機能の運用コマンド一覧を次の表に示します。

表 12-7 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 bgp	BGP4 プロトコルに関する情報を表示します。
clear ip bgp	BGP4 セッションまたは 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。
show processes cpu unicast ※	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 ※	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 ※	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 ※	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※
「運用コマンドレファレンス Vol.3 8. IPv4・IPv6 ルーティングプロトコル共通」を参照してください。

12.3.2 ピアの種別と接続形態の確認

「図 12-9 接続構成例」に対応する表示を次の図に示します。ピアの接続情報は運用コマンド show ip bgp の neighbors パラメータ指定で表示します。詳細情報を表示する場合は detail パラメータを指定します。

図 12-10 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 2006/03/18 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 12-11　show ip bgp コマンド（detail パラメータ指定）の実行結果

```
> show ip bgp neighbors detail
Date 2006/03/17 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: 2006/03/17 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
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: 2006/03/17 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
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: 2006/03/17 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 Refresh>
      Send   : <IPv4-Uni Refresh Refresh(v)>
      Receive: <IPv4-Uni Refresh Refresh(v)>
    Password: UnConfigured
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: 2006/03/17 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: <IPv4-Uni Refresh Refresh(v)>
      Send   : <IPv4-Uni Refresh Refresh(v)>
      Receive: <IPv4-Uni Refresh Refresh(v)>
    Password: UnConfigured
>
```

12.3.3 BGP4 経路選択結果の確認

BGP4 経路の選択結果は，show ip bgp コマンドで確認できます。

図 12-12 show ip bgp コマンドの実行結果

```
> show ip bgp
Date 2006/03/18 22:44:23 UTC
Local AS: 65531, Local Router ID: 192.168.1.100
Status Codes: * valid, > active
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
*> 192.169.10/24    192.168.2.2   -     100       10           i           …12
*> 192.169.20/24    192.168.2.2   -     100       10           i           …13
```

1 ～ 3. 10.10/16 の経路選択

weight 値の比較により 1 と 2 が優先され，次に LOCAL_PREF 属性の比較により 1 が選択されています。

4 ～ 5. 10.20/16 の経路選択

AS_PATH 属性長の比較により 4 が選択されています。

6 ～ 7. 172.20/16 の経路選択

ORIGIN 属性の比較により 6 が選択されています。

8 ～ 9. 172.30/16 の経路選択

MED 属性の比較により 8 が選択されています。

10 ～ 11. 192.168.10/24 の経路選択

相手 BGP 識別子の比較により 10 が選択されています。

12 ～ 13. 192.169.10/24，192.169.20/24 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。

12.3.4 BGP4 経路の広告内容の確認

広告した BGP4 経路のパス属性を確認する場合は運用コマンド show ip bgp の advertised-routes パラメータ指定を使用します。

図 12-13　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 2006/03/18 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
192.169.10/24        192.168.2.2     120    -         65531 i           …1
192.169.20/24        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
192.169.10/24        192.168.2.2     120    -         65531 i           …2
192.169.20/24        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。

12.4　拡張機能の解説

12.4.1　BGP4 ピアグループ

BGP4 ピアグループとは，ピアをグループ化し，グループ単位にコンフィグレーションコマンド neighbor による設定を行うことで，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 neighbor コマンドを設定することもでき，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することができ，ピアはその内の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は，運用コマンド clear ip 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。

12.4.2　コミュニティ

本装置では経路情報に付加された 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加されている場合，その値に従い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 12-8　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加されている場合，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加できます。

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。

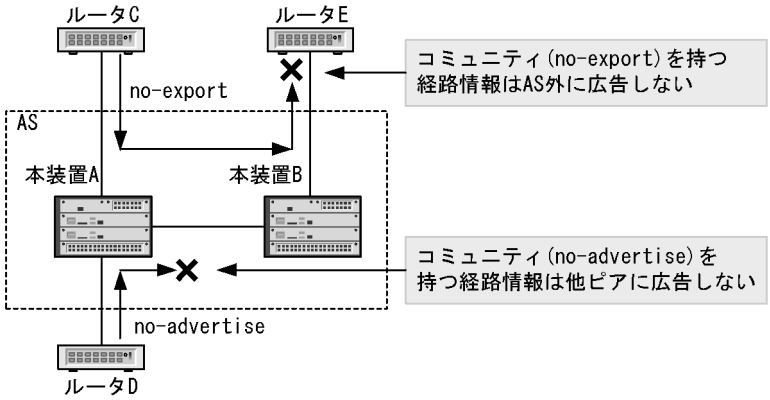
表 12-8　本装置で使用できるコミュニティ

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。

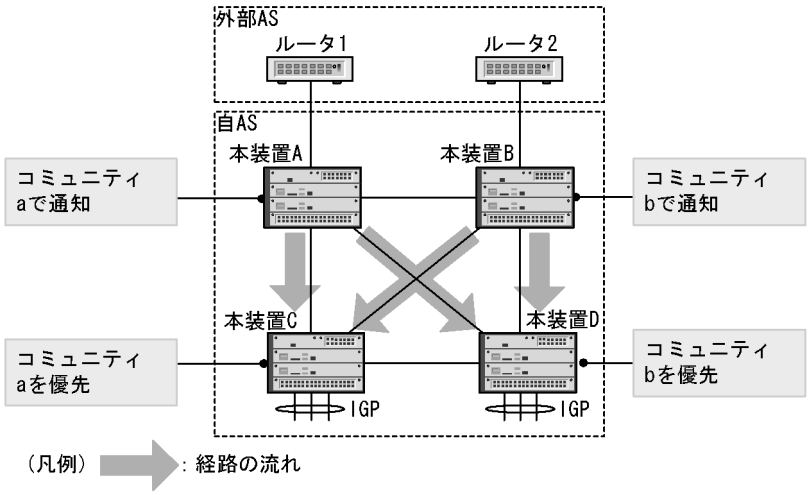
図 12-14 COMMUNITIES 属性を持つ経路情報の広告範囲



(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 12-15 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，本装置 C からのトラフィックは本装置 A を経由し 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 AS 外に優先して中継するものとします。このような場合，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 を付加します。
   （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 を付加します。
   （広告経路フィルタで指定できます）
3. 本装置 C で，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，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，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，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）

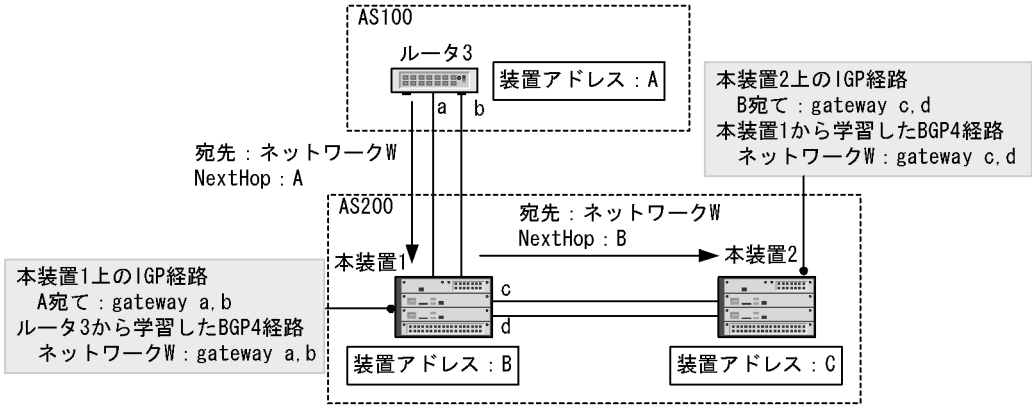
12.4.3　BGP4 マルチパス

BGP4 マルチパスは，一つの宛先ネットワークに対し複数の経路（パス）を生成し，トラフィックの負荷分散を実現します。本装置での BGP4 経路のマルチパス生成の概念について説明します。

（1） IGP 経路のマルチパス化による BGP4 経路のマルチパス

本装置は BGP4 経路のネクストホップ解決を IGP 経路に基づいて行います。ネクストホップ解決時，BGP4 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 BGP4 経路もマルチパス化されます。マルチパス生成の概念を次の図に示します。

図 12-16　IGP 経路のマルチパス化による BGP4 経路マルチパス化の概念



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は装置自体に付与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 によって，装置自体にアドレスを付与できます。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装置アドレスの使用を指定できます。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 BGP4 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」となっていることによって，BGP4 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 BGP4 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」となっていることによって，BGP4 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 BGP4 マルチパスの注意事項

本装置でマルチパス化を行える IGP 経路はスタティック経路および OSPF 経路です。スタティック経路のマルチパス化の概念については，「8.1　解説」を，OSPF 経路のマルチパス化の概念については，「10.1.7　イコールコストマルチパス」の項を参照してください。

(2) 複数のピアから学習した BGP4 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 BGP4 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 パラメータを指定して，異なる隣接 AS から学習した，BGP4 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。

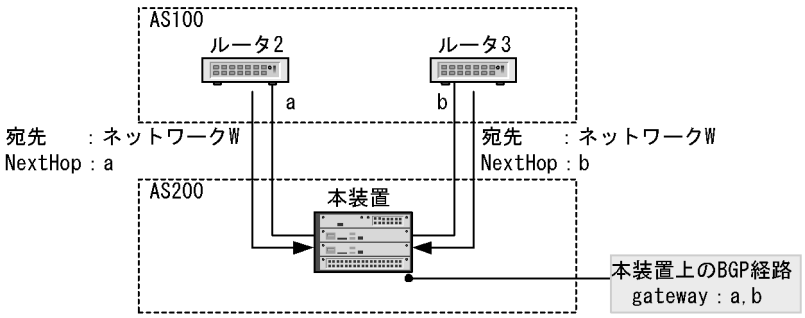
表 12-9 タイブレーク条件

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。	－
ネクストホップが等しい（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 BGP4 経路マルチパス化の概念を次の図に示します。

図 12-17 複数のピアから学習した BGP4 経路マルチパス化の概念



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 BGP4 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 BGP4 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 BGP4 経路を本装置 1 からそのほかの BGP4 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。

12.4.4 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，BGP4 コネクション確立時の OPEN

メッセージに Capability 情報を付加することによって，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。お互いに広告した Capability 情報で一致する（お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。

本装置では，「IPv4-Unicast 経路の送受信」および「ルート・リフレッシュ（Capability Code：2)」，「ルート・リフレッシュ（Capability Code：128)」，「グレースフル・リスタート（Capability Code：64)」を OPEN メッセージの Capability 情報として付加します。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-Unicast 経路の送受信」だけを行います。

ネゴシエーションできる機能を次の表に示します。

表 12-10　ネゴシエーションできる機能

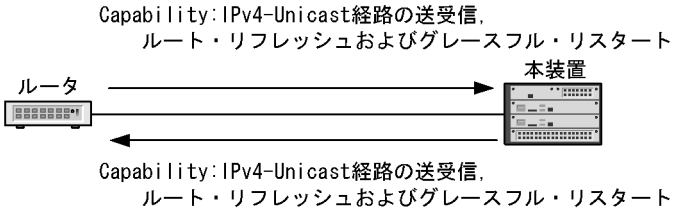
機能名称	OPEN メッセージの Capability 情報	内容
IPv4 経路の送受信	Capability Code：1 Capability Value の AFI：1 Capability Value の SAFI：1	IPv4-Unicast 経路を該当するピア間で送受信します。
ルート・リフレッシュ	Capability Code：2 Capability Value の AFI：1 ※	IPv4- 経路のルート・リフレッシュ機能を使用します。
	Capability Code：128 Capability Value の AFI：1 ※	
グレースフル・リスタート	Capability Code：64 Capability Value の AFI：1 Capability Value の SAFI：1	グレースフル・リスタート機能を使用します。

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・リフレッシュ機能を使用できます。

また，ネゴシエーションの動作概念を次の図に示します。

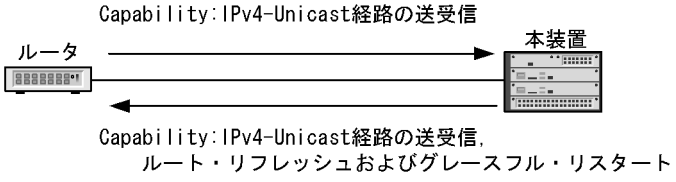
図 12-18　ネゴシエーションの動作概念

●お互いに同一のCapability情報を広告した場合の例



注　ピア間でIPv4-Unicast経路の送受信，ルート・リフレッシュおよびグレースフル・リスタート機能が使用できる。

●お互いに異なるCapability情報を広告した場合の例



注　ピア間でIPv4-Unicast経路の送受信機能だけが使用できる。

12.4.5 ルート・リフレッシュ

ルート・リフレッシュ機能は，変化が発生した経路だけを広告することを基本とする BGP4 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・リフレッシュ機能には，自装置側から経路を再広告する機能と BGP4 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，clear ip bgp コマンドで実行されます。

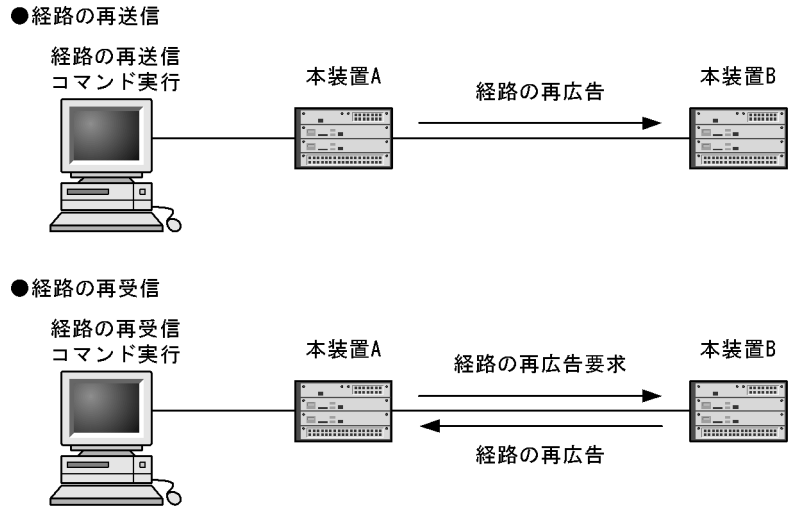
ルート・リフレッシュ機能を次の表に示します。

表 12-11 ルート・リフレッシュ機能

機能種別	経路種別	再広告方向
IPv4-Unicast 経路の再送信	IPv4 ユニキャスト経路	自装置側よりピアリングされた相手装置に経路を再広告します。
IPv4-Unicast 経路の再受信		ピアリングされた相手装置側より自装置に経路を再広告させます。

また，ルート・リフレッシュ機能の動作概念を次の図に示します。

図 12-19 ルート・リフレッシュ機能の動作概念



(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・リフレッシュ機能をサポートしている必要があります。ルート・リフレッシュ機能を使用するためには，BGP4 ピア確立時にルート・リフレッシュ機能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，相手装置側より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行いません。

本装置のルート・リフレッシュ機能は 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・リフレッシュ機能を使用するときは注意してください。

12.4.6　TCP MD5 認証

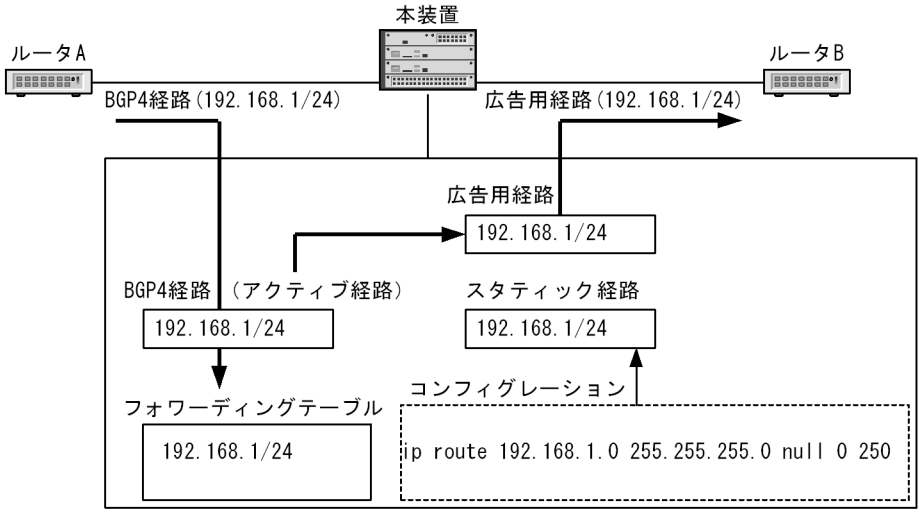
本装置は，RFC2385（TCP MD5 認証による BGP セッション保護）に準拠しています。TCP MD5 認証機能によって，BGP4 コネクションで受信した TCP セグメントが正当な送信元（ピア）から送信されてきたことを保証できます。TCP MD5 認証はピアごとに指定できます。ピアとの BGP4 コネクションに TCP MD5 認証を適用する場合，コンフィグレーションコマンド neighbor password で認証キーを指定します。なお，認証キーは該当するピア間で一致させる必要があります。一致していない場合は該当するピア間の BGP4 コネクションが確立しません。

12.4.7　BGP4 広告用経路生成

BGP4 広告用経路生成とは，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 で広告する機能です。パケットのフォワーディング用に実際の BGP4 経路を使用して，他装置広告用には生成した広告用経路を使用することによって，BGP4 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可能となります。この機能の使用例を次に示します。

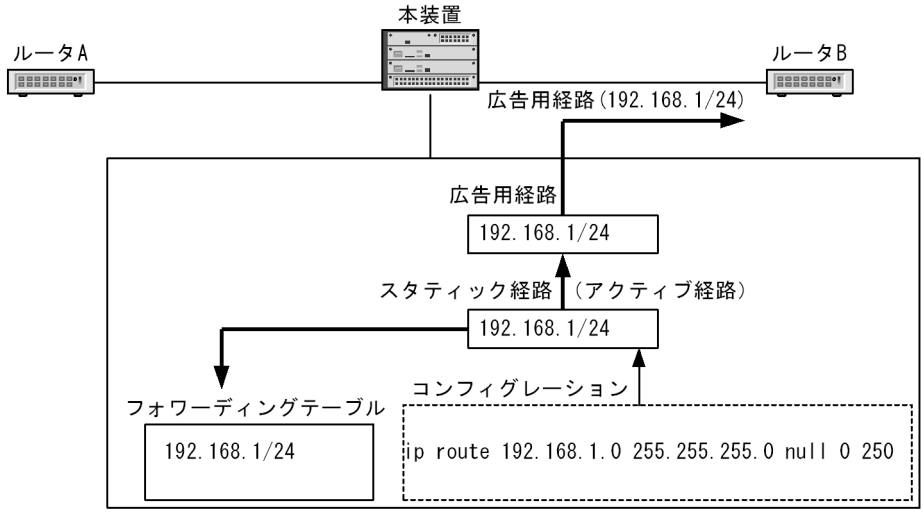
通常はルータ A から受信した BGP4 経路をフォワーディングテーブルに設定して，該当経路から生成された広告用経路をルータ B に広告します。

図 12-20　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 BGP4 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 12-21 広告用経路生成と広告（BGP4 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 BGP4 経路が使用され，かつルータ A から受信する BGP4 経路がフラップした場合でもルータ B への BGP4 経路広告に影響しません。

なお，広告用経路の生成はコンフィグレーションコマンド network を使用します。

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。BGP4 経路から生成された同じ宛先の広告用経路を BGP4 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。

12.4.8 ルート・フラップ・ダンプニング

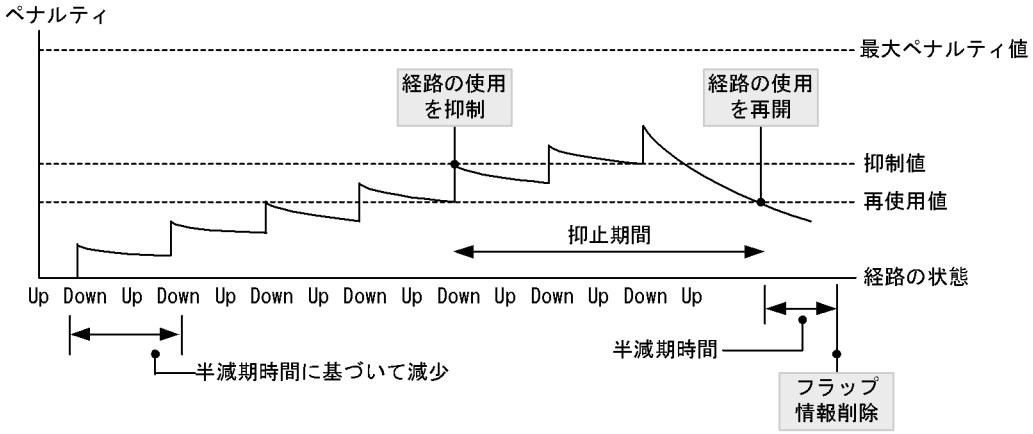
ルート・フラップ・ダンプニングは，経路情報が頻発してフラップするような場合に，一時的に該当する経路の使用を抑制して，ネットワークの不安定さを最小限にする機能です。なお，VRF では本機能をサポートしていません。ルート・フラップ・ダンプニング機能の構成要素を次の表に示します。

表 12-12 ルート・フラップ・ダンプニング機能の構成要素

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，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	ペナルティが本値以上の場合，該当する経路の使用を抑制します。
再使用値	ペナルティが本値以下の場合，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%)するために要する時間。
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・ダンプニングの動作概念を次の図に示します。

図 12-22　ルート・フラップ・ダンプニングの動作概念



12.4.9　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 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，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。

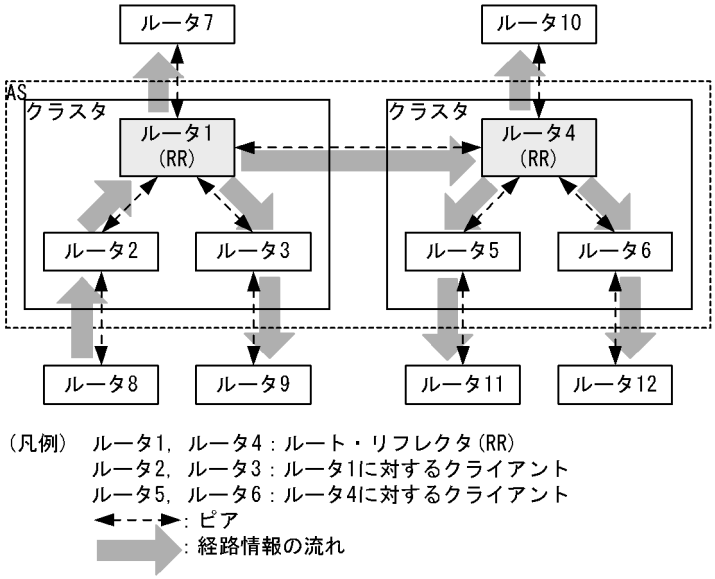
ルート・リフレクタはクラスタ内のクライアントから受信した UPDATE メッセージをすべてのノンクライアントおよび送信元のクライアントを含むクラスタ内のクライアントに配布します。また，ルート・リフレクタはノンクライアントから受信した UPDATE メッセージをクラスタ内のすべてのクライアントに配布します。これによって，クラスタ内のクライアントからノンクライアントに対する内部ピアとクラスタ内のクライアント間の内部ピアを不要とします。

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 12-23　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。

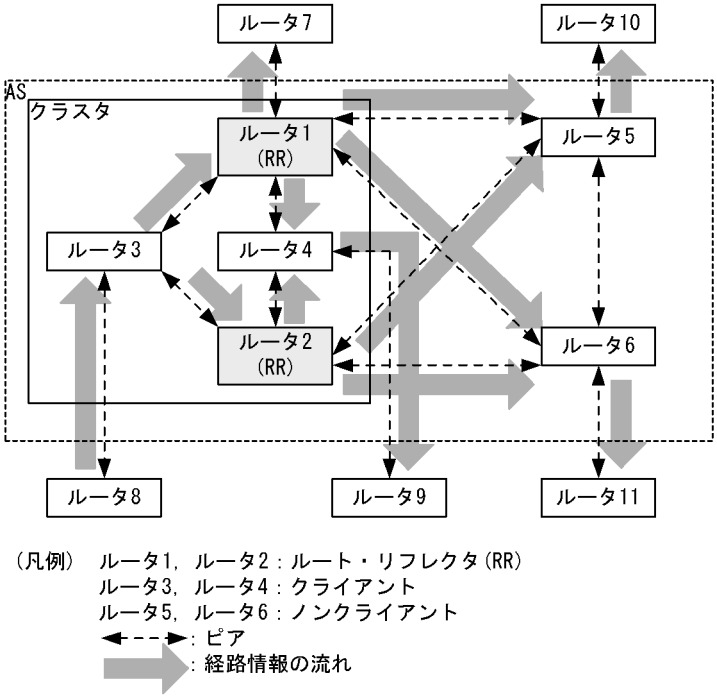
(3) クラスタ内に複数のルート・リフレクタを置く場合

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 12-23　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の通知ができるようにしています。なお，クラスタ内に複数のルート・リフレクタがある場合，それぞれのルート・リフレクタは同一のクラスタ ID（コンフィグレーションコマンド bgp cluster-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 12-24　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。

12.4.10　コンフェデレーション

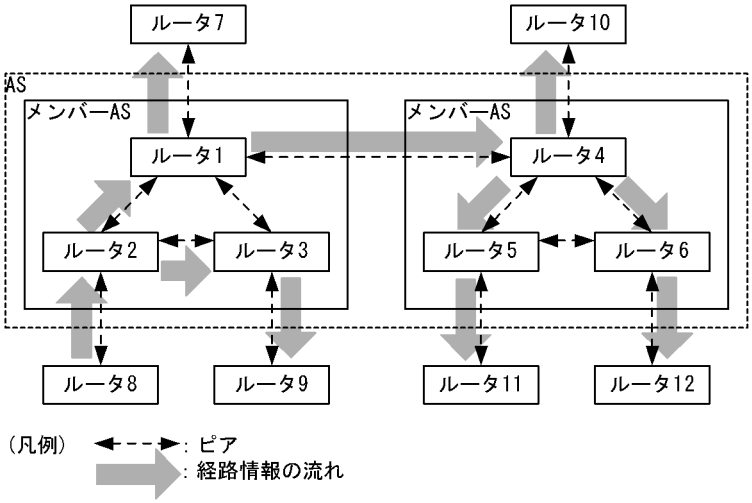
コンフェデレーションは，ルート・リフレクタと同様に AS 内でピアを形成する内部ピアの数を減らすためのもう一つの方法です。コンフェデレーションは，AS を複数のメンバー AS に分割して，AS 内のピア数を減らします。

(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しなければならず，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 12-25 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優先順位を次の表に示します。

表 12-13 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。
↑	LOCAL_PREF 属性の値が最も大きい経路を選択します。
	AS_PATH 属性の AS 数が最も短い経路を選択します。※1
	ORIGIN 属性の値で IGP，EGP，Incomplete の順で選択します。
	MED 属性の値が最も小さい経路を選択します。※2
	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。
	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。
	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。※3
↓	CLUSTER_LIST 属性長が最も短い経路を選択します。※4

優先順位	内容
低	学習元ピアのアドレスが小さい経路を選択します。※3

注※1
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。

注※2
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 を指定することで，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。

注※3
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 を指定することによって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。

注※4
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。

(3) コンフェデレーション構成での BGP 属性の取り扱い

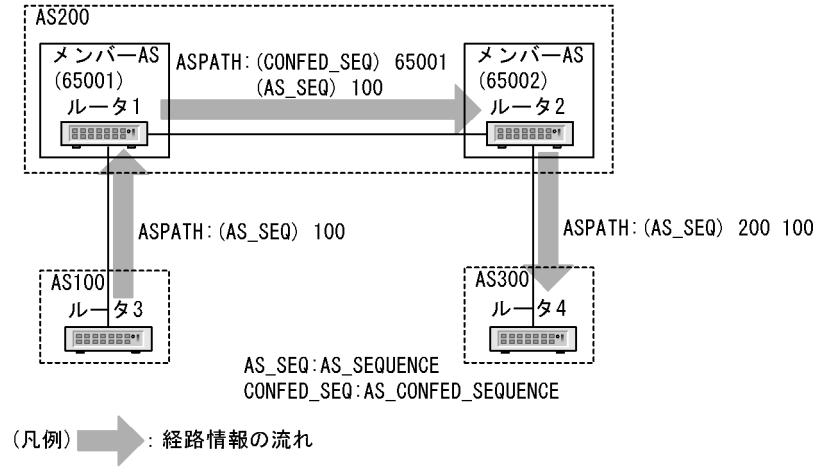
コンフェデレーション構成での BGP 属性の取り扱いは，通常構成（非コンフェデレーション構成）での BGP 属性の取り扱いとほぼ同様ですが，AS_PATH 属性，および COMMUNITIES 属性について一部動作が異なります。なお，メンバー AS 間ピアでの BGP 属性の取り扱いは，内部ピアでの BGP 属性の取り扱いと同様です。

(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 を取り除き，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 12-26 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 を取り除き，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

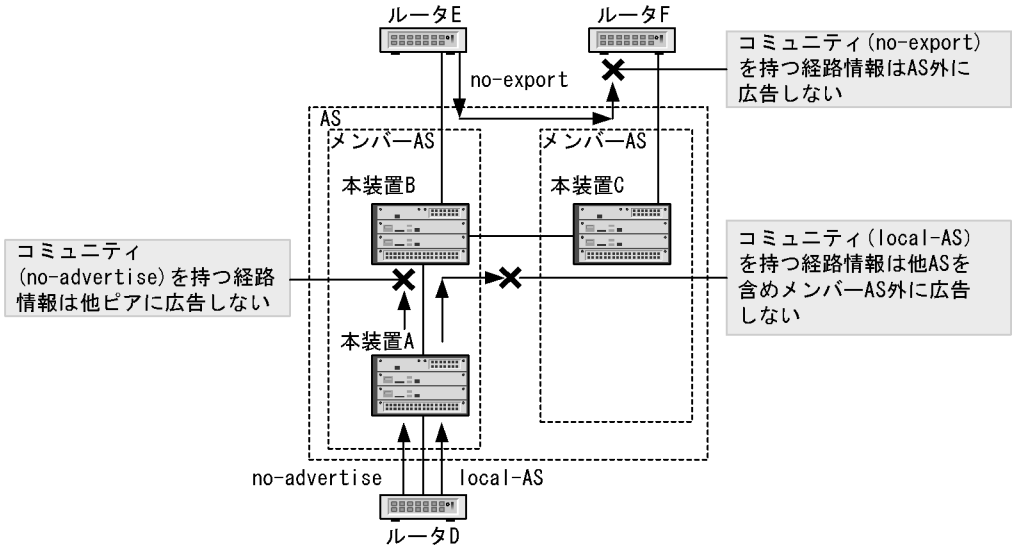
コンフェデレーション構成では RFC1997 で定義されるウェルノン・コミュニティについて，次のように取り扱います。そのほかのコミュニティの取り扱いは，通常構成と同様です。

RFC1997 で定義されるウェルノン・コミュニティを，「表 12-14 RFC1997 で定義されるウェルノン・コミュニティ」に示します。また，COMMUNITIES 属性を持つ経路情報の広告範囲を，「図 12-27 COMMUNITIES 属性を持つ経路情報の広告範囲」に示します。

表 12-14 RFC1997 で定義されるウェルノン・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。

図 12-27　COMMUNITIES 属性を持つ経路情報の広告範囲



12.4.11　グレースフル・リスタート

(1) 概要

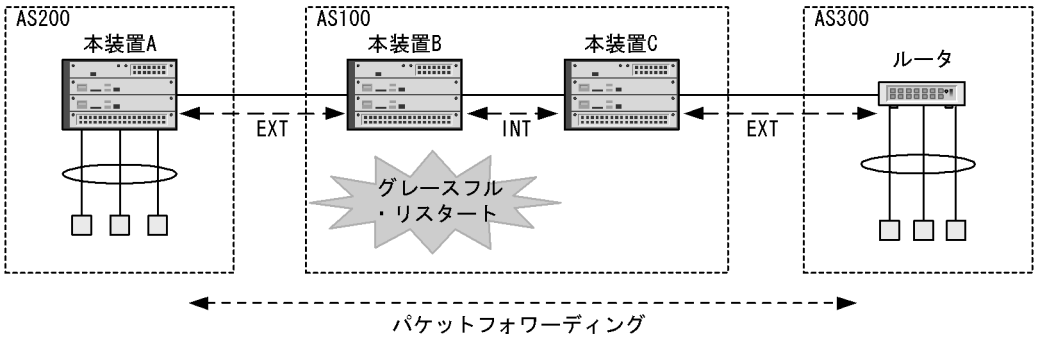
グレースフル・リスタートは，装置が系切替したり，運用コマンドなどによりルーティングプログラムが再起動したりしたときに，ネットワークから経路が消えることによる通信停止時間を短縮する機能です。

BGP4 では，グレースフル・リスタートによって BGP4 の再起動を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 12-28　グレースフル・リスタートの例



（凡例） INT：内部ピア（装置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によって装置アドレス宛ての経路情報を交換する

AS100 の本装置 B，本装置 C は装置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・リスタート機能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，本装置 B を経由するパケット・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。

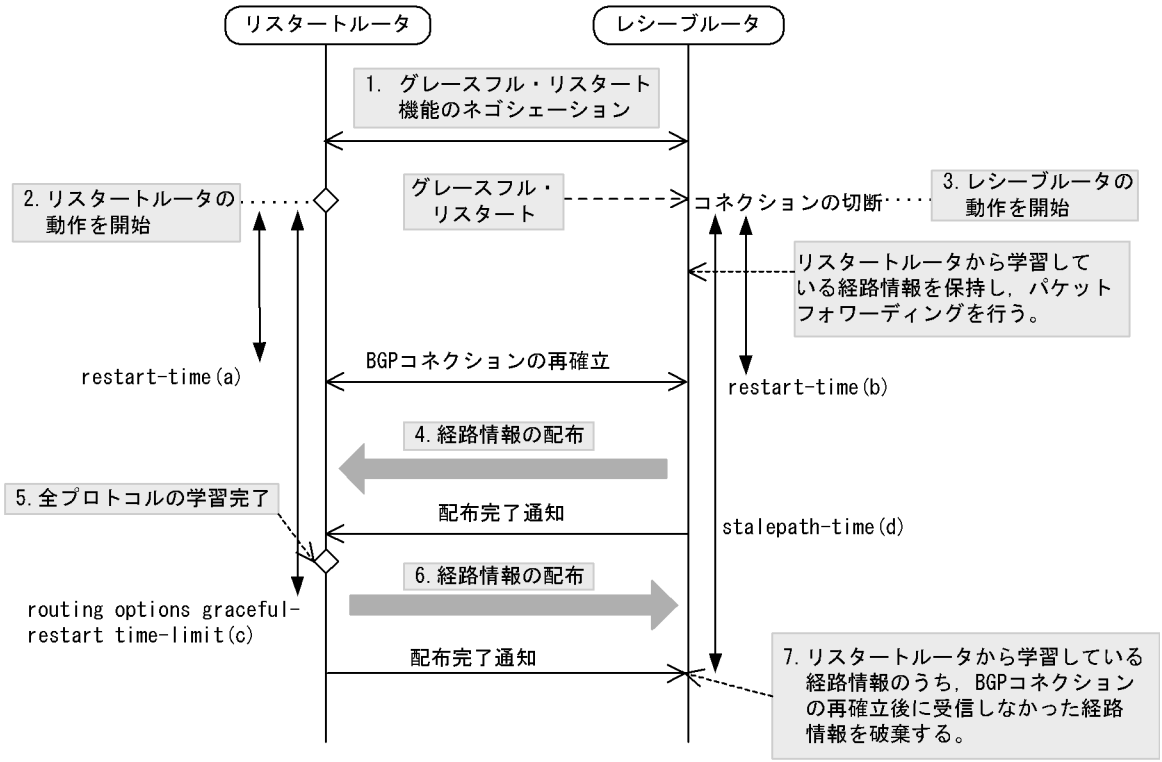
BGP4 のグレースフル・リスタートが正しく動作するための条件を次に示します。次の条件を満たさない場合，通常のリスタート動作となって通信が停止します。

- 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・リスタート機能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

BGP4 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 12-29 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・リスタート機能のネゴシエーションを行い，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，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 BGP4 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。

- 装置が系切替したとき。
- 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 12-29　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当該レシーブルータからの経路情報配布を待たずに，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当該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 12-29　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。

- コンフィグレーションコマンド bgp graceful-restart restart-time を，系切替所要時間 + コネクション確立時間よりも長く設定する。
  BGP ピアのコネクションを再確立するには，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，系切替所要時間 + コネクション確立時間よりも長く設定してください。ピアのコネクション確立にかかる時間は，構成によって異なりますが，目安として 30 秒を用いてください。
- 装置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・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。
  BGP ピアのコネクションの再確立が最も遅い場合は，コンフィグレーションコマンド bgp graceful-restart restart-time の経過後に BGP ピアからの経路学習を開始します。リスタートルータが経路配布を開始する前に経路学習・フォワーディングテーブルの更新が完了するようにするため，コンフィグレーションコマンド routing options graceful-restart time-limit の指定は restart-time より 60 秒程度長い時間を設定してください。なお，目安の設定値は，経路数および隣接ピア数に依存します。

また，BGP 経路情報の NextHop 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

BGP4 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 BGP4 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 BGP4 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 12-29　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・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・リスタート機能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 12-29　グレースフル・リスタートのシーケンス」の (d))。

各パラメータを設定する場合は，通常は次のようにしてください。

- stalepath-time はリスタートルータの全プロトコルの学習完了時間より大きい値を設定する。
  全プロトコルの学習完了時間は，リスタートルータが経路配布を開始する時間の上限となるので，経路配布が最も遅い場合は，全プロトコルの学習完了時間の経過後にレシーブルータへ経路配布を開始します。レシーブルータで，経路学習およびフォワーディングテーブルの更新後に，古い経路情報が削除されるようにするため，stalepath-time の指定は，リスタートルータの全プロトコルの学習完了時間より 120 秒程度長い時間を設定してください。なお，設定値の目安は，経路数およびリスタートルータの隣接ピア数に依存します。

(c) レシーブルータ機能が失敗するケース

BGP4 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 BGP4 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

1. 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，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。
2. 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，当該 IGP についてもグレースフル・リスタートの機能を設定してください。
3. エクストラネット使用時のグレースフル・リスタートについて**【OP-NPAR】**
   リスタートルータとして機能する本装置で VRF 間の経路交換によるエクストラネットを使用している場合，グレースフル・リスタート実施時にレシーブルータに対する経路配布処理が通常より 30 秒長く掛かります。このため，レシーブルータでの経路情報保持時間の上限値（コンフィグレーションコマンド bgp graceful-restart stalepath-time）を通常より 30 秒長く設定してください。

12.4.12 BGP4 学習経路数制限

BGP4 学習経路数制限とは，ピアから学習する BGP4 経路の数を制限し，大量の BGP4 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 BGP4 経路の数が設定した閾値を超えた場合，警告の運用メッセージを出力します。さらに，上限値を超えた場合は，警告の運用メッセージを出力した後でピアを切断します。この機能によるピア切断後は，設定した期間の経過，または運用コマンド clear ip bgp でピアを再び接続します。また，学習経路数が上限値を超えても，警告の運用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。

12.5 拡張機能のコンフィグレーション

12.5.1 BGP4 ピアグループのコンフィグレーション

(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 12-15 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）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）を設定します。ピアグループに設定したピアの AS 番号やオプション，広告フィルタなどが該当ピアに適用されます。

[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，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，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。

12.5.2 コミュニティのコンフィグレーション

(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 12-16 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用い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用い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用い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用いる経路フィルタを指定します。

コマンド名	説明
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　14. 経路フィルタリング（IPv4 ／ IPv6 共通）」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 属性を付加する場合，該当するピアにコンフィグレーションコマンド neighbor send-community 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 属性を付加す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，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
   全ピアの学習経路フィルタと全ピアの広告経路フィルタを設定します。

(3) フィルタ設定の運用への反映

[設定のポイント]

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経路フィルタを運用に反映させるには運用コマンド clear ip bgp を使用します。

[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させます。

12.5.3 BGP4 マルチパスのコンフィグレーション

(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 12-17 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 に all-as パラメータを指定する場合はあらかじめ bgp always-compare-med 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。本例では 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。

12.5.4 TCP MD5 認証のコンフィグレーション

(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 12-18 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 認証はコンフィグレーションコマンド neighbor password 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。

12.5.5 BGP4 広告用経路生成のコンフィグレーション

(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 12-19 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 の広告用経路を生成することを設定します。

(2) BGP4 広告用経路生成の設定

[設定のポイント]

BGP4 広告用経路を生成するにはコンフィグレーションコマンド network を使用します。network コ

マンドで生成した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 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 192.168.1.100
   (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)# network 192.169.10.0/24**
   (config-router)# exit
   ルーティングテーブルに 192.169.10.0/24 の経路がある場合に 192.169.10.0/24 の BGP4 広告用経路を生成します。

3. **(config)# route-map ADV_NET permit 10**
   (config-route-map)# match route-type local
   (config-route-map)# exit
   生成した BGP4 広告用経路を指定します。

4. **(config)# route-map ADV_NET deny 20**
   (config-route-map)# match protocol bgp
   (config-route-map)# exit
   BGP プロトコルを指定します。

5. **(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 のピアへ生成した 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。

6. **(config)# route-map DENY_NET deny 10**
   (config-route-map)# match route-type local
   (config-route-map)# exit
   生成した BGP4 広告用経路を指定します。

7. **(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 のピアへ生成した BGP4 広告用経路を広告しないことを指定します。

(3) フィルタ設定の運用への反映

［設定のポイント］

生成した BGP4 広告用経路を広告するには運用コマンド clear ip bgp を使用し，フィルタを運用に反映させます。

[コマンドによる設定]

1. **# clear ip bgp * out**
   BGP4 広告用経路を指定した経路フィルタを運用に反映させます。

12.5.6 ルート・フラップ・ダンプニングのコンフィグレーション

(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 12-20 コンフィグレーションコマンド一覧

コマンド名	説明
bgp 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，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 を設定します。

[コマンドによる設定]

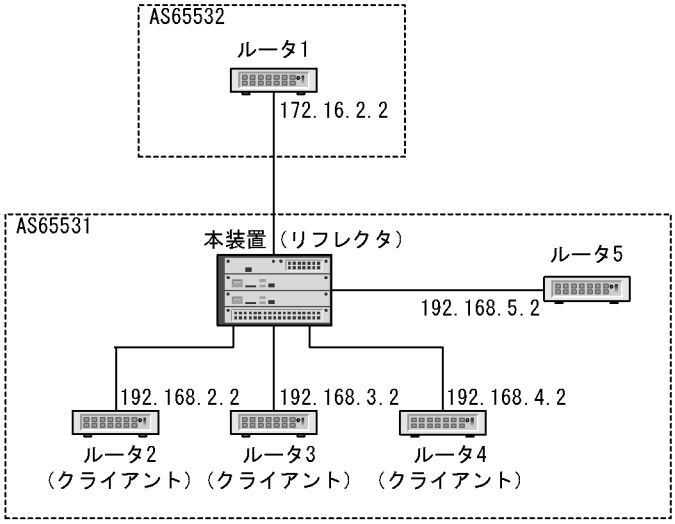
1. **(config)# router bgp 65531**
   (config-router)# bgp router-id 192.168.1.100
   (config-router)# neighbor 172.16.2.2 remote-as 65532
   (config-router)# neighbor 172.17.2.2 remote-as 65533
   BGP4 ピアを設定します。

2. **(config-router)# bgp dampening**
   ルート・フラップ・ダンプニングを適用します。

12.5.7 ルート・リフレクション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 12-30 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 12-21 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の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]

コンフィグレーションコマンド bgp client-to-client reflection はデフォルトで有効になっている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 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，ルータ 5 を内部ピアとして BGP4 ピアを設定します。

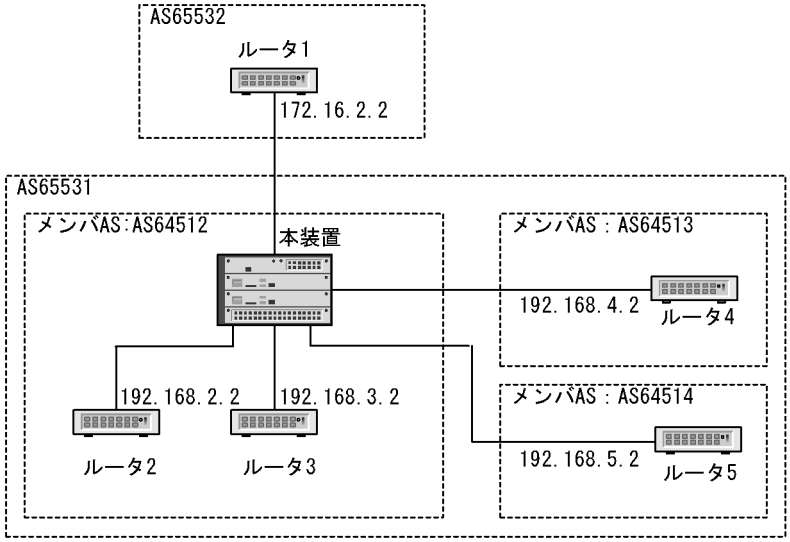
2. **(config-router)# bgp cluster-id 10.1.2.1**
クラスタ ID を設定します。

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，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。

12.5.8 コンフェデレーション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 12-31 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 12-22 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/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 で指定し，接続するほかのメンバー AS 番号は config-router モードで bgp confederation peers 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**
   接続する他のメンバー 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，ルータ 3 を内部ピア，ルータ 4，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。

12.5.9 グレースフル・リスタートのコンフィグレーション

(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 12-23 コンフィグレーションコマンド一覧

コマンド名	説明
bgp graceful-restart mode	グレースフル・リスタート機能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　8. ルーティングオプション（IPv4）」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 コマンドを設定後に設定します。
- 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 コマンドを設定後に設定します。

[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。

12.5.10 BGP4 学習経路数制限のコンフィグレーション

(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 12-24　コンフィグレーションコマンド一覧

コマンド名	説明
neighbor 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 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，警告の運用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。

12.6 拡張機能のオペレーション

12.6.1 BGP4 ピアグループの確認

(1) 運用コマンド一覧

BGP4 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 12-25 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。

(2) BGP4 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の確認は show ip bgp コマンドで peer-group パラメータを指定します。

図 12-32 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 2006/07/17 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         2006/07/16 18:42:26  Established
172.16.3.3      65531  51         63         2006/07/16 12:42:31  Established
```

(3) BGP4 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を表示するには show ip bgp コマンドで neighbors パラメータを指定します。

図 12-33 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 2006/07/17 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 BGP4 ピアグループの確認

ピアが所属するピアグループの確認は show ip bgp コマンドで neighbors パラメータ，および <Peer Address>，<Host name> パラメータを指定します。

図 12-34 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 2006/07/17 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: 2006/07/16 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
```

1. ピアグループ INTERNAL-GROUP に所属しています。

12.6.2 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 12-26 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。
show ip 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を表示する場合は show ip bgp コマンドの community パラメータ指定を使用します。

図 12-35 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 2006/03/20 21:00:18 UTC
Local AS: 65531, Local Router ID: 192.168.1.100
Status Codes: d dampened, * valid, > active, S Stale
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を表示する場合は show ip bgp コマンドの route パラメータ指定を使用します。

図 12-36 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 2006/03/20 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: * valid, > active
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フィルタリング結果は運用コマンド show ip bgp を使用して表示します。

図 12-37 show ip bgp コマンドの実行結果

```
> show ip bgp
Date 2006/03/20 21:10:09 UTC
Local AS: 65531, Local Router ID: 192.168.1.100
Status Codes: * valid, > active
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
*> 192.169.10/24       192.168.2.2     -      100       0      i
*> 192.169.20/24       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 BGP4 経路の COMMUNITIES 属性は運用コマンド show ip bgp の advertised-routes パラメータ指定を使用します。

図 12-38 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 192.169.10/24
Date 2006/03/20 21:10:25 UTC
BGP Peer: 172.16.2.2    , Remote AS: 65532
Local AS: 65531, Local Router ID: 192.168.1.100
Route 192.169.10/24
*> 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
Route 192.169.10/24
*> 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
```

12.6.3 BGP4 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 12-27 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の経路を表示します。
show ip bgp	BGP4 プロトコルに関する情報を表示します。

(2) BGP4 マルチパスの表示

マルチパスの設定は運用コマンド show ip route を使用して表示します。

図 12-39 show ip route コマンドの実行結果

```
> show ip route
Date 2006/03/20 21:40:39 UTC
Total: 19 routes
Destination       Next Hop        Interface     Metric   Protocol  Age
10.10/16          172.17.2.2      VLAN0006      -/-      BGP       33m 31s  … 1
                  172.16.2.2      VLAN0005      -        -         -
10.20/16          172.17.2.2      VLAN0006      -/-      BGP       33m 31s  … 2
                  172.16.2.2      VLAN0005      -        -         -
127/8             ----            loopback0     0/0      Connected 42m 45s
127.0.0.1/32      127.0.0.1       loopback0     0/0      Connected 42m 45s
172.17/16         172.17.2.2      VLAN0006      0/0      Connected 42m 43s
172.17.2.1/32     172.17.2.2      VLAN0006      0/0      Connected 42m 43s
172.16/16         172.16.2.2      VLAN0005      0/0      Connected 42m 43s
172.16.2.1/32     172.16.2.2      VLAN0005      0/0      Connected 42m 43s
172.10/16         172.17.2.2      VLAN0006      -/-      BGP        3s      … 3
                  172.16.2.2      VLAN0005      -        -         -
172.20/16         172.17.2.2      VLAN0006      -/-      BGP        3s      … 4
                  172.16.2.2      VLAN0005      -        -         -
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。

12.6.4 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 12-28 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。

(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運用コマンド show ip bgp の neighbors と detail パラメータ指定を使用して表示します。

図 12-40　show ip bgp コマンド（neighbors detail パラメータ指定）の実行結果

```
> show ip bgp neighbor detail
Date 2006/03/17 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: 2006/03/17 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
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: 2006/03/17 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
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: 2006/03/17 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
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: 2006/03/17 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
>
```

1. IPv4-Uni:「IPv4-Unicast 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-Unicast 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-Unicast 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。

12.6.5 ルート・リフレッシュ機能の確認

(1) 運用コマンド一覧

ルート・リフレッシュ機能の運用コマンド一覧を次の表に示します。

表 12-29 運用コマンド一覧

コマンド名	説明
clear ip bgp	BGP4 セッション，または 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 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 bgp	BGP4 プロトコルに関する情報を表示します。

(2) ルート・リフレッシュ機能のネゴシエーション確認

最初に運用コマンド show ip bgp の neighbors パラメータ指定で BGP4 経路の再広告要求を行う BGP4 ピア間でルート・リフレッシュ機能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行いません。

図 12-41 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 2006/03/17 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: 2006/03/17 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
```

1. ルート・リフレッシュ機能のネゴシエーションが成立しています。

(3) BGP4 経路の再広告要求と再広告

全 BGP4 ピアに対して BGP4 経路の再広告要求と再広告を行う場合は，運用コマンド clear ip bgp の * both パラメータを使用します。

図 12-42 clear ip bgp コマンドの実行結果

```
#clear ip bgp * both
```

(4) BGP4 経路再学習と再広告の確認

ルート・リフレッシュ機能による BGP4 経路の再学習と再広告を確認する場合は show ip bgp コマンドの neighbors パラメータ指定を使用します。

図 12-43 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 2006/03/17 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: 2006/03/17 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
```

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]

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・リフレッシュ機能（「12.4.5 ルート・リフレッシュ」参照）の両方を実行します。ルート・リフレッシュ機能の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・リフレッシュ要求は行いませんが，経路フィルタの変更は反映します。

12.6.6 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 12-30 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。

(2) TCP MD5 認証の確認

TCP MD5 認証は運用コマンド show ip bgp コマンドで neighbor と detail パラメータを指定して表示します。

図 12-44 show ip bgp コマンド（neighbor detail パラメータ指定）の実行結果

```
> show ip bgp neighbor detail
Date 2006/03/07 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: 2006/03/07 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

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: 2006/03/07 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
```

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ログメッセージを確認してください。

12.6.7 BGP4 広告用経路生成の確認

(1) 運用コマンド一覧

BGP4 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 12-31 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 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。

(2) BGP4 広告用経路の確認

(a) 生成した広告用経路の表示

生成した BGP4 広告用経路は運用コマンド show ip bgp で表示します。本例では 173.16/16 と 192.169.10/24 が生成した BGP4 広告用経路です。

図 12-45 show ip bgp コマンドの実行結果

```
> show ip bgp
Date 2006/03/20 22:43:26 UTC
Local AS: 65531, Local Router ID: 192.168.1.100
Status Codes: * valid, > active
Origin Codes: i - IGP, e - EGP, ? - incomplete
   Network             Next Hop        MED    LocalPref Weight Path
*  173.16/16           ----            -      100       0      i
*  192.169.10/24       ----            -      100       0      i
```

(b) 広告用経路の広告表示

生成した BGP4 広告用経路が広告されていることを確認する場合は運用コマンド show ip bgp コマンドの advertised-routes パラメータ指定を使用します。

図 12-46 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 173.16/16
Date 2006/03/20 22:44:54 UTC
BGP Peer: 172.16.2.2    , Remote AS: 65532
Local AS: 65531, Local Router ID: 192.168.1.100
Route 173.16/16
*  Next Hop ----
     MED: -, LocalPref: -, Type: Internal route
     Origin: IGP
     Path: 65531
     Next Hop Attribute: 172.16.2.1

> show ip bgp advertised-routes 192.169.10/24
Date 2006/03/18 22:44:58 UTC
BGP Peer: 172.16.2.2     , Remote AS: 65532
Local AS: 65531, Local Router ID: 192.168.1.100
Route 192.169.10/24
*  Next Hop ----
     MED: -, LocalPref: -, Type: Internal route
     Origin: IGP
     Path: 65531
     Next Hop Attribute: 172.16.2.1
```

12.6.8 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・ダンプニング機能の運用コマンド一覧を次の表に示します。

表 12-32 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。
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・ダンプニングにより抑止されている経路を表示する場合は運用コマンド show ip bgp の dampend-routes パラメータ（グローバルネットワークだけ）を指定します。

図 12-47 show ip bgp コマンド（dampend-routes パラメータ指定）の実行結果

```
>show ip bgp neighbor 172.16.2.2 dampened-routes
Date 2006/01/17 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・ダンプニングにより使用が抑止されている経路

フラップ状態を表示する場合は運用コマンド show ip bgp の flap-statistics パラメータ（グローバルネットワークだけ）を指定します。

図 12-48 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 2006/01/17 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
>
```

12.6.9 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・リフレクション機能の運用コマンド一覧を次の表に示します。

表 12-33 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。
show ip 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・リフレクション・クライアントを表示する場合は運用コマンド show ip bgp の neighbors パラメータと detail パラメータを指定します。

図 12-49　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 2006/03/17 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: 2006/03/17 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

BGP Peer: 192.168.3.2    , Remote AS: 65531
Remote Router ID: 192.168.1.103
    BGP Status: Established         Holdtime: 180  , Keepalive: 60
    Established Transitions: 1      Established Date: 2006/03/17 15:50:43
    BGP Version: 4                  Type: Internal RRclient             …1
    Local Address: 192.168.3.1      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

BGP Peer: 192.168.4.2    , Remote AS: 65531
Remote Router ID: 192.168.1.104
    BGP Status: Established         Holdtime: 180  , Keepalive: 60
    Established Transitions: 1      Established Date: 2006/03/17 15:50:30
    BGP Version: 4                  Type: Internal RRclient             …1
    Local Address: 192.168.4.1      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 Refresh>
      Send   : <IPv4-Uni Refresh Refresh(v)>
      Receive: <IPv4-Uni Refresh Refresh(v)>
    Password: UnConfigured

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: 2006/03/17 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: <IPv4-Uni Refresh Refresh(v)>
      Send   : <IPv4-Uni Refresh Refresh(v)>
      Receive: <IPv4-Uni Refresh Refresh(v)>
```

```
    Password: UnConfigured
>
```

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を表示する場合は運用コマンド show ip bgp の advertised-routes パラメータを指定します。

図 12-50 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 2006/01/17 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
192.169.10/24        192.168.2.2     120    100       i
192.169.20/24        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
192.169.10/24        192.168.2.2     120    100       65532 i
192.169.20/24        192.168.2.2     100    100       65532 i
```

12.6.10 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機能の運用コマンド一覧を次の表に示します。

表 12-34 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。

(2) コンフェデレーションの確認

コンフェデレーションを表示する場合は運用コマンド show ip bgp の neighbors パラメータと detail パラメータを指定します。

図 12-51　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 2006/03/17 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: 2006/03/17 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

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: 2006/03/17 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

Confederation ID: 65531, Member AS: 64512                                   …1
BGP Peer: 192.168.5.2    , Remote AS: 64514                                 …2
Remote Router ID: 192.168.1.104
    BGP Status: Established         Holdtime: 180  , Keepalive: 60
    Established Transitions: 1      Established Date: 2006/03/17 15:50:30
    BGP Version: 4                  Type: ConfedExt                        …3
    Local Address: 192.168.5.1      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

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: 2006/03/17 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: <IPv4-Uni Refresh Refresh(v)>
```

```
      Send   : <IPv4-Uni Refresh Refresh(v)>
      Receive: <IPv4-Uni Refresh Refresh(v)>
    Password: UnConfigured
>
```

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。

12.6.11 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・リスタート機能の運用コマンド一覧を次の表に示します。

表 12-35 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 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 8. 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を表示する場合は運用コマンド show ip bgp の neighbors パラメータと detail パラメータを指定します。

図 12-52 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 2006/04/17 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: 2006/04/17 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
      Restart Status : Finished    2006/04/16 18:41:35
      Receive Status : Finished    2006/04/16 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

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: 2006/04/17 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
    Graceful Restart: Both                                          …1
      Restart Status : Finished    2006/04/16 18:43:40
      Receive Status : Finished    2006/04/16 15:49:36
       Stalepath-Time: 30
    BGP Message  UpdateIn   UpdateOut  TotalIn    TotalOut
                 0          0         3          5
   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)>
    Password: UnConfigured
```

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・リスタート機能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運用コマンド show ip bgp で表示します。

図 12-53　show ip bgp コマンドの実行結果

```
> show ip bgp
Date 2006/01/17 19:12:23 UTC
Local AS: 65531, Local Router ID: 192.168.1.100
Status Codes: * valid, > active , S Stale
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
*> 192.169.10/24    192.168.2.2  -     100       10           i
*> 192.169.20/24    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

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を表示する場合は運用コマンド show graceful-restart unicast を使用します。

図 12-54 show graceful-restart unicast コマンドの実行結果

```
>show graceful-restart unicast
Date 2006/04/17 12:00:00 UTC
Status: Completed
Graceful Restart Time Limit: 180s
Start Time: 2006/04/08 17:01:23
End Time  : 2006/04/08 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)
```

12.6.12 BGP4 学習経路数制限の確認

(1) 運用コマンド一覧

BGP4 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 12-36 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。
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 学習経路数制限により切断しているピアを再接続します。

(2) BGP4 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

BGP4 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）の確認は運用コマンド show ip bgp で neighbors パラメータ，および <As>，<Peer Address>，<Host name> または detail パラメータを指定します。

図 12-55 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 2006/03/17 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: 2006/03/16 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
 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: 2006/03/16 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
```

1. 2006/03/16 18:42:26 にピアを切断しています。
2. 学習経路数制限により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. 当該ピアから学習経路数の上限値 1000 に対して 942 経路学習しています。

(3) BGP4 学習経路数制限により切断した BGP4 セッションの再接続

BGP4 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 BGP4 セッションは，運用コマンド clear ip bgp で＊または <Peer Address>，<Host Name> パラメータを指定して再接続します。

［コマンドによる BGP4 セッション再接続］

1. **# clear ip bgp 172.16.2.2**
   BGP4 学習経路数制限により切断している相手側アドレス 172.16.2.2 との BGP4 セッションを再接続します。

13 経路フィルタリング（IPv4）

この章では，経路フィルタリング（IPv4）の解説と操作方法について説明します。

13.1 経路フィルタリング解説

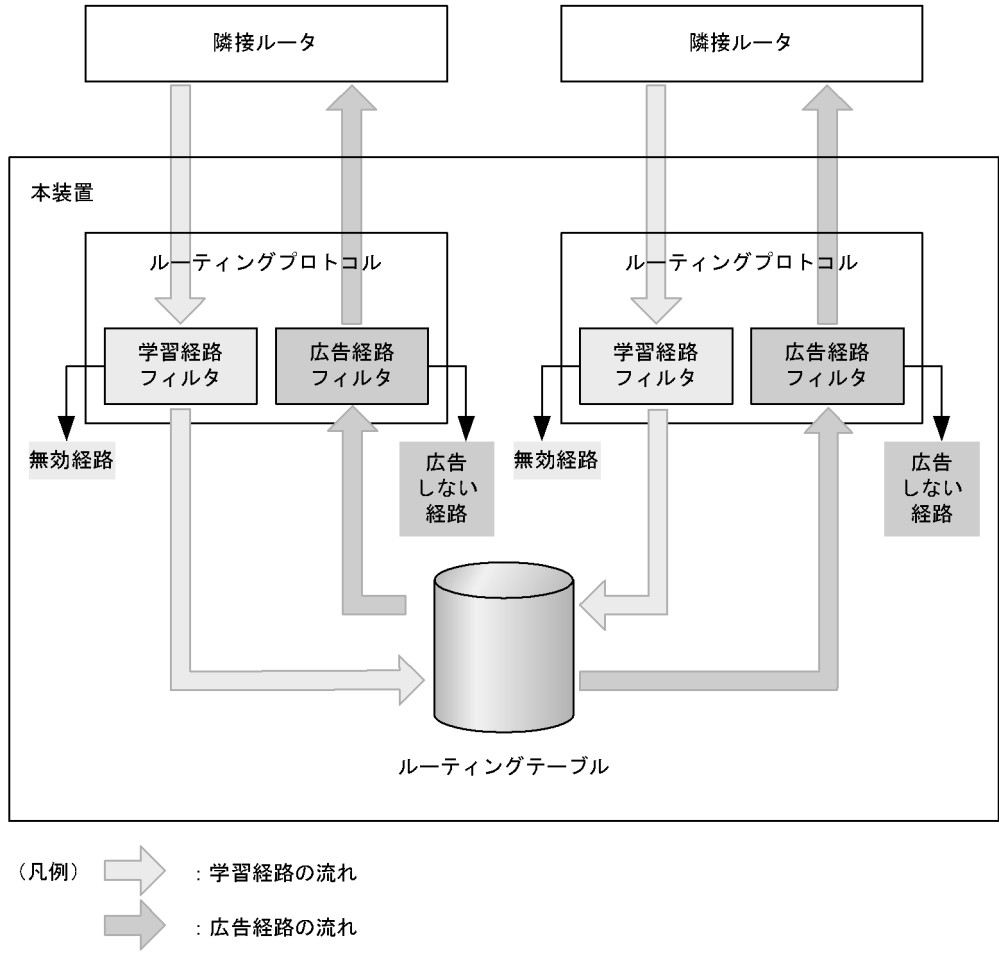
13.1.1 経路フィルタリング概要

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 13-1 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。

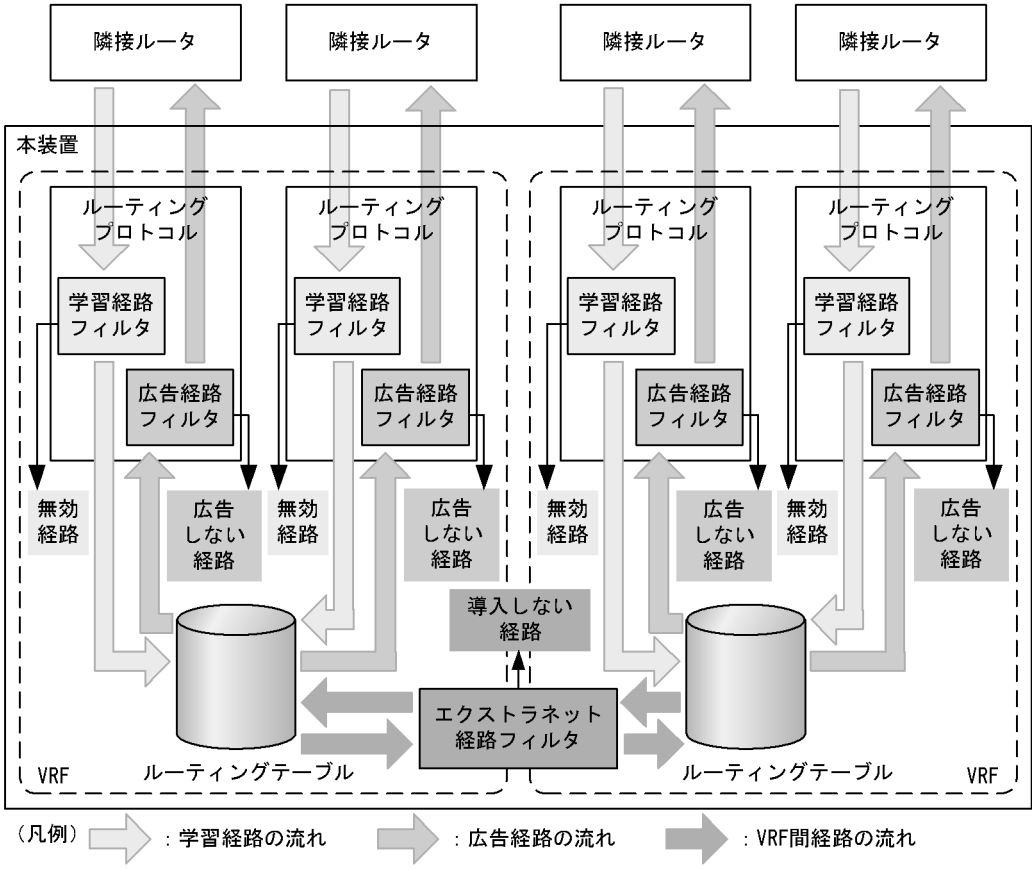
(2) エクストラネットの経路フィルタリング【OP-NPAR】

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行い，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 13-2　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。

13.1.2　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

クだけを条件にフィルタする prefix-list・access-list 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。そのほかに，BGP4 経路属性を条件とする ip as-path access-list と ip community-list があります。ip as-path access-list と ip community-list は，route-map から呼び出して使います。

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，フィルタを多数設定できます。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することが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 とみなします。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

ip 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。ip prefix-list 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，一致したものとみなします。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，一致したものとみなします。ip prefix-list の比較例を次の表に示します。

表 13-1　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

ip prefix-list は，route-map の match ip address から経路宛先条件として引用することもできます。比較方法は単体で経路フィルタとして使用した場合と同じです。

ip prefix-list は，route-map の match ip route-source から経路学習元ルータ条件として引用することもできます。この場合，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。

（b） ip access-list standard

ip access-list standard と access-list の名前 1 ～ 99 または 1300 ～ 1999 は，主にパケットやログインアクセスなど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使うこともできます。

ip access-list standard 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のアドレス部分とアドレス条件を比較します。

ip access-list standard は，route-map の match ip address から経路宛先条件として引用することもできます。比較方法は単体で経路フィルタとして使用した場合と同じです。

ip access-list standard は，route-map の match ip route-source から経路学習元ルータ条件として引用することもできます。この場合，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 と access-list の名前 100 ～ 199 または 2000 ～ 2699 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使うこともできます。

ip access-list extended 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 は，route-map の match ip address から経路宛先条件として引用することもできます。比較方法は単体で経路フィルタとして使用した場合と同じです。

ip access-list extended は，route-map の match ip route-source から経路学習元ルータ条件として引用することもできます。この場合，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，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。

（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することもできます。

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，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 でタグ値を変更し，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 13-2　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	prefix-list や access-list の識別子を条件として指定し，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，一致したとみなします。deny の場合，一致しないとみなします。	match ip address ip prefix-list ip access-list
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，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	prefix-list や access-list の識別子を条件として指定し，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，一致したとみなします。deny の場合，一致しないとみなします。 学習元隣接ルータのアドレスがあるのは，RIP 経路と 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することはありません。	match ip route-source ip access-list ip prefix-list
インタフェース	インタフェースを条件として指定し，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 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，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 とみなします。	match tag
AS_PATH 属性	ip as-path access-list の識別子を条件に指定し，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，一致したとみなします。deny の場合，一致しないとみなします。 AS_PATH 属性のない経路では，長さ 0 の AS PATH とみなします。	match as-path ip as-path access-list
COMMUNITIES 属性	ip community-list の識別子を条件に指定し，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，一致したとみなします。deny の場合，一致しないとみなします。 COMMUNITIES 属性のない経路では，コミュニティなしとみなします。	match community ip community-list
ORIGIN 属性	値 IGP・EGP・INCOMPLETE を条件に指定し，経路の ORIGIN 属性と比較します。 ORIGIN 属性のない経路では，値 IGP とみなします。	match origin
経路種別	OSPF の経路種別や local (network (BGP) 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，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，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である場合，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みなします。

表 13-3 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	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 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 属性宛の経路のメトリック引き継ぎ）
MED 属性		
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 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 番号を追加することだけ可能です。ピアの送信側 AS 番号を追加します。 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 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 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。 OSPF の広告経路フィルタリングで使用します。	set metric-type

(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，BGP4 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います。

(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，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。正規表現については，「(d) 正規表現」を参照してください。

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，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，一致したとみなします。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，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。正規表現については，「(d) 正規表現」を参照してください。

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，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 13-4 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。正規表現を使うことで，繰り返しなどのパターンを書くことができます。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，数字・小文字アルファベット・大文字アルファベット・記号（ただし，ダブルクォーテーション「"」は除く）などの通常文字と，特殊文字です。通常文字，「¥」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 13-5 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］を入力後［?］を入力してください）。
^	文字列の先頭を意味します。

特殊文字	パターン
$	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マニュアル「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 集合までネスト可能です。
|	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の結合優先順位を次の表に示します。

表 13-6　正規表現使用文字の結合優先順位

優先順位	文字
高	( )
↑	* + ?
↓	通常文字 . [ ] ^ $
低	|

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際には，正規表現の前後をダブルクォーテーション（"）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_"
```

13.1.3　RIP

（1）RIP 学習経路フィルタリング

RIP 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入りません。

（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。RIP 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。

経路を学習したら，指定したフィルタを表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，その学習経路はルーティ

ングテーブルに入りません。

表 13-7 RIP 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>	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>	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。

(b) 学習経路フィルタリングで変更可能な経路属性

RIP の学習経路フィルタリングで変更可能な属性を次の表に示します。

変更したメトリック値は，RIP の優先経路選択に用います。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用います。

表 13-8 RIP 学習経路フィルタリングで変更可能な経路の属性

属性	デフォルト値
ディスタンス値	distance (RIP) 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。

注意

- メトリック値の変更方法に，加算以外の方法を使わ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，パケットを正しく転送できなくなることがあるからです。
- メトリック値を 16 以上に変更するように設定することもできます。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後で適用します。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。
- タグ値は，経路を学習した RIP のバージョンにかかわらず変更できます。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。
  また，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，上位のビットを切り捨てます。

(2) RIP 広告経路フィルタリング

RIP では，ルーティングテーブルの優先経路だけを広告できます。ただし，スプリットホライズンおよび 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が広告対象になります。

注意

OSPF 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可能な経路属性

RIP の広告経路フィルタリングで変更可能な属性を次の表に示します。

表 13-9 RIP 広告経路フィルタリングで変更可能な経路の属性

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 で指定した値を用います。 default-metric 未設定時は 1 を用います。
	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 を用います。 inherit-metric 未設定時は default-metric で指定した値を用います。 inherit-metric も default-metric も設定していないときは 16 を用います。
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，加算以外のメトリック値変更方法を使わ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，パケットを正しく転送できなくなることがあるからです。
- 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することもできます。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。また，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，上位のビットを切り捨てます。

(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は，次に示す手順に分かれています。

1. まず，RIP 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を指定します。プロトコルを指定するには，コンフィグレーションコマンド redistribute を使用します。redistribute に経路種別を指定することで，指定した種別の経路だけを広告対象にすることができます。また，route-map を指定することで，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することもできます。redistribute では，条件の比較にルーティングテーブル上の経路属性値を使用します。
   RIP 経路と RIP インタフェースの直結経路だけは，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ることによって，広告する経路の属性を変更することもできます。
2. メトリック値をプロトコルで決められた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ている場合は，redistribute で変更した値をそのまま使用します。

RIP のメトリック値のデフォルト値については，「表 13-9　RIP 広告経路フィルタリングで変更可能な経路の属性」を参照してください。

3. redistribute で選択した経路に，distribute-list out に従ってフィルタを適用します。パラメータにインタフェースやルータを指定することで，指定広告先へ広告する場合にだけフィルタを適用できます。また，プロトコルを指定すると，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。コンフィグレーションコマンドを次の表に示します。
   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 を指定することによって，広告する経路の属性を変更することもできます。

表 13-10　RIP 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><Protocol>	指定した隣接ルータへ広告する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>	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>	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。

13.1.4　OSPF

（1）OSPF 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。フィルタした結果，学習しないことになった AS 外経路や NSSA 経路は，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・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入ります。

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経路ができます。これは，経路の元となった LSA が OSPF 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は，LSA から計算した AS 外経路や NSSA 経路は経路フィルタリングしますが，経路の元になった LSA はフィルタしません。

（a）フィルタの適用方法と適用順

学習した経路の中で AS 外経路と NSSA 経路を distribute-list in で指定したフィルタでフィルタします。OSPF 学習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。

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。

表 13-11 OSPF 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。

(b) 学習経路フィルタリングで変更可能な経路属性

OSPF 学習経路フィルタリングで変更可能な属性を次の表に示します。

OSPF 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用います。

表 13-12 OSPF 学習経路フィルタリングで変更可能な経路の属性

属性	デフォルト値
ディスタンス値	distance ospf (OSPF) に指定した値。 指定していない場合は 110。

(2) OSPF 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にかかわらず，経路の元である LSA は無条件で伝達するためです。

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 OSPF へ広告できます。AS 外経路または NSSA 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 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。

(a) 広告経路フィルタリングで変更可能な経路属性

OSPF の広告経路フィルタリングで変更可能な属性を次の表に示します。

表 13-13 OSPF 広告経路フィルタリングで変更可能な 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。

注意

メトリック値を 16777215 以上に変更するように設定することもできます。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は，次に示す手順に分かれています。

1. まず，OSPF 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を指定します。プロトコルを指定するには，コンフィグレーションコマンド redistribute を使用します。ただし，OSPF の当該ドメインを指定しても，そのドメインの経路を再広告することはありません。
   redistribute に経路種別を指定することで，指定した種別の経路だけを広告対象にすることができます。また，route-map を指定することで，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することもできます。redistribute では，条件の比較にルーティングテーブル上の経路属性値を使用します。
   redistribute に経路属性を変更する route-map や経路属性を直接指定することによって，広告する経路の属性を変更することもできます。
2. メトリック値と OSPF 経路種別をプロトコルで決められたデフォルト値に設定します。ただし，redistribute で属性値を変更している場合は，redistribute で変更した値をそのまま使用します。
   OSPF の広告経路属性のデフォルト値については，「表 13-13　OSPF 広告経路フィルタリングで変更可能な OSPF AS 外経路の属性」を参照してください。
3. redistribute で選択した経路に distribute-list out に従ってフィルタを適用します。パラメータにプロトコルを指定することで，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。コンフィグレーションコマンドを次の表に示します。
   経路を OSPF 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 を指定することで，広告する経路の属性を変更することもできます。

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 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。

表 13-14　OSPF 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。

13.1.5　BGP4【OP-BGP】

（1）BGP4 学習経路フィルタリング

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入りません。

注意

BGP4 の学習経路フィルタリングを設定または設定変更したあと，適切なタイミングで運用コマンド clear ip bgp * in または clear ip bgp * both を実行してください。上記運用コマンドを実行するまでの間は，変更前の経路フィルタリング設定に従って動作します。

clear ip bgp * in を実行すると，変更したあとの経路フィルタリング設定を学習経路フィルタリングに使用します。clear ip bgp * both を実行すると，変更したあとの経路フィルタリング設定を学習経路フィルタリングと広告経路フィルタリングに使用します。

(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。BGP4 学習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。

経路を学習したら，設定したフィルタを表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。

表 13-15 BGP4 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）	<IPv4>（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）（access-list/prefix-list 指定）	<IPv4>（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）	<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）（access-list/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。
distribute-list in（BGP4）	なし	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。

(b) 学習経路フィルタリングで変更可能な経路属性

BGP4 経路の学習経路フィルタリングで変更可能な属性を次の表に示します。

ディスタンス値以外の値は，BGP4 の優先経路選択に用います。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用います。

表 13-16 BGP4 学習経路フィルタリングで変更可能な経路の属性

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，次の値を使います。 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

属性	デフォルト値
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。

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 AS を加えることはできません。

(2) BGP4 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。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。

注意

BGP4 の広告経路フィルタリングを設定または設定変更したあと，適切なタイミングで運用コマンド clear ip bgp * out または clear ip bgp * both を実行してください。上記運用コマンドを実行するまでの間は，変更前の経路フィルタリング設定に従って動作します。
clear ip bgp * out を実行すると，変更したあとの経路フィルタリング設定を広告経路フィルタリングに使用します。clear ip bgp * both を実行すると，変更したあとの経路フィルタリング設定を学習経路フィルタリングと広告経路フィルタリングに使用します。

(a) 広告経路フィルタリングで変更可能な経路属性

BGP4 広告経路フィルタリングで変更可能な属性を次の表に示します。

表 13-17　BGP4 広告経路フィルタリングで変更可能な 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 経路であれば，メトリック値を引き継ぎます。BGP4 以外の経路の場合，default-metric で設定した値を用います。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 で設定した値を用います。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 経路であれば，メトリック値を引き継ぎます。BGP4 以外の経路の場合，default-metric で設定した値を用います。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 で設定した値を用います。bgp default local-preference を設定していない場合，値 100 を用います。 ただし，広告先ピアが外部ピアである場合，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	

属性	デフォルト値
COMMUNITIES 属性	

注意

- neighbor send-community を設定していない場合，COMMUNITIES 属性を広告しません。

(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は，次に示す手順に分かれています。

1. まず，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を指定します。プロトコルを指定するには，コンフィグレーションコマンド redistribute を使用します。redistribute に条件経路種別や route-map を指定すると，指定した種別の経路や route-map を通過した経路だけが広告対象になります。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ることによって，広告する経路の属性を変更することもできます。
2. MED 属性，LOCAL_PREF 属性をプロトコルで決められたデフォルト値に設定します。ただし，redistribute で属性値を変更している場合は，redistribute で変更した値をそのまま使用します。
   BGP の広告経路属性のデフォルト値については，「表 13-17　BGP4 広告経路フィルタリングで変更可能な BGP4 経路の属性」を参照してください。
3. redistribute で選択した経路を，neighbor out と distribute-list out に従ってフィルタします。
   neighbor out 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へ広告する場合にだけ適用します。また，プロトコルを指定すると，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。コンフィグレーションコマンドとその適用先を次の表に示します。
   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，それを表の順番に適用します。適用する経路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。フィルタした結果が 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，デフォルト広告属性値や 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。
   neighbor out や distribute-list out に属性を変更する route-map を指定することによって，広告する経路の属性を変更することもできます。

表 13-18　BGP4 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）	<IPv4>（ピアアドレス） <Protocol>	指定ピアへ広告する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）（access-list/prefix-list 指定）	<IPv4>（ピアアドレス） <Protocol>	
neighbor out（BGP4）（route-map 指定）	<IPv4>（ピアアドレス）	指定ピアへ広告する経路にフィルタを適用します。
neighbor out（BGP4）（access-list/prefix-list 指定）	<IPv4>（ピアアドレス）	
neighbor out（BGP4）（route-map 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指定したプロトコルの経路にフィルタを適用します。

コマンド名	パラメータ	フィルタ対象経路
neighbor out（BGP4）（access-list/ prefix-list 指定）	<Peer-Group>（ピアグループ） <Protocol>	
neighbor out（BGP4）（route-map 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）（access-list/ prefix-list 指定）	<Peer-Group>（ピアグループ）	
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。
	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。

13.1.6 エクストラネット【OP-NPAR】

（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入りません。

（a）フィルタの適用方法

VRF 間で導入したい経路を，import inter-vrf 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 13-19　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。

（b）VRF 間経路フィルタリングで変更可能な経路属性

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可能な属性を次の表に示します。

表 13-20　VRF 間経路フィルタリングで変更可能な経路の属性

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。
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。

13.2 コンフィグレーション

13.2.1 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 13-21 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 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	IPv4 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。
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。

コマンド名	説明
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。
access-list ※1	IPv4 フィルタとして動作するアクセスリストを設定します。
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。
router rip ※2	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 ※3	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 ※4	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。
import inter-vrf ※5	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。

注※ 1
「コンフィグレーションコマンドレファレンス Vol.2　4. 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　11. RIP」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　12. 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　13. BGP4【OP-BGP】」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　30. VRF【OP-NPAR】」を参照してください。

13.2.2 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 宛の RIP 経路だけを学習し，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 宛の経路だけ permit になる ip prefix-list を設定します。この 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 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

VLAN 10 から学習した経路について，192.168.0.0/16 宛の経路だけを学習し，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。VLAN 10 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 宛の経路だけ permit になる ip prefix-list を設定します。この prefix-list を distribute-list in VLAN 10 から参照することによって，VLAN 10 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 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 vlan 10
   VLAN 10 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，プレフィックスが 192.168.0.0/16 に含まれる場合だけ permit になる ip prefix-list を設定します。次に，この 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 から参照することによって，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 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
   上記フィルタを RIP 学習経路フィルタリングに適用することによって，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 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 から参照することによって，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 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
```
上記フィルタを RIP 学習経路フィルタリングに適用することによって，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。

13.2.3 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 宛の経路だけが permit になる ip prefix-list を設定します。次に，この 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 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，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 宛の経路だけ deny になる ip prefix-list を設定します。この prefix-list を distribute-list out から参照することによって，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 になるように 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・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。

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 VLAN 10 からは，192.168.0.0/16 だけを広告します。RIP インタフェース VLAN 20 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。
192.168.0.0/16 だけ permit になる ip prefix-list と 192.168.0.0/16 以外だけ permit になる ip prefix-list を設定します。次に，RIP インタフェース VLAN 10 と VLAN 20 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 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・マスク長に対して permit になるように 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 vlan 10
   VLAN 10 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 vlan 20**
   VLAN 20 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。これによって，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 を使用することになります。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。

13.2.4 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 宛の経路だけを学習し，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 宛の経路だけ permit になる ip prefix-list を設定します。この prefix-list を distribute-list in から参照することによって，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 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 から参照することによって，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
   上記フィルタを OSPF 学習経路フィルタリングに適用することによって，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 prefix-list を設定します。次に，この 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 から参照することによって，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 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
   上記フィルタを OSPF 学習経路フィルタリングに適用することによって，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。

13.2.5 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，match ip address で参照してください。
まず，192.168.0.0/16 宛の経路だけが 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，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 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，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 宛の経路だけ deny になる ip prefix-list を設定します。この prefix-list を distribute-list out から参照することによって，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 になるように 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・マスク長に対して permit になるように 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ぐことができます。

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 を使用することになります。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，そうでなければタグ値 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，そうでなければタグ値 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 deny になり，そうでない場合タグ値を 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。

13.2.6 BGP4 学習経路フィルタリング【OP-BGP】

（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したら deny になる ip prefix-list を設定します。この prefix-list を distribute-list in から参照することによって，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 prefix-list を設定します。

2. **(config)# router bgp 65531**
   (config-router)# distribute-list prefix DENY192168LONGER in
   その 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 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 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。

13.2.7 BGP4 広告経路フィルタリング【OP-BGP】

(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，自 AS のネットワーク（192.169.0.0/16）が宛先ネットワークである経路だけを 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 prefix-list を使用します。

[コマンドによる設定]

1. **(config)# ip prefix-list PERMIT192169LONGER seq 10 permit 192.169.0.0/16 ge 16 le 32**
   192.169.0.0/16 に含まれる経路だけ permit になる prefix-list を設定します。

2. **(config)# route-map PERMIT192169LONGER permit 10**
   (config-route-map)# match ip address prefix-list PERMIT192169LONGER
   (config-route-map)# exit

192.169.0.0/16 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 PERMIT192169LONGER
   (config-router)# redistribute static route-map PERMIT192169LONGER
   直結経路とスタティック経路について，route-map PERMIT192169LONGER 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（192.169.0.0/16）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，直結経路・スタティック経路の redistribute 用，ピア 172.18.1.1 広告用，172.18.1.1 以外の外部ピア用，内部ピア用，合計四つの route-map を設定します。
直結経路・スタティック経路については，192.169.0.0/16 に含まれている経路だけ permit になる ip prefix-list を設定し，これを参照する route-map を設定します。
ピア 172.18.1.1 については，経路プロトコルが直結・スタティックである場合だけ AS を二つ追加する route-map を設定します。
172.18.1.1 以外の外部ピアについては，AS が一つの AS_PATH 属性だけ permit になる ip as-path access-list を設定し，これを参照する route-map を設定します。
内部ピアについては，BGP4 経路だけ permit，そうでなければ 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 PERMIT192169LONGER seq 10 permit 192.169.0.0/16 ge 16 le 32**
   (config)# route-map PERMIT192169LONGER permit 10
   (config-route-map)# match ip address prefix-list PERMIT192169LONGER
   (config-route-map)# exit
   192.169.0.0/16 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・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 BGP1721811OUT 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 BGP1721811OUT 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 PERMIT192169LONGER
(config-router)# redistribute static route-map PERMIT192169LONGER
```
直結経路とスタティック経路について，route-map PERMIT192169LONGER 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 BGP1721811OUT 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 192.169.1.1 remote-as 65531
(config-router)# neighbor 192.169.1.1 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。

13.2.8 エクストラネット【OP-NPAR】

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，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，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，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。

13.3 オペレーション

13.3.1 運用コマンド一覧

経路フィルタリング動作の運用コマンド一覧を次の表に示します。

表 13-22 運用コマンド一覧

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，または 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 ip vrf	VRF の IPv4 情報を表示します。
restart unicast ※	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 ※	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 ※	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※
「運用コマンドレファレンス Vol.3　8. IPv4・IPv6 ルーティングプロトコル共通」を参照してください。

13.3.2 RIP が受信した経路（学習経路フィルタリング前）の確認

RIP が受信した経路を確認するには，運用コマンド show ip rip にパラメータ received-routes を指定して実行してください。

図 13-3 RIP 受信経路表示例

```
> show ip rip received-routes
Date 2006/03/14 12:00:00 UTC
Status Codes: * valid, > active

Neighbor Address: 192.168.1.145
   Destination        Next Hop        Interface      Metric   Tag   Timer
*> 172.10.1/24        192.168.1.145   VLAN0007       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 内部で優先しないことになった経路は，本コマンドでは表示されません。

13.3.3 OSPF の SPF 計算結果の経路確認

OSPF が SPF 計算した結果の AS 外経路・NSSA 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。無効経路を含めて OSPF が SPF 計算した結果の AS 外経路・NSSA 経路を確認するには，運用コマンド show ip route にパラメータ all-routes を指定し，さらに -T

ospf_external を指定して実行してください。

図 13-4 OSPF AS 外経路・NSSA 経路表示例

```
> show ip route all-routes -T ospf_external
Date 2006/03/14 12:00:00 UTC
Status Codes: * valid, > active
Total: 2 routes
   Destination    Next Hop        Interface   Metric   Protocol   Age
*> 200.1/24       192.168.1.145   VLAN0007    1/1      OSPF ext2  52s, Tag: 10
*  200.200.1/24   192.168.1.145   VLAN0007    1/1      OSPF ext2  52s, Tag:  0
```

13.3.4 BGP4 が受信した経路（学習経路フィルタリング前）の確認【OP-BGP】

BGP4 が受信した経路を確認するには，運用コマンド show ip bgp にパラメータ received-routes を指定して実行してください。

図 13-5 BGP4 受信経路表示例

```
> show ip bgp received-routes
Date 2006/03/14 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: * valid, > active
Origin Codes: i - IGP, e - EGP, ? - incomplete
   Network             Next Hop        MED    LocalPref Path
*> 200.1/24            192.168.1.145   -      -         1000 i
*  200.200.1/24        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 内部で優先しないことになった経路は，本コマンドでは表示されません。

BGP4 が受信した経路を詳細な経路属性を含めて確認するには，運用コマンド show ip bgp にパラメータ received-routes を指定し，さらに -F を指定して実行してください。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 13-6 BGP4 受信経路詳細表示例

```
> show ip bgp received-routes -F
Date 2006/03/14 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: * valid, > active
Route 200.1/24
*> 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 200.200.1/24
*  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 内部で優先しないことになった経路は，本コマンドでは表示されません。

13.3.5 学習経路フィルタリングした結果の経路の確認

学習経路フィルタリングした結果の経路は，ルーティングテーブルに入っています。ルーティングテーブルの経路を表示することで，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，運用コマンド show ip route にパラメータ all-routes を指定して実行してください。

図 13-7 ルーティングテーブル経路表示例 (無効経路を含む)

```
> show ip route all-routes
Date 2006/03/14 12:00:00 UTC
Status Codes: * valid, > active
Total: 12 routes
   Destination      Next Hop         Interface     Metric  Protocol   Age
*> 127/8            ----             localhost     0/0     Connected   1h 32s
*> 127.0.0.1/32     127.0.0.1        localhost     0/0     Connected   1h 32s
*> 172.10.1/24      192.168.1.145    VLAN0007      2/0     RIP         12s
*> 192.168.1/24     192.168.1.1      VLAN0007      0/0     Connected   2s
   192.168.1/24     192.168.1.1      VLAN0007      1/-     OSPF intra 48m  3s
*> 192.168.1.1/32   192.168.1.1      VLAN0007      0/0     Connected   1h 31s※
*> 200.1/24         192.168.1.145    VLAN0007      -/-     BGP         11m 26s
*> 201.110/24       192.168.1.145    VLAN0007      1/1     OSPF ext2   52s
*> 200.200.1/24     192.168.1.145    VLAN0007      0/0     Static      46m 58s
*  200.200.1/24     192.168.1.145    VLAN0007      -/-     BGP         50m 14s
*  200.200.1/24     192.168.1.145    VLAN0007      1/1     OSPF ext2   48m 52s
*  200.200.1/24     192.168.1.145    VLAN0007      2/0     RIP         12s
```

注※

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，運用コマンド show ip route にパラメータ all-routes を指定し，さらにプロトコルを指定して実行してください。

図 13-8 ルーティングテーブル経路表示例 (RIP だけ，無効経路含む)

```
> show ip route all-routes rip
Date 2006/03/14 12:00:00 UTC
Status Codes: * valid, > active
Total: 2 routes
   Destination        Next Hop         Interface      Metric   Protocol  Age
*> 172.10.1/24        192.168.1.145    VLAN0007       2/0      RIP       12s
*  200.200.1/24       192.168.1.145    VLAN0007       2/0      RIP       12s
```

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・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，運用コマンド show ip route にパラメータ all-routes を指定し，さらに -P を指定して実行してください。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 13-9 ルーティングテーブル経路ディスタンス値表示例

```
> show ip route all-routes -P
Date 2006/03/14 12:00:00 UTC
Status Codes: * valid, > active
Total: 12 routes
   Destination      Next Hop        Interface   Metric  Protocol   Age
*> 127/8            ----            localhost   0/0     Connected   1h 36m,
 Distance: 0/0/0
*> 127.0.0.1/32     127.0.0.1       localhost   0/0     Connected   1h 36m,
 Distance: 0/0/0
*> 172.10.1/24      192.168.1.145   VLAN0007    2/0     RIP        12s,
 Distance: 120/0/0
*> 192.168.1/24     192.168.1.1     VLAN0007    0/0     Connected   0s,
 Distance: 0/0/0
   192.168.1/24     192.168.1.1     VLAN0007    1/-     OSPF intra 52m 32s,
 Distance: -110/1/0
*> 192.168.1.1/32   192.168.1.1     VLAN0007    0/0     Connected   1h 35m,
 Distance: 0/0/0
*> 200.1/24         192.168.1.145   VLAN0007    -/-     BGP        12m 37s,
 Distance: 20/0/0
*> 201.110/24       192.168.1.145   VLAN0007    1/1     OSPF ext2   6m 11s,
 Distance: 110/1/0
*> 200.200.1/24     192.168.1.145   VLAN0007    0/0     Static     50m 27s,
 Distance: 2/0/0
*  200.200.1/24     192.168.1.145   VLAN0007    -/-     BGP        54m 43s,
 Distance: 20/0/0
*  200.200.1/24     192.168.1.145   VLAN0007    1/1     OSPF ext2  52m 21s,
 Distance: 110/1/0
*  200.200.1/24     192.168.1.145   VLAN0007    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，運用コマンド show ip route にパラメータ all-routes を指定し，さらに宛先ネットワークを指定して実行してください。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 13-10 ルーティングテーブル経路表示例 (無効経路含む，特定宛先だけ)

```
> show ip route all-routes 200.200.1/24
Date 2006/03/14 12:00:00 UTC
Route codes: *  = active,   + = changed to active recently
           ' ' = inactive, - = changed to inactive recently

Route 200.200.1/24
Entries 4 Announced 1 Depth 0 <>

* NextHop 192.168.1.145  , Interface   : VLAN0007
     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   : VLAN0007
     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>
```

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，運用コマンド show ip route にパラメータ all-routes を指定し，さらに -F を指定して実行してください。

図 13-11 ルーティングテーブル経路表示例 (無効経路含む，詳細表示)

```
> show ip route all-routes -F
Date 2006/03/14 12:00:00 UTC
Status Codes: * valid, > active
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 Retain Reject>
*> 127.0.0.1/32       127.0.0.1       localhost     0/0      Connected  1h 46m,
 Distance: 0/0/0, Tag: 0, AS-Path: IGP (Id 1), Communities: -, LocalPref: -,
<NoAdvise Active Retain>
*> 172.10.1/24        192.168.1.145   VLAN0007      2/0      RIP       19s,
 Distance: 120/0/0, Tag: 0, AS-Path: IGP (Id 1), Communities: -, LocalPref: -,<Int
Active Gateway>
*> 192.168.1/24       192.168.1.1     VLAN0007      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     VLAN0007      1/-      OSPF intra 1h  2m,
 Distance: -110/1/0, Tag: 0, AS-Path: IGP (Id 1), Communities: -, LocalPref: -,
<NotInstall NoAdvise Int Hidden Gateway>
*> 177.7.7.1/32       192.168.1.1     VLAN0007      0/0      Connected  1h 45m,
 Distance: 0/0/0, Tag: 0, AS-Path: IGP (Id 1), Communities: -, LocalPref: -,
<NoAdvise Active Retain>
*> 200.1/24           192.168.1.145   VLAN0007      -/-      BGP       12m 57s,
 Distance: 20/0/0, Tag: 0, AS-Path: 1000 IGP (Id 3), Communities: 120:200,
LocalPref: 100, <Ext Active Gateway>
*> 201.110.1/24       192.168.1.145   VLAN0007      1/1      OSPF ext2  3m 34s,
 Distance: 110/1/0, Tag: 10, AS-Path: IGP (Id 1), Communities: -, LocalPref: -,
<Int Ext Active Gateway>
*> 200.200.1/24       192.168.1.145   VLAN0007      0/0      Static     1h  0m,
 Distance: 2/0/0, Tag: 0, AS-Path: IGP (Id 1), Communities: -, LocalPref: -,
<Remote Int Active Gateway>
*  200.200.1/24       192.168.1.145   VLAN0007      -/-      BGP        1h  5m,
 Distance: 20/0/0, Tag: 0, AS-Path: 1000 IGP (Id 2), Communities: -, LocalPref:
100,
 <Ext Gateway>
*  200.200.1/24       192.168.1.145   VLAN0007      1/1      OSPF ext2  1h  2m,
 Distance: 110/1/0, Tag: 0, AS-Path: IGP (Id 1), Communities: -, LocalPref: -,<Int
Ext Gateway>
*  200.200.1/24       192.168.1.145   VLAN0007      2/0      RIP       19s,
 Distance: 120/0/0, Tag: 0, AS-Path: IGP (Id 1), Communities: -, LocalPref: -,<Int
Gateway>
```

13.3.6 広告経路フィルタリングする前の経路の確認

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。

ルーティングテーブルの優先経路を表示するには，運用コマンド show ip route 実行してください。

図 13-12 ルーティングテーブル経路表示例

```
> show ip route
Date 2006/03/14 12:00:00 UTC
Total: 8 routes
Destination        Next Hop        Interface      Metric   Protocol  Age
127/8              ----            localhost      0/0      Connected  1h 32s
127.0.0.1/32       127.0.0.1       localhost      0/0      Connected  1h 32s
172.10.1/24        192.168.1.145   VLAN0007       2/0      RIP       12s
192.168.1/24       192.168.1.1     VLAN0007       0/0      Connected  2s
192.168.1.1/32     192.168.1.1     VLAN0007       0/0      Connected  1h 31s
200.1/24           192.168.1.145   VLAN0007       -/-      BGP       11m 26s
201.110/24         192.168.1.145   VLAN0007       1/1      OSPF ext2 52s
200.200.1/24       192.168.1.145   VLAN0007       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，運用コマンド show ip route にパラメータとしてプロトコルを指定して実行してください。

図 13-13 ルーティングテーブル経路表示例（RIP だけ）

```
> show ip route rip
Date 2006/03/14 12:00:00 UTC
Total: 5 routes
Destination        Next Hop        Interface      Metric   Protocol  Age
172.10.1/24        192.168.1.145   VLAN0007       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，運用コマンド show ip route にパラメータ -F を指定して実行してください。

図 13-14 ルーティングテーブル経路表示例（詳細表示）

```
> show ip route -F
Date 2006/03/14 12:00:00 UTC
Total: 8 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 Retain Reject>
127.0.0.1/32       127.0.0.1       localhost      0/0      Connected  1h 46m,
 Distance: 0/0/0, Tag: 0, AS-Path: IGP (Id 1), Communities: -, LocalPref: -,
<NoAdvise Active Retain>
172.10.1/24        192.168.1.145   VLAN0007       2/0      RIP       19s,
 Distance: 120/0/0, Tag: 0, AS-Path: IGP (Id 1), Communities: -, LocalPref: -,<Int
Active Gateway>
192.168.1/24       192.168.1.1     VLAN0007       0/0      Connected  7s,
 Distance: 0/0/0, Tag: 0, AS-Path: IGP (Id 1), Communities: -, LocalPref: -,
<Active Retain>
177.7.7.1/32       192.168.1.1     VLAN0007       0/0      Connected  1h 45m,
 Distance: 0/0/0, Tag: 0, AS-Path: IGP (Id 1), Communities: -, LocalPref: -,
<NoAdvise Active Retain>
200.1/24           192.168.1.145   VLAN0007       -/-      BGP       12m 57s,
 Distance: 20/0/0, Tag: 0, AS-Path: 1000 IGP (Id 3), Communities: 120:200,
LocalPref: 100, <Ext Active Gateway>
201.110.1/24       192.168.1.145   VLAN0007       1/1      OSPF ext2  3m 34s,
 Distance: 110/1/0, Tag: 10, AS-Path: IGP (Id 1), Communities: -, LocalPref: -,
<Int Ext Active Gateway>
200.200.1/24       192.168.1.145   VLAN0007       0/0      Static     1h  0m,
 Distance: 2/0/0, Tag: 0, AS-Path: IGP (Id 1), Communities: -, LocalPref: -,
<Remote Int Active Gateway>
```

BGP4 では，ルーティングテーブル上にある BGP4 の優先でない経路も広告対象になることがあります。ルーティングテーブル上にある BGP4 経路を優先でない経路も含めて表示するには，運用コマンド show ip route にパラメータ all-routes を指定し，さらにパラメータとして bgp を指定して実行してください。

図 13-15 ルーティングテーブル経路表示例（無効経路を含む，BGP だけ）

```
> show ip route all-routes bgp
Date 2006/03/14 12:00:00 UTC
Status Codes: * valid, > active
Total: 12 routes
   Destination     Next Hop        Interface   Metric   Protocol  Age
*> 200.1/24        192.168.1.145   VLAN0007    -/-      BGP       11m 26s┐
*  200.200.1/24    192.168.1.145   VLAN0007    -/-      BGP       50m 14s┘
                                                                      ※
```

注※

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。

13.3.7 RIP 広告経路の確認

RIP の広告経路を確認するには運用コマンド show ip rip にパラメータ advertised-routes を指定して実行してください。広告先のアドレスと，そこへ広告している経路・経路属性を表示します。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 13-16 RIP 広告経路表示例

```
> show ip rip advertised-routes
Date 2006/03/20 16:47:36 UTC

Target Address: 177.7.7.255
Destination        Next Hop        Interface      Metric   Tag   Age
192.158.1/24       192.158.1.1     VLAN0006       1        0      5s
```

13.3.8 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運用コマンド show ip ospf にパラメータ database を指定し，さらに external と self-originate を指定して実行してください。

図 13-17 AS-External-LSA 表示例（自装置生成分だけ）

```
> show ip ospf database external self-originate
Date 2006/03/14 12:00:00 UTC
Domain: 1
Local Router ID : 200.199.198.197
Area : 0
Address          State Priority Cost  Neighbor   DR              Backup DR
177.7.7.1        BackupDR 1     1     1          1.4.8.0         200.199.198.197

LS Database: AS External Link
Network Address: 192.168.1/24, AS Boundary Router: 200.199.198.197      …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運用コマンド show ip ospf にパラメータ database を指定し，さらに nssa と self-originate を指定して実行してください。

図 13-18 NSSA-External-LSA 表示例

```
> show ip ospf database nssa self-originate
Date 2006/03/14 12:00:00 UTC
Domain: 1
Local Router ID : 200.199.198.197
Area : 0
Address          State Priority Cost  Neighbor   DR              Backup DR
177.7.7.1        BackupDR 1     1     1          1.4.8.0         200.199.198.197

LS Database: NSSA AS External Link
Network Address: 192.168.1/24, AS Boundary Router: 200.199.198.197      …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。

13.3.9 BGP4 広告経路の確認【OP-BGP】

BGP4 の広告経路を確認するには，運用コマンド show ip bgp にパラメータ advertised-routes を指定して実行してください。

図 13-19 BGP4 広告経路表示例

```
> show ip bgp advertised-routes
Date 2006/03/14 12:00:00 UTC
BGP Peer: 177.7.7.145    , Remote AS: 2000
Local AS: 1000, Local Router ID: 192.168.1.1
Status Codes: * valid, > active
Origin Codes: i - IGP, e - EGP, ? - incomplete
   Network              Next Hop        MED    LocalPref Path
*> 200.1/24             177.2.2.1       0      -         1000 2100 i
*> 200.200.1/24         177.2.2.1       0      -         1000 2100 i
```

BGP4 の広告経路の詳細な経路属性を確認するには，運用コマンド show ip bgp にパラメータ advertised-routes を指定し，さらに -F を指定して実行してください。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 13-20 BGP4 広告経路表示例（詳細表示）

```
> show ip bgp advertised-routes -F
Date 2006/03/14 12:00:00 UTC
BGP Peer: 177.7.7.145    , Remote AS: 2000
Local AS: 1000, Local Router ID: 192.168.1.1
Status Codes: * valid, > active
Route 200.1/24
*> Next Hop 177.2.2.1
     MED:0, LocalPref: -, Type: External route
     Origin: IGP
     Path: 1000 2100
     Next Hop Attribute: 177.2.2.1
     Communities: 1020:1200
Route 110.10/24
*> Next Hop 2.2.2.2
     MED: 0, LocalPref: -, Type: External route
     Origin: IGP
     Path: 1000 2100
     Next Hop Attribute: 177.2.2.1
     Communities: 1020:1200
```

13.3.10 エクストラネットの確認【OP-NPAR】

運用コマンド show ip route 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 13-21 show ip route コマンドの表示例

```
> show ip route vrf 2 extra-vrf
Date 2008/12/20 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        VLAN0030       0/0     Extra-Vrf  365d
>
> show ip route vrf 3 extra-vrf
Date 2008/12/20 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        VLAN0010       0/0     Extra-Vrf  365d
```

14 IPv4 マルチキャストの解説

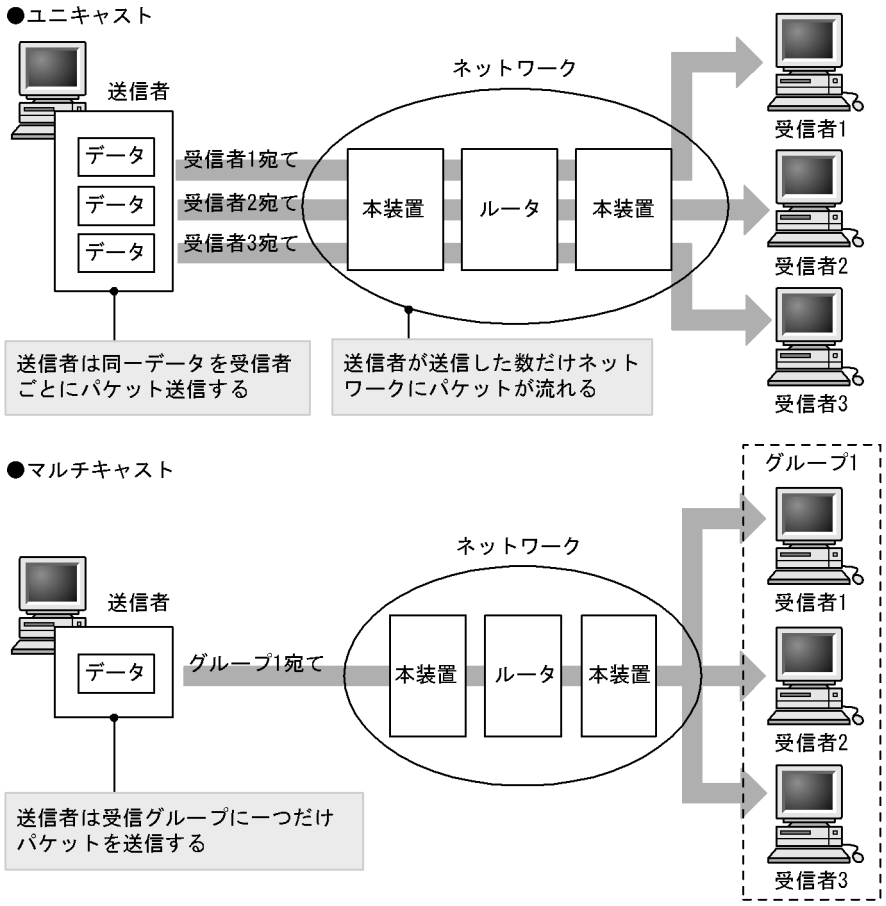
マルチキャストは，ネットワーク内で選択されたグループに対して同一の情報を送信します。この章では IPv4 ネットワークで実現するマルチキャストについて説明します。

14.1 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。

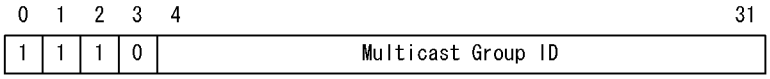
図 14-1 マルチキャストの概要（IPv4）



14.1.1 IPv4 マルチキャストアドレス

マルチキャスト通信では IP アドレスの ClassD を使用します。マルチキャストアドレスはマルチキャストデータの送受信に参加しているグループの間だけで存在し，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。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 14-2 マルチキャストアドレスのフォーマット



14.1.2 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があります。

- マルチキャストグループマネージメント機能
  グループメンバーシップ情報の送受信を行い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
  経路情報の送受信を行って中継経路を決定し，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。経路情報収集には PIM-SM（PIM-SSM を含む），または PIM-DM 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。

14.2 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，ルーターホスト間でのグループメンバー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ー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。

IGMP はルーターホスト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。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ホストからのマルチキャストグループへの参加・離脱報告によって，ルータがホストのマルチキャストグループへの参加・離脱を認識してマルチキャストパケットの中継・遮断を行います。

IGMPv3 は IPv4 マルチキャストグループマネージメント機能を実現する IGMPv2 を拡張したプロトコルで，指定した送信元からのマルチキャストパケットだけを受信する送信元フィルタリング機能が導入されています。IPv4 マルチキャストグループへの参加・離脱報告時に送信元指定が可能であるため，IGMPv3 と PIM-SSM を組み合わせて使用することで，効率のよい IPv4 マルチキャスト中継が実現できます。

本装置が送信する IGMPv2 メッセージのフォーマットおよび設定値は RFC2236 に従います。また，IGMPv3 メッセージのフォーマットおよび設定値は RFC3376 に従います。

14.2.1 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 14-1 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		マルチキャストグループの参加問い合わせ	−	−
−	General Query	全グループ宛て	○	○
	Group-Specific Query	特定グループ宛て	○	○
Version2 Membership Report		加入しているマルチキャストグループの報告 (IGMPv2 対応)	×	○
Leave Group		マルチキャストグループからの離脱報告	×	○
Version1 Membership Report		加入しているマルチキャストグループの報告 (IGMPv1 対応)	×	○

(凡例) ○：サポートする　×：サポートしない　−：該当しない

(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機能を実現します。フィルタモードには次の二つのモードがあります。

- INCLUDE：指定された送信元リストからのパケットだけ中継します
- EXCLUDE：指定された送信元リスト以外からのパケットだけ中継します

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 14-2 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	IPv4 マルチキャストグループの参加問合せ (全グループ宛て)	○	○
	Group-Specific Query	IPv4 マルチキャストグループの参加問合せ (特定グループ宛て)	○	○
	Group-and-Source-Specific Query	IPv4 マルチキャストグループの参加問合せ (特定の送信元およびグループ宛て)	○	○
Version 3 Multicast Membership Report	Current State Report	加入している IPv4 マルチキャストグループとフィルタモード報告	×	○
	State Change Report	加入している IPv4 マルチキャストグループとフィルタモードの更新報告	×	○

(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グループ加入後に変更することが可能で，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 14-3 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	○ (送信元リストは無視します)
State Change Report	CHANGE_TO_INCLUDE_MODE	フィルタモードを INCLUDE 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 に変更することを示します	○ (送信元リストは無視します)
	ALLOW_NEW_SOURCES	データの受信を希望する送信元を追加することを示します	○
	BLOCK_OLD_SOURCES	データの受信を希望する送信元を削除することを示します	○

(凡例) ○：サポートする

14.2.2 IGMP 動作

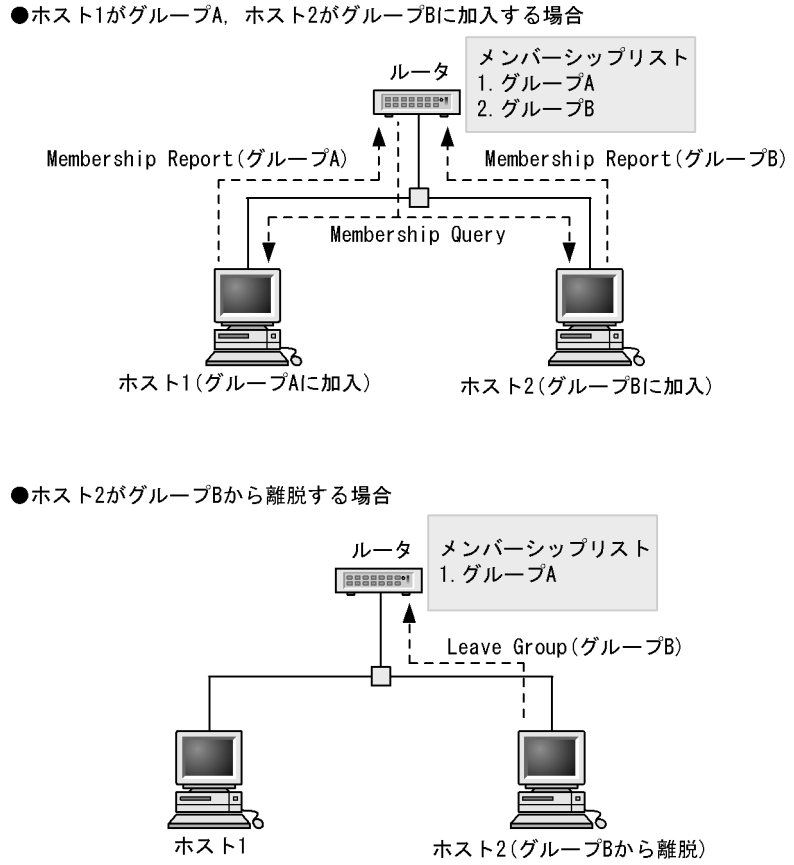
IGMPv2 メッセージを使用した IGMPv2 の動作を次に示します。

- IPv4 マルチキャストルータは，IPv4 マルチキャストメンバーシップの情報を得るため，定期的に直接接続するインタフェース上に Multicast Membership Query（General Query）メッセージを全マルチキャストホスト 224.0.0.1 宛てに送信します。

- ホストは Multicast Membership Query を受信すると，Multicast Membership Report を該当するグループ宛てに送信することで，グループへの参加状況を報告します。
- ホストから Multicast Membership Report を受信すると，IPv4 マルチキャストルータはメンバーシップリストにそのグループを追加します。
- Multicast Leave Group メッセージを受信するとそのグループをメンバーシップリストから削除します。

IGMPv2 グループの参加・離脱を次の図に示します。

図 14-3　IGMPv2 グループの参加・離脱

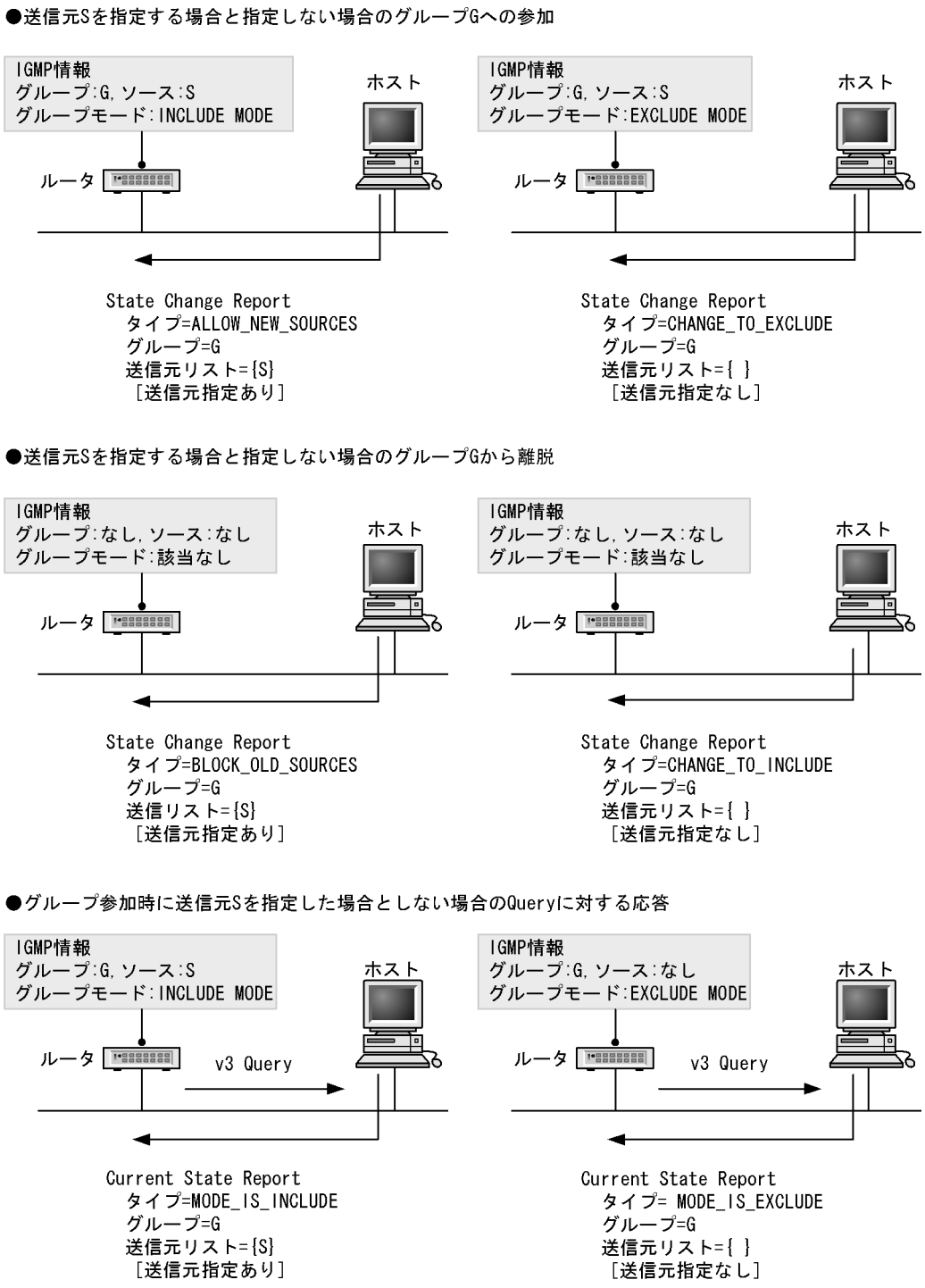


IGMPv3 メッセージを使用した IGMPv3 の動作を次に示します。

- IPv4 マルチキャストルータは，IPv4 マルチキャストメンバーシップの情報を得るため，定期的に直接接続するインタフェース上に Version 3 Multicast Membership Query（General Query）メッセージを全マルチキャストホスト 224.0.0.1 宛てに送信します。
- ホストは Version 3 Multicast Membership Query を受信すると，Version 3 Multicast Membership Report （Current State Report）を 224.0.0.22 宛てに送信することで，グループへの参加状況を報告します。
- ホストから Version 3 Multicast Membership Report（State Change Report）メッセージを受信すると IPv4 マルチキャストルータは Group Record タイプの内容に応じて，そのグループをメンバーシップへ追加，または削除します。

ホストからの IGMPv3 Report メッセージ送信動作を次の図に示します。

図 14-4　IGMPv3 グループ参加・離脱動作

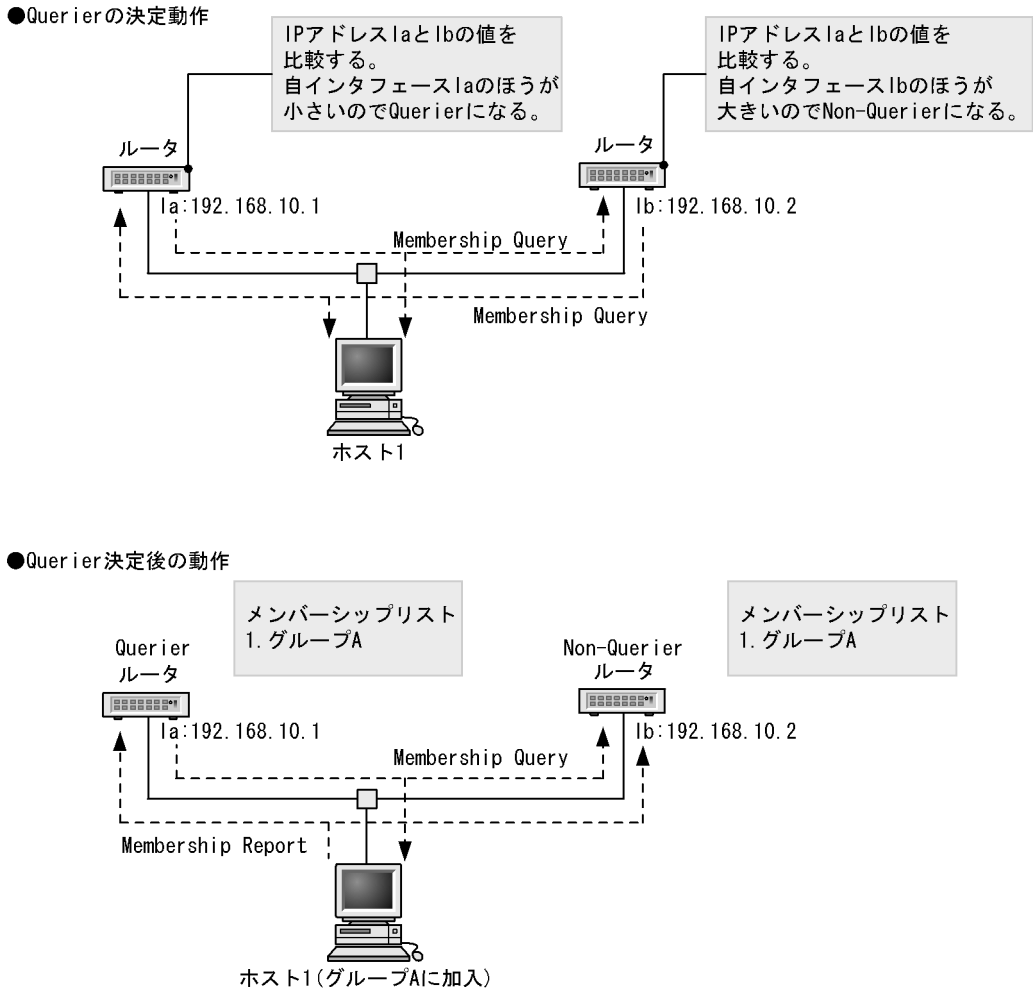


14.2.3　Querier の決定

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，定期的な Membership Query メッセージを送信する Querier を決定します。Querier の決定は，同一ネットワーク上に存在する IGMP ルータから受信した Membership Query の送信元 IP アドレスと自インタフェースの IP アドレスを比較し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，Membership Query 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 14-5　Querier と Non-Querier の決定



Querier になった場合，送信元 IP アドレスが自インタフェースより小さい Membership Query を受信するまで Querier として動作し，Membership Query を定期的（125 秒）に送信します。Non-Querier は Querier の Membership Query を受信することによって監視し，Membership Query 受信時 Membership Query の送信元 IP アドレスが自インタフェースよりも大きい場合，または Membership Query を一定時間（255 秒）受信しなかった場合，Querier として動作します。

14.2.4　グループメンバーの管理

(1) IGMPv2 使用時の IPv4 グループメンバー管理

ホストからの Membership Report を受信することでグループメンバーを登録します。また，Non-Querier でもホストからの Membership Report を受信することによって Querier 同様にグループメンバーを登録します。

Querier が，ホストからあるグループへの離脱報告である Leave Group メッセージを受信した場合，離脱

報告を受けたグループメンバーに参加している他ホストの存在を確かめるため該当するグループ宛てにMembership Query（Group-Specific Query）メッセージを連続して（1 秒間隔）送信します。このメッセージを 2 回送信したあと，Membership Report を 1 秒間受信しない場合，該当するグループを削除します。また，Non-Querier の場合は Leave Group メッセージを無視します。

(2) IGMPv3 使用時の IPv4 グループメンバー管理

IGMPv3 使用時の IPv4 グループメンバーの登録および削除について説明します。

ホストからマルチキャストグループへの加入要求を示す Report を受信することでグループ情報を登録します。ここでグループ情報とは，グループアドレスとそのグループアドレスへの送信元アドレスを指します。Querier，Non-Querier ともに Report を受信することでグループ情報を登録します。

Querier は，マルチキャストグループからの離脱要求を示す Report を受信すると，そのグループメンバーに参加しているほかのホストの存在を確かめるために，送信元リストの指定有無に応じて次に示すメッセージを 1 秒間隔で送信します。

- 送信元リスト指定無し：Group-Specific Query メッセージ
- 送信元リスト指定有り：Group-and-Source-Specific Query メッセージ

本装置が Querier の場合はこのメッセージを 2 回送信後，1 秒間 Report を受信しない場合該当するグループ情報を削除します。本装置が Non-Querier の場合は Querier が送信するこのメッセージを受信後，該当するグループ情報の削除処理を実行します。

14.2.5 IGMP タイマ

本装置が使用する IGMPv2 タイマ値を次の表に示します。

表 14-4 IGMPv2 タイマ値

タイマ	内容	タイマ値 (秒)	備考
Query Interval	Membership Query 送信周期時間	125	—
Query Response Interval	Membership Report 最大応答待ち時間	10	—
Other Querier Present Interval	Querier 監視時間	255	2 × Query Interval + Query Response Interval/2
Group Membership Interval	グループメンバーの保持時間	260	2 × Query Interval + Query Response Interval
Startup Query Interval	Startup 時 General Query を送信する時間	30	—
Last Member Query Interval	離脱要求 受信後の Specific Query 送信周期	1	—

（凡例） —：該当しない

本装置が使用する IGMPv3 タイマ値を次の表に示します。

表 14-5 IGMPv3 タイマ値

タイマ	内容	タイマ値 (秒)	備考
Query Interval	Membership Query 送信周期時間	125	―
Query Response Interval	Multicast Membership Report 最大応答待ち時間	10	―
Other Querier Present Interval	Querier 監視時間	255	Robustness Variable × Query Interval + Query Response Interval/ 2 ※
Startup Query Interval	Startup 時 General Query を送信する時間	30	―
Last Member Query Interval	離脱要求 受信後の Specific Query 送信周期	1	―
Group Membership Interval	グループメンバーの保持時間	260	Robustness Variable × Query Interval + Query Response Interval ※
Older Host Present Interval	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 × Query Interval + Query Response Interval ※

(凡例) ―：該当しない

注※ 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。

14.2.6 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 14-6 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 パケットは無視します。
version 3	IGMPv2，IGMPv3 の両方で動作可能です。 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 パケット，IGMPv2 パケットは無視します。

(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 Query を受信することで Querier を決定します（「14.2.3 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

接続はサポートしません（v2 Query 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 ホスト混在時の動作

IGMPv1 ホストと IGMPv2 ホスト，IGMPv3 ホスト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 ホストと IGMPv2 ホストは IGMPv3 Query を受信できる（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 ホストと IGMPv2 ホストの混在をサポートします。IGMPv3 ホストは無視します。

IGMPv1 ホストと IGMPv2 ホスト，IGMPv3 ホストが混在する場合，グループメンバーの登録はグループ加入を要求する IGMP のバージョンによって異なります。IGMPv1 ホストと IGMPv2 ホスト，IGMPv3 ホストが混在する場合，グループメンバーの登録を次の表に示します。

表 14-7 IGMPv1 ホストと IGMPv2 ホスト，IGMPv3 ホスト混在時のグループメンバー登録

グループ加入の要求	グループメンバーの登録
IGMPv1 で受信	IGMPv1 モードでグループメンバーを登録
IGMPv2 で受信	IGMPv2 モードでグループメンバーを登録
IGMPv3 で受信	IGMPv3 モードでグループメンバーを登録
IGMPv1 と IGMPv2 で受信	IGMPv1 モードでグループメンバーを登録
IGMPv1 と IGMPv3 で受信	IGMPv1 モードでグループメンバーを登録
IGMPv2 と IGMPv3 で受信	IGMPv2 モードでグループメンバーを登録
IGMPv1 と IGMPv2 と IGMPv3 で受信	IGMPv1 モードでグループメンバーを登録

14.2.7 静的グループ参加

IGMP 対応ホストが存在しないネットワークに IP マルチキャストパケットを中継するため，静的グループ参加機能を設定します。

静的グループ参加を設定したインタフェースは，Membership Report を受信しなくてもグループ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，該当のインタフェースの 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 でグループ参加したものと同様の動作をします。

14.2.8 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を設定した場合，PIM-SM グループの場合は (*,G) エントリ，PIM-SSM グループの場合は (S,G) エントリが作成されるまで最大 125 秒かかります。
- コンフィグレーションで設定している SSM アドレスの範囲外のグループに対して，送信元指定有りの IGMPv3 Report を受信した場合は，全送信元からのマルチキャストパケットを中継します。

14.3 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パケットはハードウェアで中継を行い，登録されていない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を行います。

(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

ハードウェアで行うマルチキャストパケット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エントリを検索します。
- マルチキャストパケットの受信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エントリが存在した場合，その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
  フィルタリングテーブルに登録された情報を参照して中継判断を行います。

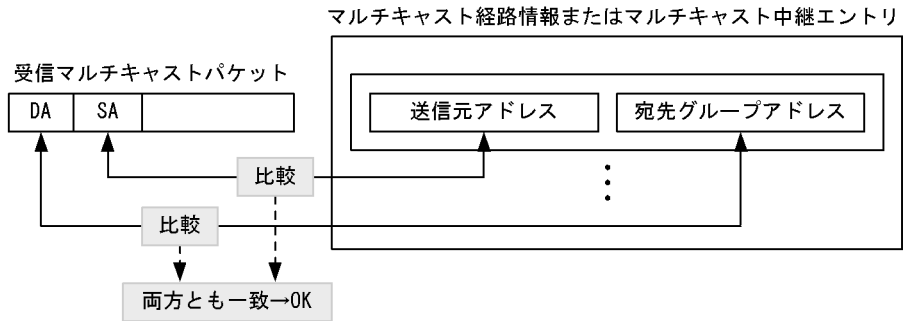
(2) ソフトウェアによるマルチキャストパケット中継処理

- ハードウェアのマルチキャスト中継エントリにエントリが存在しない場合
  ある送信元からあるマルチキャストグループ宛てのパケットを最初に受信した場合，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，ソフトウェアでパケットを中継します。同時に，ハードウェアに対して，マルチキャスト中継エントリを登録します。
- IP カプセル化処理を行う場合
  PIM-SM で一時的にランデブーポイント宛てに IP カプセル化を行い中継し，ランデブーポイントでは各中継先にデカプセル化を行い中継します。

(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 14-6 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

PIM-SM/PIM-SSM では，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ためにネガティブキャッシュを作成します。

ネガティブキャッシュは中継先インタフェースの存在しない中継エントリです。ネガティブキャッシュは，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) 系切替時の通信無停止対応機能

IPv4 PIM-SM は冗長構成運用による系切替時に，マルチキャスト中継を無停止で継続できる通信無停止対応機能をサポートしています。

系切替後，450 秒間は系切替前の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。この系切替後の 450 秒を再学習時間として，再学習時間内に学習されなかったエントリは削除されます。再学習時間の開始時と終了時は運用ログを出力します。

本機能は，コンフィグレーションコマンド ip pim nonstop-forwarding を設定した場合だけ有効になります。ただし，VRF のインタフェースで IPv4 マルチキャストを動作させた場合，本機能は無効になります。

また，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 mroute
- show ip mcache
- show ip pim mcache

(6) VRF 機能【OP-NPAR】

複数の VRF で IPv4 マルチキャストを動作させた場合，IPv4 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 IP アドレスの IPv4 マルチキャスト中継エントリを作成できます。また，IPv4 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。

なお，VRF では PIM-DM は動作しません。

14.4 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。

14.4.1 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 IPv4 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-DM（Protocol Independent Multicast-Dense Mode）
  ユニキャスト IPv4 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。マルチキャストパケットを中継したあと，不要な経路を切り離します。

マルチキャストプロトコルの適応形態を次の表に示します。

表 14-8 マルチキャストルーティングプロトコルの適応形態

マルチキャストプロトコル	適応ネットワーク
PIM-SM	マルチキャストグループメンバーがまばらで散らばっているネットワーク 小規模から大規模のマルチキャストネットワークで使用します
PIM-SSM	マルチキャストグループメンバーがまばらで散らばっているネットワーク 主に特定のサーバから配信する場合に使用します
PIM-DM	マルチキャストグループメンバーが密集しているネットワーク 主に小規模なマルチキャストネットワークで使用します

本装置では PIM-SM と PIM-DM は同時に動作できません。コンフィグレーションでどちらかのプロトコルを指定します。なお，PIM-SSM は PIM-SM の拡張機能なので，PIM-SM と PIM-SSM は同時に動作できます。

また，同一ネットワーク内に PIM-SM が動作しているルータと PIM-DM が動作しているルータが混在している場合，各ルータ間でマルチキャストパケットが正しく中継されません。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，すべてのルータで同じマルチキャストプロトコル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，「14.6.3 適応ネットワーク構成例」も参照してください。

14.4.2 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，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することによって，マルチキャストパケット送信元からの最短パスを使用して最短パス経由に切り替え，マルチキャストパケットを中継します。

本装置が送信する PIM-SM メッセージのフォーマットおよび設定値は RFC2362 に従います。

(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。

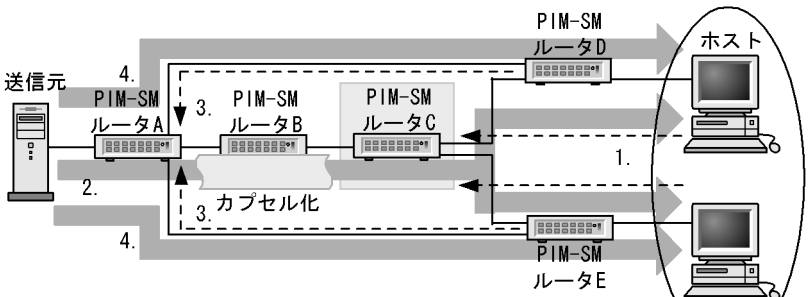
表 14-9 PIM-SM メッセージのサポート仕様

メッセージタイプ	機能
PIM-Hello	PIM 隣接ルータの検出
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
PIM-Assert	Forwarder の決定
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	BSR を決定する。また，ランデブーポイントの情報を配信する。
PIM-Candidate-RP-Advertisement	ランデブーポイントが BSR に自ランデブーポイント情報を通知する。

(2) 動作

各 PIM-SM ルータは IGMP で学習したグループ情報をランデブーポイントに通知します。ランデブーポイントは各 PIM-SM ルータからグループ情報を受信することで各グループの存在を認識します。したがって，PIM-SM は最初にマルチキャストパケットをその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ーに配送するために，送信元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。次に送信元から各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元からの最短パス配送ツリーを形成します。これによって送信元から各グループメンバーへのマルチキャストパケット中継は最短パスで行われます。PIM-SM の動作概要を次の図に示します。

図 14-7 PIM-SM の動作概要



1. グループ参加および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

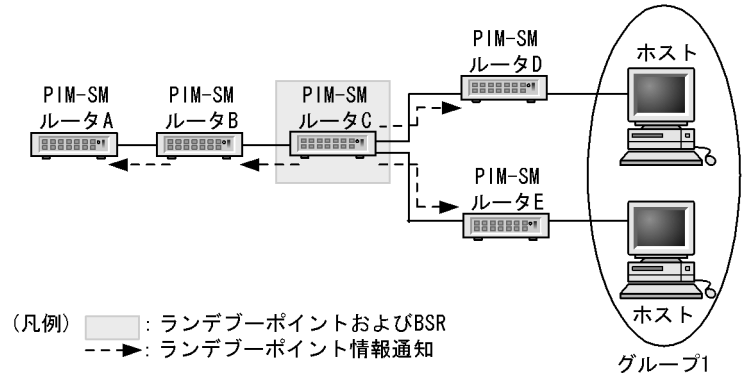
（凡例） ：ランデブーポイントおよびBSR

(a) ランデブーポイントおよびブートストラップルータ（BSR）

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（BSR）はコンフィグレーションで設定します。本装置では BSR はネットワーク（VPN）当たり最大 16 台とします。BSR はランデブーポイントの情報（IP 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。この通知はホップバイ

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 BSR の役割を次の図に示します。

図 14-8 ランデブーポイントおよびブートストラップルータ（BSR）の役割

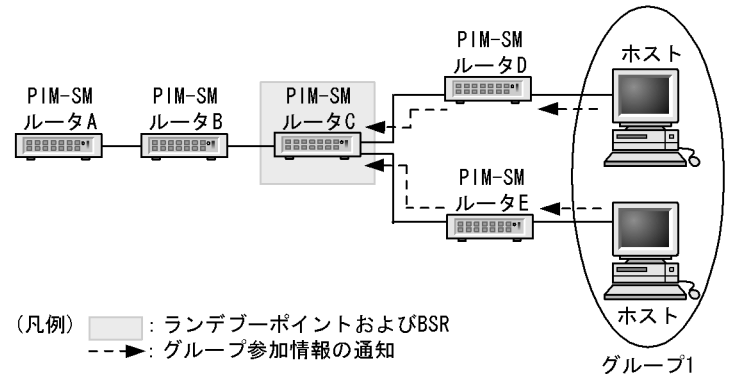


この図で，BSR（PIM-SM ルータ C）はランデブーポイント情報をすべてのマルチキャストインタフェースに通知します。ランデブーポイント情報を受信したルータはランデブーポイントの IP アドレスを学習し，受信したインタフェース以外でマルチキャストルータが存在するすべてのインタフェースにランデブーポイント情報を通知します。

(b) ランデブーポイントへのグループ参加情報の通知

各ルータは IGMP で学習したグループ参加情報をランデブーポイントに通知します。ランデブーポイントはグループ情報を受信することで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グループ参加情報の通知を次の図に示します。

図 14-9 ランデブーポイントへのグループ参加情報の通知



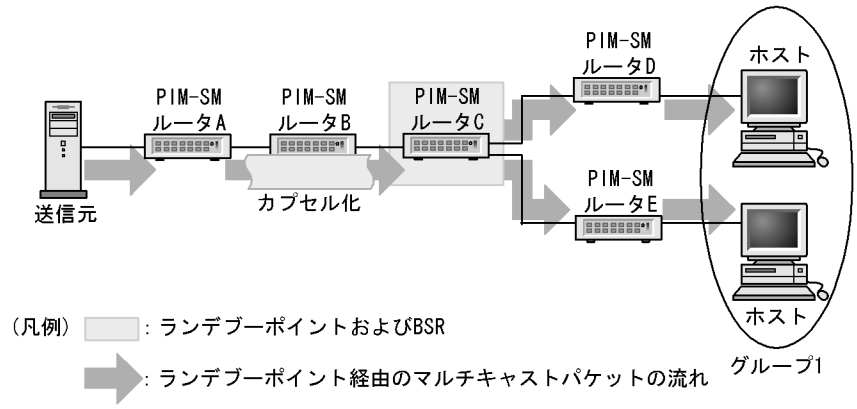
この図で，各ホストは IGMP でグループ 1 に参加します。PIM-SM ルータ D および PIM-SM ルータ E はグループ 1 情報を学習し，ランデブーポイント（PIM-SM ルータ C）にグループ 1 情報を通知します。ランデブーポイント（PIM-SM ルータ C）はグループ 1 情報を受信することによって，受信したインタフェースにグループ 1 が存在することを学習します。

(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（カプセル化）

送信者 S1 がグループ 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 パケット）して送信します（ランデブーポイントの IP アドレスは (a) で学習済み）。ランデブーポイント（PIM-SM ルータ C）は IP カプセル化したパケットを受信すると，デカプセル化してグループ 1 が存在す

るインタフェースにグループ 1 宛てのマルチキャストパケットを中継します（グループ 1 の存在は (b) で学習済み）。PIM-SM ルータ D および PIM-SM ルータ E は，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，グループ 1 が存在するインタフェースにパケットを中継します（グループ 1 の存在は (b) 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（カプセル化）を次の図に示します。

図 14-10　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（カプセル化）

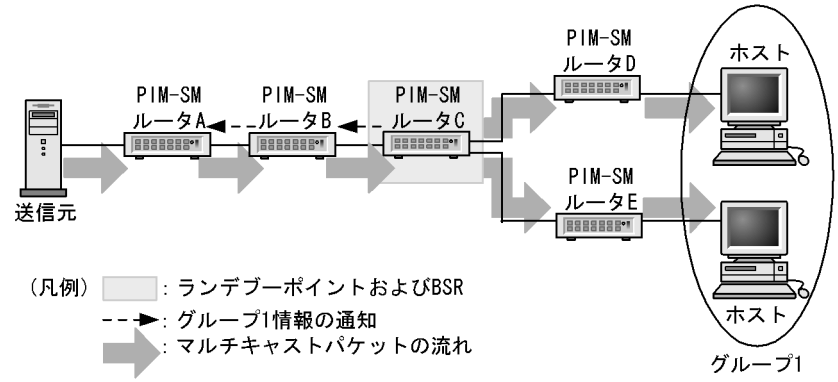


(d) ランデブーポイント経由のマルチキャストパケット通信（デカプセル化）

ランデブーポイント（PIM-SM ルータ C）は IP カプセル化したパケットを受信すると，カプセル化を解除してグループ 1 が存在するインタフェースにグループ 1 宛てのマルチキャストパケットを中継します。

ランデブーポイントはこの処理後，送信元サーバへの最短経路方向にグループ 1 情報を通知します。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にグループ 1 の存在を認識（学習）します。PIM-SM ルータ A は送信元サーバが送信したグループ 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。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，PIM-SM ルータ E はグループ 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（デカプセル化）を次の図に示します。

図 14-11　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（デカプセル化）

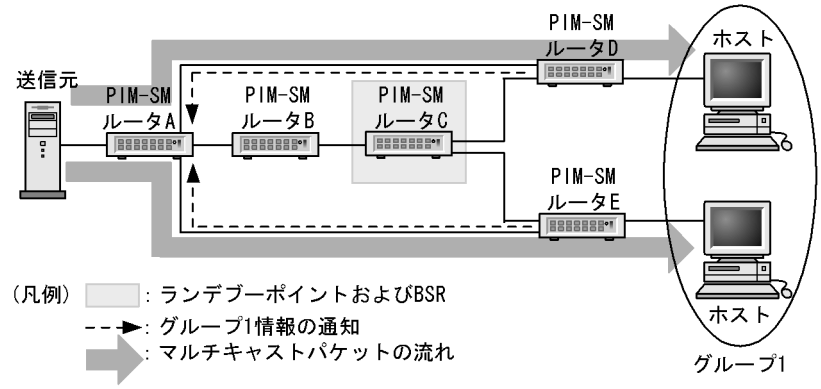


(e) 最短パスのマルチキャストパケット通信

PIM-SM ルータ D および PIM-SM ルータ E は，送信元サーバのグループ 1 宛てマルチキャストパケットを受信した場合（(c) で説明），PIM-SM ルータ D および PIM-SM ルータ E は送信者 S1 に対して最短のパス（既存のユニキャストルーティング情報）の方向にグループ 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グループ 1 の存在を認識し，送信元サーバのグループ 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。

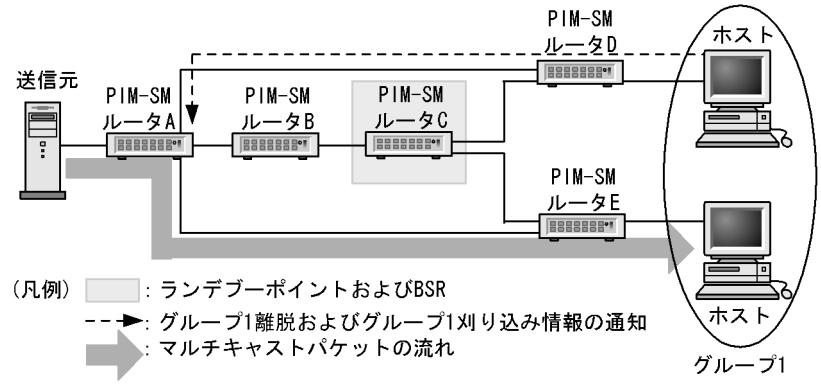
図 14-12　最短パスのマルチキャストパケット通信



(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，ホストが IGMP でグループ 1 から離脱した場合，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 14-13　マルチキャスト配送ツリーの刈り込み



(3)　近隣検出

PIM-SM ルータはマルチキャストができる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-RoutersIP マルチキャスト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 PIM 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（RFC4601 および draft-ietf-pim-sm-bsr-07 に準拠）。

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ずに送信します。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フォワードされる可能性があります。

PIM-SM ルータは同一 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フォワードする場合，PIM-Assert メッセージを使っ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，送信元ネットワークに対して最適な一つのルータをフォワーダとして選択します。

フォワーダ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。

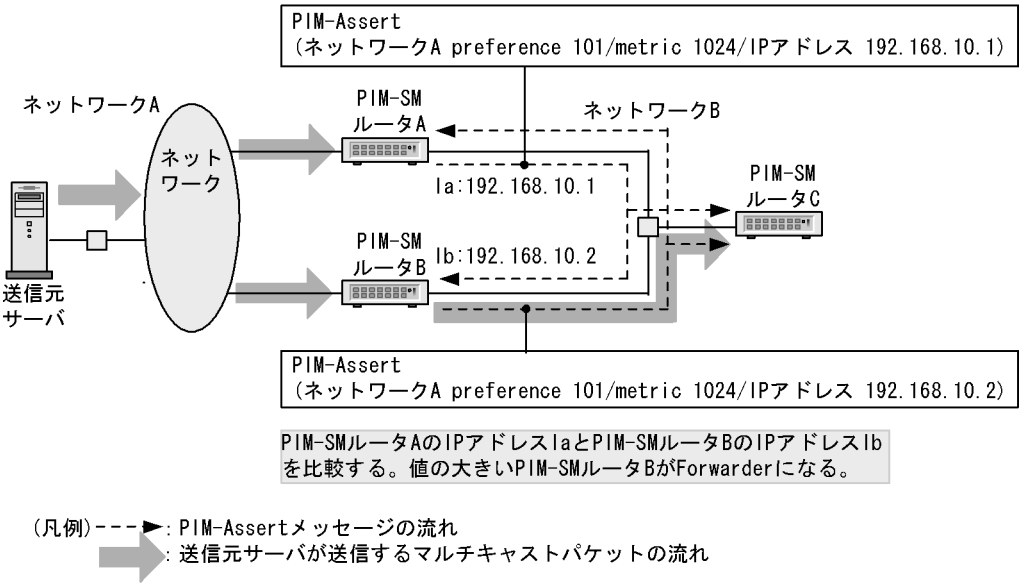
PIM-Assert メッセージによるフォワーダを決定する流れを次に示します。

1. プリファレンスを比較して，値が小さいルータがフォワーダになります。
2. プリファレンスが等しい場合に，メトリックを比較して，値が小さいルータがフォワーダになります。
3. メトリックが等しい場合に，各ルータの IP アドレスを比較して，IP アドレスが大きいルータがフォワーダになります。

本装置はマルチキャスト経路のプリファレンスを 101，メトリックを 1024 固定で PIM-Assert メッセージを送信します。ただし，送信者と直接接続する場合は，プリファレンスを 0，メトリックを 0 固定で PIM-Assert メッセージを送信します。

Forwarder の決定を次の図に示します。

図 14-14 Forwarder の決定

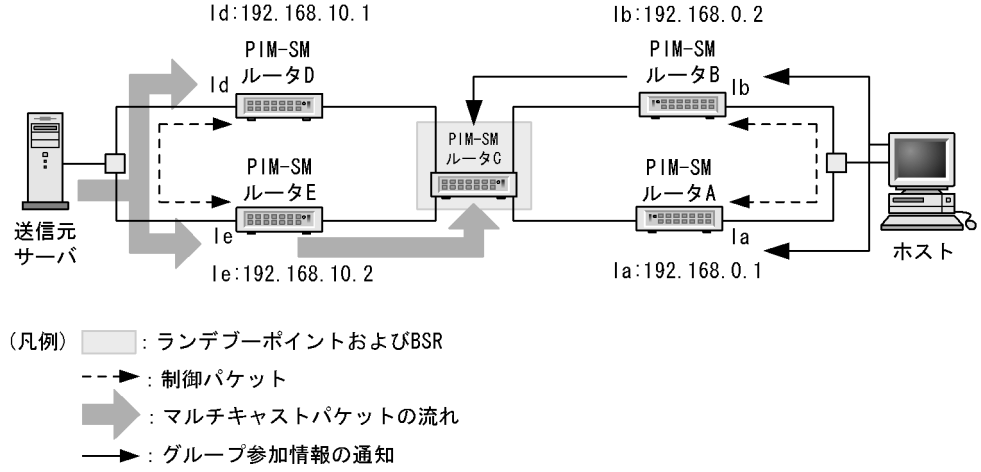


(5) DR の決定および動作

同一 LAN 上で複数の PIM-SM ルータが存在する場合，その LAN 上での中継代表ルータ（DR）を決定します。そのインタフェース上で一番大きい IP アドレスの PIM-SM ルータが DR となります。受信ホスト

からのグループ参加情報は DR がランデブーポイント宛てにグループ参加情報の通知を行います。送信元サーバ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 14-15　DR の動作

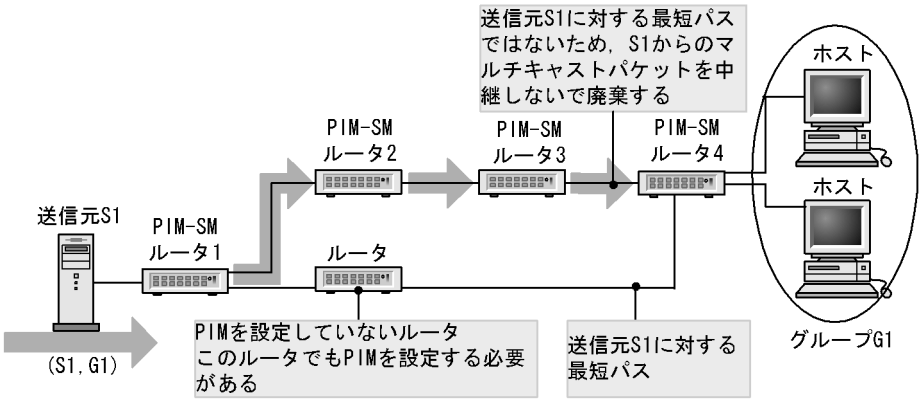


PIM-SM ルータ A と PIM-SM ルータ B の IP アドレスを比較して PIM-SM ルータ B の IP アドレスが大きい場合，PIM-SM ルータ B が DR となってランデブーポイントにグループ参加情報の通知を行います。PIM-SM ルータ D と PIM-SM ルータ E の IP アドレスを比較して PIM-SM ルータ E の IP アドレスが大きい場合，PIM-SM ルータ E が DR となってランデブーポイントに対して IP カプセル化パケットを中継します。

(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フォワード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 の設定が必要になります。

図 14-16　冗長経路時の注意



(7) PIM-SM の付加機能

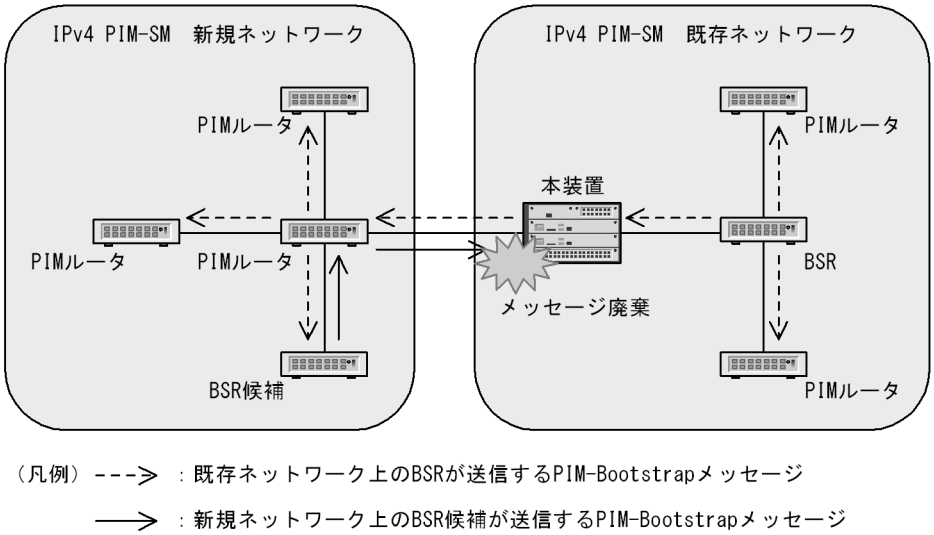
(a) ブートストラップメッセージ受信抑止機能【OP-MBSE】

運用中のマルチキャストネットワークに新しいネットワークを構築する場合，BSR 候補の設定を誤るとその BSR 候補が BSR となって，接続したマルチキャストネットワーク全体のマルチキャスト通信が停止す

るおそれがあります。

本機能は，新規ネットワーク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 pim accept-bootstrap を設定することで，新規ネットワークでの誤った設定によって受信した PIM-Bootstrap メッセージを廃棄する機能です。この結果，運用中のマルチキャストネットワークを保護できます。本機能の動作を次の図に示します。

図 14-17　ブートストラップメッセージ受信抑止機能の動作



ネットワークの境界にある本装置では，新規ネットワーク上の BSR 候補が送信する PIM-Bootstrap メッセージを廃棄します。これによって，新規ネットワークの PIM-Bootstrap メッセージが既存ネットワーク内へ中継されるのを防ぎます。一方，既存ネットワーク上の BSR が送信する PIM-Bootstrap メッセージは新設ネットワークに中継されます。

(8) 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 14-10　PIM-SM タイマ

タイマ名	内容	デフォルト値（秒）	コンフィグレーションによる設定範囲（秒）	備考
Hello-Period	PIM-Hello メッセージの送信周期	30	5 ～ 3600	―
Hello-Holdtime	隣接関係の保持期間	105	3.5 × Hello-Period	左記計算式より算出。
Assert-Timeout	PIM-Assert による中継抑止期間	180	―	―
Join/Prune-Period	PIM-Join/Prune メッセージの送信周期	60	30 ～ 3600	最大で +50% の揺らぎが生じます。
Join/Prune-Holdtime	経路情報および中継先インタフェースの保持期間	210	3.5 × Join/Prune-Period	左記計算式より算出。

タイマ名	内容	デフォルト値（秒）	コンフィグレーションによる設定範囲（秒）	備考
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※1	1/3 × Join/Prune-Holdtime	0 ～ 300	※2
Data-Timeout (Keep-alive-time)	マルチキャスト中継エントリの保持期間	210	0(無期限), 60 ～ 43200	最大で +90 秒の誤差が発生します。
Register-Supression-Timer	カプセル化送信の抑止期間	60	－	最大で± 30 秒の揺らぎが生じます。
Probe-Time	カプセル化送信の再開確認を送信する時間	5	5 ～ 60	デフォルトの 5 秒では Register-Supression-Timer が満了する 5 秒前にカプセル化送信の再開確認 (Null-Register) を一度だけ送信します。※3
C-RP-Adv-Period	ランデブーポイント候補の通知周期	60	－	－
RP-Holdtime	ランデブーポイント保持期間	150	2.5 × C-RP-Adv-Period	左記計算式より算出。
Bootstrap-Period	BSR メッセージ送信周期	60	－	－
Bootstrap-Timeout	BSR メッセージの保持期間	130	2 × Bootstrap-Period+10	左記計算式より算出。
BS_Rand_Override	BSR 切り替え遅延	5 ～ 23	－	－
Negative-Cache-Holdtime (PIM-SM)	ネガティブキャッシュの保持期間	210	10 ～ 3600	PIM-SSM の場合は 3600 秒の固定。

(凡例) －：該当しない

注※ 1

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 Join を受信した時の 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※ 2

本タイマ値は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。ただし，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※ 3

本タイマ値を 10 以上に設定すると，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。

(9) 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の制限事項に注意してください。本装置は RFC2362（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 14-11 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。	本装置では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。	本装置では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。	本装置の 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	Join/Prune メッセージはネットワークの MTU を超えてもフラグメントすることができる。	本装置では送信する PIM-Join/Prune メッセージのサイズが大きい場合，8KB 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。
PMBR との接続	RFC では PMBR(PIM Border Router) との接続および (*，*，RP) エントリについての仕様が記述されている。	本装置では PMBR との接続をサポートしていない。また，(*，*，RP) エントリもサポートしていない。
最短経路への切り替え	最短経路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。	本装置では last-hop-router にて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経路へ切り替える。

14.4.3 IPv4 PIM-SSM

PIM-SSM は PIM-SM の拡張機能です。PIM-SM と PIM-SSM は同時動作できます。PIM-SSM が使用するマルチキャストアドレスは 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 が動作するマルチキャストアドレス（グループアドレス）のアドレス範囲を指定できます。指定したアドレス以外では PIM-SM が動作します。

PIM-SM はマルチキャストエントリ作成にマルチキャスト中継パケットが必要なのに対し，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，該当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，パケットのカプセル化および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）のホストと接続している場合に動作します。また，本装置では IGMPv2 または IGMPv3（EXCLUDE モード）のホストから PIM-SSM を利用できるようにする手段を提供します。

(1) PIM-SSM メッセージサポート仕様

PIM-SM メッセージサポート仕様（「14.4.2 IPv4 PIM-SM (1) PIM-SM メッセージサポート仕様」）と同じです。

(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範囲を設定します。
- IGMPv3（INCLUDE モード）が動作するホスト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）が動作するホスト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。

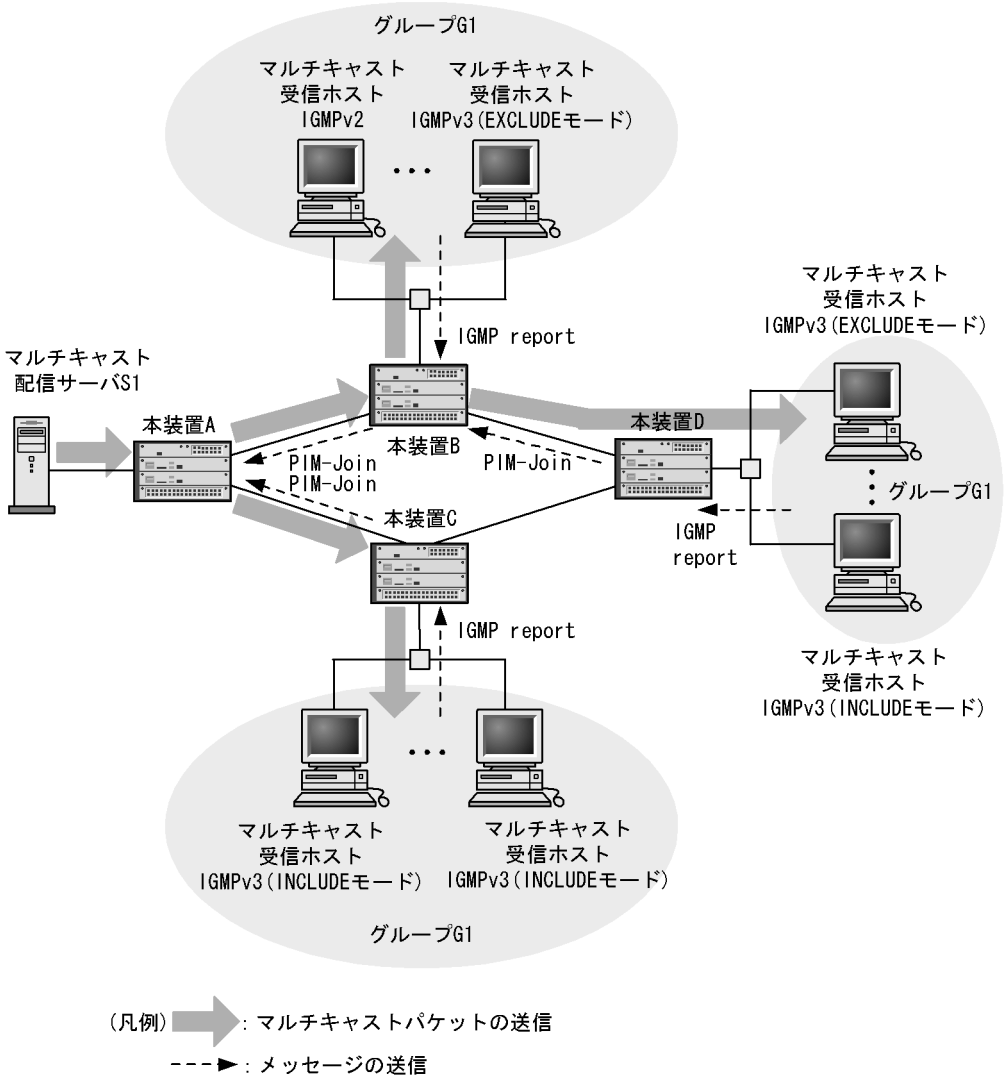
（3） PIM-SSM 動作（ホストが IGMPv3（INCLUDE モード）の場合）

マルチキャストパケット配信サーバ（送信元アドレス：S1）がグループ 1（グループアドレス：G1）にマルチキャストパケットを配信する場合の動作を次に示します。

1. ホストからマルチキャストグループに参加するための要求（IGMPv3（INCLUDE モード））を受信します。
2. 参加要求（IGMPv3（INCLUDE モード））を受信した装置は通知されたグループアドレス (G1) と送信元アドレス (S1) から送信元アドレス (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。PIM-Join メッセージを受信した各装置は送信元アドレス (S1) の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。
3. マルチキャストパケット配信サーバ (S1) がグループ 1(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 14-18　PIM-SSM **の動作概要**



(4) PIM-SSM **動作（ホストが** IGMPv2 **または** IGMPv3（EXCLUDE **モード）の場合）**

マルチキャストパケット配信サーバ（送信元アドレス：S1）がグループ 1（グループアドレス：G1）にマルチキャストパケットを配信する場合の動作を次に示します。

1. ホストからマルチキャストグループに参加するための要求（IGMPv2 または IGMPv3（EXCLUDE モード））を受信します。
2. 参加要求（IGMPv2 または IGMPv3（EXCLUDE モード））を受信した装置は通知されたグループアドレス (G1) とコンフィグレーション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，コンフィグレーションで設定した送信元アドレス (S1) への最短経路方向（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。PIM-Join メッセージを受信した各装置は送信元アドレス (S1) への最短経路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。
3. マルチキャストパケット配信サーバ (S1) がグループ 1(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パケットを中継します。

PIM-SSM の動作概要については，「図 14-18　PIM-SSM の動作概要」を参照してください。

(5) 近隣検出

PIM-SM（「14.4.2　IPv4 PIM-SM　(3) 近隣検出」）と同じです。

(6) Forwarder の決定

PIM-SM（「14.4.2　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（「14.4.2　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（「14.4.2　IPv4 PIM-SM　(6) 冗長経路時の注意事項」）と同じです。

14.4.4　IPv4 PIM-DM

PIM-DM 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して，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。また，ユニキャストルーティングを利用することで，マルチキャストパケット送信元からの最短パスを使用してマルチキャストパケットを中継します。

本装置が送信する PIM-DM メッセージのフォーマットおよび設定値は PIM-DM インターネットドラフトに従います。

(1) PIM-DM メッセージサポート仕様

PIM-DM メッセージのサポート仕様を次の表に示します。

表 14-12　PIM-DM メッセージのサポート仕様

メッセージタイプ	機能
PIM-Hello	PIM 隣接ルータの検出
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
PIM-Assert	Forwarder の決定
PIM-Graft	マルチキャスト配送ツリーの再接続
PIM-Graft-Ack	PIM-Graft メッセージに対する応答

(2) 動作

PIM-DM はマルチキャストパケットをその送信元ネットワークからすべてのグループメンバに配送するために，送信元を頂点とした配送ツリーを形成します。この配送ツリーは，グループのすべてのメンバに到達するために必要な最小の配送ツリーとして保たれます。グループメンバが存在しないインタフェースの場合，最初のマルチキャストパケット中継後に PIM-Prune メッセージで刈り込まれます。新しいメンバがグループに参加した場合，PIM-Graft メッセージの送受信によって再度配送ツリーに追加されます。

また，送信元から各グループへの最短パスの決定には，ユニキャストルーティングを使用します。ユニキャストルーティングで得た最短パスは，受信したマルチキャストパケットを中継するときの，送信元か

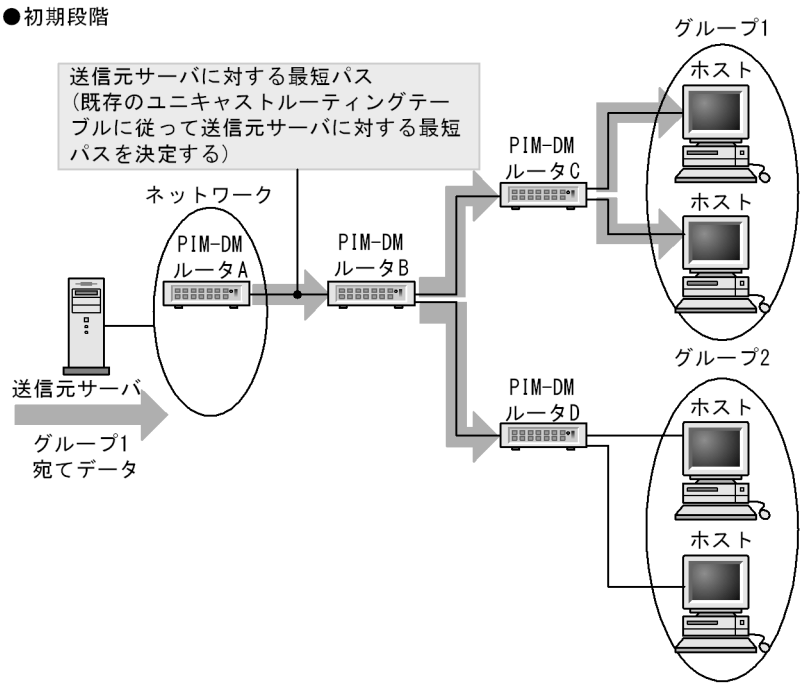
ら最短パス経由で受信できているかを判断する Reverse Path Forwarding チェックで使用します。

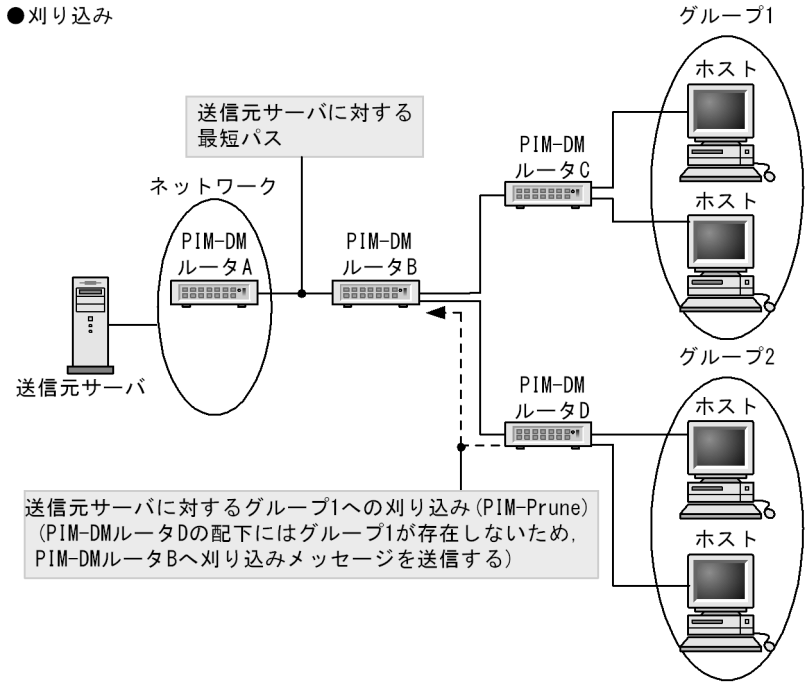
PIM-DM は次の順序で動作します。

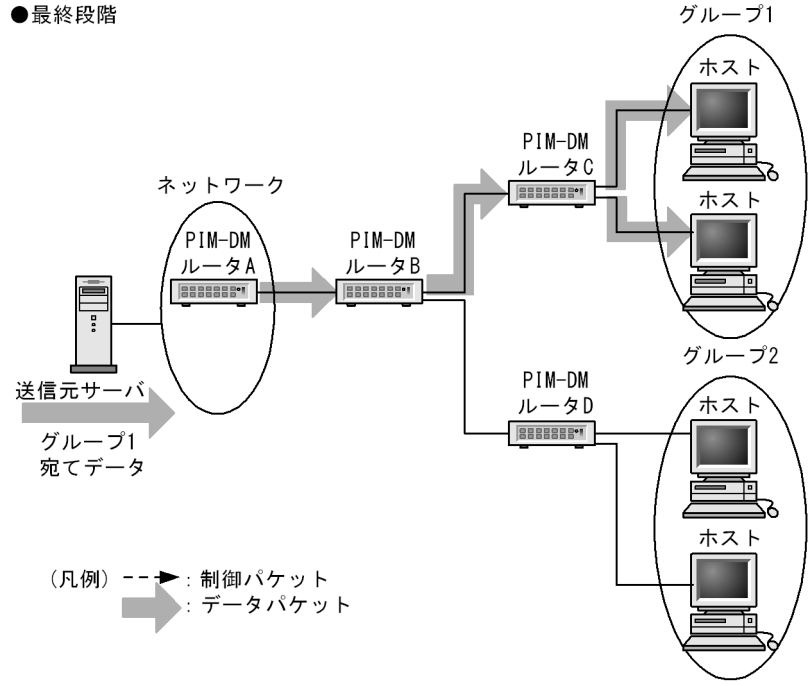
1. 最初のマルチキャストパケットを上流インタフェースから受信すると，受信インタフェースを除いて，中継できるすべてのインタフェースにマルチキャストパケットを中継します。
2. 中継先のないルータは，上流ルータに対して刈り込みメッセージ（PIM-Prune メッセージ）を送信します。
3. 刈り込み終了後，そのパケットを必要とするホストに対するマルチキャスト配送ツリーを形成して，マルチキャストパケットを中継します。

PIM-DM の動作の流れを次の図に示します。

図 14-19　PIM-DM によるマルチキャストパケット中継処理







(3) 近隣検出

PIM-SM(「14.4.2 IPv4 PIM-SM (3) 近隣検出」)と同じです。

(4) Forwarder の決定

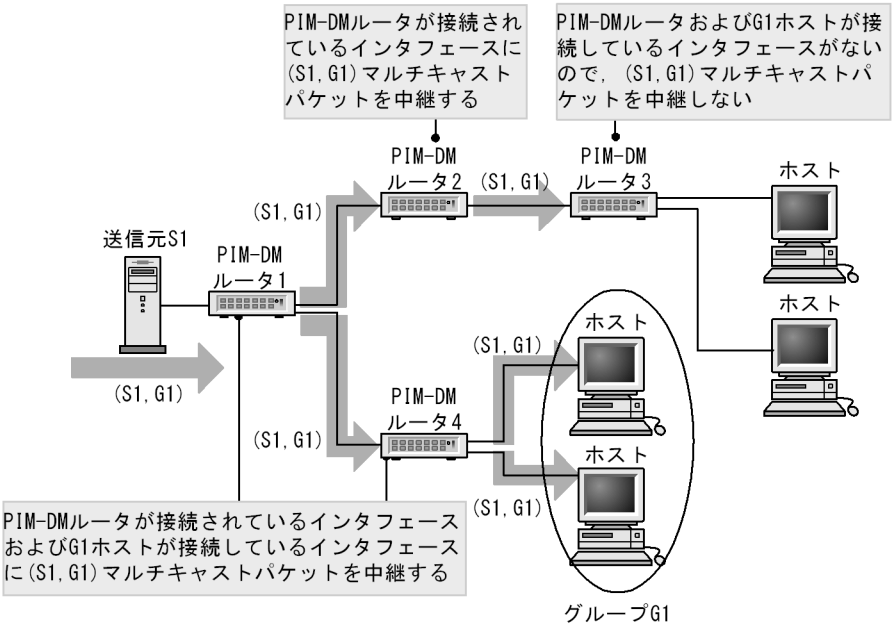
PIM-SM(「14.4.2 IPv4 PIM-SM (4) Forwarder の決定」)と同じです。

(5) マルチキャスト配送ツリーの刈り込み

(a) 刈り込み前の動作

最初にマルチキャストパケットを受信したとき，PIM-DM ルータは中継できるインタフェース（PIM-DM 隣接ルータが存在する，または IGMP メンバーシップ情報があるインタフェース）をすべて配送ツリーに登録します。中継できるインタフェースがない場合，送信元に対する次ホップルータ（Forwarder）に対して，刈り込みメッセージ（PIM-Prune メッセージ）で中継する必要がないことを通知します。
PIM-Prune メッセージを受信した PIM-DM ルータは，あらかじめ登録してあった配送ツリーから PIM-Prune メッセージを受信したインタフェースを刈り込みます。マルチキャスト配送ツリーの刈り込み前の動作を次の図に示します。

図 14-20 マルチキャスト配送ツリーの刈り込み前の動作

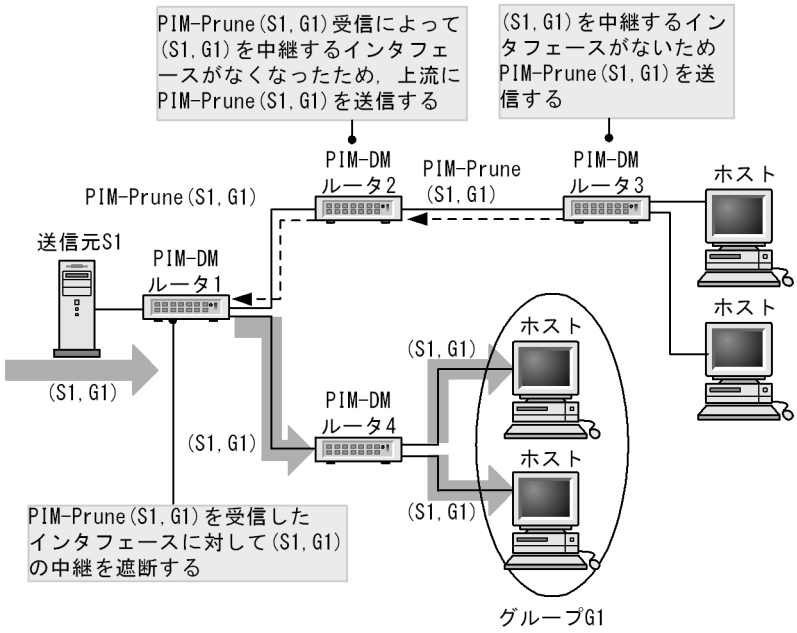


（凡例） (S1,G1)：送信元S1，宛先G1のマルチキャストパケット

(b) 刈り込み動作

PIM-DM ルータ 3 では，(S1,G1) マルチキャストパケットを中継するインタフェースがありません。このため，(S1,G1) マルチキャストパケットを受信したインタフェースに対して PIM-Prune(S1,G1) メッセージを送信して，該当するインタフェースから (S1,G1) マルチキャストパケットを受信する必要がないことを通知します。また，PIM-DM ルータ 2 は PIM-DM ルータ 3 から PIM-Prune(S1,G1) メッセージを受信したため，(S1,G1) マルチキャストパケットを中継するインタフェースがなくなります。このため，(S1,G1) マルチキャストパケットを受信したインタフェースに対して PIM-Prune(S1,G1) メッセージを送信します。マルチキャスト配送ツリーの刈り込み動作を次の図に示します。

図 14-21　マルチキャスト配送ツリーの刈り込み動作



（凡例）　PIM-Prune(S1,G1)：送信元S1，宛先G1のマルチキャスト経路の刈り込み

(6) マルチキャスト配送ツリーの再接続

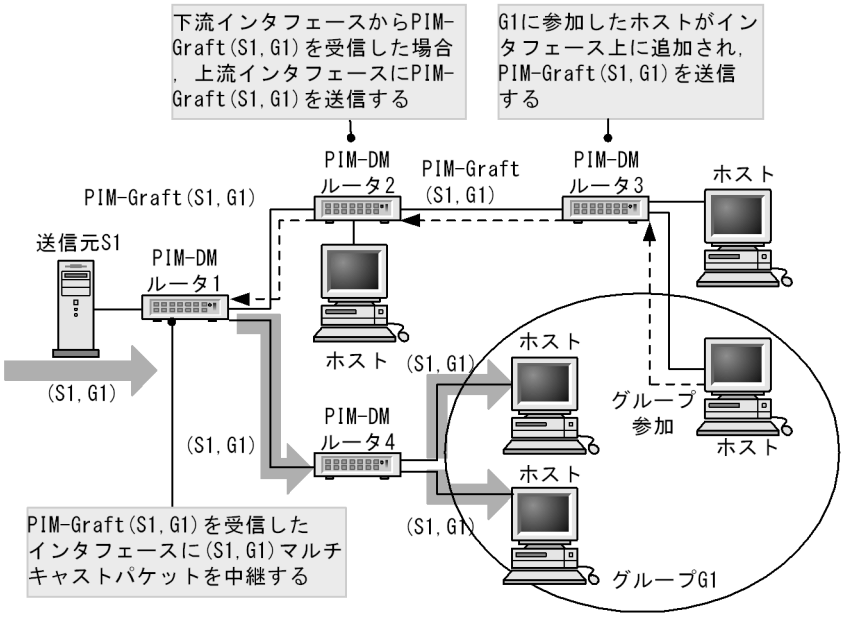
マルチキャスト配送ツリーから刈り込んだツリーへは，該当する送信元から該当するグループへパケットを中継しません。しかし，刈り込んだツリーに新しくマルチキャストグループへの参加があった場合，刈り込んだツリーに対し再接続メッセージ（PIM-Graft メッセージ）を送信します。PIM-DM ルータは PIM-Graft メッセージを受信したら配送ツリーに該当するインタフェースを追加して，PIM-Graft Ack メッセージを返信します。

(a) 再接続動作

PIM-DM ルータ 3 では，新しくグループ G1 に参加したホストが下流インタフェース上に追加された場合，G1 に対する PIM-Prune(S1,G1) メッセージを送信したインタフェースへ PIM-Graft(S1,G1) メッセージを送信して，再接続を要求します。PIM-DM ルータ 2 では，PIM-Prune(S1,G1) メッセージを受信したインタフェースから PIM-Graft(S1,G1) メッセージを受信した場合，PIM-Prune(S1,G1) メッセージを送信したインタフェースへ PIM-Graft(S1,G1) メッセージを送信します。

「図 14-21　マルチキャスト配送ツリーの刈り込み動作」に示すマルチキャスト配送ツリーの刈り込み状態から該当するマルチキャストグループに新しく参加があった場合の，マルチキャスト配送ツリーへの再接続動作を次の図に示します。

図 14-22 マルチキャスト配送ツリーへの再接続動作



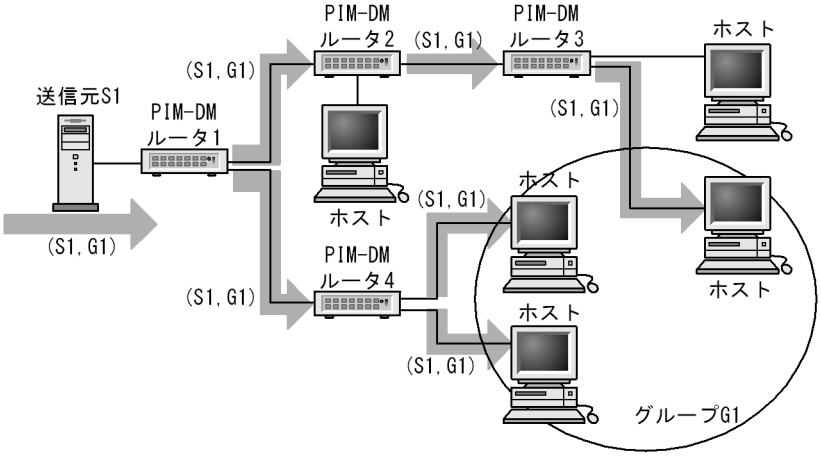
（凡例） (S1,G1)：送信元S1，宛先G1のマルチキャストパケット
PIM-Graft(S1,G1)：送信元S1，宛先G1のマルチキャスト経路の再接続

(b) 再接続後のマルチキャストパケットの流れ

PIM-DM ルータ 1 にはマルチキャストパケットが中継されているため，PIM-Graft(S1,G1) メッセージを受信したインタフェースへ (S1,G1) マルチキャストパケットを中継します。

「図 14-21 マルチキャスト配送ツリーの刈り込み動作」に示すマルチキャスト配送ツリーの刈り込み状態から該当するマルチキャストグループに新しく参加があった場合の，マルチキャスト配送ツリーへの再接続後動作を次の図に示します。

図 14-23 マルチキャスト配送ツリーへの再接続後動作



（凡例） (S1,G1)：送信元S1，宛先G1のマルチキャストパケット

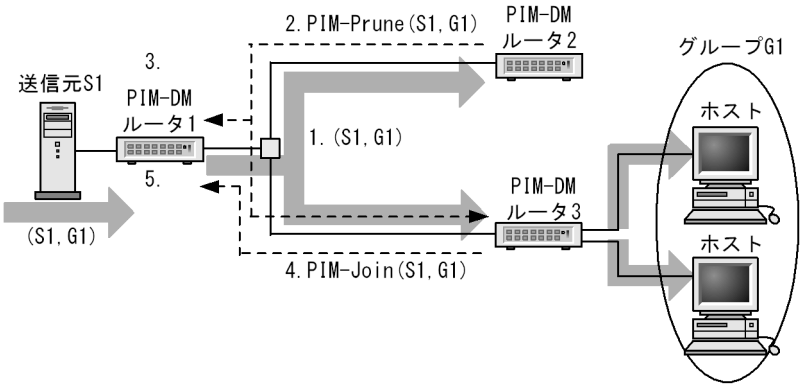
(7) 同一 LAN 上の刈り込み

同一 LAN 上で PIM-DM ルータ 2 が PIM-DM ルータ 1 へグループ G1 に対する PIM-Prune メッセージを送信した場合，PIM-DM ルータ 1 は該当するインタフェースを刈り込むまで 4 秒間待ちます。その間にグ

ループ G1 に対する PIM-Join メッセージ（以前に送信された PIM-Prune メッセージをキャンセルするメッセージ）を受信しない場合，該当するインタフェースを刈り込みます。PIM-Join メッセージを受信した場合は，刈り込みを中止します。

PIM-DM ルータ 2 から PIM-DM ルータ 1 へ送信された PIM-Prune メッセージを受信した PIM-DM ルータ 3 で，PIM-DM ルータ 1 からグループ G1 宛てのパケットを受信したい場合は，3 秒以内に PIM-DM ルータ 1 へ PIM-Join メッセージを送信して PIM-DM ルータ 1 に刈り込みを中止させます。同一 LAN 上での PIM-Prune および PIM-Join メッセージの動作を次の図に示します。

図 14-24　同一 LAN 上での PIM-Prune および PIM-Join メッセージの動作

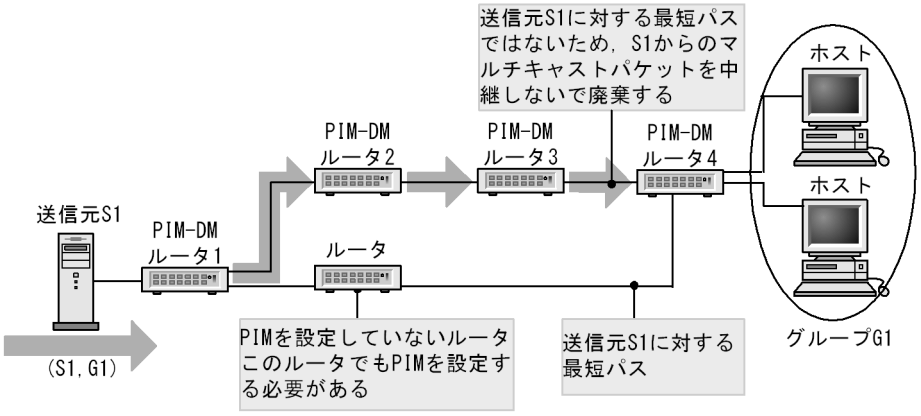


1. PIM-DM ルータ 1 が G1 宛てのマルチキャストパケットを送信する。
2. PIM-DM ルータ 2 では G1 宛てのデータは必要ないため，PIM-Prune(S1,G1) メッセージを PIM-DM ルータ 1 へ送信する。
3. PIM-DM ルータ 1 が PIM-Prune(S1,G1) メッセージを受信したため，PIM-Join(S1,G1) メッセージを 4 秒間監視する。
4. PIM-DM ルータ 3 が PIM-Prune(S1,G1) メッセージを受信したあと，ルータ 3 配下に G1 が存在するため PIM-Join(S1,G1) メッセージを PIM-DM ルータ 1 へ送信する。
5. PIM-DM ルータ 1 が 4 秒以内に PIM-Join(S1,G1) メッセージを受信したため，刈り込みを中止する。

(8) 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ため注意してください。したがって，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 の設定が必要になります。

図 14-25　冗長経路時の注意



(9) PIM-DM タイマ仕様

PIM-DM が使用するタイマ値を次の表に示します。

表 14-13 PIM-DM タイマ

タイマ名	内容	デフォルト値（秒）	コンフィグレーションによる設定範囲（秒）	備考
Hello-Period	PIM-Hello メッセージ周期	30	―	―
Hello-Holdtime	近隣タイムアウト	105	―	3.5 × PIM-Hello メッセージ周期
Assert-Timeout	PIM-Assert タイムアウト	210	―	―
Deletion-Delay-Time	PIM-PruneDelay タイマ	4	―	―
Data-Timeout (Keep-alive-time)	マルチキャスト中継エントリの保持期間	210	0（無期限），60 ～ 43200	最大で＋ 90 秒の誤差が発生します。
Prune Life Time	Prune Life Time	210	―	PIM-Prune メッセージを受信している場合は，受信している PIM-Prune の Life time の最大値

（凡例） ―：該当しない

(10) PIM-DM 使用上の注意事項

PIM-DM 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注意してください。本装置はインターネットドラフト（draft-ietf-pim-v2-dm-03）に準拠していますが，一部インターネットドラフトとの差分があります。インターネットドラフトとの差分を次の表に示します。

表 14-14 インターネットドラフトとの差分

項目	インターネットドラフト	本装置
ユニキャスト経路の切り替え	ユニキャスト経路に変化があった場合，(S,G) エントリも同様に変化する。 • Prune メッセージを古い上流インタフェースに送信すべきである。 • Graft メッセージを新しい上流インタフェースに送信すべきである。	本装置ではユニキャスト経路の切り替えによって，マルチキャスト経路情報の上流インタフェースを切り替えたときに新しい上流インタフェースに PIM-Graft メッセージを送信しますが，古い上流インタフェースに PIM-Prune メッセージを送信しません。
PIM-Hello オプション	PIM Hello メッセージには Generation ID オプションを付加すべきである。	本装置では PIM-Hello メッセージに GenerationID オプションを付けないで送信します。受信した PIM-Hello メッセージに GenerationID オプションが付いていた場合，GenerationID オプションを無視します。

14.4.5 IGMPv3 使用時の IPv4 経路制御動作

(1) IGMPv3 使用時の IPv4 PIM-SSM 動作

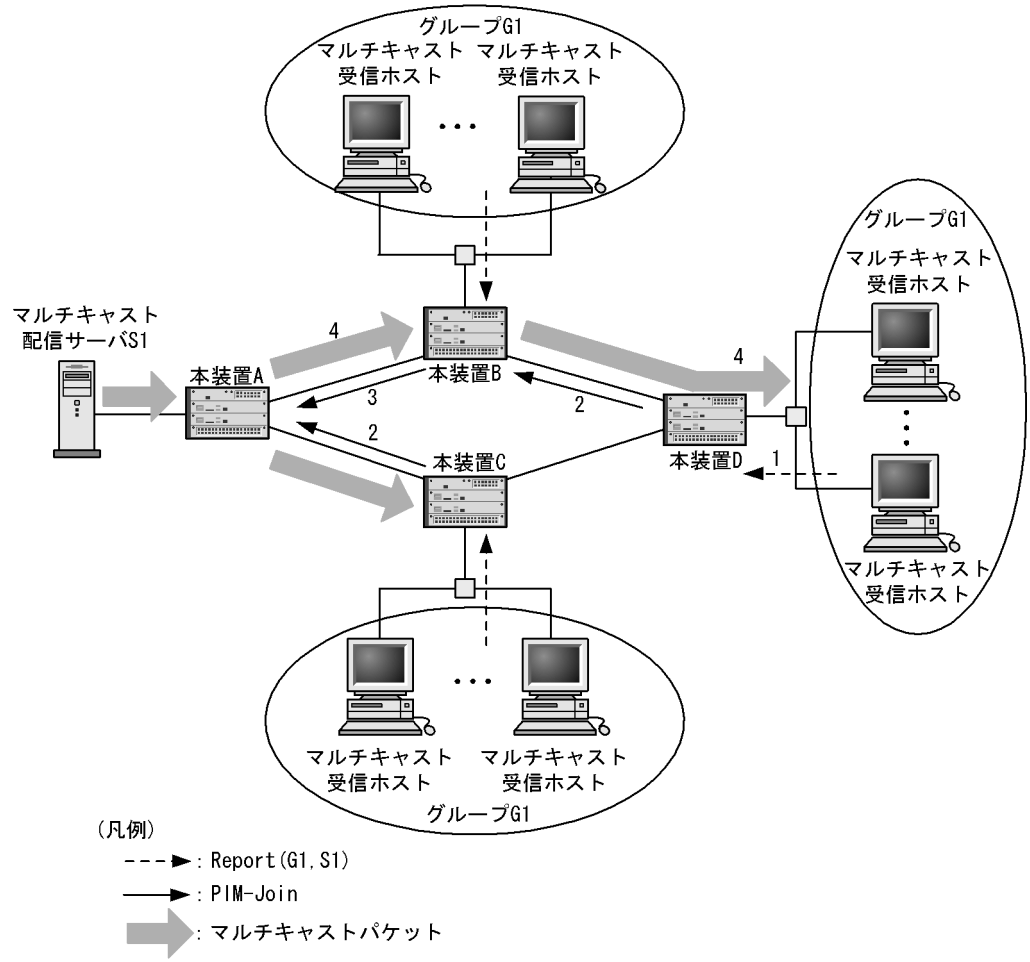
PIM-SSM を使用するためには送信元の情報が必要となります。本装置では IGMPv2 を使用する際には送信元をコンフィグレーションで設定することで PIM-SSM を使用することができます。IGMPv3 では送信元をコンフィグレーションで設定することなく PIM-SSM を使用できます（コンフィグレーションで

PIM-SSM を設定する必要があります)。

マルチキャスト配信サーバ（送信元アドレス S1）がマルチキャストグループ G1 にマルチキャストパケットを送信する場合の IPv4 PIM-SSM の動作を次に示します。

1. ホスト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) を受信します。
2. IGMPv3 Report(G1,S1) を受信した装置は Report で通知されたグループアドレス (G1) とコンフィグレーションで指定した SSM グループアドレス（範囲）を比較します。グループアドレスが一致した場合は，Report で通知された送信元アドレス (S1) への最短経路方向にグループアドレス (G1) と送信元アドレス (S1) を含んだ 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各装置は，送信元アドレス (S1) への最短経路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各装置は，PIM-Join メッセージを受信したインタフェースだけに送信元アドレス S1 からのマルチキャストパケットを中継するように (S1,G1) の配送ツリーを形成します。
4. マルチキャスト配信サーバ S1 がグループ 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マルチキャスト中継情報に従いマルチキャストパケットを中継します。

図 14-26　IGMPv3 使用時の IPv4 PIM-SSM 動作概要



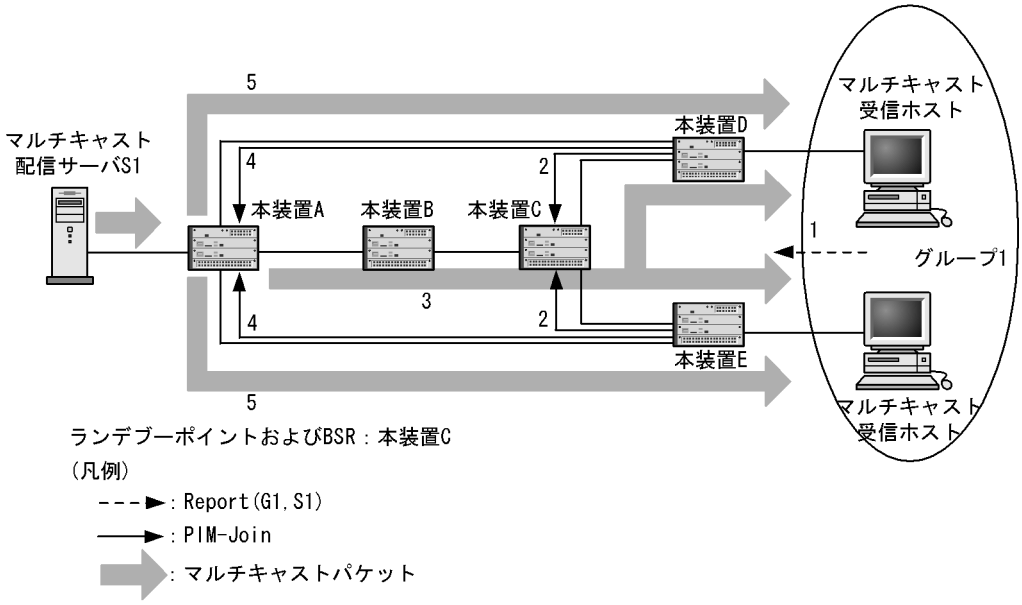
(2) IGMPv3 使用時の IPv4 PIM-SM 動作

コンフィグレーションで PIM-SSM が設定されていない場合は PIM-SM で動作します。マルチキャスト配信サーバ（送信元アドレス S1）がマルチキャストグループ G1 にマルチキャストパケットを送信する場合

の IPv4 PIM-SM 動作を次に示します。

1. ホスト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) を受信します。
2. IGMPv3 Report(G1,S1) を受信した装置はランデブーポイントへの最短経路方向にグループアドレス (G1) を含んだ 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ーに配送するために，送信元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. 送信元から各グループメンバー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元からの最短パスを決定します（PIM-Join メッセージを送信元への最短経路方向に送信し，最短パス配送ツリーを形成します)。
5. マルチキャスト配信サーバ S1 がグループ G1 宛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いマルチキャストパケットを中継します。

図 14-27　IGMPv3 使用時の IPv4 PIM-SM 動作概要



(3) IGMPv3 使用時の IPv4 PIM-DM 動作

INCLUDE と EXCLUDE のどちらも，参加グループだけを参照して動作します。

(4) IGMPv1/IGMPv2 ホストおよび IGMPv3 ホスト混在時の IPv4 経路制御

IGMPv2 で PIM-SSM を使用する設定をしている状態で，IGMPv1 ホスト，IGMPv2 ホストと IGMPv3 ホストが混在する場合の IPv4 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 対象アドレス範囲に含まれるグループアドレスに対して加入要求を受けた場合は PIM-SSM が動作します（「表 14-15　IGMPv1/IGMPv2 および IGMPv3 ホスト混在時の IPv4 経路制御動作」を参照してください)。IGMPv1 Report，IGMPv2 Report で加入要求を受けた場合，送信元リストはコンフィグレーションで設定した送信元アドレスを使用します。IGMPv1 Report，IGMPv2 Report と IGMPv3 Report（EXCLUDE）で同じグループアドレスに対して加入要求を受けた場合，送信元リストはコンフィグレーションで設定された送信元アドレスと IGMPv3 Report （INCLUDE）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。

IGMPv1/IGMPv2 および IGMPv3 ホスト混在時の IPv4 経路制御動作を次の表に示します。

表 14-15 IGMPv1/IGMPv2 および IGMPv3 ホスト混在時の IPv4 経路制御動作

加入グループアドレス	IGMPv1 Report IGMPv2 Report IGMPv3 Report(EXCLUDE)	IGMPv3 Report(INCLUDE)
SSM アドレス範囲内	PIM-SSM	PIM-SSM
SSM アドレス範囲外	PIM-SM	PIM-SM

14.4.6 VRF での IPv4 マルチキャスト【OP-NPAR】

(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 IPv4 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 IPv4 マルチキャストを動作させます。VRF 上の IPv4 マルチキャストでは，ランデブーポイント，BSR，各種タイマ，SSM アドレス範囲などにそれぞれ異なる設定ができます。ただし，PIM-DM を使用する場合は IPv4 マルチキャストの VRF 機能を使用できません。PIM-DM を使用した IPv4 マルチキャストが動作するのはグローバルネットワークだけです。

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 14-28 VRF での IPv4 マルチキャスト

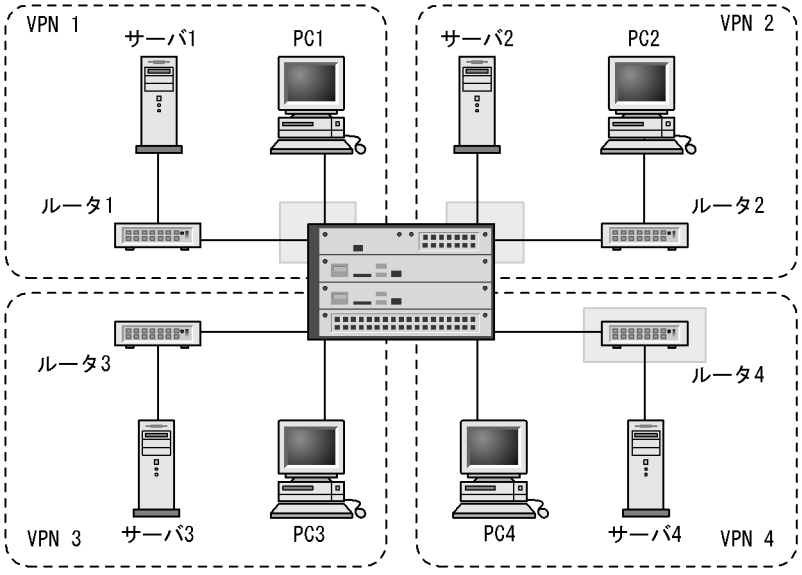


表 14-16 本装置での設定情報

VPN	運用 プロトコル	ループバック 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	SSM アドレス
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

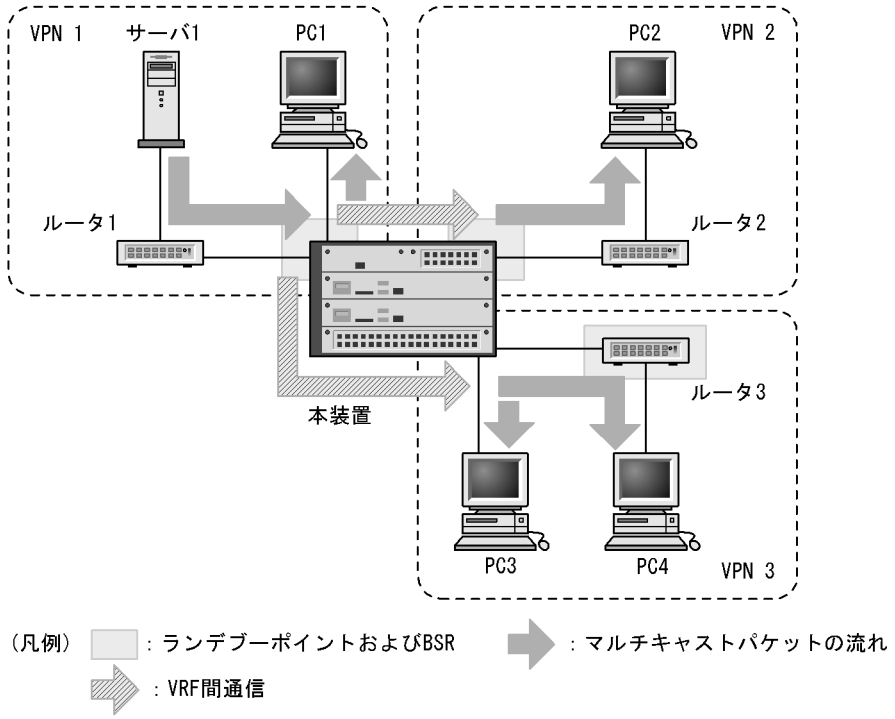
(2) IPv4 マルチキャストエクストラネット

IPv4 マルチキャストエクストラネットを使用すると，VRF 間で IPv4 マルチキャスト中継ができます。また，IPv4 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。

なお，last-hop-router 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。

IPv4 マルチキャストエクストラネットの動作概要を次の図に示します。

図 14-29 IPv4 マルチキャストエクストラネットの動作概要



(3) PIM-SM VRF ゲートウェイ

PIM-SM でマルチキャスト通信をするには，last-hop-router に IPv4 マルチキャストパケットを中継する必要があります。PIM-SM をエクストラネットで使用する場合でも，各 VRF にあるすべての last-hop-router に IPv4 マルチキャストパケットを中継する必要があります。

本装置では，各 VRF のランデブーポイントに IPv4 マルチキャストパケットを転送するために，PIM-SM VRF ゲートウェイを使用します。

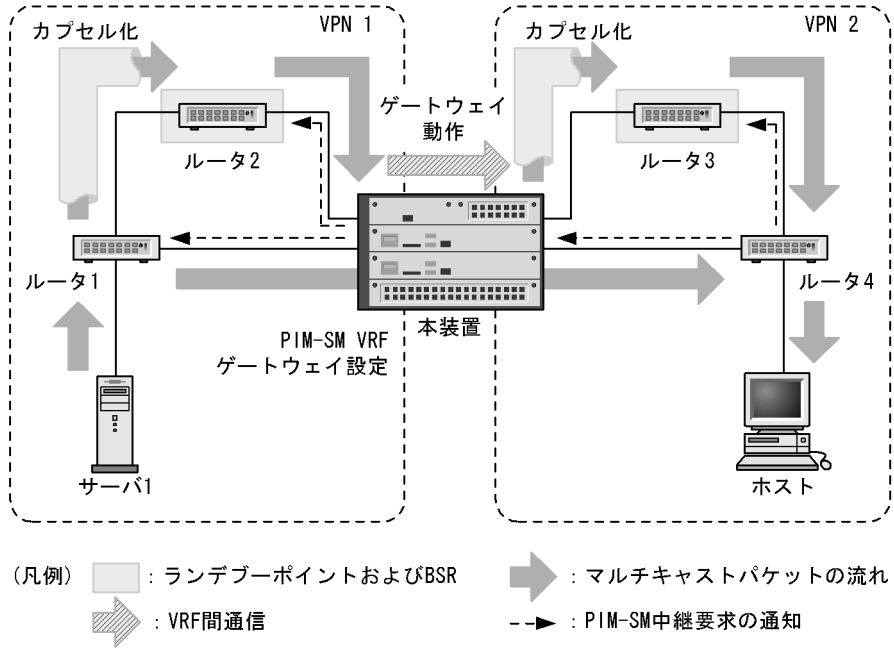
送信者（マルチキャスト配信サーバ）が存在する VRF に PIM-SM VRF ゲートウェイを設定すると，指定グループに対して該当 VPN での last-hop-router として動作し，ランデブーポイントに中継要求をします。ランデブーポイントから IPv4 マルチキャストパケットを受信すると，そのパケットを中継対象となる VRF に転送します。

転送先の VPN では first-hop-router として動作し，各 VRF のランデブーポイントへ IPv4 マルチキャストパケットをカプセル化（PIM-Register メッセージ）して送信します。PIM-Register メッセージを受信したランデブーポイントは通常の PIM-SM の動作に従って，デカプセル化して IPv4 マルチキャストパケットを last-hop-router に転送します。そのあと，last-hop-router から送信元への最短パス配送ツリー

を形成します。このとき，エクストラネットの IPv4 マルチキャストパケットもハードウェア中継となります。

このように PIM-SM VRF ゲートウェイを使用すると，本装置以外の設定を変更しないで PIM-SM によるエクストラネットができます。PIM-SM VRF ゲートウェイの動作概要を次の図に示します。

図 14-30　PIM-SM VRF ゲートウェイの動作概要



(4) IPv4 マルチキャストエクストラネット使用時の注意事項

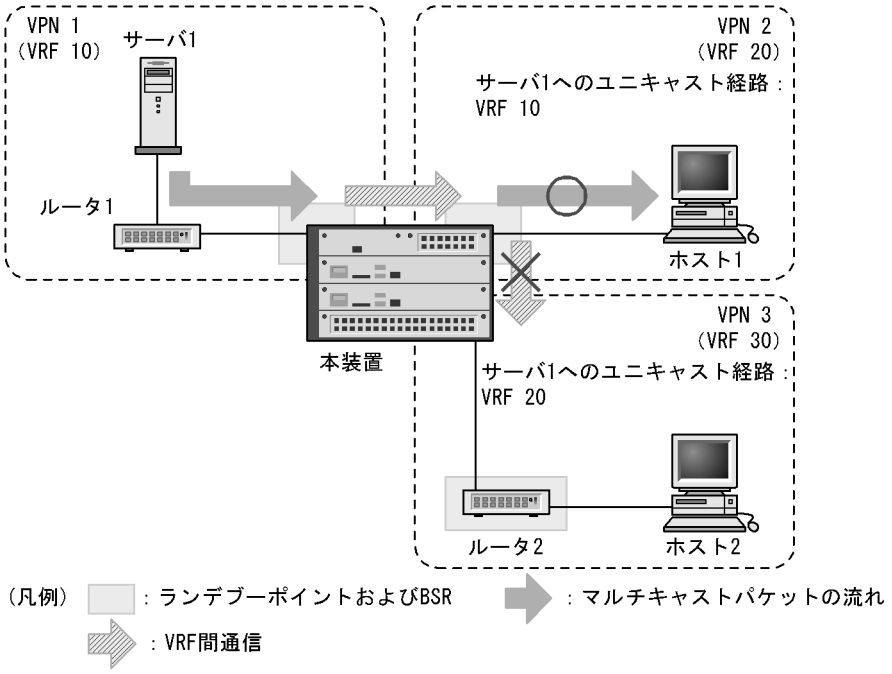
(a) 装置内での 2 段以上の VRF 中継

IPv4 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 IPv4 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 上のサーバ 1 が送信する IPv4 マルチキャストパケットを VPN 2 上のホスト 1 は受信できますが，VPN 3 のホスト 2 は受信できません。

図 14-31 IPv4 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) PIM-SM/PIM-SSM 相互接続

IPv4 マルチキャストエクストラネットを使用して VRF 間でマルチキャスト中継をする場合は，使用するグループアドレスのプロトコルを同じにしてください（IPv4 マルチキャスト VRF では，VRF ごとに PIM-SSM で使用するグループアドレスを指定できます)。

プロトコルが異なる場合，IPv4 マルチキャストエクストラネットによるマルチキャスト中継はできません。VRF 間のプロトコル不一致で中継できない例および本装置の設定情報を次に示します。

図 14-32 IPv4 マルチキャストエクストラネット使用時に VRF 間プロトコル不一致で中継できない例

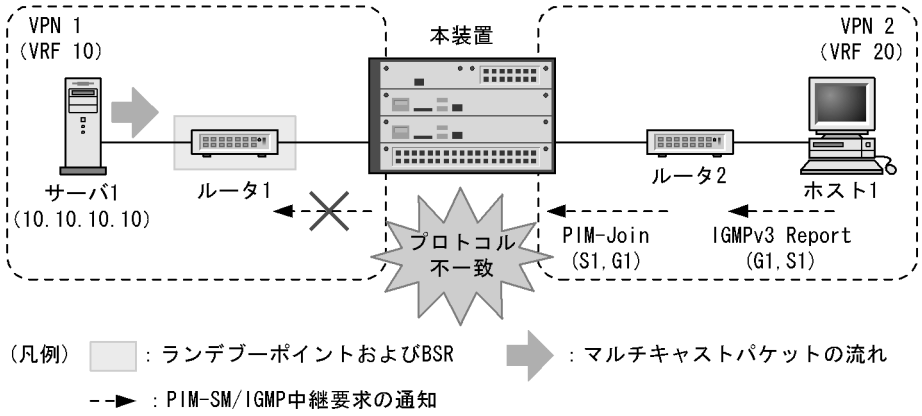


表 14-17 本装置の設定情報

VPN	運用プロトコル	ランデブーポイント () 内はランデブーポイントアドレス	SSM アドレス
1	PIM-SM	本装置（1.1.1.1）	未使用
2	PIM-SSM	なし	232.0.0.0/8

G1：232.10.10.10
S1：10.10.10.10

14.5 IPv4 マルチキャストソフト処理パケット制御機能

IPv4 マルチキャストソフト処理パケット制御機能とは，本装置が受信するマルチキャストデータパケットを，コンフィグレーションで設定した受信要因と受信パケット数に従って制御することで，マルチキャストパケット受信による本装置の輻輳を抑止する機能です。本機能は，コンフィグレーションコマンド ip pim rate-limit で設定します。なお，本機能は中継パケットには影響ありません。

14.5.1 パケット制御対象受信要因

パケット制御の対象受信要因とその内容を次の表に示します。

表 14-18 パケット制御対象受信要因

パケット受信要因	内容
wrong-incoming-interface	ハードウェアの IPv4 マルチキャスト中継エントリに登録済みのエントリと一致したマルチキャストデータ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 IPv4 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データパケットを受信した場合に発生する要因
register-request	first-hop-router で受信した IPv4 マルチキャストパケットを PIM-Register メッセージとしてランデブーポイントに送信する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

注

アクセスリストロギングまたは DHCP snooping を使用した場合，受信した PIM-Register メッセージは，受信要因を register-receive ではなく register-request として制御されます。

14.5.2 パケット制御

(1) AX6700S の場合

NIF から受信したソフト処理用データパケットを BCU 内の CPU に転送する際，コンフィグレーションによって設定した受信要因と比較し一致した場合，設定した受信パケット数に従って転送数を制御します。

CPU に転送するパケット数は，運用系 BSU の枚数によって異なります。運用系 BSU 枚数別の，CPU に転送するパケットの最大数を次の表に示します。

表 14-19 CPU に転送するパケットの最大数

運用系 BSU 枚数	CPU に転送するパケットの最大数
1 枚	設定値の約 2 倍
2 枚	設定値の約 4 倍
3 枚	設定値の約 6 倍

(2) AX6600S の場合

NIF から受信したソフト処理用データパケットを CSU 内の CPU に転送する際，コンフィグレーションによって設定した受信要因と比較し一致した場合，設定した受信パケット数に従って転送数を制御します。

CPU に転送するパケット数は，運用系 PSP の数によって異なります。運用系 PSP 数別の，CPU に転送

するパケットの最大数を次の表に示します。

表 14-20 CPU に転送するパケットの最大数

運用系 PSP 数	CPU に転送するパケットの最大数
1	設定値
2	設定値の約 2 倍

(3) AX6300S の場合

NIF から受信したソフト処理用データパケットを MSU 内の CPU に転送する際，コンフィグレーションによって設定した受信要因と比較し一致した場合，設定した受信パケット数に従って転送数を制御します。

CPU に転送するパケットの最大数は，運用系 MSU が 1 枚だけなので，設定値と同じになります。

14.6　ネットワーク設計の考え方

14.6.1　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には次の点に注意してください。

(1) プロトコル共通

(a) 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。

(b) 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 IPv4 マルチキャストは動作しません。

(c) プロトコルの混在

本装置は，PIM-SM と PIM-DM が混在するシステム構成をサポートしていません。そのため，ネットワーク内の全装置で同じマルチキャストプロトコル（PIM-SM または PIM-DM）を使用してください。ただし，PIM-SSM は PIM-SM の拡張機能なので，PIM-SM と PIM-SSM は混在できます。

(d) 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。

(e) ルーティングプログラムの再起動に伴う中継断

運用コマンド restart ipv4-multicast を実行して IP 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は，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。

(f) ハードウェア中継切り替え時のパケット追い越し

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，それまでのソフトウェアによるマルチキャストパケットの中継処理がハードウェア中継へと切り替わります。このときに一部のパケットで追い越しが発生し，パケットの順序が入れ替わる場合があります。

(2) PIM-SM の使用

PIM-SM を使用する場合は次の点に注意してください。なお，この注意事項は PIM-SSM には該当しません。

(a) ソフトウェア中継処理時のパケットロス

本装置は，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ソフトウェアでマルチキャストパケットを中継するため，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パケットをロスする場合があります。

(b) パス切り替え時の二重中継またはパケットロス

本装置は，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切り替え動作は「14.4.2　IPv4 PIM-SM」を参照してください。

(c) 装置アドレス到達可能性

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，装置管理情報のローカルアドレスで設定された 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。この装置管理情報のローカル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。

(d) 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（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の 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。

(e) 静的ランデブーポイント

静的ランデブーポイントは，BSR 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はコンフィグレーションによって設定します。

静的ランデブーポイントは BSR 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 BSR 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，BSR を使用しないで静的ランデブーポイントを使っ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の設定が必要です。

また，静的ランデブーポイントを使用する場合，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。

(f) 系切替時の通信無停止対応機能使用時の注意事項

系切替時の通信無停止対応機能使用時（コンフィグレーションコマンド ip pim nonstop-forwarding の設定時）の注意事項を次に示します。

- 再学習時間内は PIM-SSM の動作範囲をコンフィグレーションで変更しないでください。再学習時間内に PIM-SSM の動作範囲をコンフィグレーションで変更して，マルチキャスト中継エントリが PIM-SM から PIM-SSM の経路，または PIM-SSM から PIM-SM の経路になった場合，マルチキャスト中継の動作は保証できません。

(g) 系切替時の通信無停止対応機能での IPv4 マルチキャスト中継エントリ再学習時の注意事項

系切替時の通信無停止対応機能を使用している場合に，IPv4 マルチキャスト中継エントリを再学習するときの注意事項を次に示します。なお，各注意事項は IPv4 マルチキャスト中継エントリの再学習時間終了後（系切替から 450 秒後）に解消されます。

- 系切替するルータおよび近隣ルータでは，使用するユニキャストルーティングプロトコルのグレースフル・リスタートを有効にしてください。グレースフル・リスタートが無効な場合，系切替の直後は PIM メッセージが正しく送受信されないため，マルチキャスト中継が一時的に中断するおそれがあります。
- 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 draft-ietf-pim-sm-bsr-07 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，系切替の直後に PIM メッセージが正しく送受信されないため，

マルチキャスト中継が一時的に中断するおそれがあります。なお，Generation ID オプションについては「14.4.2　IPv4 PIM-SM」の「(3) 近隣検出」を参照してください。

● 再学習時間内は次の場合にパケットロスが発生することがあります。
- 中継対象のマルチキャスト中継エントリの下流インタフェースに，カプセル化インタフェースが含まれている場合
  ランデブーポイント情報を学習するまで，カプセル化インタフェースへの中継が止まります。
- ランデブーポイント経由の中継が最短パス経由の中継に遷移している途中で系切替した場合
- ランデブーポイントを系切替したときに，新たなグループ参加要求を受信した場合
- 中継対象のマルチキャスト中継エントリの上流インタフェースが変更された場合

● 上流方向へ PIM-Join/Prune メッセージを送信する装置で系切替した場合，グレースフル・リスタート開始後にすべてのユニキャスト経路をルーティングテーブルに登録するまでの時間が PIM-Join/Prune メッセージの送信間隔の 1.5 倍以上になると，パケットロスが発生することがあります。すべてのユニキャスト経路がルーティングテーブルに登録されて，該当する装置が上流方向へ PIM-Join/Prune メッセージを送信すると，このパケットロスは解消されます。パケットロスの発生を防ぐためには，該当する装置で PIM-Join/Prune メッセージの送信間隔を 130 秒以上に設定してください。
なお，この設定をしても，BGP で多数の近隣装置と大量の経路情報を交換する場合やグレースフル・リスタートの設定によっては，パケットロスが発生するおそれがあります。その場合は，系切替対象装置に，送信元アドレスおよびランデブーポイント装置アドレスへのスタティック経路を最低の優先度で設定してから，系切替してください。

● 再学習時間内は次に示す意図しない中継が発生することがあります。
- マルチキャストデータの二重中継が発生した場合，その解消に時間が掛かることがあります。
  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と，PIM-Assert メッセージによって二重中継が抑制されます。
- 中継対象のマルチキャスト中継エントリのインタフェースに障害が発生して，その後回復した場合，再学習に関係なく中継を再開することがあります。
- 中継対象のマルチキャスト中継エントリのインタフェースをコンフィグレーションで変更，またはプロトコル処理で削除した場合，中継が停止しないことがあります。
- ランデブーポイント経由の中継が最短パス経由の中継に遷移している途中では，両方の経路から二重にパケットが中継されることがあります。

● 再学習時間内はマルチキャスト中継エントリの無通信を監視しないで，再学習の終了時に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，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，再学習の終了時にマルチキャスト中継エントリは保持されません。

● BSR を系切替した場合，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。そのため，再学習時間内は通常の間隔（60 秒）よりも短い間隔で PIM Bootstrap メッセージを送信します。

● ランデブーポイントで本機能を有効にした場合，PIM Candidate-RP-Advertisement メッセージのランデブーポイント保持期間を 210 秒に設定して広告します（通常は 150 秒）。

(3) PIM-DM の使用

PIM-DM を使用する場合は次の点に注意してください。

(a) ソフトウェア中継処理時のパケットロス

本装置は，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ソフトウェアでマルチキャストパケットを中継するため，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パケットをロスする場合があります。

14.6.2 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の注意点について説明します。

(1) 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接続要求を送信してから上流からマルチキャストデータが到着するまでの「加入通知時間」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 BSR 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 BSR 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 BSR 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)

- BSR 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 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切り替えを行った場合も，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) 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接続要求を送信してから上流からマルチキャストデータが到着するまでの「加入通知時間」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 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)

(3) PIM-DM の使用

PIM-DM 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接続要求を送信してから上流からマルチキャストデータが到着するまでの「加入通知時間」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≦210の時：210秒

U＞210の時：U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。

U≦210の時：210秒
U＞210の時：U秒

14.6.3 適応ネットワーク構成例

（1） PIM-SM を使用する構成

本構成は次の場合に適応します。

- マルチキャストパケットを送信するユーザを限定しない場合
- マルチキャストパケットを送信するユーザが多数存在する場合

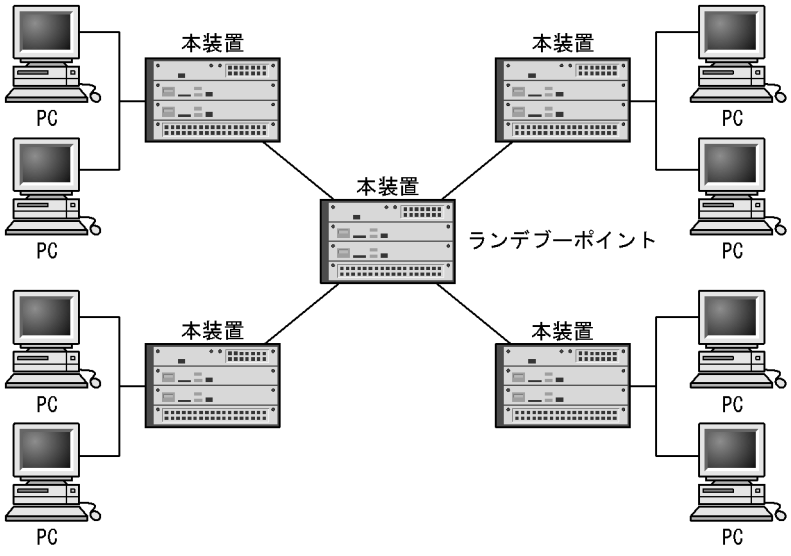
［ネットワークの環境］

1. 前提条件として，すべてのルータでサーバへの IP 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は PIM-SM を使用します。
3. 各グループと本装置間のグループ管理制御は 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 BSR 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 14-33 PIM-SM を使用する構成図



（2） PIM-SSM を使用する構成

本構成は次の場合に適応します。

- マルチキャストパケットを送信するユーザを限定する場合（主に配信サーバなど）
- ブロードバンドマルチキャスト通信を行う場合

• 多チャンネルマルチキャスト通信を行う場合

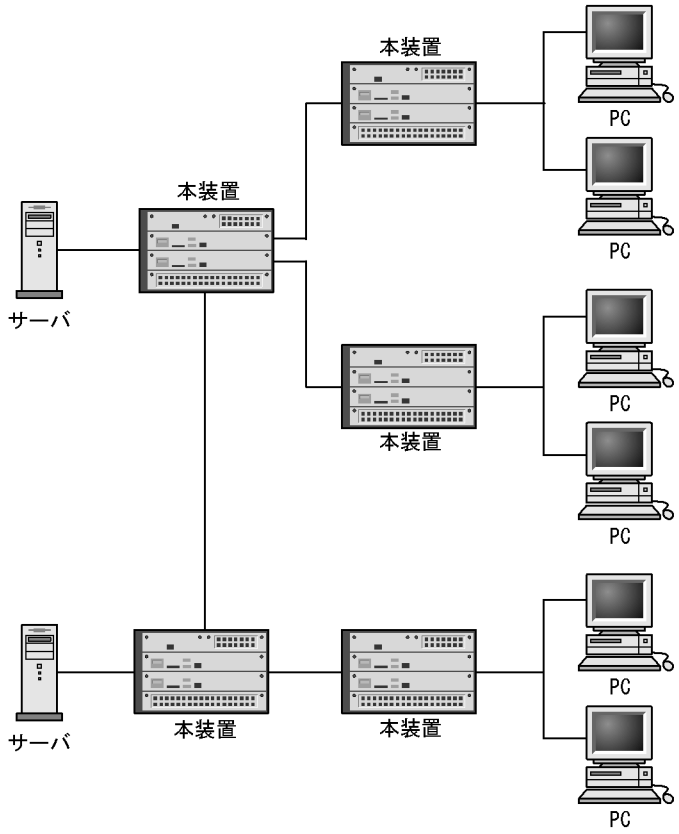
[ネットワークの環境]

1. 前提条件として，すべてのルータでサーバへの IP 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は PIM-SSM を使用します。PIM-SSM は PIM-SM の拡張機能です。
3. グループ管理制御は IGMPv2 を使用します（IGMPv2 で SSM を連携動作させる設定が必要です）。

[構成図]

構成図を次に示します。

図 14-34 PIM-SSM を使用する構成図



(3) PIM-DM を使用する構成

本構成は次の場合に適応します。

• マルチキャストパケットを受信するユーザが多数存在する場合
• 小規模なマルチキャストネットワークで運用する場合

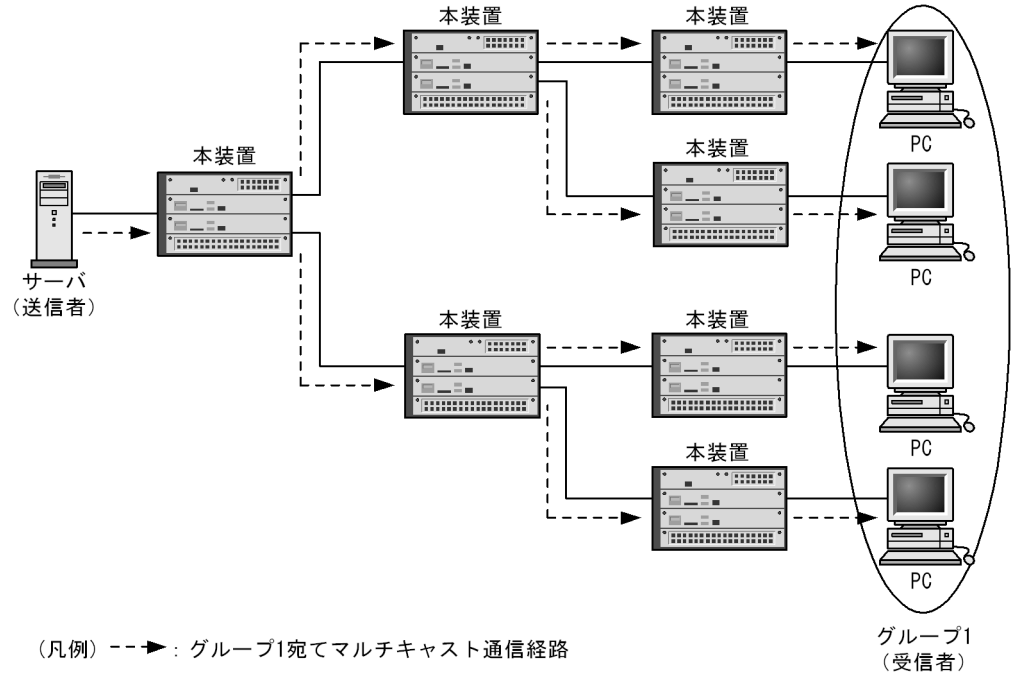
[ネットワークの環境]

1. 前提条件として，すべてのルータでサーバへの IP 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は PIM-DM を使用します。
3. 各グループと本装置間のグループ管理制御は IGMP を使用します。

[構成図]

構成図を次に示します。

図 14-35 PIM-DM を使用する構成図



14.6.4 ネットワーク構成での注意事項

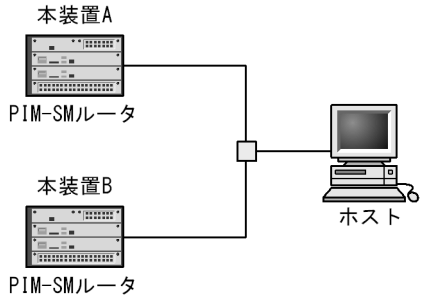
マルチキャストはサーバ（送信者）から各グループ（受信者）にデータを配信する 1（送信者）: N（受信者）の片方向通信に適します。IPv4 マルチキャストの適応ネットワーク構成，注意事項を次に示します。

(1) PIM-SM および PIM-SSM 共通

(a) 注意が必要な構成

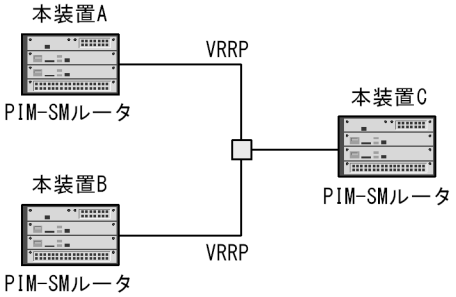
次に示す構成で PIM-SM または PIM-SSM を使用する場合，注意が必要です。

- 次の図に示す構成のようにホスト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，マルチキャストデータが二重に中継されることがあります。



- 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ルートを設定した環境では，PIM プロトコルが上流ルータを検出できず，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する場合は，本装置 C にランデブーポイントアドレスと BSR アドレスとマルチキャストデータ送信元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ルートを設定する必要があります。

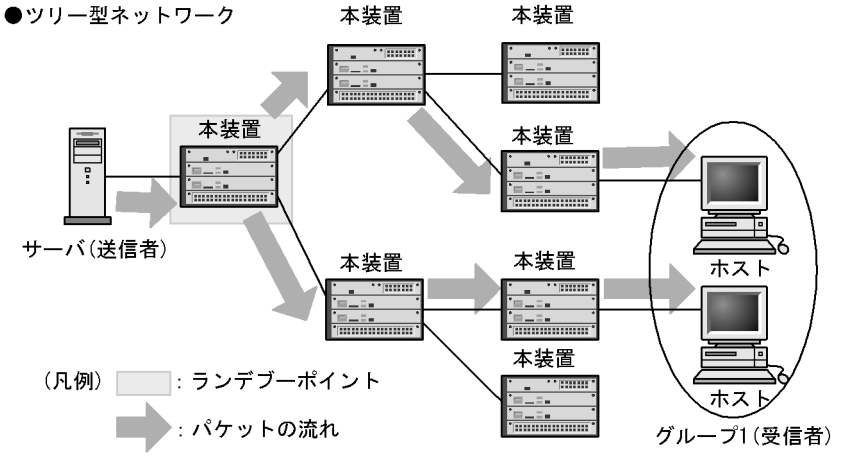


(2) PIM-SM

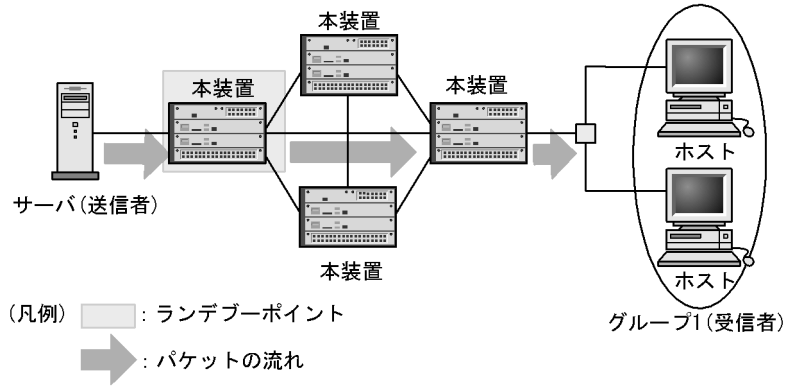
(a) 推奨構成

PIM-SM によるネットワークの構成に当たっては，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 14-36　PIM-SM 推奨ネットワーク構成



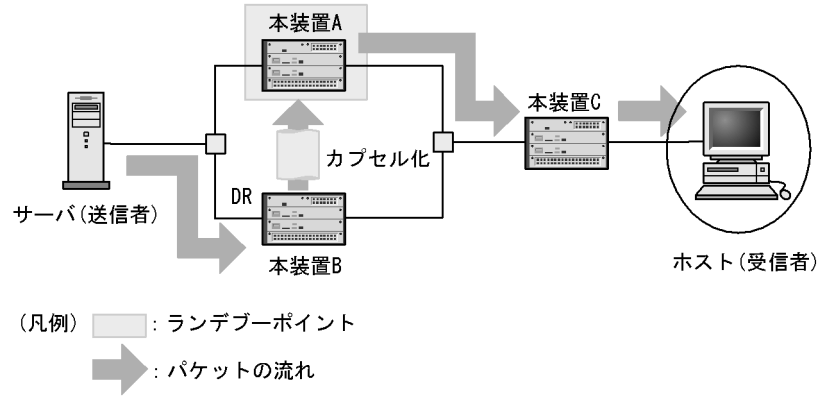
●冗長構成が複数存在するネットワーク



(b) 注意が必要な構成

次に示す構成は注意が必要です。

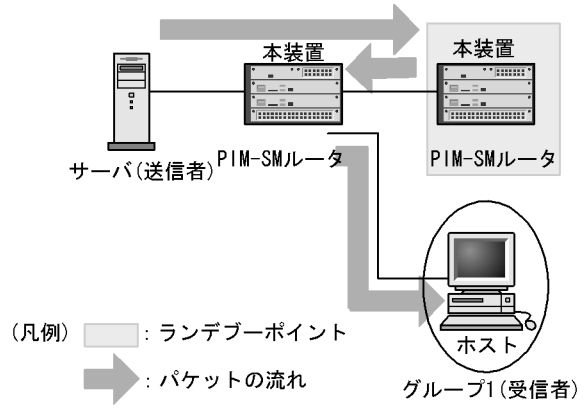
● 次の図に示すように送信者と直接接続するルータが同一ネットワーク上に 2 台以上存在する構成で，どれかをランデブーポイントとする場合は，ランデブーポイントが DR になるようにしてください。
ランデブーポイント以外を DR にした場合，DR からランデブーポイントに対し PIM-Register メッセージを送信するため，本装置 A，B に負荷が掛かります。また，PIM-Register メッセージ中のマルチキャストパケットを中継するときに，ランデブーポイントでパケットロスが発生するおそれがあります。なお，ランデブーポイントを DR にした場合は，PIM-Register メッセージによるカプセル化は行いません。



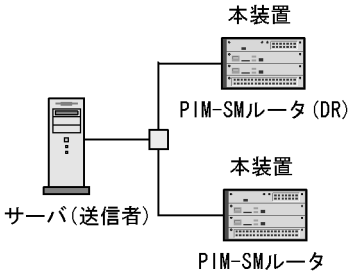
(c) 不適応な構成

次に示す構成で PIM-SM は使用しないでください。

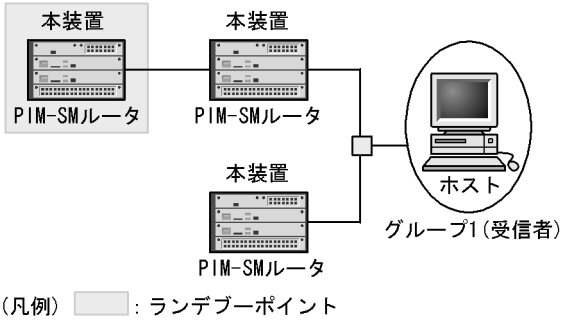
● 送信者とランデブーポイントの間に受信者が存在する構成
次に示す構成でサーバからグループ 1 のマルチキャスト通信を行う場合，ランデブーポイント経由の中継が効率よく行えません。



● 送信者と同一回線上に複数の PIM-SM ルータが動作する構成
次に示す構成でサーバがマルチキャストデータを送信した場合，DR でない PIM-SM ルータに不要な負荷がかかり，本装置の他機能に大きく影響を与えることがあります。回線を分けてください。



● マルチキャストグループ（受信者）と同一回線上に複数の PIM-SM ルータを動作させ，ランデブーポイントに接続しない PIM-SM ルータが存在する構成
次に示す構成でグループ 1 宛てのマルチキャスト通信をした場合，送信者とグループ 1 間で最短パスが確立しない場合があります。PIM-SM ルータ 1 および PIM-SM ルータ 2 はランデブーポイントと接続してください。

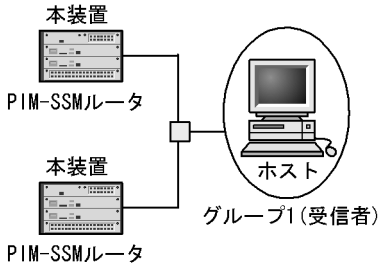


(3) PIM-SSM

(a) 注意が必要な構成

次に示す構成は注意が必要です。

● マルチキャストグループ（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
次に示す構成で IGMPv2 の PIM-SSM を動作させる場合は，同一回線上の全ルータの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。

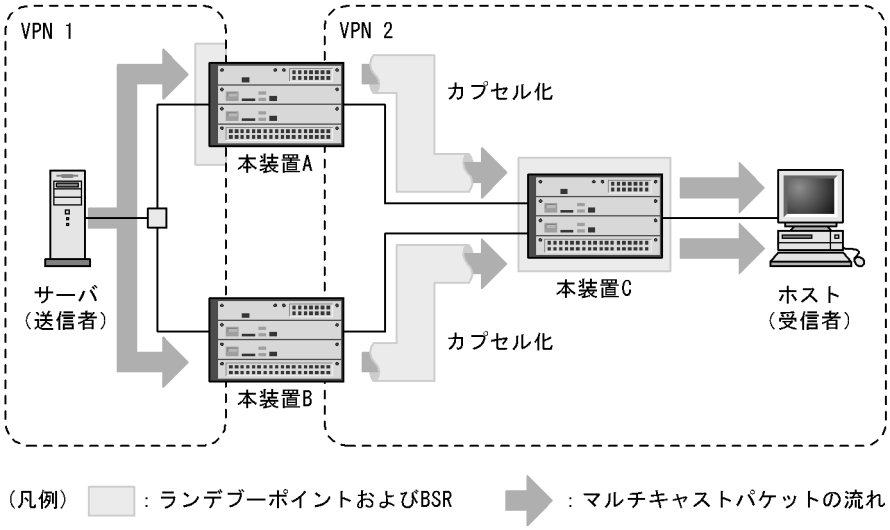


(4) PIM-SM VRF ゲートウェイ【OP-NPAR】

(a) 注意が必要な構成

次に示す構成は注意が必要です。

- PIM-SM VRF ゲートウェイを使用した IPv4 マルチキャストエクストラネットで，2 台以上の VRF 境界ルータで冗長構成を構築する場合，VRF 境界ルータのどれかをランデブーポイントに設定してください。
  VRF 境界ルータ以外をランデブーポイントにした場合，最短パス配送ツリーが形成されるまでの間，IPv4 マルチキャストパケットが境界ルータの数だけ多重中継になります。

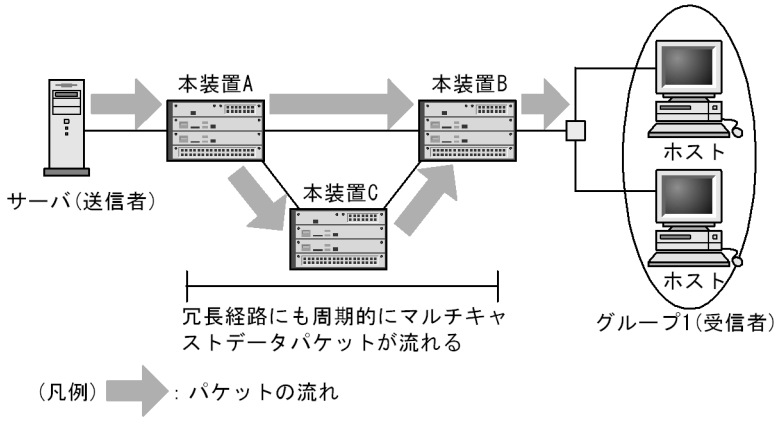


(5) PIM-DM

(a) 注意が必要な構成

次に示す構成は注意が必要です。

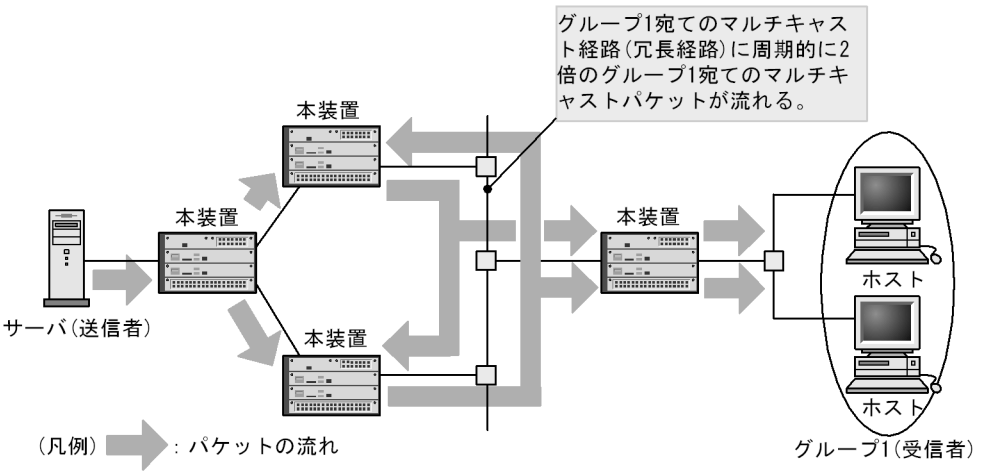
- 冗長構成が存在する構成
  次に示す構成で冗長構成が存在する場合，冗長経路にマルチキャストデータパケットが周期的（約 3 分）に流れます。
  また，グループ（受信者）の有無とは関係なく，マルチキャストデータパケットの転送量とマルチキャスト経路情報数によって，冗長経路にマルチキャストデータパケットが流れ続けることがあります。この場合，本装置 B および本装置 C で IPv4 マルチキャストソフト処理パケット制御機能を使用すると抑止できます。コンフィグレーションコマンド ip pim rate-limit wrong-incoming-interface で，受信要因が wrong-incoming-interface となるパケットの受信数を変更してください。



(b) 不適応な構成

次に示す構成で PIM-DM は使用しないでください。

● 同一 VLAN 上に冗長経路が存在するネットワーク構成
同一 VLAN 上に冗長経路が存在するネットワーク構成では，周期的にすべての経路でマルチキャスト通信を行います。ネットワーク全体に負荷が掛かるので，PIM-DM ではなく PIM-SM を使用してください。



15 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。

15.1 コンフィグレーション

15.1.1 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 15-1 コンフィグレーションコマンド一覧

コマンド名	PIM-SM/ PIM-SSM	PIM-DM	説明
ip igmp group-limit	○	○	インタフェースで動作できる最大グループ数を指定します。
ip igmp router	○	×	該当インタフェースで IGMP を動作させます。
ip igmp source-limit	○	○	グループ参加時のソース最大数を指定します。
ip igmp ssm-map enable	○	×	IGMPv2/IGMPv3（EXCLUDE モード）での IPv4 PIM-SSM 連携動作を使えるように設定します。
ip igmp ssm-map static	○	×	PIM-SSM が動作するグループアドレスとソースアドレスを設定します。
ip igmp static-group	○	○	IGMP グループへ静的に加入できるように設定します。
ip igmp version	○	○	IGMP バージョンを変更します。
ip multicast-routing	○	○	IPv4 マルチキャスト機能を使えるように設定します。
ip multicast protocol	○	○	IPv4 マルチキャストの動作プロトコルを設定します。
ip pim accept-bootstrap	○	×	該当インタフェースから受信したブートストラップメッセージの廃棄を設定します。
ip pim bsr-candidate	○	×	BSR 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変更します。
ip pim dense-mode	×	○	IPv4 PIM-DM 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変更します。
ip pim max-interface	○	○	IPv4 PIM を動作させるインタフェースの最大数を変更します。
ip pim mcache-limit	○	×	マルチキャスト中継エントリの最大数を指定します。
ip pim message-interval	○	×	PIM-Join/Prune メッセージの送信間隔を変更します。
ip pim mroute-limit	○	×	マルチキャスト経路情報の最大数を指定します。
ip pim negative-cache-time	○	×	ネガティブキャッシュの保持期間を変更します。
ip pim nonstop-forwarding	○	×	系切替時に，IPv4 PIM-SM のマルチキャスト中継を一時的に停止しないように指定します。
ip pim query-interval	○	×	PIM-Hello メッセージの送信間隔を変更します。
ip pim rate-limit cache-misshit	○	○	マルチキャスト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要因による受信パケット数の上限を指定します。
ip pim rate-limit register-receive	○	○	ランデブーポイントで受信できる PIM-Register メッセージ数の上限を指定します。
ip pim rate-limit register-request	○	○	first-hop-router で受信したマルチキャストパケットを PIM-Register メッセージとしてランデブーポイントに送信する場合のパケット数の受信上限を指定します。

コマンド名	PIM-SM/ PIM-SSM	PIM-DM	説明
ip pim rate-limit wrong-incoming-interface	○	○	マルチキャストエントリの入力インタフェース以外から受信できるマルチキャストパケット数の上限を指定します。
ip pim register-checksum	○	×	PIM-Register メッセージのチェックサム範囲を変更します。
ip pim register-probe-time	○	×	PIM-Register メッセージ送信抑止時間を基に null-Register の送信開始時間を指定します。
ip pim rp-address	○	×	静的ランデブーポイントを設定します。
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を指定します。
ip pim sparse-mode	○	×	IPv4 PIM-SM を設定します。
ip pim ssm	○	×	IPv4 PIM-SSM アドレスを設定します。
ip pim vrf-gateway	○	×	PIM-SM VRF ゲートウェイを設定します。

（凡例）
○：該当するコマンド
×：該当しないコマンド

15.1.2 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の設定
- IPv4 PIM-SM 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 BSR 候補の設定（自装置を BSR にする場合）
- IGMP の設定

● PIM-SM（静的ランデブーポイント）を使用する場合

- IPv4 マルチキャストルーティングの設定
- IPv4 PIM-SM 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 静的ランデブーポイントの設定
- 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の設定
- IPv4 PIM-SM の設定
- IPv4 PIM-SSM の設定
- IGMP の設定

● PIM-DM を使用する場合

- IPv4 マルチキャストルーティングの設定
- IPv4 PIM-DM 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の設定

- VRF での IPv4 PIM-SM 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 BSR 候補の設定（該当 VPN で自装置を BSR 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）を使用する場合

- VRF での IPv4 マルチキャストルーティングの設定
- VRF での IPv4 PIM-SM 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 静的ランデブーポイントの設定
- 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の設定
- VRF での IPv4 PIM-SM 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-SM を使用する場合（PIM-SM VRF ゲートウェイ）

- VRF での IPv4 マルチキャストルーティングの設定
- VRF での IPv4 PIM-SM の設定
- VRF での 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）
- VRF での IPv4 PIM-SM BSR 候補の設定（自装置を BSR にする場合）
- PIM-SM VRF ゲートウェイの設定
- 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の設定
- VRF での IPv4 PIM-SM 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

15.1.3 IPv4 マルチキャストルーティングの設定

[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を動作させるための設定をします。設定はグローバルコンフィグレーションモードで行います。

IPv4 PIM-SM/SSM を使用する場合，ここでの設定のほかに，一つ以上のインタフェースで IPv4 PIM-SM/SSM（ip pim sparse-mode コマンド）の設定が必要です。また，IPv4 PIM-DM を使用する場合，ここでの設定のほかに，一つ以上のインタフェースで IPv4 PIM-DM（ip pim dense-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**

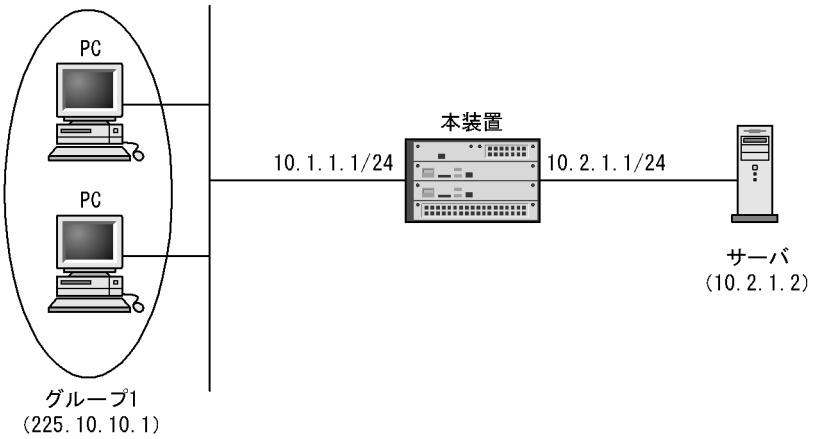
   IPv4 マルチキャスト機能を使用できるようにします。

15.1.4 IPv4 PIM-SM の設定

[設定のポイント]

IPv4 マルチキャストルーティングを動作させるインタフェースには，IPv4 PIM-SM（sparse モード）の設定をする必要があります。IPv4 PIM-SM（sparse モード）の設定はインタフェースコンフィグレーションモードで行います。例として，インタフェースの IP アドレスを 10.1.1.1/24 とした IPv4 PIM-SM 構成例を次の図に示します。

図 15-1 IPv4 PIM-SM 構成例



[コマンドによる設定]

1. **(config)# interface vlan 10**
   vlan を設定します。

2. **(config-if)# ip address 10.1.1.1 255.255.255.0**
   IP アドレスを設定します。

3. **(config-if)# ip pim sparse-mode**
   IPv4 PIM-SM として動作することを指定します。

15.1.5 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 loopback 0 のインタフェースへのアドレス設定，およびグローバルコンフィグレーションモードで次の設定をします。例として，管理するマルチキャストグループアドレスを 225.10.10.0/24，本装置のループバックアドレスを 10.10.10.10 とした設定を示します。

[コマンドによる設定]

1. **(config)# interface loopback 0**
   (config-if)# ip address 10.10.10.10
   (config-if)# exit
   ループバックのアドレスを設定します。

2. **(config)# access-list 1 permit 225.10.10.0 0.0.0.255**
   (config)# exit
   管理するマルチキャストグループアドレスのアクセスリストを作成します。

3. **(config)# ip pim rp-candidate loopback 0 group-list 1**
   本装置をランデブーポイント候補として設定します（管理するマルチキャストグループアドレスは手順2で作成したアクセスリストを指定します）。

15.1.6 IPv4 PIM-SM BSR 候補の設定

[設定のポイント]

本装置を BSR 候補として使用する場合，BSR アドレスとして loopback 0 のインタフェースへのアドレス設定，およびグローバルコンフィグレーションモードで次の設定をします。例として，本装置のループバックアドレスを 10.10.10.10 とした設定を示します。

[コマンドによる設定]

1. **(config)# interface loopback 0**
   (config-if)# ip address 10.10.10.10
   (config-if)# exit
   ループバックのアドレスを設定します。

2. **(config)# ip pim bsr-candidate loopback 0**
   本装置を BSR 候補として設定します。

15.1.7 IPv4 PIM-SM 静的ランデブーポイントの設定

[設定のポイント]

静的ランデブーポイントを指定する場合，グローバルコンフィグレーションモードで次の設定をします。例として，静的ランデブーポイントの装置アドレスを 10.10.10.1 とした設定を示します。

[コマンドによる設定]

1. **(config)# ip pim rp-address 10.10.10.1**
   10.10.10.1 をランデブーポイントとして指定します。

15.1.8 IPv4 PIM-SSM の設定

(1) IPv4 PIM-SSM アドレスの設定

[設定のポイント]

本装置で IPv4 PIM-SSM を使用するにはグローバルコンフィグレーションモードで次の設定をします。本設定によって IPv4 PIM-SM が設定されたインタフェースでは，指定した SSM アドレス範囲で IPv4 PIM-SSM が動作します。本装置で使用できる SSM アドレス設定は一つだけです。例として，PIM-SSM が動作する SSM アドレス範囲をデフォルト（232.0.0.0/8）で使用する設定を示します。なお，SSM アドレス範囲を指定する場合には ip pim ssm range で設定してください。

［コマンドによる設定］

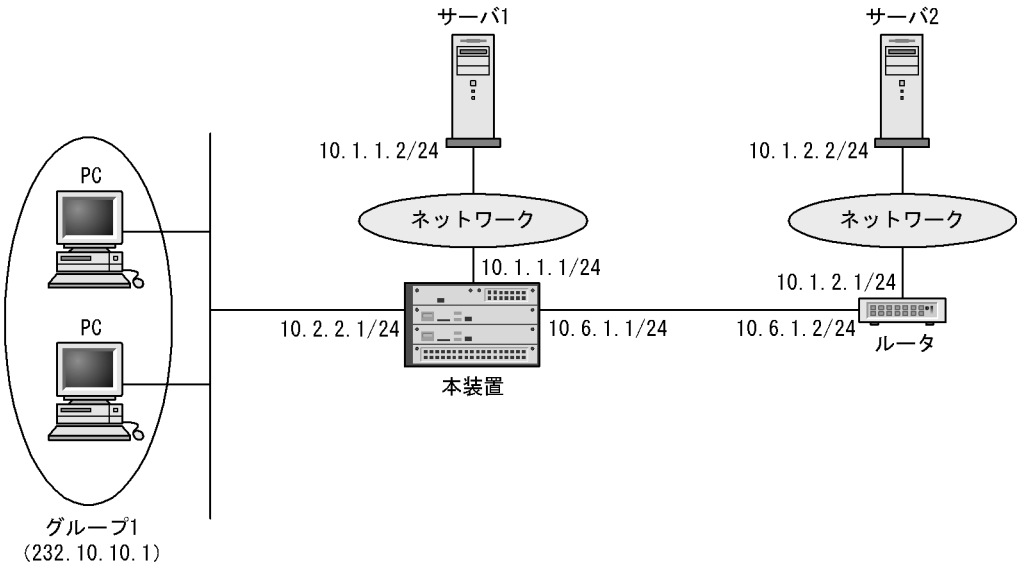
1. **(config)# ip pim ssm default**
   IPv4 PIM-SSM を使用できるようにします（SSM アドレス範囲は 232.0.0.0/8 となります）。

（2） IGMPv2/IGMPv3（EXCLUDE モード）で IPv4 PIM-SSM を連携動作させる設定

［設定のポイント］

IGMPv2/IGMPv3（EXCLUDE モード）ではソースアドレスを特定できないため，PIM-SSM への連携ができません。本装置では，PIM-SSM が動作するグループアドレスとソースアドレスの設定をすることで PIM-SSM への連携を行います。PIM-SSM が動作するグループアドレスは IPv4 PIM-SSM アドレスの設定で指定した SSM アドレス範囲内である必要があります。例として，グループアドレスを 232.10.10.1 とし，二つのサーバを使用する場合，サーバ 1 のソースアドレスを 10.1.1.2，サーバ 2 のソースアドレスを 10.1.2.2 とした PIM-SSM 構成例を次の図に示します。

図 15-2 IPv4 PIM-SSM 構成例



［コマンドによる設定］

1. **(config)# access-list 2 permit 232.10.10.1**
   グループアドレスを指定したアクセスリストを作成します。

2. **(config)# ip igmp ssm-map static 2 10.1.1.2**
   (config)# ip igmp ssm-map static 2 10.1.2.2
   PIM-SSM が動作するグループアドレス，およびサーバ 1 とサーバ 2 のソースアドレスを設定します（グループアドレスは手順 1 で作成したアクセスリストを指定します）。

3. **(config)# ip igmp ssm-map enable**
   IGMPv2/IGMPv3（EXCLUDE モード）で IPv4 PIM-SSM を使用できるようにします。

15.1.9 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。ただし，インタフェースに IPv4 PIM-SM（sparse モード）または IPv4 PIM-DM（dense モード）の設定をしても IGMP が動作します。

デフォルトでは IGMP バージョン 2，3 混在モードです。IGMP バージョンを変更する場合は，コンフィグレーションコマンド ip igmp version で設定してください。

なお，ip igmp router コマンドによる設定は PIM-SM/PIM-SSM 時だけ有効です。

[コマンドによる設定]

1. **(config-if)# ip igmp router**

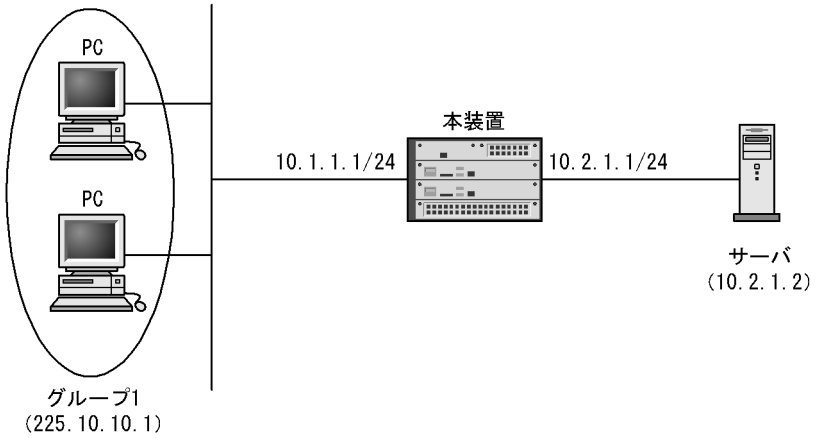
   該当インタフェースで IGMP バージョン 2，3 混在モード（デフォルト）を動作させることを指定します。

15.1.10 IPv4 PIM-DM の設定

[設定のポイント]

本装置で使用するマルチキャストプロトコルを PIM-DM に設定します。IPv4 マルチキャストルーティングを動作させるインタフェースには，IPv4 PIM-DM（dense モード）の設定をする必要があります。IPv4 PIM-DM（dense モード）の設定はインタフェースコンフィグレーションモードで行います。例として，インタフェースの IP アドレスを 10.1.1.1/24 とした IPv4 PIM-DM 構成例を次の図に示します。

図 15-3 IPv4 PIM-DM 構成例



[コマンドによる設定]

1. **(config)# ip multicast protocol pim-dm**

   本装置で使用するマルチキャストプロトコルを PIM-DM に設定します。

2. **(config)# interface vlan 10**

   VLAN 10 を設定します。

3. **(config-if)# ip address 10.1.1.1 255.255.255.0**

VLAN 10 に IP アドレスを設定します。

4. **(config-if)# ip pim dense-mode**
   (config-if)# exit
   VLAN 10 に IPv4 PIM-DM を指定します。

5. **(config)# interface vlan 20**
   VLAN 20 を設定します。

6. **(config-if)# ip address 10.2.1.1 255.255.255.0**
   VLAN 20 に IP アドレスを設定します。

7. **(config-if)# ip pim dense-mode**
   (config-if)# exit
   VLAN 20 に IPv4 PIM-DM を指定します。

15.1.11 VRF での IPv4 マルチキャストルーティングの設定【OP-NPAR】

[設定のポイント]

VRF で IPv4 マルチキャストを使用するために，VRF ごとに IPv4 マルチキャストルーティングを動作させます。設定はグローバルコンフィグレーションモードで行います。例として VRF 10 での IPv4 マルチキャストルーティングの設定を示します。

なお，IPv4 PIM-SM/SSM を使用する場合，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 IPv4 PIM-SM/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)# 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 マルチキャスト機能を使用できるようにします。

15.1.12 VRF での IPv4 PIM-SM の設定【OP-NPAR】

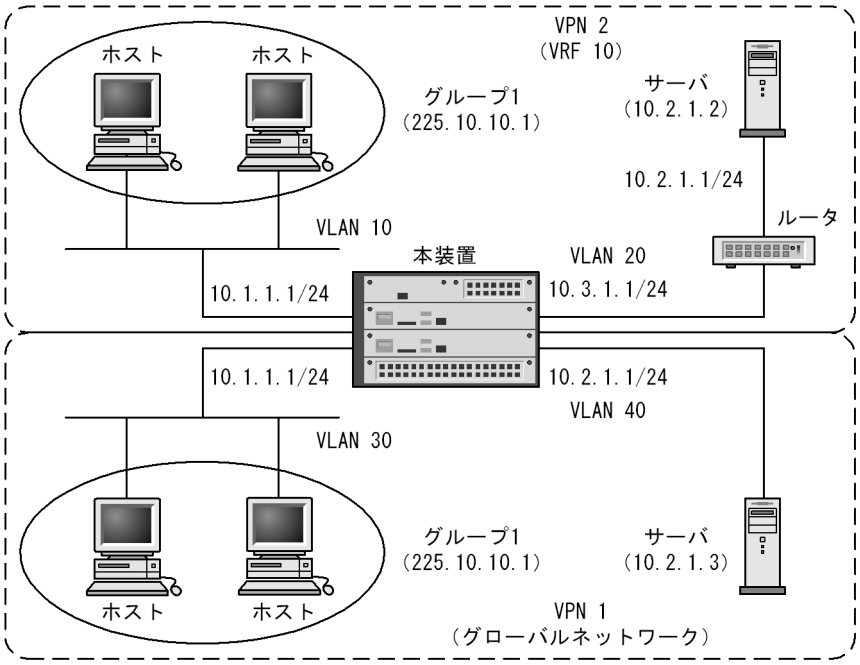
[設定のポイント]

VRF で IPv4 PIM-SM を使用するために，VRF に IPv4 マルチキャストルーティング機能を設定し，その VRF のインタフェースに IPv4 PIM-SM（sparse モード）を設定します。

IPv4 PIM-SM（sparse モード）の設定はインタフェースコンフィグレーションモードで行います。

例として，VPN 2 に VRF 10 を対応させ，VRF 10 のインタフェース VLAN20 の IP アドレスを 10.3.1.1/24 とした IPv4 PIM-SM 構成例を次の図に示します。

図 15-4 VRF での IPv4 PIM-SM 構成例



［コマンドによる設定］

1. **(config)# interface vlan 20**
   VLAN 20 を設定します。

2. **(config-if)# vrf forwarding 10**
   VLAN 20 を VRF 10 に設定します。

3. **(config-if)# ip address 10.3.1.1 255.255.255.0**
   VLAN 20 に IP アドレスを設定します。

4. **(config-if)# ip pim sparse-mode**
   (config-if)# exit
   VLAN 20 に IPv4 PIM-SM を指定します。

15.1.13 VRF での IPv4 PIM-SM ランデブーポイント候補の設定【OP-NPAR】

［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へのアドレス設定，およびグローバルコンフィグレーションモードで次の設定をします。例として，VRF 10 で管理するマルチキャストグループアドレスを 225.10.10.0/24，該当 VRF のループバックインタフェースを loopback 30，ループバックアドレスを 10.10.10.10 とした設定を示します。

［コマンドによる設定］

1. **(config)# interface loopback 30**
   (config-if)# vrf forwarding 10
   (config-if)# ip address 10.10.10.10
   (config-if)# exit
   VRF 10 のループバックインタフェース loopback 30 にループバックのアドレスを設定します。

2. **(config)# access-list 1 permit 225.10.10.0 0.0.0.255**
   VRF 10 で管理するマルチキャストグループアドレスのアクセスリストを作成します。

3. **(config)# ip pim vrf 10 rp-candidate loopback 30 group-list 1**
   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（管理するマルチキャストグループアドレスは手順 2 で作成したアクセスリストを指定します）。

15.1.14 VRF での IPv4 PIM-SM BSR 候補の設定【OP-NPAR】

[設定のポイント]

本装置を BSR 候補として使用する場合，BSR アドレスとして loopback 30 のインタフェースへのアドレス設定，およびグローバルコンフィグレーションモードで次の設定をします。例として，本装置のループバックアドレスを 10.10.10.10 とした設定を示します。

[コマンドによる設定]

1. **(config)# interface loopback 30**
   (config-if)# vrf forwarding 10
   (config-if)# ip address 10.10.10.10
   (config-if)# exit
   VRF 10 のループバックインタフェース loopback 30 にループバックの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 BSR 候補として設定します。

15.1.15 VRF での IPv4 PIM-SM 静的ランデブーポイントの設定【OP-NPAR】

[設定のポイント]

VRF で静的ランデブーポイントを設定する場合，グローバルコンフィグレーションモードで次の設定をします。例として，VRF 10 の静的ランデブーポイントの IP アドレスを 10.10.10.1 とした設定を示します。

[コマンドによる設定]

1. **(config)# ip pim vrf 10 rp-address 10.10.10.1**
   VRF 10 で 10.10.10.1 をランデブーポイントとして指定します。

15.1.16 VRF での IPv4 PIM-SSM の設定【OP-NPAR】

(1) IPv4 PIM-SSM アドレスの設定

[設定のポイント]

VRF で，本装置で IPv4 PIM-SSM を使用するには，グローバルコンフィグレーションモードで次の設定をします。本設定によって IPv4 PIM-SM が設定された VRF のインタフェースでは，指定した SSM アドレス範囲で IPv4 PIM-SSM が動作します。本装置で使用できる SSM アドレス設定は VRF ごとに一つだけです。例として，VRF 10 で IPv4 PIM-SSM が動作する SSM アドレス範囲をデフォルト（232.0.0.0/8）で使用する設定を示します。

[コマンドによる設定]

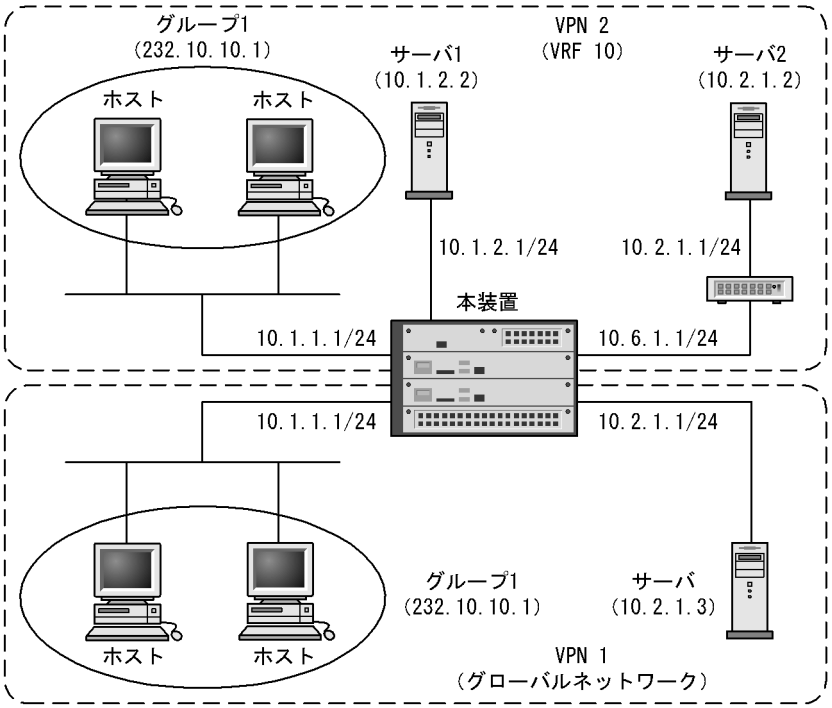
1. **(config)# ip pim vrf 10 ssm default**
   VRF 10 で IPv4 PIM-SSM を使用できるようにします（SSM アドレス範囲は 232.0.0.0/8 となります）。

(2) IGMPv2/IGMPv3（EXCLUDE モード）で IPv4 PIM-SSM を連携動作させる設定

[設定のポイント]

IGMPv2/IGMPv3（EXCLUDE モード）ではソースアドレスを特定できないため，IPv4 PIM-SSM への連携ができません。本装置では，IPv4 PIM-SSM が動作するグループアドレスとソースアドレスを設定することで IPv4 PIM-SSM への連携を行います。本機能は VRF ごとに設定します。IPv4 PIM-SSM が動作するグループアドレスは，IPv4 PIM-SSM アドレスの設定で該当 VRF に指定した SSM アドレス範囲内である必要があります。例として，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を 232.10.10.1，同一 VPN 内で二つのサーバを使用する場合，サーバ 1 のソースアドレスを 10.1.2.2，サーバ 2 のソースアドレスを 10.2.1.2 とした IPv4 PIM-SSM 構成例を次の図に示します。

図 15-5 VRF での IPv4 PIM-SSM 構成例



[コマンドによる設定]

1. **(config)# access-list 2 permit 232.10.10.1**
   グループアドレスを指定したアクセスリストを作成します。

2. **(config)# ip igmp ssm-map vrf 10 static 2 10.1.2.2**
   (config)# ip igmp ssm-map vrf 10 static 2 10.2.1.2
   VPN 2 で IPv4 PIM-SSM が動作するグループアドレス，およびサーバ 1 とサーバ 2 のソースアドレスを VRF 10 に設定します（グループアドレスは手順 1 で作成したアクセスリストを指定します）。

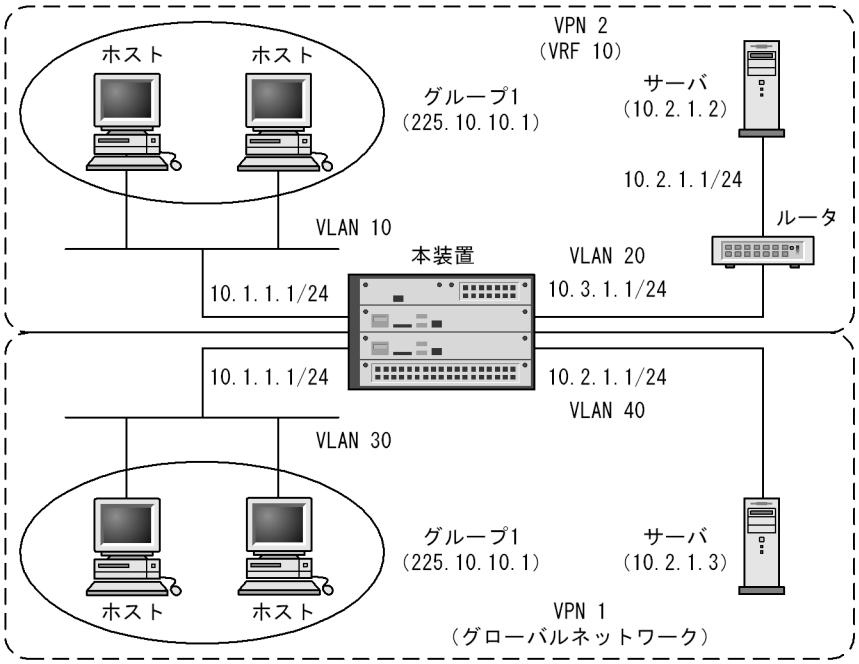
3. **(config)# ip igmp vrf 10 ssm-map enable**
   VRF 10 で IGMPv2/IGMPv3（EXCLUDE モード）で IPv4 PIM-SSM を使用できるようにします。

15.1.17 VRF での IGMP の設定【OP-NPAR】

[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。ただし，該当 VRF のインタフェースに IPv4 PIM-SM（sparse モード）を設定しても IGMP は動作します。
デフォルトでは IGMP バージョン 2，3 混在モードです。IGMP バージョンを変更する場合は，コンフィグレーションコマンド ip igmp version で設定してください。
例として，VPN 2 に VRF 10 を対応させ，VRF 10 のインタフェース VLAN10 の IP アドレスを 10.1.1.1/24 とした IGMP 構成例を次の図に示します。

図 15-6 VRF での IGMP 構成例



[コマンドによる設定]

1. **(config)# interface vlan 10**
   VLAN 10 を設定します。

2. **(config-if)# vrf forwarding 10**
   VLAN 10 を VRF 10 に設定します。

3. **(config-if)# ip address 10.1.1.1 255.255.255.0**
   VLAN 10 に IP アドレスを設定します。

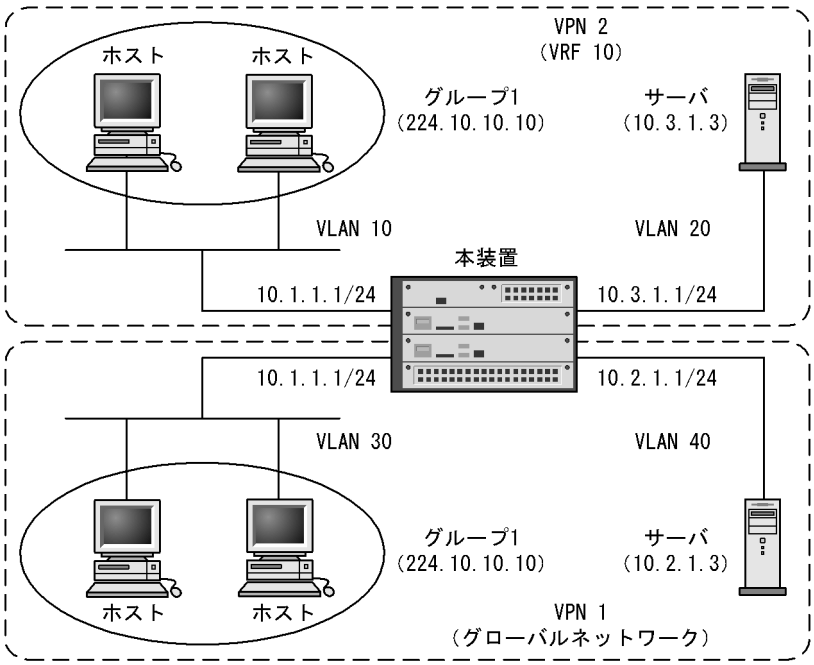
4. **(config-if)# ip igmp router**
   (config-if)# exit
   VLAN 10 に IGMP を指定します。

15.1.18 IPv4 マルチキャストエクストラネットの設定【OP-NPAR】

[設定のポイント]

IPv4 マルチキャストエクストラネットでは，中継先 VRF に送信元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，すべてのマルチキャスト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の設定はグローバルコンフィグレーションモードで行います。例として，VPN 2 に VRF 10 を対応させ，VRF 10 のインタフェースの IP アドレスを 10.1.1.1/24，10.3.1.1/24 とした 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）上のサーバ（10.3.1.3）へのユニキャスト経路が存在する必要があります。

図 15-7 VRF での PIM-SSM 構成例（IPv4 マルチキャストエクストラネット）



[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。

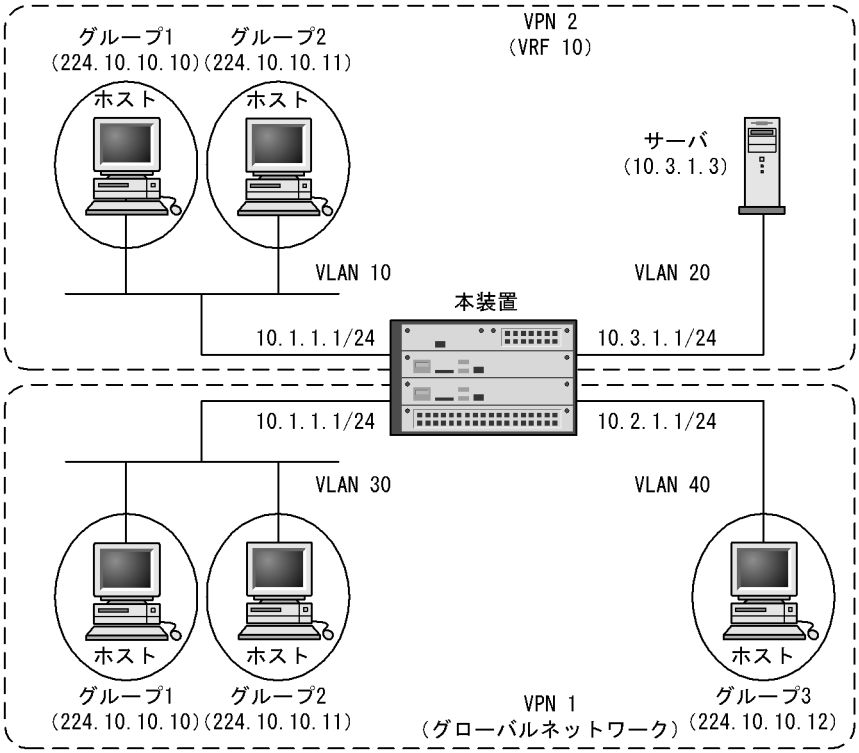
2. **(config)# vrf definition 10**
   (config-vrf)# import multicast inter-vrf MLTEXNET
   (config-vrf)# exit
   VRF 10 にすべての VRF からのマルチキャスト中継要求を許可する設定を適用します。

15.1.19 PIM-SM VRF ゲートウェイの設定【OP-NPAR】

[設定のポイント]

IPv4 マルチキャストエクストラネットでは，中継先 VRF に送信元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。
PIM-SM でマルチキャストエクストラネットによるマルチキャスト VRF 間通信をする場合，PIM-SM VRF ゲートウェイの設定が必要です。PIM-SM VRF ゲートウェイは，マルチキャスト送信者が存在する VRF に設定します。設定はグローバルコンフィグレーションモードで行います。エクストラネットで使用するグループアドレスを，ホストアドレス指定ですべてマルチキャスト経路フィルタリングに指定して，PIM-SM VRF ゲートウェイを設定します。このとき，ワイルドカードマスクによる範囲指定をしたグループアドレスは，PIM-SM VRF ゲートウェイの制御対象外となります。例として，224.10.10.10，224.10.10.11 および 224.10.10.12 のグループアドレスを，VRF 10 からグローバルネットワークに中継する設定を示します。この場合，VPN 1（グローバルネットワーク）に，VPN 2（VRF 10）上のサーバ（10.3.1.3）へのユニキャスト経路が存在する必要があります。

図 15-8 VRF での PIM-SM 構成例（PIM-SM VRF ゲートウェイ）



[コマンドによる設定]

1. **(config)# ip access-list standard MLTGROUP**

```
(config-std-nacl)# permit host 224.10.10.10
(config-std-nacl)# permit host 224.10.10.11
(config-std-nacl)# permit host 224.10.10.12
(config-std-nacl)# exit
(config)# route-map MLTEXNET permit 10
(config-route-map)# match ip address MLTGROUP
(config-route-map)# exit
```

PIM-SM VRF ゲートウェイで使用するグループアドレスとして 224.10.10.10，224.10.10.11 および 224.10.10.12 を指定します。

2.
```
(config)# vrf definition 10
(config-vrf)# import multicast inter-vrf MLTEXNET
(config-vrf)# exit
```

VRF 10 から他 VRF に対して中継するグループを指定します。

3.
```
(config)# ip pim vrf 10 vrf-gateway
```

VRF 10 に PIM-SM VRF ゲートウェイを設定します。

15.2 オペレーション

15.2.1 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 15-2 運用コマンド一覧

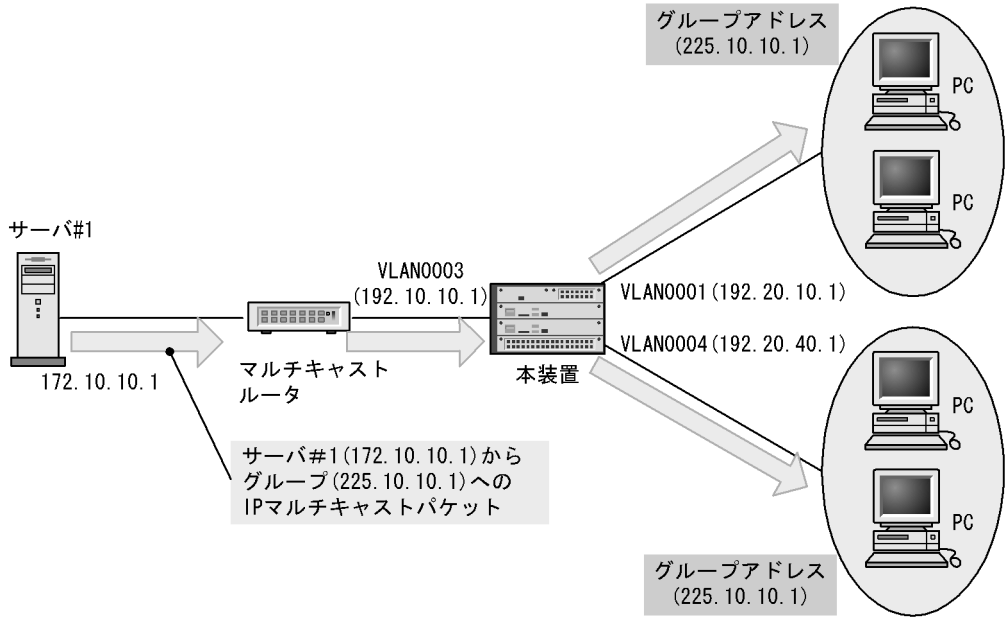
コマンド名	説明
show ip mcache	IPv4 マルチキャストの中継エントリを表示します。
show ip mroute	IPv4 マルチキャストの経路情報を表示します。
show ip pim interface	IPv4 PIM のインタフェース情報を表示します。
show ip pim neighbor	IPv4 マルチキャストインタフェースの隣接情報を表示します。
show ip pim mcache	IPv4 マルチキャストの中継エントリを表示します。
show ip pim bsr	PIM-SM BSR 情報を表示します。
show ip pim rp-mapping	PIM-SM ランデブーポイント情報を表示します。
show ip pim rp-hash	PIM-SM 各グループ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。
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で使用している各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（mrp）を再起動します。
dump protocols ipv4-multicast	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	イベントトレース情報，制御テーブル情報，コアファイルのダンプを削除します。

15.2.2 IPv4 マルチキャストグループアドレスへの経路確認

本装置で IPv4 マルチキャストを使用する場合は，show ip mcache 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。存在しない場合，および outgoing が正しくない場合は，「15.2.3 IPv4 PIM-SM 情報の確認」および「15.2.4 IGMP 情報の確認」について確認してください。

図 15-9 show ip mcache コマンドの実行結果

```
> show ip mcache
Date 2009/04/01 15:20:00 UTC
Total: 1 route
- Forwarding entry ----------------------------------------------------------
Group Address    Source Address  Flags  Uptime    Expires
225.10.10.1      172.10.10.100           01:00     02:00
     incoming:
         VLAN0003(192.10.10.1)
     outgoing:
         VLAN0001(192.20.10.1)
         VLAN0004(192.20.40.1)
>
```



15.2.3 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情報で，PIM-SM 機能を設定した場合の確認内容には次のものがあります。

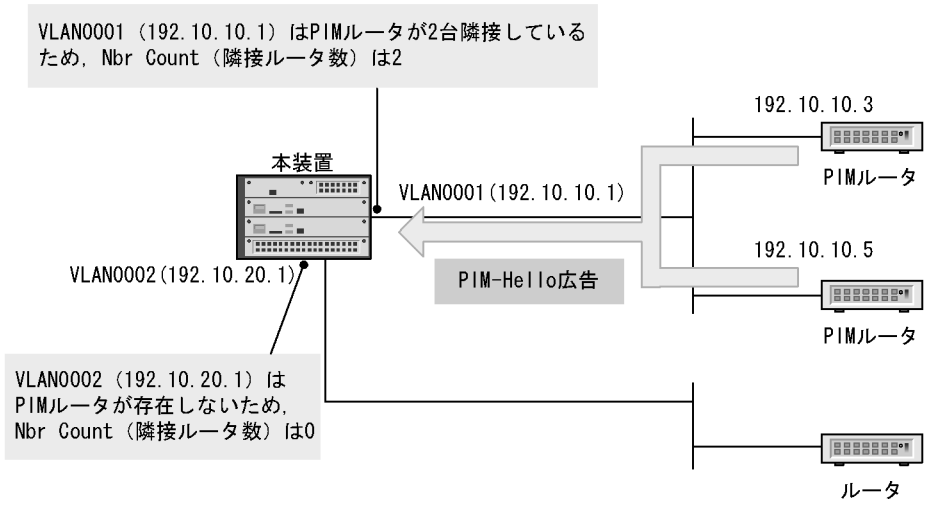
(1) インタフェース情報

show ip pim interface コマンドを実行して，次のことを確認してください。

- Address 内のインタフェースを確認してください。存在しない場合，そのインタフェースで PIM-SM は動作していません。コンフィグレーションの該当インタフェースに IGMP または IPv4 PIM-SM が設定されているか確認してください。また，そのインタフェースに障害が発生していないか確認してください。
- 該当インタフェースの Nbr Count（PIM 隣接ルータ数）を確認してください。0 の場合は隣接ルータが存在しないか，隣接ルータが PIM-Hello メッセージを広告していない可能性があります。隣接ルータを調査してください。

図 15-10 show ip pim interface コマンドの実行結果

```
> show ip pim interface
Date 2006/03/01 15:20:00 UTC
Address         Interface       Component Vif Nbr   Hello DR
                                            Count Intvl Address
192.10.10.1     VLAN0001        PIM-SM      1     2    30 192.10.10.5
192.10.20.1     VLAN0002        PIM-SM      2     0    30 This system
>
```

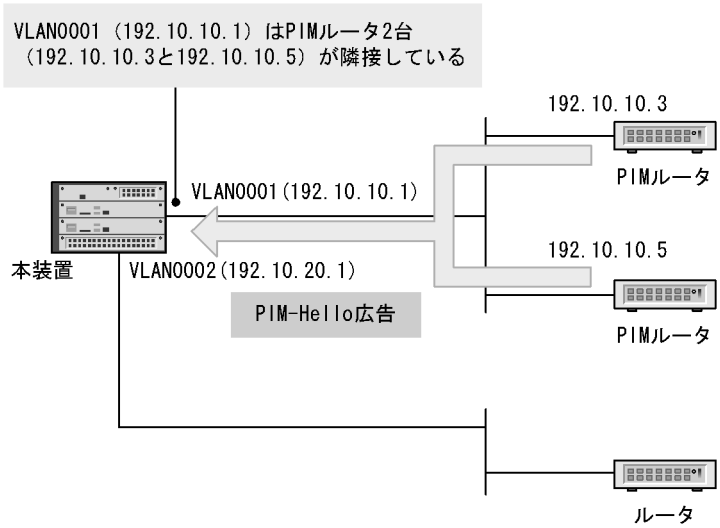


(2) 隣接情報

show ip pim neighbor コマンドを実行し，該当インタフェースの Neighbor Address 内の IP アドレスで隣接相手を確認してください。ある特定の隣接が存在しない場合，隣接ルータが PIM-Hello メッセージを広告していない可能性があります。隣接ルータを調査してください。

図 15-11　show ip pim neighbor コマンドの実行結果

```
> show ip pim neighbor
Date 2006/03/01 15:20:00 UTC
Address          Interface        Neighbor Address Uptime  Expires
192.10.10.1      VLAN0001         192.10.10.3      00:05   01:40
                                  192.10.10.5      00:10   01:35
>
```

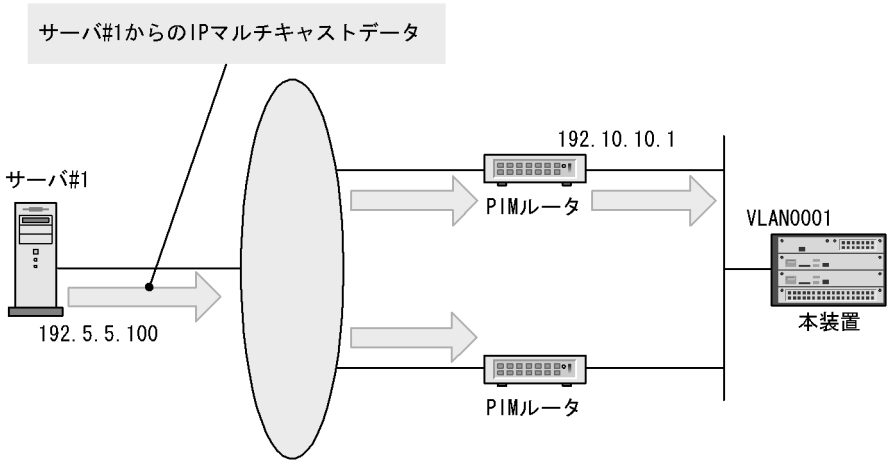


(3) 送信元ルート情報

show ip rpf コマンドを実行し，送信元のルート情報を確認してください。

図 15-12 show ip rpf コマンドの実行結果

```
> show ip rpf 192.5.5.100
Date 2006/03/01 15:20:00 UTC
Incoming: VLAN0001(192.5.5.1) Upstream: 192.10.10.1
```



(4) PIM-SM BSR 情報

show ip pim bsr コマンドを実行し，BSR アドレスが表示されていることを確認してください。” ---- ” 表示の場合，BSR が Bootstrap メッセージを広告していないか，BSR が存在していない可能性があります。BSR を調査してください。なお，PIM-SSM では BSR は使用しませんのでご注意ください。

図 15-13 show ip pim bsr コマンドの実行結果

```
> show ip pim bsr
Date 2006/03/01 15:20:00 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
>
```

(5) PIM-SM ランデブーポイント情報

show ip pim rp-mapping コマンドを実行し，該当の IPv4 マルチキャストグループアドレスに対する C-RP Address が表示されていることを確認してください。表示のない場合，BSR が Bootstrap メッセージを広告していないか，ランデブーポイントまたは BSR が存在していない可能性があります。ランデブーポイントおよび BSR を調査してください。なお，PIM-SSM ではランデブーポイントは使用しませんのでご注意ください。

図 15-14 show ip pim rp-mapping コマンドの実行結果

```
> show ip pim rp-mapping
Date 2007/04/20 15:20:00 UTC
Status : Not Candidate Rendezvous Point
Total: 2 routes, 2 groups, 1 RP
Group/Masklen       C-RP Address Priority Uptime  Expires
224.100.100.0/24    192.1.1.1         100 02:00   02:30
224.100.200.0/24    192.1.1.1         100 02:00   02:30
>
```

(6) PIM-SM 経路情報

show ip mroute コマンドを実行し，該当する宛先アドレスへの経路が存在するかどうかを確認してください。(S,G) エントリが存在しない場合は，(*,G) エントリが存在しているかを確認してください。(*,G) が存在しない場合，および incoming，outgoing が正しくない場合は隣接ルータを調査してください。なお，PIM-SSM では (*,G) は使用しません（存在しません）。

図 15-15 PIM-SM マルチキャスト経路情報の表示

```
> show ip mroute
Date 2007/04/20 15:20:00 UTC
Total: 5 routes, 4 groups, 2 sources

(S,G) 3 routes -------------------------------------------------------------
Group Address      Source Address  Protocol Flags  Uptime  Expires  Assert
224.100.100.10     192.1.1.1       SM       F      02:00   02:30    01:00
    incoming: VLAN0001 (192.1.1.3)  upstream: Direct, reg-sup: 30s
    outgoing: VLAN0002 (192.1.2.3)  uptime 02:30, expires 00:40

224.100.100.20     192.1.1.1       SM       F      02:00   02:30    01:00
    incoming: VLAN0001 (192.1.1.3)  upstream: Direct
    outgoing: register  <Register to 192.1.5.1>

224.100.100.30     192.1.4.1       SM       F      02:00   02:30    01:00
    incoming: VLAN0001 (192.1.1.3)  upstream: 192.1.1.5
    outgoing: VLAN0002 (192.1.2.3)  uptime 02:30, expires 00:40

(*,G) 2 routes -------------------------------------------------------------
Group Address      RP Address      Protocol Flags  Uptime  Expires  Assert
225.100.100.10     192.1.5.1       SM       R      02:00   02:30    01:00
    incoming: register  upstream: This System
    outgoing: VLAN0002 (192.1.2.3)  uptime 02:30, expires 00:40

225.100.100.10     192.1.5.1       SM       R      02:00   02:30    01:00
    incoming: VLAN0001 (192.1.1.3)  upstream: 192.1.1.2
    outgoing: VLAN0003 (192.1.3.3)  uptime 02:30, expires 00:40
```

15.2.4 IGMP 情報の確認

本装置の IPv4 マルチキャストルーティング情報で IGMP 機能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

show ip igmp interface コマンドを実行し，次のことを確認してください。

- Address 内のインタフェースを確認してください。存在しない場合，そのインタフェースで IGMP は動作していません。コンフィグレーションの該当インタフェースで IGMP または IPv4 PIM-SM が設定されているか確認してください。また，そのインタフェースに障害が発生していないか確認してください。
- 該当インタフェースの Group Count（加入グループ数）を確認してください。0 の場合は加入グループが存在しないかグループ加入ホストが IGMP-Report を広告していない可能性があります。ホストを調査してください。
- Version 欄に表示されているバージョンが該当のインタフェースで使用しているホストと接続可能であるか確認してください。
- Notice 欄にコードが表示される場合は IGMP パケットが廃棄されています。コードから廃棄理由を調

査してください。

図 15-16 show ip igmp interface コマンドの実行結果

```
> show ip igmp interface
Date 2008/04/10 15:10:00 UTC
Total: 5 Interfaces
Address     Interface  Version  Flags  Querier     Expires  Group Count  Notice
192.10.1.2  VLAN0001       2     S      192.10.1.2     -              2
192.20.2.2  VLAN0002       2     S      192.20.2.1   02:30            0
192.30.3.2  VLAN0003       3            192.30.3.1   00:50            2
202.30.3.2  VLAN0004     (3)            202.30.3.2     -              0   Q
210.40.4.2  VLAN0005       3            210.40.4.1   03:15            3  L
```

(2) グループ情報

show ip igmp group コマンドを実行し，Group Address 内のグループを確認してください。存在しない場合，次のことを確認してください。

- そのグループメンバー（ホスト）が IGMP-Report を広告していないおそれがあります。ホストを調査してください。
- 本装置の IGMP インタフェースのバージョンとホストの IGMP バージョンを確認して，ホストと接続可能であることを確認してください。
- ホストが IGMPv3 Query を無視する場合，IGMPv3 を使用することはできません。該当するインタフェースの IGMP バージョンを 2 に設定してください。

図 15-17 show ip igmp group コマンドの実行結果

```
> show ip igmp group brief
Date 2006/08/01 15:10:00 UTC
Total: 7 groups
Group Address   Interface       Version  Mode      Source Count
224.1.1.1       VLAN0001           2     EXCLUDE              0
232.1.1.2       VLAN0001           2     EXCLUDE              2
234.1.1.1       VLAN0003           2     EXCLUDE              1
234.1.1.2       VLAN0003           3     INCLUDE              1
232.1.1.1       VLAN0004           3     INCLUDE              1
232.1.1.3       VLAN0004           3     INCLUDE              2
235.1.1.1       VLAN0004           3     EXCLUDE              3
```

15.2.5 IPv4 PIM-DM 情報の確認

本装置の IPv4 マルチキャストルーティング情報で，PIM-DM を設定した場合の確認内容には次のものがあります。

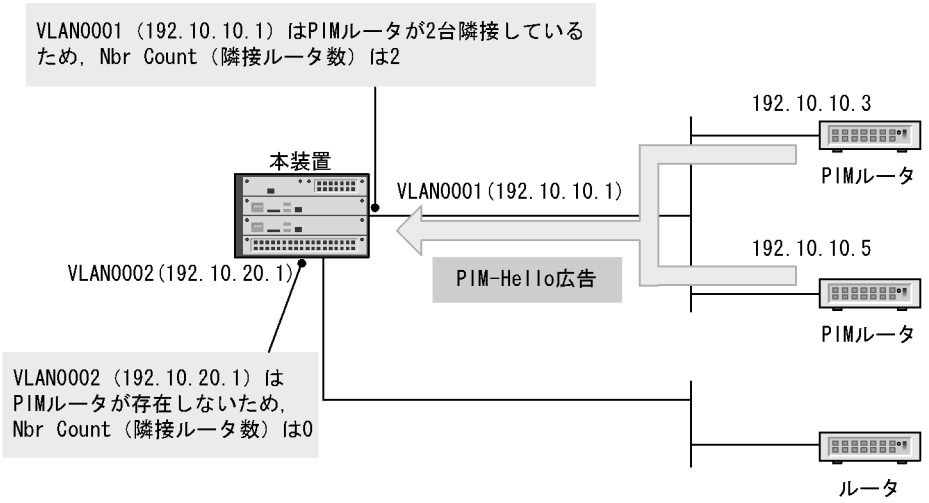
(1) インタフェース情報

show ip pim interface コマンドを実行して，次のことを確認してください。

- Address 内のインタフェースを確認してください。存在しない場合，そのインタフェースで PIM-DM は動作していません。コンフィグレーションの該当インタフェースに IPv4 PIM-DM が設定されているか確認してください。また，そのインタフェースに障害が発生していないか確認してください。
- 該当インタフェースの Nbr Count（PIM 隣接ルータ数）を確認してください。0 の場合は隣接ルータが存在しないか，隣接ルータが PIM-Hello メッセージを広告していない可能性があります。隣接ルータを調査してください。

図 15-18 show ip pim interface コマンドの実行結果

```
> show ip pim interface
Date 2011/06/01 13:22:00 UTC
Address         Interface       Component Vif Nbr   Hello DR
                                          Count Intvl Address
192.10.10.1     VLAN0001        PIM-DM      1     2    30 192.10.10.5
192.10.20.1     VLAN0002        PIM-DM      2     0    30 This system
>
```

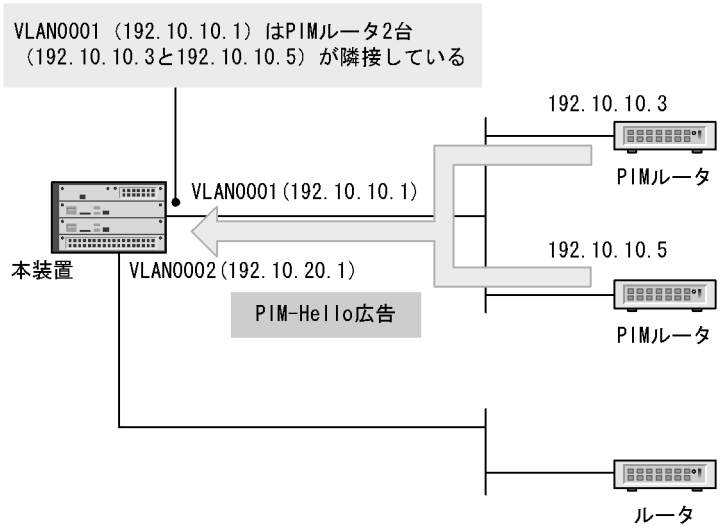


(2) 隣接情報

show ip pim neighbor コマンドを実行して，該当インタフェースの Neighbor Address 内の IP アドレスで隣接相手を確認してください。ある特定の隣接が存在しない場合，隣接ルータが PIM-Hello メッセージを広告していない可能性があります。隣接ルータを調査してください。

図 15-19 show ip pim neighbor コマンドの実行結果

```
> show ip pim neighbor
Date 2011/06/01 13:22:20 UTC
Address         Interface       Neighbor Address Uptime  Expires
192.10.10.1     VLAN0001        192.10.10.3      00:05   01:40
                                192.10.10.5      00:10   01:35
>
```



（3） PIM-DM 経路情報

show ip mroute コマンドを実行して，該当する宛先アドレスへの経路が存在するかどうかを確認してください。（S,G）エントリが存在しない場合，および incoming，outgoing が正しくない場合は隣接ルータを調査してください。

図 15-20　PIM-DM マルチキャスト経路情報の表示

```
> show ip mroute
Date 2011/06/01 13:23:25 UTC
Total: 2 routes, 2 groups, 2 sources

(S,G) 2 routes ------------------------------------------------------------
Group Address      Source Address  Protocol Flags  Uptime  Expires  Assert
224.100.100.10     192.10.10.10    DM       F      02:00   02:30    01:00
    incoming: VLAN0001 (192.10.10.1)  upstream: Direct, reg-sup: 0s
    outgoing: VLAN0002 (192.10.20.1)  uptime 02:30, expires --:--

224.100.100.30     192.1.4.1       DM       F      02:00   02:30    01:00
    incoming: VLAN0001 (192.10.10.1)  upstream: 192.1.1.5
    outgoing: VLAN0002 (192.10.20.1)  uptime 02:30, expires --:--
```

16 IPv4 マルチキャスト経路フィルタリング【OP-NPAR】

この章では，IPv4 マルチキャスト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。

16.1 IPv4 マルチキャスト経路フィルタリング解説

16.1.1 IPv4 マルチキャスト経路フィルタリング概説

IPv4 マルチキャスト経路フィルタリングは，IPv4 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 IPv4 マルチキャストエクストラネットだけで使用します。

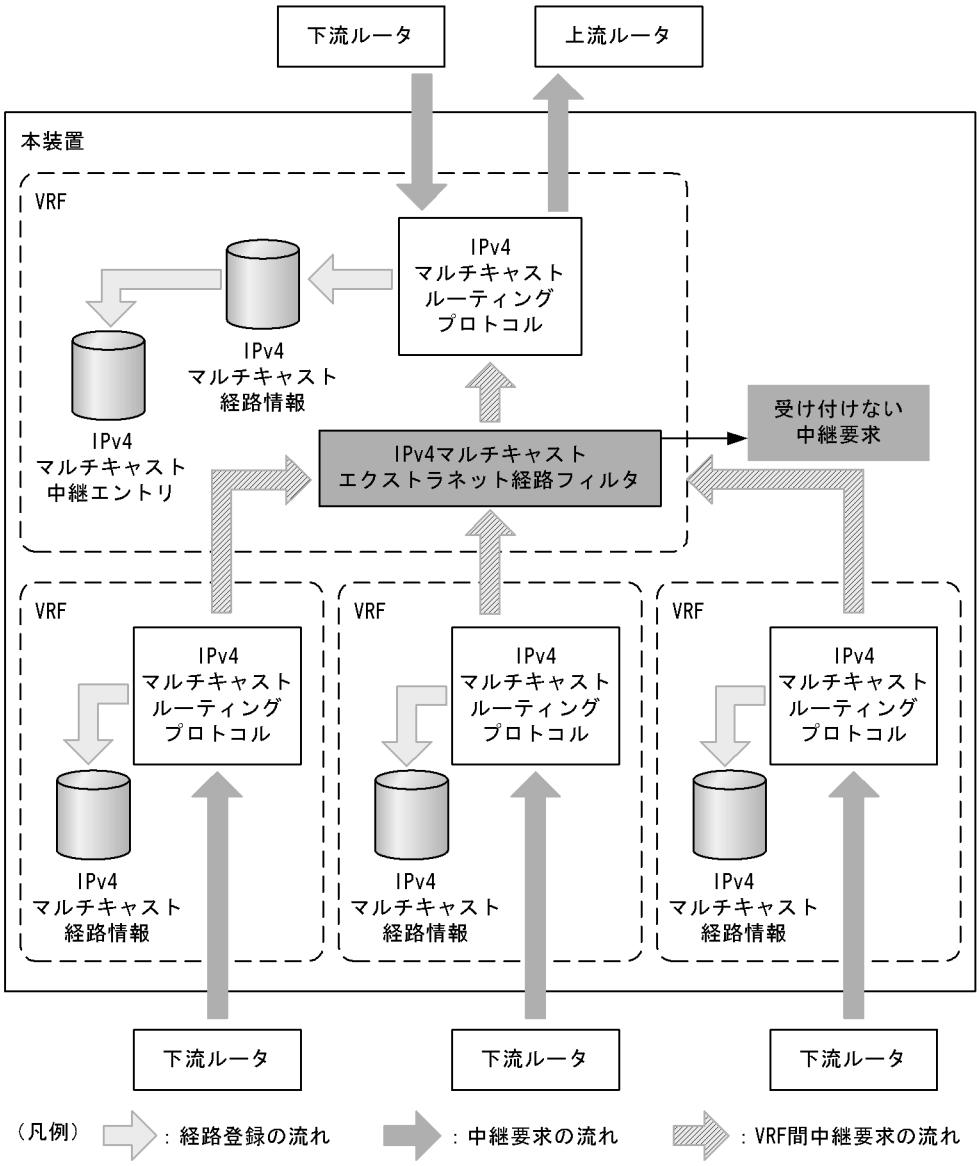
(1) IPv4 マルチキャストエクストラネットの経路フィルタリング

IPv4 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。IPv4 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宛先 IP 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，IPv4 マルチキャストルーティングプロトコルは送信元 IP 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。

IPv4 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。

IPv4 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を次の図に示します。

図 16-1　IPv4 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



16.1.2　IPv4 マルチキャストフィルタ方法

IPv4 マルチキャストフィルタ方法については,「13.1.2　フィルタ方法」を参照してください。

IPv4 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 16-1　IPv4 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 prefix-list	未サポートです。指定した場合は無視します。
ip access-list standard	permit だけを使用します。 deny を指定した IP アドレスは無視します。
ip access-listt extended	未サポートです。指定した場合は無視します。
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。

コンフィグレーションコマンド	説明
ip as-path access-list	未サポートです。指定した場合は無視します。
ip community-list standard	未サポートです。指定した場合は無視します。
ip community-list extended	未サポートです。指定した場合は無視します。

16.1.3 IPv4 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 IPv4 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 import multicast inter-vrf 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 IPv4 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。

IPv4 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 16-2 IPv4 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。

IPv4 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 16-3 IPv4 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
宛先 IPv4 マルチキャストグループアドレス	access-list の識別子を条件として指定し，指定したフィルタで宛先の IPv4 マルチキャスト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，一致したとみなします。 本条件を設定しない場合，すべての IPv4 マルチキャスト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
VRF ID	VRF ID を条件として指定し，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 IPv4 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

IPv4 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。IPv4 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，IPv4 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 IP アドレスへの経路を自 VRF となるように設定します。

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

IPv4 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 16-4 コンフィグレーションコマンド一覧

コマンド名	説明
access-list ※1	IPv4 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 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。
match ip address ※2	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 vrf ※2	route-map に VRF によるフィルタ条件を設定します。
import multicast inter-vrf ※3	他 VRF またはグローバルネットワークからの IPv4 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。

注※ 1
「コンフィグレーションコマンドレファレンス Vol.2　4. 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　14. 経路フィルタリング（IPv4 ／ IPv6 共通）」を参照してください。

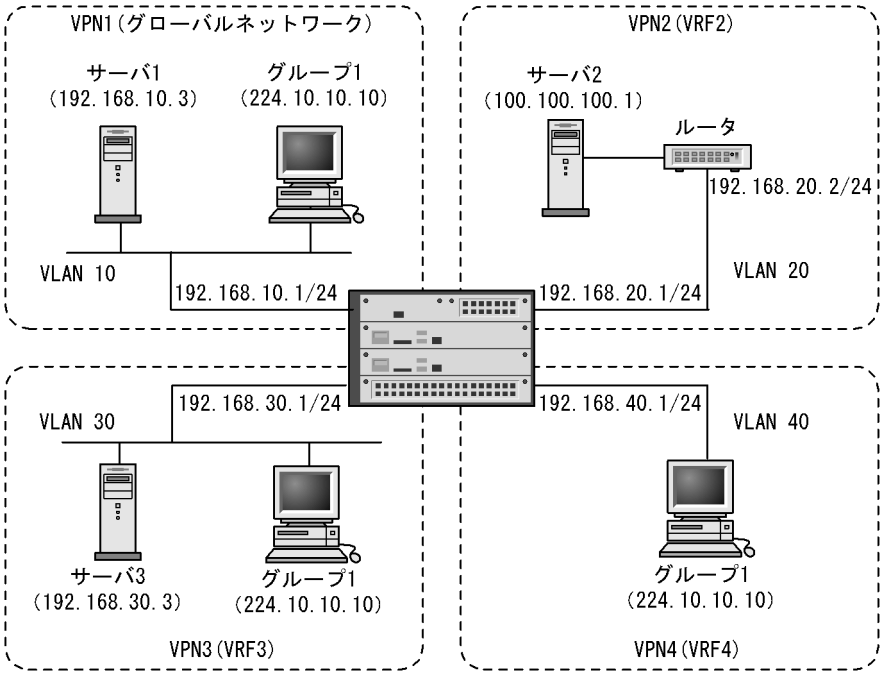
注※ 3
「コンフィグレーションコマンドレファレンス Vol.3　30. VRF【OP-NPAR】」を参照してください。

16.2.2 IPv4 マルチキャストエクストラネット

次の図のようなネットワーク構成で，IPv4 マルチキャストエクストラネットを設定します。

IPv4 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 16-2 IPv4 マルチキャストエクストラネットの構成例



(1) すべての VRF からの要求を許可する設定

VRF 2 が，すべての VRF およびグローバルネットワークからの IPv4 マルチキャスト中継要求を許可す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，中継先 VRF およびグローバルネットワークから IPv4 マルチキャスト送信元への経路が 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 IPv4 マルチキャスト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 IPv4 マルチキャスト中継要求を許可するように設定します。

(2) 特定 VRF だけ許可する設定

VRF 2 が VRF 3 および VRF 4 からの IPv4 マルチキャスト中継要求を許可す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，VRF3 および VRF4 から IPv4 マルチキャスト送信元への経路が VRF2 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 IPv4 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 IPv4 マルチキャスト中継要求だけ許可にします。

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 IPv4 マルチキャストエクストラネットに適用して，VRF3 および VRF4 からの IPv4 マルチキャスト中継要求を許可するように設定します。

(3) 特定グループアドレスだけ許可する設定

224.10.0.0/16 の範囲内のグループアドレスだけ IPv4 マルチキャスト中継要求を許可するように設定します。

[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 224.10.0.0 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を 224.10.0.0/16 に設定します。

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 IPv4 マルチキャスト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 224.10.0.0/16 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，IPv4 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 IPv4 マルチキャスト送信元への経路が，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 224.10.10.0 0.0.0.255
   (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 VRF4 からのグループアドレス 224.10.10.0/24 に対する IPv4 マルチキャスト中継要求を許可にします。

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 IPv4 マルチキャストエクストラネットに適用して，相互に IPv4 マルチキャスト中継要求を許可するように設定します。

16.3 オペレーション

16.3.1 運用コマンド一覧

IPv4 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 16-5 運用コマンド一覧

コマンド名	説明
show ip mcache ※	IPv4 マルチキャスト中継エントリを一覧表示します。
show ip mroute ※	IPv4 マルチキャスト経路情報を一覧表示します。
show ip multicast resources ※	IPv4 マルチキャストルーティングで使用している各エントリ数を表示します。

注※
「運用コマンドレファレンス Vol.3　7. 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。

16.3.2 IPv4 マルチキャストエクストラネットの確認

show ip mroute 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参照できます。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。

図 16-3 show ip mroute コマンドの実行結果

```
> show ip mroute vrf all group 224.10.10.10 source 100.100.100.1
Date 2009/02/20 02:34:22 UTC
Total: 4 routes
VRF: global  Total: 1 route , 1 group , 1 source

(S,G) 1 routes  -----------------------------------------------------
Group Address  Source Address  Protocol Flags  Uptime  Expires  Assert
224.10.10.10   100.100.100.1   SM              00:03   03:27    00:00
    incoming: VRF 2     upstream: Extra  reg-sup: 0s
    outgoing: VLAN0010(192.168.10.1)     uptime 00:03  expires 03:27
              VLAN0011(192.168.11.1)     uptime 00:03  expires 03:27

VRF: 2  Total: 1 routes, 1 groups, 1 source

(S,G) 1 routes  -----------------------------------------------------
Group Address  Source Address  Protocol Flags  Uptime  Expires  Assert
224.10.10.10   100.100.100.1   SM       L      00:03   03:27    00:00
    incoming: VLAN0020(192.168.20.1)     upstream: 192.168.20.2
    outgoing: VLAN0021(192.168.21.1)     uptime 00:03  expires 03:27
              global                     uptime --:--
              VRF 3                      uptime --:--
              VRF 4                      uptime --:--

VRF: 3  Total: 1 routes, 1 groups, 1 source

(S,G) 1 routes  -----------------------------------------------------
Group Address  Source Address  Protocol Flags  Uptime  Expires  Assert
224.10.10.10   100.100.100.1   SM       L      00:03   03:27    00:00
    incoming: VRF 2     upstream: Extra  reg-sup: 0s
    outgoing: VLAN0030(192.168.30.1)     uptime 00:03  expires --:--

VRF: 4  Total: 1 routes, 1 groups, 1 source

(S,G) 1 routes  -----------------------------------------------------
Group Address  Source Address  Protocol Flags  Uptime  Expires  Assert
224.10.10.10   100.100.100.1   SM              00:03   03:27    00:00
    incoming: VRF 2     upstream: Extra  reg-sup: 0s
    outgoing: VLAN0040(192.168.40.1)     uptime 00:03  expires 03:27
```

図 16-4　show ip mcache コマンドの実行結果

```
> show ip mcache vrf all source 100.100.100.1 group 224.10.10.10
Date 2009/02/20 02:34:43 UTC
Total: 4 routes
VRF: global  Total: 1 route
- Forwarding entry ------------------------------------------------
Group Address    Source Address  Flags  Uptime  Expires
224.10.10.10     100.100.100.1   D       00:19   03:27
     incoming:
         VRF 2
     outgoing:
         VLAN0010(192.168.10.1)
         VLAN0011(192.168.11.1)

VRF: 2  Total: 1 routes
- Forwarding entry ------------------------------------------------
Group Address    Source Address  Flags  Uptime  Expires
224.10.10.10     100.100.100.1   U       00:19   03:27
     incoming:
         VLAN0020(192.168.20.1)
     outgoing:
         VLAN0021(192.168.21.1)
         VLAN0010(192.168.10.1)     global
         VLAN0011(192.168.11.1)     global
         VLAN0030(192.168.30.1)     VRF 3
         VLAN0040(192.168.40.1)     VRF 4

VRF: 3  Total: 1 routes
- Forwarding entry ------------------------------------------------
Group Address    Source Address  Flags  Uptime  Expires
224.10.10.10     100.100.100.1   D       00:19   03:27
     incoming:
         VRF 2
     outgoing:
         VLAN0030(192.168.30.1)

VRF: 4  Total: 1 routes
- Forwarding entry ------------------------------------------------
Group Address    Source Address  Flags  Uptime  Expires
232.0.0.1        10.2.0.100      D       00:18   03:27
     incoming:
         VRF 2
     outgoing:
         VLAN0040(192.168.40.1)
```

17 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。

17.1 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。

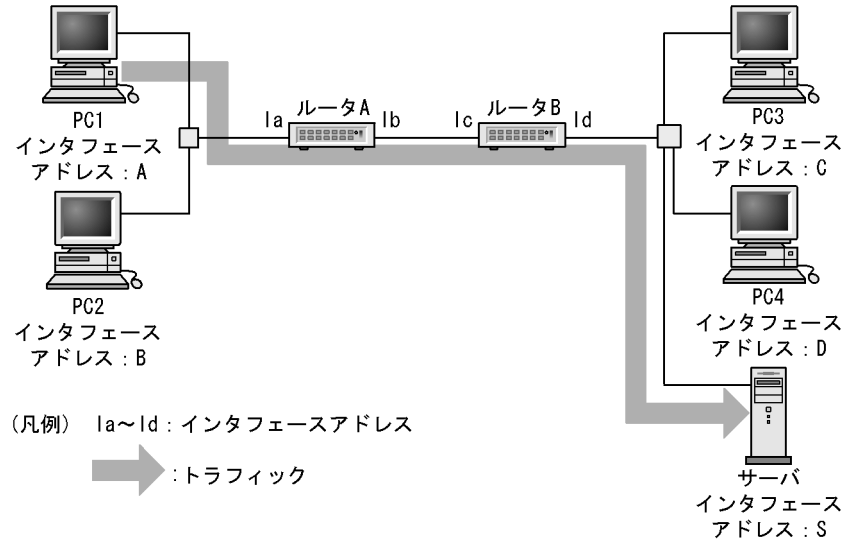
17.1.1 IPv6 アドレス

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。

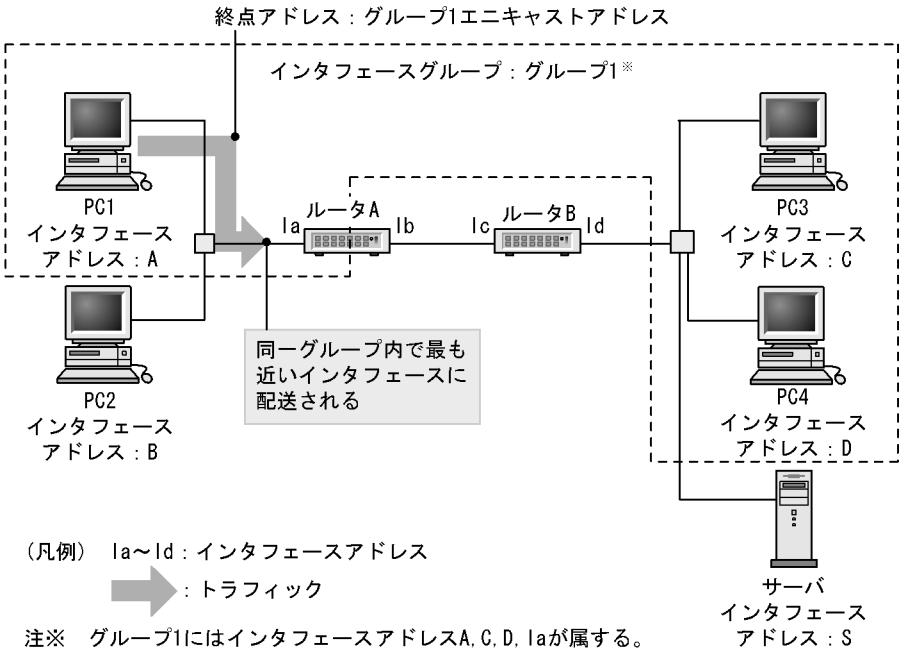
図 17-1 ユニキャストアドレス通信



(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，インタフェース集合のうち，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。

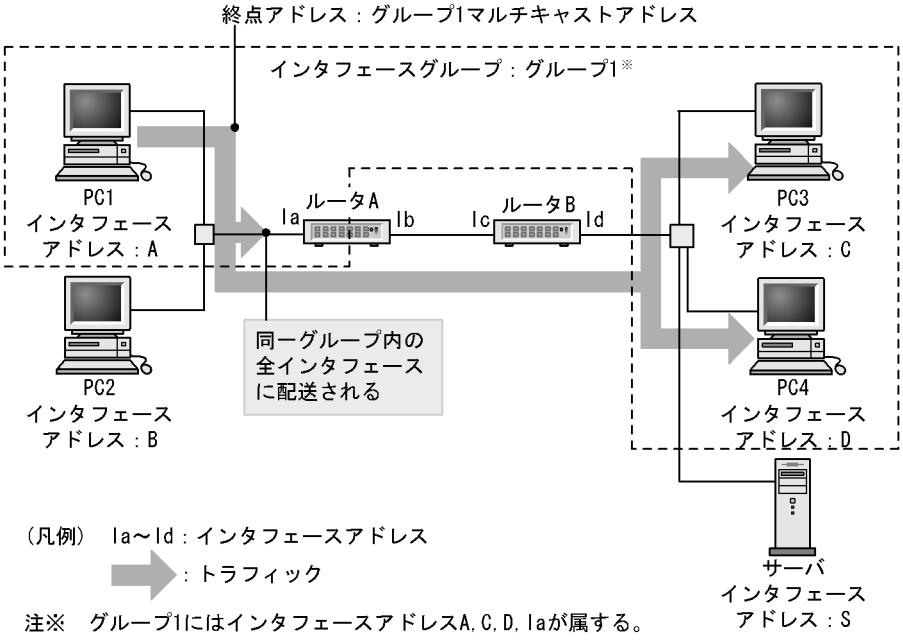
図 17-2　エニキャストアドレス通信



(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集合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 17-3　マルチキャストアドレス通信



17.1.2　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。

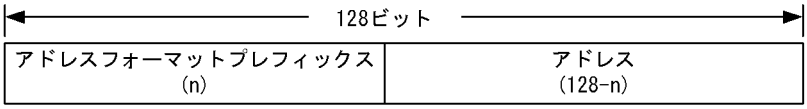
- 16 進数で 16 ビットごとにコロン " : " で区切った形式で表記します。
  （例） 3ffe:0501:0811:ff02:0000:08ff:fe8b:3090
- 16 進数の先頭にくる "0" は省略できます。
  （例） 3ffe:501:811:ff02:0:8ff:fe8b:3090
- 連続する "0" は二つのコロン "::" に置換できます。ただし，"::" に置換できるのは一つのアドレス表記に 1 か所までと定義されています。
  （例） 次に示す IPv6 アドレスのときの置換方法
  fe80:0000:0000:0000:0000:0000:0000:3090 → 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。

17.1.3 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 17-4 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 17-1 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	予備
0000 0001	未割り当て
0000 001	NSAP 割り当て用予約
0000 010	IPX 割り当て用予約
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

プレフィックス (2 進数)	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	未割り当て
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	サイトローカルユニキャストアドレス
1111 1111	マルチキャストアドレス

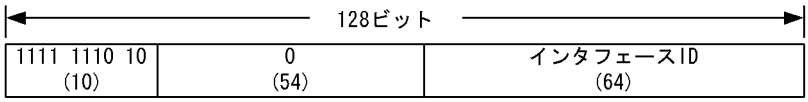
17.1.4 ユニキャストアドレス

(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することはありません。

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 17-5 IPv6 リンクローカルアドレス

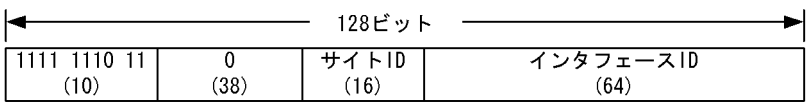


( )内の数字はビット数を示す。

(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。サイトローカルアドレスは，RFC3879 で廃止されることが決定しているため，使用することはお勧めできません。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。

図 17-6 IPv6 サイトローカルアドレス

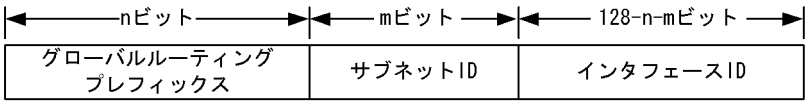


( )内の数字はビット数を示す。

(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，インターネットを介した通信を行う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。

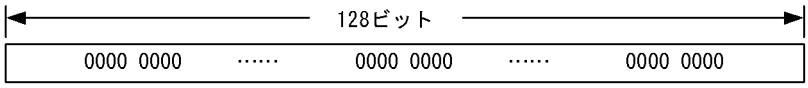
図 17-7 IPv6 グローバルアドレス



(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。未指定アドレスをノードに対して意図的に割り当てることはできません。未指定アドレスを次の図に示します。

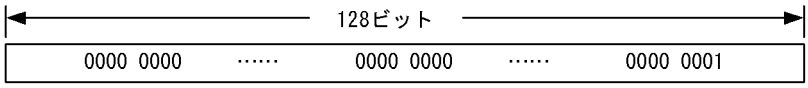
図 17-8 未指定アドレス



(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通信を行う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をインタフェースに対して割り当てることはできません。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。

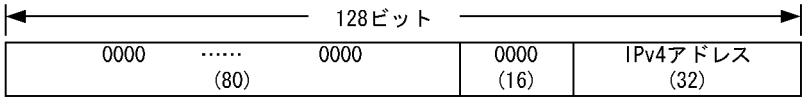
図 17-9 ループバックアドレス



(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を行う場合に使用します。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。

図 17-10 IPv4 互換アドレス

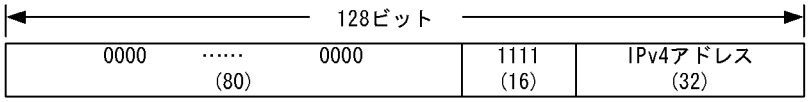


（ ）内の数字はビット数を示す。

(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 17-11 IPv4 射影アドレス

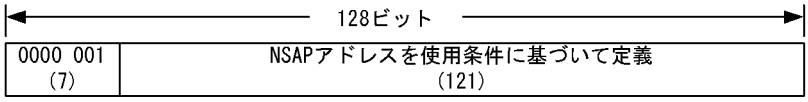


（ ）内の数字はビット数を示す。

(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。

図 17-12 NSAP 互換アドレス

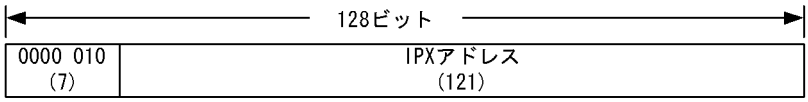


（ ）内の数字はビット数を示す。

(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。

図 17-13 IPX 互換アドレス



（ ）内の数字はビット数を示す。

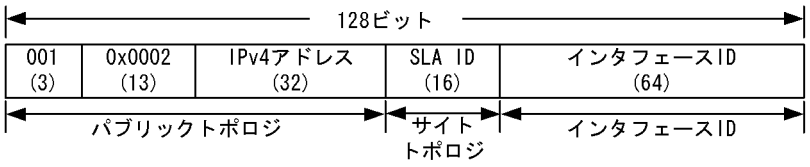
(10) 6to4 アドレス

6to4 トンネルで使用するアドレス形式です。6to4 トンネル用として，IANA(Internet Assigned Numbers

Authority) から IPv6 グローバルアドレスにおける集約子の一つである TLA ID には 0x0002 が割り当てられています。また，NLA ID には 6to4 トンネルを使用するサイトが持つグローバル・ユニキャスト・IPv4 アドレスが定義されます。

6to4 アドレスを次の図に示します。

図 17-14　6to4 アドレス

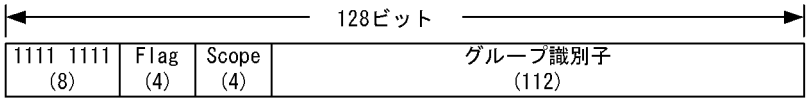


（　）内の数字はビット数を示す。

17.1.5　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属することができます。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することはできません。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 17-15　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定義されています。4 ビット目は T(transient) フラグビットと定義されており，次の値になります。

1. 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
2. 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 17-2　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	ノードローカルスコープ
2	リンクローカルスコープ
3	未割り当て
4	未割り当て
5	サイトローカルスコープ
6	未割り当て

値	スコープの範囲
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) 予約マルチキャストアドレス

次に示すマルチキャストアドレスはあらかじめ予約されており，どのマルチキャストグループにも割り当てることができません。

1. ff00:0:0:0:0:0:0:0
2. ff01:0:0:0:0:0:0:0
3. ff02:0:0:0:0:0:0:0
4. ff03:0:0:0:0:0:0:0
5. ff04:0:0:0:0:0:0:0
6. ff05:0:0:0:0:0:0:0
7. ff06:0:0:0:0:0:0:0
8. ff07:0:0:0:0:0:0:0
9. ff08:0:0:0:0:0:0:0
10. ff09:0:0:0:0:0:0:0
11. ff0a:0:0:0:0:0:0:0
12. ff0b:0:0:0:0:0:0:0
13. ff0c:0:0:0:0:0:0:0
14. ff0d:0:0:0:0:0:0:0
15. ff0e:0:0:0:0:0:0:0
16. ff0f:0:0:0:0:0:0:0

(2) 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。

1. ff01:0:0:0:0:0:0:1 ノードローカル・全ノードアドレス
2. ff02:0:0:0:0:0:0:1 リンクローカル・全ノードアドレス

(3) 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。

1. ff01:0:0:0:0:0:0:2 ノードローカル・全ルータアドレス

2. ff02:0:0:0:0:0:0:2 リンクローカル・全ルータアドレス
3. ff05:0:0:0:0:0:0:2 サイトローカル・全ルータアドレス

(4) 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。

17.1.6 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付与する IPv6 アドレスとして次のアドレスを使用できます。

1. グローバルユニキャストアドレス
2. 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。

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

(2) 設定できないアドレス

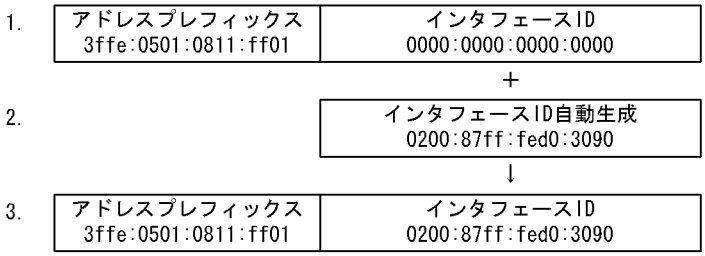
次に示す形式の IPv6 アドレスはインタフェースに付与することはできません。

1. マルチキャストアドレス
2. 未定義アドレス
3. ループバックアドレス
4. IPv4 互換アドレス
5. IPv4 射影アドレス
6. 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
7. 上位 10 ビットが 1111 1111 10 で始まり，以降のビットがすべて 0 のアドレス
8. プレフィックス長が 64 以外のときに，インタフェース ID 部がすべて 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 17-16　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する。(例 3ffe:0501:0811: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する。(例 0200:87ff: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する。

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，自動的にリンクローカルユニキャストアドレスを生成し設定します。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条件

本装置では，インタフェース ID の指定がない場合は自動生成を行います。インタフェース ID の長さは 64 ビット固定となっているため，プレフィックス長で 64 または省略以外の指定が行われた場合は，インタフェース ID を自動生成しないで，入力されたプレフィックスをアドレスとして判断します。そのため下位 64 ビットがすべて 0 になるようなアドレス指定は設定できません。プレフィックス長で設定できる条件を次の表に示します。

表 17-3　プレフィックス長で設定できる条件

アドレス指定形式	設定許可	説明
3ffe:501::/1 ～ 3ffe:501::/31	○	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。
3ffe:501::/32 ～ 3ffe:501::/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。
3ffe:501::/64 or 3ffe:501::	○	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。
3ffe:501::/65 ～ 3ffe:501::/128	×	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。

(凡例)　○：設定できる　×：設定できない

17.1.7　ステートレスアドレス自動設定機能

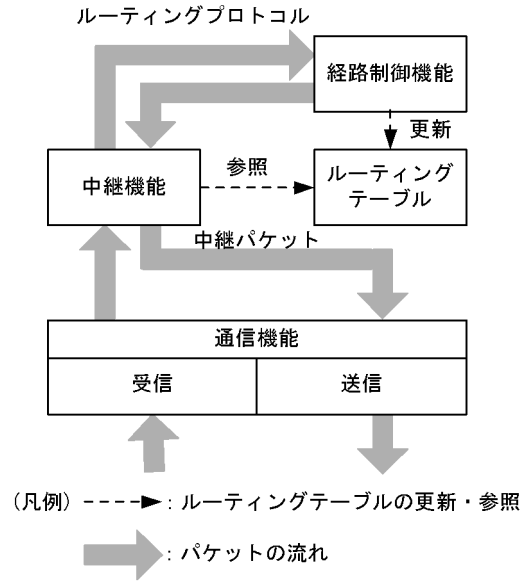
IPv6 リンクローカルアドレスを装置内で自動生成する機能，およびホストが IPv6 アドレスを自動生成する場合に必要な情報をルータから通知する機能です。本装置では IPv6 ステートレスアドレス自動設定 (RFC2462 準拠) をサポートしています。

17.2　IPv6 レイヤ機能

17.2.1　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。次の図に IPv6 ルーティング機能の概要を示します。

図 17-17　IPv6 ルーティング機能の概要



- 通信機能
  IPv6 レイヤの送信および受信処理を行う機能です。
- 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。

17.2.2　IPv6 アドレス付与単位

本装置では VLAN 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 アドレスを設定することができ，IPv6 アドレスを設定した VLAN 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。

17.3 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。

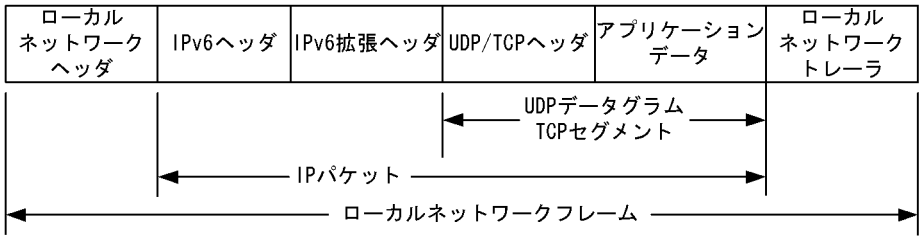
- IPv6
- ICMPv6
- NDP

17.3.1 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 17-18　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 17-19 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チェックを行います。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 17-4 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処理	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	廃棄する	送出しない
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	パケット長と比較する パケット長＜ペイロード長	廃棄する	送出しない
	パケット長と比較する パケット長≧ペイロード長	パケットの後部をペイロード長で削除する	送出しない
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	－	－
	フォワーディング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	廃棄する	送出する※
送信元アドレス	次の条件を満たすこと 1. リンクローカルアドレスでないこと 2. マルチキャストアドレスでないこと	廃棄する	送出しない
宛先アドレス	次の条件を満たすこと 1. ループバックアドレスでないこと 2. インタフェース ID 部が 0 でないこと(ただし，未定義アドレスを除く)	廃棄する	送出しない

（凡例）　－：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 17-5　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	○	○	－
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
本装置が着信するパケットが次の条件に該当する場合，パケットは廃棄されます。
・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，パケットは廃棄されます。
・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

17.3.2　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 RFC2463 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 17-6　ICMPv6 メッセージサポート仕様

ICMPv6 メッセージ				サポート
タイプ（種別）	値（10 進）	コード（詳細種別）	値（10 進）	
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	○

ICMPv6 メッセージ				サポート
タイプ (種別)	値 (10 進)	コード (詳細種別)	値 (10 進)	
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	○

（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。

- フォワーディングする受信 IPv6 パケットの Hoplimit が 1 の場合
- 受信パケットが ICMPv6 以外の IPv6 パケット

17.3.3 NDP

本装置が送信する NDP フレームのフォーマット，および設定値は RFC2461 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 を動作させることができます。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後，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 show ipv6 neighbors コマンドで 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。

17.4　中継機能

中継機能とは，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処理機能です。

17.4.1　ルーティングテーブルの内容

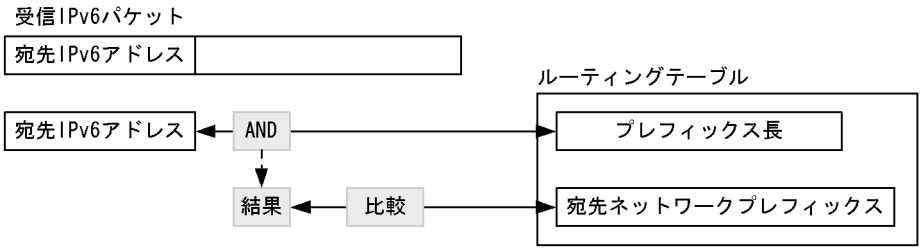
ルーティングテーブルは複数個のエントリから構成されており，各エントリは次の内容を含んでいます。本装置のルーティングテーブルの内容は show ipv6 route コマンドで表示できます。

- 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。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る中継を行う場合には 128 を表示します。
- Next Hop：次に中継するルータの IPv6 アドレス
- Interface：Next Hop のあるインタフェース名称
- Metric　：ルートのメトリック
- Protocol ：学習元プロトコル
- Age　　：ルートが確認，または変更されてからの時間 (秒)

17.4.2　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よりマスク (AND) を取り，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 17-20　ルーティングテーブルの検索



17.5 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 バイト以上と規定されています (RFC2460)。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 通信を行うインタフェースの 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，本装置を介した IPv6 中継が発生することがあります。

この際，ICMPv6 Redirect の送信可否判定を行うため，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) IPv6 アドレス重複

IPv6 には RFC2462 で規定されている DAD（Duplicate Address Detection）機能があります。DAD でアドレスが重複した場合，その IPv6 アドレスでは通信できません。show ipv6 interface コマンドまたは show ip-dual interface コマンドで表示される IPv6 アドレスの横に duplicated と表示された場合，その IPv6 アドレスは他装置と重複していますので，次のように対応してください。

- 他装置の IPv6 アドレスが誤っている場合
  他装置の IPv6 アドレスを修正後，本装置の IPv6 アドレスをいったん削除して再度設定するか，本装置を再起動してください。
- 本装置の IPv6 アドレスが誤っている場合
  コンフィグレーションで本装置の重複している IPv6 アドレスを削除して，正しい IPv6 アドレスを設定してください。
- 自動生成された IPv6 アドレスが重複する場合
  VLAN インタフェースでループ構成が発生しているか，本装置の IPv6 アドレスになりすましている端末があります。要因を取り除いてから，いったん no ipv6 enable コマンドを実行後，再度 ipv6 enable コマンドを実行してください。

(4) 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が行われません。

- 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の VLAN をリスタートしてください。

(5) IPv6 拡張オプション付きパケットのレイヤ 3 中継

- 中継点オプション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加している 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。

18 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。

18.1 コンフィグレーション

18.1.1 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 18-1 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 redirects	ICMPv6 リダイレクトメッセージの送信可否を指定します。

18.1.2 インタフェースの設定

[設定のポイント]

VLAN 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 vlan 100**
   VLAN ID 100 のインタフェースコンフィグレーションモードに移行します。

2. **(config-if)# ipv6 enable**
   VLAN ID 100 に IPv6 アドレス使用可を設定します。

3. **(config-if)# ipv6 address 2001:100::1/64**
   VLAN ID 100 に IPv6 アドレス 2001:100::1，プレフィックス長 64 を設定します。

4. **(config-if)# ipv6 address 2001:200::1/64**
   VLAN ID 100 に IPv6 アドレス 2001:200::1，プレフィックス長 64 を追加します。

18.1.3 リンクローカルアドレスの手動設定

[設定のポイント]

本装置ではコンフィグレーションコマンドの ipv6 enable 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 vlan 100**
   VLAN ID 100 のインタフェースコンフィグレーションモードに移行します。

2. **(config-if)# ipv6 enable**
   VLAN ID 100 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**
   VLAN ID 100 の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。

18.1.4 loopback 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**
   ループバックのインタフェース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::1**
   装置に IPv6 アドレス 2001::1 を設定します。

18.1.5 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 2001:100::2 interface vlan 100 0012.e240.0a00**
   VLAN ID 100 にネクストホップ IPv6 アドレス 2001:100::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。

18.2 オペレーション

18.2.1 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 18-2 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。
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。
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。
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。

18.2.2 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，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 18-1 「IPv6 インタフェース状態」の表示例

```
> show ipv6 interface summary
vlan100: UP  2001::1/64
vlan200: UP  2002::1/64
>
```

18.2.3 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，通信相手となる装置に対して通信できるかどうかを，ping ipv6 コマンドを実行して確認してください。

図 18-2 ping ipv6 コマンドの実行結果（通信可の場合）

```
> ping ipv6 2001::2
PING6 (56=40+8+8 Bytes) 2001::1 -->2001::2
16 bytes from 2001::2, icmp_seq=0 ttl=255 time=0.286 ms
16 bytes from 2001::2, icmp_seq=1 ttl=255 time=0.271 ms
16 bytes from 2001::2, icmp_seq=2 ttl=255 time=0.266 ms
^C
--- 2001::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 18-3 ping ipv6 コマンドの実行結果（通信不可の場合）

```
> ping ipv6 2001::2
PING6 (56=40+8+8 bytes) 2001::1 --> 2001::2
^C
--- 2001::2 ping6 statistics ---
12 packets transmitted, 0 packets received, 100% packet loss
>
```

18.2.4 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 18-4 traceroute ipv6 コマンドの実行結果

```
> traceroute ipv6 2003::1 numeric
traceroute6 to 2003::1 (2003::1), 30 hops max, 40 byte packets
1  2001::1  0.612 ms  0.541 ms  0.532 ms
2  2002::1  0.905 ms  0.816 ms  0.807 ms
3  2003::1  1.325 ms  1.236 ms  1.227 ms
>
```

18.2.5 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，本装置と隣接装置間のアドレス解決をしているか（NDP エントリ情報があるか）どうかを確認してください。

図 18-5 show ipv6 neighbors コマンドの実行結果

```
> show ipv6 neighbors interface vlan 100
Date 2006/03/25 14:00 UTC
Total: 3 entries
Neighbor             Linklayer Address Netif      Expire    S Flgs P
2001::1              0012.e222.f298    VLAN0100   7s        R
2002::1              0012.e26b.8e1b    VLAN0100   24s       R
fe80::1%VLAN0100     0012.e240.3f90    VLAN0100   2s        R R
```

19 Null インタフェース（IPv6）

この章では，IPv6 ネットワークの 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。

19.1 解説

IPv6 は Null インタフェースをサポートします。Null インタフェースの詳細については，「3.1 解説」を参照してください。

なお，IPv6 スタティックルーティングおよび経路制御の詳細については，「25 スタティックルーティング（IPv6）」～「29 BGP4+【OP-BGP】」を参照してください。

19.2 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

Null インタフェース（IPv6）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 19-1 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。
ipv6 route ※	IPv6 スタティック経路を生成します。

注※
「コンフィグレーションコマンドレファレンス Vol.3　24. スタティックルーティング（IPv6）」を参照してください。

19.2.2 Null インタフェースの設定

［設定のポイント］

Null インタフェースを設定し，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際，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。

19.3 オペレーション

19.3.1 運用コマンド一覧

Null インタフェース（IPv6）の運用コマンド一覧を次の表に示します。

表 19-2 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を表示します。
clear counters null-interface ※1	Null インタフェースの IPv4 および IPv6 統計情報をクリアします。
show ipv6 interface ※1	IPv6 インタフェースの状態を表示します。
clear counters ipv6 null-interface ※1	Null インタフェースの IPv6 統計情報をクリアします。
show ipv6 route ※2	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　9. IPv6・NDP・ICMPv6」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　13. IPv6 ルーティングプロトコル」を参照してください。

19.3.2 Null インタフェースの確認

本装置で Null インタフェースの機能を使用した場合の確認内容には次のものがあります。

(1) コンフィグレーション設定後の確認

(a) 経路情報の確認

show ipv6 route コマンドを実行し，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かどうかを確認してください。

図 19-1 NULL インタフェース経路情報表示

```
> show ipv6 route static
Total: 1 routes
Destination              Next Hop   Interface      Metric   Protocol  Age
3ffe:501:811:ffcc::/64   ----       null0          0/0      Static    16s
>
```

(2) 運用中の確認

(a) パケット廃棄数の確認

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

図 19-2 Null インタフェースパケット廃棄数表示例

```
> show ipv6 interface delete-packets null-interface
Interface Name:null0
Discard Packets(IPv6) :92(pkts)
>
```

20 ポリシーベースルーティング（IPv6）

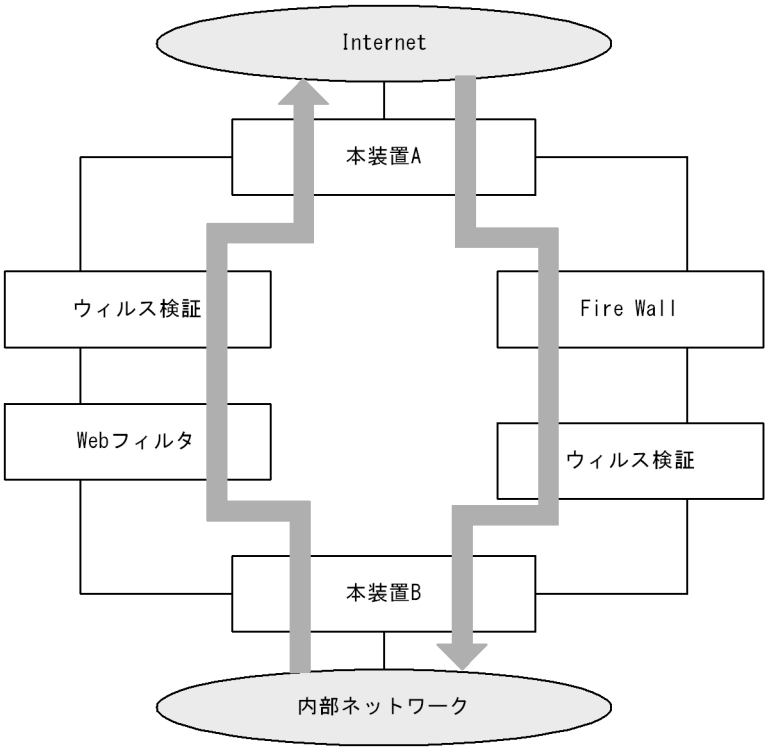
この章では，ポリシーベースルーティング（IPv6）の解説と操作方法について説明します。

20.1 解説

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や，コンフィグレーションコマンドで登録された経路情報に従わないで，ユーザが設定した宛先装置にパケットをレイヤ 3 中継する機能です。

ポリシーベースルーティングの構成例を次の図に示します。

図 20-1 ポリシーベースルーティングの構成例



本装置 A は，Internet から受信したすべてのパケットを Fire Wall およびウィルス検証などのセキュリティ装置に中継します。本装置 B は，内部ネットワークから受信したすべてのパケットを Web フィルタおよびウィルス検証などのフィルタ／セキュリティ装置に中継します。送受信するパケットで異なるセキュリティチェックを実施できます。また，負荷分散や認証などにも適用できます。

このようにポリシーベースルーティングは，経路情報に関係なく，ユーザが指定した経路に従って中継できます。

20.1.1 ポリシーベースルーティングの制御

本装置のポリシーベースルーティングはフィルタの一部機能として動作します。

受信側の VLAN インタフェースに設定したフィルタのフロー検出条件に一致した場合，同フィルタエントリに設定されているポリシーベースルーティングの設定内容に従って，パケットを中継します。

なお，ポリシーベースルーティングの対象となるのはレイヤ 3 中継のパケットだけです。また，送信先のインタフェースは IPv6 機能が有効である必要があります。

ポリシーベースルーティングの設定では，アクセスリストの動作に中継先の経路を指定してください。中継先の経路は，送信先インタフェースの VLAN ID およびネクストホップアドレスで設定します。

送信先インタフェースが障害などで中継できない場合の動作を**デフォルト動作**といいます。アクセスリス

トの動作に中継先の経路を指定した場合，デフォルト動作は廃棄です。

なお，送信先インタフェースが障害などから復旧して中継可能になった場合は，該当する中継先の経路から中継を再開します。

IPv6 ポリシーベースルーティングでは，ポリシーベースルーティンググループは動作しません。

20.1.2 ポリシーベースルーティング対象パケット

ポリシーベースルーティングの対象となるパケットについて次の表に示します。

表 20-1 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	アドレス種別	対象可否
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	×
	自宛 IP パケット	×※
	自発 IP パケット	×
IPv6 パケット以外		×

（凡例）○：対象　　×：対象外

注※

ポリシーベースルーティングがデフォルト動作に従っているときは廃棄します。その場合，該当するアクセスリストの統計情報にカウントされます。

20.1.3 ネクストホップに設定可能なアドレス種別

ポリシーベースルーティングのネクストホップに設定できる IPv6 アドレス種別を次の表に示します。

表 20-2 ポリシーベースルーティングのネクストホップに設定できる IPv6 アドレス種別

アドレス種別	設定可否
ユニキャスト（非リンクローカル） （受信インタフェース含む）	○※
ユニキャスト（リンクローカル） （受信インタフェース含む）	○
送信先インタフェースに設定された IPv6 アドレス	×
マルチキャスト	×

（凡例）○：設定できる　　×：設定できない

注※　送信先インタフェースに設定したアドレスと同一ネットワークのアドレスだけが設定できます。

20.1.4 ポリシーベースルーティングの注意事項

(1) ポリシーベースルーティングと uRPF 機能の併用について

ポリシーベースルーティングと uRPF 機能が同時に設定された場合，uRPF 機能が優先的に動作します。このため，ポリシーベースルーティング機能は動作しない状態になりますが，対象パケットがフィルタ条件で検出されるため，統計情報はカウントされます。

（2） ポリシーベースルーティングと sFlow 統計機能の併用について

sFlow 統計の対象パケットをポリシーベースルーティングの対象とした場合，sFlow 統計で採取する次の情報はポリシーベースルーティングによる中継先の経路情報ではなく，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

（3） ポリシーベースルーティングとフロー制御の併用について

ポリシーベースルーティングの対象となるパケットを QoS フローリストで検出した場合，ポリシーベースルーティングによる中継と QoS フローリストで設定したフロー制御がどちらも動作します。

（4） フロー検出拡張モードでのポリシーベースルーティング

advance access-list を VLAN インタフェースに適用した場合，そのフィルタエントリはレイヤ 2 中継およびレイヤ 3 中継の両方をフロー検出の対象にします。しかし，動作にポリシーベースルーティングを設定したフィルタエントリは，レイヤ 3 中継だけをフロー検出の対象にします。そのため，レイヤ 2 中継フレームはフロー検出の対象外となり，統計情報はカウントされません。

（5） ポリシーベースルーティングと MTU

ポリシーベースルーティングリスト情報を設定したアクセスリストを適用している受信側インタフェースの MTU が，ポリシーベースルーティングの送信先インタフェースの MTU より大きいと，ポリシーベースルーティングが動作しないことがあります。ポリシーベースルーティングを使用する場合は，受信側インタフェースの MTU を送信側インタフェースの MTU 以下の値で設定してください。

20.2 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

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 20-3 コンフィグレーションコマンド一覧

コマンド名	説明
advance access-group ※	VLAN インタフェースに対して Advance フィルタを適用し，Advance フィルタ機能を有効にします。
advance access-list ※	Advance 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 ※	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 traffic-filter ※	VLAN インタフェースに対して IPv6 フィルタを適用し，IPv6 フィルタ機能を有効にします。
permit ※	フィルタでのアクセス中継する条件を指定します。

注※
「コンフィグレーションコマンドレファレンス Vol.2　4. アクセスリスト」を参照してください。

20.2.2 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を設定する例を次に示します。

(1) アクセスリストの動作に中継先の経路を指定

IPv6 パケットをフロー検出条件として，IPv6 アドレスをネクストホップとするポリシーベースルーティングを設定する例を次に示します。

[設定のポイント]

アクセスリストを使用してポリシーベースルーティングを設定します。

[コマンドによる設定]

1. **(config)# ipv6 access-list WEB-FILTER**
   ipv6 access-list（WEB-FILTER）を作成します。本リストを作成すると，IPv6 パケットフィルタの動作モードに移行します。

2. **(config-ipv6-acl)# permit ipv6 any 2001:100::1/64 action policy interface vlan 200 next-hop 2001:1000::1**
   宛先 IP アドレス 2001:100::1/64 へのパケットをポリシーベースルーティングする IPv6 パケットフィルタを設定します。ネクストホップ IP アドレスは，2001:1000::1 を設定します。なお，送信先インタフェースに指定する VLAN200 の IPv6 機能は，事前に有効にしておく必要があります。

3. **(config-ipv6-acl)# exit**
   IPv6 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。

4. **(config)# interface vlan 20**
   VLAN20 のインタフェースモードに移行します。

5. **(config-if)# ipv6 traffic-filter WEB-FILTER in layer3-forwarding**
   受信側にレイヤ 3 中継を対象とするポリシーベースルーティングを設定した IPv6 フィルタを有効にします。

20.2.3 ポリシーベースルーティングでのエクストラネットの設定【OP-NPAR】

ネットワーク・パーティションのエクストラネットを実現するため，ポリシーベースルーティングを設定します。

VRF 間で通信できるように，二つの VRF を設定したあと，それぞれの VRF（VLAN）にポリシーベースルーティングを設定します。

（1）二つの VRF の設定

［設定のポイント］

二つの VRF を設定し，それぞれ異なる VLAN 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 vlan 20
   (config-if)# vrf forwarding 2
   (config-if)# ipv6 enable
   (config-if)# ipv6 address 2001:db8:1:20::1/64
   (config-if)# exit
   VRF 2 を設定し，VLAN 20 に VRF 2 と IPv6 アドレス 2001:db8:1:20::1，プレフィックス長 64 を設定します。

2. **(config)# vrf definition 3**
   (config-vrf)# exit
   (config)# interface vlan 30
   (config-if)# vrf forwarding 3
   (config-if)# ipv6 enable
   (config-if)# ipv6 address 2001:db8:1:30::1/64
   (config-if)# exit
   VRF 3 を設定し，VLAN 30 に VRF 3 と IPv6 アドレス 2001:db8:1:30::1，プレフィックス長 64 を設定します。

（2）VRF 間のポリシーベースルーティングの設定

［設定のポイント］

VRF の異なる VLAN 間でポリシーベースルーティングを設定します。ポリシーベースルーティングはアクセスリストを使用して設定します。

［コマンドによる設定］

1. **(config)# ipv6 access-list EXTRA_NET_POLICY_VLAN_20_TO_30**
   ipv6 access-list（EXTRA_NET_POLICY_VLAN_20_TO_30）を作成します。本リストを作成すると，IPv6 パケットフィルタの動作モードに移行します。

2. **(config-ipv6-acl)# permit ipv6 any 2001:db8:1:30::0/64 action policy interface vlan 30 next-hop 2001:db8:1:30::2**
   宛先 IP アドレス 2001:db8:1:30::0/64 の IPv6 パケットをポリシーベースルーティングする IPv6 パケットフィルタを設定します。ネクストホップ IP アドレスは，VLAN 30 の 2001:db8:1:30::2 を設定します。

3. **(config-ipv6-acl)# permit ipv6 any any**
   (config-ipv6-acl)# exit
   すべてのフレームを中継する IPv6 パケットフィルタを設定して，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 vlan 20**
   (config-if)# ipv6 traffic-filter EXTRA_NET_POLICY_VLAN_20_TO_30 in layer3-forwarding
   VLAN 20 の受信側にレイヤ 3 中継を対象とする ipv6 access-list（EXTRA_NET_POLICY_VLAN_20_TO_30）を有効にします。

5. **(config)# ipv6 access-list EXTRA_NET_POLICY_VLAN_30_TO_20**
   ipv6 access-list（EXTRA_NET_POLICY_VLAN_30_TO_20）を作成します。本リストを作成すると，IPv6 パケットフィルタの動作モードに移行します。

6. **(config-ipv6-acl)# permit ipv6 any 2001:db8:1:20::0/64 action policy interface vlan 20 next-hop 2001:db8:1:20::2**
   宛先 IP アドレス 2001:db8:1:20::0/64 の IPv6 パケットをポリシーベースルーティングする IPv6 パケットフィルタを設定します。ネクストホップ IP アドレスは，VLAN 20 の 2001:db8:1:20::2 を設定します。

7. **(config-ipv6-acl)# permit ipv6 any any**
   (config-ipv6-acl)# exit
   すべてのフレームを中継する IPv6 パケットフィルタを設定して，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 vlan 30**
   (config-if)# ipv6 traffic-filter EXTRA_NET_POLICY_VLAN_30_TO_20 in layer3-forwarding
   VLAN 30 の受信側にレイヤ 3 中継を対象とする ipv6 access-list（EXTRA_NET_POLICY_VLAN_30_TO_20）を有効にします。

20.3 オペレーション

20.3.1 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 20-4 運用コマンド一覧

コマンド名	説明
show access-filter ※	アクセスグループコマンド（ipv6 traffic-filter，advance access-group）で設定したアクセスリスト（ipv6 access-list，advance access-list）の統計情報を表示します。
clear access-filter ※	アクセスグループコマンド（ipv6 traffic-filter，advance access-group）で設定したアクセスリスト（ipv6 access-list，advance access-list）の統計情報をクリアします。

注※

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

20.3.2 ポリシーベースルーティングの確認

(1) アクセスリストの動作に中継先の経路を指定したポリシーベースルーティングの確認

show access-filter コマンドを実行して，アクセスリストの動作に中継先の経路を指定したポリシーベースルーティングの動作を確認できます。指定した VLAN インタフェースのフィルタに「IPv6 access-list: WEB-FILTER layer3-forwarding」および「action policy interface vlan 200 next-hop 2001: 1000::1」が表示されること，「matched packets」がカウントされていることを確認します。

図 20-2 show access-filter コマンドの実行結果

```
> show access-filter interface vlan 10 WEB-FILTER in
Date 2006/10/01 12:00:00 UTC
Using Interface:vlan 20 in
IPv6 access-list: WEB-FILTER layer3-forwarding
      remark "permit Web-Filter policy"
      permit ipv6 any 2001:100::1/64 action policy interface vlan 200 next-hop
2001: 1000::1
         matched packets       :            74699826
      implicitly denied packets:                2698
```

21 RA

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

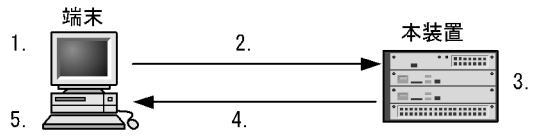
21.1 解説

21.1.1 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，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 21-1 RA による端末のアドレス設定



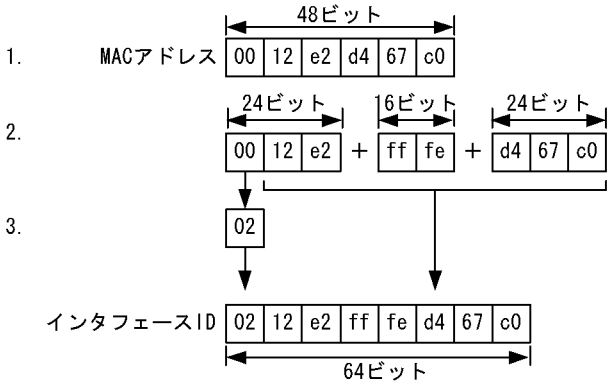
1. インタフェースIDを生成する。
2. プレフィックスを要求する。
3. RAで配布するプレフィックスを設定する。
4. プレフィックスを通知する。
5. 通知されたプレフィックスとインタフェースIDを組み合わせてアドレスを生成し，設定する。

21.1.2 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 Type 134 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，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 21-2 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する。
2. 中間に固定値"ff fe"を挿入する。
3. 最初の8ビットの下位2ビット目の値を反転する。

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 21-1 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 以外の方法（DHCPv6 など）による IPv6 アドレス設定を，RA 受信を契機に端末で自動的に行わせることを指定するフラグ。 このフラグの値に関係なく，RA によるアドレス設定は必ず行われます。通常は OFF 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 以外の方法（DHCPv6 など）による IPv6 アドレス以外の情報（DNS サーバなど）を，RA 受信を契機に端末で自動的に行わせることを指定するフラグ。通常は OFF 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。インタフェースの MTU よりも大きい値を通知することはできません。	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

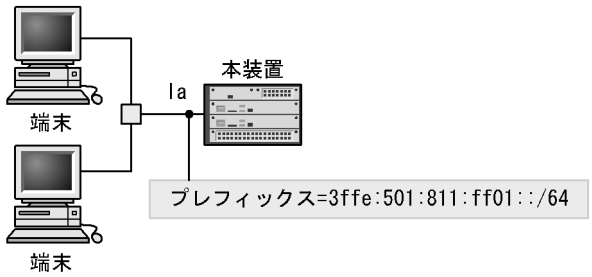
配布情報	説明	設定できる範囲	省略時の初期値
可到達時間（ReachableTime）	IPv6 では ICMPv6 によって隣接ノードの到達性を確認しますが，その確認結果の有効期間を端末に指定します。未指定または 0 を指定した場合は端末ごとに定められたデフォルト値が到達性確認結果の有効期間になります。なお，0 以外の値を指定した場合は，本装置の該当インタフェースで学習する NDP エントリの Reachable 状態遷移時間のベース値にも適用されます。	0 ～ 4294967295（ミリ秒）	0
再送時間（RetransTimer）	IPv6 では ICMPv6 によって隣接ノードの到達性を確認しますが，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みなしません。	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，各端末でデフォルトゲートウェイのリンク層アドレス解決を行います。	ON/OFF	ON
ルータ優先度（DefaultRouterPreference）	端末が複数ルータより 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

配布情報	説明	設定できる範囲	省略時の初期値
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ついているリンクローカルではない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，インタフェースにつ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，サイトローカルプレフィックス	インタフェースの非リンクローカルプレフィックス
自律設定有効フラグ（AutonomousFlag）	このオプションが OFF のプレフィックスは端末に付与されません。RA の試験運用以外のときは常時 ON 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 OFF のプレフィックスについては，端末での redirect メッセージの送信が抑制されます。RA の試験運用以外の時は常時 ON にしてください。	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）
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）

21.1.3 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，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 21-3　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行います。
   - Ia のプレフィックス = 3ffe:501:811:ff01::/64
2. Ia のプレフィックスを 3ffe:501:811:ff01::/64 から 3ffe:501:811:ff22::/64 に変更する設定を行います。
   - Ia で新しく広告するプレフィックス 3ffe:501:811:ff22::/64 の広告間隔を短く設定し，広告を開始します。
   - Ia で利用を停止するプレフィックス 3ffe:501:811: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行います。
   - Ia での 3ffe:501:811: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 3ffe:501:811:ff01::/64 の広告を停止します。

21.1.4　RA 送信の間隔時間の目安

RA 送信の最大間隔時間と最小間隔時間は，次の計算式を目安に指定してください。

（RA送信の最大間隔時間（秒）＋RA送信の最小間隔時間（秒））
　　≧（RAを送信するインタフェース数／100）

21.2 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。

21.2.1 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 21-2 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用いるホップリミットの初期値を指定します。
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 などの RA 以外の手段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	RA 以外の手段によって 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 を受けた端末が，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。

21.2.2 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 vlan 10**
   (config-if)# ipv6 nd suppress-ra
   インタフェース vlan 10 で RA 送信を抑止する設定を行います。

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

インタフェース vlan 10 に IPv6 アドレス 2001:db8:1:1::1/64 を設定します。

21.2.3 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 の配布情報の設定は，インタフェースモードで行います。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情報設定フラグ（OtherConfigFlag）の設定と，ipv6 nd router-preference コマンドによるルータ優先度（DefaultRouterPreference）の設定を行います。

[コマンドによる設定]

1. **(config)# interface vlan 10**
   (config-if)# ipv6 nd other-config-flag
   インタフェース vlan 10 から送信する RA に，アドレス以外情報設定フラグ（OtherConfigFlag）を設定します。端末は RA 受信を契機に，DHCPv6 など RA 以外の手段によって，アドレス情報以外の取得を行います。

2. **(config-if)# ipv6 nd router-preference high**
   インタフェース vlan 10 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。

21.2.4 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 vlan 10**
   (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。

21.3 オペレーション

21.3.1 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 21-3 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 ipv6 interface ※	IPv6 インタフェースの状態を表示します。
show netstat(netstat)(IPv6) ※	ネットワークの状態・統計を表示します。

注※

「運用コマンドレファレンス Vol.3　9. IPv6・NDP・ICMPv6」を参照してください。

21.3.2 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 21-4 RA を送信しているインタフェースの一覧

```
> show ipv6 routers global
Date 2006/03/14 12:00:00 UTC
#Index Name            Prefix
#2     VLAN0010        2001:db8:1:1::/64
#3     VLAN0020        2001:db8:1:2::/64
#4     VLAN0030        2001:db8:1:3::/64
```

21.3.3 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 21-5 RA を送信しているインタフェースの詳細情報

```
> show ipv6 routers interface vlan 10
Date 2006/03/14 12:00:00 UTC
Index: 3, Name: VLAN0010
Statistics:
RSin(wait): 5(0), RAout: 10, RAin(invalid): 0(0)
Intervals:
Advertise: 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

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

22 IPv6 DHCP リレー【OP-DH6R】

この章は，IPv6 DHCP リレーエージェントの解説，コンフィグレーションおよび確認方法について説明します。IPv6 DHCP リレーエージェントは，IPv6 DHCP サーバと IPv6 DHCP クライアントが異なるネットワークセグメントにある場合に，IPv6 DHCP パケットを中継する機能で，以降 IPv6 DHCP リレーと呼びます。

22.1 解説

22.1.1 概要

IPv6 DHCP リレーは，IPv6 DHCP サーバと IPv6 DHCP クライアントが異なるネットワークセグメントにある場合，IPv6 DHCP パケットを IPv6 DHCP サーバで受信できるように，IPv6 DHCP パケットをネットワークセグメント間で中継するための機能です。中継は，コンフィグレーションで設定した転送先（IPv6 DHCP サーバの IP アドレス，または IPv6 DHCP サーバのあるネットワークセグメントへ中継できる IPv6 DHCP リレーの IP アドレス）を，IPv6 DHCP パケットの宛先アドレスとして設定することで行います。

本装置による IPv6 DHCP リレーでは，次の二つをクライアント装置として利用できます。これらのクライアントを合わせて，IPv6 DHCP **クライアント**と呼びます。

- IPv6 DHCP-PD（Prefix Delegation）クライアント
- IPv6 アドレスを要求する IPv6 DHCP クライアント

同様に，IPv6 DHCP-PD サーバ，および IPv6 アドレスを配布する IPv6 DHCP サーバを合わせて，IPv6 DHCP **サーバ**と呼びます。

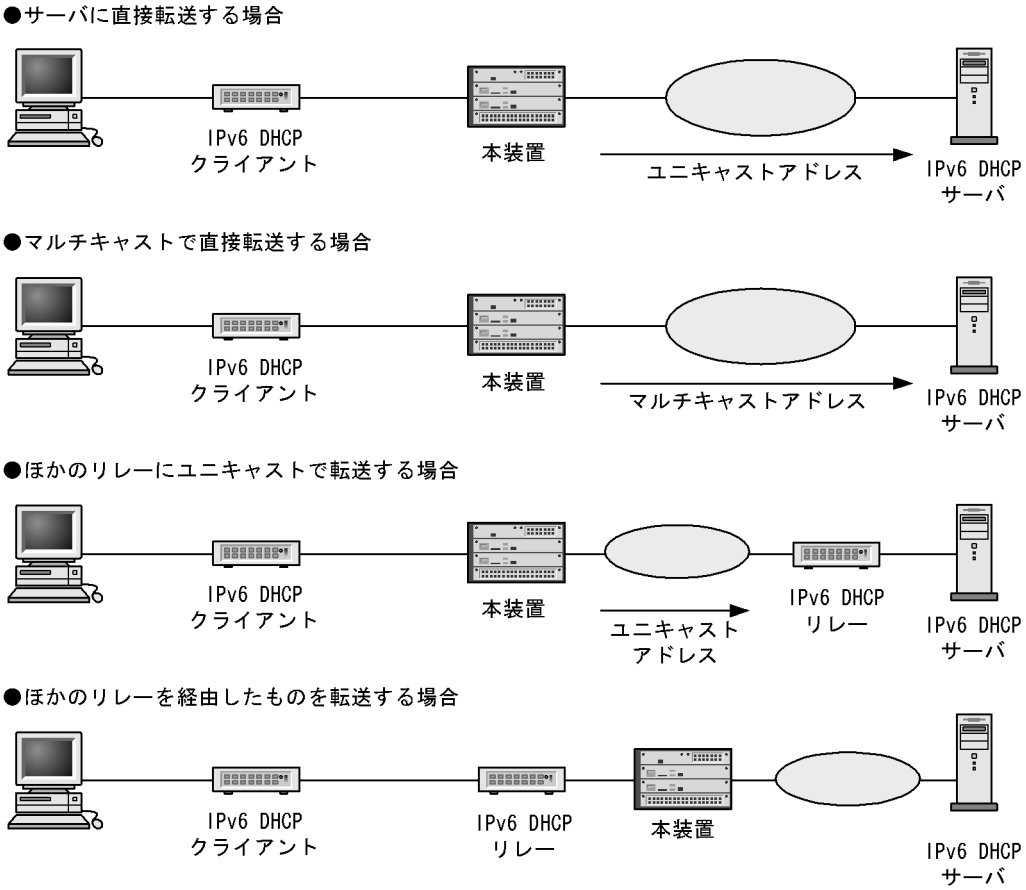
IPv6 DHCP クライアントは，IPv6 DHCP サーバが提供するサービスを利用するために，リンクローカルマルチキャスト通信を使用します。したがって，IPv6 DHCP サーバは IPv6 DHCP クライアントと同一ネットワークセグメントに設置されている必要があります。しかし，本装置の IPv6 DHCP リレーを使用すると，IPv6 DHCP クライアントが送信した IPv6 DHCP パケットを異なるネットワークセグメントに転送できるため，異なるネットワークセグメントにある IPv6 DHCP サーバが提供するサービスを利用できます。

本装置で IPv6 DHCP リレーを動作させるには，オプションライセンス OP-DH6R の設定が必要です。

なお，本章では，IPv6 DHCP-PD を例にした構成図を使っていますが，IPv6 アドレスを要求する IPv6 DHCP クライアントでも，配布プレフィックスに連動した経路自動生成や配布プレフィックス情報管理によるバインディング情報の表示などの一部の機能を除き，同様に動作します。

IPv6 DHCP リレーの接続構成を次の図に示します。

図 22-1 IPv6 DHCP リレーの接続構成



22.1.2 サポート仕様

本装置の IPv6 DHCP リレーのサポート仕様を次の表に示します。

表 22-1 IPv6 DHCP リレーのサポート仕様

項目	仕様	サポート
接続形態（クライアント側）	IPv6 DHCP クライアント直結	○
	IPv6 DHCP リレー経由	○
接続形態（サーバ側）	サーバ宛てユニキャストアドレス	○
	リレー宛てユニキャストアドレス	○
	全サーバ宛てマルチキャスト	○
	全サーバ／リレー宛てマルチキャスト	×
	ローカルアドレス対応	○
インタフェース	イーサネット	○
	リンクアグリゲーション	○
	マネージメントポート	×
機能	パケット長（UDP ペイロード）	○※
	IPv6 DHCP サーバとの同時動作	×

項目	仕様	サポート
	配布プレフィックスに対する経路自動生成	○
	uRPF と経路自動生成の同時動作	○
	冗長化構成での配布プレフィックス情報同期	○

（凡例） ○：サポートする　×：サポートしない
注※　977 オクテットまでが対象です。

22.1.3 中継動作

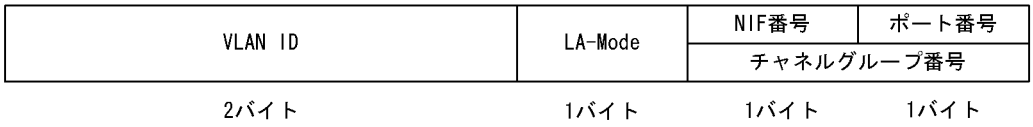
本装置の IPv6 DHCP リレーの中継動作について説明します。

(1) インタフェース ID の付与

IPv6 DHCP リレーは，IPv6 DHCP サーバに転送する IPv6 DHCP パケットにインタフェース ID を付与します。インタフェース ID は，IPv6 DHCP サーバからの応答パケットを IPv6 DHCP クライアントに送信するときに，送信先の判別に使用します。

Interface-ID Option に設定する Interface-id 情報の形式を次の図に示します。

図 22-2　Interface-id 情報の形式



LA-Mode：NIF番号/ポート番号指定＝0
　　チャネルグループ番号指定＝1

(2) 装置アドレス（loopback 0 インタフェース）を設定した場合の動作

IPv6 DHCP サーバに IPv6 DHCP パケットを送信するとき，本装置にコンフィグレーションコマンド interface loopback 0 および ipv6 address で装置アドレスが設定されている場合，装置アドレスを送信元アドレスとして送信します。

装置アドレスが設定されていない場合，IPv6 DHCP サーバ側の出力インタフェースのアドレスを送信元アドレスとして送信します。そのため，IPv6 DHCP サーバと IPv6 DHCP リレー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 IPv6 DHCP リレーが中継した IPv6 DHCP パケットの応答を受信できません。

装置アドレスが設定されている場合，IPv6 DHCP サーバは IPv6 DHCP 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 IPv6 DHCP パケットを受信できます。

22.1.4 配布プレフィックスに対する経路自動生成

本装置は，IPv6 DHCP クライアントのゲートウェイとして利用する場合，配布プレフィックスへの経路を自動で設定できます。IPv6 DHCP クライアントに経路情報の広告機能がない場合に，コンフィグレーションコマンド ipv6 dhcp relay static-route-setting で経路自動生成を有効にすると，本装置で配布プレフィックスに対する経路を自動的に追加します。

配布プレフィックスに対する経路自動生成で設定された経路のディスタンス値は，250 固定となります。

22.1.5 配布プレフィックスに関する情報

割り当てられたプレフィックスの管理情報（以降，リース情報と呼ぶ）は IPv6 DHCP リレー内で保持され，経路設定の情報として使用されます。また，リース情報は運用コマンド show ipv6 dhcp relay binding で表示して確認できます。

なお，配布プレフィックスの管理は IPv6 DHCP-PD に含まれる PD オプションの監視によって行われます。このため，本オプションを含まない IPv6 アドレス配布などのパケットでは，配布情報などの監視や経路自動生成のような機能は動作しません。

(1) リース情報の変更契機

リース情報が追加または削除される契機を次の表に示します。

表 22-2 リース情報が追加または削除される契機

変更内容	契機
追加	プレフィックス配布中継
削除	プレフィックス解放要求中継※1
	プレフィックスリース期間満了
	プレフィックスの割り当てが中継された，コンフィグレーションコマンド ipv6 dhcp relay destination で設定したコンフィグレーションの削除※2
	運用コマンド copy <file> running-config の実行※3
	運用コマンド clear ipv6 dhcp relay binding による削除

注※1
プレフィックスが配布されたときと異なるインタフェースからの解放要求を受信した場合は，リース情報は削除されません。なお，解放要求は中継されます。

注※2
該当の ipv6 dhcp relay destination コマンドの設定に従って中継したプレフィックスの，リース情報が削除されます。

注※3
すべてのリース情報が削除されます。

(2) リース情報の関連情報の引き継ぎ

リース情報の関連情報の引き継ぎ状況を次の表に示します。なお，リース情報を基に作成される関連情報には経路自動生成情報があります。

表 22-3 リース情報の関連情報の引き継ぎ状況

リース情報の関連情報	IPv6 リレー再起動	本装置の再起動※1	冗長化構成時の系切替
経路自動生成情報	○※2※3	×	○※4

（凡例）○：保証される　×：削除される

注※1
冗長化構成時，運用系と待機系がどちらも再起動した場合は，本装置の再起動と同等となります。

注※2

IPv6 DHCP リレープログラム再起動中に次のどちらかの操作をすると，リース情報が不正になるおそれがあります。不正となった場合，該当するリース情報は削除されます。
・コンフィグレーションコマンド ipv6 dhcp relay destination の設定を削除
・運用コマンド copy <file> running-config を実行

注※ 3
運用コマンド restart ipv6-dhcp relay で core-file パラメータを指定した場合，情報の引き継ぎは保証されません。

注※ 4
冗長化構成時，運用系または待機系の起動から 30 秒以内に系切替が発生した場合，リース情報は同期が取れた情報しか引き継がれません。また，運用系と待機系で IPv6 DHCP パケットの転送先が一致しない場合，新運用系に存在しない転送先で中継されたリース情報も削除されます。

(3) 冗長化構成での情報同期

冗長化構成時，IPv6 DHCP リレーではリース情報を運用系と待機系でそれぞれ保有して，常に同期をとります。運用系でリース情報を変更した場合，運用系は待機系に変更内容を通知して情報を同期します。このため，系切替が発生しても，新運用系は旧運用系と同等のリース情報を使用して運用を開始できます。

22.1.6 IPv6 DHCP リレー使用時の注意事項

IPv6 DHCP リレー使用時の注意事項について説明します。

(1) IPv6 DHCP サーバ機能との共存について

本装置では，IPv6 DHCP リレーと IPv6 DHCP サーバ機能を同時に使用できません。IPv6 DHCP リレーを使用する場合は，あらかじめ，コンフィグレーションコマンド no service ipv6 dhcp で IPv6 DHCP サーバ機能を未使用状態にしてください。

(2) IPv6 マルチキャスト機能との共存について

本装置で IPv6 マルチキャスト機能と IPv6 DHCP リレーを同時に使用する場合は，IPv6 DHCP リレーの転送先として各 IPv6 DHCP サーバのユニキャストアドレスを指定することを推奨します。転送先に全 IPv6 DHCP サーバ宛てのマルチキャストを使用する場合は，次の点に注意してください。

- 本装置の IPv6 DHCP パケットの転送先として全 IPv6 DHCP サーバ宛てのマルチキャストを指定して，かつ IPv6 マルチキャスト機能を同時に使用する場合は，本装置の対向のルータ側で次の設定が必要です。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。
  - 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 VLAN 内の最大値に設定し，IPv6 マルチキャストルーティングプロトコルでの中継代表ルータ（DR）になるようにしてください。
- 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 マルチキャスト機能を設定してください。

(3) IPv6 DHCP リレーパケット転送の注意事項

- 次の条件をどちらも満たす場合，IPv6 DHCP クライアントに応答パケットを正しく転送できません。
  - コンフィグレーションコマンド ipv6 dhcp relay destination を設定したインタフェースに，IPv6 グローバルアドレスが設定されていない。
  - 本装置が転送時に付ける Interface-ID が，IPv6 DHCP サーバからの応答パケットに含まれていない。
- 本装置で中継できるパケットは，IP パケットサイズが 1500 バイト以下で，かつフラグメント化されていないパケットです。

(4) ループバックアドレス使用時の注意事項

本装置と IPv6 DHCP サーバの間にルータが存在する状態で，IPv6 DHCP パケットの転送先として全 IPv6 DHCP サーバ宛てのマルチキャストを指定して，かつループバックインタフェースに IPv6 アドレスを設定する場合は，本装置の対向のルータ側で次の設定が必要です。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。

- 本装置のループバックインタフェースの IPv6 アドレスを直接接続サーバとして扱い，動作できるように設定してください。

22.2 コンフィグレーション

22.2.1 コンフィグレーションコマンド一覧

IPv6 DHCP リレー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 22-4 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	IPv6 DHCP パケットの転送先を指定します。
ipv6 dhcp relay hop-limit	IPv6 DHCP 転送パケットの最大ホップカウント数を指定します。
ipv6 dhcp relay static-route-setting	IPv6 DHCP リレーの経路情報オプションを指定することで，配布済みのプレフィックスを自動で本装置の経路情報テーブルに追加します。
service ipv6 dhcp relay	IPv6 DHCP リレーの使用／未使用を設定します。

22.2.2 コンフィグレーションの流れ

(1) IPv6 DHCP リレーを経由するユニキャスト送信の設定

1. あらかじめクライアントに対するインタフェースを設定します。
2. あらかじめ IPv6 DHCP サーバへ中継するインタフェースを設定します。
3. あらかじめ IPv6 DHCP サーバを未使用状態に設定します。
4. ipv6 dhcp relay destination コマンドで，転送先の IPv6 DHCP サーバのアドレスを設定します。
5. 最大ホップ数を設定します。
6. プレフィックス配布先への経路を自動生成する設定をします。

(2) IPv6 DHCP リレーを経由するマルチキャスト送信の設定

1. あらかじめクライアントに対するインタフェースを設定します。
2. あらかじめ IPv6 DHCP サーバへ中継するインタフェースを設定します。
3. あらかじめ IPv6 DHCP サーバを未使用状態に設定します。
4. ipv6 dhcp relay destination コマンドで，転送先の IPv6 DHCP サーバのインタフェースを設定します。
5. 最大ホップ数を設定します。
6. プレフィックス配布先への経路を自動生成する設定をします。

(3) 複数の IPv6 DHCP リレーを経由する設定

(a) 本装置 A 側の設定

1. あらかじめクライアントに対するインタフェースを設定します。
2. あらかじめ IPv6 DHCP サーバへ中継するインタフェースを設定します。
3. あらかじめ IPv6 DHCP サーバを未使用状態に設定します。
4. ipv6 dhcp relay destination コマンドで，転送先の本装置 B のアドレスを設定します。
5. 最大ホップ数を設定します。
6. プレフィックス配布先への経路を自動生成する設定をします。

(b) 本装置 B 側の設定

1. あらかじめクライアントに対するインタフェースを設定します。
2. あらかじめ IPv6 DHCP サーバへ中継するインタフェースを設定します。

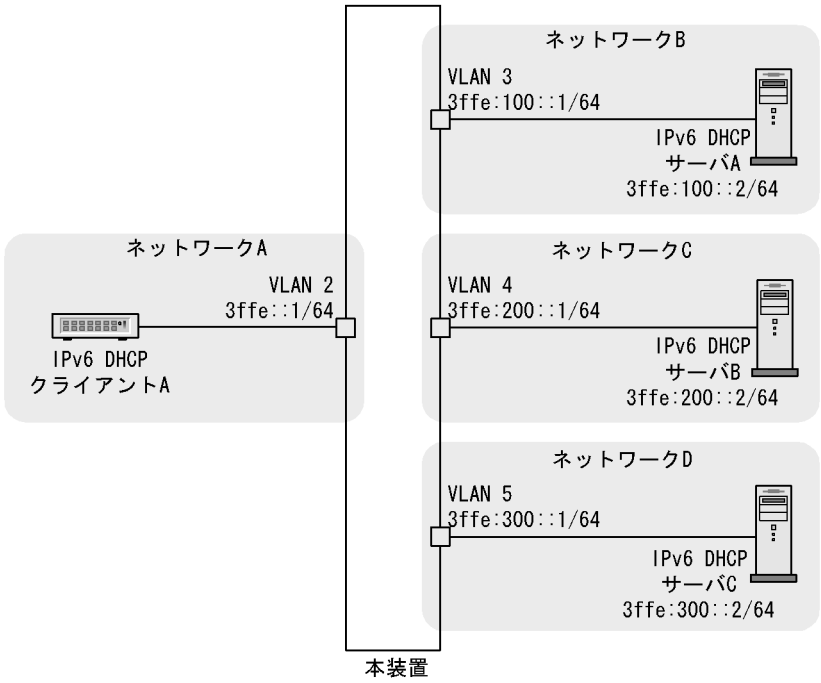
3. あらかじめ IPv6 DHCP サーバを未使用状態に設定します。
4. ipv6 dhcp relay destination コマンドで，転送先の IPv6 DHCP サーバのアドレスを設定します。
5. 最大ホップ数を設定します。

22.2.3 1 台の IPv6 DHCP リレーを経由するユニキャスト送信

[設定のポイント]

ipv6 dhcp relay destination コマンドで，転送先の IPv6 DHCP サーバの IPv6 アドレスを指定します。

図 22-3 1 台の IPv6 DHCP リレーを経由するユニキャスト送信時の構成



[コマンドによる設定]

1. **(config)# no service ipv6 dhcp**
   あらかじめ IPv6 DHCP サーバを未使用状態に設定します。

2. **(config)# service ipv6 dhcp relay**
   IPv6 DHCP リレーを使用状態に設定します。

3. **(config)# interface vlan 2**
   (config-if)# ipv6 dhcp relay destination 3ffe:100::2 3ffe:200::2 3ffe:300::2
   転送先として 3ffe:100::2，3ffe:200::2，3ffe:300::2 を設定します。

4. **(config-if)# ipv6 dhcp relay hop-limit 0**
   (config-if)# exit
   最大ホップ数を 0 に設定します。

5. **(config)# ipv6 dhcp relay static-route-setting**
   本装置に外部からプレフィックス配布先への経路自動設定機能を有効にします。ただし，対象プレ

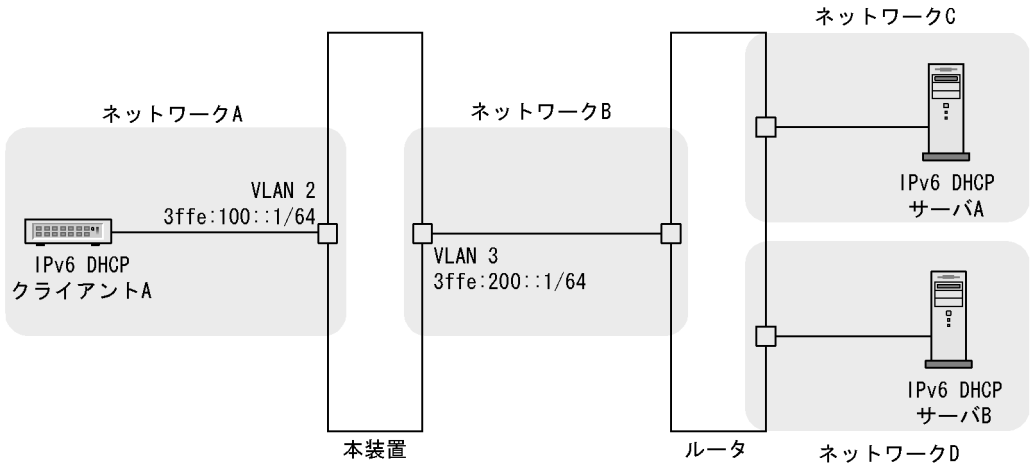
フィックスの配布が完了するまで経路は設定されません。

22.2.4 1 台の IPv6 DHCP リレーを経由するマルチキャスト送信

[設定のポイント]

ipv6 dhcp relay destination コマンドで，転送先の IPv6 DHCP サーバのインタフェースを指定します。

図 22-4 1 台の IPv6 DHCP リレーを経由するマルチキャスト送信時の構成



[コマンドによる設定]

1. **(config)# no service ipv6 dhcp**
   あらかじめ IPv6 DHCP サーバを未使用状態に設定します。

2. **(config)# service ipv6 dhcp relay**
   IPv6 DHCP リレーを使用状態に設定します。

3. **(config)# interface vlan 2**
   (config-if)# ipv6 dhcp relay destination all-servers vlan 3
   転送先として VLAN 3 を設定します。

4. **(config-if)# ipv6 dhcp relay hop-limit 0**
   (config-if)# exit
   最大ホップ数を 0 に設定します。

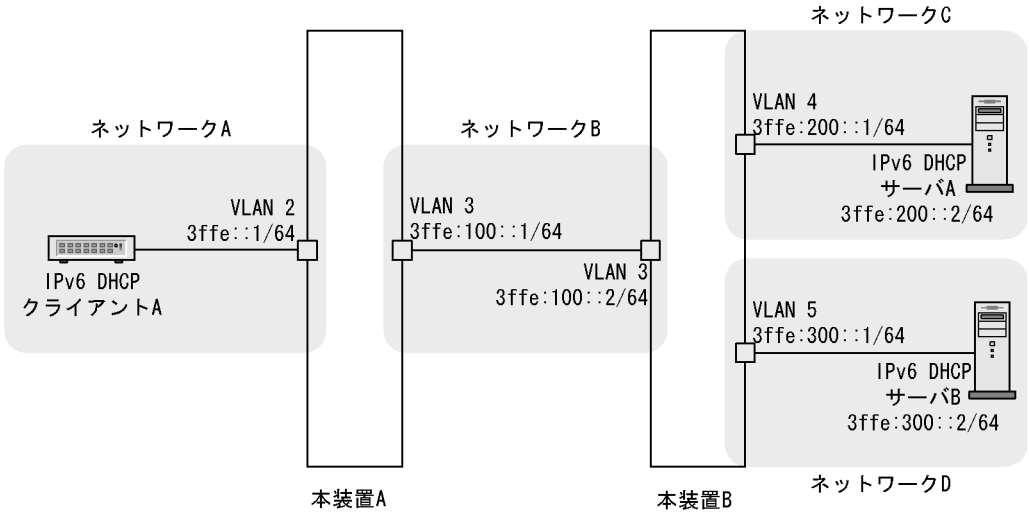
5. **(config)# ipv6 dhcp relay static-route-setting**
   本装置に外部からプレフィックス配布先への経路自動設定機能を有効にします。ただし，対象プレフィックスの配布が完了するまで経路は設定されません。

22.2.5 複数の IPv6 DHCP リレーを経由する

[設定のポイント]

ipv6 dhcp relay destination コマンドで，転送先の IPv6 アドレスを指定します。

図 22-5 複数の IPv6 DHCP リレーを経由する構成



[コマンドによる設定]

● 本装置 A 側の設定

1. **(config)# no service ipv6 dhcp**
   あらかじめ IPv6 DHCP サーバを未使用状態に設定します。

2. **(config)# service ipv6 dhcp relay**
   IPv6 DHCP リレーを使用状態に設定します。

3. **(config)# interface vlan 2**
   (config-if)# ipv6 dhcp relay destination 3ffe:100::2
   転送先として 3ffe:100::2 を設定します。

4. **(config-if)# ipv6 dhcp relay hop-limit 0**
   (config-if)# exit
   最大ホップ数を 0 に設定します。

5. **(config)# ipv6 dhcp relay static-route-setting**
   本装置に外部からプレフィックス配布先への経路自動設定機能を有効にします。ただし，対象プレフィックスの配布が完了するまで経路は設定されません。

● 本装置 B 側の設定

1. **(config)# no service ipv6 dhcp**
   あらかじめ IPv6 DHCP サーバを未使用状態に設定します。

2. **(config)# service ipv6 dhcp relay**
   IPv6 DHCP リレーを使用状態に設定します。

3. **(config)# interface vlan 3**
   (config-if)# ipv6 dhcp relay destination 3ffe:200::2 3ffe:300::2

転送先として 3ffe:200::2，3ffe:300::2 を設定します。

4. **(config-if)# ipv6 dhcp relay hop-limit 1**
   (config-if)# exit
   最大ホップ数を 1 に設定します。

22.3 オペレーション

22.3.1 運用コマンド一覧

IPv6 DHCP リレーの運用コマンド一覧を次の表に示します。

表 22-5 運用コマンド一覧

コマンド名	説明
show ipv6 dhcp traffic	IPv6 DHCP リレーの統計情報を表示します。
clear ipv6 dhcp traffic	IPv6 DHCP リレーの統計情報を削除します。
show ipv6 dhcp relay binding	IPv6 DHCP リレー上のリース情報を表示します。
clear ipv6 dhcp relay binding	IPv6 DHCP リレーのデータベースからリース情報を削除します。
restart ipv6-dhcp relay	IPv6 DHCP リレープログラムを再起動します。
dump protocols ipv6-dhcp relay	IPv6 DHCP リレープログラムで採取しているリレーのログをファイルへ出力します。

22.3.2 配布済みプレフィックスの確認

IPv6 DHCP サーバによってクライアントへ割り当てられたプレフィックスは，show ipv6 dhcp binding コマンドを実行して確認してください。リースを満了していないプレフィックスが表示されます。

図 22-6 配布済みプレフィックスの表示例

```
> show ipv6 dhcp relay binding
Date 2010/04/09 12:00:00 UTC
Total：2 prefixes
<Interface>      <Prefix>                                    <Lease expires>
vlan 10          3ffe:1234:5678::/48                         10/04/10 11:11:11
vlan 20          3ffe:aaaa:1234::/48                         10/04/10 12:12:12
>
```

22.3.3 配布プレフィックスの経路情報の確認

配布プレフィックスに対して経路自動生成を行った場合の経路情報は，show ipv6 route コマンドを実行して確認してください。経路情報にはスタティック経路として登録されます。

図 22-7 経路情報の表示例

```
> show ipv6 route -s static
Date 2010/04/09 12:00:00 UTC
Total: 5 routes
Destination                                 Next Hop
Interface      Metric   Protocol  Age
3ffe:abcd:1234::/64                         fe80::203:ffff:fe20:9982%VLAN0030
VLAN0030       0/0      Static     4m 33s , <Active Gateway Dhcp>
3ffe:aaaa:1234::/64                         fe80::203:ffff:fe20:9982%VLAN0020
VLAN0020       0/0      Static     4m 33s , <Active Gateway Dhcp>
3ffe:1234:5678::/64                         fe80::203:ffff:fe20:9982%VLAN0010
VLAN0010       0/0      Static     4m 33s , <Active Gateway Dhcp>
>
```

23 IPv6 DHCP サーバ機能

IPv6 DHCP サーバ機能は，IPv6 DHCP クライアントに対して，プレフィックス，DNS サーバアドレスなどの情報を動的に割り当てるための機能です。なお，IPv6 DHCP サーバが IPv6 DHCP クライアントへプレフィックスを割り当てることを Prefix Delegation と呼びます。
この章では，IPv6 DHCP サーバ機能の解説およびコンフィグレーションについて説明します。

23.1 解説

IPv6 DHCP **サーバ機能**は，IPv6 DHCP クライアントに対して，プレフィックス，DNS サーバアドレスなどの情報を動的に割り当てるための機能です。

23.1.1 サポート仕様

本装置の IPv6 DHCP サーバ機能のサポート仕様を次の表に示します。IPv6 DHCP サーバと IPv6 DHCP クライアント間の接続は，同一ネットワーク内直結で行います。

表 23-1 IPv6 DHCP サーバ機能のサポート仕様

項目	仕様
接続構成	IPv6 DHCP クライアント直接収容
	IPv6 DHCP リレー経由
IPv4/IPv6 デュアルスタック（IPv6 対応）	サポート

23.1.2 サポート DHCP オプション

本装置でサポートする IPv6 DHCP オプションを次の表に示します。

表 23-2 本装置で対応する IPv6 DHCP オプション

Option Code	オプション名称	意味	値の設定方法
1	Client Identifier	Client Identifier オプションは，クライアントとサーバの間で，クライアントを識別する DUID ※を運ぶのに使用されます。	△
2	Server Identifier	Server Identifier オプションは，クライアントとサーバの間で，サーバを識別している DUID を運ぶのに使用されます。	○
3	Identity Association option	Identity Association オプション（IA オプション）は，identity association，IA と関連するパラメータ，IA と関連するアドレスを運ぶのに使用されます。	－
4	Identity Association for Temporary Addresses option	Temporary Addresses(IA_TA) オプションのための Identity Association は，IA，IA と関連するパラメータ，IA と関連するアドレスを運ぶのに使用されます。RFC3041 で規定されているように，このオプション中のアドレスすべてが，一時的なアドレスとしてクライアントによって使用されます。	－
5	IA Address option	IA Address オプションは，IA と関連する IPv6 アドレスを指定するのに使用されます。IA Address オプションは，Identity Association オプションの Options フィールドにカプセル化されなければなりません。Options フィールドは，このアドレスに特有であるそれらのオプションをカプセル化します。	－
6	Option Request	Option Request オプションは，クライアントとサーバの間で，メッセージの中のオプションのリストを識別するのに使用されます。	○
7	Preference	Preference オプションは，クライアントによるサーバの選択に影響を及ぼすために，クライアントにサーバによって送られます。	○

Option Code	オプション名称	意味	値の設定方法
8	Elapsed Time option	クライアントがどれくらいの間 IPv6 DHCP メッセージ交換を完了しているかを示すために含めるオプション。経過時間は，メッセージ交換においてクライアントが最初のメッセージを送った時間から測られます。そして，メッセージ交換において最初のメッセージの elapsed-time フィールドは 0 に設定されます。例えば，プライマリ・サーバが合理的な時間で応答しなかったとき，経過時間オプションは，セカンダリ IPv6 DHCP サーバが要請に応じるのを許可します。	―
9	Relay Message option	Relay Message オプションは，Relay-forward または Relay-reply メッセージの中の IPv6 DHCP メッセージを運びます。	○
11	Authentication option	Authentication オプションは，IPv6 DHCP メッセージ識別と内容を認証するために，認証情報を運びます。	―
12	Server unicast option	サーバは，クライアントがメッセージをサーバにユニキャストすることが許されるということをクライアントに知らせるために，クライアントにこのオプションを送ります。	―
13	Status Code	このオプションは，それが現れる IPv6 DHCP メッセージまたはオプションに関連する状態表示の値を返します。	○
14	Rapid Commit	Rapid Commit オプションは，アドレス割り当てのための二つのメッセージ交換の使用を合図するのに使用されます。	○
15	User Class option	User Class オプションは，それが表すユーザまたはアプリケーションのタイプまたはカテゴリを識別するために，クライアントによって使用されます。	―
16	Vendor Class Option	このオプションは，クライアントが動いているハードウェアを製造したベンダーを識別するために，クライアントによって使用されます。このオプションのデータ領域に含まれる情報は，ハードウェア構成の詳細を識別する一つ以上の不明解なフィールドに含まれます。	―
17	Vendor-specific Information option	このオプションは，vendor-specific 情報を交換するために，クライアントとサーバによって使用されます。	―
18	Interface-Id Option	リレーエージェントは，クライアントメッセージが受け取られたインタフェースを識別するために Interface-id オプションを送ることができます。リレーエージェントが Interface-id オプションを持つ Relay-reply メッセージを受け取った場合は，リレーエージェントはそのオプションによって識別されるインタフェースを通じて，クライアントにメッセージを転送します。	―
19	Reconfigure Message option	サーバは，クライアントが Renew メッセージか Information-request メッセージで応じるかどうかクライアントに示すために，Reconfigure Message に Reconfigure Message オプションを含めます。	―
20	Reconfigure Nonce option	サーバがセキュリティを Reconfigure Message に提供するために reconfigure nonce を使う場合に，サーバは各クライアントのために nonce 値を保持します。 サーバは，最初にクライアントに nonce 値を知らせて，それからクライアントに送るあらゆる Reconfigure Message に nonce 値を含めます。	―
21	SIP Servers Domain Name List	そのクライアントが使用する SIP の outbound のプロキシサーバのドメインネーム。	◎
22	SIP Servers IPv6 Address List	このオプションは，クライアントに利用可能な SIP の outbound のプロキシサーバを示す IPv6 アドレスのリストを指定する。	◎
23	DNS Recursive Name Server	サーバが DNS サーバのアドレスをクライアントにリスト形式で渡す場合に指定するオプション。	◎
24	Domain Search List	クライアントはこのオプションを受け取ると，DNS によってホスト名の解決を行うときにこれに与えたドメインリストから検索します。このオプションはホスト名解決以外には使用すべきではありません。	◎

Option Code	オプション名称	意味	値の設定方法
25	Identify Association for Prefix Delegation Option	Prefix Delegation アイデンティティ関連を配送するために使用するオプション。	◎
26	IA_PD Prefix Option	IPv6 アドレスプレフィックスが IA_ID との関連づけを指定します。	◎
31	Network Time Protocol (NTP) Servers	サーバがクライアントに対して NTP サーバのアドレスリストを通知するときに使用します。	◎

（凡例）
◎：コンフィグレーションで設定する　○：自動的に設定する
△：クライアントが設定した値を使用する　－：未サポート（無視する）
注※　DHCP Unique Identifier の略。

23.1.3 配布プレフィックスの経路情報

本装置は，クライアントのゲートウェイとして利用する場合に，配布したプレフィックスへの経路設定として次に示す 2 とおりの方法を提供します。

- クライアントが経路情報の広告機能を保有しない場合
  本装置の IPv6 DHCP サーバコンフィグレーションの配布プレフィックスへの経路自動設定機能を有効にすることで，配布先への経路が本装置に自動的に追加されます。
  また，このとき設定された経路のディスタンス値は 250 固定となります。
- クライアントが経路情報の広告機能を保有する場合
  この場合，本装置～クライアント間で経路情報を交換し，経路を自動生成するため，本装置の IPv6 DHCP サーバコンフィグレーションの配布プレフィックスへの経路自動設定機能は無効にします。

23.1.4 IPv6 DHCP サーバ機能使用時の注意事項

IPv6 DHCP サーバ機能使用時の注意事項について説明します。

（1） DUID(DHCP Unique Identifier) について

本装置は IPv6 DHCP で装置を区別するために使用するように規定される DUID を IPv6 DHCP サーバ機能が初めて導入されたときに生成します。生成した DUID は，装置内メモリに静的に保存されます。
DUID の値は，show ipv6 dhcp server statistics コマンドで表示される Server DUID の値で確認できます。本装置を交換した場合は，それまでの DUID の値と異なります。DUID をそれまでの DUID の値で使用したい場合は，set ipv6-dhcp server duid コマンドで再設定してください。

（2） 本装置再起動時の動作

本装置では，次に示す事象が発生した場合に制限事項があります。各状態の情報の保有性を次の表に示します。

表 23-3　各状態の情報の保有性

プレフィックスに関する保有情報	サーバ機能再起動		本装置再起動
	restart ipv6-dhcpserver コマンド実行	サーバ障害	
クライアントへの経路情報	○	△	×

プレフィックスに関する保有情報	サーバ機能再起動		本装置再起動
	restart ipv6-dhcpserver コマンド実行	サーバ障害	
クライアントへの配布情報	○	△	×

（凡例）
○：保証される。
△：保証される。ただし，一部直前に配布したものについては反映されない可能性があります。
×：保証されない（各状態の情報が初期化される）。

（3） 配布プレフィックスに対する経路自動設定機能使用時の注意

本装置では，クライアントに経路情報の広告機能がない場合など，特定条件下で経路情報の広告機能を使用せずに自動で経路情報を設定する機能がありますが，マルチパスや動的に経路が変更されるようなケースでは経路情報の広告機能を使用してください。

また，クライアントと本装置の間にほかの装置が存在する場合も，その装置に対する経路情報の広告は行われないため，経路情報の広告機能を使用してください。

（4） IPv6 DHCP サーバと IPv6 PIM を同一インタフェースで使用する場合の注意事項

IPv6 PIM を有効にしたインタフェースで IPv6 DHCP サーバを使用する場合，IPv6 DHCP リレーからの DHCP 制御パケットは，全サーバ宛てマルチキャスト（FF05::1:3）ではなく，本装置のグローバルユニキャストアドレス宛てに送信してください。

23.2 コンフィグレーション

23.2.1 コンフィグレーションコマンド一覧

IPv6 DHCP サーバ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 23-4 コンフィグレーションコマンド一覧

コマンド名	説明
dns-server	IPv6 DHCP サーバの DNS サーバアドレス情報を設定します。IPv6 DHCP クライアントからの要求に応じて DNS サーバアドレス情報を配布できます。
domain-name	IPv6 DHCP サーバのドメインネーム情報を設定します。IPv6 DHCP クライアントからの要求に応じてドメインネーム情報を配布できます。
ipv6 dhcp pool	IPv6 DHCP アドレスプールの情報を設定します。「23.2.3 クライアントごとの固定プレフィックスの設定」のように，コンフィグ DHCP モードへ移行することができ，固定プレフィックスの設定などを行えます。
ipv6 dhcp server	プレフィックスを配布するための設定をします。「23.2.5 クライアントにプレフィックスを配布するための優先順位の設定」では，プレフィックスの優先を配布するためにサーバ優先順位を設定に使用しています。
ipv6 dhcp static-route-setting	IPv6 DHCP サーバによってプレフィックスを配布したクライアントへの経路情報を，本装置の経路情報テーブル上に自動で追加します。「23.2.6 プレフィックスを配布したクライアントへの経路自動生成の設定」の設定例のように使用します。
ipv6 local pool	動的に割り当てるプレフィックスを設定します。「23.2.4 動的プレフィックス提供範囲の設定」の設定例のように使用します。
prefix-delegation	指定されたプール内で使用する固定 IPv6 プレフィックスおよび IAID, lifetime を設定します。「23.2.3 クライアントごとの固定プレフィックスの設定」の設定例のように使用します。
prefix-delegation pool	ローカルプール設定で指定された IPv6 プレフィックス範囲に対して，IAID および lifetime を設定します。「23.2.4 動的プレフィックス提供範囲の設定」の設定例のように使用します。
service ipv6 dhcp	IPv6 DHCP サーバの使用／未使用を設定します。
sip-domain-name	IPv6 DHCP サーバの SIP ドメインネーム情報を設定します。IPv6 DHCP クライアントからの要求に応じて SIP ドメインネーム情報を配布できます。
sip-server	IPv6 DHCP サーバの SIP サーバ IPv6 アドレス情報を設定します。IPv6 DHCP クライアントからの要求に応じて SIP サーバ IPv6 アドレス情報を配布できます。
sntp-server	IPv6 DHCP サーバの SNTP サーバアドレス情報を設定します。IPv6 DHCP クライアントからの要求に応じて SNTP サーバアドレス情報を配布できます。

23.2.2 IPv6 DHCP サーバのコンフィグレーションの流れ

(1) クライアントに固定プレフィックスを配布する設定

1. あらかじめ interface コマンドで VLAN インタフェースを設定する。
2. あらかじめ ipv6 address コマンドで IPv6 アドレスを設定する。
3. あらかじめ ipv6 enable コマンドで IPv6 アドレスを自動生成させる。
4. クライアントごとに固定プレフィックスを設定する。
5. クライアントにプレフィックスを配布する設定をする。

6. プレフィックス配布先であるクライアントの経路を自動生成する設定をする。

(2) クライアントに動的にプレフィックスを配布する設定

1. あらかじめ interface コマンドで VLAN インタフェースを設定する。
2. あらかじめ ipv6 address コマンドで IPv6 アドレスを設定する。
3. あらかじめ ipv6 enable コマンドで IPv6 アドレスを自動生成させる。
4. 動的プレフィックスの提供範囲を設定する。
5. クライアントにプレフィックスを配布する設定をする。
6. プレフィックス配布先であるクライアントの経路を自動生成する設定をする。

(3) クライアントにオプション情報だけを配布する設定

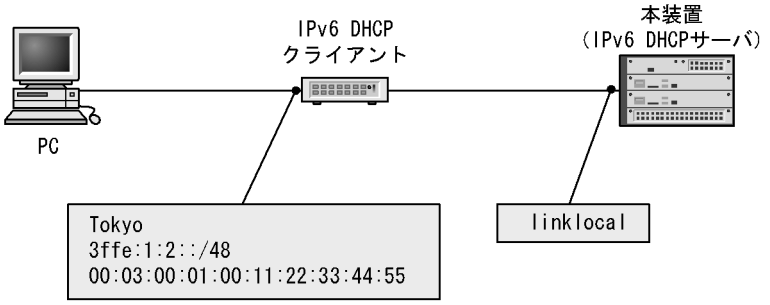
1. あらかじめ interface コマンドで VLAN インタフェースを設定する。
2. あらかじめ ipv6 address コマンドで IPv6 アドレスを設定する。
3. あらかじめ ipv6 enable コマンドで IPv6 アドレスを自動生成させる。
4. クライアントにオプションを配布する設定をする。

23.2.3 クライアントごとの固定プレフィックスの設定

[設定のポイント]

IPv6 DHCP プール情報を設定し，DHCP モードでプレフィックスとクライアント ID（DUID）を設定します。

図 23-1 クライアントごとに固定プレフィックスを指定する構成



[コマンドによる設定]

1. **(config)# ipv6 dhcp pool Group1**
   IPv6 DHCP プール情報を設定します。コンフィグ DHCP モードへ移行します。

2. **(config-dhcp)# prefix-delegation 3ffe:1:2::/48 00:03:00:01:00:11:22:33:44:55**
   (config-dhcp)# exit
   プレフィックスとクライアント ID（DUID）を設定します。
   複数のクライアントに固定プレフィックスを配布する場合は，繰り返しプレフィックスとクライアント ID（DUID）を設定します。

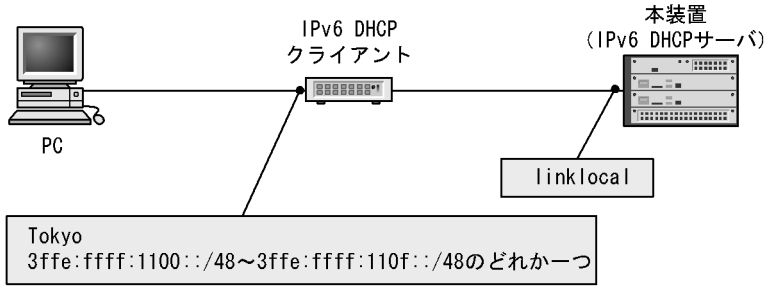
3. **(config)# interface vlan 10**
   (config-if)# ipv6 dhcp server Group1
   (config-if)# exit
   VLAN インタフェースにプール名称を設定します。

23.2.4 動的プレフィックス提供範囲の設定

[設定のポイント]

IPv6 DHCP プール情報を設定した上で，動的に割り当てするローカルプールを設定し，DHCP モードで動的に配布するプレフィックスの範囲を指定します。

図 23-2 動的にプレフィックスを割り当てる構成



[コマンドによる設定]

1. **(config)# ipv6 local pool Group1Local 3ffe:ffff:1100::/44 48**
   動的に配布するプレフィックスを設定します。

2. **(config)# ipv6 dhcp pool Group1**
   IPv6 DHCP プール情報を設定します。

3. **(config-dhcp)# prefix-delegation pool Group1Local**
   (config-dhcp)# exit
   ローカルプール設定情報で設定されたローカルプール名称を設定します。

4. **(config)# interface vlan 10**
   (config-if)# ipv6 dhcp server Group1
   (config-if)# exit
   VLAN インタフェースにプール名称を設定します。

23.2.5 クライアントにプレフィックスを配布するための優先順位の設定

[設定のポイント]

プレフィックスを配布するためにサーバの優先順位を設定します。

[コマンドによる設定]

1. **(config)# ipv6 local pool Group1Local 3ffe:ffff:1100::/44 48**
   (config)# ipv6 dhcp pool Group1
   (config-dhcp)# prefix-delegation pool Group1Local
   (config-dhcp)# exit
   あらかじめ IPv6 DHCP プール情報を設定しておきます。プレフィックスの設定については，動的に設定した例です。

2. **(config)# interface vlan 10**
   (config-if)# ipv6 dhcp server Group1 preference 255
   プレフィックスを配布するためにサーバの優先順位に 255 を設定する例です。

23.2.6 プレフィックスを配布したクライアントへの経路自動生成の設定

[設定のポイント]

プレフィックスを配布したクライアントの経路を自動生成するための設定をします。

[コマンドによる設定]

1. **(config)# ipv6 local pool Group1Local 3ffe:ffff:1100::/44 48**
   (config)# ipv6 dhcp pool Group1
   (config-dhcp)# prefix-delegation pool Group1Local
   (config-dhcp)# exit
   あらかじめ IPv6 DHCP プール情報を設定しておきます。プレフィックスの設定については，動的に設定した例です。

2. **(config)# interface vlan 10**
   (config-if)# ipv6 dhcp server Group1
   (config-if)# exit
   VLAN インタフェースにプール名称を設定します。

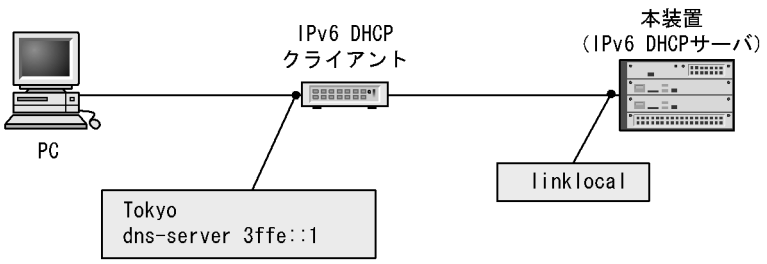
3. **(config)# ipv6 dhcp static-route-setting**
   本装置に外部からプレフィックス配布先への自動経路設定機能を有効にします。ただし，対象プレフィックスの配布が完了するまで経路は設定されません。

23.2.7 クライアントにオプション情報だけを配布する設定

[設定のポイント]

プレフィックスを必要としないクライアントに，DNS サーバオプションなどのオプション情報だけを配布するための設定をします。

図 23-3 クライアントにオプション情報を配布する構成



[コマンドによる設定]

1. **(config)# ipv6 local pool Group1Local 3ffe:ffff:1100::/44 48**
   動的に配布するプレフィックスを設定します。

2. **(config)# ipv6 dhcp pool Group1**
   IPv6 DHCP プール情報を設定します。
   コンフィグ DHCP モードへ移行します。

3. **(config-dhcp)# prefix-delegation pool Group1Local**
   ローカルプール設定情報で設定されたローカルプール名称を設定します。

4. **(config-dhcp)# dns-server 3ffe::1**
   (config-dhcp)# exit
   DNS サーバオプションを設定します。

5. **(config)# interface vlan 10**
   (config-if)# ipv6 dhcp server Group1
   (config-if)# exit
   VLAN インタフェースにプール名称を設定します。

23.3 オペレーション

23.3.1 運用コマンド一覧

IPv6 DHCP サーバの運用コマンド一覧を次の表に示します。

表 23-5 運用コマンド一覧

コマンド名	説明
show ipv6 dhcp binding	IPv6 DHCP サーバ上の結合情報を表示します。
clear ipv6 dhcp binding	IPv6 DHCP サーバ上の結合情報を削除します。削除したプレフィックスを使用していた IPv6 DHCP クライアントは通信ができなくなりますので注意してください。
show ipv6 dhcp server statistics	IPv6 DHCP サーバの統計情報を表示します。
clear ipv6 dhcp server statistics	IPv6 DHCP サーバの統計情報をリセットします。
restart ipv6-dhcp server	IPv6 DHCP サーバデーモンプロセスを再起動します。
dump protocols ipv6-dhcp server	IPv6 DHCP サーバで採取しているサーバのログ，およびパケットの送受信ログをファイルへ出力します。
ipv6-dhcp server monitor	IPv6 DHCP サーバで送受信するパケットの送受信ログの採取を開始します。
no ipv6-dhcp server monitor	IPv6 DHCP サーバでのパケットの送受信ログの採取を停止します。
set ipv6-dhcp server duid	IPv6 DHCP サーバ DUID ファイルを設定します。
show ipv6-dhcp server duid	IPv6 DHCP サーバ DUID ファイルを表示します。
erase ipv6-dhcp server duid	IPv6 DHCP サーバ DUID ファイルを削除します。

23.3.2 割り当て可能なプレフィックス数の確認

クライアントに割り当て可能なプレフィックスは，show ipv6 dhcp server statistics コマンドの実行結果「prefix pools」で示されます。この数が配布したいクライアント装置数より多いことを確認してください。

図 23-4 show ipv6 dhcp server statistics コマンドの実行結果

```
> show ipv6 dhcp server statistics
Date 2008/10/15 12:00:00 UTC
   < DHCP Server use statistics >
     prefix pools           :20
     automatic prefixes     :50
     manual prefixes        :4
     expired prefixes       :3
     over pools requests    :0
     discard packets        :0
   < Receive Packets >
     SOLICIT                :54
     REQUEST                :54
     RENEW                  :54
     REBIND                 :0
     INFORMATION-REQUEST    :0
     CONFIRM                :0
     RELEASE                :0
     DECLINE                :0
     RELAY-FORW             :0
   < Send Packets >
     ADVERTISE              :54
     REPLY                  :108
     RELAY-REPL             :0
   < Server DUID >
     00:01:00:01:3e:00:2e:22:11:22:33:44:55:01
>
```

23.3.3 配布したプレフィックスの確認

実際に配布したプレフィックスは，show ipv6 dhcp binding コマンドを実行して確認してください。リース満了していないプレフィックスアドレスが表示されます。

図 23-5 show ipv6 dhcp binding コマンドの実行結果

```
> show ipv6 dhcp binding
Date 2008/10/15 12:00:00 UTC
Total: 2 prefixes
<Prefix>                <Lease expiration>   <Type>
3ffe:1:2::/48           08/10/16 11:15:00    Manual
3ffe:ffff:1101::/48     08/10/16 11:29:00    Automatic
>
```

24 IPv6 ルーティングプロトコル概要

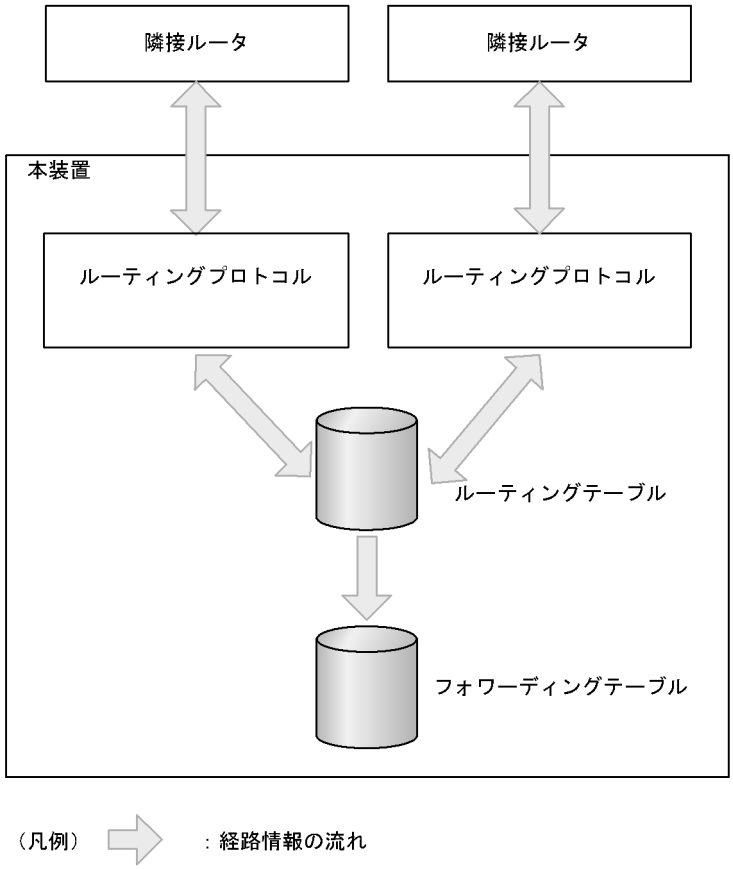
この章では，IPv6 のルーティングプロトコルの概要について説明します。

24.1 IPv6 ルーティング共通の解説

24.1.1 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 24-1 ルーティングの概要



24.1.2 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 RIPng，OSPFv3，BGP4+ をサポートしています。

24.1.3 経路情報

本装置が取り扱う経路情報（ルーティング対象とするアドレスの種類）を次の表に示します。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 24-1 経路情報

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	（プレフィックス：fe80::% インタフェース名称 /64）
	マルチキャストアドレス	（プレフィックス：ff00::/8）
	IPv4 予約アドレス	（プレフィックス：::/8）

（凡例）－：特になし

24.1.4 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の表に示します。

表 24-2 ルーティングプロトコルごとの適用範囲

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

24.1.5 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RIPng）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 24-3　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+ の外部ピア学習経路	20
OSPFv3 の AS 内経路	110
OSPFv3 の AS 外経路	110
RIPng 経路	120
集約経路	130
BGP4+ の内部ピア学習経路	200
BGP4+ のメンバー 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

(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，「30　経路フィルタリング（IPv6）」を参照してください。

(a) RIPng での経路広告

RIPng はひとつのルーティングプロトコルとして動作します。

(b) OSPFv3 での経路広告

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 OSPFv3 ドメインに由来する複数の OSPFv3 AS 内経路，または OSPFv3 AS 外経路が存在することがあります。OSPFv3 の経路間でディスタンス値が同じ場合は，ドメイン番号の小さい経路を優先します。OSPFv3 の 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 OSPFv3 ドメイン間で互いに経路を広告することはありません。OSPFv3 AS 内経路や OSPFv3 AS 外経路をほかの OSPFv3 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+ 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 BGP4 経路はほかの AS に広告されます。この場合，BGP4+ 以外のルーティングプロトコルで BGP4+ 経路と同一宛先経路が存在しても BGP4+ で選択された最適な 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。

24.1.6 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・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 取得に時間がかかる場合があります。

24.2 IPv6 ルーティング共通のオペレーション

24.2.1 運用コマンド一覧

IPv6 ルーティングプロトコル共通の運用コマンド一覧を次の表に示します。

表 24-4 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 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 processes cpu unicast ※2	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 ※2	ユニキャストルーティングプログラムを再起動します。
debug protocols unicast ※2	ユニキャストルーティングプログラムが出力するイベントログ情報の運用メッセージ表示を開始します。
no debug protocols unicast ※2	ユニキャストルーティングプログラムが出力するイベントログ情報の運用メッセージ表示を停止します。
dump protocols unicast ※2	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 ※2	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。
show ipv6 interface ※3	IPv6 インタフェースの状態を表示します。
show netstat(netstat)(IPv6) ※3	ネットワークの状態・統計を表示します。
ping ipv6 ※3	指定 IPv6 アドレスの装置へ試験パケットを送信し，通信可能であるかどうかを判定します。
traceroute ipv6 ※3	宛先ホストまで IPv6 データグラムが通ったルートを表示します。

注※ 1

「運用コマンドレファレンス Vol.1　9. ソフトウェアバージョンと装置状態の確認」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　8. IPv4・IPv6 ルーティングプロトコル共通」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　9. IPv6・NDP・ICMPv6」を参照してください。

24.2.2 宛先アドレスへの経路確認

本装置で 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。

図 24-2 show ipv6 route コマンドの実行結果

```
> show ipv6 route
Date 2006/03/14 12:00:00 UTC
Total: 11 routes
Destination                                    Next Hop
      Interface      Metric   Protocol  Age
4000:110:1:1::/64                              4000:110:1:1::1
      VLAN0010       0/0      Connected 22m 53s
cafe:1001::/64                                 4000:110:1:1::200            …1
      VLAN0010       0/0      Static    41s
      :
      :
>
```

1. 宛先アドレスに対する経路が存在するかどうか確認してください。

24.3 ネットワーク設計の考え方

この節では，IPv6 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。

24.3.1 アドレス設計

IPv6 アドレス割り当て時には次のような考え方に従うと，注意しなければならない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。

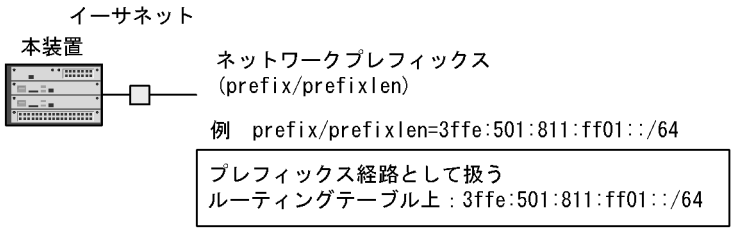
- NLA や SLA を，ネットワークトポロジの階層構造に従って分割します。

24.3.2 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 24-3 直結経路の取り扱い（ブロードキャスト型の場合）



24.4　ロードバランスの解説

24.4.1　ロードバランス概説

ロードバランスは，マルチパス接続によって 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。ロードバランスの詳細については，「7.4.1　ロードバランスの概要」を参照してください。

24.4.2　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 24-5　IPv6 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可能な最大マルチパス数	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（IPv6） • OSPFv3 • 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（IPv6）：6 • OSPFv3：4 • 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 24-6　IPv6 ロードバランス仕様

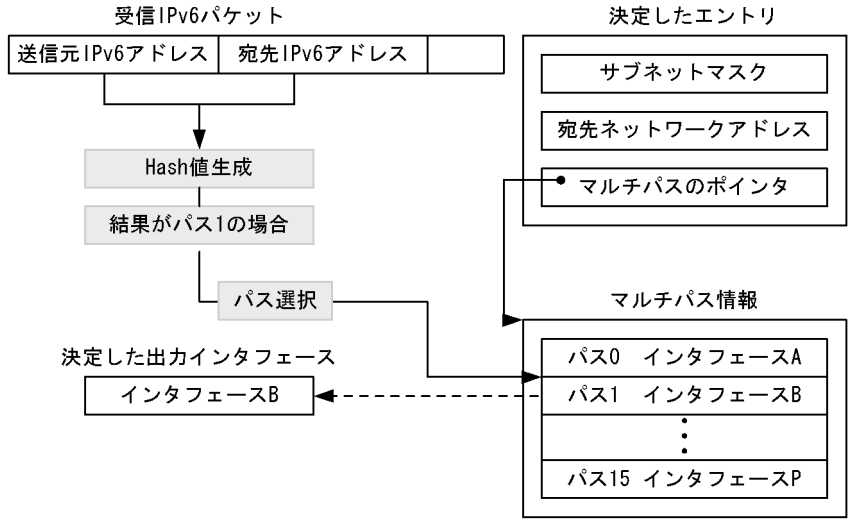
項目	仕様	備考
マルチパスの振り分け方法	宛先 IPv6 アドレスと送信元 IPv6 アドレスから 16 パスに振り分ける値（Hash 値）を算出し，決定した出力パスに振り分けます。 宛先 IPv6 アドレスと送信元 IPv6 アドレスが同一のパケットは，同一出力パスを選択します。これによって，送信の順序性を保証します。	－
ルーティングテーブル内のマルチパス情報	ルーティングテーブルに設定する各出力インタフェースの Hash 値の割り当て比率は，ほぼ均等になります。	「24.4.4　ロードバランス使用時の注意事項」の 1 を参照
各パスの重み付け	できません。	
出力帯域を超えたパケットの処理	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パケットを廃棄します。	

（凡例）　－：該当しない

24.4.3 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 IPv6 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を決定するには，受信した IPv6 パケットの送信元 IPv6 アドレス（Source IPv6 Address）と宛先 IPv6 アドレス（Destination IPv6 Address）から Hash 値を生成し，それによってマルチパスの候補の一つを選択します。出力インタフェースの決定を次の図に示します。

図 24-4 出力インタフェースの決定



24.4.4 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 16 パスの内 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. 各パスに重み付けを付けないため，回線速度が異なる場合は速度に比例した分配は行いません。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するパスの出力帯域を超えて，継続的にパケットを送出しようとした場合，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（IPv6）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，次の注意が必要です。
   - traceroute（IPv6）コマンドを受信したインタフェースの IPv6 アドレスを送信元 IPv6 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（IPv6）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 IPv6 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ような場合，中継性能が極端に低下することがあります。そのような場合には，すべての中継経路（ゲートウェイ）に対してスタティック NDP を設定してください。
6. 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+ 経路のマルチパスに Null インタフェースを含む場合，該当経路を使用して中継されないことがあります。そのような場合，BGP 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+ 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。**【OP-NPAR】**

24.5 ロードバランスのコンフィグレーション

24.5.1 スタティック経路を使用したロードバランス

「25.2.4 マルチパス経路の設定」を参照してください。

24.5.2 OSPFv3 でのロードバランス

「27.2.6 マルチパスの設定」を参照してください。

24.5.3 BGP4+ でのロードバランス【OP-BGP】

「29.5.3 BGP4+ マルチパスのコンフィグレーション」を参照してください。

24.6　ロードバランスのオペレーション

24.6.1　選択パスの確認

(1) 経路情報の確認

show ipv6 route コマンドを実行し，マルチパス経路の設定内容が正しく反映されているかどうかを確認してください。

図 24-5　マルチパスの経路情報表示

```
> show ipv6 route
Date 2006/03/14 12:00:00 UTC
Total: 11 routes
Destination                                    Next Hop
      Interface      Metric   Protocol  Age
4000:110:1:1::/64                              4000:110:1:1::1
      VLAN0010       0/0      Connected 22m 53s
4000:110:1:1::1/128                            ::1
      localhost      0/0      Connected 22m 53s
4000:120:1:1::/64                              4000:120:1:1::1
      VLAN0020       0/0      Connected 22m 53s
4000:120:1:1::1/128                            ::1
      localhost      0/0      Connected 22m 53s
4000:130:1:1::/64                              4000:130:1:1::1
      VLAN0030       0/0      Connected 22m 53s
4000:130:1:1::1/128                            ::1
      localhost      0/0      Connected 22m 53s
4000:210:1:1::/64                              4000:110:1:1::200
      VLAN0010       0/0      Static     6s
                                               4000:120:1:1::200
      VLAN0020        -        -         -
                                               4000:130:1:1::200
      VLAN0030        -        -         -
      :
      :
>
```

(2) 当該宛先アドレスとの通信可否を確認する

ロードバランスで使用する本装置のインタフェースについて，通信相手となる装置に対して通信できるかどうかを，ping ipv6 <IPv6 Address> specific-route source <Source Address> コマンドを実行して確認してください。ping ipv6 コマンドの <Source Address> には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 IPv6 アドレスを指定してください。

24.7 経路集約の解説

24.7.1 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，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，2001:db8:1:ff01::/64 の経路情報や 2001:db8:1:ff02::/64 の経路情報を学習した場合に，2001:db8:1:ff00::/56 の集約された経路情報を生成するなどです。

経路集約の指定はコンフィグレーションコマンド 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。

24.7.2 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無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。

24.7.3 AS_PATH 属性の集約

BGP4+ 経路が集約元経路に含まれる場合は集約した経路に BGP4+ 経路のパス属性を付加します。集約元の 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 属性について以下の編集を行います。

（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 パスに関しては，コンフィグレーションコマンド 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+ 経路を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。

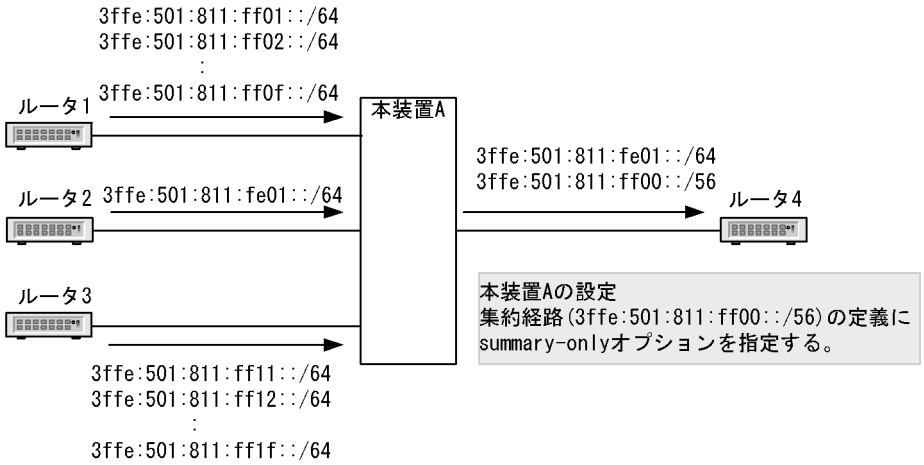
24.7.4　集約元経路の広告抑止

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 RIPng 経路は広告したいが集約元の RIPng 経路を広告しないなどです。

集約元経路の広告抑止は集約経路単位または全集約経路に対して指定できます。集約経路単位に指定する場合は，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。

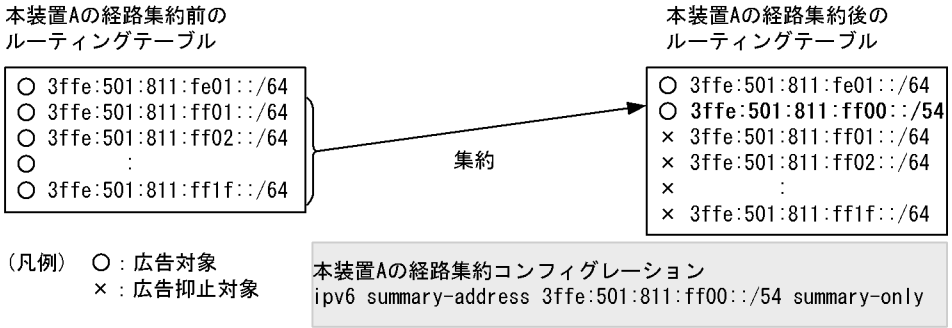
集約元経路の広告抑止の適用例を次の図に示します。

図 24-6　集約元経路の広告抑止の適用例



本装置 A は，ルータ 1 より 3ffe:501:811:ff01::/ 3ffe:501:811:ff02::/64，…，3ffe:501:811:ff0f::/64 を受信し，ルータ 2 より 3ffe:501:811:fe01::/64 を受信し，ルータ 3 より 3ffe:501:811:ff11::/64，3ffe:501:811:ff12::/64，…，3ffe:501:811:ff1f::/64 を学習します。本装置 A では，集約経路 3ffe:501:811:ff00::/56 と学習経路 3ffe:501:811: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 3ffe:501:811: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 24-7　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



24.8 経路集約のコンフィグレーション

24.8.1 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 24-7 コンフィグレーションコマンド一覧

コマンド名	説明
ipv6 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（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。

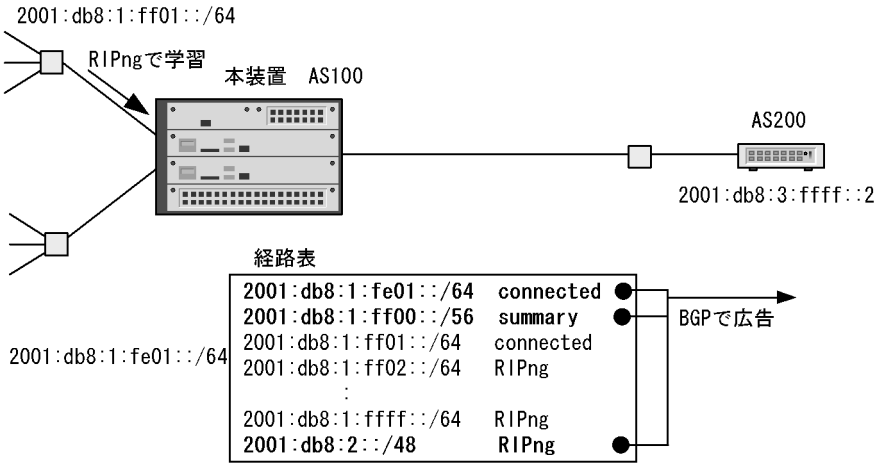
注※

「コンフィグレーションコマンドレファレンス Vol.3　14. 経路フィルタリング（IPv4 ／ IPv6 共通）」を参照してください。

24.8.2 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 24-8 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 vlan 10**
   (config-if)# ipv6 address 2001:db8:1:fe01::1/64
   インタフェース vlan 10 に IPv6 アドレス 2001:db8:1:fe01::1/64 を設定します。

2. **(config-if)# exit**
   (config)# interface vlan 20
   (config-if)# ipv6 address 2001:db8:1:ff01::1/64
   インタフェース vlan 20 に IPv6 アドレス 2001:db8:1:ff01::1/64 を設定します。

3. **(config-if)# ipv6 rip enable**
   インタフェース vlan 20 で RIPng パケットの送受信を行う設定をします。

4. **(config-if)# exit**
   (config)# ipv6 summary-address 2001:db8:1:ff00::/56 summary-only
   集約経路 2001:db8:1:ff00::/56 を生成する設定を行います。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+ 接続を行う設定をします。

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。

24.9 経路集約のオペレーション

24.9.1 運用コマンド一覧

経路集約の運用コマンド一覧を次の表に示します。

表 24-8 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。
restart unicast ※	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 ※	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 ※	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※

「運用コマンドレファレンス Vol.3 8. IPv4・IPv6 ルーティングプロトコル共通」を参照してください。

24.9.2 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。集約経路の表示例を次の図に示します。

図 24-9 集約経路の表示例

```
> show ipv6 route brief summary_routes
Date 2006/03/14 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。アクティブ経路の表示例を次の図に示します。

図 24-10 アクティブ経路の表示例

```
> show ipv6 route brief 2001:db8:1:ff00::/56 longer-prefixes
Date 2006/03/14 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
```

24.10　経路削除保留機能

経路削除保留機能については,「7.10　経路削除保留機能」を参照してください。

24.11 グレースフル・リスタートの概要

IPv6 でのグレースフル・リスタートの動作は IPv4 と同様です。詳細は「7.11 グレースフル・リスタートの概要」を参照してください。

24.12 高速経路切替機能

24.12.1 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 優先経路が使用不可能になったとき，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 24-9 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+ 経路の NextHop 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+ 経路の NextHop 変更	第 2 優先経路への切り替え

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 24-10 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					
		BGP4+	OSPFv3	RIPng	スタティック※	集約経路	直結経路
第 2 優先経路	BGP4+	○	○	○	○	×	×
	OSPFv3	○	－	○	○	×	×
	RIPng	○	○	○	○	×	×
	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 ipv6 route のパラメータとして次を指定した場合
   - reject
   - noinstall
2. コンフィグレーションコマンド ipv6 route のインタフェースとして次を指定した場合
   - Null インタフェース
   - ループバックインタフェース

・マネージメントポート

24.12.2 使用上の注意事項

第 2 優先経路のネクストホップが 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 BGP4+ や OSPFv3 など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，NDP によって動的にアドレス解決が行わ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，ネクストホップの動的なアドレス解決が行われないため，スタティック NDP の設定などの措置が必要となります。

24.13 VRF の解説【OP-NPAR】

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，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 IPv6 アドレス空間を分離するため，各 VRF インスタンスは同じ IPv6 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。

24.13.1 サポート範囲

VRF でサポートする IPv6 ルーティングプロトコルの機能を次の表に示します。

表 24-11 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	RIPng	○
	OSPFv3	○
	BGP4+	○
マルチパス／ロードバランス		○※
経路集約		○
経路削除保留機能		○
グレースフル・リスタート		○
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	○
	ポリシーベースルーティング	○

（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。

24.13.2 経路数の制限

VRF 単位で，収容する経路数を制限できます。

(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，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) 警告メッセージの出力

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，警告メッセージを出力します。

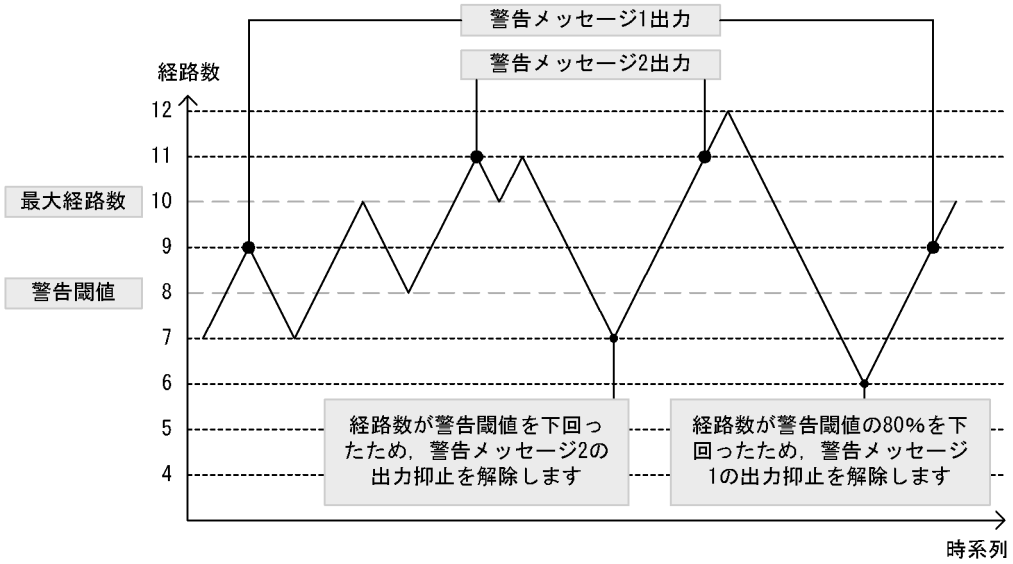
警告閾値を超過したときの警告メッセージ（警告メッセージ 1）の再出力は，経路数が警告閾値の 80% を

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警告メッセージ（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。

経路数と警告メッセージ出力の関係を次の図に示します。

図 24-11　経路数と警告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 ipv6 route を実行してください。

24.13.3　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三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
- ポリシーベースルーティング

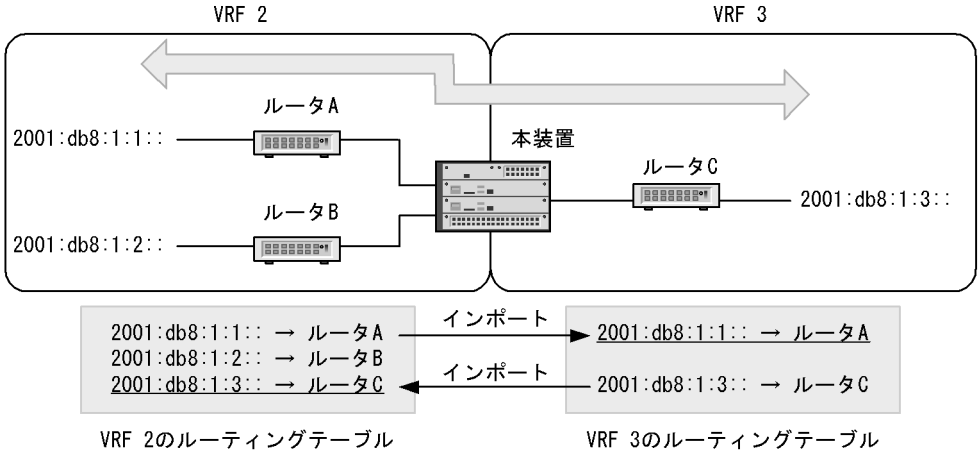
ここでは，ルーティングテーブルを操作する VRF 間の経路交換，および VRF 間にわたるスタティックルーティングについて説明します。また，VRF 間でインポートできる経路について説明します。

（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 24-12 VRF 間の経路交換

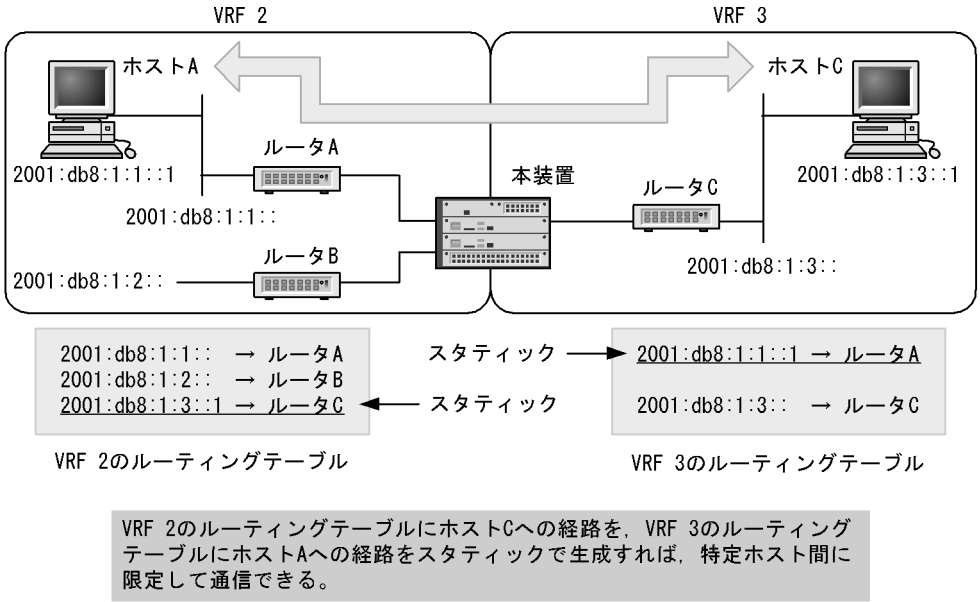


(2) VRF 間にわたるスタティックルーティング

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 24-13 VRF 間にわたるスタティックルーティング



(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。

表 24-12 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

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	○
loopback インタフェースで設定した IPv6 装置アドレスの経路	○
VLAN インタフェースの直結経路（グローバルアドレス）	○
VLAN 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 VLAN インタフェースとなる経路	○
出力インタフェースが loopback 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 Null 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

なお，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。

24.14 VRF のコンフィグレーション【OP-NPAR】

24.14.1 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 24-13 コンフィグレーションコマンド一覧

コマンド名	説明
match vrf ※1	route-map に VRF によるフィルタ条件を設定します。
route-map ※1	route-map を設定します。
ipv6 route ※2	IPv6 スタティック経路を生成します。
ipv6 import inter-vrf ※3	他 VRF またはグローバルネットワークから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 ※3	VRF の最大経路数と警告の運用メッセージ出力閾値を設定します。
vrf definition ※3	VRF 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 14. 経路フィルタリング（IPv4 ／ IPv6 共通）」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 24. 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 30. VRF【OP-NPAR】」を参照してください。

24.14.2 最大経路数の設定

VRF の最大経路数と警告メッセージ出力の閾値を設定します。

[設定のポイント]

ipv6 maximum routes コマンドを使用して，最大経路数と警告メッセージ出力の閾値を設定します。

[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)# ipv6 maximum routes 1000 80**
   VRF 2 で収容できる IPv6 の最大経路数として 1000 を設定します。また，警告メッセージを出力する閾値を 80%に設定します。

24.14.3 エクストラネットの設定

エクストラネットの設定については，「25.2.7 VRF 間にわたるスタティック経路の設定【OP-NPAR】」，および「30.2.8 エクストラネット【OP-NPAR】」を参照してください。

24.15 VRF のオペレーション【OP-NPAR】

24.15.1 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 24-14 運用コマンド一覧

コマンド名	説明
show ipv6 vrf	VRF の IPv6 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経路情報を表示します。
show ipv6 static	スタティック経路に関する情報を表示します。

24.15.2 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 ipv6 vrf コマンドで表示します。

図 24-14 show ipv6 vrf の実行結果

```
> show ipv6 vrf 2
Date 2009/03/14 12:00:00 UTC
VRF              Routes        Neighbor
2                12/100        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 24-15 show ipv6 vrf detail の実行結果

```
> show ipv6 vrf 2 detail
Date 2009/03/14 12:00:00 UTC
VRF 2
  Maximum routes: 100, Warn threshold: 70%, Current routes: 12     …1
  Maximum Neighbor entries: 50, Current Neighbor entries: 7
  Import inter-vrf: -
Interface
Name           Address                                       Status
VLAN0009       3ffe:501:ffff:2::200/64                       Up
VLAN0009       fe80::1001:201a:1%VLAN0009/64                 Up
localhost      ::1/128                                       Up
localhost      fe80::1%localhost/64                          Up
>
```

1. 最大経路数，警告メッセージ出力の閾値，現在の経路数の順に表示します。

24.15.3 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，「30.3.9 エクストラネットの確認【OP-NPAR】」を参照してください。

25 スタティックルーティング（IPv6）

この章では，IPv6 のスタティックルーティングについて説明します。

25.1 解説

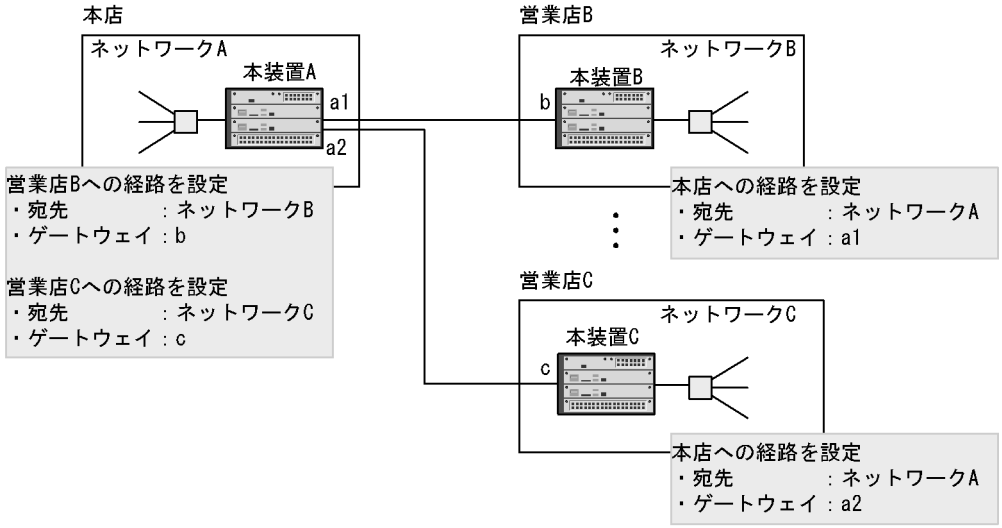
25.1.1 概要

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，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の通信はできません。

図 25-1 スタティックルーティングのネットワーク構成例



25.1.2 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分けし，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い，複数の経路が選択され，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 6 ですが，コンフィグレーションコマンドの ipv6 route static maximum-paths で変更できます。

表 25-1 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。

25.1.3 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，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・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・削除を制御します。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 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ぶことができます。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せずに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）により，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せずに 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違い，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「19　Null インタフェース（IPv6）」を参照してください。

25.1.4 動的監視機能

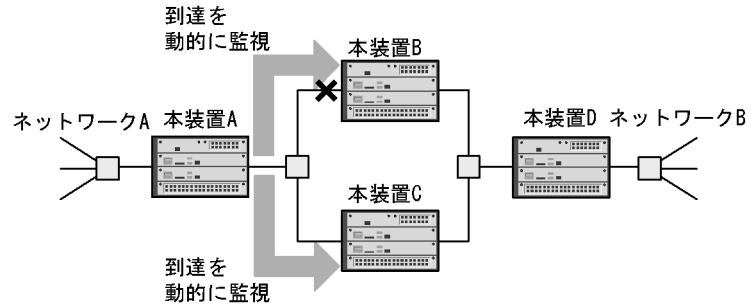
スタティック経路は，ゲートウェイと直接接続されたインタフェースの状態，またはゲートウェイへの経路の有無によって経路の生成・削除を制御します。したがって，経路が生成されている場合でも，該当するゲートウェイへの到達保証はありません。本装置は，生成されたスタティック経路のゲートウェイに対する，ICMPv6 のエコー要求およびエコー応答メッセージを使用した周期的なポーリングによって，到達性を動的に監視する機能を持ちます。この機能を使用することによって，「25.1.3　スタティック経路の中継経路指定」の経路生成・削除条件に加え，該当するゲートウェイへの到達性が確保できている場合だけ，スタティック経路を生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 25-2 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。動的監視を行っていない状態で，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。これによって，本装置 C 経由のスタティック経路への切り替えが行われないで，本装置 A －ネットワーク B 間の通信が停止します。

動的監視を行っている場合，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し，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の切り替えが行われ，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

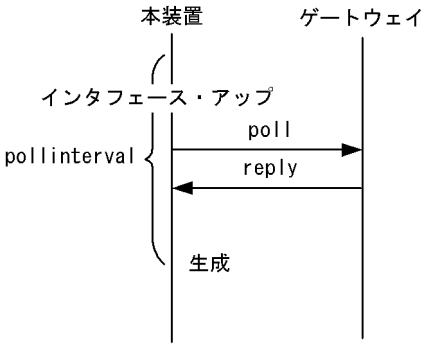
スタティック経路の動的監視による経路の生成，削除および再生成タイミングはコンフィグレーションコマンドの ipv6 route static poll-interval および ipv6 route static poll-multiplier の設定値に依存します。

以降，ipv6 route static poll-interval の設定値を pollinterval，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 25-3 スタティック経路の動的監視による経路生成

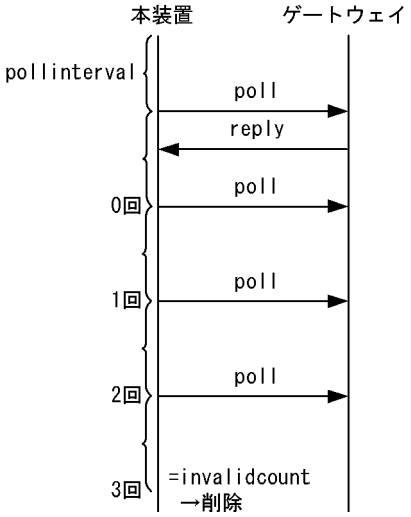


(b) 経路削除タイミング

pollinterval 周期でのポーリングに対し，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 の場合は，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。

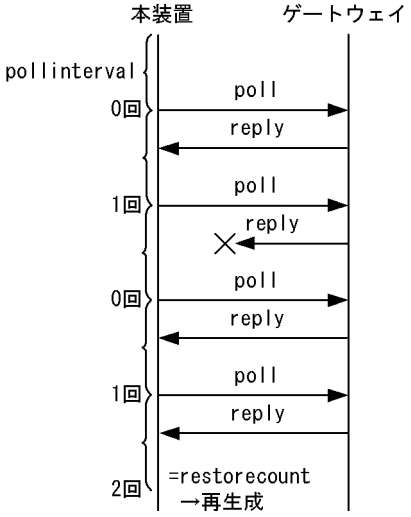
図 25-4　スタティック経路の動的監視による経路削除（invalidcount=3 の場合）



(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，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 の場合は，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 25-5　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）



25.2 コンフィグレーション

25.2.1 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（IPv6）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 25-2 コンフィグレーションコマンド一覧

コマンド名	説明
ipv6 route	IPv6 スタティック経路を生成します。
ipv6 route static poll-interval	ポーリング間隔時間を指定します。
ipv6 route static poll-multiplier	ポーリング回数，連続応答回数を指定します。

25.2.2 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。

[設定のポイント]

スタティック経路の設定は 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。

25.2.3 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。

[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 vlan 10 200 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インタフェース vlan 10 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。本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。

25.2.4 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。

[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設定において，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ことで，マルチパスを構築できます。

[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。

25.2.5 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・生成のタイミングを調整した後に，スタティック経路に動的監視機能を適用します。

[設定のポイント]

ポーリング間隔と回数の設定は 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。

25.2.6 VRF でのスタティック経路の設定【OP-NPAR】

VRF でスタティック経路を設定します。

[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。

25.2.7 VRF 間にわたるスタティック経路の設定【OP-NPAR】

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。

25.2.8 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【OP-NPAR】

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 vlan 2**
   (config-if)# vrf forwarding 2
   (config-if)# ipv6 enable
   (config-if)# ipv6 address 2001:db8:ffff:ffff::1/64
   VLAN ID 2 に VRF 2 と IPv6 アドレスを指定します。

2. **(config)# interface vlan 3**
   (config-if)# vrf forwarding 3
   (config-if)# ipv6 enable
   (config-if)# ipv6 address 2001:db8:ffff:fff0::1/64
   VLAN ID 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 vlan 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インタフェース vlan3 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 vlan 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インタフェース vlan 2 のリンクローカルアドレス fe80::4 を指定します。

25.3 オペレーション

25.3.1 運用コマンド一覧

スタティックルーティング（IPv6）の運用コマンド一覧を次の表に示します。

表 25-3 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 static	スタティック経路に関する情報を表示します。
clear ipv6 static-gateway	スタティック経路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ポーリングをし，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。
restart unicast ※	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 ※	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 ※	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※

「運用コマンドレファレンス Vol.3　8. IPv4・IPv6 ルーティングプロトコル共通」を参照してください。

25.3.2 経路情報の確認

スタティック経路情報を確認します。

図 25-6 show ipv6 static route の実行結果

```
>show ipv6 static route
Date 2006/03/14 12:00:00 UTC
Status Codes: * valid, > active
   Destination                                  Next hop
         Distance Weight Status      Flag
   ::/0                                         2001:db8:1:1::2
         2        0      IFdown      -
*> 2001:db8:ffff:1::/64                         2001:db8:1:2::2
         100      0      Act         -
*  2001:db8:ffff:1::/64                         fe80::2%VLAN0010
         200      0      Act         NoResolve
*> 2001:db8:ffff:2::/64                         2001:db8:2:1::2
         2        0      Act         NoResolve
                                                2001:db8:2:2::2
         2        0      Act         NoResolve
*> 2001:db8:ffff:3::/64                         2001:db8:3:1::2
         2        0      Act Reach   Poll
   2001:db8:ffff:4::/64                         2001:db8:3:1::3
         2        0      Unreach     Poll
```

［確認のポイント］

1. 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。
2. 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 として「>」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。
3. Status Codes として「*」および「>」が表示されていない無効経路は，Status に何らかの障害要因が示されます。「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表します。また，「UnReach」は動的監視機能によって，到達性が確認されていないことを表します。

25.3.3 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を確認します。

図 25-7 show ipv6 static gateway の実行結果

```
>show ipv6 static gateway
Date 2006/03/14 12:00:00 UTC
Gateway                                 Status  Success     Failure  Transition
2001:db8:1:1::2                         IFDown  -           -           -
2001:db8:1:2::2                         -       -           -           -
2001:db8:2:1::2                         -       -           -           -
2001:db8:2:2::2                         -       -           -           -
2001:db8:3:1::2                         Reach   -           0/4         13m 39s
2001:db8:3:2::2                         UnReach 1/2         -           21s
fe80::3%VLAN0010                        -       -           -           -
```

［確認のポイント］

1. 動的監視を行っ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。
2. 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。上記実行結果で，ゲートウェイ 2001:db8:3:2::2 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。

26 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。

26.1 解説

26.1.1 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，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，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，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，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，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，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

なお，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 26-1 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	○	○
ポイズンリバース	×	×
ホールドダウン	×	×

機能	RIPng（IPv6）	RIP（IPv4）
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

26.1.2 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。経路選択の優先順位を次の表に示します。

表 26-2　経路選択の優先順位

優先順位	内容
高	メトリック値が最も小さい経路を選択します。
↑	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。
↓	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。※
低	そのほかの場合，新しく学習した経路を無視します。

注※　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。

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 26-3　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

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，次の表に従って同じ宛先への経路情報の優先度を決定します。

表 26-4　第 2 優先経路の登録を指定した場合の経路選択の優先順位

優先順位	内容
高	メトリック値が小さい経路を選択します。
↑	ネクストホップアドレスが小さい経路を選択します。※ 1
	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。※ 2
↓	今まで第 1 優先であった経路を選択します。
低	そのほかの場合，新しく学習した経路を無視します。

注

ネクストホップアドレスが同じ場合は第 1 優先経路だけ生成します。

注※ 1

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。

注※ 2

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。

26.1.3　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 26-5　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	
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）

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
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
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

次の表に RIPng で広告対象のアドレス種別を示します。

表 26-6 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およびサイトローカ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（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）に対して，経路情報の広告が行われます。

(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。

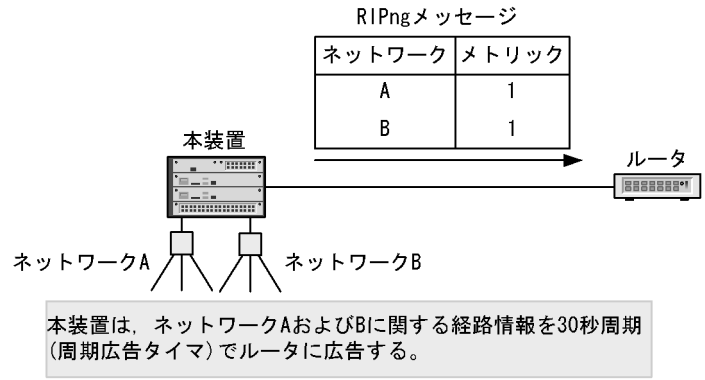
表 26-7 経路広告タイミング

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。

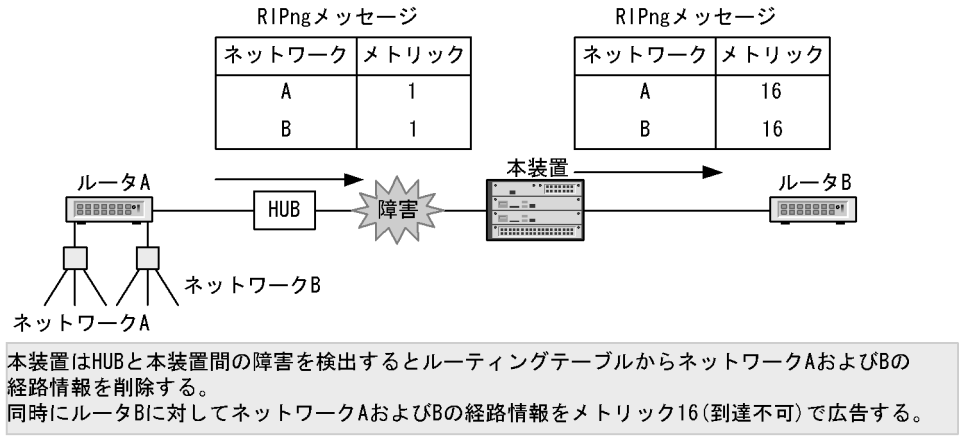
図 26-1 周期的な経路情報広告



(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 26-2 triggered update による経路情報の広告

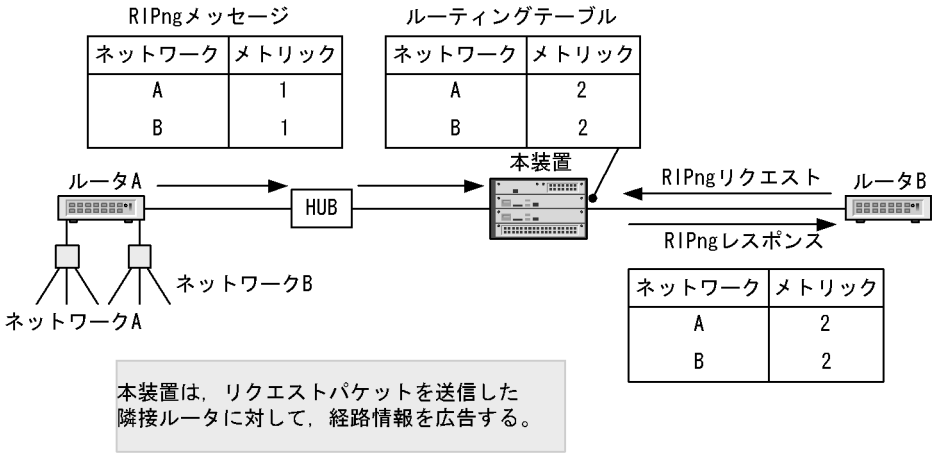


(c) リクエストパケットに対する応答

本装置は，リクエストパケットを受信した際に，本パケットを送信した隣接ルータに対して経路情報を通

知します。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。

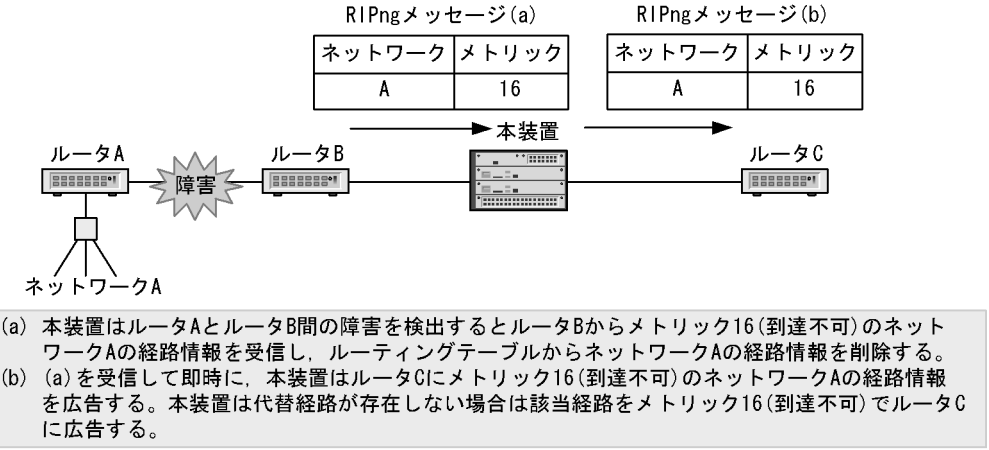
図 26-3 リクエストパケット受信による経路情報の広告



(d) ルートポイズニング

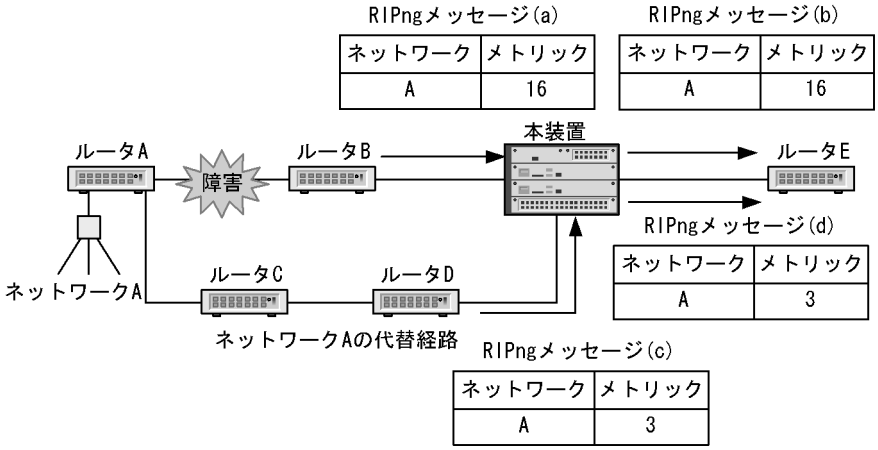
到達できる状態から到達できない状態（メトリック 16 受信または，インタフェース障害によって該当するインタフェースから学習した経路を削除）となった経路に対して，一定時間（60 秒：ガーベジコレクトタイマ）はメトリック 16（到達できない）で隣接ルータに広告します。ルートポイズニングを次の図に示します。

図 26-4 ルートポイズニング



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 26-5　ルートポイズニング期間中の再学習



(a) 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，ルーティングテーブルからネットワークAの経路情報を削除する。
(b) 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の経路情報を広告する。
(c) 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，ルーティングテーブルに追加する(切り替え時間はルータDの周期広告時間による)。
(d) 本装置はルータEに対してネットワークAの経路情報を広告する。

26.1.4　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（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。

(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。

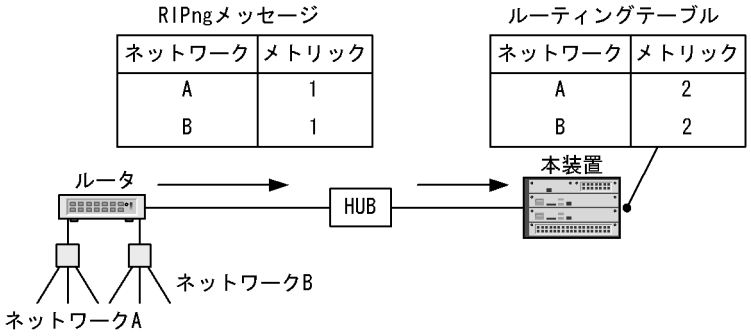
表 26-8　経路情報の学習・切り替えのタイミング

機能	内容
隣接ルータからのレスポンスパケット受信	隣接ルータから通知に従い，経路情報を追加，変更または削除を行います。
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，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 26-6　レスポンスパケット受信による経路情報の生成

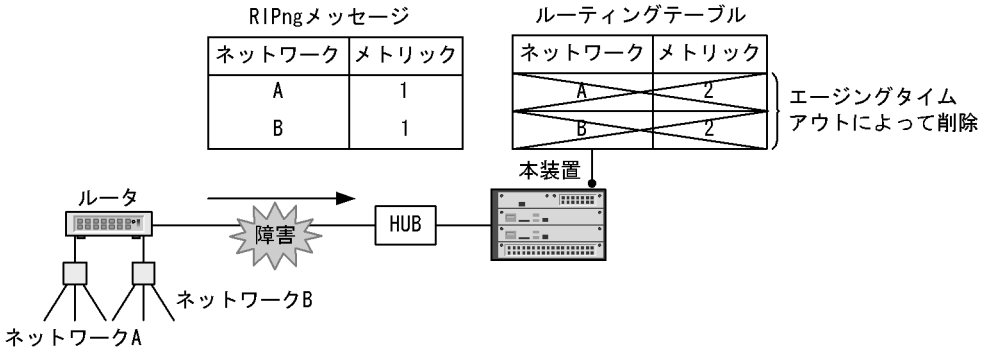


本装置は，隣接ルータから学習したネットワークAおよびBに関する経路情報をルーティングテーブルに追加する。

(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 26-7　エージングタイムアウトによる経路情報の削除

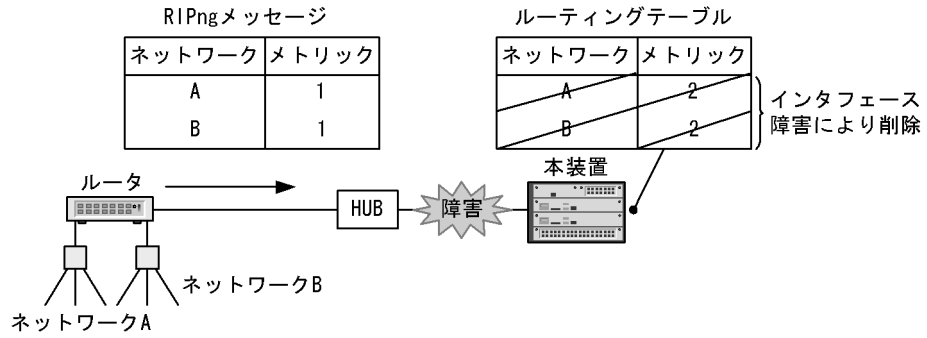


ルータとHUB間で障害が発生すると，本装置にネットワークAおよびBの経路情報が広告されない。本装置は180秒(エージングタイムアウト値)間広告のない経路情報をルーティングテーブルから削除する。

(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した際に，当該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 26-8　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，当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する。

26.1.5　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，およびエキスポート・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インタフェース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。

26.1.6 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 26-9 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。
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。

26.2 コンフィグレーション

26.2.1 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 26-10 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 RIPng パケットで経路情報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　14. 経路フィルタリング（IPv4 ／ IPv6 共通）」を参照してください。

26.2.2 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 vlan 10**
   (config-if)# ipv6 address 2001:db8:1:1::1/64
   (config-if)# ipv6 enable
   インタフェース vlan 10 に IPv6 アドレス 2001:db8:1:1::1/64 を設定します。

2. **(config-if)# ipv6 rip enable**
   インタフェース vlan 10 で RIPng パケットの送受信を有効にします。

3. **(config-if)# exit**
   (config)# interface vlan 20
   (config-if)# ipv6 address 2001:db8:1:2::1/64
   インタフェース vlan 20 に IPv6 アドレス 2001:db8:1:2::1/64 を設定します。

4. **(config-if)# ipv6 rip enable**
   インタフェース vlan 20 で RIPng パケットの送受信を有効にします。

5. **(config-if)# exit**

26.2.3 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 vlan 10**

```
(config-if)# ipv6 rip metric-offset 2 out
```
インタフェース vlan 10 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。

26.2.4 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。

26.2.5 VRF での RIPng の適用【OP-NPAR】

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 vlan 10
(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 のインタフェース vlan 10 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 vlan 20
(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 のインタフェース vlan 20 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。

26.3 オペレーション

26.3.1 運用コマンド一覧

RIPng 情報の確認で使用する運用コマンド一覧を次の表に示します。

表 26-11 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。
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。
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 processes cpu unicast ※	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。
debug protocols unicast ※	ユニキャストルーティングプログラムが出力するイベントログ情報の運用メッセージ表示を開始します。
no debug protocols unicast ※	ユニキャストルーティングプログラムが出力するイベントログ情報の運用メッセージ表示を停止します。
dump protocols unicast ※	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 ※	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※

「運用コマンドレファレンス Vol.3　8. IPv4・IPv6 ルーティングプロトコル共通」を参照してください。

26.3.2 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 26-9 show ipv6 rip の実行結果

```
> show ipv6 rip
Date 2006/03/14 12:00:00 UTC
RIPng Flags: <ON>
Default Metric: 10, Distance: 120
Timers (seconds)
  Update              : 40
  Aging               : 200
  Garbage-Collection : 100
```

26.3.3 送信先情報の確認

RIPng の送信先情報を表示します。

図 26-10　show ipv6 rip target の実行結果

```
> show ipv6 rip target
Date 2006/03/14 12:00:00 UTC
Source Address                          Destination    Flags
fe80::4048:47ff:fe10:1%VLAN0010         VLAN0010       <Multicast>
fe80::4048:47ff:fe10:1%VLAN0020         VLAN0020       <Multicast>
```

26.3.4　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 26-11　show ipv6 rip route の実行結果

```
> show ipv6 rip route brief 4001::/16
Date 2006/03/14 12:00:00 UTC
Status Codes: * valid, > active
   Destination                          Interface      Metric Tag   Timer
*> 4001:21f7:2910:3029::/64             VLAN0010       3      0      4s
*> 4001:64b9:4ba6:dd65::/64             VLAN0020       4      0     10s
*> 4001:652c:7a78:c37::/64              VLAN0020       3      0      9s
*> 4001:ddd9:158:9a2f::/64              VLAN0010       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 26-12　show ipv6 rip received-routes の実行結果

```
> show ipv6 rip received-routes brief 4001::/16
Date 2006/03/14 12:00:00 UTC
Status Codes: * valid, > active
Neighbor Address: fe80::4048:47ff:fe10:10%VLAN0010
   Destination                          Interface      Metric Tag   Timer
*> 4001:21f7:2910:3029::/64             VLAN0010       3      0      9s
*> 4001:ddd9:158:9a2f::/64              VLAN0010       5      0      9s
Neighbor Address: fe80::4048:47ff:fe10:20%VLAN0020
   Destination                          Interface      Metric Tag   Timer
*> 4001:64b9:4ba6:dd65::/64             VLAN0020       4      0     15s
*> 4001:652c:7a78:c37::/64              VLAN0020       3      0     14s
```

26.3.5　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 26-13　show ipv6 rip advertised-routes の実行結果

```
> show ipv6 rip advertised-routes brief interface vlan 10
Date 2006/03/14 12:00:00 UTC
Target Interface: VLAN0010
Destination                             Interface      Metric Tag  Age
*> 2001:db8:1:2::/64                    VLAN0020       1      0    22m 37s
*> 4001:64b9:4ba6:dd65::/64             VLAN0020       5      0    21s
*> 4001:652c:7a78:c37::/64              VLAN0020       4      0    20s
```

27 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。

27.1 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。

27.1.1 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。

27.1.2 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 27-1 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	○※	○
仮想リンク	○	○
マルチバックボーン	○	○

機能	OSPFv3（IPv6）	OSPF（IPv4）
グレースフル・リスタート	○	○
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 を最大四つの OSPFv3 ネットワークに分割し，OSPFv3 ネットワークごとに個別に経路の交換，計算，生成を行えます。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。

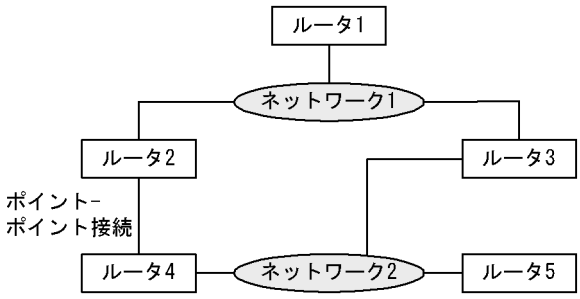
なお，VRF で OSPFv3 を使用した場合，各 VRF を最大四つのドメインに分割できます。

27.1.3 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，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，これを基に各頂点への経路を決定します。

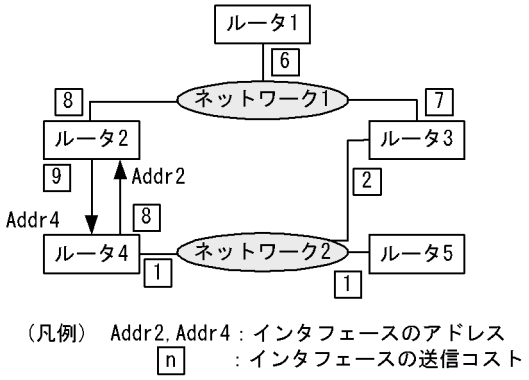
ネットワーク構成の例を次の図に示します。

図 27-1　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。

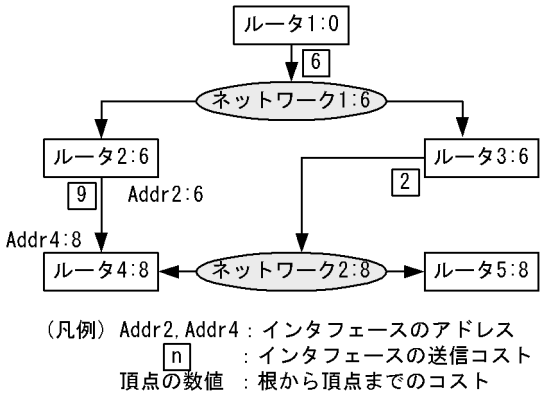
図 27-2　トポロジとコストの設定例



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 27-2　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 27-2　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 27-3　ルータ 1 を根とする最短木



27.1.4　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，以下の情報を付加して 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
  Type 1 と Type 2 の 2 種類があります。Type 1 と Type 2 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ることはありません。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。

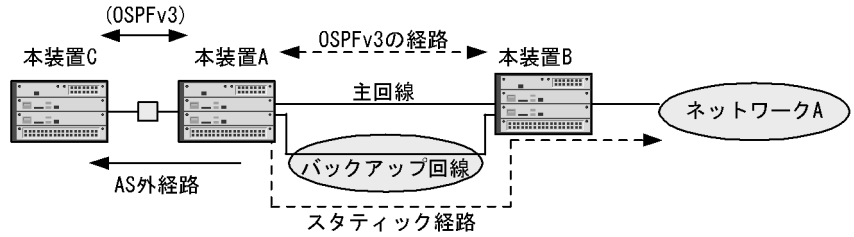
表 27-2 別ドメインの経路を再配布する場合のフィルタ属性

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 Type 2。	
タグ値	経路のタグ値を引き継ぎます。	広告しません。

27.1.5 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 27-4 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。

27.1.6 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選択を行います。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，それぞれ個別に SPF アルゴリズムに基づいて経路選択を行います。

OSPFv3 内における経路選択の優先順位を次の表に示します。なお，この優先順位は変更できません。

表 27-3 経路選択の優先順位

優先順位	選択項目	詳細
高	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）は，AS 外経路より優先します。
↑	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。
	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も優先します。
	AS 外経路タイプ	メトリックタイプが Type1 の AS 外経路を，Type 2 の AS 外経路より優先します。

優先順位	選択項目	詳細
	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。
	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。
↓	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。
低	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，それぞれ個別の値を設定できます。

27.1.7 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，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。

27.1.8 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に当たって，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 は，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することはできませ

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行っても，同一ドメイン内での LSA 広告は抑止されません。

また，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

装置アドレスを複数の 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 ドメインに設定することはできません。

（4） OSPFv3 の制限事項

本装置は，RFC2740（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

27.2 OSPFv3 基本機能のコンフィグレーション

27.2.1 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 27-4 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 27-5 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として，固定の値を設定します。
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 外経路広告を行う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　14. 経路フィルタリング（IPv4 ／ IPv6 共通）」を参照してください。

表 27-6 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　14. 経路フィルタリング（IPv4 ／ IPv6 共通）」を参照してください。

27.2.2 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。

27.2.3 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 の交換を行います。
- エリア分割しない場合，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 100.1.1.1**
(config-rtr)# exit
ルータ ID として 100.1.1.1 を使用します。

3. **(config)# interface vlan 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。

27.2.4 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。
- 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デフォルトメトリック値で広告します。

27.2.5 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，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 vlan 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。

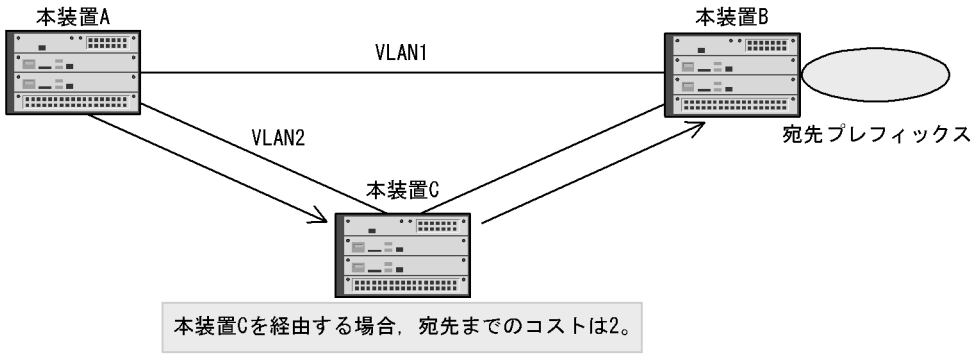
3. **(config)# interface vlan 2**
   (config-if)# ipv6 ospf 1 area 0
   (config-if)# ipv6 ospf cost 2
   コストを 2 に設定します。VLAN2 のコスト値を VLAN1 のコスト値よりも小さくすることによって，VLAN2 を経由する経路が優先されます。

27.2.6 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 27-5 マルチパスの構成



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 vlan 2**
   (config-if)# ipv6 ospf 1 area 0
   (config-if)# exit

2. **(config)# interface vlan 1**

```
(config-if)# ipv6 ospf 1 area 0
(config-if)# ipv6 ospf cost 2
```

VLAN1 のコスト値を 2 とすることで，VLAN2 を経由する経路とコストを等しくします。

27.2.7 VRF での OSPFv3 の適用【OP-NPAR】

[設定のポイント]

ipv6 ospf area コマンドを使用します。

[コマンドによる設定]

ループバックアドレスをルータ ID として使用し，VRF 2 で OSPFv3 を適用します。

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 100.1.1.1
(config-if)# exit
```

   VRF2 を指定して，IP アドレスを 100.1.1.1 にします。

3. `(config)# interface vlan 1`

   インタフェースモードへ移行して，VLAN 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。

27.3 インタフェースの解説

27.3.1 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。

27.3.2 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。

（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について，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，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。

27.3.3 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 パケットによって当該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。

あるルータのどこかのインタフェースの priority を 0 と設定すると，このルータはインタフェースが接続しているエリアについて，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。

27.3.4 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。LSA は，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，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。

27.3.5 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 パケットの送受信を行いません。

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。

27.4 インタフェースのコンフィグレーション

27.4.1 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 27-7 コンフィグレーションコマンド一覧

コマンド名	説明
ipv6 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。
passive-interface（ospfv3 モード）	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 27-8 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 長を指定します。
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　12. 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　3. ループバックインタフェース（IPv4）」を参照してください。

27.4.2 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行います。priority や passive-interface コマンドを設定することで，動作を変えられます。

(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 vlan 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 vlan 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 vlan 2
   VLAN2 をパッシブインタフェースに設定します。

27.5 OSPFv3 のオペレーション

27.5.1 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 27-9 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。
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。
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 processes cpu unicast ※	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 ※	ユニキャストルーティングプログラムを再起動します。
debug protocols unicast ※	ユニキャストルーティングプログラムが出力するイベントログ情報の運用メッセージ表示を開始します。
no debug protocols unicast ※	ユニキャストルーティングプログラムが出力するイベントログ情報の運用メッセージ表示を停止します。
dump protocols unicast ※	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 ※	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※
「運用コマンドレファレンス Vol.3 8. IPv4・IPv6 ルーティングプロトコル共通」を参照してください。

27.5.2 ドメインの確認

OSPFv3 が動作中である場合，ルータ ID やディスタンス値などの，コンフィグレーションの内容の確認は，運用コマンド show ipv6 ospf で行います。

図 27-6 show ipv6 ospf コマンドの実行結果

```
>show ipv6 ospf
Date 2006/03/14 12:00:00 UTC
OSPFv3 protocol: ON

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
    -                                               -
```

27.5.3 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 の確認は，運用コマンド show ipv6 ospf neighbor で行います。

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，隣接関係の確立を行います。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，運用コマンド show ipv6 ospf interface または show ipv6 ospf neighbor detail 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 内より 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，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 27-7 show ipv6 ospf neighbor コマンドの実行結果

```
>show ipv6 ospf neighbor
Date 2006/03/14 12:00:00 UTC
Domain: 1
Area: 0
Neighbor Address          State               Router ID   Priority Interface
fe80::1000:00ff:fe00:2002 Full/BackupDR       172.16.10.12       1 VLAN0003
fe80::1000:00ff:fe00:2003 Full/DR Other       172.16.10.13       1 VLAN0003
fe80::1000:00ff:fe00:2004 Exch Start/DR Other 172.126.10.14      1 VLAN0003
```

図 27-8 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 vlan 10
Date 2009/05/30 12:00:00 UTC
Domain: 1
Area: 0
Interface ID: 2,Link Local Address : fe80::1000:00ff:fe00:0001%VLAN0010
    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::1000:00ff:fe00:2002  Full         172.16.1.2           0
>
```

図 27-9 show ipv6 ospf neighbor コマンド（detail）の実行結果

```
>show ipv6 ospf neighbor detail
Date 2009/05/30 12:00:00 UTC
Domain: 1
Area: 0
Interface: VLAN0020, Interface State: Backup DR
    Neighbor Address: fe80::1000:00ff:fe00:2002, 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
    Last Hello: 6s, Last Exchange: 45d 12h
    DS: 0, LSR: 0, Retrans: 0, <Master>
    Neighbor Address: fe80::1000:00ff:fe00:2001, 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
    Last Hello:  3s, Last Exchange:  1m  8s
    DS: 0, LSR: 0, Retrans: 1, <>
>
```

27.5.4 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の名称（Interface），状態（State），Priority，コスト値（Cost），隣接ルータ数（Neighbor）の確認は，運用コマンド show ipv6 ospf interface で行います。

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 27-10 show ipv6 ospf interface コマンドの実行結果

```
>show ipv6 ospf interface
Date 2006/03/14 12:00:00 UTC
Domain: 1
Area: 0
  Interface         State     Priority  Cost   Neighbor
  VLAN0003          DR           1      1      1

Area: 1
  Interface         State     Priority  Cost   Neighbor
  VLAN0004          BackupDR     10     20     10
```

27.5.5 LSA の確認

(1) LSA 数

OSPFv3 で保持している LSA の数の確認は，運用コマンド show ipv6 ospf database database-summary で行います。

図 27-11 show ipv6 ospf database database-summary コマンドの実行結果

```
>show ipv6 ospf database database-summary
Date 2006/03/14 12:00:00 UTC
Domain: 1
Local Router ID: 172.16.251.141
Area: 0
  [Linklocal scope]
    Link              :     1
    Opaque-Link       :     1
  [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 の一覧を表示します。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，以下の 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。
   なお，広告している経路の宛先を確認する場合，show ipv6 ospf database external コマンドによって，詳細な情報を表示してください。

図 27-12 show ipv6 ospf database コマンドの実行結果

```
>show ipv6 ospf database
Date 2006/03/14 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
    255.255.255.255     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: VLAN0003
    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: VLAN0004
    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 27-13 show ipv6 ospf database external コマンドの実行結果

```
> show ipv6 ospf database external
Date 2006/03/14 12:00:00 UTC
Domain: 1
Local Router ID: 100.1.1.1
LS Database: AS-external-LSA
Advertising Router: 100.1.1.1
    LSID: 00000000, Age: 6, Length: 44
    Sequence: 80000001, Checksum: 5373
    Prefix: 3ffe:4:1::1/128
       Prefix Options: <LocalAddress>
       Type: 2, Metric: 20, Tag: ----
```

28 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。

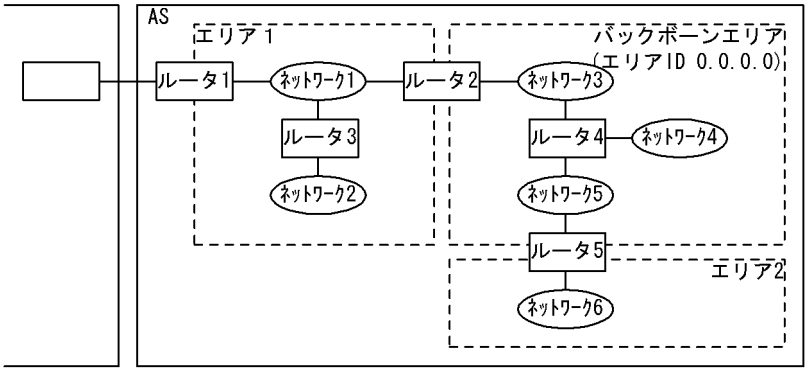
28.1 エリアとエリア分割機能の解説

28.1.1 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 28-1 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の交換を行うため，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

エリア分割を行うと，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，エリア分割を行わ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，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，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，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。

28.1.2 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 28-1 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
3ffe:501:811:10::/60 3ffe:501:811:20::/61 3ffe:501:811:28::/61 3ffe:501:811:30::/60	なし	3ffe:501:811:10::/60 3ffe:501:811:20::/61 3ffe:501:811:28::/61 3ffe:501:811:30::/60
3ffe:501:811:10::/60 3ffe:501:811:20::/61 3ffe:501:811:28::/61 3ffe:501:811:30::/60	3ffe:501:811::/59 3ffe:501:811::20::/60	3ffe:501:811::/59 3ffe:501:811:20::/60 3ffe:501:811:30::/60
3ffe:501:811:10::/60 3ffe:501:811:20::/61 3ffe:501:811:28::/61 3ffe:501:811:30::/60 3ffe:501:811:ff00::/58	3ffe:501:811::/58（抑止） 3ffe:501:811:ff00::/56	3ffe:501:811: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り，アドレスの範囲をコンフィグレーションで設定することによって，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，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。

28.1.3 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）。

28.1.4 仮想リンク

OSPFv3 では，スタブエリアとして設定しておらず，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。

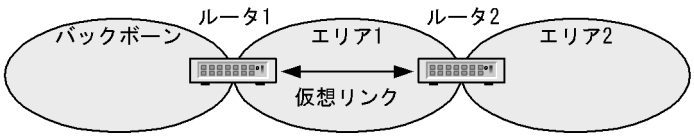
仮想リンクの使い方として，次に示す三つの例を挙げます。

- 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ことによって，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り，エリア 2 をバックボーンに接続しているとみなせるようになります。

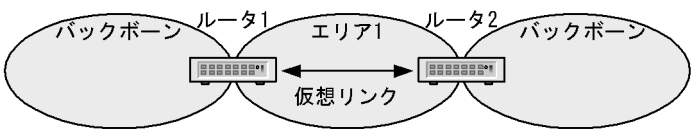
図 28-2 エリアのバックボーンへの接続



(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ことによって，バックボーンが結合されることになり，この障害を回避できます。

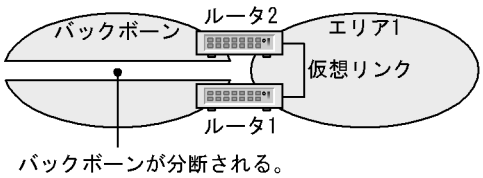
図 28-3 バックボーン間の接続



(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，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 28-4 バックボーン分断に対する予備経路



28.1.5 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 グローバルまたは IPv6 サイトローカルアドレスを使用して，仮想リンクの隣接ルータと OSPFv3 パケットの送受信を行います。このアドレスは，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，以下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 グローバルまたは IPv6 サイトローカルアドレスが設定されている必要があります。IPv6 グローバルまたは IPv6 サイトローカ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。

28.2 エリア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

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，「27 OSPFv3」で解説している機能のコマンドは，「表 27-5 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 27-6 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 27-7 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 28-2 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 28-3 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。

28.2.2 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。**

28.2.3 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 100.1.1.1**
   (config-rtr)# exit
   ルータ ID として 100.1.1.1 を使用します。

4. **(config)# interface vlan 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。

28.2.4 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り，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における，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 3ffe:501:811::/59
   エリア 0 においてプレフィックス 3ffe:501:811::/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 3ffe:501:811::20::/60**
   (config-rtr)# exit
   エリア 1 においてプレフィックス 3ffe:501:811::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 vlan 3**
   (config-if)# ipv6 ospf 1 area 0

```
(config-if)# exit
(config)# interface vlan 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。

28.2.5 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 vlan 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。

28.3 グレースフル・リスタートの解説

28.3.1 概要

グレースフル・リスタートは，装置が系切替したときや，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停止時間を短縮する機能です。

OSPFv3 では，グレースフル・リスタートによって OSPFv3 の再起動を行う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。

28.3.2 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・リスタートを行っている間，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以下に示します。

- 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インタフェースすべて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，以下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，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，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，ヘルパー機能を削除した場合。

28.3.3 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。

- 装置が系切替したとき。
- 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 28-5 OSPFv3 グレースフル・リスタート手順

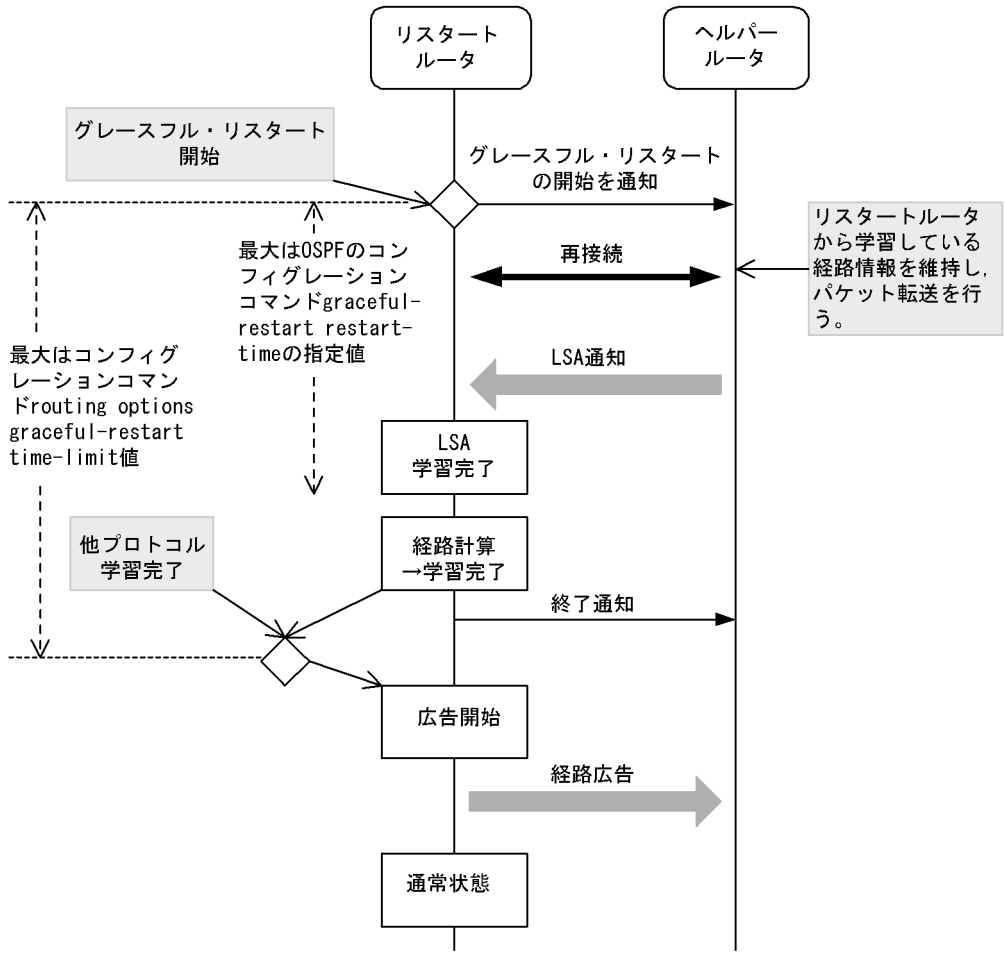


表 28-4 OSPFv3 グレースフル・リスタート手順

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	装置が系切替したとき。	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 情報のパケット交換を行います。
		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完了し，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行い，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行います。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，経路計算を行います。
3	広告開始	OSPFv3 の経路学習が完了し，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。
- 再接続を行っ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の graceful-restart mode を変更し，リスタートルータ機能を削除した場合。

(4) 注意事項

1. 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。
2. 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。
3. 本装置の系切替時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ルーティングエントリが削除されることがあります。
4. 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することができず，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。

28.4 グレースフル・リスタート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

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 28-5 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	ヘルパールータにおいて，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　8. ルーティングオプション（IPv4）」を参照してください。

28.4.2 ヘルパー機能

[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。

28.4.3 リスタート機能

[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。

28.5 スタブルータの解説

28.5.1 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，このような通知を行っているルータを，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ぐことができます。

(1) マックスメトリック

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，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装置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。

28.5.2 スタブルータ動作

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。

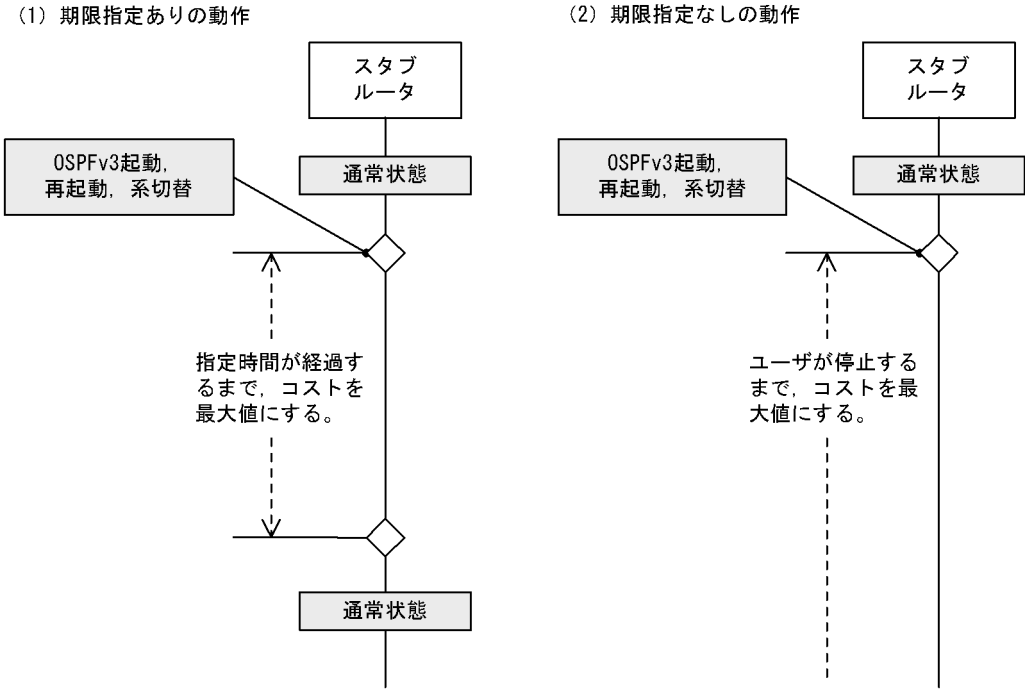
(2) 起動後にスタブルータとして動作する場合

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。

- 装置の系切替後（グレースフル・リスタート成功時を除く）
- ユニキャストルーティングプログラムの再起動後（グレースフル・リスタート成功時を除く）
- 装置起動
- グレースフル・リスタートが発生し，本装置がリスタートルータとしての経路学習に失敗した後

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 28-6 スタブルータの動作



(3) 注意事項

1. 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。
2. 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。
3. 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，仮想ネーバはその仮想リンクを到達不能とみなします。

28.6 スタブルータのコンフィグレーション

28.6.1 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 28-6 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。

28.6.2 スタブルータ機能

[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。

28.7 OSPFv3 拡張機能のオペレーション

28.7.1 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 28-7 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 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 8. IPv4・IPv6 ルーティングプロトコル共通」を参照してください。

28.7.2 エリアボーダの確認

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，運用コマンド show ipv6 ospf を実行し，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かどうかを確認してください。

図 28-7 show ipv6 ospf コマンドの実行結果

```
>show ipv6 ospf
Date 2006/03/14 12:00:00 UTC
OSPFv3 protocol: ON

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
    Helper Status : Finished  2006/03/08 14:12:22
Area: 0, Interfaces: 2
    Network Range                                   State
    3ffe:501:ffff:100::/64                          DoNotAdvertise
    3ffe:501:ffff:200::/64                          Advertise
Area: 1, Interfaces: 1
    Network Range                                   State
    -                                               -
```

28.7.3 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かどうかを確認してください。運用コマンド show ipv6 ospf に area パラメータを指定した場合，エリアの一覧を表示します。

図 28-8 show ipv6 ospf コマンド（area パラメータ）の実行結果

```
>show ipv6 ospf area
Date 2006/03/14 12:00:00 UTC
Domain: 1
Area ID          Neighbor  SPFcount  Flags
0                3         14        <ASBoundary>
10               2         8         <Stub>
>
```

28.7.4 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

グレースフル・リスタートの状態を，運用コマンド show ipv6 ospf を実行し，確認してください。

図 28-9 show ipv6 ospf コマンドの実行結果

```
>show ipv6 ospf
Date 2006/03/14 12:00:00 UTC
OSPFv3 protocol: ON

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
    Helper Status : Finished  2006/03/08 14:12:22
Area: 0, Interfaces: 2
    Network Range                                   State
    3ffe:501: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

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，show graceful-restart unicast コマンドを実行し，確認してください。

図 28-10 show graceful-restart unicast コマンドの実行結果

```
>show graceful-restart unicast
Date 2006/04/14 12:00:00 UTC
Status: Completed
Graceful Restart Time Limit: 180s
Start Time: 2006/04/08 17:01:23
End Time  : 2006/04/08 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)
```

29 BGP4+【OP-BGP】

この章では，BGP4+ の仕様や使用する上での注意点を中心に説明します。

29.1 基本機能の解説

29.1.1 概要

BGP4+（Multiprotocol Extensions for Border Gateway Protocol 4）は，インターネットのバックボーンで使用されているルーティングプロトコル 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。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+（IPv6）と BGP4（IPv4）の機能差分を次の表に示します。

表 29-1 BGP4+(IPv6) と BGP4(IPv4) の機能差分

機能	BGP4+(IPv6)	BGP4(IPv4)
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	○	○
グレースフル・リスタート	○	○
学習経路数制限	○	○

（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
注※2 VRF では取り扱いません。

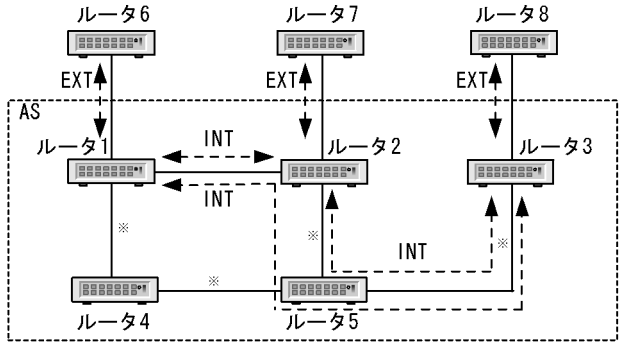
29.1.2 ピアの種別と接続形態

BGP4+ 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。BGP4+ が動作するルータを BGP4+ スピーカと呼びます。この BGP4+ スピーカはそのほかの BGP4+ 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。なお，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，メンバー AS 間ピアが追加されます。メンバー AS 間ピアについては，「29.4.10 コンフェデレーション」を参照してください。

ネットワーク構成に合わせてピアを使用してください。外部ピアと内部ピアを次の図に示します。

図 29-1 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BGP4+スピーカ
ルータ6，ルータ7，ルータ8：外部BGP4+スピーカ
ルータ4，ルータ5　　：内部非BGP4+スピーカ
INT ：内部ピア
EXT ：外部ピア
注※ IGPが動作する。

(1) 外部ピア

外部ピアは異なる AS に属する BGP4+ 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 アドレスは直接接続されたインタフェースのリンクローカルまたはグローバルインタフェース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の neighbor ebgp-multihop を使用することによって，直接接続されたインタフェースのインタフェースアドレス以外のアドレス（例えば装置アドレス）で接続できます。

「図 29-1 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

内部の同じ AS に属する BGP4+ スピーカ間に形成するピアです。BGP4+ 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 BGP4+ 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 BGP4+ スピーカ間で論理的にフルメッシュに形成されなければなりません。これは，内部ピアで受信した経路情報は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 29-1 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) 装置アドレスを使用したピアリング

本装置では装置に対して IPv6 アドレスを割り当てることができます。これを装置アドレスと呼びます。この装置アドレスを外部ピアや内部ピアの IPv6 アドレスとして使用することによって，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 29-1 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 IPv6 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 間の内部ピアは確立できません。しかし，内部ピアの IPv6 アドレスとして装置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。

[装置アドレス使用上の注意事項]

装置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）でお互いに学習していなければなりません。なお，本装置は装置アドレスを直結経路情報として扱います。

[内部ピアで非 BGP4+ スピーカを経由する場合の注意事項]

内部ピアで非 BGP4+ 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 BGP4+ スピーカで IGP 経由でその経路情報を学習していなければなりません。これは該当する経路情報の通知によって通知先 BGP4+ スピーカから入ってくる該当宛先への IPv6 パケットが，該当する経路を学習していない非 BGP4+ 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 29-1　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 IPv6 パケットがルータ 5 で廃棄されるのを防ぐためです。

29.1.3　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を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学習した同じ宛先への複数の経路情報から次の表に示す優先順位で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（RIPng，OSPFv3，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。

なお，コンフェデレーション構成での経路選択は，「29.4.10　コンフェデレーション」を参照してください。

表 29-2　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。
↑	LOCAL_PREF 属性の値が最も大きい経路を選択します。
	AS_PATH 属性の AS 数が最も短い経路を選択します。※ 1
	ORIGIN 属性の値で IGP，EGP，Incomplete の順で選択します。
	MED 属性の値が最も小さい経路を選択します。※ 2
	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。
	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。
	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。※ 3
↓	CLUSTER_LIST 属性長が最も短い経路を選択します。※ 4
低	学習元ピアのアドレスが小さい経路を選択します。※ 3

注※ 1

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。

注※ 2

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 を指定することによって，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。

注※ 3

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 を指定することによって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。

注※ 4

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。

weight 値と，経路選択に関連する経路情報に含まれる BGP 属性（LOCAL_PREF 属性，AS_PATH 属性，ORIGIN 属性，MED 属性，MP_REACH_NLRI 属性）の概念を次に説明します。

（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 の範囲で指定します。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 コマンド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 の範囲で指定します。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 を設定して，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。

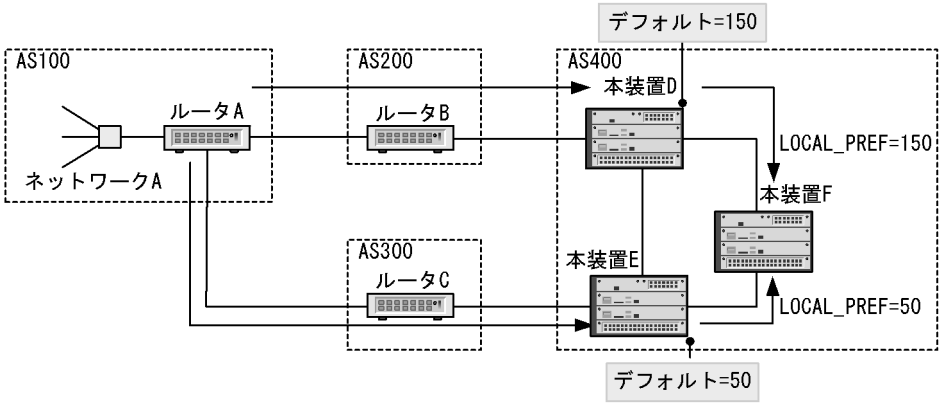
（b） LOCAL_PREF 属性のフィルタ単位での変更

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 を組み合わせることによって，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 29-2 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け取ります。本装置 D の LOCAL_PREF 値を 150 に，本装置 E の LOCAL_PREF 値を 50 に設定するとします。それによって，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 に設定し，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。本装置 F でのネットワーク A への経路情報は，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 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 29-3 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。
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 を組み合わせることによって，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。

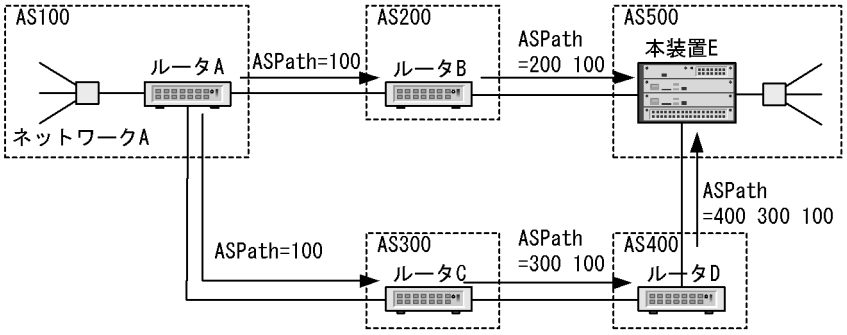
(4) AS_PATH 属性

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 との組み合わせによって複数の自 AS 番号を AS_PATH 属性に追加することもできます。これはある宛先ネットワークへの複数の経路が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 29-3 AS_PATH 属性による経路選択

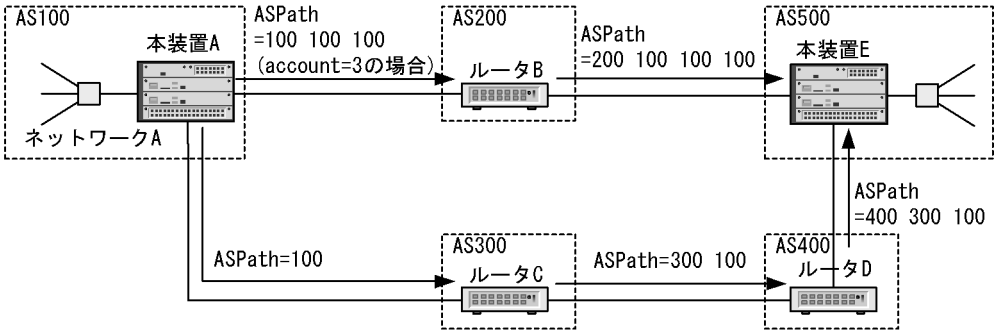


ルータ A が自 AS に存在するネットワーク A を AS200 経由で通知するとき，AS500 に到達する経路情報の AS_PATH 属性は「200 100」を持ちます。ルータ A が自 AS 内のネットワーク A を AS300，AS400 経由で通知するとき，AS500 に到達する経路情報の AS_PATH 属性は「400 300 100」を持ちます。したがって，AS500 の本装置 E は最も短い AS_PATH 属性を持つ AS200 経由で到達した経路を選択します。

(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 の例を次の図に示します。

図 29-4 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 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」を持ち，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。

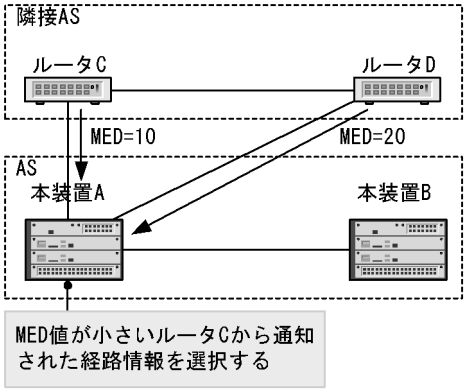
(5) MED 属性

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 BGP4+ 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 を指定して，異なる隣接 AS から学習した BGP4+ 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 29-5 MED 属性による経路選択



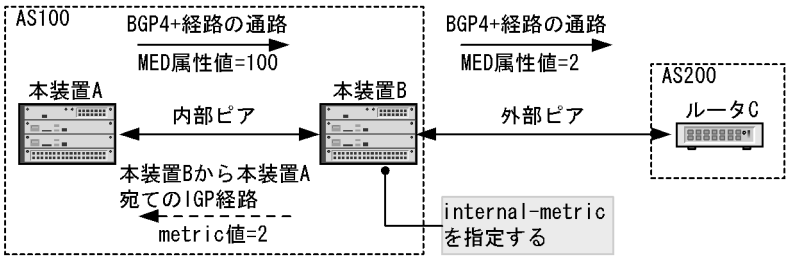
ある宛先ネットワークに対する経路情報をルータ C は MED 属性値 10 で，ルータ D は MED 属性値 20 で本装置 A に通知しているものとします。この場合，本装置 A はルータ C から通知された経路情報を該当する宛先ネットワークへの経路として選択します。

(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 を組み合わせることによって，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，set metric-type に internal を指定した場合，NextHop 解決に使用している IGP 経路のメトリック値を，通知する BGP4+ 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 29-6 set metric-type internal の使用例



この図では本装置 A，本装置 B の間で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 BGP4+ 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 属性値に設定したい場合，本装置 B でコンフィグレーションコマンド set metric を指定します。

(6) MP_REACH_NLRI 属性のネクストホップ情報

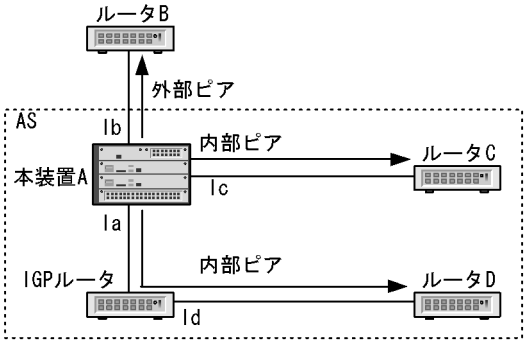
BGP4+ では BGP4+ ピアから受信した NextHop 属性の値を無視します。その代わりに MP_REACH_NLRI 属性のネクストホップ情報を経路のネクストホップとして採用します。

BGP4+ では相手 BGP4+ スピーカに経路情報を通知する場合，MP_REACH_NLRI 属性のネクストホップ情報として IPv6 グローバルアドレスでピアリングしたときだけ，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の設定例を次の図に示します。

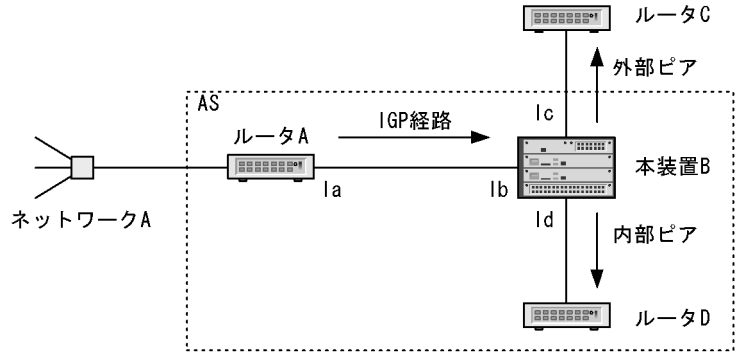
図 29-7 BGP4+ ピアから学習した経路を広告する場合に通知する経路情報のネクストホップの設定例



- **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 側のグローバルおよびリンクローカルアドレス Ib が割り当てられます。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含まれていた場合は，そのアドレスをネクストホップとして使用します。両方のアドレスが含まれていた場合は，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**
  MP_REACH_NLRI 属性のネクストホップにはルータ 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に設定されているグローバルアドレスが設定されます。
  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にグローバルアドレスが設定されていない場合，本装置 A －ルータ C 間のインタフェースの本装置側のグローバルアドレスが設定されます。
- **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にはルータ 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に設定されているグローバルアドレスが設定されます。
  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にグローバルアドレスが設定されていない場合，本装置 A －ルータ D 間のインタフェースの本装置側のグローバル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の設定例を次の図に示します。

図 29-8 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って，MP_REACH_NLRI 属性のネクストホップ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。BGP4+ 経路のネクストホップへ到達可能な経路の中から，宛先のマスク長が最も長い経路を選択し，該当する経路のパスを 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，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，NextHop を解決した経路がスタティック経路で，かつ noinstall 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。

29.1.4 VRF での BGP4+ の機能【OP-NPAR】

(1) 概要

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。なお，異なる VRF 間のピア接続はできません。

(2) VRF で 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 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+ 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りますので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・リフレクション機能）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。

29.1.5 BGP4+ 使用時の注意事項

BGP4+ 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注意してください。

(1) BGP4+ の制限事項

本装置は 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），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 29-4 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。
	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。

RFC 番号	RFC		本装置
		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 回数により変化する可変値 (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。

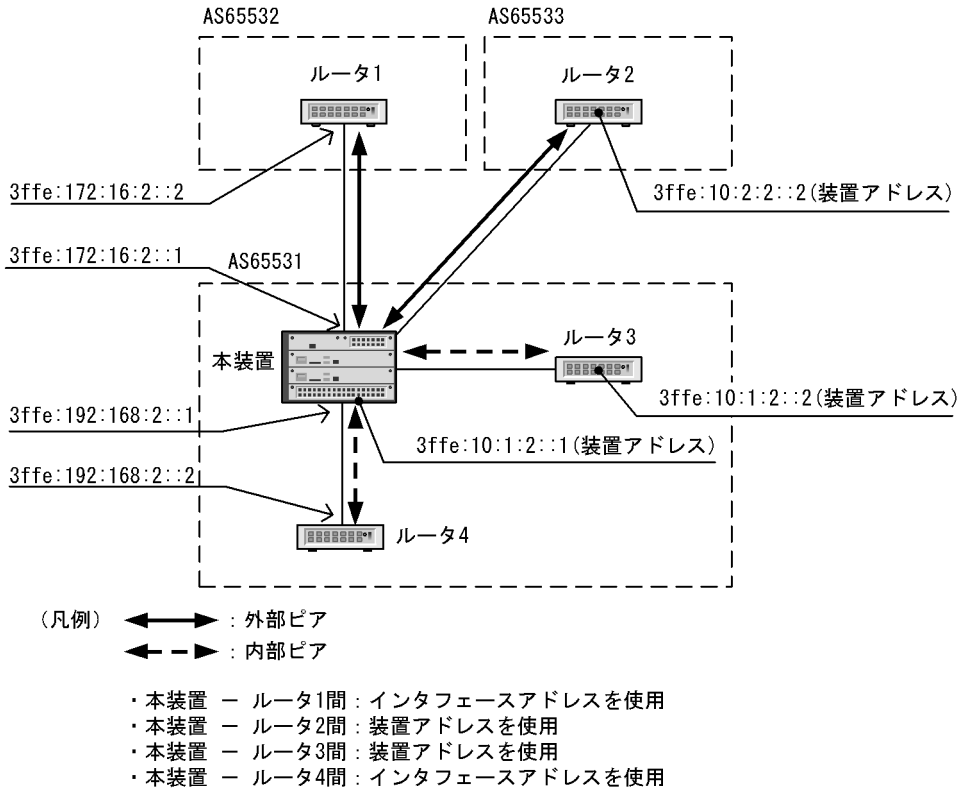
(2) 直接接続されたインタフェース上でピアリングする場合の注意事項

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，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 を設定することによってコネクションが確立します。

29.2 基本機能のコンフィグレーション

次の図の接続構成例をもとにコンフィグレーションを説明します。

図 29-9 接続構成例



29.2.1 コンフィグレーションコマンド一覧

ピア種別と接続形態（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の表に示します。

表 29-5 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。
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。

コマンド名	説明
disable ※1	BGP4/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 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をピアリングに使用する自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アドレスに装置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/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。
distribute-list in（BGP4+）※2	BGP4+ の学習経路フィルタリングの条件として用いる経路フィルタを指定します。
distribute-list out（BGP4+）※2	BGP4+ の広告経路フィルタリングの条件として用いる経路フィルタを指定します。
neighbor in（BGP4+）※2	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用いる経路フィルタを指定します。
neighbor out（BGP4+）※2	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用いる経路フィルタを指定します。
redistribute（BGP4+）※2	BGP4+ で広告する経路のプロトコルを指定します。

注※ 1

BGP4（IPv4）ピアと共用コマンドです。

注※ 2

「コンフィグレーションコマンドレファレンス Vol.3　14. 経路フィルタリング（IPv4 ／ IPv6 共通）」を参照してください。

表 29-6 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	1. 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リング設定を適用します。 ・全 BGP4+ ピアに BGP4+ 経路の再広告要求を行います 2. パラメータに * out を指定した場合 ・BGP4+ 広告用経路フィルタリングに最新の経路フィルタリング設定を適用します。 ・neighbor remove-private-as の設定を運用に反映します。 ・全 BGP4+ ピアに BGP4+ 経路の再広告を行います。 3. 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リング設定を適用します。 ・neighbor remove-private-as 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行います。 4. パラメータに * を指定した場合 全 BGP4+ ピアを切断します。

29.2.2 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自装置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. **フィルタ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コンフィグレーションコマンド neighbor activate 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+ ピアの接続ができません。
- 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行います。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，コンフィグレーションコマンド neighbor remote-as の設定前に，コンフィグレーションコマンド disable 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コンフィグレーションコマンド disable を削除してください。

29.2.3 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/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 3ffe:172:16:2::2 remote-as 65532**
   外部ピア（相手側アドレス：3ffe:172:16:2::2，AS 番号：65532）を設定します。

4. **(config-router)# neighbor 3ffe:10:2:2::2 remote-as 65533**
   外部ピア（相手側アドレス：3ffe:10:2:2::2，AS 番号：65533）を設定します。

5. **(config-router)# neighbor 3ffe:10:2:2::2 ebgp-multihop**
   ピアリングに使用するピアアドレスにピアと直接接続されたインタフェースのインタフェースアドレスを使用しないことを設定します。

6. **(config-router)# neighbor 3ffe:10:2:2::2 update-source loopback 0**
   ピアリングに使用する自側アドレスに装置アドレスを指定します。

7. **(config-router)# neighbor 3ffe:192:168:2::2 remote-as 65531**
   内部ピア（相手側アドレス：3ffe:192.168:2::2）を設定します。

8. **(config-router)# neighbor 3ffe:10:1:2::2 remote-as 65531**
   内部ピア（相手側アドレス：3ffe:10:1:2::2）を設定します。

9. **(config-router)# neighbor 3ffe:10:1:2::2 update-source loopback 0**
   ピアリングに使用する自アドレスに装置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 3ffe:172:16:2::2 activate**
    外部ピア（相手側アドレス：3ffe:172:16:2::2）の IPv6 アドレスファミリを有効にします。

12. **(config-router-af)# neighbor 3ffe:10:2:2::2 activate**
    外部ピア（相手側アドレス：3ffe:10:2:2::2）の IPv6 アドレスファミリを有効にします。

13. **(config-router-af)# neighbor 3ffe:192:168:2::2 activate**
    内部ピア（相手側アドレス：3ffe:192.168:2::2）の IPv6 アドレスファミリを有効にします。

14. **(config-router-af)# neighbor 3ffe:10:1:2::2 activate**
    内部ピア（相手側アドレス：3ffe:10:1:2::2）の IPv6 アドレスファミリを有効にします。

29.2.4 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 3ffe:172:16:2::2 weight 20**
   (config-router-af)# neighbor 3ffe:10:2:2::2 weight 20
   (config-router-af)# neighbor 3ffe:10:1:2::2 weight 10
   (config-router-af)# neighbor 3ffe: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。

29.2.5 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-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。

29.2.6 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，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 3ffe:10:10::/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 3ffe:10:10::/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 3ffe:172:20::/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 3ffe:172:20::/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 3ffe:172:30::/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 3ffe:172:30::/64 の場合，MED 属性値に 100 を設定します。

29.2.7 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，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 3ffe:192:169:10::/64
(config)# ipv6 prefix-list MY_NET_2 seq 10 permit 3ffe:192:169:20::/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 3ffe:192:169:10::/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 3ffe:192:169:20::/64 も広告対象にします。

29.2.8 学習経路フィルタリングの条件の設定

[設定のポイント]

ピアごとに学習フィルタを適用する場合は neighbor in 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 3ffe:172:16:2::2 route-map SET_LOCPREF_IN in
   ピア（相手側アドレス：3ffe:172:16:2::2) から学習した宛先ネットワークが 3ffe:10:10.::/64 の経路の LOCAL_PREF 属性値に 120 を設定し，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 3ffe:10:2:2::2 route-map SET_ASPREPEND_IN in**
   ピア（相手側アドレス：3ffe: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，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 3ffe:10:1:2::2 route-map SET_ORIGIN_IN in**
   ピア（相手側アドレス：3ffe:10:1:2::2) から学習した宛先ネットワークが 3ffe:172:20:0::/64 の経路の ORIGIN 属性に INCOMPLETE を設定し，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 3ffe:192:168:2::2 route-map SET_MED_IN in**
   ピア（相手側アドレス：3ffe:192:168:2::2) から学習した宛先ネットワークが 3ffe:172:30::/64 の経路の MED 属性に 100 を設定します。

29.2.9 広告用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経路フィルタを適用する場合は distribute-list out 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 3ffe:192:169:10::/64 と 3ffe:192:169:20::/64 の経路を広告します。

29.2.10 フィルタ設定の運用への反映

[設定のポイント]

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させるには，運用コマンド clear ipv6 bgp を使用します。

[コマンドによる設定]

1. **# clear ipv6 bgp * both**
   学習経路フィルタと広告経路フィルタを運用に反映させます。

[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・リフレッシュ機能（「29.4.5　ルート・リフレッシュ」参照）の両方を実行します。ルート・リフレッシュ機能の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・リフレッシュ要求は行いませんが経路フィルタの変更は反映します。

29.2.11　VRF での BGP4+ の設定【OP-NPAR】

[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。

29.3 基本機能のオペレーション

29.3.1 運用コマンド一覧

基本機能の運用コマンド一覧を次の表に示します。

表 29-7 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 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，BGP4+ プロトコルに関する情報のクリア，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行います。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。
show processes cpu unicast ※	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 ※	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 ※	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 ※	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※

「運用コマンドレファレンス Vol.3 8. IPv4・IPv6 ルーティングプロトコル共通」を参照してください。

29.3.2 ピアの種別と接続形態の確認

「図 29-9 接続構成例」に対応する表示を以下に示します。ピアの接続情報は運用コマンド show ipv6 bgp 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 neighbors と detail パラメータを指定します。

図 29-10 show ipv6 bgp コマンド（neighbors パラメータ指定）の実行結果

```
> show ipv6 bgp neighbors
Date 2006/03/18 22:45:55 UTC
Peer Address      Peer AS  Local Address     Local AS  Type      Status
3ffe:10:1:2::2    65531    3ffe:10:1:2::1    65531     Internal  Established
3ffe:192:168:2::2 65531    3ffe:192:168:2::1 65531     Internal  Established
3ffe:10:2:2::2    65533    3ffe:10:1:2::1    65531     External  Established
3ffe:172:16:2::2  65532    3ffe:172:16:2::1  65531     External  Established
```

図 29-11 show ipv6 bgp コマンド (neighbors detail パラメータ指定) の実行結果

```
> show ipv6 bgp neighbors detail
Date 2006/03/17 15:52:14 UTC
BGP Peer: 3ffe: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: 2006/03/17 15:51:00
    BGP Version: 4                  Type: Internal
    Local Address: 3ffe: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: <IPv6-Uni Refresh Refresh(v)>
      Send   : <IPv6-Uni Refresh Refresh(v)>
      Receive: <IPv6-Uni Refresh Refresh(v)>
    Password: UnConfigured
BGP Peer: 3ffe: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: 2006/03/17 15:50:43
    BGP Version: 4                  Type: Internal
    Local Address:3ffe: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: <IPv6-Uni Refresh Refresh(v)>
      Send   : <IPv6-Uni Refresh Refresh(v)>
      Receive: <IPv6-Uni Refresh Refresh(v)>
    Password: UnConfigured
BGP Peer: 3ffe: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: 2006/03/17 15:50:30
    BGP Version: 4                  Type: External
    Local Address: 3ffe: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: <IPv6-Uni Refresh>
      Send   : <IPv6-Uni Refresh Refresh(v)>
      Receive: <IPv6-Uni Refresh Refresh(v)>
    Password: UnConfigured
BGP Peer: 3ffe: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: 2006/03/17 15:49:35
    BGP Version: 4                  Type: External
    Local Address:3ffe172:16:2::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: <IPv6-Uni Refresh Refresh(v)>
      Send   : <IPv6-Uni Refresh Refresh(v)>
      Receive: <IPv6-Uni Refresh Refresh(v)>
    Password: UnConfigured
>
```

29.3.3 BGP4+ 経路選択結果の確認

BGP4+ 経路の選択結果は運用コマンド show ipv6 bgp で確認できます。

図 29-12 show ipv6 bgp コマンドの実行結果

```
# show ipv6 bgp
Date 2006/03/18 22:44:23 UTC
Local AS: 65531, Local Router ID: 192.168.1.100
Status Codes: * valid, > active
Origin Codes: i - IGP, e - EGP, ? - incomplete
   Network                                  Next Hop
         MED    LocalPref weight Path
*> 3ffe:10:10::/64                          fe80::200:87ff:fe16:90d5%VLAN0005
         -      120         20     65532 65528 i                          …1
*  3ffe:10:10::/64                          3ffe:10:2:2::2
         -      80          20     65533 65533 65529 i                    …2
*  3ffe:10:10::/64                          3ffe:10:1:2::2
         -      80          10     65534 i                                …3
*> 3ffe:10:20::/64                          fe80::200:87ff:fe16:90d5%VLAN0005
         -      80          20     65532 65528 i                          …4
*  3ffe:10:20::/64                          3ffe:10:2:2::2
         -      80          20     65533 65533 65529 i                    …5
*> 3ffe:172:20::/64                         3ffe:10:1:2::2
         -      100         10     65534 i                                …6
*  3ffe:172:20::/64                         3ffe:192:168:2::2
         -      100         10     65530 ?                                …7
*> 3ffe:172:30::/64                         3ffe:10:1:2::2
         -      100         10     65534 i                                …8
*  3ffe:172:30::/64                         3ffe:192:168:2::2
         100    100         10     65530 i                                …9
*> 3ffe:192:168:10::/64                     3ffe:10:1:2::2
         -      100         10     65534 i                               …10
*  3ffe:192:168:10::/64                     3ffe:192:168:2::2
         -      100         10     65530 i                               …11
*> 3ffe:192:169:10::/64                     3ffe:192:168:2::2
         -      100         10     65530 i                               …12
*> 3ffe:192:169:20::/64                     3ffe:192:168:2::2
         -      100         10     65530 i                               …13
```

1 ～ 3. 3ffe:10:10::/64 の経路選択

weight 値の比較により 1 と 2 が優先され，次に LOCAL_PREF 属性の比較により 1 が選択されています。

4 ～ 5. 3ffe:10:20::/64 の経路選択

AS_PATH 属性長の比較により 4 が選択されています。

6 ～ 7. 3ffe:172:20::/64 の経路選択

ORIGIN 属性の比較により 6 が選択されています。

8 ～ 9. 3ffe:172:30::/64 の経路選択

MED 属性に比較により 8 が選択されています。

10 ～ 11. 3ffe:192:168:10::/64 の経路選択

相手 BGP 識別子の比較により 10 が選択されています。

12 ～ 13. 3ffe:192:169:10::/64, 3ffe:192:169:20::/64 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。

29.3.4 BGP4+ 経路の広告内容の確認

広告した BGP4+ 経路のパス属性を確認する場合は運用コマンド show ipv6 bgp の advertised-routes パラメータ指定を使用します。

図 29-13 show ipv6 bgp コマンド（advertised-routes パラメータ指定）の実行結果

```
> show ipv6 bgp advertised-routes
Date 2006/03/18 22:44:54 UTC
BGP4+ Peer: 3ffe: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
3ffe:192:169:10::/64                       3ffe:192:168:2::2
      120    -         65531 i                                  …1
3ffe:192:169:20::/64                       3ffe:192:168:2::2
      100    -         65531 i
BGP4+ Peer: 3ffe: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
3ffe:192:169:10::/64                       3ffe:192:168:2::2
      120    -         65531 i                                  …2
3ffe:192:169:20::/64                       3ffe: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。

29.4 拡張機能の解説

29.4.1 BGP4+ ピアグループ

BGP4+（IPv6）のピアグループ機能の基本動作は BGP4（IPv4）のピアグループ機能と同様です。詳細は，「12.4.1 BGP4 ピアグループ」を参照してください。

29.4.2 コミュニティ

BGP4+（IPv6）のコミュニティの基本動作は BGP4（IPv4）でのコミュニティと同様です。詳細は，「12.4.2 コミュニティ」を参照してください。

29.4.3 BGP4+ マルチパス

BGP4+（IPv6）でのマルチパスの基本動作は BGP（IPv4）でのマルチパスと同様です。詳細は，「12.4.3 BGP4 マルチパス」を参照してください。

IGP 経路のマルチパス化に伴う BGP4+ マルチパスの注意事項

本装置でマルチパス化を行える 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の概念は，「25 スタティックルーティング（IPv6）」を，OSPFv3 経路のマルチパス化の概念は，「27.1.7 イコールコストマルチパス」を参照してください。

29.4.4 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，BGP4+ コネクション確立時の OPEN メッセージに Capability 情報を付加することによって，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。お互いに広告した Capability 情報で一致する（お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。

本装置では，「IPv6-Unicast 経路の送受信」および「ルート・リフレッシュ (Capability Code：2)」，「ルート・リフレッシュ (Capability Code：128)」，「グレースフル・リスタート (Capability Code：64)」を OPEN メッセージの Capability 情報として常に付加します。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-Unicast 経路の送受信」だけを行います。

ネゴシエーションできる機能を次の表に示します。

表 29-8 ネゴシエーションできる機能

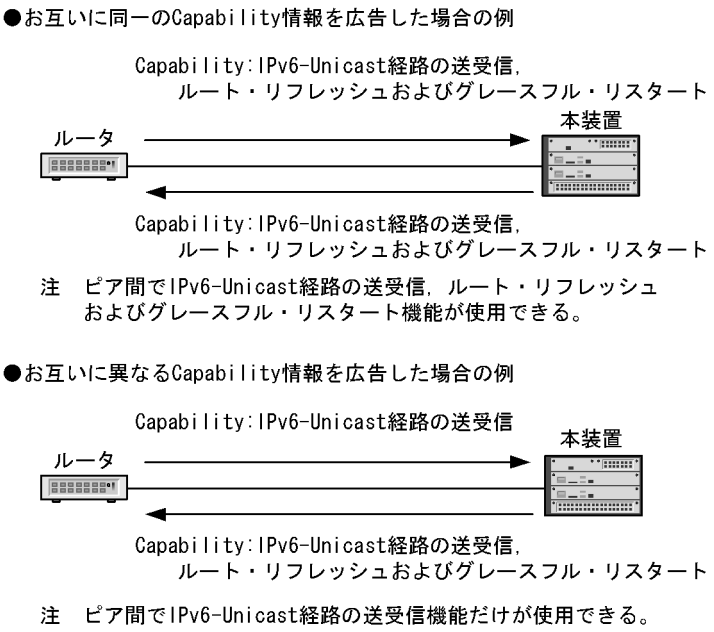
機能名称	OPEN メッセージの Capability 情報	内容
IPv6 経路の送受信	Capability Code：1 Capability Value の AFI：2 Capability Value の SAFI：1	IPv6-Unicast 経路を該当するピア間で送受信します。
ルート・リフレッシュ	Capability Code：2 Capability Value の AFI：2 ※	IPv6 経路のルート・リフレッシュ機能を使用します。
	Capability Code：128 Capability Value の AFI：2 ※	

機能名称	OPEN メッセージの Capability 情報	内容
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・リスタート機能を使用します。

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・リフレッシュ機能を使用できます。

また，ネゴシエーションの動作概念を次の図に示します。

図 29-14　ネゴシエーションの動作概念



29.4.5　ルート・リフレッシュ

ルート・リフレッシュ機能は，変化が発生した経路だけを広告することを基本とする BGP4+ 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・リフレッシュ機能には，自装置側から経路を再広告する機能と BGP4+ 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，clear ipv6 bgp コマンドで実行されます。

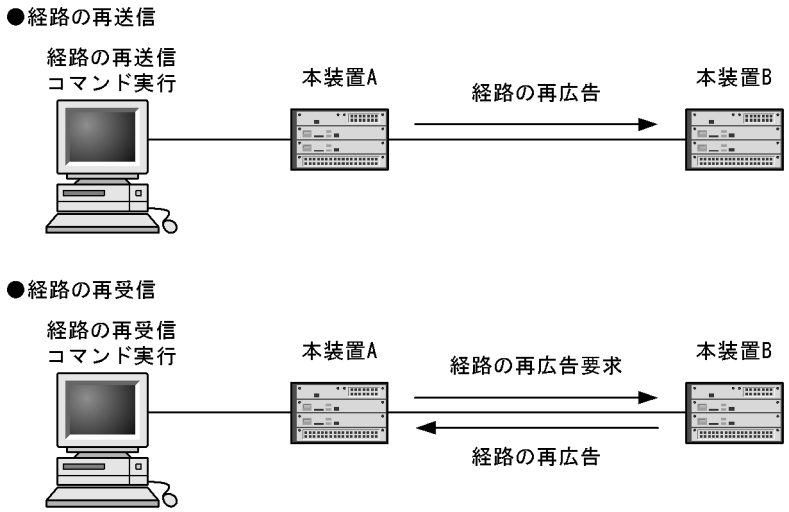
ルート・リフレッシュ機能を次の表に示します。

表 29-9　ルート・リフレッシュ機能

機能種別	経路種別	再広告方向
IPv6-Unicast 経路の再送信	IPv6 ユニキャスト経路	自装置側よりピアリングされた相手装置に経路を再広告します。
IPv6-Unicast 経路の再受信		ピアリングされた相手装置側より自装置に経路を再広告させます。

また，ルート・リフレッシュ機能の動作概念を次の図に示します。

図 29-15　ルート・リフレッシュ機能の動作概念



(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・リフレッシュ機能をサポートしている必要があります。ルート・リフレッシュ機能を使用するためには，BGP4+ ピア確立時にルート・リフレッシュ機能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，相手装置側より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行いません。

本装置のルート・リフレッシュ機能は 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・リフレッシュ機能を使用するときは注意してください。

29.4.6　TCP MD5 認証

BGP4+（IPv6）での TCP MD5 認証の基本動作は BGP4（IPv4）での TCP MD5 認証と同様です。詳細は，「12.4.6　TCP MD5 認証」を参照してください。

29.4.7　BGP4+ 広告用経路生成

BGP4+（IPv6）での広告用経路生成の基本動作は bgp4（IPv4）での広告用経路生成と同様です。詳細は，「12.4.7　BGP4 広告用経路生成」を参照してください。

29.4.8　ルート・フラップ・ダンプニング

BGP4+（IPv6）のルート・フラップ・ダンプニングの基本動作は BGP4（IPv4）のルート・フラップ・ダンプニングと同様です。詳細は，「12.4.8　ルート・フラップ・ダンプニング」を参照してください。

29.4.9 ルート・リフレクション

BGP4+（IPv6）のルート・リフレクションは BGP4（IPv4）のルート・リフレクションと同様です。詳細は,「12.4.9 ルート・リフレクション」を参照してください。

29.4.10 コンフェデレーション

BGP4+（IPv6）のコンフェデレーションの基本動作は BGP4（IPv4）のコンフェデレーションと同様です。詳細は,「12.4.10 コンフェデレーション」を参照してください。

29.4.11 グレースフル・リスタート

BGP4+（IPv6）のグレースフル・リスタートの基本動作は BGP4（IPv4）のグレースフル・リスタートと同様です。詳細は,「12.4.11 グレースフル・リスタート」を参照してください。

29.4.12 BGP4+ 学習経路数制限

BGP4+（IPv6）での学習経路数制限の基本動作は BGP4（IPv4）での学習経路数制限と同様です。詳細は,「12.4.12 BGP4 学習経路数制限」を参照してください。

29.5 拡張機能のコンフィグレーション

29.5.1 BGP4+ ピアグループのコンフィグレーション

(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 29-10 コンフィグレーションコマンド一覧

コマンド名	説明
neighbor 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）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）を設定します。

[コマンドによる設定]

1. **(config-router)# neighbor 3ffe: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：3ffe: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 3ffe: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：3ffe: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 3ffe:192:168:4::4 remote-as 65533**
   (config-router)# neighbor 3ffe:192:168:4::4 peer-group EXTERNAL-GROUP
   ピア（相手側アドレス：3ffe:192:168:4::4）を設定し，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 3ffe:192:168:5::5 remote-as 65534**
   (config-router)# neighbor 3ffe:192:168:5::5 peer-group EXTERNAL-GROUP
   ピア（相手側アドレス：3ffe:192:168:5::5）を設定し，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。

29.5.2 コミュニティのコンフィグレーション

(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 29-11 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用いる経路フィルタを指定します。

コマンド名	説明
distribute-list out（BGP4+）※	BGP4+ の広告経路フィルタリングの条件として用い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用い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用い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　14. 経路フィルタリング（IPv4 ／ IPv6 共通）」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 属性を付加する場合，該当するピアにコンフィグレーションコマンド neighbor send-community 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 3ffe:192:168:2::2 remote-as 65531
   (config-router)# neighbor 3ffe:172:16:2::2 remote-as 65532
   (config-router)# neighbor 3ffe:10:2:2::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 3ffe:172:16:2::2 send-community**
   (config-router-af)# neighbor 3ffe:10:2:2::2 send-community
   (config-router-af)# exit
   (config-router)# exit
   ピアに広告する BGP4+ 経路に COMMUNITIES 属性を付加す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，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 3ffe:192:168::/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 3ffe:192:168::/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
```
全ピアの学習経路フィルタと全ピアの広告経路フィルタを設定します。

7.
```
(config-router-af)# neighbor 3ffe:192:168:2::2 activate
(config-router-af)# neighbor 3ffe:172:16:2::2 activate
(config-router-af)# neighbor 3ffe:10:2:2::2 activate
```
IPv6 アドレスファミリを有効にします。

(3) フィルタ設定の運用への反映

[設定のポイント]

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経路フィルタを運用に反映させるには運用コマンド clear ipv6 bgp を使用します。

[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させます。

29.5.3 BGP4+ マルチパスのコンフィグレーション

(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 29-12 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 に all-as パラメータを指定する場合はあらかじめ bgp always-compare-med 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 3ffe:172:16:2::2 remote-as 65532
   (config-router)# neighbor 3ffe: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。本例では 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 3ffe:172:16:2::2 activate**
   (config-router-af)# neighbor 3ffe:172:17:2::2 activate
   IPv6 アドレスファミリを有効にします。

29.5.4 TCP MD5 認証のコンフィグレーション

(1) コンフィグレーションコマンド一覧

TCP MD5 認証（BGP4+）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 29-13 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 認証はコンフィグレーションコマンド neighbor password 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 3ffe:172:16:2::2 remote-as 65532
   (config-router)# neighbor 3ffe:192:168:2::2 remote-as 65531
   BGP4+ ピアを設定します。

2. **(config-router)# neighbor 3ffe:172:16:2::2 password "authmd5_65532"**
   相手側アドレスが 3ffe: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。

3. **(config-router)# address-family ipv6**
   config-router-af（ipv6）モードへ移行します。

4. **(config-router-af)# neighbor 3ffe:172:16:2::2 activate**
   (config-router-af)# neighbor 3ffe:192:168:2::2 activate
   IPv6 アドレスファミリを有効にします。

29.5.5 BGP4+ 広告用経路生成のコンフィグレーション

(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 29-14 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+ の広告用経路を生成することを設定します。

(2) BGP4+ 広告用経路生成の設定

[設定のポイント]

BGP4+ 広告用経路を生成するにはコンフィグレーションコマンド network を使用します。network コマンドで生成した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 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 192.168.1.100
   (config-router)# neighbor 3ffe:172:16:2::2 remote-as 65532
   (config-router)# neighbor 3ffe:192:168:2::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)# network 3ffe:192:169:10::/64**
   (config-router-af)# exit
   ルーティングテーブルに 3ffe:192:169:10::/64 の経路がある場合に 3ffe:192:169:10::/64 の BGP4+ 広告用経路を生成します。

4. **(config)# route-map ADV_NET permit 10**
   (config-route-map)# match route-type local

```
(config-route-map)# exit
```
生成した BGP4+ 広告用経路を指定します。

5.
```
(config)# route-map ADV_NET deny 20
(config-route-map)# match protocol bgp
(config-route-map)# exit
```
BGP プロトコルを指定します。

6.
```
(config)# router bgp 65531
(config-router)# address-family ipv6
(config-router-af)# neighbor 3ffe:172:16:2::2 route-map ADV_NET out
```
相手側アドレスが 3ffe:172:16:2::2 のピアへ生成した 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。

7.
```
(config)# route-map DENY_NET deny 10
(config-route-map)# match route-type local
(config-route-map)# exit
```
生成した BGP4+ 広告用経路を指定します。

8.
```
(config)# router bgp 65531
(config-router)# address-family ipv6
(config-router-af)# neighbor 3ffe:192:168:2::2 route-map DENY_NET out
```
相手側アドレスが 3ffe:192:168:2::2 のピアへ生成した BGP4+ 広告用経路を広告しないことを指定します。

9.
```
(config-router-af)# neighbor 3ffe:172:16:2::2 activate
(config-router-af)# neighbor 3ffe:192:168:2::2 activate
```
IPv6 アドレスファミリを有効にします。

(3) フィルタ設定の運用への反映

[設定のポイント]

生成した BGP4+ 広告用経路を広告するには運用コマンド clear ipv6 bgp を使用し，フィルタを運用に反映させます。

[コマンドによる設定]

1.
```
# clear ipv6 bgp * out
```
BGP4+ 広告用経路を指定した経路フィルタを運用に反映させます。

29.5.6 ルート・フラップ・ダンプニングのコンフィグレーション

(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 29-15 コンフィグレーションコマンド一覧

コマンド名	説明
bgp 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，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 3ffe:172:16:2::2 remote-as 65532
   (config-router)# neighbor 3ffe:172:17:2::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。

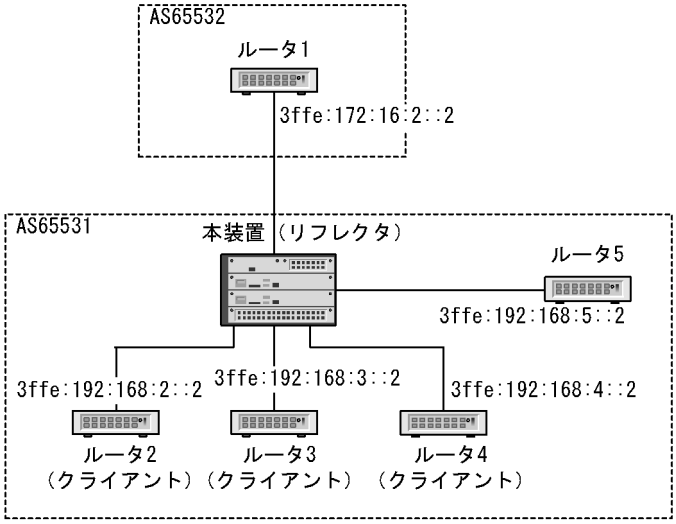
3. **(config-router-af)# bgp dampening**
   ルート・フラップ・ダンプニングを適用します。

4. **(config-router-af)# neighbor 3ffe:172:16:2::2 activate**
   (config-router-af)# neighbor 3ffe:172:17:2::2 activate
   IPv6 アドレスファミリを有効にします。

29.5.7 ルート・リフレクション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 29-16 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 29-16 コンフィグレーションコマンド一覧

コマンド名	説明
bgp 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の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になっている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 3ffe:172:16:2::2 remote-as 65532
   (config-router)# neighbor 3ffe:192:168:2::2 remote-as 65531
   (config-router)# neighbor 3ffe:192:168:3::2 remote-as 65531
   (config-router)# neighbor 3ffe:192:168:4::2 remote-as 65531
   (config-router)# neighbor 3ffe: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，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。

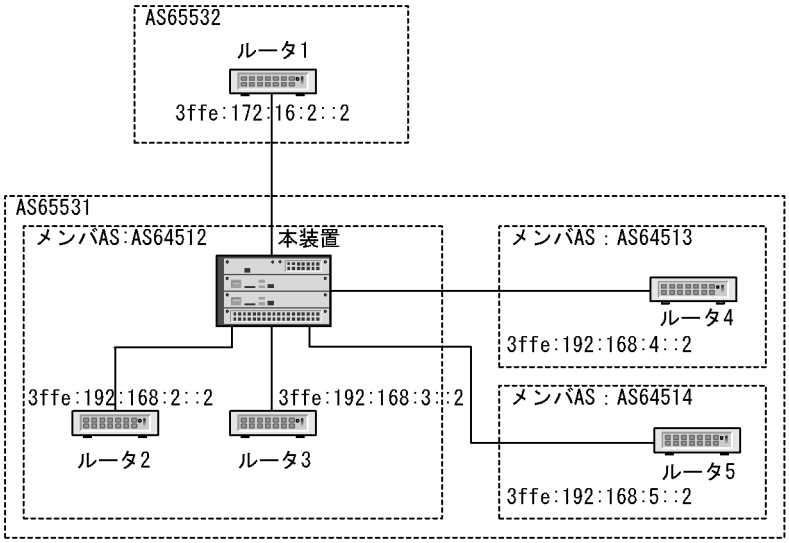
4. **(config-router-af)# neighbor 3ffe:192:168:2::2 route-reflector-client**
   (config-router-af)# neighbor 3ffe:192:168:3::2 route-reflector-client
   (config-router-af)# neighbor 3ffe:192:168:4::2 route-reflector-client
   ルータ 2，ルータ 3，ルータ 4 をルート・リフレクタ・クライアントに指定します。

5. **(config-router-af)# neighbor 3ffe:172:16:2::2 activate**
   (config-router-af)# neighbor 3ffe:192:168:2::2 activate
   (config-router-af)# neighbor 3ffe:192:168:3::2 activate
   (config-router-af)# neighbor 3ffe:192:168:4::2 activate
   (config-router-af)# neighbor 3ffe:192:168:5::2 activate
   IPv6 アドレスファミリを有効にします。

29.5.8 コンフェデレーション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 29-17 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 29-17 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/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 で指定し，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**
   接続する他のメンバー AS 番号（64513，64514）を指定します。

5. **(config-router)# neighbor 3ffe:172:16:2::2 remote-as 65532**
   (config-router)# neighbor 3ffe:192:168:2::2 remote-as 64512
   (config-router)# neighbor 3ffe:192:168:3::2 remote-as 64512
   (config-router)# neighbor 3ffe:192:168:4::2 remote-as 64513
   (config-router)# neighbor 3ffe:192:168:5::2 remote-as 64514
   ルータ 1 を外部ピア，ルータ 2，ルータ 3 を内部ピア，ルータ 4，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 3ffe:172:16:2::2 activate**
   (config-router-af)# neighbor 3ffe:192:168:2::2 activate
   (config-router-af)# neighbor 3ffe:192:168:3::2 activate
   (config-router-af)# neighbor 3ffe:192:168:4::2 activate
   (config-router-af)# neighbor 3ffe:192:168:5::2 activate
   IPv6 アドレスファミリを有効にします。

29.5.9 グレースフル・リスタートのコンフィグレーション

(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 29-18 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・リスタート機能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 8. ルーティングオプション（IPv4)」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・リスタート機能を使用する場合は，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 3ffe:172:16:2::2 remote-as 65532
   (config-router)# neighbor 3ffe: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。

3. **(config-router)# address-family ipv6**
   config-router-af（ipv6）モードへ移行します。

4. **(config-router-af)# neighbor 3ffe:172:16:2::2 activate**
   (config-router-af)# neighbor 3ffe:192:168:2::2 activate
   IPv6 アドレスファミリを有効にします。

29.5.10 BGP4+ 学習経路数制限のコンフィグレーション

(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 29-19 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 3ffe:172:16:2::2 remote-as 65532
   (config-router)# neighbor 3ffe:192:168:2::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 3ffe:172:16:2::2 maximum-prefix 1000 80 restart 60**
   外部ピア（相手側アドレス：3ffe:172:16:2::2）から学習する経路数の上限値を 1000 経路，警告の運用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 3ffe:192:168:2::2 maximum-prefix 100 warning-only**
   内部ピア（相手側アドレス：3ffe:172:16:2::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 3ffe:172:16:2::2 activate**
   (config-router-af)# neighbor 3ffe:192:168:2::2 activate
   IPv6 アドレスファミリを有効にします。

29.6　拡張機能のオペレーション

29.6.1　BGP4+ ピアグループの確認

(1) 運用コマンド一覧

BGP4+ 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 29-20　運用コマンド一覧

コマンド名	説明
show ipv6 bgp	BGP4+ プロトコルに関する情報を表示します。

(2) BGP4+ 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の確認は show ipv6 bgp コマンドで peer-group パラメータを指定します。

図 29-18　show ipv6 bgp コマンド（peer-group パラメータ指定）の実行結果

```
>show ipv6 bgp peer-group INTERNAL-GROUP
Date 2006/07/17 18:40:00 UTC
Local AS: 65531, Local Router ID: 172.16.2.100
BGP4+ Peer                                  AS     Received   Sent
Up/Down            Status
3ffe:172:16:2::2                            65531  36         42
2006/07/16 18:42:26  Established
3ffe:172:17:3::3                            65531  51         63
2006/07/16 12:42:31  Established
```

(3) BGP4+ 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を表示するには show ipv6 bgp コマンドで neighbors パラメータ，および peer-group，detail パラメータを指定します。

図 29-19　show ipv6 bgp コマンド（neighbors，peer-group パラメータ指定）の実行結果

```
>show ipv6 bgp neighbors EXTERNAL-GROUP
Date 2006/07/17 18:45:09 UTC
Peer Address                                 Peer AS  Local Address
             Local AS Type      Status
3ffe:192:168:4::4                            65533    3ffe:192:168:4::214
             65531    External  Established
3ffe:192:168:5::5                            65534    3ffe:192:168:5::189
             65531    External  Active
```

(4) ピアが所属する BGP4+ ピアグループの確認

ピアが所属するピアグループの確認は show ipv6 bgp コマンドで neighbors パラメータ，および <Peer Address>，<Host name> パラメータを指定します。

図 29-20 show ipv6 bgp コマンド（neighbors，<Peer Address> パラメータ指定）の実行結果

```
>show ipv6 bgp neighbors 3ffe:172:16:2::2
Date 2006/07/17 18:45:09 UTC
BGP4+ Peer: 3ffe:172:16:2::2, Remote AS: 65531
Remote Router ID: 172.16.2.20, Peer Group: INTERNAL-GROUP                    …1
    BGP4+ Status:Established        HoldTime: 90   , Keepalive: 30
    Established Transitions: 1      Established Date: 2006/07/16 18:42:26
    BGP4+ Version: 4                Type: Internal
    Local Address: 3ffe: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
    BGP4+ Message  UpdateIn UpdateOut TotalIn TotalOut
                   12       14        36      42
    BGP4+ Capability Negotiation: <Refresh Refresh(v) IPv6-Uni>
      Send   : <Refresh Refresh(v) IPv6-Uni>
      Receive: <Refresh Refresh(v) IPv6-Uni>
    Password : UnConfigured
```

1. ピアグループ INTERNAL-GROUP に所属しています。

29.6.2 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 29-21 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。
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の表示

「29.5.2 コミュニティのコンフィグレーション」に対応する表示を以下に示します。

特定のコミュニティを持つ経路を表示する場合は show ipv6 bgp コマンドの community パラメータ指定を使用します。

図 29-21 show ipv6 bgp コマンド（community パラメータ指定）の実行結果

```
> show ipv6 bgp community 1000:1002
Date 2006/03/20 21:00:00 UTC
Local AS: 65531, Local Router ID: 192.168.1.100
Status Codes: d dampened, * valid, > active, S Stale
Origin Codes: i - IGP, e - EGP, ? - incomplete
   Network                                NextHop
            MED   LocalPref   Weight   Path
*> 3ffe:10:10::/64                      fe80::200:87ff:fe16:90d5%VLAN0005
            -     100         0        65532 i
*> 3ffe:10:20::/64                      fe80::200:87ff:fe16:90d5%VLAN0005
            -     100         0        65532 i
```

経路が持つコミュニティを表示する場合は show ipv6 bgp コマンドの route パラメータ指定を使用します。

図 29-22 show ipv6 bgp コマンド（route パラメータ指定）の実行結果

```
> show ipv6 bgp route 3ffe:10:10::/64
Date 2006/03/20 21:09:12 UTC
BGP Peer: 3ffe:172:16:2::2  , Remote AS: 65532
Local AS: 65531, Local Router ID: 192.168.1.100
Status Codes: * valid, > active
Route 3ffe:10:10::/64
*> Next Hop fe80::200:87ff:fe16:90d5%VLAN0005
     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フィルタリング結果は運用コマンド show ipv6 bgp を使用して表示します。

図 29-23 show ipv6 bgp コマンドの実行結果

```
> show ipv6 bgp
Date 2006/03/20 21:10:09 UTC
Local AS: 65531, Local Router ID: 192.168.1.100
Status Codes: * valid, > active
Origin Codes: i - IGP, e - EGP, ? - incomplete
   Network                                 Next Hop
         MED    LocalPref weight  Path
*> 3ffe:10:10::/64                         fe80::200:87ff:fe16:90d5%VLAN0005
         -      120       0       65532 i
*  3ffe:10:10::/64                         3ffe:10:2:2::2
         -      80        0       65533 i
*> 3ffe:10:20::/64                         fe80::200:87ff:fe16:90d5%VLAN0005
         -      120       0       65532 i
*  3ffe:10:20::/64                         3ffe:10:2:2::2
         -      80        0       65533 i
*> 3ffe:192:169:10::/64                    3ffe:192:168:2::2
         -      100       0       i
*> 3ffe:192:169:20::/64                    3ffe:192:168:2::2
         -      100       0       i
```

(4) 広告経路のコミュニティの表示

広告した BGP4+ 経路の COMMUNITIES 属性は運用コマンド show ipv6 bgp コマンドの advertised-routes パラメータ指定を使用して表示します。

図 29-24 show ipv6 bgp コマンド（advertised-routes パラメータ指定）の実行結果

```
> show ipv6 bgp advertised-routes 3ffe:192:169:10::/64
Date 2006/03/18 22:44:54 UTC
BGP Peer: 3ffe:10:2:2::2     , Remote AS: 65533
Local AS: 65531, Local Router ID: 192.168.1.100
Route 3ffe:192:169:10::/64
*> Next Hop 3ffe:192:168:2::2
     MED: -, LocalPref: -, Type: Internal route
     Origin: IGP
     Path: 65531
     Next Hop Attribute: 3ffe:10:1:2::1
     Communities: 1000:1001

BGP Peer: 3ffe:172:16:2::2  , Remote AS: 65532
Local AS: 65531, Local Router ID: 192.168.1.100
Route 3ffe:192:169:10::/64
*> Next Hop 3ffe:192:168:2::2
     MED: -, LocalPref: - , Type: Internal route
     Origin: IGP
     Path: 65531
     Next Hop Attribute: 3ffe:172:16:2::1
                         fe80::200:87ff:fe21:90da
    Communities: 1000:1001
```

29.6.3 BGP4+ 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 29-22 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の経路を表示します。
show ipv6 bgp	BGP4+ プロトコルに関する情報を表示します。

(2) BGP4+ マルチパスの表示

「29.5.3 BGP4+ マルチパスのコンフィグレーション」に対応した表示内容を以下に示します。マルチパスの設定は運用コマンド show ipv6 route を使用して表示します。

図 29-25 show ipv6 route コマンドの実行結果

```
> show ipv6 route
Date 2006/03/28 21:47:11 UTC
Total: 13 routes
Destination           Next Hop           Interface  Metric Protocol  Age
::1/128               ::1                localhost  0/0    Connected 10m 51s
3ffe:10:10::/64       fe80::5%VLAN0005   VLAN0005   -/-    BGP4+      4m 50s…1
                      fe80::6%VLAN0006   VLAN0006    -      -         -
3ffe:10:20::/64       fe80::5%VLAN0005   VLAN0005   -/-    BGP4+      4m 50s…2
                      fe80::6%VLAN0006   VLAN0006   -/-    BGP4+      4m 56s
3ffe:172:16::/64      3ffe:172:16:2::2   VLAN0007   0/0    Connected 10m 49s
3ffe:172:16:2::2/128  ::1                localhost  0/0    Connected 10m 49s
3ffe:172:17::/64      3ffe:172:17:2::2   VLAN0005   0/0    Connected 10m 49s
3ffe:172:17:2::2/128  ::1                localhost  0/0    Connected 10m 49s
3ffe:172:10::/64      fe80::5%VLAN0005   VLAN0005   -/-    BGP4+      4m 50s…3
                      fe80::6%VLAN0006   VLAN0006   -/-    BGP4+      4m 56s
3ffe:172:20::/64      fe80::5%VLAN0005   VLAN0005   -/-    BGP4+      4m 50s…4
                      fe80::6%VLAN0006   VLAN0006    -      -         -
3ffe:192:168:2::/64   3ffe:192:168:2::2  VLAN0006   0/0    Connected 10m 48s
3ffe:192:168:2::2     ::1                localhost  0/0    Connected 10m 48s
```

1 ～ 4：マルチパス化された経路です。

29.6.4 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 29-23 運用コマンド一覧

コマンド名	説明
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運用コマンド show ipv6 bgp コマンドの neighbors と detail パラメータを指定して表示します。

図 29-26　show ipv6 bgp コマンド（neighbors detail パラメータ指定）の実行結果

```
> show ipv6 bgp neighbors detail
Date 2006/03/17 15:52:14 UTC
BGP Peer: 3ffe: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: 2006/03/17 15:51:00
    BGP Version: 4                  Type: Internal
    Local Address: 3ffe: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: <IPv6-Uni Refresh Refresh(v)>            …1
      Send   : <IPv6-Uni Refresh Refresh(v)>
      Receive: <IPv6-Uni Refresh Refresh(v)>
    Password: UnConfigured
BGP Peer: 3ffe: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: 2006/03/17 15:50:43
    BGP Version: 4                  Type: Internal
    Local Address:3ffe: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: <IPv6-Uni Refresh>                       …2
      Send   : <IPv6-Uni Refresh Refresh(v)>
      Receive: <IPv6-Uni Refresh >
    Password: UnConfigured
BGP Peer: 3ffe: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: 2006/03/17 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: <IPv6-Uni>                               …3
      Send   : <IPv6-Uni Refresh Refresh(v)>
      Receive: <IPv6-Uni>
    Password: UnConfigured
BGP Peer: 3ffe: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: 2006/03/17 15:49:35
    BGP Version: 4                  Type: External
    Local Address:3ffe: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   : <IPv6-Uni Refresh Refresh(v)>
      Receive: <>
    Password: UnConfigured
>
```

1. IPv6-Uni:「IPv6-Unicast 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. IPv6-Uni:「IPv6-Unicast 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. IPv6-Uni:「IPv6-Unicast 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。

29.6.5 ルート・リフレッシュ機能の確認

(1) 運用コマンド一覧

ルート・リフレッシュ機能の運用コマンド一覧を次の表に示します。

表 29-24 運用コマンド一覧

コマンド名	説明
clear ipv6 bgp	BGP4+ セッション，BGP4+ プロトコルに関する情報のクリア，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行います。
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 bgp	BGP4+ プロトコルに関する情報を表示します。

(2) ルート・リフレッシュ機能のネゴシエーション確認

最初に運用コマンド show ipv6 bgp の neighbors パラメータ指定で，BGP4+ 経路の再広告要求を行う BGP4+ ピア間でルート・リフレッシュ機能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行いません。

図 29-27 show ipv6 bgp コマンド（neighbors パラメータ）の実行結果

```
> show ipv6 bgp neighbors 3ffe:172:16:2::2
Date 2006/03/17 16:52:14 UTC
BGP Peer: 3ffe: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: 2006/03/17 16:49:35
    BGP Version: 4                  Type: External
    Local Address: 3ffe:172:16:2::1    Local AS: 65531
    Local Router ID: 192.168.1.100
    Next Connect Retry: -           Connect Retry Timer: -
    Last Keep Alive Sent: 16:51:35  Last Keep Alive Received: 16:51:35
    BGP Message  UpdateIn   UpdateOut  TotalIn    TotalOut
                 1          1          4          6
    BGP Capability Negotiation: <IPv6-Uni Refresh Refresh(v)>     …1
      Send   : <IPv6-Uni Refresh Refresh(v)>
      Receive: <IPv6-Uni Refresh Refresh(v)>
    Password: UnConfigured
```

1. ルート・リフレッシュ機能のネゴシエーションが成立しています。

(3) BGP4+ 経路の再広告要求と再広告

全 BGP4+ ピアに対して BGP4+ 経路の再広告要求と再広告を行う場合は運用コマンド clear ipv6 bgp の * both パラメータ指定を使用します。

図 29-28 clear ipv6 bgp コマンドの実行結果

```
#clear ipv6 bgp * both
```

(4) BGP4+ 経路再学習と再広告の確認

ルート・リフレッシュ機能による BGP4+ 経路の再学習と再広告を確認する場合は show ipv6 bgp コマンドの neighbors パラメータ指定を使用します。

図 29-29 show ipv6 bgp コマンド（neighbors パラメータ指定）の実行結果

```
> show ipv6 bgp neighbors 3ffe:172:16:2::2
Date 2006/03/17 16:52:14 UTC
BGP Peer: 3ffe: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: 2006/03/17 16:49:35
    BGP Version: 4                  Type: External
    Local Address: 3ffe:172:16:2::1    Local AS: 65531
    Local Router ID: 192.168.1.100
    Next Connect Retry: -           Connect Retry Timer: -
    Last Keep Alive Sent: 16:51:35  Last Keep Alive Received: 16:51:35
    BGP Message  UpdateIn   UpdateOut  TotalIn    TotalOut
                 2          2          11          14                ···1
    BGP Capability Negotiation: <IPv6-Uni Refresh Refresh(v)>
      Send   : <IPv6-Uni Refresh Refresh(v)>
      Receive: <IPv6-Uni Refresh Refresh(v)>
    Password: UnConfigured
```

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]

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・リフレッシュ機能（「29.4.5 ルート・リフレッシュ」参照）の両方を実行します。ルート・リフレッシュ機能の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・リフレッシュ要求は行いませんが経路フィルタの変更は反映します。

29.6.6 TCP MD5 認証の確認

(1) 運用コマンド一覧

TCP MD5 認証（BGP4+）の運用コマンド一覧を次の表に示します。

表 29-25 運用コマンド一覧

コマンド名	説明
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 認証は運用コマンド show ipv6 bgp で neighbors と detail パラメータを指定して表示します。

図 29-30 show ipv6 bgp コマンド（neighbors detail パラメータ指定）の実行結果

```
> show ipv6 bgp neighbor detail
Date 2006/03/07 21:24:24 UTC
BGP Peer: 3ffe: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: 2006/03/07 21:23:48
    BGP Version: 4                  Type: Internal
    Local Address:3ffe: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: <IPv6-Uni Refresh Refresh(v)>
      Send   : <IPv6-Uni Refresh Refresh(v)>
      Receive: <IPv6-Uni Refresh Refresh(v)>
    Password: UnConfigured                                          …1

BGP Peer: 3ffe: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: 2006/03/07 21:23:58
    BGP Version: 4                  Type: External
    Local Address:3ffe: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: <IPv6-Uni Refresh Refresh(v)>>
      Send   : <IPv6-Uni Refresh Refresh(v)>
      Receive: <IPv6-Uni Refresh Refresh(v)>
    Password: Configured                                            …2
```

1. ピアアドレス：3ffe:192:168:2::2 のピアとの接続で MD5 認証を適用していません。
2. ピアアドレス：3ffe:172:16:2::2 のピアとの接続で 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ログメッセージを確認してください。

29.6.7 BGP4+ 広告用経路生成の確認

(1) 運用コマンド一覧

BGP4+ 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 29-26 運用コマンド一覧

コマンド名	説明
show ipv6 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経路情報を表示します。

(2) BGP4+ 広告用経路の確認

(a) 生成した広告用経路の表示

生成した BGP4+ 広告用経路は運用コマンド show ipv6 bgp で表示します。本例では 3ffe:173:16::/48 と 3ffe:192:169:10::/64 が生成した BGP4+ 広告用経路です。

図 29-31 show ipv6 bgp コマンドの実行結果

```
> show ipv6 bgp
Date 2006/03/20 22:43:26 UTC
Local AS: 65531, Local Router ID: 192.168.1.100
Status Codes: * valid, > active
Origin Codes: i - IGP, e - EGP, ? - incomplete
   Network                Next Hop        MED    LocalPref Weight Path
*  3ffe:173:16::/48       ----            -      100       0      i
*  3ffe:192:169:10::/64   ----            -      100       0      i
```

(b) 広告用経路の広告表示

生成した BGP4+ 広告用経路が広告されていることを確認する場合は運用コマンド show ipv6 bgp の advertised-routes パラメータ指定を使用します。

図 29-32 show ipv6 bgp コマンド（advertised-routes パラメータ指定）の実行結果

```
> show ipv6 bgp advertised-routes 3ffe:173:16::/48
Date 2006/03/29 18:08:54 UTC
BGP4+ Peer: 3ffe:172:16:2::2, Remote AS: 65532
Local AS: 65531, Local Router ID: 192.168.1.100
Route 3ffe:173:16::/48
*  Next Hop ----
     MED: -, LocalPref: -,   Type: Internal route
     Origin: IGP
     Path:65531
     Next Hop Attribute: 3ffe:172:16:2::1

> show ipv6 bgp advertised-routes 3ffe:192:169:10::/64
BGP4+ Peer: 3ffe:172:16:2::2, Remote AS: 65532
Local AS: 65531, Local Router ID: 192.168.1.100
Route 3ffe: 3ffe:192:169:10::/64
*  Next Hop ----
     MED: -, LocalPref: -, Type: Internal route
     Origin: IGP
     Path:65531
     Next Hop Attribute: 3ffe:172:16:2::1
```

29.6.8 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・ダンプニング機能の運用コマンド一覧を次の表に示します。

表 29-27 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。
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・ダンプニングにより抑止されている経路を表示する場合は，運用コマンド show ipv6 bgp の dampend-routes パラメータ（グローバルネットワークだけ）を指定します。

図 29-33 show ipv6 bgp コマンド（dampend-routes パラメータ指定）の実行結果

```
>show ipv6 bgp neighbor 3ffe:172:16:2::2 dampened-routes
Status Codes: d dampened, h history, * valid, > active
   Network                                       Peer Address
     ReUse
 d 3ffe:172:21:211::/64                          3ffe:172:16:2::2
     00:07:11
 d 3ffe:172:21:212::/64                          3ffe:172:16:2::2
     00:19:10
```

フラップ状態を表示する場合は，運用コマンド show ipv6 bgp の flap-statistics パラメータ（グローバルネットワークだけ）を指定します。

図 29-34 show ipv6 bgp コマンド（flap-statistics パラメータ指定）の実行結果

```
>show ipv6 bgp flap-statistics
Status Codes: d dampened, h history, * valid, > active
   Network                                       Peer Address
          Flaps      Duration ReUse    Penalty
 d 3ffe:172:21:211::/64                          3ffe:172:16:2::2
          114        00:12:30 00:07:11 5.0
 d 3ffe:172:21:212::/64                          3ffe:172:16:2::2
          108        00:12:30 00:19:10 4.0
 h 3ffe:172:27:119::/64                          3ffe:192:168:2::2
          2          00:11:20          1.7
 h 3ffe:172:27:191::/64                          3ffe:192:168:2::2
          2          00:11:20          1.7
*> 3ffe:172:30:189::/64                          3ffe:192:168:79:188
          1          00:05:10          0.6
*> 3ffe:172:30:192::/64                          3ffe:192:168:79:188
          3          00:05:10          0.6
>
```

29.6.9 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・リフレクション機能の運用コマンド一覧を次の表に示します。

表 29-28 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。
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・リフレクション・クライアントを表示する場合は，運用コマンド show ipv6 bgp の neighbors パラメータと detail パラメータを指定します。

図 29-35 show ipv6 bgp コマンド（neighbors，detail パラメータ指定）の実行結果

```
> show ipv6 bgp neighbors detail
Date 2006/03/17 15:52:14 UTC
BGP Peer: 3ffe: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: 2006/03/17 15:51:00
    BGP Version: 4                   Type: Internal RRclient              …1
    Local Address: 3ffe: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   : <IPv6-Uni Refresh Refresh(v)>
      Receive: <IPv6-Uni Refresh Refresh(v)>
    Password: UnConfigured

BGP Peer: 3ffe:192:168:3::2    , Remote AS: 65531
Remote Router ID: 192.168.1.103
    BGP Status: Established         Holdtime: 180  , Keepalive: 60
    Established Transitions: 1      Established Date: 2006/03/17 15:50:43
    BGP Version: 4                  Type: Internal RRclient              …1
    Local Address: 3ffe:192:168:3::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   : <IPv6-Uni Refresh Refresh(v)>
      Receive: <IPv6-Uni Refresh Refresh(v)>
    Password: UnConfigured

BGP Peer: 3ffe:192:168:4::2    , Remote AS: 65531
Remote Router ID: 192.168.1.104
    BGP Status: Established         Holdtime: 180  , Keepalive: 60
    Established Transitions: 1      Established Date: 2006/03/17 15:50:30
    BGP Version: 4                  Type: Internal RRclient              …1
    Local Address: 3ffe:192:168:4::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 Refresh>
      Send   : <IPv6-Uni Refresh Refresh(v)>
      Receive: <IPv6-Uni Refresh Refresh(v)>
    Password: UnConfigured

BGP Peer: 3ffe: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: 2006/03/17 15:49:35
    BGP Version: 4                  Type: External
    Local Address: 3ffe: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: <IPv4-Uni Refresh Refresh(v)>
      Send   : <IPv6-Uni Refresh Refresh(v)>
      Receive: <IPv6-Uni Refresh Refresh(v)>
```

```
    Password: UnConfigured
>
```

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を表示する場合は，運用コマンド show ipv6 bgp の advertised-routes パラメータを指定します。

図 29-36　show ipv6 bgp コマンド（advertised-routes パラメータ指定）の実行結果

```
> show ipv6 bgp advertised-routes
Date 2006/01/18 22:44:54 UTC
BGP Peer: 3ffe: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
3ffe:192:169:10::/64                    3ffe:192:168:2::2
         120    100      i
3ffe:192:169:20::/64                    3ffe:192:168:2::2
         100    100      i
BGP Peer: 3ffe: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
3ffe:192:169:10::/64                    3ffe:192:168:2::2
         120    100      i
3ffe:192:169:20::/64                    3ffe:192:168:2::2
         100    100      i
```

29.6.10　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機能の運用コマンド一覧を次の表に示します。

表 29-29　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。
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を表示する場合は，運用コマンド show ipv6 bgp の neighbors パラメータと detail パラメータを指定します。

図 29-37　show ipv6 bgp コマンド（neighbors，detail パラメータ指定）の実行結果

```
> show ipv6 bgp neighbors detail
Date 2006/03/17 15:52:14 UTC
BGP Peer: 3ffe: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: 2006/03/17 15:51:00
    BGP Version: 4                  Type: Internal
    Local Address: 3ffe: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: <IPv6-Uni Refresh Refresh(v)>
      Send   : <IPv6-Uni Refresh Refresh(v)>
      Receive: <IPv6-Uni Refresh Refresh(v)>
    Password: UnConfigured

Confederation ID: 65531, Member AS: 64512                                 …1
BGP Peer: 3ffe: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: 2006/03/17 15:50:30
    BGP Version: 4                  Type: ConfedExt                       …3
    Local Address: 3ffe: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: <IPv6-Uni Refresh>
      Send   : <IPv6-Uni Refresh Refresh(v)>
      Receive: <IPv6-Uni Refresh Refresh(v)>
    Password: UnConfigured

Confederation ID: 65531, Member AS: 64512                                 …1
BGP Peer: 3ffe:192:168:5::2    , Remote AS: 64514                         …2
Remote Router ID: 192.168.1.104
    BGP Status: Established         Holdtime: 180  , Keepalive: 60
    Established Transitions: 1      Established Date: 2006/03/17 15:50:30
    BGP Version: 4                  Type: ConfedExt                       …3
    Local Address: 3ffe:192:168:5::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: <IPv6-Uni Refresh>
      Send   : <IPv6-Uni Refresh Refresh(v)>
      Receive: <IPv6-Uni Refresh Refresh(v)>
    Password: UnConfigured

BGP Peer: 3ffe: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: 2006/03/17 15:49:35
    BGP Version: 4                  Type: External
    Local Address: 3ffe: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: <IPv6-Uni Refresh Refresh(v)>
```

```
      Send    : <IPv6-Uni Refresh Refresh(v)>
      Receive: <IPv6-Uni Refresh Refresh(v)>
    Password: UnConfigured
>
```

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。

29.6.11 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・リスタート機能の運用コマンド一覧を次の表に示します。

表 29-30 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。
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 8. 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を表示する場合は，運用コマンド show ipv6 bgp の neighbors パラメータと detail パラメータを指定します。

図 29-38　show ipv6 bgp コマンド（neighbors，detail パラメータ指定）の実行結果

```
> show ipv6 bgp neighbors detail
Date 2006/04/17 15:52:14 UTC
BGP Peer: 3ffe: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: 2006/04/17 15:51:00
    BGP Version: 4                  Type: Internal
    Local Address: 3ffe: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
     Restart Status : Finished    2006/04/16 18:46:14
     Receive Status : Finished    2006/04/16 19:16:42
       Stalepath-Time: 30

    BGP Message  UpdateIn   UpdateOut  TotalIn    TotalOut
                 0          0          2          4
    BGP Capability Negotiation: <IPv6-Uni Refresh Refresh(v) GracefulRestart>…2
      Send   : <IPv6-Uni Refresh Refresh(v) GracefulRestart(RestartTime:120s)>
      Receive: <IPv6-Uni Refresh Refresh(v) GracefulRestart(RestartTime:120s)>
    Password: UnConfigured

BGP Peer: 3ffe: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: 2006/04/17 15:49:35
    BGP Version: 4                  Type: External
    Local Address: 3ffe: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
    Graceful Restart: Both                                          …1
     Restart Status : Finished    2006/04/16 18:43:40
     Receive Status : Finished    2006/04/16 15:49:36
       Stalepath-Time: 30
    BGP Message  UpdateIn   UpdateOut  TotalIn    TotalOut
                 0          0          3          5
    BGP Capability Negotiation: <IPv6-Uni Refresh Refresh(v) GracefulRestart>…2
      Send   : <IPv6-Uni Refresh Refresh(v) GracefulRestart(RestartTime:120s)>
      Receive: <IPv6-Uni Refresh Refresh(v) GracefulRestart(RestartTime:120s,
IPv6-uni)>
    Password: UnConfigured
```

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. BGP4+ 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・リスタート機能を適用し，経路の送信元ルータがリスタート中の経路を表示するには，運用コマンド show ipv6 bgp を指定します。

図 29-39 show ipv6 bgp コマンドの実行結果

```
> show ipv6 bgp
Date 2006/01/16 19:12:23 UTC
Local AS: 65531, Local Router ID: 192.168.1.100
Status Codes: * valid, > active , S Stale
Origin Codes: i - IGP, e - EGP, ? - incomplete
   Network                                Next Hop
      MED   LocalPref Weight Path
S  3ffe:10:10::/48                        3ffe:172:16:2::2
      -     120       20     65532 65528 i                      …1
S  3ffe:10:20::/48                        3ffe:172:16:2::2
      -     80        20     65532 65528 i                      …1
*> 3ffe:172:20::/48                       3ffe:192:168:2::2
      -     100       10     65530    i
*  3ffe:172:30::/48                       3ffe:192:168:2::2
      100   100       10     65530 i
*  3ffe:192:168:10::/64                   3ffe:192:168:2::2
      -     100       10     65530 i
*> 3ffe:192:169:10::/64                   3ffe:192:168:2::2
      -     100       10           i
*> 3ffe:192:169:20::/64                   3ffe: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を示しています。

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を表示する場合は運用コマンド show graceful-restart unicast コマンドを使用します。

図 29-40 show graceful-restart unicast コマンドの実行結果

```
>show graceful-restart unicast
Date 2006/04/17 12:00:00 UTC
Status: Completed
Graceful Restart Time Limit: 180s
Start Time: 2006/04/08 17:01:23
End Time  : 2006/04/08 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)
```

29.6.12 BGP4+ 学習経路数制限の確認

(1) 運用コマンド一覧

BGP4+ 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 29-31 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。
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+ 学習経路数制限により切断しているピアを再接続します。

(2) BGP4+ 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

BGP4+ 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）の確認は，運用コマンド show ipv6 bgp で neighbors パラメータ，および <As>，<Peer Address>，<Host name> または detail パラメータを指定します。

図 29-41　show ipv6 bgp コマンド（neighbors，detail パラメータ指定）の実行結果

```
>show ipv6 bgp neighbors detail
 Date 2006/03/13 18:45:09
 BGP Peer: 3ffe:172:16:2::2, Remote AS: 65532
 Remote Router ID: 172.16.2.200
     BGP Status:Idle                 HoldTime: 90
     Established Transitions: 1      Established Date: 2006/03/13 18:42:26…1
     BGP Version: 4                  Type: External
     Local Address: 3ffe:172:16:23::214,  Local AS: 65531
     Local Router ID: 172.16.2.100
     Next Connect Retry: 00:32,      Connect Retry Timer: 00:32
     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            1000          60m         80%
     BGP Capability Negotiation: <IPv6-Uni>
       Send   : <IPv6-Uni>
       Receive: <IPv6-Uni>
     Password : Configured
 BGP Peer: 3ffe:192:168:2::1, Remote AS: 65531
 Remote Router ID: 192.168.2.200
     BGP Status:Active               HoldTime: 90
     Established Transitions: 1      Established Date: 2006/03/13 18:42:31
     BGP Version: 4                  Type: Internal
     Local Address: 3ffe: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
                  12       14        36      42
     BGP Routes  Accepted     MaximumPrefix RestartTime Threshold         …4
                 94           1000          none        75%
     BGP Capability Negotiation: <IPv6-Uni>
       Send   : <IPv6-Uni>
       Receive: <IPv6-Uni>
     Password : Configured
```

1. 2006/03/13 18:42:26 にピアを切断しています。
2. 学習経路数制限により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. 当該ピアから学習経路数の上限値 1000 に対して 94 の経路学習をしています。

(3) BGP4+ 学習経路数制限により切断した BGP4+ セッションの再接続

BGP4+ 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 BGP4+ セッションは，運用コマンド clear ipv6 bgp で *，または <Peer Address>，<Host Name> パラメータを指定して再接続します。

［コマンドによる BGP4+ セッション再接続］

1. **# clear ipv6 bgp 3ffe:172:16:2::2**

BGP4+ 学習経路数制限により切断している相手側アドレス 3ffe:172:16:2::2 との BGP4+ セッションを再接続します。

30 経路フィルタリング（IPv6）

この章では，経路フィルタリング（IPv6）について説明します。

30.1　経路フィルタリング解説

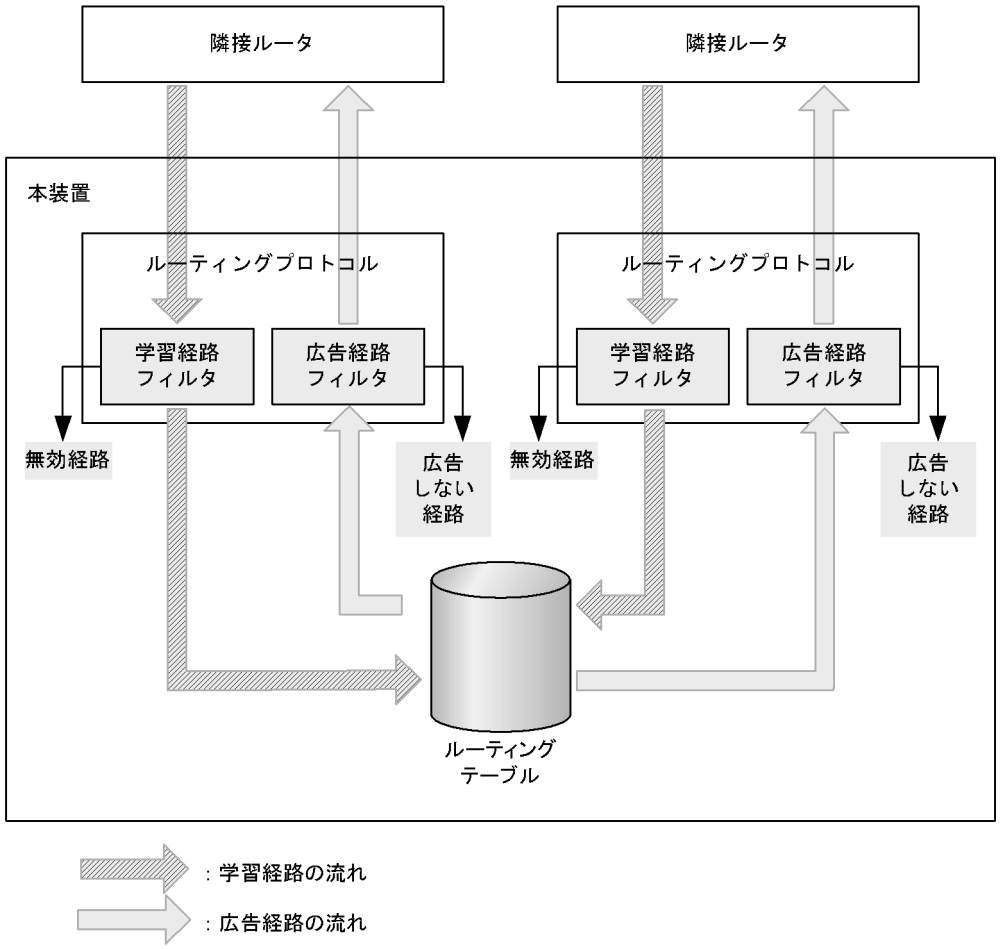
30.1.1　経路フィルタリング概要

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と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 30-1　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。

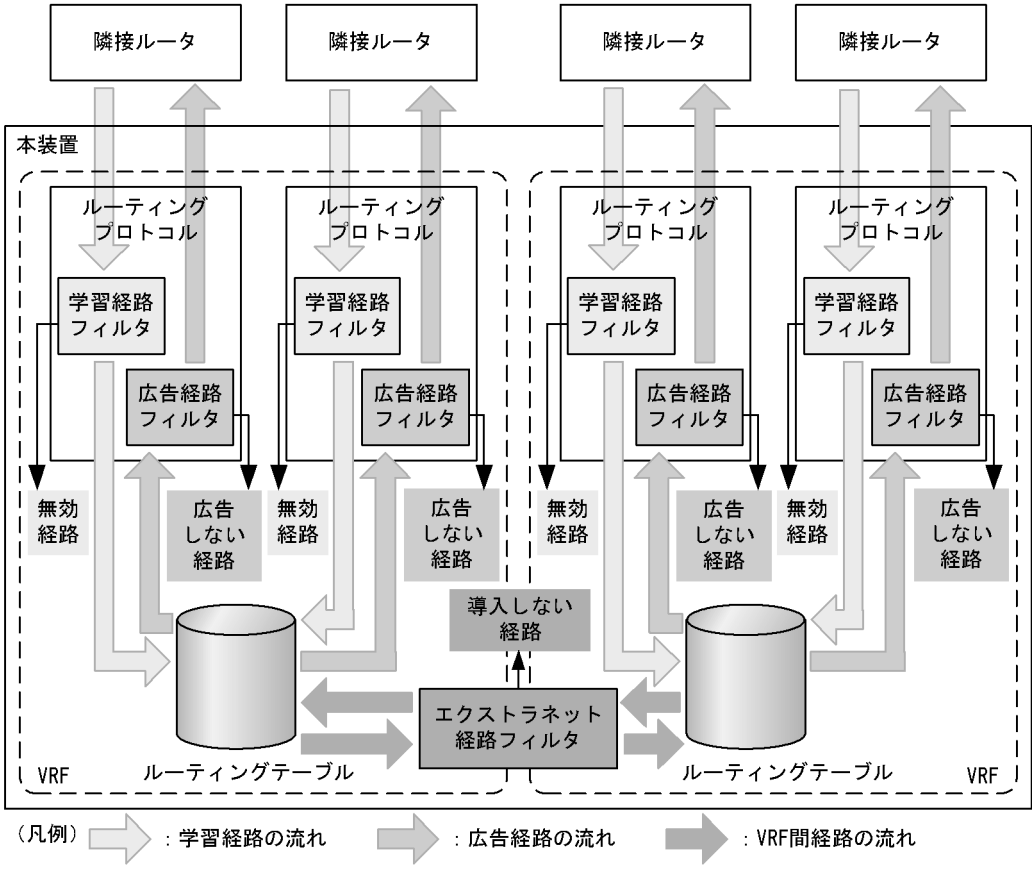
(2) エクストラネットの経路フィルタリング【OP-NPAR】

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行い，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 30-2　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。

30.1.2　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により，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

クだけを条件にフィルタする prefix-list と，主要な経路属性ほとんどを条件にフィルタし，経路属性も変更できる route-map です。そのほかに，IPv6 アドレスを条件とする ipv6 access-list，BGP 経路属性を条件とする ip as-path access-list と ip community-list があります。ipv6 access-list，ip as-path access-list，ip community-list は，route-map から呼び出して使います。

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，フィルタを多数設定することができます。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，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することが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 とみなします。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） ipv6 prefix-list

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。ipv6 prefix-list 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，一致したものとみなします。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，一致したものとみなします。ipv6 prefix-list の比較例を次の表に示します。

表 30-1　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		
	3ffe:5555::/32 **マスク長 32 だけ一致**	3ffe:5555::/32 ge 32 le 48 **マスク長 32 以上 48 以下と一致**	3ffe:5555::/32 ge 16 le 48 **マスク長 16 以上 48 以下と一致**
::/0	×	×	×
3ffe::/16	×	×	○
3fff::/16	×	×	×
3ffe:5555::/32	○	○	○
3ffe:5556::/32	×	×	×
3ffe:5555:feed::/48	×	○	○
3ffe:5555:feed:beef::/64	×	×	×

（凡例） ○：一致する　×：一致しない

ipv6 prefix-list は，route-map の match ipv6 address から経路宛先条件として引用することもできます。比較方法は単体で経路フィルタとして使用した場合と同じです。

ipv6 prefix-list は，route-map の match ipv6 route-source から経路学習元ルータ条件として引用することもできます。この場合，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。

(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することもできます。

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することができます。1 行の中に指定した複数の条件は OR 条件として取り扱います。シーケンス番号の中に設定した複数の行は AND 条件として取り扱います。

指定してあるフィルタ条件を，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 により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（RIPng）でタグ値を変更する route-map を適用し，distribute-list out（RIPng）でタグ値を条件とする route-map を適用した場合，まず，redistribute でタグ値を変更し，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 30-2　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
宛先ネットワーク	prefix-list や access-list の識別子を条件として指定し，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，一致したとみなします。deny の場合，一致しないとみなします。	match ipv6 address ipv6 prefix-list ipv6 access-list
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，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	prefix-list や access-list の識別子を条件として指定し，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，一致したとみなします。deny の場合，一致しないとみなします。 学習元隣接ルータのアドレスがあるのは，RIPng 経路と 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することはありません。	match ipv6 route-source ipv6 access-list ipv6 prefix-list
インタフェース	インタフェースを条件として指定し，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+ の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，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 とみなします。	match tag

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
AS_PATH 属性	ip as-path access-list の識別子を条件に指定し，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，一致したとみなします。deny の場合，一致しないとみなします。 AS_PATH 属性のない経路では，長さ 0 の AS PATH とみなします。	match as-path ip as-path access-list
COMMUNITIES 属性	ip community-list の識別子を条件に指定し，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，一致したとみなします。deny の場合，一致しないとみなします。 COMMUNITIES 属性のない経路では，コミュニティなしとみなします。	match community ip community-list
ORIGIN 属性	値 IGP・EGP・INCOMPLETE を条件に指定し，経路の ORIGIN 属性と比較します。 ORIGIN 属性のない経路では，値 IGP とみなします。	match origin
経路種別	OSPFv3 の経路種別や local（network（BGP）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，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，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である場合，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みなします。

表 30-3　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でだけ有効です。	set distance
メトリック値	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+ 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 属性宛の経路のメトリック引き継ぎ)
MED 属性		
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+ 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 番号を追加することだけできます。ピアの送信側 AS 番号を追加します。 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+ 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+ の経路フィルタリングで使用します。	set origin

変更できる属性	説明	コンフィグレーションコマンド
OSPF メトリック種別	メトリック種別を変更します。 OSPFv3 の広告経路フィルタリングで使用します。	set metric-type

（3） そのほかのフィルタ

上記で説明したもののほかに，以下のフィルタを経路フィルタリングに使用できます。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います。

（a） ipv6 access-list

ipv6 access-list 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，経路をフィルタするのに使うこともできます。

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。

（b） 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，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。正規表現については，「（e） 正規表現」を参照してください。

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。

(c) 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，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，一致したとみなします。route-map の match community から呼び出して使用します。

(d) 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，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。正規表現については，「(e) 正規表現」を参照してください。

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，値の小さいものから順に空白文字で接続したものたものです。コミュニティ値の文字列表現を次の表に示します。

表 30-4 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

(e) 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。正規表現を使うことで，繰り返しなどのパターンを書くことができます。正規表現は，AS_PATH 属性や COMMUNITIES 属性のフィルタ条件指定に使用します。

正規表現で使える文字は，数字・小文字アルファベット・大文字アルファベット・記号（ただし，ダブルクォーテーション「 ”」は除く）などの通常文字と，特殊文字です。通常文字，「¥」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 30-5 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］を入力後［?］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。

特殊文字	パターン
[ ]	[ ] 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 - のあと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マニュアル「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 集合までネスト可能です。
|	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の結合優先順位を次の表に示します。

表 30-6　正規表現使用文字の結合優先順位

優先順位	文字
高	( )
↑	* + ?
↓	通常文字 . [ ] ^ $
低	|

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際には，正規表現の前後をダブルクォーテーション (") で囲んで指定してください。

例 1

```
> show ipv6 bgp aspath-regexp "^$"
```

例 2

```
(config)# ip as-path access-list 10 permit "_100_"
```

30.1.3　RIPng

(1) RIPng 学習経路フィルタリング

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入りません。

(a) フィルタの適用方法と適用順

学習した経路を distribute-list in で設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を指定することにより，特定のインタフェースから学習した経路にだけフィルタを適用することができます。RIPng 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。

経路を学習したら，指定したフィルタを表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，その学習経路はルーティングテーブルに入りません。

表 30-7 RIPng 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 (RIPng)	<Interface>	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。

(b) 学習経路フィルタリングで変更可能な経路属性

RIPng の学習経路フィルタリングで変更可能な属性を次の表に示します。

変更したメトリック値は，RIPng の優先経路選択に用います。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用います。

表 30-8 RIPng 学習経路フィルタリングで変更可能な経路の属性

属性	デフォルト値
ディスタンス値	distance（RIPng）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。

注意

- メトリック値の変更方法に，加算以外の方法を使わ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，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することもできます。しかし，変更後のメトリック値が 16 以上の 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 による変更の結果，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 RIPng 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，上位のビットを切り捨てます。

(2) RIPng 広告経路フィルタリング

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ます。ただし，スプリットホライズン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，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

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可能な経路属性

RIPng の広告経路フィルタリングで変更可能な属性を次の表に示します。

表 30-9 RIPng 広告フィルタリングで変更可能な経路の属性

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 で指定した値を用います。 default-metric 未設定時は 1 を用います。
	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 を用います。 inherit-metric 未設定時は default-metric で指定した値を用います。 inherit-metric も default-metric も設定していない場合は 16 を用います。
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

- 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わ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，パケットを正しく転送できなくなることがあるからです。
- メトリック値を 16 以上に変更するように設定することもできます。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 による変更の結果，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，上位のビットを切り捨てます。

(3) フィルタの適用方法と適用順

広告経路フィルタリングは，三つの手順に分かれています。

1. まず，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を指定します。プロトコルを指定するには，コンフィグレーションコマンド redistribute を使用します。redistribute に条件経路種別を指定することにより，指定した種別の経路だけを広告対象にすることができます。また，route-map を指定することにより，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することもできます。redistribute では，条件の比較にルーティングテーブル上の経路属性値を使用します。
   RIPng 経路と RIPng インタフェースの直結経路だけは，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ることで，広告する経路の属性を変更することもできます。
2. メトリック値をプロトコルで決められた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ている場合は redistribute で変更した値をそのまま使用します。
   RIPng のメトリック値のデフォルト値については，「表 30-9 RIPng 広告フィルタリングで変更可能な経路の属性」を参照してください。
3. redistribute で選択した経路に，distribute-list out に従ってフィルタを適用します。パラメータにインタフェースを指定することにより，指定したインタフェースへ広告する場合にだけフィルタを適用することができます。また，プロトコルを指定すると，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。コンフィグレーションコマンドを次の表に示します。

経路を RIPng インタフェース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 を指定することによって，広告する経路の属性を変更することもできます。

表 30-10　RIPng 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 (RIPng)	<Interface>	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。

30.1.4　OSPFv3

（1）OSPFv3 学習経路フィルタリング

OSPFv3 では，SPF 計算で求まった経路の中で，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 AS 外経路は，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・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入ります。

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経路ができます。これは，経路の元となった LSA が OSPFv3 ドメイン内のほかのルータへ伝わるからです。学習経路フィルタリングは，LSA から計算した AS 外経路は経路フィルタリングしますが，経路の元になった LSA はフィルタしません。

（a）フィルタの適用方法と適用順

学習した経路の中で 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。OSPFv3 学習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。

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。

表 30-11　OSPFv3 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 (OSPFv3)	設定した OSPFv3 ドメインで求まった AS 外経路がフィルタリング対象になります。

（b）学習経路フィルタリングで変更可能な経路属性

OSPFv3 学習経路フィルタリングで変更可能な属性を次の表に示します。

OSPFv3 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用います。

表 30-12　OSPFv3 学習経路フィルタリングで変更可能な経路の属性

属性	デフォルト値
ディスタンス値	distance ospf（OSPFv3）に指定した値。 指定していない場合は 110。

(2) OSPFv3 広告経路フィルタリング

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。これは，広告経路フィルタリングでは制御できません。

また，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にかかわらず，経路の元である LSA は無条件で伝達するからです。

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 OSPFv3 へ広告できます。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，OSPFv3 インタフェースの直結経路と OSPFv3 経路のほかは，どの経路も広告しません。

(a) 広告経路フィルタリングで変更可能な経路属性

OSPFv3 の広告経路フィルタリングで変更可能な属性を次の表に示します。

表 30-13　OSPFv3 広告経路フィルタリングで変更可能な 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することもできます。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は，次に示す手順に分かれています。

1. まず，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を指定します。プロトコルを指定するには，コンフィグレーションコマンド redistribute を使用します。ただし，OSPFv3 の当該ドメインを指定しても，そのドメインの経路を再広告することはありません。
   redistribute に経路種別を指定することにより，指定した種別の経路だけを広告対象にすることができます。また，route-map を指定することにより，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することもできます。redistribute では，条件の比較にルーティングテーブル上の経路属性値を使用します。

redistribute に経路属性を変更する route-map や経路属性を直接指定することで，広告する経路の属性を変更することもできます。

2. メトリック値と OSPFv3 経路種別をプロトコルで決められたデフォルト値に設定します。ただし，redistribute で属性値を変更している場合は redistribute で変更した値をそのまま使用します。
   OSPFv3 の広告経路属性のデフォルト値については，「表 30-13　OSPFv3 広告経路フィルタリングで変更可能な OSPFv3 AS 外経路の属性」を参照してください。
3. redistribute で選択した経路に distribute-list out に従ってフィルタを適用します。パラメータにプロトコルを指定することにより，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。コンフィグレーションコマンドを次の表に示します。
   経路を OSPFv3 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 を指定することで，広告する経路の属性を変更することもできます。

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 OSPFv3 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。

表 30-14　OSPFv3 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 (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。

30.1.5　BGP4+【OP-BGP】

（1）BGP4+ 学習経路フィルタリング

BGP4+ では，学習した経路すべてをフィルタできます。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入りません。

注意

BGP4+ の学習経路フィルタリングを設定または変更したあと，適切なタイミングで運用コマンド clear ipv6 bgp * in または clear ipv6 bgp * both を実行してください。上記運用コマンドを実行するまでの間は，変更前の経路フィルタリング設定に従って動作します。
clear ipv6 bgp * in を実行すると，変更したあとの経路フィルタリング設定を学習経路フィルタリングに使用します。clear ipv6 bgp * both を実行すると，変更したあとの経路フィルタリング設定を学習経路フィルタリングと広告経路フィルタリングに使用します。

(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。BGP4+ 学習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。

経路を学習したら，設定したフィルタを表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。

表 30-15 BGP4+ 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）	<IPv6>（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+）（prefix-list 指定）	<IPv6>（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）	<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+）（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。
distribute-list in（BGP4+）	なし	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。

(b) 学習経路フィルタリングで変更可能な経路属性

BGP4+ 経路の学習経路フィルタリングで変更可能な属性を次の表に示します。

ディスタンス値以外の値は，BGP4+ の優先経路選択に用います。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用います。

表 30-16 BGP4+ 経路フィルタリングで変更可能な経路の属性

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，次の値を使います。 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。

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 AS を加えることはできません。

(2) BGP4+ 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。この 3 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。

注意

BGP4+ の広告経路フィルタリングを設定または変更したあと，適切なタイミングで運用コマンド clear ipv6 bgp * out または clear ipv6 bgp * both を実行してください。上記運用コマンドを実行するまでの間は，変更前の経路フィルタリング設定に従って動作します。
clear ipv6 bgp * out を実行すると，変更したあとの経路フィルタリング設定を広告経路フィルタリングに使用します。clear ipv6 bgp * both を実行すると，変更したあとの経路フィルタリング設定を学習経路フィルタリングと広告経路フィルタリングに使用します。

(a) 広告経路フィルタリングで変更可能な経路属性

BGP4+ 広告経路フィルタリングで変更可能な属性を次の表に示します。

表 30-17 BGP4+ 広告経路フィルタリングで変更可能な 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+ 経路であれば，メトリック値を引き継ぎます。BGP4+ 以外の経路の場合，default-metric で設定した値を用います。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 で設定した値を用います。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+ 経路であれば，メトリック値を引き継ぎます。BGP4+ 以外の経路の場合，default-metric で設定した値を用います。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 で設定した値を用います。bgp default local-preference を設定していない場合，値 100 を用います。ただし，広告先ピアが外部ピアである場合，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

neighbor send-community を設定していない場合，COMMUNITIES 属性を広告しません。

(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は，次に示す手順に分かれています。

1. まず，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を指定します。プロトコルを指定するには，コンフィグレーションコマンド redistribute を使用します。redistribute に条件経路種別や route-map を指定すると，指定した種別の経路や route-map を通過した経路だけが広告対象になります。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ることで，広告する経路の属性を変更することもできます。
2. MED 属性，LOCAL_PREF 属性をプロトコルで決められたデフォルト値に設定します。ただし，redistribute で属性値を変更している場合は redistribute で変更した値をそのまま使用します。
   BGP4+ の広告経路属性のデフォルト値については，「表 30-17　BGP4+ 広告経路フィルタリングで変更可能な BGP4+ 経路の属性」を参照してください。
3. redistribute で選択した経路を，neighbor out と distribute-list out に従ってフィルタします。
   neighbor out 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へ広告する場合にだけ適用します。また，プロトコルを指定すると，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。コンフィグレーションコマンドとその適用先を次の表に示します。
   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，それを表の順番に適用します。適用する経路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。フィルタした結果が 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，デフォルト広告属性値や 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。
   neighbor out や distribute-list out に属性を変更する route-map を指定することによって，広告する経路の属性を変更することもできます。

表 30-18　BGP4+ 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）	<IPv6>（ピアアドレス） <Protocol>	指定ピアへ広告する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+）（prefix-list 指定）	<IPv6>（ピアアドレス） <Protocol>	
neighbor out（BGP4+）（route-map 指定）	<IPv6>（ピアアドレス）	指定ピアへ広告する経路にフィルタを適用します。
neighbor out（BGP4+）（prefix-list 指定）	<IPv6>（ピアアドレス）	
neighbor out（BGP4+）（route-map 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+）（prefix-list 指定）	<Peer-Group>（ピアグループ） <Protocol>	
neighbor out（BGP4+）（route-map 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+）（prefix-list 指定）	<Peer-Group>（ピアグループ）	
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。

コマンド名	パラメータ	フィルタ対象経路
	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。

30.1.6 エクストラネット【OP-NPAR】

（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入りません。

（a）フィルタの適用方法

VRF 間で導入したい経路を，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 30-19 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
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可能な経路属性

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可能な属性を次の表に示します。

表 30-20 VRF 間経路フィルタリングで変更可能な経路の属性

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。
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。

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

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 30-21 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 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。
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。

コマンド名	説明
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。
router bgp ※ 2	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。
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。
ipv6 import inter-vrf ※ 5	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。

注※ 1
「コンフィグレーションコマンドレファレンス Vol.2　4. 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　13. BGP4【OP-BGP】」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　25. 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　26. 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　30. VRF【OP-NPAR】」を参照してください。

30.2.2　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

3ffe:501:811:ff01::/64 宛の RIPng 経路だけを学習し，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，3ffe:501:811:ff01::/64 宛の経路だけ permit になる ipv6 prefix-list を設定します。この 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 3ffe:501:811:ff01::/64**

3ffe:501:811:ff01::/64 だけ permit になる 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

VLAN 10 から学習した経路について，3ffe:501:811:ff01::/64 宛の経路だけを学習し，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。VLAN 10 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，3ffe:501:811:ff01::/64 宛の経路だけ permit になる ipv6 prefix-list を設定します。この prefix-list を distribute-list in VLAN 10 から参照することによって，VLAN 10 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 3ffe:501:811:ff01::/64**
   3ffe:501:811:ff01::/64 だけ permit になる 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 vlan 10
   VLAN 10 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 3ffe:501::/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，3ffe:501::/32 に含まれるプレフィックスだけが permit になる prefix-list を設定します。次に，この 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 から参照することによって，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 LONGER3ffe0501 seq 10 permit 3ffe:501::/32 ge 32 le 128**
   3ffe:501::/32 に含まれる経路だけ permit になる prefix-list を設定します。

2. **(config)# route-map TAG permit 10**
   (config-route-map)# match ipv6 address prefix-list LONGER3ffe0501
   (config-route-map)# match tag 15
   (config-route-map)# exit
   3ffe:501::/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 LONGER3ffe0501
   (config-route-map)# exit
   シーケンス番号 10 にマッチしないで，かつ 3ffe:501::/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
   上記フィルタを RIPng 学習経路フィルタリングに適用することによって，3ffe:501::/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 3ffe:501::/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，3ffe:501::/32 を含む経路だけ permit になる prefix-list を設定します。次に，この 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 から参照することによって，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 LONGER3ffe0501 seq 10 permit 3ffe:501::/32 ge 32 le 128**
   3ffe:501::/32 に含まれる経路だけ permit になる prefix-list を設定します。

2. **(config)# route-map Distance50 permit 10**
   (config-route-map)# match ipv6 address prefix-list LONGER3ffe0501
   (config-route-map)# set distance 50
   (config-route-map)# exit
   3ffe:501::/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
   上記フィルタを RIPng 学習経路フィルタリングに適用することによって，3ffe:501::/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。

30.2.3 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 3ffe:501:811: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，3ffe:501:811:ff01::/64 宛の経路だけが permit になる ipv6 prefix-list を設定します。次に，この 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 3ffe:501:811:ff01::/64**
   3ffe:501:811:ff01::/64 だけ permit になる 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 3ffe:501:811: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，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

3ffe:501:811:ff01::/64 宛の経路に限り，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，3ffe:501:811:ff01::/64 宛の経路だけ deny になる ipv6 prefix-list を設定します。この prefix-list を distribute-list out から参照することによって，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 3ffe:501:811:ff01::/64**
   3ffe:501:811:ff01::/64 が deny になるように 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・マスク長に対して permit になるように ipv6 prefix-list を設定します。
   OMIT0811ff01 にはほかに条件がないので，3ffe:501:811: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 VLAN 10 からは，3ffe:501:811:ff01::/64 だけを広告します。RIPng インタフェース VLAN 20 からは，3ffe:501:811: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，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。
3ffe:501:811:ff01::/64 だけ permit になる ipv6 prefix-list と 3ffe:501:811:ff01::/64 以外だけ permit になる ipv6 prefix-list を設定します。次に，RIPng インタフェース VLAN 10 と VLAN 20 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 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 3ffe:501:811:ff01::/64**

3ffe:501:811:ff01::/64 だけ permit になる 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 3ffe:501:811:ff01::/64**
   3ffe:501:811:ff01::/64 だけ deny になる 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・マスク長に対して permit になるように，prefix-list を設定します。
   OMIT0811ff01 にはほかに条件がないので，3ffe:501:811: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 vlan 10
   VLAN 10 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 vlan 20**
   VLAN 20 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 を使用することになります。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。

30.2.4 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

3ffe:501:811:ff01::/64 宛の経路だけを学習し，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，3ffe:501:811:ff01::/64 宛の経路だけ permit になる ipv6 prefix-list を設定します。この prefix-list を distribute-list in から参照することによって，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 3ffe:501:811:ff01::/64
```
3ffe:501:811:ff01::/64 だけ permit になる 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 から参照することによって，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
   上記フィルタを OSPFv3 学習経路フィルタリングに適用することによって，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 3ffe:501::/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，3ffe:501::/32 を含む経路が permit になる prefix-list を設定します。次に，この 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 から参照することによって，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 LONGER3ffe0501 seq 10 permit 3ffe:501::/32 ge 32 le 128**
   3ffe:501::/32 に含まれる経路だけ permit になる prefix-list を設定します。

2. **(config)# route-map Distance150 permit 10**
   (config-route-map)# match ipv6 address prefix-list LONGER3ffe0501
   (config-route-map)# set distance 150
   (config-route-map)# exit
   3ffe:501::/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

上記フィルタを OSPFv3 学習経路フィルタリングに適用することで，3ffe:501::/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。

30.2.5 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 3ffe:501:811: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，match ipv6 address で参照してください。
まず，3ffe:501:811:ff01::/64 宛の経路だけが permit になる ipv6 prefix-list を設定します。次に，この 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 3ffe:501:811:ff01::/64**
   3ffe:501:811:ff01::/64 だけ permit になる 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 3ffe:501:811: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，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，3ffe:501:811:ff01::/64 宛の経路に限り，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，3ffe:501:811:ff01::/64 宛の経路だけ deny になる ipv6 prefix-list を設定します。この prefix-list を distribute-list out から参照することによって，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 3ffe:501:811:ff01::/64**
   3ffe:501:811:ff01::/64 が deny になるように 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・マスク長に対して permit になるように，prefix-list を設定します。
   OMIT0811ff01 にはほかに条件がないので，3ffe:501:811: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 を使用することになります。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，そうでなければタグ値 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，そうでなければタグ値 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。

30.2.6 BGP4+ 学習経路フィルタリング【OP-BGP】

（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 3ffe:501::/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，3ffe:501::/32 に含まれる経路と一致したら deny になる ipv6 prefix-list を設定します。この prefix-list を distribute-list in から参照することによって，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 LONGER3ffe0501DENY seq 10 deny 3ffe:501::/32 ge 32 le 128**
   (config)# ipv6 prefix-list LONGER3ffe0501DENY seq 20 permit ::/0 ge 0 le 128
   3ffe:501::/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 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 LONGER3ffe0501DENY in
   その 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 3ffe:501::/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。受け付けた経路の 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，3ffe:501::/32 に含まれるなら permit になる 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 LONGER3ffe0501 seq 10 permit 3ffe:501::/32 ge 32 le 128**
   プレフィックスが 3ffe:501::/32 に含まれる場合に permit になる 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 LONGER3ffe0501
(config-route-map)# exit
```
route-map BGP65502IN を，宛先ネットワークが 3ffe:501::/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 3ffe:502:811:1::1 remote-as 65532
(config-router)# address-family ipv6
(config-router-af)# neighbor 3ffe:502:811:1::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。

30.2.7 BGP4+ 広告経路フィルタリング【OP-BGP】

（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（3ffe:501::/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 prefix-list を使用します。

[コマンドによる設定]

1.
```
(config)# ipv6 prefix-list LONGER3ffe0501 seq 10 permit 3ffe:501::/32 ge 32 le 128
```
3ffe:501::/32 に含まれる経路だけ permit になる prefix-list を設定します。

2.
```
(config)# route-map LONGER3ffe0501PERMIT permit 10
(config-route-map)# match ipv6 address prefix-list LONGER3ffe0501
(config-route-map)# exit
```
3ffe:501::/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 LONGER3ffe0501PERMIT
(config-router-af)# redistribute static route-map LONGER3ffe0501PERMIT
```

直結経路とスタティック経路について，LONGER3ffe0501PERMIT 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（3ffe:501::/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 3ffe:502:812:1::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，直結経路・スタティック経路の redistribute 用，ピア 3ffe:502:812:1::1 広告用，3ffe:502:812:1::1 以外の外部ピア用，内部ピア用，合計四つの route-map を設定します。
直結経路・スタティック経路については，3ffe:501::/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 3ffe:502:812:1::1 については，経路プロトコルが直結・スタティックである場合だけ AS を二つ追加する route-map を設定します。
3ffe:502:812:1::1 以外の外部ピアについては，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。
内部ピアについては，BGP4+ 経路だけ permit，そうでなければ 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 LONGER3ffe0501 seq 10 permit 3ffe:501::/32 ge 32 le
128
(config)# route-map LONGER3ffe0501PERMIT permit 10
(config-route-map)# match ipv6 address prefix-list LONGER3ffe0501
(config-route-map)# exit
```

3ffe:501::/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・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受け付ける 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 BGP81211OUT 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 BGP81211OUT 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受け付け，AS を二つ追加する route-map を設定します。ピア 3ffe:502:812:1::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 LONGER3ffe0501PERMIT
   (config-router-af)# redistribute static route-map LONGER3ffe0501PERMIT
   (config-router-af)# exit
   直結経路とスタティック経路について，route-map LONGER3ffe0501PERMIT 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 3ffe:502:811:1::1 remote-as 65532**
   (config-router)# address-family ipv6
   (config-router-af)# neighbor 3ffe:502:811:1::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 3ffe:502:812:1::1 remote-as 65533**
   (config-router)# address-family ipv6
   (config-router-af)# neighbor 3ffe:502:812:1::1 route-map BGP81211OUT out
   (config-router-af)# exit
   外部ピア 3ffe:502:812:1::1 への広告経路のフィルタに BGP81211OUT を使用します。

8. **(config-router)# neighbor 3ffe:501:811:ff01::1 remote-as 65531**
   (config-router)# address-family ipv6
   (config-router-af)# neighbor 3ffe:501:811: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。

30.2.8 エクストラネット【OP-NPAR】

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，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，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，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。

30.3 オペレーション

経路フィルタリング（IPv6）の運用コマンド一覧を次の表に示します。

表 30-22 運用コマンド一覧

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，BGP4+ プロトコルに関する情報のクリア，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行います。
show ipv6 vrf	VRF の IPv6 情報を表示します。
restart unicast ※	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 ※	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 ※	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※
「運用コマンドレファレンス Vol.3　8. IPv4・IPv6 ルーティングプロトコル共通」を参照してください。

30.3.1 RIPng が受信した経路（学習経路フィルタリング前）の確認

RIPng が受信した経路を確認するには，運用コマンド show ipv6 rip にパラメータ received-routes を指定して実行してください。

図 30-3 RIPng 受信経路表示例

```
> show ipv6 rip received-routes
Date 2006/03/14 12:00:00 UTC
Status Codes: * valid, > active

Neighbor Address: fe80::200:87ff:fe28:90d7%VLAN0007
   Destination                                    Next Hop
         Interface      Metric   Tag   Timer
*> 3ffe:3b01:6705:1::/64                         fe80::200:87ff:fe28:90d7%VLAN0007
         VLAN0007       1        0      5s
```

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 RIPng 内部での優先しないことになった経路は，本コマンドでは表示されません。

30.3.2 OSPFv3 の SPF 計算結果の経路確認

OSPFv3 が SPF 計算した結果の 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。無効経路も含めて OSPFv3 が SPF 計算した結果の AS 外経路を確認するには，運用コマンド show ipv6 route にパラメータ all-routes を指定し，さらに -T ospf external を指定してを実行してください。

図 30-4 OSPFv3 AS 外経路表示例

```
> show ipv6 route all-routes -T ospf external
Date 2006/03/14 12:00:00 UTC
Status Codes: * valid, > active
Total: 2 routes
   Destination                                  Next Hop
         Interface      Metric  Protocol    Age
*> 3ffe:3b21:6705:1::/64                       fe80::200:87ff:fe28:90d7%VLAN0007
         VLAN0007       1/1     OSPFv3 ext2 24m 33s , Tag: 100
*  3ffe:8703:2005:1::/64                       fe80::200:87ff:fe28:90d7%VLAN0007
         VLAN0007       1/1     OSPFv3 ext2 26m 52s , Tag: 100
```

30.3.3 BGP4+ が受信した経路（学習経路フィルタリング前）の確認【OP-BGP】

BGP4+ が受信した経路を確認するには，運用コマンド show ipv6 bgp にパラメータ received-routes を指定して実行してください。

図 30-5 BGP4+ 受信経路表示例

```
> show ipv6 bgp received-routes
Date 2006/03/14 12:00:00 UTC
BGP4+ Peer: 3ffe:177:7:7::145, Remote AS: 1000
Local AS: 200, Local Router ID: 200.201.202.203
Status Codes: * valid, > active
Origin Codes: i - IGP, e - EGP, ? - incomplete
   Network                                      Next Hop
         MED    LocalPref Path
*> 3ffe:3b11:6705:1::/64                       fe80::200:87ff:fe28:90d7%VLAN0007
         -      -         1000 i
*  3ffe:8703:2005:1::/64                       fe80::200:87ff:fe28:90d7%VLAN0007
         -      -         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+ 内部で優先しないことになった経路は，本コマンドでは表示されません。

BGP4+ が受信した経路を詳細な経路属性を含めて確認するには，運用コマンド show ipv6 bgp にパラメータ received-routes を指定し，さらに -F を指定して実行してください。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 30-6　BGP4+ 受信経路詳細表示例

```
> show ipv6 bgp received-routes  -F
Date 2006/03/14 12:00:00 UTC
BGP4+ Peer: 3ffe:177:7:7::145, Remote AS: 1000
Local AS: 200, Local Router ID: 200.201.202.203
Status Codes: * valid, > active
Route 3ffe:3b11:6705:1::/64
*> Next Hop fe80::200:87ff:fe28:90d7%VLAN0007
     MED: -, LocalPref: -, Type: External route
     Origin: IGP, IGP Metric: 0
     Path: 1000
     Next Hop Attribute: 3ffe:177:7:7::145
                         fe80::200:87ff:fe28:90d7

Route 3ffe:8703:2005:1::/64
*  Next Hop fe80::200:87ff:fe28:90d7%VLAN0007
     MED: -, LocalPref: -, Type: External route
     Origin: IGP, IGP Metric: 0
     Path: 1000
     Next Hop Attribute: 3ffe:177:7:7::145
                         fe80::200:87ff:fe28:90d7
     Communities: 300:300
```

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+ 内部で優先しないことになった経路は，本コマンドでは表示されません。

30.3.4　学習経路フィルタリングした結果の経路の確認

学習経路フィルタリングした結果の経路は，ルーティングテーブルに入っています。ルーティングテーブルの経路を表示することで，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，運用コマンド show ipv6 route にパラメータ all-routes を指定して実行してください。

図 30-7 ルーティングテーブル経路表示例 (無効経路を含む)

```
> show ipv6 route all-routes
Date 2006/03/14 12:00:00 UTC
Status Codes: * valid, > active
Total: 11 routes
   Destination                                Next Hop
         Interface     Metric Protocol    Age
*> ::1/128                                    ::1
         localhost     0/0    Connected    4h 44m
*> 3ffe:177:7:7::/64                         3ffe:177:7:7::1
         VLAN0007      0/0    Connected   39m 41s
*  3ffe:177:7:7::/64                         3ffe:177:7:7::1
         VLAN0007      1/-    OSPFv3 intra 6m 52s
*> 3ffe:177:7:7::1/128                       ::1
         localhost     0/0    Connected   39m 41s
*> 3ffe:3b01:6705:1::/64                     fe80::200:87ff:fe28:90d7%VLAN0007
         VLAN0007      2/0    RIPng        2s
*> 3ffe:3b11:6705:1::/64                     fe80::200:87ff:fe28:90d7%VLAN0007※
         VLAN0007      -/-    BGP4+        4m  5s
*> 3ffe:3b21:6705:1::/64                     fe80::200:87ff:fe28:90d7%VLAN0007
         VLAN0007      1/1    OSPFv3 ext2  4m  3s
*> 3ffe:8703:2005:1::/64                     3ffe:177:7:7::145
         VLAN0007      0/0    Static       1m 15s
*  3ffe:8703:2005:1::/64                     fe80::200:87ff:fe28:90d7%VLAN0007
         VLAN0007      -/-    BGP4+        8m 27s
*  3ffe:8703:2005:1::/64                     fe80::200:87ff:fe28:90d7%VLAN0007
         VLAN0007      1/1    OSPFv3 ext2  6m 22s
*  3ffe:8703:2005:1::/64                     fe80::200:87ff:fe28:90d7%VLAN0007
         VLAN0007      2/0    RIPng        2s
```

注※

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，運用コマンド show ipv6 route にパラメータ all-routes を指定し，さらにプロトコル名を指定してください。

図 30-8 ルーティングテーブル経路表示例 (RIPng だけ，無効経路含む)

```
> show ipv6 route all-routes rip
Date 2006/03/14 12:00:00 UTC
Status Codes: * valid, > active
Total: 2 routes
   Destination                                 Next Hop
         Interface      Metric   Protocol  Age
*> 3ffe:3b01:6705:1::/64                      fe80::200:87ff:fe28:90d7%VLAN0007
         VLAN0007       2/0      RIPng      3s
*  3ffe:8703:2005:1::/64                      fe80::200:87ff:fe28:90d7%VLAN0007
         VLAN0007       2/0      RIPng      3s
```

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・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，運用コマンド show ipv6 route にパラメータ all-routes を指定し，さらに -P を指定して実行してください。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 30-9 ルーティングテーブル経路ディスタンス値表示例

```
> show ipv6 route all-routes -P
Date 2006/03/14 12:00:00 UTC
Status Codes: * valid, > active
Total: 11 routes
   Destination                                Next Hop
         Interface   Metric Protocol    Age
*> ::1/128                                    ::1
         localhost   0/0    Connected    4h 46m , Distance: 0/0/0
*> 3ffe:177:7:7::/64                         3ffe:177:7:7::1
         VLAN0007    0/0    Connected   42m  0s , Distance: 0/0/0
*  3ffe:177:7:7::/64                         3ffe:177:7:7::1
         VLAN0007    1/-    OSPFv3 intra 9m 11s , Distance: 110/1/0
*> 3ffe:177:7:7::1/128                       ::1
         localhost   0/0    Connected   42m  0s , Distance: 0/0/0
*> 3ffe:3b01:6705:1::/64                     fe80::200:87ff:fe28:90d7%VLAN0007
         VLAN0007    2/0    RIPng       16s     , Distance: 120/0/0
*> 3ffe:3b11:6705:1::/64                     fe80::200:87ff:fe28:90d7%VLAN0007
         VLAN0007    -/-    BGP4+        6m 24s , Distance: 20/0/0
*> 3ffe:3b21:6705:1::/64                     fe80::200:87ff:fe28:90d7%VLAN0007
         VLAN0007    1/1    OSPFv3 ext2  6m 22s , Distance: 110/1/0
*> 3ffe:8703:2005:1::/64                     3ffe:177:7:7::145
         VLAN0007    0/0    Static       3m 34s , Distance: 2/0/0
*  3ffe:8703:2005:1::/64                     fe80::200:87ff:fe28:90d7%VLAN0007
         VLAN0007    -/-    BGP4+       10m 46s , Distance: 20/0/0
*  3ffe:8703:2005:1::/64                     fe80::200:87ff:fe28:90d7%VLAN0007
         VLAN0007    1/1    OSPFv3 ext2  8m 41s , Distance: 110/1/0
*  3ffe:8703:2005:1::/64                     fe80::200:87ff:fe28:90d7%VLAN0007
         VLAN0007    2/0    RIPng       16s     , 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，運用コマンド show ipv6 route にパラメータ all-routes を指定し，さらに宛先ネットワークを指定して実行してください。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 30-10　ルーティングテーブル経路表示例 (無効経路含む，特定宛先だけ)

```
> show ipv6 route all-routes 3ffe:8703:2005:1::/64
Date 2006/03/14 12:00:00 UTC
Route codes: *  = active,   + = changed to active recently
             ' ' = inactive, - = changed to inactive recently

Route 3ffe:8703:2005:1::/64
Entries 4 Announced 1 Depth 0 <>

* NextHop 3ffe:177:7:7::145, Interface: VLAN0007
     Protocol <Static>
     Source Gateway ----
     Metric/2    : 0/0
     Distance/2/3: 2/0/0
     Tag : 0, Age :  4m 35s
     AS Path : IGP (Id 1)
     Communities: -
     LocalPref : -
     RT State: <Remote Int Active Gateway>

  NextHop fe80::200:87ff:fe28:90d7%VLAN0007, Interface: VLAN0007
     Protocol <BGP4+>
     Source Gateway fe80::200:87ff:fe28:90d7%VLAN0007
     Metric/2    : -/-
     Distance/2/3: 20/0/0
     Tag : 0, Age : 11m 47s
     AS Path : 1000 IGP (Id 3)
     Communities: -
     LocalPref : 100
     RT State: <Ext Gateway>
```

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，運用コマンド show ipv6 route にパラメータ all-routes を指定し，さらに -F を指定して実行してください。

図 30-11 ルーティングテーブル経路表示例 (無効経路含む，詳細表示)

```
> show ipv6 route all-routes -F
Date 2006/03/14 12:00:00 UTC
Status Codes: * valid, > active
Total: 11 routes
   Destination                                Next Hop
     Interface      Metric   Protocol     Age
*> ::1/128                                   ::1
     localhost      0/0      Connected     4h 55m , Distance: 0/0/0, Tag: 0, AS
-Path: IGP (Id 1), Communities: -, LocalPref: -, <NoAdvise Active Retain>
*> 3ffe:177:7:7::/64                        3ffe:177:7:7::1
     VLAN0007       0/0      Connected    51m  2s , Distance: 0/0/0, Tag: 0, AS
-Path: IGP (Id 1), Communities: -, LocalPref: -, <Active Retain>
*  3ffe:177:7:7::/64                        3ffe:177:7:7::1
     VLAN0007       1/-      OSPFv3 intra 18m 13s , Distance: 110/1/0, Tag: 0,
AS-Path: IGP (Id 1), Communities: -, LocalPref: -, <Int Gateway>
*> 3ffe:177:7:7::1/128                       ::1
     localhost      0/0      Connected    51m  2s , Distance: 0/0/0, Tag: 0, AS
-Path: IGP (Id 1), Communities: -, LocalPref: -, <NoAdvise Int Active Retain>
*> 3ffe:3b01:6705:1::/64                     fe80::200:87ff:fe28:90d7%VLAN0007
     VLAN0007       2/0      RIPng         4s     , Distance: 120/0/0, Tag: 0,
AS-Path: IGP (Id 1), Communities: -, LocalPref: -, <Int Active Gateway>
*> 3ffe:3b11:6705:1::/64                     fe80::200:87ff:fe28:90d7%VLAN0007
     VLAN0007       -/-      BGP4+         3m  6s , Distance: 20/0/0, Tag: 0, A
S-Path: 1000 IGP (Id 3), Communities: -, LocalPref: 100, <Ext Active Gateway>
*> 3ffe:3b21:6705:1::/64                     fe80::200:87ff:fe28:90d7%VLAN0007
     VLAN0007       1/1      OSPFv3 ext2  15m 24s , Distance: 110/1/0, Tag: 0,
 AS-Path: IGP (Id 1), Communities: -, LocalPref: -, <Int Ext Active Gateway>
*> 3ffe:8703:2005:1::/64                     3ffe:177:7:7::145
     VLAN0007       0/0      Static       12m 36s , Distance: 2/0/0, Tag: 0, AS
-Path: IGP (Id 1), Communities: -, LocalPref: -, <Remote Int Active Gateway>
*  3ffe:8703:2005:1::/64                     fe80::200:87ff:fe28:90d7%VLAN0007
     VLAN0007       -/-      BGP4+         3m  6s , Distance: 20/0/0, Tag: 0, A
S-Path: 1000 IGP (Id 5), Communities: 300:300, LocalPref: 100, <Ext Gateway>
*  3ffe:8703:2005:1::/64                     fe80::200:87ff:fe28:90d7%VLAN0007
     VLAN0007       1/1      OSPFv3 ext2  17m 43s , Distance: 110/1/0, Tag: 0,
 AS-Path: IGP (Id 1), Communities: -, LocalPref: -, <Int Ext Gateway>
*  3ffe:8703:2005:1::/64                     fe80::200:87ff:fe28:90d7%VLAN0007
     VLAN0007       2/0      RIPng         4s     , Distance: 120/0/0, Tag: 0,
AS-Path: IGP (Id 1), Communities: -, LocalPref: -, <Int Gateway>
```

30.3.5 広告経路フィルタリングする前の経路の確認

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。

ルーティングテーブルの優先経路を表示するには，運用コマンド show ipv6 route を実行してください。

図 30-12 ルーティングテーブル経路表示例

```
> show ipv6 route
Date 2006/03/14 12:00:00 UTC
Total: 7 routes
Destination                                 Next Hop
      Interface      Metric   Protocol    Age
::1/128                                     ::1
      localhost      0/0      Connected    5h  7m
3ffe:177:7:7::/64                           3ffe:177:7:7::1
      VLAN0007       0/0      Connected    1h  2m
3ffe:177:7:7::1/128                         ::1
      localhost      0/0      Connected    1h  2m
3ffe:3b01:6705:1::/64                       fe80::200:87ff:fe28:90d7%VLAN0007
      VLAN0007       2/0      RIPng       35s
3ffe:3b11:6705:1::/64                       fe80::200:87ff:fe28:90d7%VLAN0007
      VLAN0007       -/-      BGP4+       14m 29s
3ffe:3b21:6705:1::/64                       fe80::200:87ff:fe28:90d7%VLAN0007
      VLAN0007       1/1      OSPFv3 ext2 26m 47s
3ffe:8703:2005:1::/64                       3ffe:177:7:7::145
      VLAN0007       0/0      Static      23m 59s
```

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，運用コマンド show ipv6 route にパラメータとしてプロトコルを指定して実行してください。

図 30-13 ルーティングテーブル経路表示例 (BGP4+ だけ)

```
> show ipv6 route bgp
Date 2006/03/14 12:00:00 UTC
Total: 1 routes
Destination                                 Next Hop
      Interface      Metric   Protocol  Age
3ffe:3b11:6705:1::/64                       fe80::200:87ff:fe28:90d7%VLAN0007
      VLAN0007       -/-      BGP4+     34m  8s
```

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，運用コマンド show ipv6 route にパラメータ -F を指定して実行してください。

図 30-14 ルーティングテーブル経路表示例 (詳細表示)

```
> show ipv6 route -F
Date 2006/03/14 12:00:00 UTC
Total: 7 routes
Destination                                Next Hop
      Interface    Metric  Protocol    Age
::1/128                                    ::1
      localhost    0/0     Connected    5h 27m , Distance: 0/0/0, Tag: 0, AS-Pa
th: IGP (Id 1), Communities: -, LocalPref: -, <NoAdvise Active Retain>
3ffe:177:7:7::/64                          3ffe:177:7:7::1
      VLAN0007     0/0     Connected    1h 22m , Distance: 0/0/0, Tag: 0, AS-Pa
th: IGP (Id 1), Communities: -, LocalPref: -, <Active Retain>
3ffe:177:7:7::1/128                        ::1
      localhost    0/0     Connected    1h 22m , Distance: 0/0/0, Tag: 0, AS-Pa
th: IGP (Id 1), Communities: -, LocalPref: -, <NoAdvise Int Active Retain>
3ffe:3b01:6705:1::/64                      fe80::200:87ff:fe28:90d7%VLAN0007
      VLAN0007     2/0     RIPng       13s     , Distance: 120/0/0, Tag: 0, AS-
Path: IGP (Id 1), Communities: -, LocalPref: -, <Int Active Gateway>
3ffe:3b11:6705:1::/64                      fe80::200:87ff:fe28:90d7%VLAN0007
      VLAN0007     -/-     BGP4+       34m 56s , Distance: 20/0/0, Tag: 0, AS-P
ath: 1000 IGP (Id 3), Communities: -, LocalPref: 100, <Ext Active Gateway>
3ffe:3b21:6705:1::/64                      fe80::200:87ff:fe28:90d7%VLAN0007
      VLAN0007     1/1     OSPFv3 ext2 47m 15s , Distance: 110/1/0, Tag: 0, AS
-Path: IGP (Id 1), Communities: -, LocalPref: -, <Int Ext Active Gateway>
3ffe:8703:2005:1::/64                      3ffe:177:7:7::145
      VLAN0007     0/0     Static      44m 27s , Distance: 2/0/0, Tag: 0, AS-Pa
th: IGP (Id 1), Communities: -, LocalPref: -, <Remote Int Active Gateway>
```

BGP4+ では，ルーティングテーブル上にある BGP4+ の優先でない経路も広告対象になることがあります。ルーティングテーブル上にある BGP4+ 経路を優先でない経路も含めて表示するには，運用コマンド show ipv6 route にパラメータ all-routes を指定し，さらにパラメータとして bgp を指定して実行してください。

図 30-15 ルーティングテーブル経路表示例 (無効経路を含む，BGP4+ だけ)

```
> show ipv6 route all-routes bgp
Date 2006/03/14 12:00:00 UTC
Status Codes: * valid, > active
Total: 2 routes
   Destination                             Next Hop
        Interface     Metric Protocol Age
*> 3ffe:3b11:6705:1::/64                   fe80::200:87ff:fe28:90d7%VLAN0007┐
        VLAN0007      -/-    BGP4+    35m 57s                                 │
*  3ffe:8703:2005:1::/64                   fe80::200:87ff:fe28:90d7%VLAN0007 │
        VLAN0007      -/-    BGP4+    35m 57s                                 ┘
                                                                              ※
```

注※

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。

30.3.6 RIPng 広告経路の確認

RIPng の広告経路を確認するには運用コマンド show ipv6 rip にパラメータ advertised-routes を指定して実行してください。広告先のインタフェース名と，そこへ広告している経路・経路属性を表示します。

図 30-16 RIPng 広告経路表示例

```
> show ipv6 rip advertised-routes
Date 2006/03/14 12:00:00 UTC

Target Interface: VLAN0006
Destination                                Next Hop
      Interface      Metric   Tag   Age
3ffe:3b01:6705:1::/64                      fe80::200:87ff:fe28:90d7%VLAN0007
      VLAN0007       2        0      3s
```

30.3.7 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運用コマンド show ipv6 ospf にパラメータ database を指定し，さらに external と self-originate を指定して実行してください。

図 30-17 AS-External-LSA 表示例 (自装置生成分だけ)

```
> show ipv6 ospf database external self-originate
Date 2006/03/14 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: 3ffe:177:7:7::/64                                          …1
       Prefix Options: <>
       Type: 2, Metric: 20, Tag: 100
```

1. Prefix（3ffe:177:7:7::/64）は経路宛先ネットワークを示します。

30.3.8 BGP4+ 広告経路の確認【OP-BGP】

BGP4+ の広告経路を確認するには，運用コマンド show ipv6 bgp にパラメータ advertised-routes を指定して実行してください。

図 30-18 BGP4+ 広告経路表示例

```
> show ipv6 bgp advertised-routes
Date 2006/03/14 12:00:00 UTC
BGP4+ Peer: 3ffe:192:158:1::145, Remote AS: 1000
Local AS: 200, Local Router ID: 200.201.202.203
Origin Codes: i - IGP, e - EGP, ? - incomplete
Network                                    Next Hop
      MED    LocalPref Path
3ffe:3b11:6705:1::/64                      fe80::200:87ff:fe28:90d7%VLAN0007
      -      -         200 1000 i
3ffe:8703:2005:1::/64                      fe80::200:87ff:fe28:90d7%VLAN0007
      -      -         200 1000 i
```

BGP4+ の広告経路の詳細な経路属性を確認するには，運用コマンド show ipv6 bgp にパラメータ advertised-routes を指定し，さらに -F を指定して実行してください。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 30-19　BGP4+ 広告経路表示例 (詳細表示)

```
> show ipv6 bgp advertised-routes -F
Date 2006/03/14 12:00:00 UTC
BGP4+ Peer: 3ffe:192:158:1::145, Remote AS: 1000
Local AS: 200, Local Router ID: 200.201.202.203
Route 3ffe:3b11:6705:1::/64
*> Next Hop fe80::200:87ff:fe28:90d7%VLAN0007
     MED: -, LocalPref: -, Type: External route
     Origin: IGP, IGP Metric: 0
     Path: 200 1000
     Next Hop Attribute: 3ffe:192:158:1::1
                         fe80::4048:47ff:fe10:4
     Communities: 200:1200
Route 3ffe:8703:2005:1::/64
*  Next Hop fe80::200:87ff:fe28:90d7%VLAN0007
     MED: -, LocalPref: -, Type: External route
     Origin: IGP, IGP Metric: 0
     Path: 200 1000
     Next Hop Attribute: 3ffe:192:158:1::1
                         fe80::4048:47ff:fe10:4
     Communities: 200:1200
```

30.3.9　エクストラネットの確認【OP-NPAR】

運用コマンド show ipv6 route 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 30-20　show ipv6 route コマンドの表示例

```
> show ipv6 route vrf 2 extra-vrf
Date 2009/03/14 12:00:00 UTC
VRF:2  Total: 1 routes
Destination                                Next Hop
     Interface     Metric  Protocol  Age
3ffe:210:6705:1::/64                       3ffe:501:811:ff01::1
     VLAN0010      0/0     Extra-Vrf 365d
:
>
> show ipv6 route vrf 3 extra-vrf
Date 2009/03/14 12:00:00 UTC
VRF:3  Total: 1 routes
Destination                                Next Hop
     Interface     Metric  Protocol  Age
3ffe:109:2011:1::/64                       3ffe:500:811:1000::1
     VLAN0011      0/0     Extra-Vrf 365d
>
```

31 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。

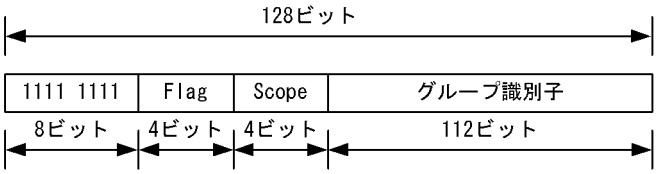
31.1 IPv6 マルチキャスト概説

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,「14.1 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。

31.1.1 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データの送受信に参加している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 31-1 マルチキャストアドレスのフォーマット



31.1.2 IPv6 マルチキャストルーティング機能

本装置は受信した IPv6 マルチキャストパケットを IPv6 マルチキャスト中継エントリに従って中継します。IPv6 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。

- IPv6 マルチキャストグループマネージメント機能
  IPv6 グループメンバーシップ情報の送受信を行い IPv6 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。
- IPv6 経路制御機能
  経路情報を送受信して中継経路を決定し，IPv6 マルチキャスト経路情報および IPv6 マルチキャスト中継エントリを作成する機能です。経路情報収集には PIM-SM(PIM-SSM を含む) を使用します。
- IPv6 中継機能
  IPv6 マルチキャストパケットを IPv6 マルチキャスト中継エントリに従いハードウェアおよびソフトウェアで中継する機能です。
  本装置の IPv6 マルチキャスト中継機能を QoS 機能やフィルタ機能などと併用することによって，IPv6 マルチキャストに QoS 機能を持たせたり不要なパケットをフィルタリングしたりすることもできます。

31.2 IPv6 マルチキャストグループマネージメント機能

IPv6 マルチキャストグループマネージメント機能とは，ルーターホスト間での IPv6 グループメンバー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 IPv6 マルチキャストグループメンバーの存在を学習する機能です。本装置では IPv6 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に MLD をサポートしています。

31.2.1 MLD の概要

MLD はルーターホスト間で使用される IPv6 マルチキャストグループ管理プロトコルで，IPv4 マルチキャストの IGMP と同様の機能を持っています。

MLD を使用すると，ルータからの IPv6 マルチキャストグループの参加問い合わせとホストからの IPv6 マルチキャストグループへの参加・離脱報告によって，ルータはホストの IPv6 マルチキャストグループへの参加・離脱を認識して IPv6 マルチキャストパケットを中継・遮断します。通信に使用するアドレスに IPv6 アドレスを使用する点以外は，IGMP とまったく同じです。

MLD はバージョン 1 とバージョン 2 が RFC で規定されています。

MLDv2 は IPv6 マルチキャストグループマネージメント機能を実現する MLDv1 を拡張したプロトコルで，指定した送信元からのマルチキャストパケットだけを受信する送信元フィルタリング機能が導入されています。IPv6 マルチキャストグループへの参加・離脱報告時に送信元指定が可能であるため，MLDv2 と PIM-SSM を組み合わせて使用することで，効率のよい IPv6 マルチキャスト中継が実現できます。

本装置が送信する MLDv1 メッセージのフォーマットおよび設定値は RFC2710 に従います。また，MLDv2 メッセージのフォーマットおよび設定値は RFC3810 に従います。

31.2.2 MLD の動作

(1) MLDv1 の動作

本装置がサポートする MLDv1 メッセージの仕様を次の表に示します。

表 31-1 MLDv1 メッセージ

タイプ		意味	サポート	
			送信	受信
Multicast Listener Query	General Query	IPv6 マルチキャストグループの参加問い合わせ (全グループ宛て)	○	○
	Group-Specific Query	IPv6 マルチキャストグループの参加問い合わせ (特定グループ宛て)	○	○
Multicast Listener Report		加入している IPv6 マルチキャストグループの報告	×	○
Multicast Listener Done		IPv6 マルチキャストグループからの離脱報告	×	○

(凡例) ○：サポートする　×：サポートしない

(2) MLDv2 の動作

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機能を実現します。フィルタモードには次の二つのモードがあります。

- INCLUDE：指定された送信元リストからのパケットだけ中継します
- EXCLUDE：指定された送信元リスト以外からのパケットだけ中継します

本装置がサポートする MLDv2 メッセージの仕様を次の表に示します。

表 31-2 MLDv2 メッセージ

タイプ		意味	サポート	
			送信	受信
Version 2 Multicast Listener Query	General Query	IPv6 マルチキャストグループの参加問い合わせ（全グループ宛て）	○	○
	Multicast Address Specific Query	IPv6 マルチキャストグループの参加問い合わせ（特定グループ宛て）	○	○
	Multicast Address and Source Specific Query	IPv6 マルチキャストグループの参加問合せ（特定の送信元およびグループ宛て）	○	○
Version 2 Multicast Listener Report	Current StateReport	加入している IPv6 マルチキャストグループとフィルタモード報告	×	○
	State ChangeReport	加入している IPv6 マルチキャストグループとフィルタモードの更新報告	×	○

（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グループ加入後に変更することが可能で，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 31-3 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	○ （送信元リストは無視します）
State Change Report	CHANGE_TO_ INCLUDE_MODE	フィルタモードを INCLUDE 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 に変更することを示します	○ （送信元リストは無視します）
	ALLOW_NEW_ SOURCES	データの受信を希望する送信元を追加することを示します	○
	BLOCK_OLD_ SOURCES	データの受信を希望する送信元を削除することを示します	○

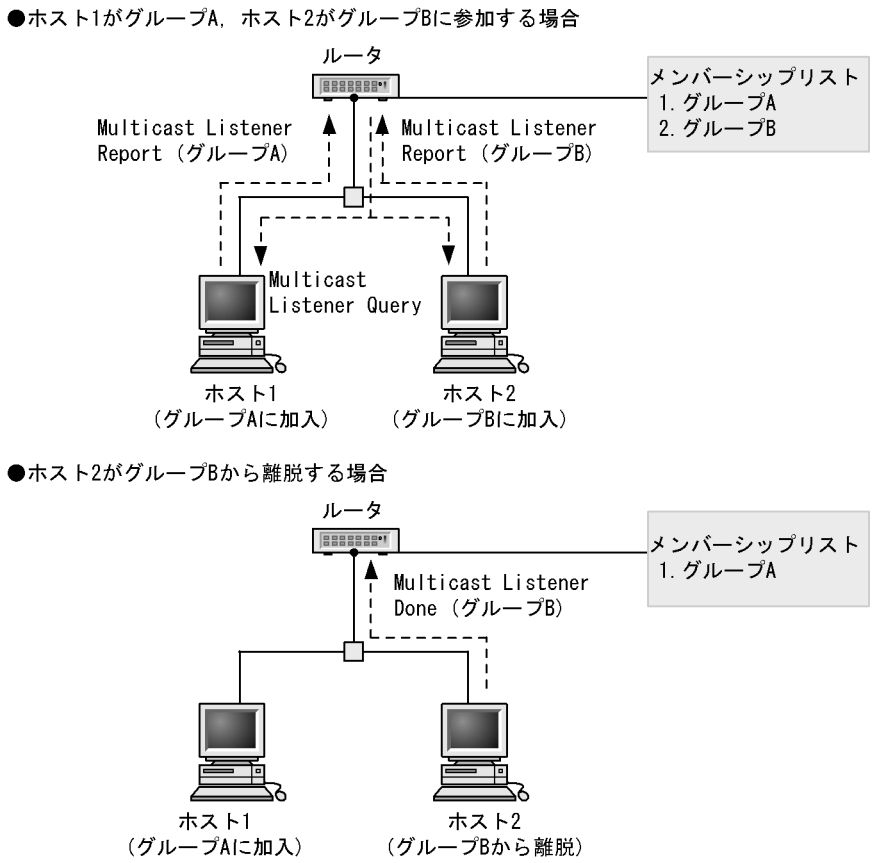
（凡例） ○：サポートする

MLDv1 メッセージを使用した MLDv1 の動作を次に示します。

- IPv6 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 IPv6 マルチキャストメンバーシップの情報を得るために，定期的に Multicast Listener 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。
- ホストは Multicast Listener Query を受信すると，Multicast Listener Report を該当するグループ宛てに送信することで，グループへの参加状況を報告します。
- ホストから Multicast Listener Report を受信すると，IPv6 マルチキャストルータはメンバーシップリストにそのグループを追加します。
- Multicast Listener Done メッセージを受信するとそのグループをメンバーシップリストから削除します。

MLDv1 グループ参加・離脱動作を次の図に示します。

図 31-2　MLDv1 グループ参加・離脱動作



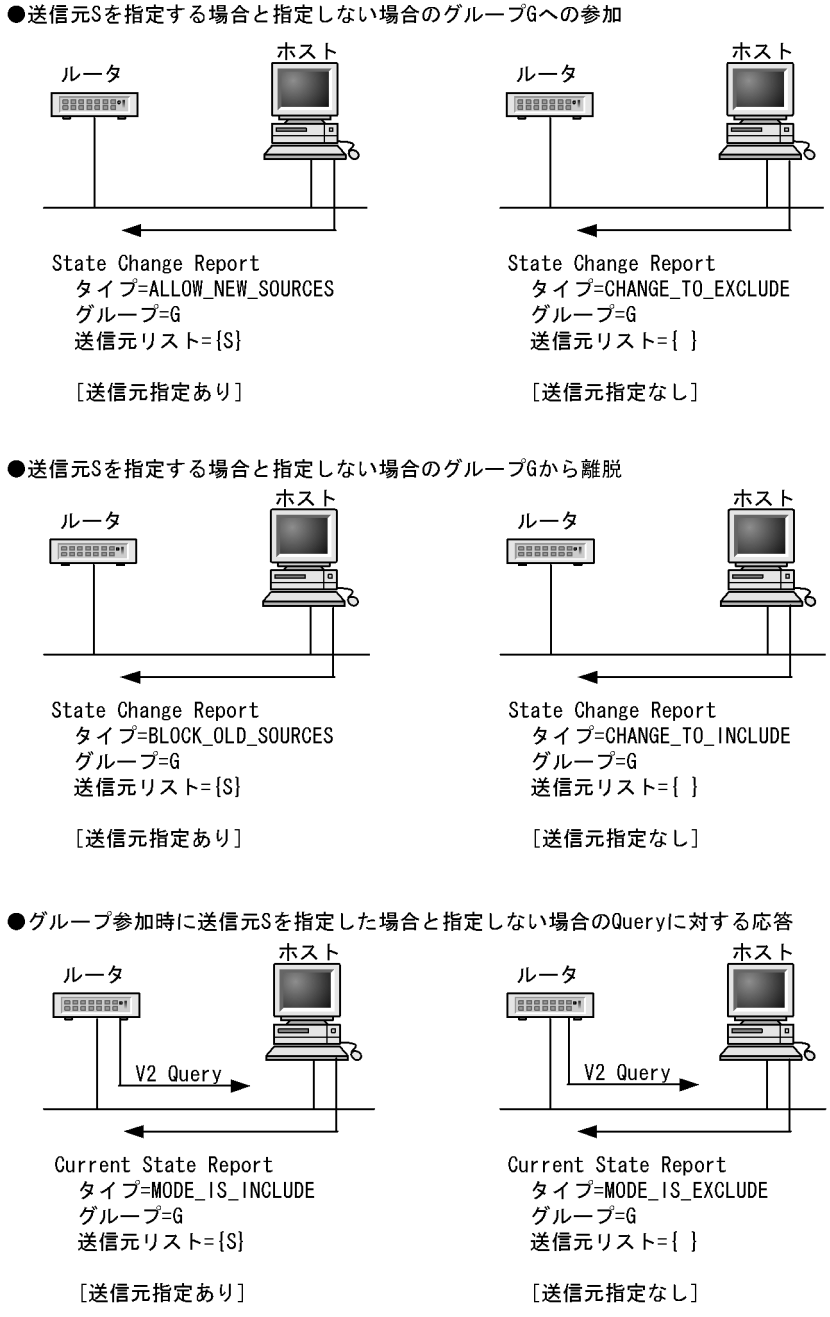
MLDv2 メッセージを使用した MLDv2 の動作を次に示します。

- IPv6 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 IPv6 マルチキャストメンバーシップの情報を得るために，定期的に Version 2 Multicast Listener 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。
- ホストは Version 2 Multicast Listener Query を受信すると，Version 2 Multicast listener Report（Current State Report）を ff02::16 宛てに送信することで，グループへの参加状況を報告します。
- ホストから Version 2 Multicast Listener Report（State Change Report）メッセージを受信すると

IPv6 マルチキャストルータは Multicast Address Record タイプの内容に応じてメンバーシップリストへのグループ追加，あるいはメンバーシップリストからのグループ削除を行います。

ホストからの MLDv2 Report メッセージ送信動作を次の図に示します。

図 31-3　MLDv2 グループ参加・離脱動作



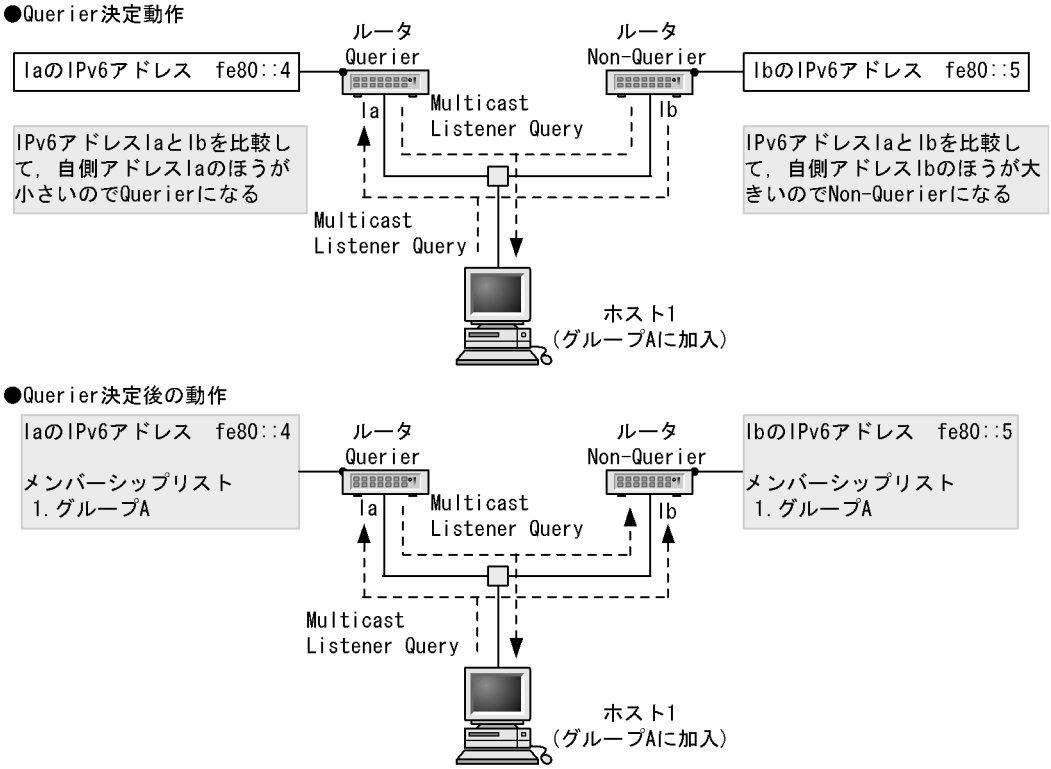
31.2.3　Querier の決定

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 Multicast Listener 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 Multicast Listener Query 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，Multicast Listener Query 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 31-4　Querier と Non-Querier の決定



Querier になった場合，送信元 IPv6 アドレスが自インタフェースより小さい Multicast Listener Query を受信するまで Querier として動作して，Multicast Listener Query を定期的（125 秒）に送信します。Non-Querier が Querier として動作するのは次に示す場合です。

- Querier の送信した Multicast Listener Query を監視し，Multicast Listener Query 受信時に Multicast Listener Query の送信元 IPv6 リンクローカルアドレスが自インタフェースのリンクローカルアドレスよりも大きい場合
- Multicast Listener Query を一定時間（255 秒）受信しなかった場合

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。

MLDv2 ルータは MLDv1 ルータと同じ方法で Querier を決定します。

31.2.4 IPv6 グループメンバーの管理

(1) MLDv1 使用時の IPv6 グループメンバー管理

MLDv1 使用時の IPv6 グループメンバーの登録および削除について説明します。

ホストから Multicast Listener Report を受信することで IPv6 グループメンバーを登録します。なお，Non-Querier でもホストからの Multicast Listener Report を受信することによって Querier 同様に IPv6 グループメンバーを登録します。

Querier が，ホストからある IPv6 グループへの離脱報告である Multicast Listener Done メッセージを受信した場合，離脱報告を受けたグループメンバーに参加しているそのほかのホストの存在を確認するために，該当するグループ宛てに Multicast Listener Query（Group-Specific Query）メッセージを連続して（1 秒間隔）送信します。このメッセージを 2 回送信したあと，Multicast Listener Report を 1 秒間受信しない場合，該当するグループを削除します。なお，Non-Querier の場合は Multicast Listener Done メッセージを無視し，Querier が送信した Multicast Listener Query（Group-Specific Query）メッセージを 2 回受信したあと Multicast Listener Report を 1 秒間受信しない場合，該当するグループを削除します。

(2) MLDv2 使用時の IPv6 グループメンバー管理

MLDv2 使用時の IPv6 グループメンバーの登録および削除について説明します。

ホストからマルチキャストグループへの加入要求を示す Report を受信することでグループ情報を登録します。ここでグループ情報とは，グループアドレスと当該グループアドレスへの送信元アドレスを指します。Querier，Non-Querier ともに Report を受信することでグループ情報を登録します。

Querier は，マルチキャストグループからの離脱要求を示す Report を受信すると，当該グループメンバーに参加しているほかのホストの存在を確かめるために，送信元リストの指定有無に応じて次に示すメッセージを 1 秒間隔で送信します。

- 送信元リスト指定無し：Multicast Address Specific Query メッセージ
- 送信元リスト指定有り：Multicast Address and Source Specific Query メッセージ

本装置が Querier の場合は上記のメッセージを 2 回送信後，1 秒間 Report を受信しない場合該当するグループ情報を削除します。本装置が Non-Querier の場合は Querier が送信する上記メッセージを受信後，該当するグループ情報の削除処理を実行します。

31.2.5 MLD 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 31-4 MLDv1 タイマ値

タイマ	内容	デフォルト値 (秒)	コンフィグレーションによる設定範囲 (秒)	備考
Query Interval	Multicast Listener Query 送信周期時間	125	60 ～ 3600	―
Query Response Interval	Multicast Listener Report 最大応答待ち時間	10	―	―

タイマ	内容	デフォルト値 (秒)	コンフィグレーションによる設定範囲 (秒)	備考
Other Querier Present Interval	Querier 監視時間	255	Query interval × 2 + QueryResponse Interval / 2	左記計算式より算出。
Startup Query Interval	Startup 時 GenaralQuery を送信する時間	30	Query Interval / 4	左記計算式より算出。
Last Member Query Interval	Done 受信後の Specific Query 送信周期	1	―	―
Multicast Listener Interval	グループメンバーの保持時間	260	Query interval × 2 + QueryResponse Interval	左記計算式より算出。

(凡例) ―：該当しない

本装置が使用する MLDv2 タイマ値を次の表に示します。

表 31-5 MLDv2 タイマ値

タイマ	内容	デフォルト値 (秒)	コンフィグレーションによる設定範囲 (秒)	備考
Query Interval	Multicast Listener Query 送信周期時間	125	60 ～ 3600	―
Query Response Interval	Multicast Listener Report 最大応答待ち時間	10	―	―
Other Querier Present Interval	Querier 監視時間	255	Query Interval × 2 + QueryResponse Interval / 2	左記計算式より算出。
Startup Query Interval	Startup 時 General Query を送信する時間	30	Query Interval / 4	左記計算式より算出。
Last Listener Query Interval	離脱要求受信後の Specific Query 送信周期	1	―	―
Multicast Address Listening Interval	グループメンバーの保持時間	260	Query Interval × 2 + Query Response Interval	左記計算式より算出。
Older Version Host Present Interval	MLDv2 マルチキャストアドレス互換モードへの移行時間	260	Query Interval × 2 + Query Response Interval	左記計算式より算出。

(凡例) ―：該当しない

31.2.6 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の 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 31-6 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 パケットは無視します。
version 2	MLDv1，MLDv2 の両方で動作可能です。 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 パケットは無視します。

(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 Query を受信することで Querier を決定します（「31.2.3 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 あるいは version 2 only に設定されているインタフェースでの MLDv1 ルータとの接続はサポートしません（V1 Query 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，当該インタフェースの MLD バージョンを version 1 に設定してください。

(2) MLDv1/MLDv2 ホスト混在時の動作

MLDv1 ホストと MLDv2 ホストが混在するネットワークと接続する場合は，当該インタフェースの 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 ホストは MLDv2 Query を MLDv1 Query として受信できる（RFC 仕様）ことが必要になります。

MLDv1/MLDv2 ホストが混在する場合，グループメンバーの登録はグループ加入を要求する MLD のバージョンによって次の表に従います。

表 31-7 MLDv1/MLDv2 ホスト混在時のグループメンバー登録

グループ加入の要求	グループメンバーの登録
MLDv1 で受信	MLDv1 モードでグループメンバーを登録
MLDv2 で受信	MLDv2 モードでグループメンバーを登録
MLDv1 と MLDv2 で受信	MLDv1 モードでグループメンバーを登録

31.2.7 静的グループ参加

MLD 対応ホストが存在しないネットワークに IPv6 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。

静的グループ参加を設定したインタフェースは，Multicast Listener Report を受信しなくてもグループ参加したものと同様の動作を行います。

この機能は MLDv1 の機能のため，当該インタフェースの 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 に設定されている場合は MLDv1 でグループ参加したものと同様の動作を行います。

31.2.8 MLD 使用時の注意事項

- 構成変更によって静的グループ参加を設定した場合，PIM-SM グループの場合は (*,G) エントリ，PIM-SSM グループの場合は (S,G) エントリが作成されるまで最大 125 秒かかります。

- コンフィグレーションで設定している SSM アドレスの範囲外のグループに対して，送信元指定ありの MLDv2 Report を受信した場合は全送信元からのマルチキャストパケットを中継します。

31.3 IPv6 マルチキャスト中継機能

IPv6 マルチキャストパケットの中継処理は IPv6 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 IPv6 マルチキャストパケットの中継情報をハードウェアの IPv6 マルチキャスト中継エントリに登録します。登録された IPv6 パケットはハードウェアで中継を行い，登録されていない IPv6 パケットはソフトウェアの IPv6 マルチキャスト経路情報から生成した IPv6 マルチキャスト中継エントリに従って中継を行います。中継対象アドレスについての制限を除き，IPv4 マルチキャスト中継機能とは特別な違いはありません。

31.3.1 中継対象アドレス

IPv6 マルチキャストアドレスのうち，ノードローカル・マルチキャストアドレスおよびリンクローカル・マルチキャストアドレスは IPv6 マルチキャスト中継処理の対象外です。

IPv6 マルチキャストアドレスについては，「17.1.5　マルチキャストアドレス」を参照してください。

31.3.2 IPv6 マルチキャストパケット中継処理

IPv6 マルチキャストのパケット中継はハードウェアの中継処理，ソフトウェアの中継処理によって行われます。

(1) ハードウェアの中継処理

ハードウェアによる IPv6 マルチキャストのパケット中継処理は次に示す四つの手順で実行されます。

1. IPv6 マルチキャスト中継エントリの検索
   IPv6 マルチキャストグループ宛てのパケットを受信した場合，ハードウェアの IPv6 マルチキャスト中継エントリから該当エントリを検索します。
2. パケット受信インタフェースの正常性チェック
   1 の手順でエントリが存在した場合，その IPv6 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。
3. フィルタリング
   IPv6 フィルタリングテーブルに登録された情報を参照して中継するかどうかを判断します。
4. ホップリミットに基づいた中継判断と TTL 値のデクリメント
   パケット中のホップリミット値から中継するかを判断し，中継する場合は該当するパケットのホップリミット値をデクリメントします。

(2) ソフトウェアの中継処理

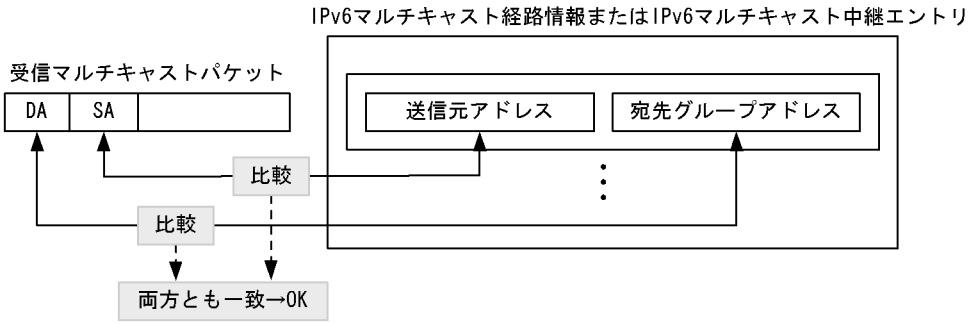
ソフトウェアによる IPv6 マルチキャストパケット中継処理は次に示す場合ごとに処理が異なります。

- ハードウェアの IPv6 マルチキャスト中継エントリにエントリがない場合
  ある送信元からある IPv6 マルチキャストグループ宛てのパケットを最初に受信した場合，IPv6 マルチキャスト経路情報から生成した中継エントリに従って，ソフトウェアで中継します。同時にハードウェアに対して IPv6 マルチキャスト中継エントリを登録します。
- IPv6 カプセル化処理を行う場合
  一時的にランデブーポイント宛てに IPv6 カプセル化を行って中継し，ランデブーポイントでは各中継先にデカプセル化して中継します。

(3) IPv6 マルチキャスト経路情報または IPv6 マルチキャスト中継エントリの検索

受信した IPv6 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 IPv6 マルチキャスト経路情報または IPv6 マルチキャスト中継エントリから検索します。IPv6 マルチキャスト経路情報または IPv6 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 31-5 IPv6 マルチキャスト経路情報または IPv6 マルチキャスト中継エントリの検索方法



(4) VRF 機能【OP-NPAR】

複数の VRF で IPv6 マルチキャストを動作させた場合，IPv6 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 IP アドレスの IPv6 マルチキャスト中継エントリを作成できます。また，IPv6 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。

31.3.3 ネガティブキャッシュ

ネガティブキャッシュは，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は中継先インタフェースの存在しない中継エントリです。ネガティブキャッシュは，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。

31.3.4 系切替時の通信無停止対応機能

IPv6 PIM-SSM は冗長構成運用による系切替時に，マルチキャスト中継を無停止で継続できる通信無停止対応機能をサポートしています。

系切替後，460 秒間は系切替前の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。この系切替後の 460 秒を再学習時間として，再学習時間内に学習されなかったエントリは削除されます。再学習時間の開始時と終了時は運用ログを出力します。

本機能は，コンフィグレーションコマンド ipv6 pim nonstop-forwarding を設定した場合だけ有効になります。ただし，VRF のインタフェースで IPv6 マルチキャストを動作させた場合，本機能は無効になります。

また，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 mroute
- show ipv6 mcache

- show ipv6 pim mcache

31.4 IPv6 経路制御機能

IPv6 マルチキャスト経路制御機能とは，IPv6 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グループ情報を基に，IPv6 マルチキャスト経路情報および IPv6 マルチキャスト中継エントリを作成する機能です。

31.4.1 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。本装置が送信する IPv6 PIM-SM メッセージのフォーマットおよび設定値は RFC2362 に従います。

- PIM-SM（Protocol Independent Multicast-Sparse Mode）
  ユニキャスト IPv6 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 で同一のグループを使用することはできません。また，同一ネットワーク内に PIM-SM が動作しているルータ，PIM-DM が動作しているルータが混在している場合，各ルータ間でマルチキャストパケットの中継は行われません。同一ネットワーク内でマルチキャストパケットの中継を行いたい場合は，すべてのルータで同じマルチキャストプロトコルが動作するように設定してください。

31.4.2 IPv6 PIM-SM

IPv6 PIM-SM メッセージのサポート仕様を次の表に示します。すべてのメッセージが送信および受信をサポートしています。

表 31-8 IPv6 PIM-SM メッセージのサポート仕様

タイプ	機能
PIM-Hello	PIM 隣接ルータの検出
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
PIM-Assert	Forwarder の決定
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カプセル化する。
PIM-Register-stop	Register メッセージを抑止する。
PIM-Bootstrap	BSR を決定する。またランデブーポイントの情報を配信する。
PIM-Candidate-RP-Advertisement	ランデブーポイントが BSR に自ランデブーポイント情報を通知する。

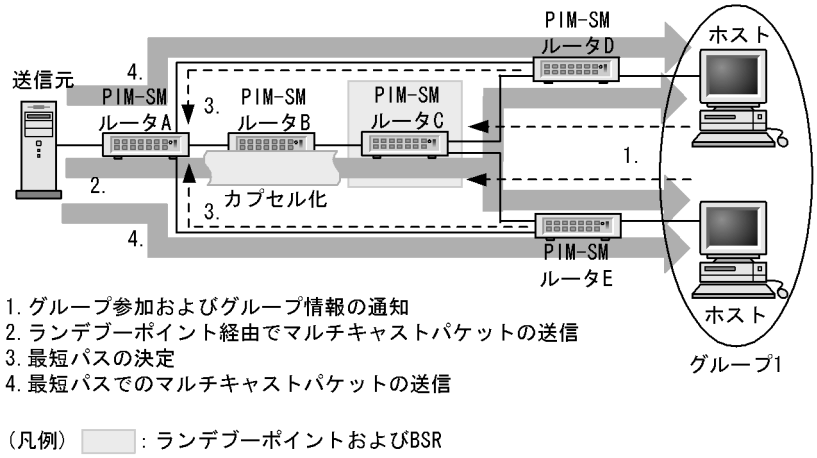
IPv6 PIM-SM の動作の流れを次に示します。

1. 各 IPv6 PIM-SM ルータは MLD で学習した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 IPv6 PIM-SM からグループ情報の受信で各グループの存在を認識します。
3. IPv6 PIM-SM は最初にマルチキャストパケットをその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ーに配送するために，送信元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. 送信元から各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

して送信元からの最短パスを決定します（最短パス配送ツリーを形成します）。
5. 送信元から最短パスで各グループメンバーへのマルチキャストパケット中継を行います。

PIM-SM の動作概要を次の図に示します。

図 31-6　PIM-SM の動作概要

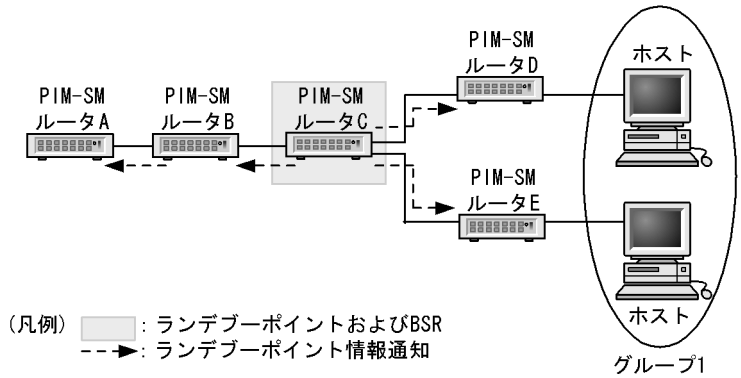


（1）ランデブーポイントおよびブートストラップルータ（BSR）

ランデブーポイントルータおよび BSR はコンフィグレーションで設定します。本装置では BSR はネットワーク（VPN）当たり最大 16 台とします。なお，IPv4 PIM-SM と IPv6 PIM-SM とで，ランデブーポイントおよび BSR を設定するルータを別にすることもできます。

BSR 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。この通知はホップバイホップで全 PIM ルータリンクローカル・マルチキャストアドレス（ff02::d）宛てに行われます。ランデブーポイントおよびブートストラップルータ（BSR）を次の図に示します。

図 31-7　ランデブーポイントおよびブートストラップルータ（BSR）

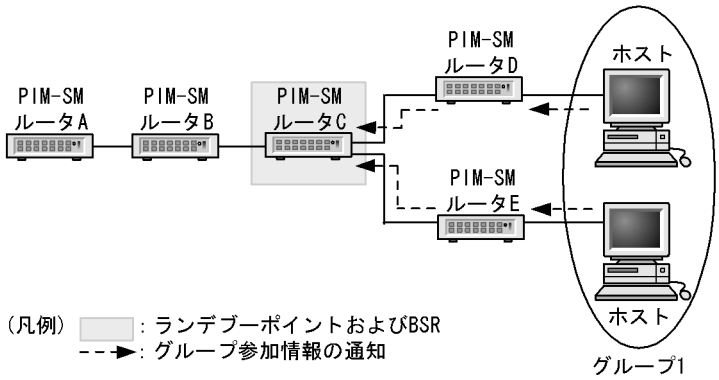


BSR（PIM-SM ルータ C）はランデブーポイント情報をすべての IPv6 マルチキャストインタフェースに通知します。ランデブーポイント情報を受信したルータはランデブーポイントの IPv6 アドレスを学習し，受信したインタフェース以外で IPv6 PIM ルータが存在するすべてのインタフェースにランデブーポイント情報を通知します。

(2) ランデブーポイントに対するグループ参加情報の通知

各ルータは MLD で学習した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装置アドレスになります。ランデブーポイントは IPv6 グループ情報を受信することで，IPv6 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に対するグループ参加情報の通知を次の図に示します。

図 31-8 ランデブーポイントへのグループ参加情報の通知



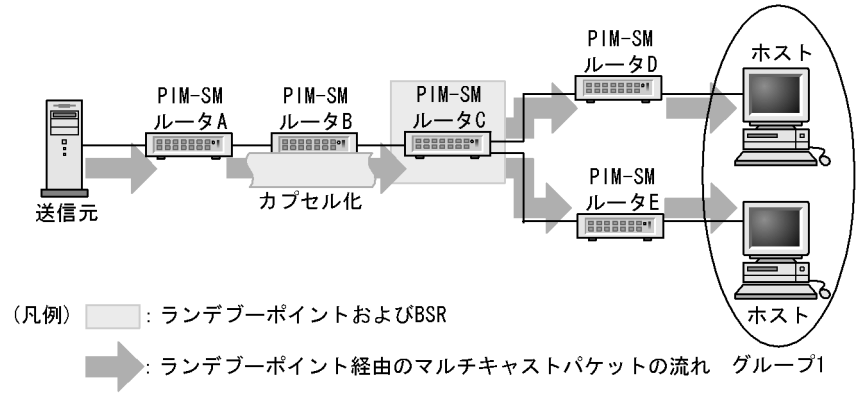
まず，各ホストは MLD でグループ 1 に参加します。PIM-SM ルータ D および PIM-SM ルータ E はグループ 1 情報を学習し，ランデブーポイント（PIM-SM ルータ C）にグループ 1 情報を通知します。ランデブーポイント（PIM-SM ルータ C）はグループ 1 情報を受信することによって受信したインタフェースにグループ 1 が存在することを学習します。

(3) IPv6 マルチキャストパケット通信（カプセル化）

送信元のサーバがグループ 1 宛ての IPv6 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 IPv6 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 IPv6 カプセル化（Register パケット）して送信します。本装置の場合，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装置アドレスになります（ランデブーポイントの IPv6 アドレスは「(1) ランデブーポイントおよびブートストラップルータ（BSR)」で学習済み)。

ランデブーポイント（PIM-SM ルータ C）は IPv6 カプセル化したパケットを受信すると，デカプセル化してグループ 1 が存在するインタフェースにグループ 1 宛てのマルチキャストパケットを中継します（グループ 1 の存在は「(2) ランデブーポイントに対する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，グループ 1 宛ての IPv6 マルチキャストパケットを受信すると，グループ 1 が存在するインタフェースに IPv6 マルチキャストパケットを中継します（グループ 1 の存在は「(2) ランデブーポイントに対するグループ参加情報の通知」の MLD で学習済み)。IPv6 マルチキャストパケット通信（カプセル化）を次の図に示します。

図 31-9 IPv6 マルチキャストパケット通信（カプセル化）



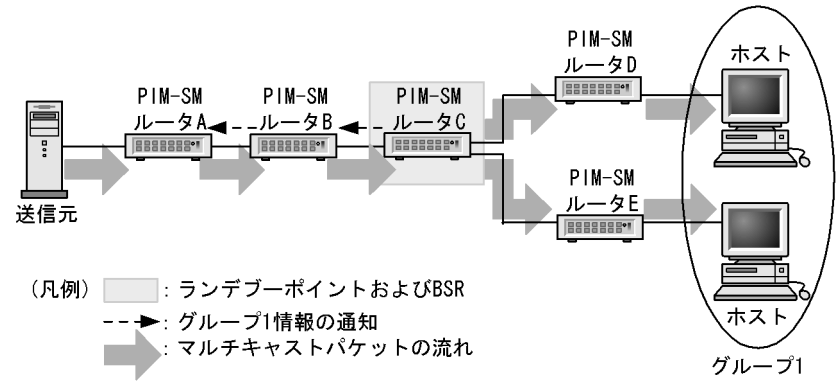
(4) IPv6 マルチキャストパケット通信（デカプセル化）

ランデブーポイント（PIM-SM ルータ C）は IPv6 カプセル化したパケットを受信すると，デカプセル化してグループ 1 が存在するインタフェースにグループ 1 宛ての IPv6 マルチキャストパケットを中継します（「(3) IPv6 マルチキャストパケット通信（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 IPv6 ユニキャストルーティング情報を基に決定された送信元のサーバへの最短経路方向にグループ 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 PIM ルータリンクローカル・マルチキャストアドレス（ff02::d）です。

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 は送信元サーバが送信したグループ 1 宛ての IPv6 マルチキャストパケットを IPv6 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。グループ 1 宛ての IPv6 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，PIM-SM ルータ E はグループ 1 が存在するインタフェースに中継します。IPv6 マルチキャストパケット通信（デカプセル化）を次の図に示します。

図 31-10 IPv6 マルチキャストパケット通信（デカプセル化）



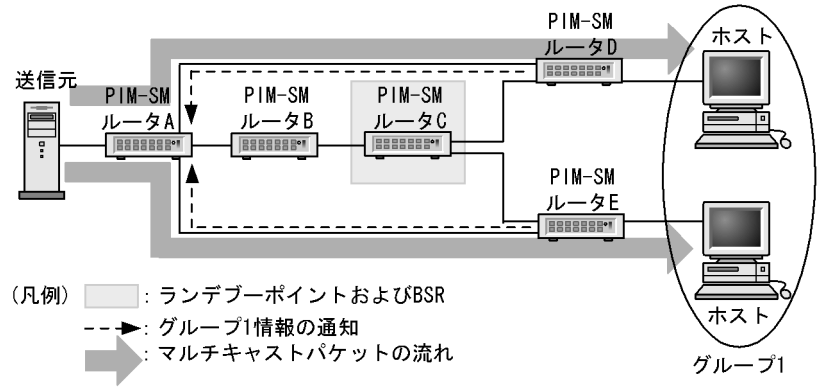
(5) 最短パスのマルチキャストパケット通信

PIM-SM ルータ D および PIM-SM ルータ E は，送信元サーバのグループ 1 宛て IPv6 マルチキャストパケットを受信した場合（「(4) IPv6 マルチキャストパケット通信（デカプセル化）」で説明），PIM-SM ルータ D および PIM-SM ルータ E は送信元サーバに対して最短のパス（既存の IPv6 ユニキャストルーティング情報）の方向にグループ 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

PIM ルータリンクローカル・マルチキャストアドレス（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グループ 1 の存在を認識し，送信元サーバのグループ 1 宛ての IPv6 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 IPv6 マルチキャストパケット通信を次の図に示します。

図 31-11　最短パスの IPv6 マルチキャストパケット通信

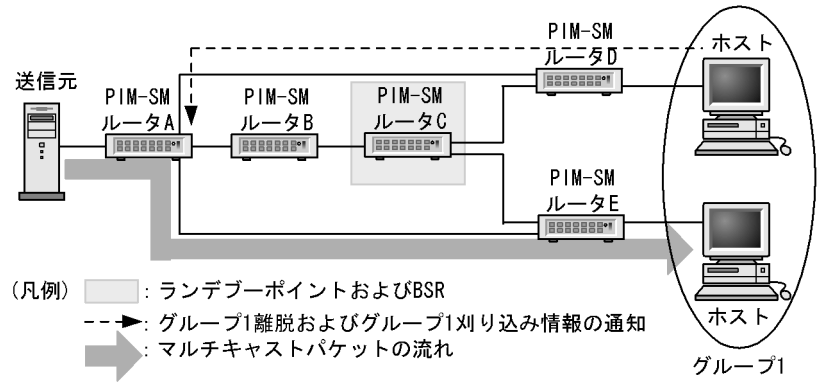


(6) IPv6 マルチキャスト配送ツリーの刈り込み

PIM-SM ルータ D は，ホストが MLD でグループ 1 から離脱をした場合，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 PIM ルータリンクローカル・マルチキャストアドレス（ff02::d）です。

PIM-SM ルータ A はグループ 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グループ 1 宛ての IPv6 マルチキャストパケットの中継を中止します。IPv6 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 31-12　IPv6 マルチキャスト配送ツリーの刈り込み



31.4.3　近隣検出

IPv6 PIM ルータは IPv6 PIM を有効にしたすべてのインタフェースに定期的に IPv6 PIM-Hello メッセージを送信します。PIM-Hello メッセージの送信先は全 PIM ルータリンクローカル・マルチキャストアドレス宛て（ff02::d）です。このメッセージを受信することによって近隣の IPv6 PIM 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（RFC4601

および draft-ietf-pim-sm-bsr-07 に準拠)。

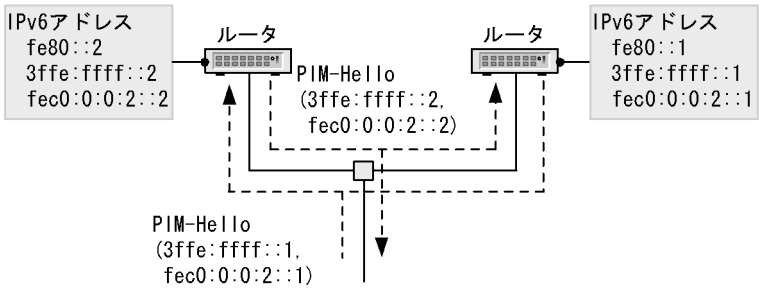
Generation ID はマルチキャストインタフェースごとに持つ 32 ビットの乱数で，PIM-Hello メッセージ送信時に Generation ID を付加して送信します。Generation ID はマルチキャストインタフェースが Up 状態になるたびに再生成します。受信した PIM-Hello メッセージに Generation ID オプションが付加されていれば Generation ID を記憶し，Generation ID の変化によって近隣装置のインタフェース障害を検出します。Generation ID の変化を検出すると，近隣装置情報の更新と PIM-Hello メッセージ，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ずに送信します。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 およびタイプ 65001）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ことによって，本装置は隣接する IPv6 PIM 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 IPv6 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によって本装置は送信者へ到達するための IPv6 PIM ルータを検出できます。

隣接 PIM ルータのアドレス受信例を次の図に示します。

図 31-13　PIM-Hello メッセージによる隣接ルータアドレス受信



31.4.4　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フォワードされる可能性があります。

PIM-SM ルータは同一 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フォワードする場合，PIM-Assert メッセージを使っ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，送信元ネットワークに対して最適な一つのルータをフォワーダとして選択します。

フォワーダ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。

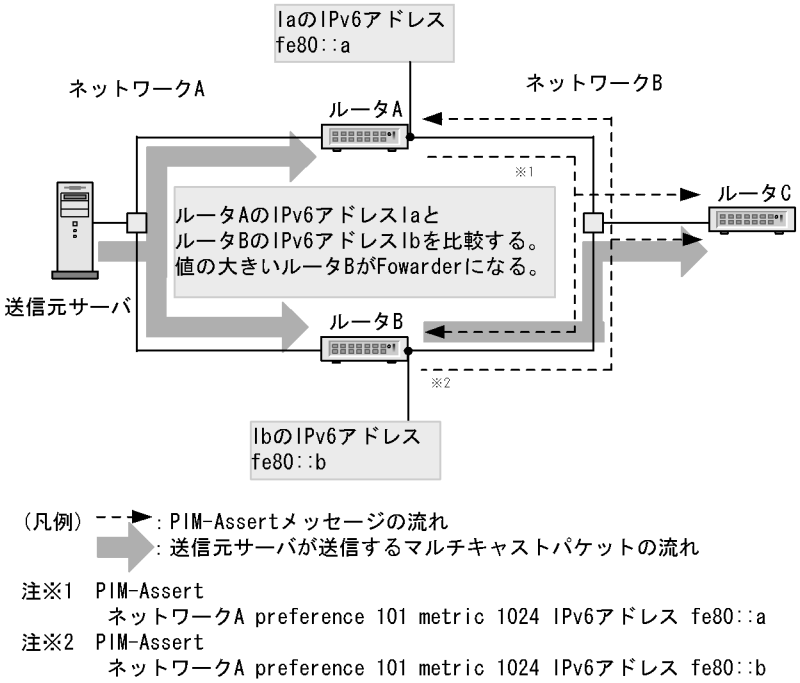
PIM-Assert メッセージによるフォワーダを決定する流れを次に示します。

1. プリファレンスを比較して，値が小さいルータがフォワーダになります。
2. プリファレンスが等しい場合に，メトリックを比較して，値が小さいルータがフォワーダになります。
3. メトリックが等しい場合に，各ルータの IP アドレスを比較して，IP アドレスが大きいルータがフォワーダになります。

本装置はマルチキャスト経路のプリファレンスを 101，メトリックを 1024 固定で PIM-Assert メッセージを送信します。ただし，送信者と直接接続する場合は，プリファレンスを 0，メトリックを 0 固定で PIM-Assert メッセージを送信します。また，コンフィグレーションによって，ユニキャストの情報から経路のディスタンスとメトリックを取得して，PIM-Assert メッセージのプリファレンスとメトリックとして送信することもできます。

Forwarder の決定を次の図に示します。

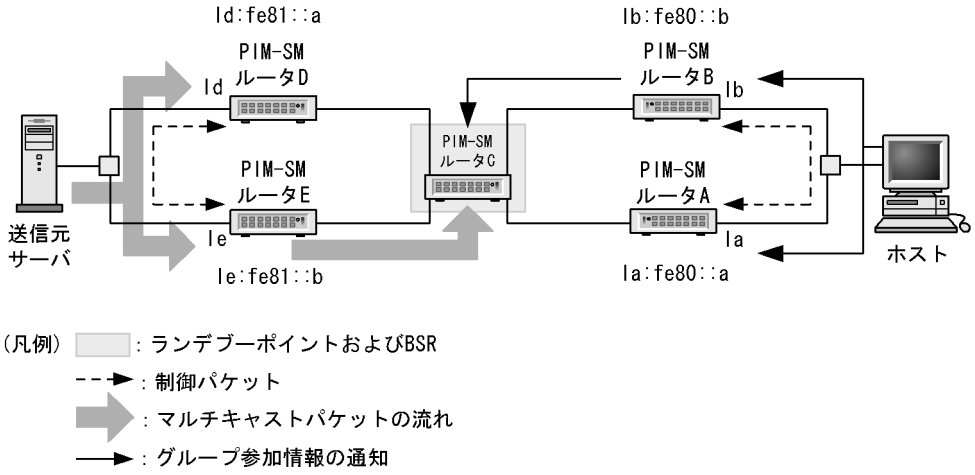
図 31-14　Forwarder の決定



31.4.5　DR の決定および動作

同一 LAN 上で複数の IPv6 PIM-SM ルータが存在する場合，その LAN 上での中継代表ルータ（DR）を決定します。そのインタフェース上で一番大きい IPv6 リンクローカルアドレスのルータが DR となります。受信ホストからのグループ参加情報は DR がランデブーポイント宛てにグループ参加情報の通知を行います。送信元サーバが送信したマルチキャストパケットは DR が IPv6 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 31-15 DR の動作



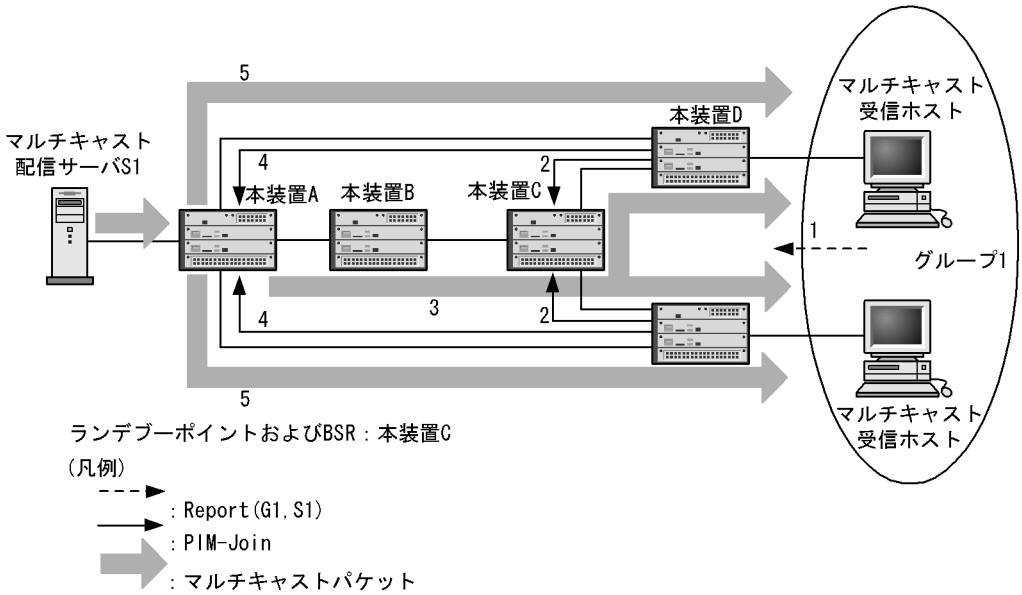
PIM-SM ルータ A と PIM-SM ルータ B の IPv6 アドレスを比較して PIM-SM ルータ B の IPv6 アドレスの方が大きい場合，PIM-SM ルータ B が DR となってランデブーポイントにグループ参加情報の通知を行います。PIM-SM ルータ D と PIM-SM ルータ E の IPv6 アドレスを比較して PIM-SM ルータ E の IPv6 アドレスの方が大きい場合，PIM-SM ルータ E が DR となってランデブーポイントに対して IPv6 カプセル化パケットを中継します。

31.4.6 MLDv2 使用時の IPv6 PIM-SM 動作

マルチキャスト配信サーバ（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 G1 にマルチキャストパケットを送信し，ホストが MLDv2 でグループ参加する場合の IPv6 PIM-SM 動作を次に示します。

1. ホスト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) を受信します。
2. MLDv2 Report(G1,S1) を受信した装置はランデブーポイントへの最短経路方向にグループアドレス (G1) を含んだ PIM-Join を送信します。
3. PIM-Join を受信したランデブーポイントは各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ーに配送するために，送信元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. 送信元から各グループメンバー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元からの最短パスを決定します（PIM-Join を送信元への最短経路方向に送信し，最短パス配送ツリーを形成します)。
5. マルチキャスト配信サーバ S1 がグループ G1 宛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いマルチキャストパケットを中継します。

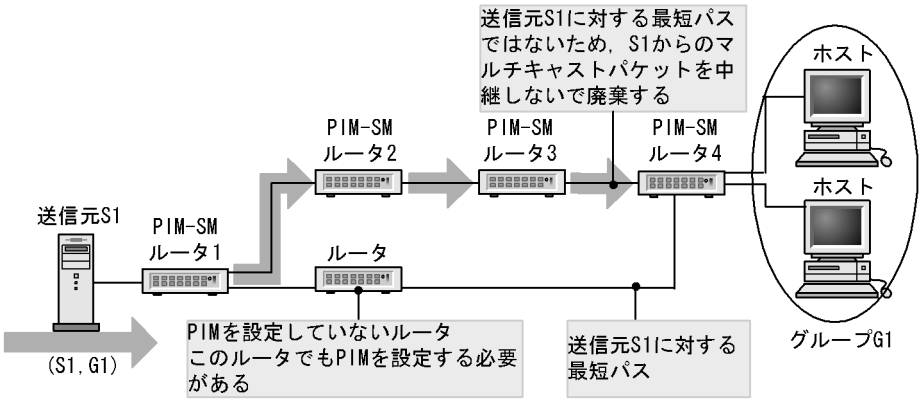
図 31-16　MLDv2 使用時の IPv6 PIM-SM 動作概要



31.4.7　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，IPv6 マルチキャストパケットがフォワード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 IPv6 PIM-SM の設定が必要になります。

図 31-17　冗長経路時の注意事項



31.4.8　IPv6 PIM-SM タイマ仕様

IPv6 PIM-SM タイマ値を次の表に示します。

表 31-9　IPv6 PIM-SM タイマ値

タイマ名	内容	デフォルト値（秒）	コンフィグレーションによる設定範囲（秒）	備考
Hello-Period	Hello の送信周期	30	5 ～ 3600	－
Hello-Holdtime	隣接関係の保持期間	105	3.5 × Hello-Period	左記計算式より算出。

タイマ名	内容	デフォルト値(秒)	コンフィグレーションによる設定範囲(秒)	備考
Assert-Timeout	Assert による中継抑止期間	180	―	―
Join/Prune-Period	Join/Prune の送信周期	60	30 ～ 3600	最大で +50% の揺らぎが生じます。
Join/Prune-Holdtime	経路情報および中継先インタフェースの保持期間	210	3.5 × Join/Prune-Period	左記計算式より算出。
Deletion-Delay-Time	Prune 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	1/3 × Join/Prune-Holdtime	0 ～ 300	※2
Data-Timeout (Keep-alive-time)	マルチキャスト中継エントリの保持期間	210	0（無期限），60 ～ 43200	最大で +90 秒の誤差が発生します。
Register-Supression-Timer	カプセル化送信の抑止期間	60	―	最大で± 30 秒の揺らぎが生じます。
Probe-Time	カプセル化送信の再開確認を送信する時間	5	5 ～ 60	デフォルトの 5 秒では Register-Supression-Timer が満了する 5 秒前にカプセル化送信の再開確認 (Null-Register) を一度だけ送信します。※3
C-RP-Adv-Period	ランデブーポイント候補の通知周期	60	―	―
RP-Holdtime	ランデブーポイント保持期間	150	2.5 × C-RP-Adv-Period	左記計算式より算出。
Bootstrap-Period	BSR メッセージ送信周期	60	―	―
Bootstrap-Timeout	BSR メッセージの保持期間	130	2 × Bootstrap-Period+10	左記計算式より算出。
Negative-Cache-Holdtime(PIM-SM)	ネガティブキャッシュの保持期間	210	10 ～ 3600	PIM-SSM の場合は 3600 秒の固定。

(凡例) ―：該当しない

注※ 1

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 Join を受信した時の 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※ 2

本タイマ値は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。ただし，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※ 3

本タイマ値を 10 以上に設定すると，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。

31.4.9 IPv6 PIM-SM 使用時の注意事項

IPv6 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留意してください。

本装置は RFC2362（PIM-SM 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。

表 31-10 RFC との差分

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。
Join/Prune フラグメント	Join/Prune メッセージはネットワークの MTU を超えてもフラグメントできる。	送信する Join/Prune メッセージのサイズが大きい場合，8k バイトに分割して送信する。さらに分割して送信する 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。
PMBR との接続	RFC では PMBR(PIM Border Router) との接続および (*，*，RP) エントリに関する仕様が記述されている。	PMBR との接続はサポートしていない。また，(*，*，RP) エントリもサポートしていない。
最短経路への切り替え	最短経路への切り替えタイミングの例としてデータレートを基に切り替える方法がある。	last-hop-router 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経路へ切り替える。
C-RP-Adv 受信と Bootstrap 送信	Bootstrap メッセージは生成したメッセージ長が最大パケット長を超えた場合にフラグメントすることが許される。しかし，フラグメント発生を抑止するためにランデブーポイント候補の最大数を設定することが望ましい。	BSR はシステムで 2 台である。さらに，ランデブーポイントで設定できるグループプレフィックスは最大 128 個である。 本装置では送信する Bootstrap メッセージのサイズが大きい場合，ネットワークの MTU 長で IP フラグメントして送信される。
Hello メッセージオプション	RFC では HoldTime オプション (タイプ 1) が定義されている。	HoldTime オプションのほかに，隣接ルータアドレスリストオプション (タイプ 24 およびタイプ 65001) を使用する。(「31.4.3 近隣検出」参照)

31.4.10 IPv6 PIM-SSM

PIM-SSM は PIM-SM の拡張機能です。PIM-SM と PIM-SSM は同時動作できます。PIM-SSM が使用するマルチキャストアドレスは 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 が動作するマルチキャストアドレス（グループアドレス）のアドレス範囲を指定できます。指定したアドレス以外では PIM-SM が動作します。

PIM-SM はマルチキャストエントリ作成にマルチキャスト中継パケットが必要なのに対し，PIM-SSM はマルチキャスト経路情報（PIM-Join）の交換で IPv6 マルチキャスト中継エントリを作成し，該当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のパケットのカプセル化および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。また，本装置では MLD で PIM-SSM を動作できるようにする手段を提供します。

(1) IPv6 PIM-SSM メッセージサポート仕様

PIM-SM メッセージと同じです。

(2) IPv6 PIM-SSM を動作させる前提条件

本装置ではコンフィグレーションで次の設定が必要です。

- 各装置の設定
  PIM-SSM が動作するグループアドレスの範囲を設定します。
- MLD が動作するホストが直結している装置
  MLD 受信で PIM-SSM が動作するグループアドレス，送信元アドレスを設定します。

(3) IPv6 PIM-SSM 動作（ホストが MLDv1 または MLDv2（EXCLUDE モード）の場合）

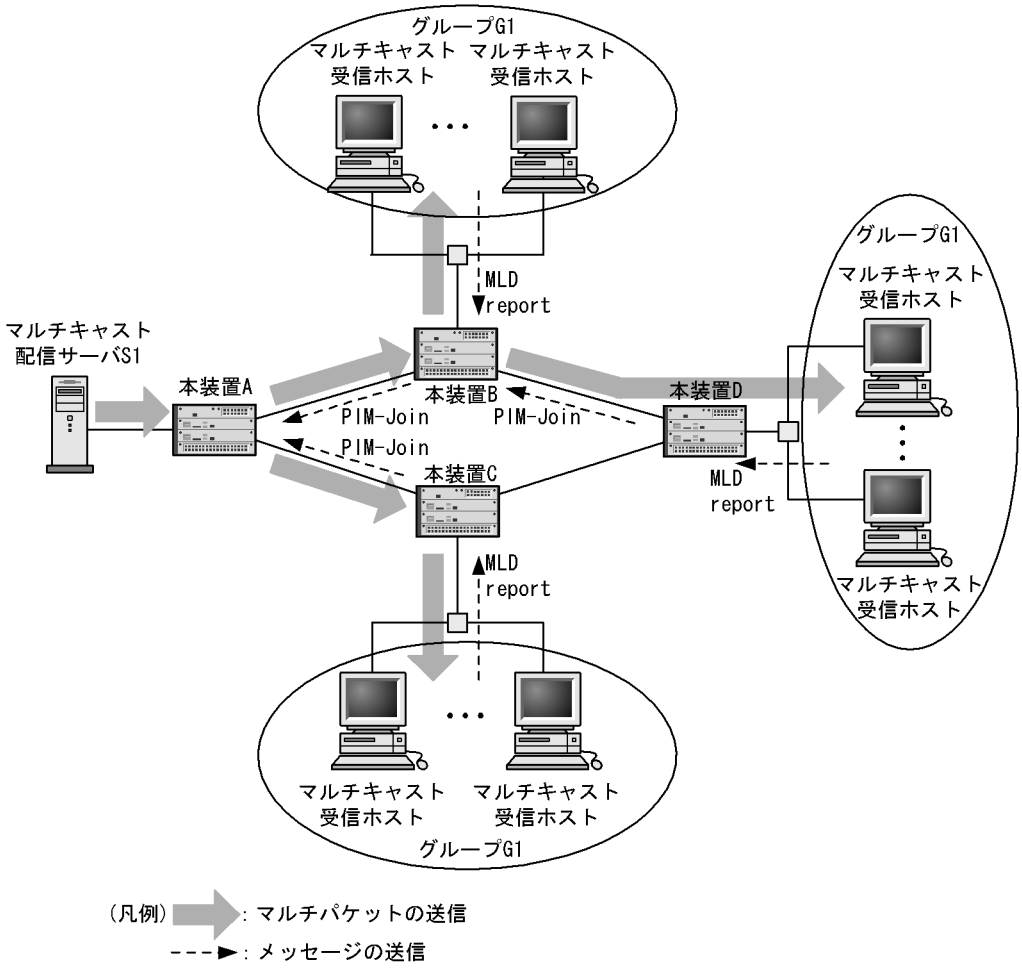
PIM-SSM を使用するためには送信元の情報が必要になります。本装置では MLDv1 を使用する際には送信元をコンフィグレーションで設定することで PIM-SSM を使用できます。

マルチキャスト配信サーバ（送信元アドレス S1）がマルチキャストグループ G1 にマルチキャストパケットを送信する場合の IPv6 PIM-SSM 動作を次に示します。

1. ホストからマルチキャストグループに参加するための MLD Report(G1) を受信します。
2. MLD Report を受信した装置は Report で通知されたグループアドレス (G1) とコンフィグレーション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，コンフィグレーションで設定した送信元アドレス (S1) への最短経路方向（ユニキャストのルーティング情報で決定）に PIM-Join を送信します。この場合，PIM-Join 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。PIM-Join を受信した各装置は送信元アドレス (S1) への最短経路方向にホップバイホップで PIM-Join を送信します。PIM-Join 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 IPv6 マルチキャスト経路情報を学習します。
3. マルチキャストパケット配信サーバ (S1) がグループ 1(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 IPv6 マルチキャスト経路情報から生成した IPv6 マルチキャスト中継エントリに従いパケットを中継します。

IPv6 PIM-SSM の動作概要を次の図に示します。

図 31-18 IPv6 PIM-SSM の動作概要（ホストが MLDv1 または MLDv2（EXCLUDE モード）の場合）



（4） IPv6 PIM-SSM 動作（ホストが MLDv2（INCLUDE モード）の場合）

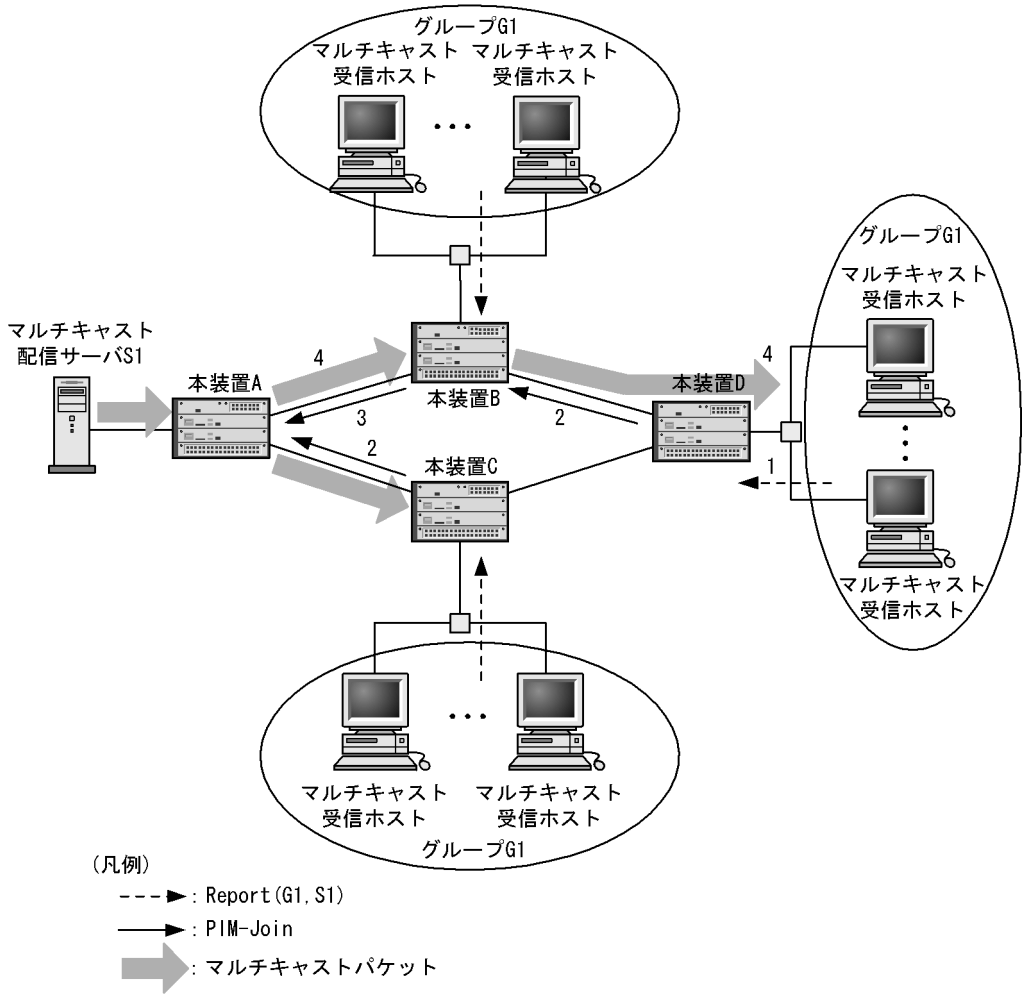
PIM-SSM を使用するためには送信元の情報が必要となります。MLDv2 では送信元を Report メッセージで指定することで PIM-SSM を使用できます。

マルチキャスト配信サーバ（送信元アドレス S1）がマルチキャストグループ G1 にマルチキャストパケットを送信する場合の IPv6 PIM-SSM 動作を次に示します。

1. ホスト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) を受信します。
2. MLDv2 Report(G1,S1) を受信した装置は Report で通知されたグループアドレス (G1) とソースアドレス (S1) を含んだ PIM-Join を送信します。
3. PIM-Join を受信した各装置は，送信元アドレス (S1) への最短経路方向にホップバイホップで PIM-Join を送信します。PIM-Join を受信した各装置は，PIM-Join を受信したインタフェースだけに送信元アドレス S1 からのマルチキャストパケットを中継するように (S1,G1) の配送ツリーを形成します。
4. マルチキャスト配信サーバ S1 がグループ G1 宛に送信したマルチキャストパケットを受信した装置はマルチキャスト中継情報に従いマルチキャストパケットを中継します。

IPv6 PIM-SSM の動作概要を次の図に示します。

図 31-19 MLDv2 使用時の IPv6 PIM-SSM 動作概要（ホストが MLDv2（INCLUDE モード）の場合）



(5) MLDv1/MLDv2 ホスト混在時の IPv6 経路制御

MLDv1 で PIM-SSM を使用する設定をしている状態で，MLDv1 と MLDv2 ホストが混在する場合の IPv6 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 対象アドレス範囲に含まれるグループアドレスに対して加入要求を受けた場合は，次の表に示すように PIM-SSM が動作します。MLDv1 Report で加入要求を受けた場合，送信元リストはコンフィグレーションで設定した送信元アドレスを使用します。MLDv1 Report と MLDv2 Report（EXCLUDE モード）で同じグループアドレスに対して加入要求を受けた場合，送信元リストはコンフィグレーションで設定された送信元アドレスと MLDv2 Report（INCLUDE モード）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。

表 31-11 MLDv1/MLDv2 ホスト混在時の IPv6 経路制御動作

加入グループアドレス	MLDv1 Report MLDv2 Report (EXCLUDE モード)	MLDv2 Report (INCLUDE モード)
SSM アドレス範囲内	PIM-SSM	PIM-SSM
SSM アドレス範囲外	PIM-SM	PIM-SM

(6) 近隣検出

PIM-SM(「31.4.3　近隣検出」) と同じです。

(7) Forwarder の決定

PIM-SM(「31.4.4　Forwarder の決定」) と同じです。

(8) DR の決定および動作

PIM-SM(「31.4.5　DR の決定および動作」) と同じです。

(9) 冗長経路時の注意事項

PIM-SM(「31.4.7　冗長経路時の注意事項」) と同じです。

31.4.11　VRF での IPv6 マルチキャスト【OP-NPAR】

(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 IPv6 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 IPv6 マルチキャストを動作させます。VRF 上の IPv6 マルチキャストでは，ランデブーポイント，BSR，各種タイマ，SSM 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 31-20　VRF での IPv6 マルチキャスト

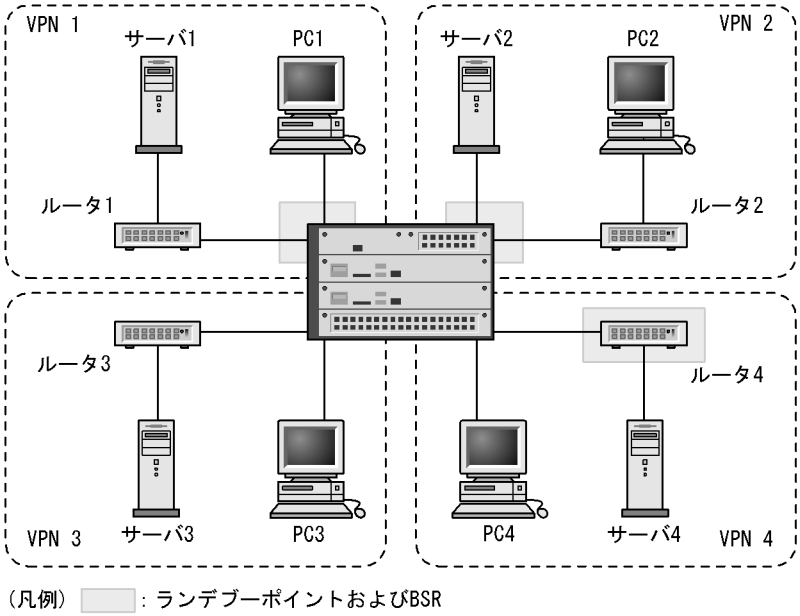


表 31-12　本装置での設定情報

VPN	運用 プロトコル	ループバック 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	SSM アドレス
1	PIM-SM	2001:db8::1	本装置（2001:db8::1）	未使用

VPN	運用プロトコル	ループバックアドレス	ランデブーポイント（）内はランデブーポイントアドレス	SSM アドレス
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

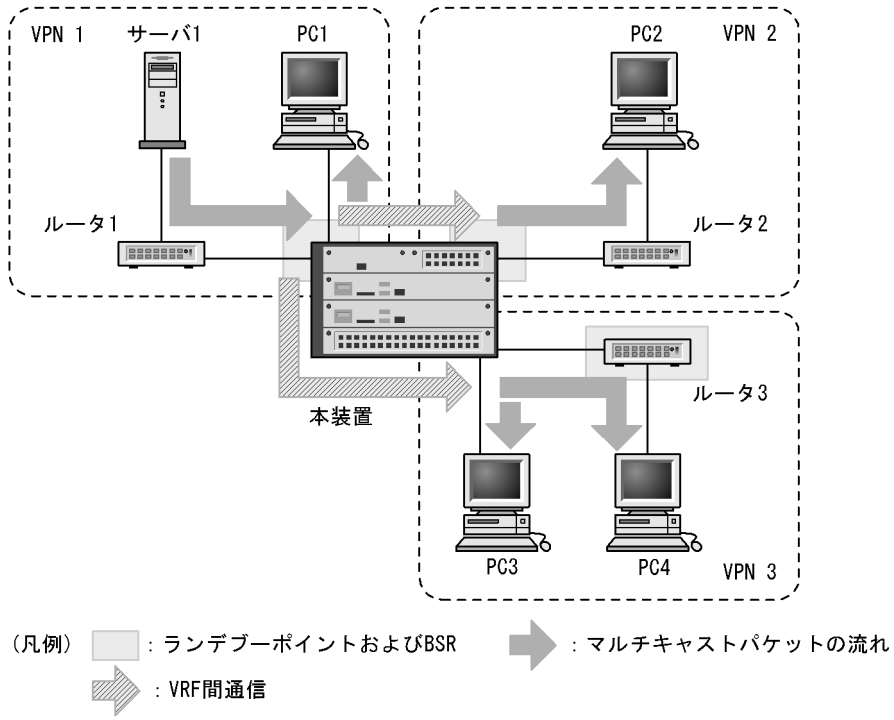
（2） IPv6 マルチキャストエクストラネット

IPv6 マルチキャストエクストラネットを使用すると，VRF 間で IPv6 マルチキャスト中継ができます。また，IPv6 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。

なお，last-hop-router 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。

IPv6 マルチキャストエクストラネットの動作概要を次の図に示します。

図 31-21 IPv6 マルチキャストエクストラネットの動作概要



（3） PIM-SM VRF ゲートウェイ

PIM-SM でマルチキャスト通信をするには，last-hop-router に IPv6 マルチキャストパケットを中継する必要があります。PIM-SM をエクストラネットで使用する場合でも，各 VRF にあるすべての last-hop-router に IPv6 マルチキャストパケットを中継する必要があります。

本装置では，各 VRF のランデブーポイントに IPv6 マルチキャストパケットを転送するために，PIM-SM VRF ゲートウェイを使用します。

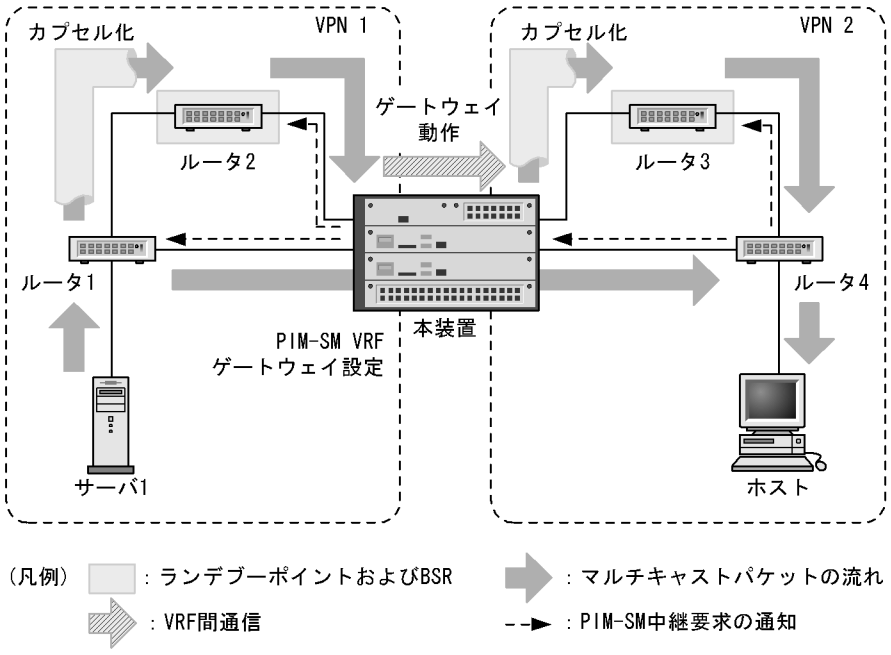
送信者（マルチキャスト配信サーバ）が存在する VRF に PIM-SM VRF ゲートウェイを設定すると，指定

グループに対して該当 VPN での last-hop-router として動作し，ランデブーポイントに中継要求をします。ランデブーポイントから IPv6 マルチキャストパケットを受信すると，そのパケットを中継対象となる VRF に転送します。

転送先の VPN では first-hop-router として動作し，各 VRF のランデブーポイントへ IPv6 マルチキャストパケットをカプセル化（Register パケット）して送信します。Register パケットを受信したランデブーポイントは通常の PIM-SM の動作に従って，デカプセル化して IPv6 マルチキャストパケットを last-hop-router に転送します。そのあと，last-hop-router から送信元への最短パス配送ツリーを形成します。このとき，エクストラネットの IPv6 マルチキャストパケットもハードウェア中継となります。

このように PIM-SM VRF ゲートウェイを使用すると，本装置以外の設定を変更しないで PIM-SM によるエクストラネットができます。PIM-SM VRF ゲートウェイの動作概要を次の図に示します。

図 31-22　PIM-SM VRF ゲートウェイの動作概要



(4) IPv6 マルチキャストエクストラネット使用時の注意事項

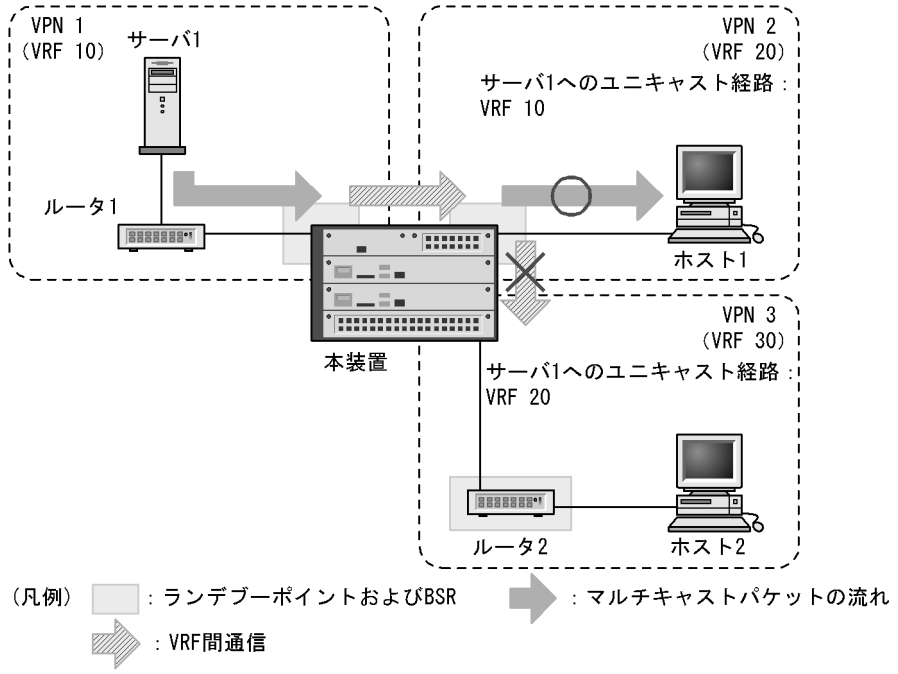
(a) 装置内での 2 段以上の VRF 中継

IPv6 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 IPv6 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 上のサーバ 1 が送信する IPv6 マルチキャストパケットを VPN 2 上のホスト 1 は受信できますが，VPN 3 のホスト 2 は受信できません。

図 31-23 IPv6 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) PIM-SM/PIM-SSM 相互接続

IPv6 マルチキャストエクストラネットを使用して VRF 間でマルチキャスト中継をする場合は，使用するグループアドレスのプロトコルを同じにしてください（IPv6 マルチキャスト VRF では，VRF ごとに PIM-SSM で使用するグループアドレスを指定できます）。

プロトコルが異なる場合，IPv6 マルチキャストエクストラネットによるマルチキャスト中継はできません。VRF 間のプロトコル不一致で中継できない例および本装置の設定情報を次に示します。

図 31-24 IPv6 マルチキャストエクストラネット使用時に VRF 間プロトコル不一致で中継できない例

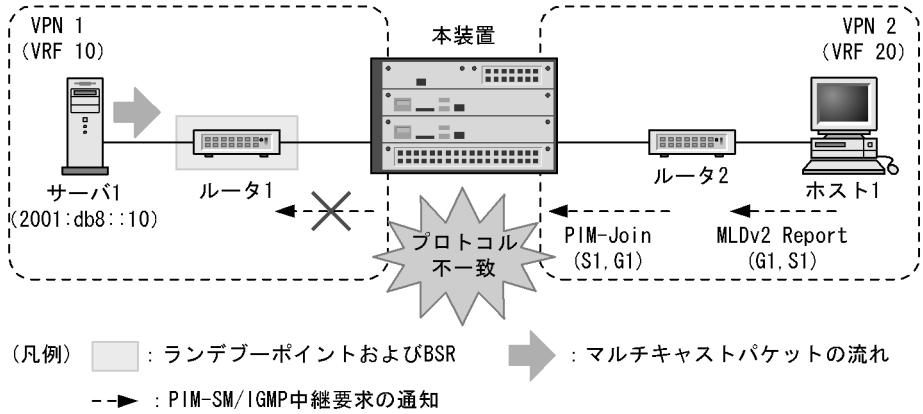


表 31-13 本装置の設定情報

VPN	運用プロトコル	ランデブーポイント () 内はランデブーポイントアドレス	SSM アドレス
1	PIM-SM	本装置（2001:db8::100）	未使用
2	PIM-SSM	なし	ff30::/12

G1：ff35::1
S1：2001:db8::10

31.5 IPv6 マルチキャストソフト処理パケット制御機能

IPv6 マルチキャストソフト処理パケット制御機能とは，本装置が受信するマルチキャストデータパケットを，コンフィグレーションで設定した受信要因と受信パケット数に従って制御することで，マルチキャストパケット受信による本装置の輻輳を抑止する機能です。本機能は，コンフィグレーションコマンド ipv6 pim rate-limit で設定します。なお，本機能は中継パケットには影響ありません。

31.5.1 パケット制御対象受信要因

パケット制御の対象受信要因とその内容を次の表に示します。

表 31-14 パケット制御対象受信要因

パケット受信要因	内容
wrong-incoming-interface	ハードウェアの IPv6 マルチキャスト中継エントリに登録済みのエントリと一致したマルチキャストデータ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 IPv6 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データパケットを受信した場合に発生する要因
register-request	first-hop-router で，受信した IPv6 マルチキャストパケットを Register パケットとしてランデブーポイントに送信する場合に発生する要因
register-receive	ランデブーポイントで，Register パケットを受信した場合に発生する要因

注

アクセスリストロギングまたは DHCP snooping を使用した場合，受信した PIM-Register パケットは，受信要因を register-receive ではなく register-request として制御されます。

31.5.2 パケット制御

(1) AX6700S の場合

NIF から受信したソフト処理用データパケットを BCU 内の CPU に転送する際，コンフィグレーションによって設定した受信要因と比較し一致した場合，設定した受信パケット数に従って転送数を制御します。

CPU に転送するパケット数は，運用系 BSU の枚数によって異なります。運用系 BSU 枚数別の，CPU に転送するパケットの最大数を次の表に示します。

表 31-15 CPU に転送するパケットの最大数

運用系 BSU 枚数	CPU に転送するパケットの最大数
1 枚	設定値の約 2 倍
2 枚	設定値の約 4 倍
3 枚	設定値の約 6 倍

(2) AX6600S の場合

NIF から受信したソフト処理用データパケットを CSU 内の CPU に転送する際，コンフィグレーションによって設定した受信要因と比較し一致した場合，設定した受信パケット数に従って転送数を制御します。

CPU に転送するパケット数は，運用系 PSP の数によって異なります。運用系 PSP 数別の，CPU に転送

するパケットの最大数を次の表に示します。

表 31-16 CPU に転送するパケットの最大数

運用系 PSP 数	CPU に転送するパケットの最大数
1	設定値
2	設定値の約 2 倍

(3) AX6300S の場合

NIF から受信したソフト処理用データパケットを MSU 内の CPU に転送する際，コンフィグレーションによって設定した受信要因と比較し一致した場合，設定した受信パケット数に従って転送数を制御します。

CPU に転送するパケットの最大数は，運用系 MSU が 1 枚だけなので，設定値と同じになります。

31.6 ネットワーク設計の考え方

31.6.1 IPv6 マルチキャスト中継

本装置で IPv6 マルチキャストパケットを中継する場合には次の点に注意してください。

(1) IPv6 PIM-SM および IPv6 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

本装置は，restart ipv6-multicast コマンド実行による IPv6 マルチキャストルーティングプログラムの再起動を行う場合は，IPv6 マルチキャスト経路情報を再学習するまで IPv6 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) ポイントーポイント型の回線

ユニキャストのスタティック経路を設定したポイントーポイント型の回線を使用して，IPv6 マルチキャスト通信を行う場合は，接続先アドレスを明示的に指定（ゲートウェイ指定）してください。

(c) タイミングによるパケット追い越し

本装置で送信者からのマルチキャストデータと受信者側からの PIM-Join メッセージを同時に受信した場合，タイミングによっては一部のパケットで追い越しが発生し，パケットの順序が入れ替わる場合があります。

(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) ソフトウェア中継処理時のパケットロス

本装置は，最初の IPv6 マルチキャストパケット受信で IPv6 マルチキャスト通信を行うための IPv6 マルチキャスト中継エントリをハードウェアへ設定します。エントリを作成するまでの間ソフトウェアで IPv6 マルチキャストパケットを中継するため，一時的にパケットをロスする場合があります。

(b) ハードウェア中継切り替え時のパケット追い越し

本装置ではハードウェアへの IPv6 マルチキャスト中継エントリの設定が完了すると，それまでのソフトウェアによる IPv6 マルチキャストパケットの中継処理がハードウェア中継へと切り替わります。この時に一部のパケットで追い越しが発生し，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

本装置は，ランデブーポイント経由での IPv6 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 IPv6 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切り替え動作は「31.4.2　IPv6 PIM-SM」を参照してください。

(d) 装置アドレスの設定必須

本装置を first-hop-router として使用する場合，ランデブーポイントへの通信には装置管理情報のローカルアドレスで設定された IPv6 アドレスが用いられます。そのため IPv6 PIM-SM では，IPv4 PIM-SM とは異なりランデブーポイントや BSR でない場合にも装置アドレスの設定が必須です。

(e) 装置アドレス到達可能性

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，装置管理情報のローカルアドレスで設定された 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となります。この装置管理情報のローカルアドレスは IPv6 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

静的ランデブーポイントは，BSR 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 BSR から 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 BSR から 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，BSR を使用しないで静的ランデブーポイントを使っ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の設定が必要です。

また，静的ランデブーポイントを使用する場合，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。

(3) IPv6 PIM-SSM

(a) 系切替時の通信無停止対応機能使用時の注意事項

- 系切替後の IPv6 マルチキャスト中継エントリの再学習時間内の注意事項を次に示します。各注意事項は再学習時間終了後に解消されます。
  - 再学習時間内にマルチキャストデータの二重中継が発生した場合，その解消に時間が掛かることがあります。
  - 再学習時間内に中継中の IPv6 マルチキャスト中継エントリのインタフェースに障害が発生し，その後回復した場合，再学習に関係なく中継を再開することがあります。
  - 再学習時間内に，中継中の IPv6 マルチキャスト中継エントリのインタフェースをコンフィグレーションまたはプロトコル処理によって削除した場合，中継が停止しないことがあります。
  - 再学習時間内に中継中の IPv6 マルチキャスト中継エントリの受信インタフェースが変更された場合，パケットロスが発生することがあります。
- 再学習時間内は PIM-SSM の動作範囲をコンフィグレーションで変更しないでください。再学習時間内に PIM-SSM の動作範囲をコンフィグレーションで変更して，マルチキャスト中継エントリが PIM-SM から PIM-SSM の経路，または PIM-SSM から PIM-SM の経路になった場合，マルチキャスト中継の動作は保証できません。
- 系切替によって隣接ルータの次に示すどちらかの情報がタイムアウトし，IPv6 マルチキャスト中継が中断する場合があります。
  - 隣接ルータ情報
  - IPv6 マルチキャスト中継エントリ下流インタフェース

  系切替時の通信無停止対応機能を使用する場合は，コンフィグレーションの ipv6 pim hello-interval，ipv6 pim join-prune-interval，ipv6 mld query-interval の値を次の表に示す推奨値か算出式で求めた値に設定してください。ipv6 pim join-prune-interval の値は，last-hop-router と last-hop-router 以外の両方の役割を持つ場合は大きい値を設定してください。

表 31-17 ipv6 pim hello-interval，ipv6 pim join-prune-interval，ipv6 mld query-interval の推奨値と算出式

設定項目	推奨値（秒）（デフォルト）	算出式（秒）
ipv6 pim hello-interval	30（30）	（2 × a）／ 1.5
ipv6 pim join-prune-interval（last-hop-router の場合）	120（60）	（2 × a + 2 × d + e）／ 2.5
ipv6 pim join-prune-interval（last-hop-router 以外の場合）	180（60）	（2 × a + b + c）／ 2.5
ipv6 mld query-interval	125（125）	―

（凡例） ―：該当しない

a：系切替時間
系切替後，運用コマンド show ipv6 pim interface または show ipv6 mld interface で全マルチキャストインタフェースが表示されるまでの時間を指定します。CPU が高負荷になる場合を考慮し，20 秒以上で計算してください。

b：隣接ルータからの PIM-Hello メッセージ最大受信周期

c：隣接ルータからの PIM-Join メッセージ最大受信周期

d：Multicast Listener Query 送信周期

e：Multicast Listener Report 最大応答待ち時間
10 秒で計算してください。本装置が Querier の場合 10 秒（固定）で動作します。

● 通信無停止対応機能を使用する場合，次の条件で使用してください。
- 隣接ルータからの PIM-Hello メッセージ受信周期：150 秒以内
- 隣接ルータからの PIM-Join メッセージ受信周期：260 秒以内
- Multicast Listener Query 送信周期：125 秒以内
- Multicast Listener Report 最大応答遅延時間：10 秒以内

31.6.2 冗長経路（障害などによる経路切り替え）

本装置で IPv6 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

IPv6 PIM-SM の場合，次に示す経路切り替えで IPv6 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接続要求を送信してから上流からマルチキャストデータが到着するまでの「加入通知時間」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 BSR 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 BSR 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 BSR 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)

- BSR 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 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切り替えを行った場合も，IPv6 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。

特にランデブーポイントおよび BSR を別装置に変更する場合は，新しいランデブーポイントおよび BSR のコンフィグレーションの priority 値を古いランデブーポイントおよび BSR の値よりも優先度が高くなるように設定してください。

(2) IPv6 PIM-SSM の使用

IPv6 PIM-SSM の場合，次に示す経路切り替えで IPv6 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接続要求を送信してから上流からマルチキャストデータが到着するまでの「加入通知時間」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 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)

31.6.3 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。

- マルチキャストパケットを送信するユーザを限定しない場合
- マルチキャストパケットを送信するユーザが多数存在する場合

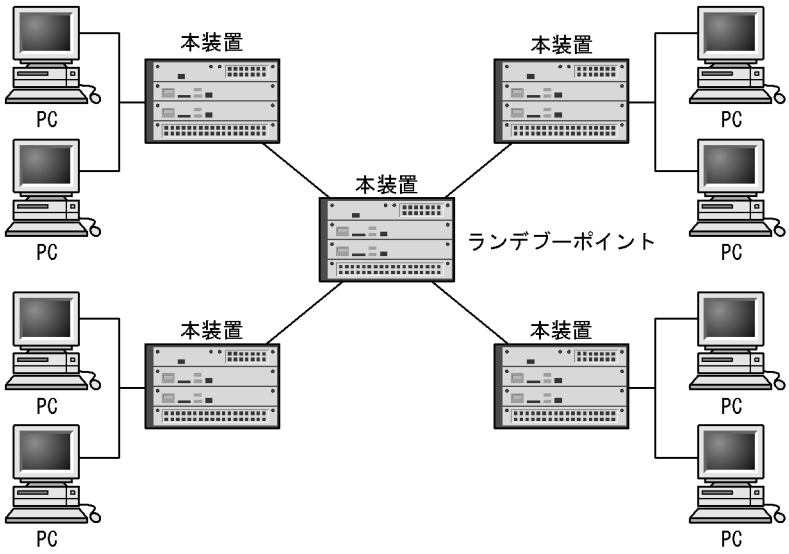
[ネットワークの環境]

1. 前提条件としてすべてのルータで IPv6 ユニキャストルーティングプロトコルの動作が必要です。
2. 本装置間の IPv6 マルチキャストルーティングプロトコルは IPv6 PIM-SM を使用します。
3. 各グループと本装置間は MLDv1 または MLDv2 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 BSR とします。

[構成図]

構成図を次に示します。

図 31-25 IPv6 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。

- マルチキャストパケットを送信するユーザを限定する場合（主に配信サーバなど）
- マルチキャストを受信するユーザが MLDv2 対応で送信するサーバ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行う場合
- 多チャンネルマルチキャスト通信を行う場合

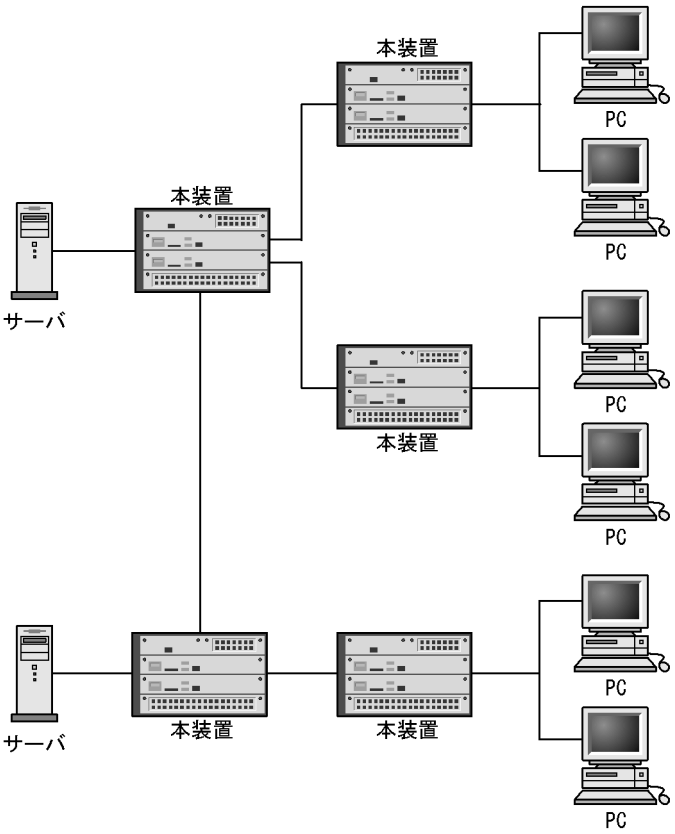
[ネットワークの環境]

1. 前提条件としてすべてのルータで IPv6 ユニキャストルーティングプロトコルの動作が必要です。
2. 本装置間の IPv6 マルチキャストルーティングプロトコルは IPv6 PIM-SSM を使用します。IPv6 PIM-SSM は PIM-SM の拡張機能です。
3. 本装置とグループ間のグループ管理制御は MLDv1 または MLDv2 を使用します（MLDv1 で SSM を連携動作させる設定が必要です）。

[構成図]

構成図を次に示します。

図 31-26 IPv6 PIM-SSM を使用する構成図



31.6.4 ネットワーク構成での注意事項

IPv6 マルチキャストはサーバ（送信者）から各グループ（受信者）にデータを配信する 1（送信者）：N（受信者）の片方向通信に適します。IPv6 マルチキャストの推奨ネットワーク構成，注意事項を次に示します。

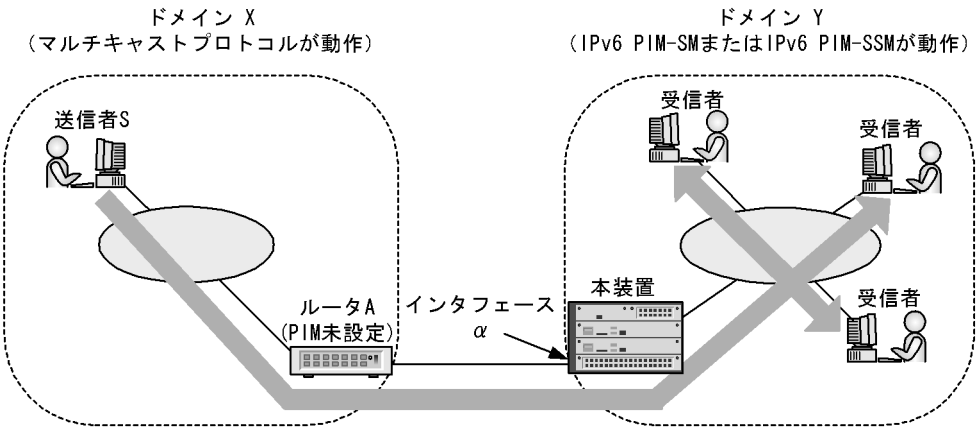
(1) IPv6 PIM-SM および IPv6 PIM-SSM 共通

(a) 適用構成

IPv6 PIM-SM または IPv6 PIM-SSM（以下，PIM と略す）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の中継が行えません。隣接ルータが PIM を設定していない場合には，コンフィグレーションコマンド ipv6 pim direct を設定するとパケットの中継ができるようになります。

「図 31-27 コンフィグレーションコマンド ipv6 pim direct を設定する場合の適応例」はコンフィグレーションコマンド ipv6 pim direct を設定する場合の適用例です。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 にいる送信元からドメイン Y にいる受信者にマルチキャストデータ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データは本装置にて廃棄されます。ここで本装置のインタフェース α にコンフィグレーションコマンド ipv6 pim direct で送信者 S を設定すると，ドメイン Y 内へのマルチキャストパケットの転送が行われるようになります。

図 31-27 コンフィグレーションコマンド ipv6 pim direct を設定する場合の適応例

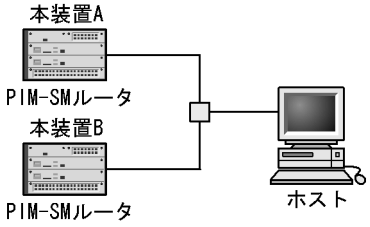


コンフィグレーションコマンド ipv6 pim direct の設定は上図のような構成に適用されますので，これ以外の構成ではマルチキャストパケットを中継できなくなるおそれがあります。

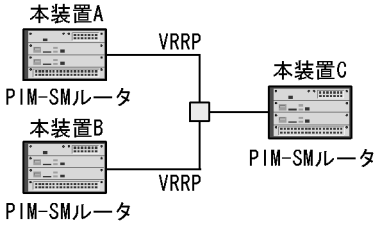
(b) 注意が必要な構成

次に示す構成で IPv6 PIM-SM または IPv6 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ホスト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には，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に PIM-SM を動作させずに MLD だけを動作させた場合は，マルチキャストデータが二重中継される場合があります。



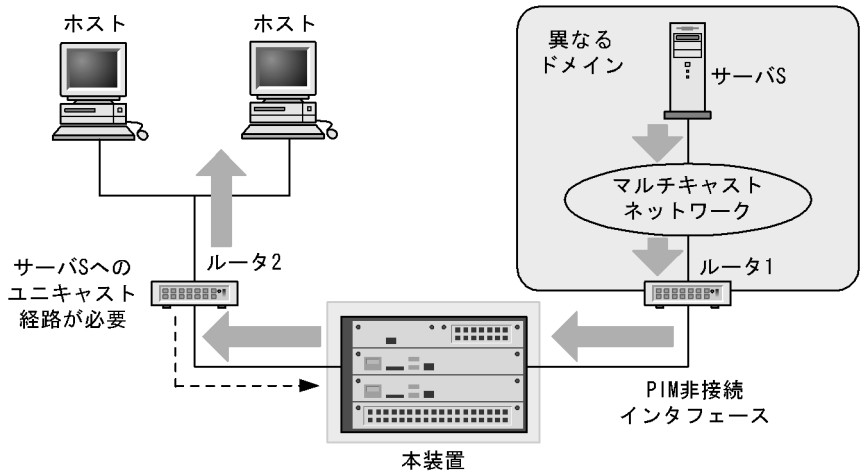
- 次の図に示す構成のように本装置 C が本装置 A と本装置 B に VRRP を設定した仮想インタフェースをゲートウェイとするスタティックルートを設定した環境では，PIM プロトコルが上流ルータを検出できず，マルチキャスト通信ができません（PIM-SSM も同じです）。
  この構成でマルチキャスト通信する場合は，本装置 C にランデブーポイントアドレスと BSR アドレスとマルチキャストデータ送信元アドレスへのゲートウェイアドレスを本装置 A または本装置 B の実アドレスとするスタティックルートを設定する必要があります。

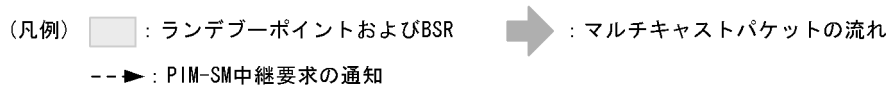


- 異なるドメイン上のルータと PIM-SM/PIM-SSM プロトコルを使用しないでマルチキャスト中継をする場合，そのルータとのインタフェースを PIM 非接続インタフェースと呼びます。

次の図に示す構成のように異なるドメイン上のサーバ 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。

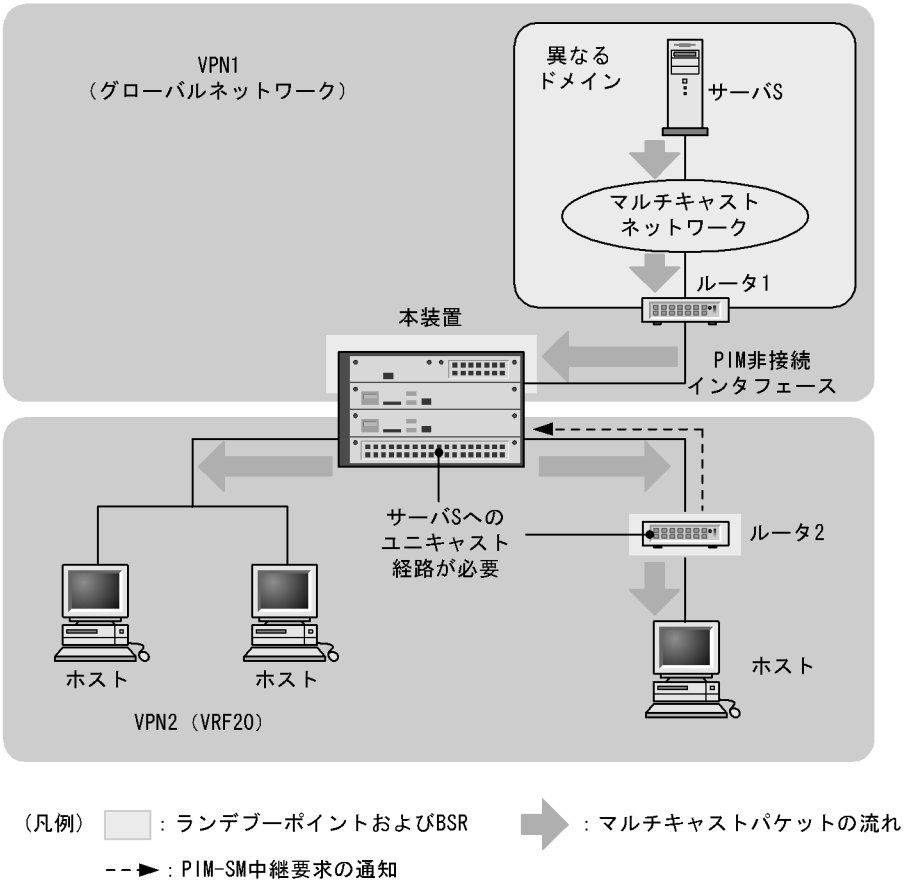
- 本装置の下流ルータ（ルータ 2）に，サーバ S へのユニキャスト経路を設定する。
- 本装置の PIM 非接続インタフェースに，コンフィグレーションコマンド ipv6 pim direct を設定する。





● 次の図に示す構成のように，上流となる VPN1（グローバルネットワーク）で異なるドメイン上のサーバ 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 VPN2（VRF20）にマルチキャスト中継する場合，次の設定が必要です。**【OP-NPAR】**

- 本装置では，上流となる VRF の PIM 非接続インタフェースにコンフィグレーションコマンド ipv6 pim direct を設定する。また，IPv6 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，サーバ 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，サーバ S へのユニキャスト経路を設定する。



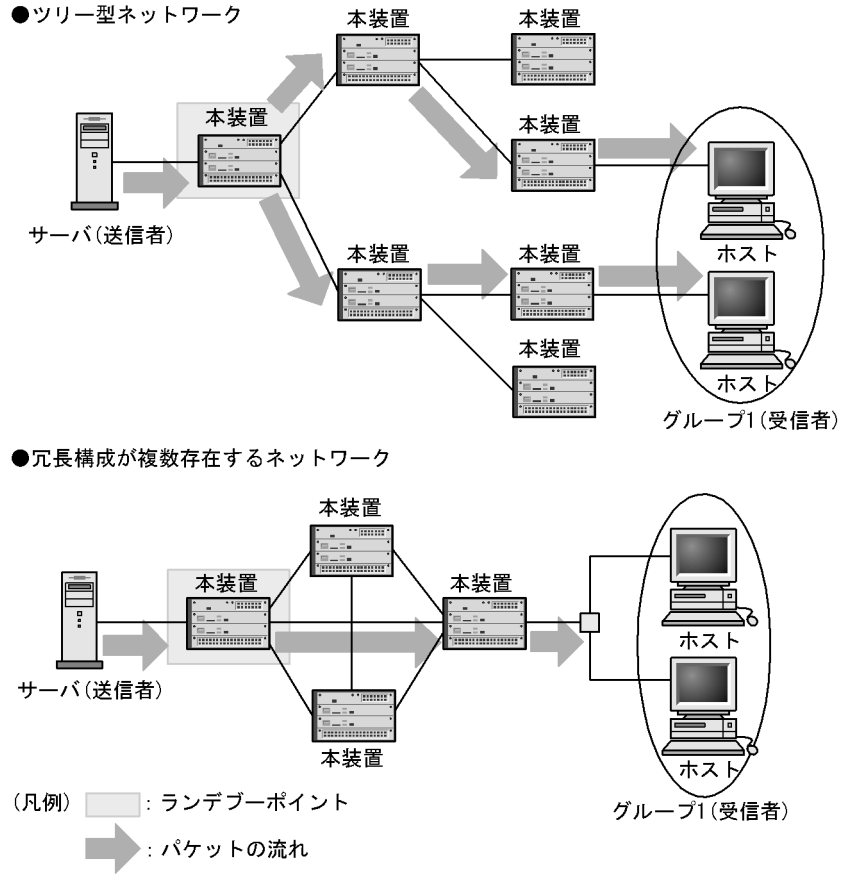
(2) IPv6 PIM-SM

(a) 推奨構成

IPv6 PIM-SM によるネットワーク構成に当たっては，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お勧めします。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。IPv6 PIM-SM のモード切り替えによる IPv6 マルチキャスト送信パス変化処理の負荷を軽減するため，ランデブーポイントは送信者の直近に置くことをお勧めします。

IPv6 PIM-SM 推奨ネットワーク構成を次の図に示します。

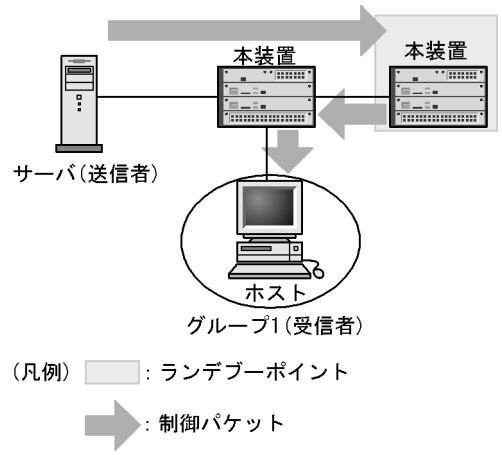
図 31-28 IPv6 PIM-SM 推奨ネットワーク構成



(b) 不適応な構成

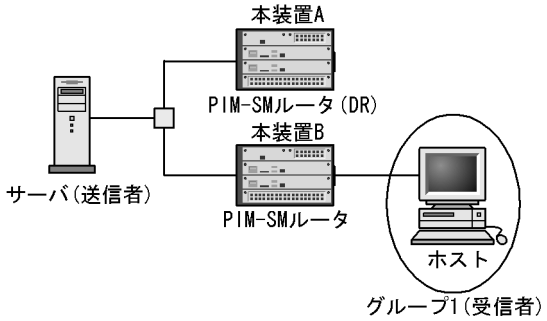
次に示す構成で IPv6 PIM-SM は使用しないでください。

● 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
次に示す構成でサーバからグループ 1 の IPv6 マルチキャスト通信を行う場合，ランデブーポイント経由の中継が効率よく行えません。

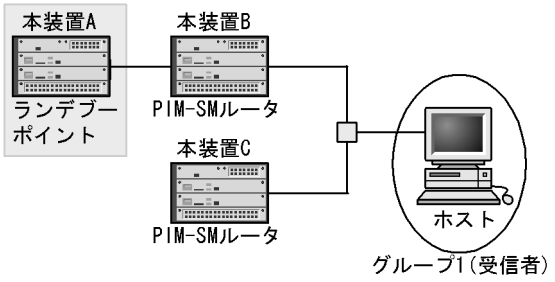


● 送信者と同一回線上に複数の IPv6 PIM-SM ルータが動作する構成
次に示す構成でサーバが IPv6 マルチキャストデータを送信した場合，DR でない IPv6 PIM-SM ルータ

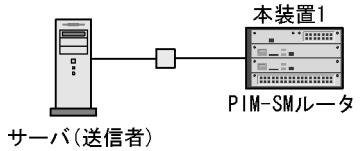
に不要な負荷がかかり，本装置の他機能に大きく影響を与えることがあります。本装置 A と B とで回線を分けてご使用ください。



● IPv6 マルチキャストグループ（受信者）と同一回線上に複数の IPv6 PIM-SM ルータを動作させ，ランデブーポイントに接続しない IPv6 PIM-SM ルータが存在する構成
次に示す構成でグループ 1 宛ての IPv6 マルチキャスト通信をした場合，送信者とグループ 1 間で最短パスが確立しない場合があります。
本装置 A および本装置 B はそれぞれ本装置 B および本装置 A を通らないでランデブーポイントと接続するようにしてください。



● 受信者不在の構成
次に示す構成でサーバが IPv6 マルチキャストデータを大量に送信した場合，本装置にはデータ廃棄処理で負荷がかかるため，本装置の他機能に大きく影響を与えることがあります。そのため，IPv6 マルチキャスト利用時は受信者を一つは設置して利用してください。

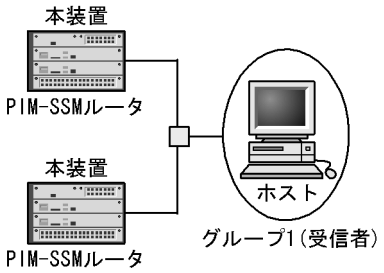


(3) IPv6 PIM-SSM

(a) 注意が必要な構成

次に示す構成で IPv6 PIM-SSM を使用する場合注意が必要です。

● IPv6 マルチキャストグループ（受信者）と同一回線上に複数の IPv6 PIM-SSM ルータが動作する構成
次に示す構成で MLDv1 で PIM-SSM を動作させる場合は，同一回線上のすべてのルータを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 で設定してください。



(b) 端末側に複数のアドレスを設定したときの注意事項

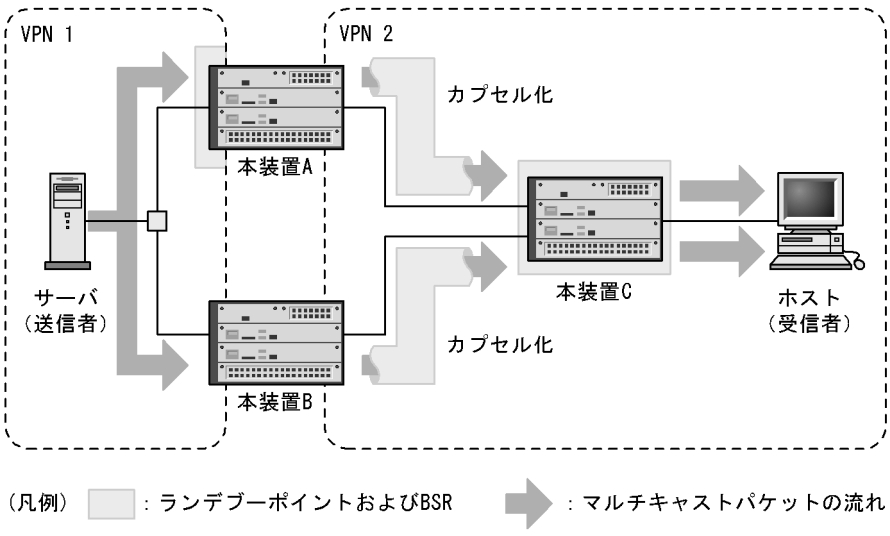
SSM 通信時，データ送信を行う端末に複数の IPv6 アドレスを付与して運用する場合，送信されるデータの送信元アドレスが本装置にコンフィグレーションコマンド ipv6 mld ssm-map static で設定した送信元アドレス情報と一致するようにしてください。特に，RA などのアドレス自動設定機能を使用した場合は，端末側が自動設定されたアドレスを使用して通信を行う場合があります。

(4) PIM-SM VRF ゲートウェイ【OP-NPAR】

(a) 注意が必要な構成

次に示す構成は注意が必要です。

- PIM-SM VRF ゲートウェイを使用した IPv6 マルチキャストエクストラネットで，2 台以上の VRF 境界ルータで冗長構成を構築する場合，VRF 境界ルータのどれかをランデブーポイントに設定してください。
  VRF 境界ルータ以外をランデブーポイントにした場合，最短パス配送ツリーが形成されるまでの間，IPv6 マルチキャストパケットが境界ルータの数だけ多重中継になります。
  PIM-SM VRF ゲートウェイによって，カプセル化されたパケットが二重中継となる動作を次の図に示します。



32 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。

32.1 コンフィグレーション

32.1.1 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 32-1 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	同一リンク上に MLD リスナが 1 台だけの場合に限り，グループの離脱を即時に行う機能を設定します。
ipv6 mld group-limit	インタフェースで動作できる最大グループ数を指定します。
ipv6 mld query-interval	query メッセージの送信間隔を変更します。
ipv6 mld router	MLD を使えるように設定します。
ipv6 mld source-limit	グループ参加時のソース最大数を指定します。
ipv6 mld ssm-map enable	MLDv1/MLDv2（EXCLUDE モード）での IPv6 PIM-SSM 連携動作を使えるように設定します。
ipv6 mld ssm-map static	PIM-SSM が動作するグループアドレスとソースアドレスを設定します。
ipv6 mld static-group	MLD グループへ静的に加入できるように設定します。
ipv6 mld version	MLD バージョンを変更します。
ipv6 multicast-routing	IPv6 マルチキャスト機能を使えるように設定します。
ipv6 pim	IPv6 PIM-SM を設定します。
ipv6 pim assert-metric	assert メッセージで使用する metric 値を変更します。
ipv6 pim assert-preference	assert メッセージで使用する preference 値を変更します。
ipv6 pim bsr candidate bsr	BSR を設定します。
ipv6 pim bsr candidate rp	ランデブーポイントを設定します。
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変更します。
ipv6 pim direct	遠隔のマルチキャストサーバアドレスを直接接続サーバとして扱う機能を設定します。
ipv6 pim hello-interval	PIM-Hello メッセージの送信間隔を変更します。
ipv6 pim join-prune-interval	PIM-Join/Prune メッセージの送信間隔を変更します。
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変更します。
ipv6 pim max-interface	IPv6 PIM を動作させるインタフェースの最大数を変更します。
ipv6 pim mcache-limit	マルチキャスト中継エントリの最大数を指定します。
ipv6 pim mroute-limit	マルチキャストルーティングエントリの最大数を指定します。
ipv6 pim negative-cache-time	ネガティブキャッシュの保持期間を変更します。
ipv6 pim nonstop-forwarding	系切替時に，IPv6 PIM-SSM のマルチキャスト中継を一時的に停止しないように指定します。
ipv6 pim rate-limit cache-misshit	マルチキャスト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要因による受信パケット数の上限を指定します。
ipv6 pim rate-limit register-receive	ランデブーポイントで，受信できる PIM-Register メッセージ数の上限を指定します。

コマンド名	説明
ipv6 pim rate-limit register-request	first-hop-router で，受信したマルチキャストパケットを PIM-Register メッセージとしてランデブーポイントに送信する場合のパケット数の上限を指定します。
ipv6 pim rate-limit wrong-incoming-interface	マルチキャストエントリの入力インタフェース以外から受信できるマルチキャストパケット数の上限を指定します。
ipv6 pim register-probe-time	PIM-Register メッセージ送信抑止時間を基に null-Register の送信開始時間を指定します。
ipv6 pim rp-address	静的ランデブーポイントを設定します。
ipv6 pim rp-mapping-algorithm	ランデブーポイント選出アルゴリズムを指定します。
ipv6 pim ssm	IPv6 PIM-SSM アドレスを設定します。
ipv6 pim vrf-gateway	PIM-SM VRF ゲートウェイを設定します。

32.1.2 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の設定
- IPv6 PIM-SM 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 BSR 候補の設定（自装置を BSR にする場合）
- MLD の設定

● PIM-SM（静的ランデブーポイント）を使用する場合

- IPv6 マルチキャストルーティングの設定
- IPv6 PIM-SM 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 静的ランデブーポイントの設定
- 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の設定
- IPv6 PIM-SM 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の設定
- VRF での IPv6 PIM-SM 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 BSR 候補の設定（該当 VPN で自装置を BSR 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）を使用する場合

- VRF での IPv6 マルチキャストルーティングの設定
- VRF での IPv6 PIM-SM 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 静的ランデブーポイントの設定
- 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の設定
- VRF での IPv6 PIM-SM 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-SM を使用する場合（PIM-SM VRF ゲートウェイ）
- VRF での IPv6 マルチキャストルーティングの設定
- VRF での IPv6 PIM-SM の設定
- VRF での 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）
- VRF での IPv6 PIM-SM BSR 候補の設定（自装置を BSR にする場合）
- PIM-SM VRF ゲートウェイの設定

● 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の設定
- VRF での IPv6 PIM-SM 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

32.1.3 IPv6 マルチキャストルーティングの設定

[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を動作させるには，本装置のループバックアドレスとして loopback 0 のインタフェースへのアドレス設定，およびグローバルコンフィグレーションモードで次の設定が必要です。例として，本装置のループバックアドレスを 2001:db8::b とした設定を示します。

なお，ここでの設定のほかに，一つ以上のインタフェースで IPv6 PIM（ipv6 pim コマンド）の設定が必要です。

[コマンドによる設定]

1.
```
(config)# interface loopback 0
(config-if)# ipv6 address 2001:db8::b
(config-if)# exit
```
ループバックのアドレスを設定します。

2.
```
(config)# ipv6 multicast-routing
```
IPv6 マルチキャスト機能を使用できるようにします。

32.1.4 IPv6 PIM-SM の設定

[設定のポイント]

IPv6 マルチキャストルーティングを動作させるインタフェースには，IPv6 PIM-SM（sparse モード）の設定をする必要があります。IPv6 PIM-SM（sparse モード）の設定はインタフェースコンフィグレーションモードで行います。例として，インタフェースの IPv6 アドレスを 2001:db8::a/16 とした

設定を示します。

[コマンドによる設定]

1. **(config)# interface vlan 10**
   (config-if)# ipv6 address 2001:db8::a/16
   (config-if)# ipv6 enable
   IPv6 アドレスを設定します。

2. **(config-if)# ipv6 pim**
   IPv6 PIM-SM（sparse モード）として動作することを指定します。

32.1.5 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，グローバルコンフィグレーションモードで次の設定をします。ランデブーポイントアドレスは loopback 0 のインタフェースへ設定したアドレスを使用してください。例として，本装置のループバックアドレスを 2001:db8::b とし，管理するマルチキャストグループアドレスを ff15::/16 とした設定を示します。

[コマンドによる設定]

1. **(config)# ipv6 access-list GROUP1**
   (config-ipv6-acl)# permit ipv6 any ff15::/16
   (config-ipv6-acl)# exit
   管理するマルチキャストグループアドレスのアクセスリストを作成します。

2. **(config)# ipv6 pim bsr candidate rp 2001:db8::b 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（管理するマルチキャストグループアドレスは手順 1 で作成したアクセスリストを指定します）。

32.1.6 IPv6 PIM-SM BSR 候補の設定

[設定のポイント]

本装置を BSR 候補として使用する場合，グローバルコンフィグレーションモードで次の設定をします。BSR アドレスは loopback 0 のインタフェースへ設定したアドレスを使用してください。例として，本装置のループバックアドレスを 2001:db8::b とした設定を示します。

[コマンドによる設定]

1. **(config)# ipv6 pim bsr candidate bsr 2001:db8::b**
   本装置を BSR 候補として設定します。

32.1.7 IPv6 PIM-SM 静的ランデブーポイントの設定

[設定のポイント]

静的ランデブーポイントを指定する場合，グローバルコンフィグレーションモードで次の設定をしま

す。例として，静的ランデブーポイントの装置のアドレスを 2001:db8::b とした設定を示します。

［コマンドによる設定］

1. **(config)# ipv6 pim rp-address 2001:db8::b**
   2001:db8::b をランデブーポイントとして指定します。

32.1.8 IPv6 PIM-SSM の設定

（1） IPv6 PIM-SSM アドレスの設定

［設定のポイント］

本装置で IPv6 PIM-SSM を使用するにはグローバルコンフィグレーションモードで次の設定をします。本設定によって IPv6 PIM-SM が設定されたインタフェースでは，指定した SSM アドレス範囲で IPv6 PIM-SSM が動作します。本装置で使用できる SSM アドレス設定は一つだけです。例として，PIM-SSM が動作する SSM アドレス範囲を ff35::/16 とした設定を示します。

［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
   SSM アドレス範囲のアクセスリストを作成します。

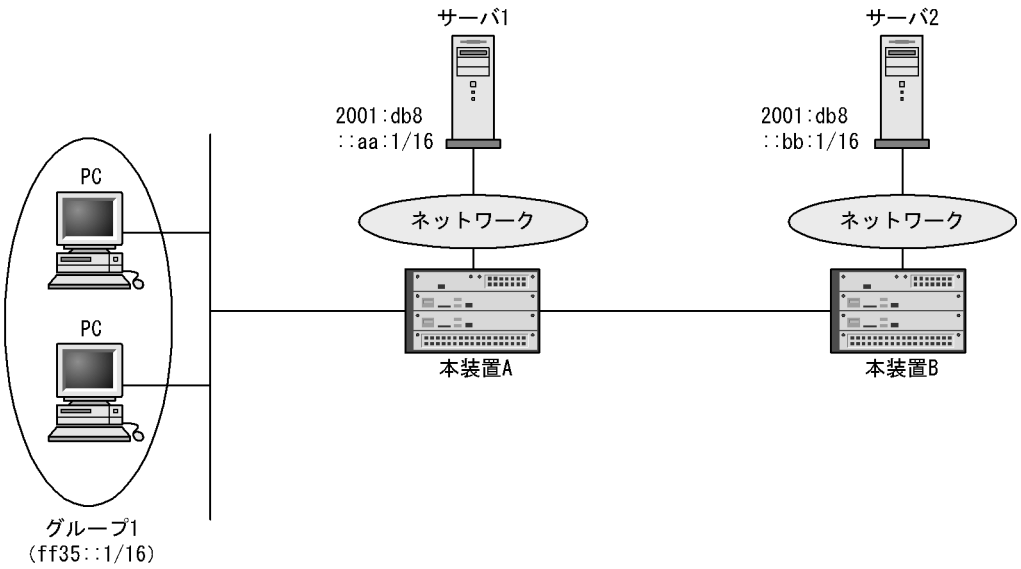
2. **(config)# ipv6 pim ssm range GROUP2**
   IPv6 PIM-SSM を使用できるようにします（SSM アドレス範囲は手順 1 で作成したアクセスリストを指定します）。

（2） MLDv1/MLDv2（EXCLUDE モード）で IPv6 PIM-SSM を連携動作させる設定

［設定のポイント］

MLDv1/MLDv2（EXCLUDE モード）ではソースアドレスが特定できないため PIM-SSM への連携ができません。本装置では，PIM-SSM が動作するグループアドレスとソースアドレスの設定をすることで PIM-SSM への連携を行います。例として，グループアドレスを ff35::1 とし，二つのサーバを使用する場合，サーバ 1 のソースアドレスを 2001:db8::aa:1，サーバ 2 のソースアドレスを 2001:db8::bb:1 とした PIM-SSM 構成例を次の図に示します。

図 32-1 IPv6 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 host ff35::1
   (config-ipv6-acl)# exit
   グループアドレスを指定したアクセスリストを作成します。

2. **(config)# ipv6 mld ssm-map static GROUP3 2001:db8::aa:1**
   (config)# ipv6 mld ssm-map static GROUP3 2001:db8::bb:1
   PIM-SSM が動作するグループアドレス，およびサーバ 1 とサーバ 2 のソースアドレスを設定します（グループアドレスは手順 1. で作成したアクセスリストを指定します）。

3. **(config)# ipv6 mld ssm-map enable**
   IPv6 PIM-SSM を使用できるようにします。

32.1.9 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。

[コマンドによる設定]

1. **(config-if)# ipv6 mld router**
   当該インタフェースで MLD version 1，2 混在モード（デフォルト）を動作させることを指定します。

32.1.10 VRF での IPv6 マルチキャストルーティングの設定【OP-NPAR】

[設定のポイント]

VRF で IPv6 マルチキャストルーティングを動作させるには，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，およびグローバルコンフィグレーションモードでの次の設定が必要です。例として，VRF 10 のループバックアドレスを 2001:db8::10 とした IPv6 マルチキャストルーティングの設定を示します。
なお，ここでの設定のほかに，VRF ごとに一つ以上のインタフェースで IPv6 PIM（ipv6 pim コマンド）の設定が必要です。

［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::10
   (config-if)# exit
   VRF 10 のループバックインタフェース loopback 30 にループバックのアドレスを設定します。

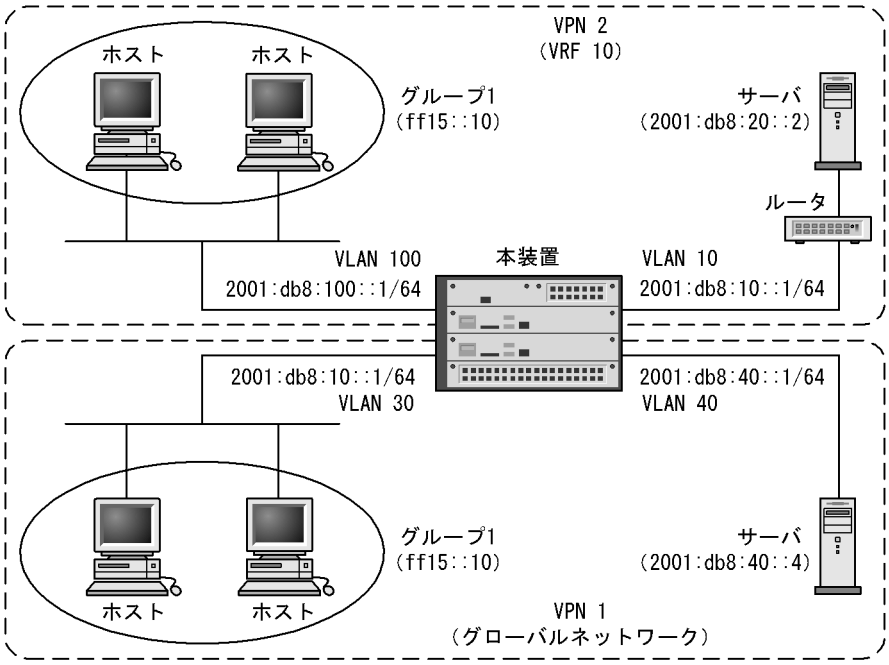
3. **(config)# ipv6 multicast-routing vrf 10**
   VRF 10 で IPv6 マルチキャスト機能を使用できるようにします。

32.1.11 VRF での IPv6 PIM-SM の設定【OP-NPAR】

［設定のポイント］

VRF で IPv6 PIM-SM を使用するために，VRF に IPv6 マルチキャストルーティング機能を設定し，その VRF の一つ以上のインタフェースに IPv6 PIM-SM（sparse モード）を設定します。IPv6 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。
IPv6 PIM-SM（sparse モード）の設定はインタフェースコンフィグレーションモードで行います。
例として，VPN 2 に VRF 10 を対応させ，VRF 10 のインタフェース VLAN 10 の IPv6 アドレスを 2001:db8:10::1/64 とした IPv6 PIM-SM 構成例を次の図に示します。

図 32-2 VRF での IPv6 PIM-SM 構成例



[コマンドによる設定]

1. **(config)# interface vlan 10**
   VLAN 10 を設定します。

2. **(config-if)# vrf forwarding 10**
   VLAN 10 を VRF 10 に設定します。

3. **(config-if)# ipv6 address 2001:db8:10::1/64**
   (config-if)# ipv6 enable
   VLAN 10 に IPv6 アドレスを設定します。

4. **(config-if)# ipv6 pim**
   (config-if)# exit
   VLAN 10 に IPv6 PIM-SM を設定します。

32.1.12 VRF での IPv6 PIM-SM ランデブーポイント候補の設定【OP-NPAR】

[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，グローバルコンフィグレーションモードで次の設定をします。例として，VRF 10 のループバックアドレスを 2001:db8::10，管理するマルチキャストグループアドレスを ff15::/16 とした設定を示します。

[コマンドによる設定]

1. **(config)# ipv6 access-list GROUP1**

```
(config-ipv6-acl)# permit ipv6 any ff15::/16
(config-ipv6-acl)# exit
```
VRF 10 で管理するマルチキャストグループアドレスのアクセスリストを作成します。

2. **(config)# ipv6 pim vrf 10 bsr candidate rp 2001:db8::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（管理するマルチキャストグループアドレスは手順 1 で作成したアクセスリストを指定します）。

32.1.13 VRF での IPv6 PIM-SM BSR 候補の設定【OP-NPAR】

[設定のポイント]

VRF で本装置を BSR 候補として使用する場合，グローバルコンフィグレーションモードで次の設定をします。例として，本装置のループバックアドレスを 2001:db8::10 とした設定を示します。

[コマンドによる設定]

1. **(config)# ipv6 pim vrf 10 bsr candidate bsr 2001:db8::10**
本装置を VRF 10 の BSR 候補として設定します。

32.1.14 VRF での IPv6 PIM-SM 静的ランデブーポイントの設定【OP-NPAR】

[設定のポイント]

VRF で静的ランデブーポイントを設定する場合，グローバルコンフィグレーションモードで次の設定をします。例として，VRF 10 の静的ランデブーポイントの IPv6 アドレスを 2001:db8::10 とした設定を示します。

[コマンドによる設定]

1. **(config)# ipv6 pim vrf 10 rp-address 2001:db8::10**
VRF 10 で 2001:db8::10 をランデブーポイントとして指定します。

32.1.15 VRF での IPv6 PIM-SSM の設定【OP-NPAR】

(1) IPv6 PIM-SSM アドレスの設定

[設定のポイント]

VRF で，本装置で IPv6 PIM-SSM を使用するには，グローバルコンフィグレーションモードで次の設定をします。本設定によって IPv6 PIM-SM が設定された VRF のインタフェースでは，指定した SSM アドレス範囲で IPv6 PIM-SSM が動作します。本装置で使用できる SSM アドレス設定は VRF ごとに一つだけです。例として，VRF 10 で IPv6 PIM-SSM が動作する SSM アドレス範囲をデフォルト（ff30::/12）で使用する設定を示します。

[コマンドによる設定]

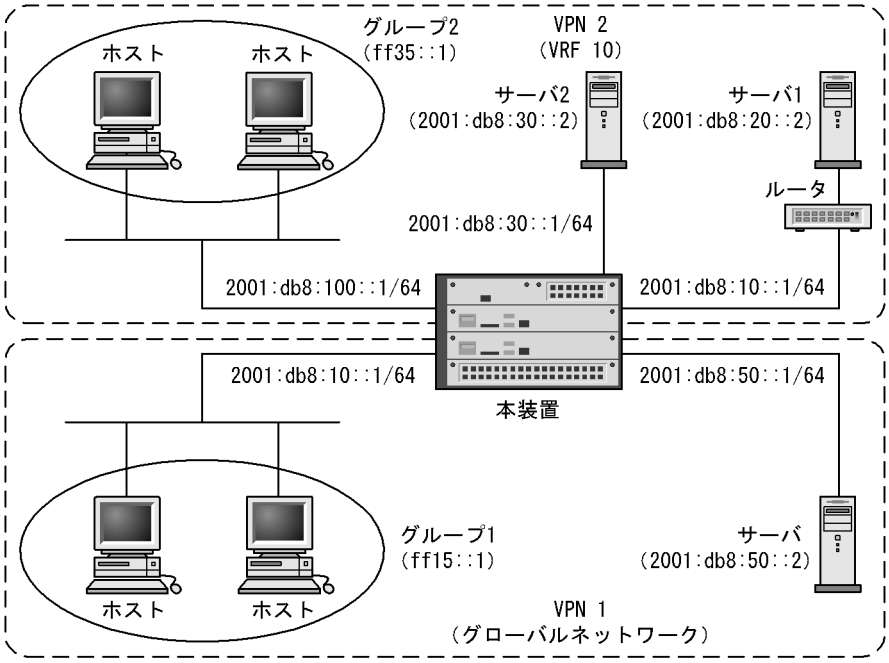
1. **(config)# ipv6 pim vrf 10 ssm default**
VRF 10 で IPv6 PIM-SSM を使用できるようにします（SSM アドレス範囲は ff30::/12 となります）。

(2) MLDv1/MLDv2（EXCLUDE モード）で IPv6 PIM-SSM を連携動作させる設定

[設定のポイント]

MLDv1/MLDv2（EXCLUDE モード）ではソースアドレスを特定できないため，IPv6 PIM-SSM への連携ができません。本装置では，IPv6 PIM-SSM が動作するグループアドレスとソースアドレスを設定することで IPv6 PIM-SSM への連携を行います。本機能は VRF ごとに設定します。IPv6 PIM-SSM が動作するグループアドレスは，IPv6 PIM-SSM アドレスの設定で該当 VRF に指定した SSM アドレス範囲内である必要があります。例として，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を ff35::1，同一 VPN 内で二つのサーバを使用する場合，サーバ 1 のソースアドレスを 2001:db8:20::2，サーバ 2 のソースアドレスを 2001:db8:30::2 とした IPv6 PIM-SSM 構成例を次の図に示します。

図 32-3 VRF での IPv6 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 host ff35::1
   (config-ipv6-acl)# exit
   VRF 10 で管理するマルチキャストグループアドレスのアクセスリストを作成します。

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 IPv6 PIM-SSM が動作するグループアドレス，およびサーバ 1 とサーバ 2 のソースアドレスを VRF 10 に設定します（グループアドレスは手順 1 で作成したアクセスリストを指定します）。

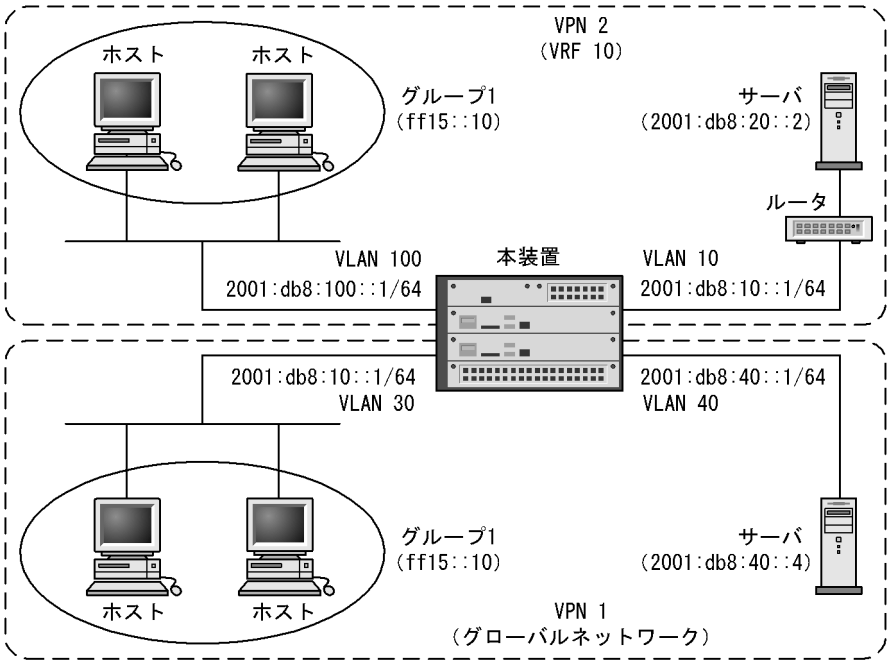
3. **(config)# ipv6 mld vrf 10 ssm-map enable**
   VRF 10 で MLDv1/MLDv2（EXCLUDE モード）で IPv6 PIM-SSM を使用できるようにします。

32.1.16 VRF での MLD の設定【OP-NPAR】

[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。
デフォルトでは MLD バージョン 1，2 混在モードです。MLD バージョンを変更する場合は，コンフィグレーションコマンド ipv6 mld version で設定してください。例として，VPN 2 に VRF 10 を対応させ，VRF 10 のインタフェース VLAN 100 の IPv6 アドレスを 2001:db8:100::1/64 とした MLD 構成例を次の図に示します。

図 32-4 VRF での MLD 構成例



[コマンドによる設定]

1. **(config)# interface vlan 100**
   VLAN 100 を設定します。

2. **(config-if)# vrf forwarding 10**
   VLAN 100 を VRF 10 に設定します。

3. **(config-if)# ipv6 address 2001:db8:100::1/64**
   (config-if)# ipv6 enable
   VLAN 100 に IPv6 アドレスを設定します。

4. **(config-if)# ipv6 mld router**
   (config-if)# exit
   VLAN 100 に MLD を設定します。

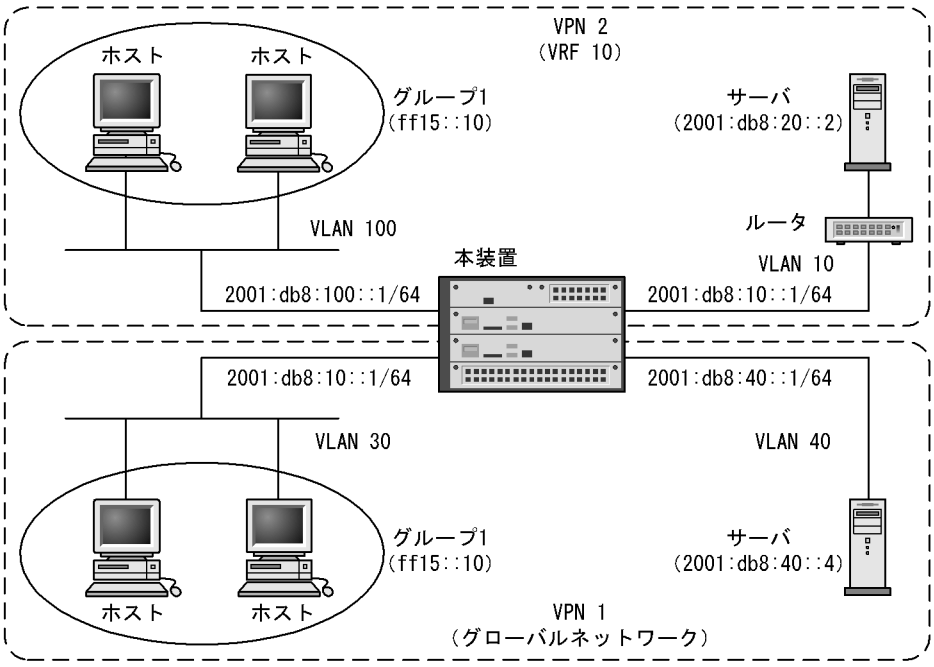
32.1.17 IPv6 マルチキャストエクストラネットの設定【OP-NPAR】

[設定のポイント]

IPv6 マルチキャストエクストラネットでは，中継先 VRF に送信元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，すべてのマルチキャスト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の設定はグローバルコンフィグレーションモードで行います。例として，VPN 2 に VRF 10 を対応させ，VRF 10 のインタフェースの IP アドレスを 2001:db8:100::1/64，2001:db8:10::1/64 とした 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）上のサーバ（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 32-5 VRF での PIM-SSM 構成例（IPv6 マルチキャストエクストラネット）



[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。

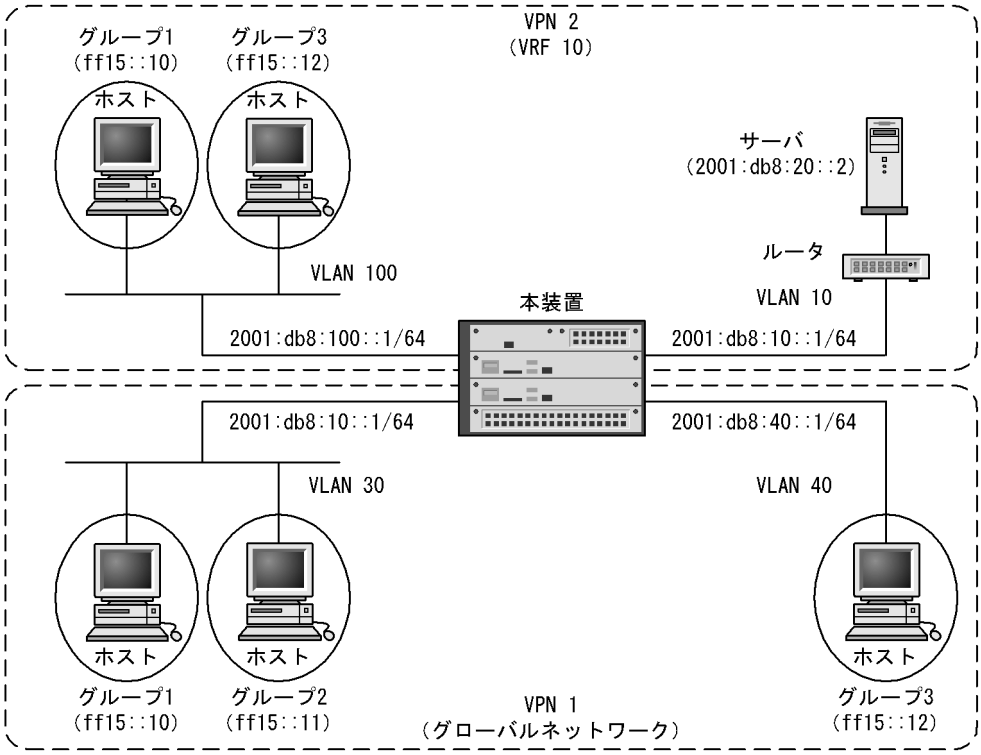
2. **(config)# vrf definition 10**
   (config-vrf)# ipv6 import multicast inter-vrf MLT6EXNET
   (config-vrf)# exit
   VRF 10 にすべての VRF からの IPv6 マルチキャスト中継要求を許可する設定を適用します。

32.1.18 PIM-SM VRF ゲートウェイの設定【OP-NPAR】

[設定のポイント]

IPv6 マルチキャストエクストラネットでは，中継先 VRF に送信元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。
PIM-SM でマルチキャストエクストラネットによるマルチキャスト VRF 間通信をする場合，PIM-SM VRF ゲートウェイの設定が必要です。PIM-SM VRF ゲートウェイは，マルチキャスト送信者が存在する VRF に設定します。設定はグローバルコンフィグレーションモードで行います。エクストラネットで使用するグループアドレスを，ホストアドレス指定ですべてマルチキャスト経路フィルタリングに指定して，PIM-SM VRF ゲートウェイを設定します。このとき，プレフィックスによる範囲指定をしたグループアドレスは，PIM-SM VRF ゲートウェイの制御対象外となります。例として，ff15::10，ff15::11 および ff15::12 のグループアドレスを，VRF 10 からグローバルネットワークに中継する設定を示します。この場合，VPN 1（グローバルネットワーク）に，VPN 2（VRF 10）上のサーバ（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 32-6　VRF での PIM-SM 構成例（PIM-SM VRF ゲートウェイ）



［コマンドによる設定］

1. **(config)# ipv6 access-list MLT6GROUP**
   (config-ipv6-acl)# permit ipv6 host ff15::10 any
   (config-ipv6-acl)# permit ipv6 host ff15::11 any
   (config-ipv6-acl)# permit ipv6 host ff15::12 any
   (config-ipv6-acl)# exit
   (config)# route-map MLT6EXNET permit 10
   (config-route-map)# match ipv6 address MLT6GROUP
   (config-route-map)# exit
   PIM-SM VRF ゲートウェイで使用するグループアドレスとして ff15::10，ff15::11 および ff15::12 を指定します。

2. **(config)# vrf definition 10**

```
(config-vrf)# ipv6 import multicast inter-vrf MLT6EXNET
(config-vrf)# exit
```

VRF 10 から他 VRF に対して中継するグループを指定します。

3. **(config)# ipv6 pim vrf 10 vrf-gateway**
   VRF 10 に PIM-SM VRF ゲートウェイを設定します。

32.2 オペレーション

32.2.1 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 32-2 運用コマンド一覧

コマンド名	説明
show ipv6 mcache	すべてのマルチキャスト経路を一覧で表示します。
show ipv6 mroute	PIM-SM マルチキャストルート情報を表示します。
show ipv6 pim interface	IPv6 PIM-SM/SSM インタフェースの状態を表示します。
show ipv6 pim neighbor	IPv6 PIM-SM/SSM インタフェースの隣接情報を表示します。
show ipv6 pim mcache	IPv6 PIM-SM/SSM のマルチキャスト中継エントリを表示します。
show ipv6 pim bsr	IPv6 PIM-SM BSR 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	IPv6 PIM-SM 各グループ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 インタフェースの状態を表示します。
show ipv6 mld group	MLD 情報を表示します。
show ipv6 rpf	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で使用している各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。
debug protocols ipv6-multicast	IPv6 マルチキャストルーティングプログラムが出力するイベント情報の syslog を出力します。
no debug protocols ipv6-multicast	IPv6 マルチキャストルーティングプログラムが出力するイベント情報の syslog の出力を停止します。
dump protocols ipv6-multicast	IPv6 マルチキャストルーティングプログラムで採取している制御テーブル情報・イベントトレース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プログラムが作成したイベントトレース情報ファイル，制御テーブル情報ファイル，コアファイルのダンプを削除します。

32.2.2 IPv6 マルチキャストグループアドレスへの経路確認

本装置で IPv6 マルチキャストルーティング情報の設定を行った場合は，show ipv6 mcache コマンドと show netstat multicast 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。存在しない場合，および outgoing が正しくない場合は，「32.2.3　IPv6 PIM-SM 情報の確認」と「32.2.4　MLD 情報の確認」について確認してください。

show ipv6 mcache コマンドは IPv6 マルチキャストルーティングプログラムが保持している IPv6 マルチキャスト中継エントリを表示し，show netstat multicast コマンドはハードウェアに登録したマルチキャスト中継エントリを表示します。

図 32-7　show ipv6 mcache コマンドの実行結果

```
> show ipv6 mcache
Date 2007/04/20 15:20:00 UTC
Total: 1 route
- Forwarding entry  ------------------------------------------------------
Group Address                              Source Address
ff15::2                                    2001:db8::100
    uptime: 00:20    expires: 02:40    flags:
    incoming:
        VLAN0002
    outgoing:
        VLAN0001
        VLAN0003
>
```

図 32-8　show netstat multicast コマンドの実行結果

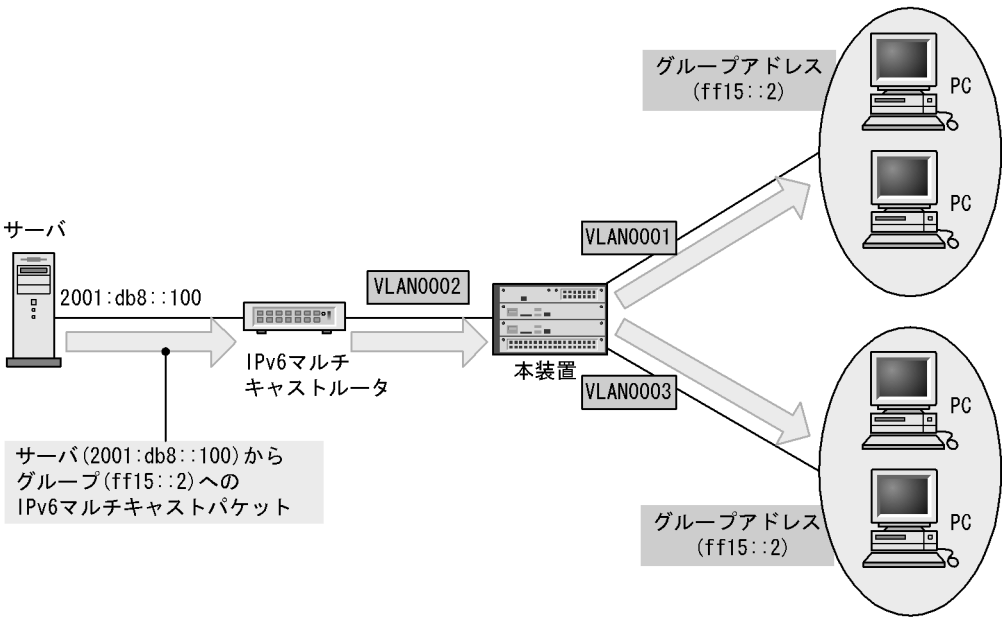
```
> show netstat multicast
Date 2008/04/10 15:20:00 UTC
Virtual Interface Table is empty

Multicast Forwarding Cache is empty

IPv6 Virtual Interface Table
 Mif   Rate       PhyIF          Pkts-In   Pkts-Out
   0      0   VLAN0004                0          0
   1      0   VLAN0002                0          0
   2      0   VLAN0001                0          0
   3      0   VLAN0003                0          0

IPv6 Multicast Forwarding Cache
 Origin                  Group           Packets Waits In-Mif Out-Mifs
 2001:db8::100           ff15::2               0     0    1    2  3

Total no. of entries in cache: 1
```



32.2.3　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情報で，PIM-SM 機能を設定した場合の確認内容には次のも

のがあります。

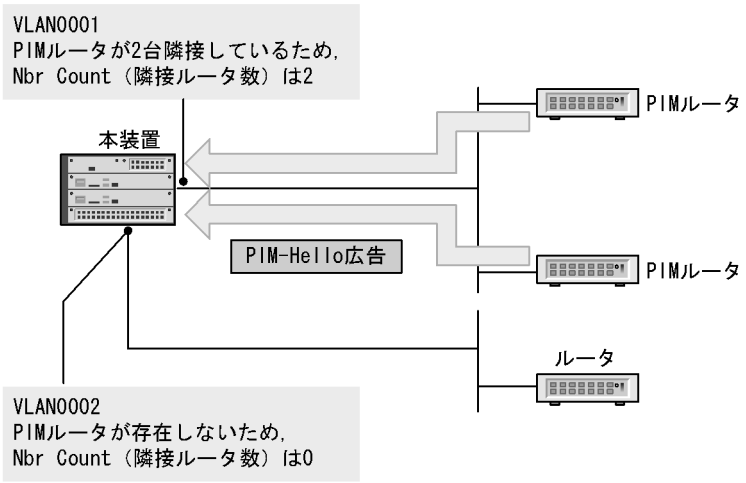
(1) インタフェース情報

show ipv6 pim interface を実行して，次のことを確認してください。

図 32-9 show ipv6 pim interface コマンドの実行結果

```
> show ipv6 pim interface
Date 2006/03/01 15:20:00 UTC
Interface      Component  Vif Nbr    Hello DR                        This
                             Count  Intvl Address                     System
VLAN0001       PIM-SM       1     2     30 fe80::200:87ff:fe10:a95a Y
(以下省略)
```

- 当該インタフェース名称が含まれていることを確認してください。当該インタフェース名称が含まれていない場合，そのインタフェースで IPv6 PIM-SM は動作していません。コンフィグレーションで当該インタフェースで IPv6 PIM が enable になっているか確認してください。また，そのインタフェースに障害が発生していないか確認してください。
- 該当インタフェースの Nbr Count（PIM 隣接ルータ数）を確認してください。0 の場合は隣接ルータが存在しないか，隣接ルータが PIM-Hello を広告していない可能性があります。隣接ルータを調査してください。

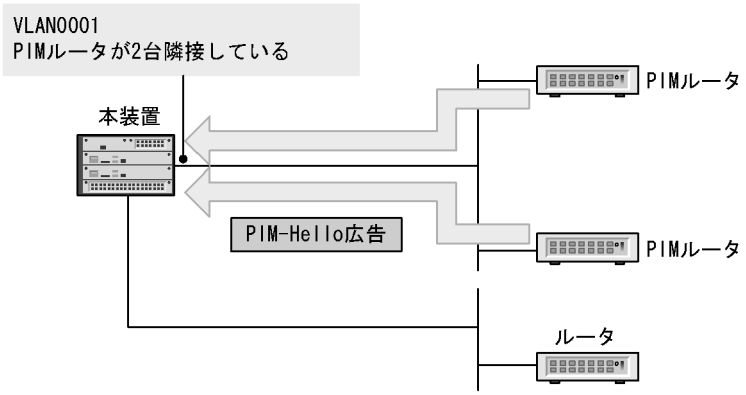


(2) 隣接情報

show ipv6 pim neighbor を実行して，当該インタフェースに関する隣接相手を確認してください。ある特定の隣接が存在しない場合，隣接ルータが PIM-Hello を広告していない可能性があります。隣接ルータを調査してください。

図 32-10 show ipv6 pim neighbor コマンドの実行結果

```
> show ipv6 pim neighbor
Date 2006/03/01 15:20:00 UTC
Neighbor Address          Interface Uptime Expires
fe80::200:87ff:fea0:abcd  VLAN0001  00:05  01:40
fe80::200:87ff:feb0:1234  VLAN0001  00:05  01:40
(以下省略)
```

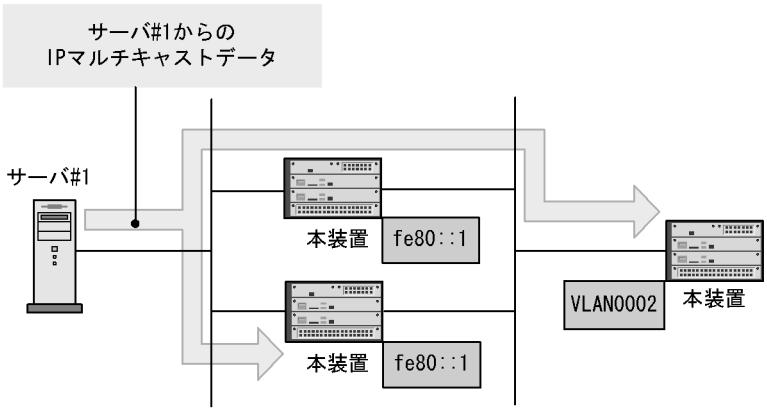


(3) 送信元ルート情報

show ipv6 rpf コマンドを実行して，送信元のルート情報を確認してください。

図 32-11　show ipv6 rpf コマンドの実行結果

```
> show ipv6 rpf 2001:db8::100
Date 2010/04/15 12:13:13 UTC
Incoming: VLAN0002 Upstream: fe80::1
（以下省略）
```



(4) PIM-SM BSR 情報

show ipv6 pim bsr を実行して，BSR アドレスが表示されていることを確認してください。”----”表示の場合，BSR が Bootstrap メッセージを広告していないか，BSR が存在していない可能性があります。BSR を調査してください。なお，PIM-SSM では BSR は使用しませんのでご注意ください。

図 32-12　show ipv6 pim bsr コマンドの実行結果

```
> show ipv6 pim bsr
Date 2006/03/01 15:20:00 UTC
Status : Not Candidate Bootstrap Router
BSR Address : 2001:db8::1
    Priority: 100    Hash mask length: 30
    Uptime  : 03:00
    Bootstrap Timeout : 130 seconds
>
```

(5) PIM-SM ランデブーポイント情報

show ipv6 pim rp-mapping を実行して，該当の IPv6 マルチキャストグループアドレスに対する C-RP Address が表示されていることを確認してください。表示のない場合，BSR が Bootstrap メッセージを広告していないか，ランデブーポイントまたは BSR が存在していない可能性があります。ランデブーポイントおよび BSR を調査してください。なお，PIM-SSM ではランデブーポイントは使用しませんのでご注意ください。

図 32-13 show ipv6 pim rp-mapping コマンドの実行結果

```
> show ipv6 pim rp-mapping brief
Date 2006/03/01 15:20:00 UTC
Status : Not Candidate Rendezvous Point
Total: 2 routes, 2 groups, 1 RP
Group/Masklen                   C-RP Address
ff15:100::/32                   2001:db8::1
ff15:200::/64                   2001:db8::1
>
```

(6) PIM-SM ルーティング情報

show ipv6 mroute コマンドを実行し，当該宛先アドレスへの経路が存在するかどうかを確認してください。(S,G) エントリが存在しない場合は，(*,G) エントリが存在しているかを確認してください。(*,G) が存在しない場合，および incoming，outgoing が正しくない場合は隣接ルータを調査してください。なお，PIM-SSM では (*,G) は使用しません（存在しません）。

図 32-14 PIM-SM マルチキャストルート情報の表示

```
> show ipv6 mroute
Date 2007/04/20 15:20:00 UTC
Total: 4 routes, 2 groups, 2 sources

(S,G) 2 routes  -------------------------------------------------
Group Address                           Source Address
ff15:100::50                            2001:db8::100
    uptime 02:00    expires 02:30    assert 00:00    flags F  protocol SM
    incoming: VLAN0002  upstream: Direct  reg-sup: 30s
    outgoing: VLAN0003  uptime 02:30    expires --:--

ff15:200::1                             2001:db8::200
    uptime 02:00    expires 02:30    assert 00:00    flags F  protocol SM
    incoming: VLAN0001  upstream: Direct  reg-sup: 30s
    outgoing: VLAN0003  uptime 02:30    expires --:--

(*,G) 2 routes  -------------------------------------------------
Group Address                           RP Address
ff15:100::50                            2001:db8::1
    uptime 02:00    expires --:--    assert 00:00    flags R  protocol SM
    incoming: VLAN0001  upstream: This System
    outgoing: VLAN0003  uptime 02:30    expires --:--

ff15:200::1                             2001:db8::2
    uptime 02:00    expires --:--    assert 00:00    flags R  protocol SM
    incoming: VLAN0001  upstream: fe80::1200:87ff:fe10:1234
    outgoing: VLAN0003  uptime 02:30    expires --:--
              VLAN0004  uptime 02:30    expires --:--
>
```

32.2.4 MLD 情報の確認

本装置の IPv6 マルチキャストルーティング情報で MLD 機能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

show ipv6 mld interface を実行して，次のことを確認してください。

- Interface 欄に表示されているインタフェースを確認してください。表示されているインタフェースで MLD が動作しています。期待したインタフェースが表示されない場合は mld のコンフィグレーションを確認してください。また，そのインタフェースに障害が発生していないか確認してください。
- 該当インタフェースの Group Count（加入グループ数）を確認してください。0 の場合は加入グループが存在しないかグループ加入ホストが MLD-Report を広告していない可能性があります。ホストを調査してください。
- Version 欄に表示されているバージョンが当該インタフェースで使用しているホストと接続可能であるか確認してください。
- Notice 欄にコードが表示される場合は MLD パケットが廃棄されています。コードから廃棄理由を調査してください。

図 32-15 show ipv6 mld interface コマンドの実行結果

```
> show ipv6 mld interface
Date 2008/04/10 15:10:00 UTC
Total: 10 Interfaces
Interface   Version   Flags  Querier             Expires  Group Count  Notice
VLAN0001        1      S     fe80::10:87ff:2959   02:30             4  L
VLAN0003        2            fe80::10:87ff:2959   01:30             2
VLAN0004      (2)            fe80::10:87ff:2959     -               5   QR
VLAN0005        1            fe80::1234           01:00             3   Q
VLAN0006        1            fe80::2592           02:30             6
(以下省略)
```

(2) グループ情報

show ipv6 mld group を実行し，Group Address 内のグループを確認してください。存在しない場合，次のことを確認してください。

- そのグループメンバー（ホスト）が MLD-Report を広告していない可能性があります。ホストを調査してください。
- 本装置の MLD インタフェースのバージョンとホストの MLD バージョンを確認して，ホストと接続可能であることを確認してください。
- ホストが MLDv2 Query を無視する場合，MLDv2 を使用することはできません。当該インタフェースの MLD バージョンを 1 に設定してください。

図 32-16 show ipv6 mld group コマンドの実行結果

```
> show ipv6 mld group brief
Date 2006/03/01 15:20:00 UTC
Total: 20 groups
Group Address       Interface    Version  Mode  Source Count
ff15::100::50       VLAN0001        1     EXCLUDE          9
ff15::100::60       VLAN0003        2     INCLUDE          2
ff15::200::1        VLAN0003        1     EXCLUDE          0
ff15::200::2        VLAN0004        2     EXCLUDE          1
(以下省略)
```

33 IPv6 マルチキャスト経路フィルタリング【OP-NPAR】

この章では，IPv6 マルチキャスト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。

33.1 IPv6 マルチキャスト経路フィルタリング解説

33.1.1 IPv6 マルチキャスト経路フィルタリング概説

IPv6 マルチキャスト経路フィルタリングは，IPv6 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 IPv6 マルチキャストエクストラネットだけで使用します。

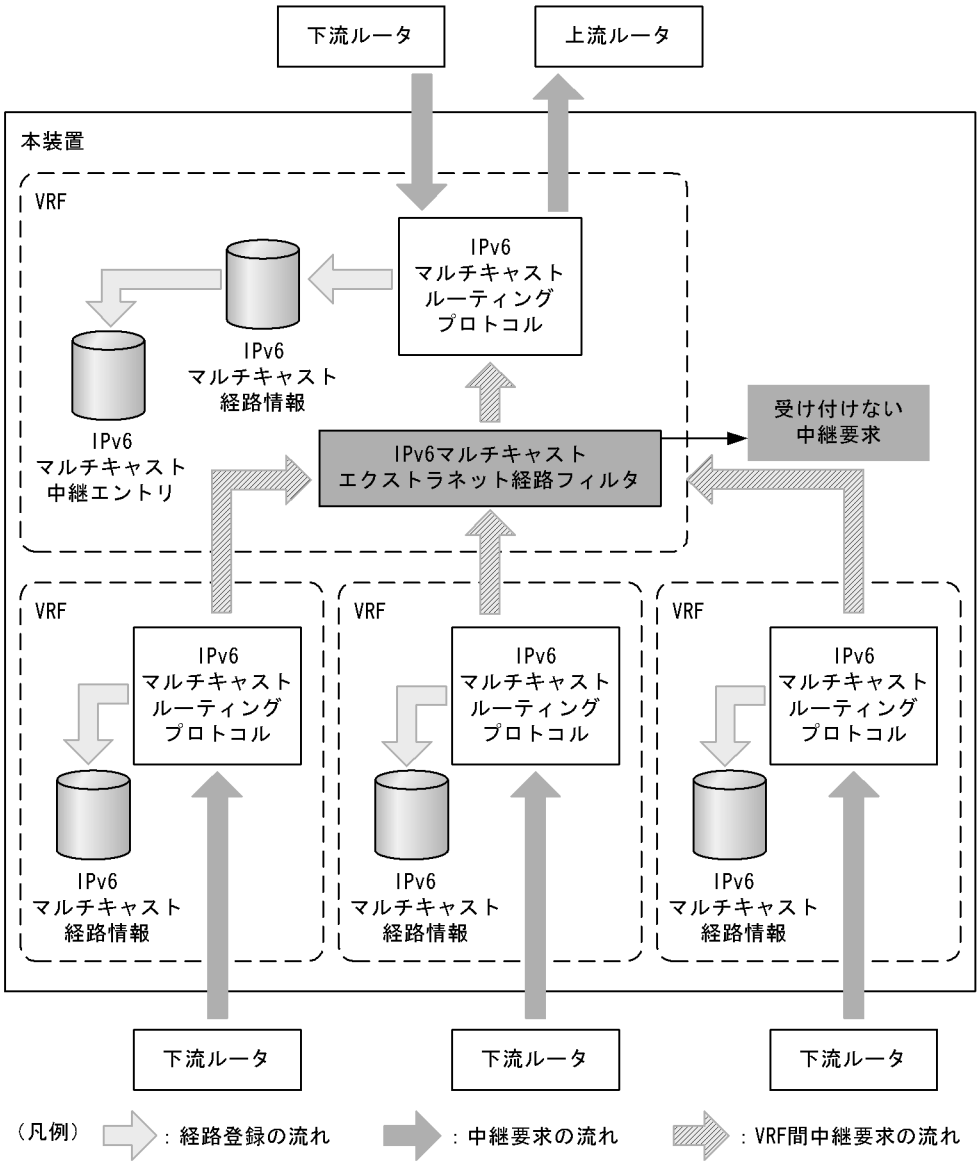
(1) IPv6 マルチキャストエクストラネットの経路フィルタリング

IPv6 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。IPv6 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宛先 IP 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，IPv6 マルチキャストルーティングプロトコルは送信元 IP 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。

IPv6 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。

IPv6 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を次の図に示します。

図 33-1　IPv6 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



33.1.2　IPv6 マルチキャストフィルタ方法

IPv6 マルチキャストフィルタ方法については,「30.1.2　フィルタ方法」を参照してください。

IPv6 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 33-1　IPv6 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
ipv6 prefix-list	未サポートです。指定した場合は無視します。
ipv6 access-list	permit だけを使用します。 deny を指定した IP 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。
ip as-path access-list	未サポートです。指定した場合は無視します。

コンフィグレーションコマンド	説明
ip community-list standard	未サポートです。指定した場合は無視します。
ip community-list extended	未サポートです。指定した場合は無視します。

33.1.3 IPv6 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 IPv6 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 ipv6 import multicast inter-vrf 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 IPv6 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。

IPv6 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 33-2 IPv6 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
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。

IPv6 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 33-3 IPv6 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
宛先 IPv6 マルチキャストグループアドレス	access-list の識別子を条件として指定し，指定したフィルタで宛先の IPv6 マルチキャスト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，一致したとみなします。 本条件を設定しない場合，すべての IPv6 マルチキャストグループアドレスが許可対象になります。	match ipv6 address ipv6 access-list
VRF ID	VRF ID を条件として指定し，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 IPv6 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 IPv6 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。IPv6 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，IPv6 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 IP アドレスへの経路を自 VRF となるように設定します。

33.2 コンフィグレーション

33.2.1 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 33-4 コンフィグレーションコマンド一覧

コマンド名	説明
ipv6 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。
match ipv6 address ※2	route-map に IPv6 宛先アドレスによるフィルタ条件を設定します。
match vrf ※2	route-map に VRF によるフィルタ条件を設定します。
ipv6 import multicast inter-vrf ※3	他 VRF またはグローバルネットワークからの IPv6 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。

注※ 1
「コンフィグレーションコマンドレファレンス Vol.2　4. 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　14. 経路フィルタリング（IPv4 ／ IPv6 共通）」を参照してください。

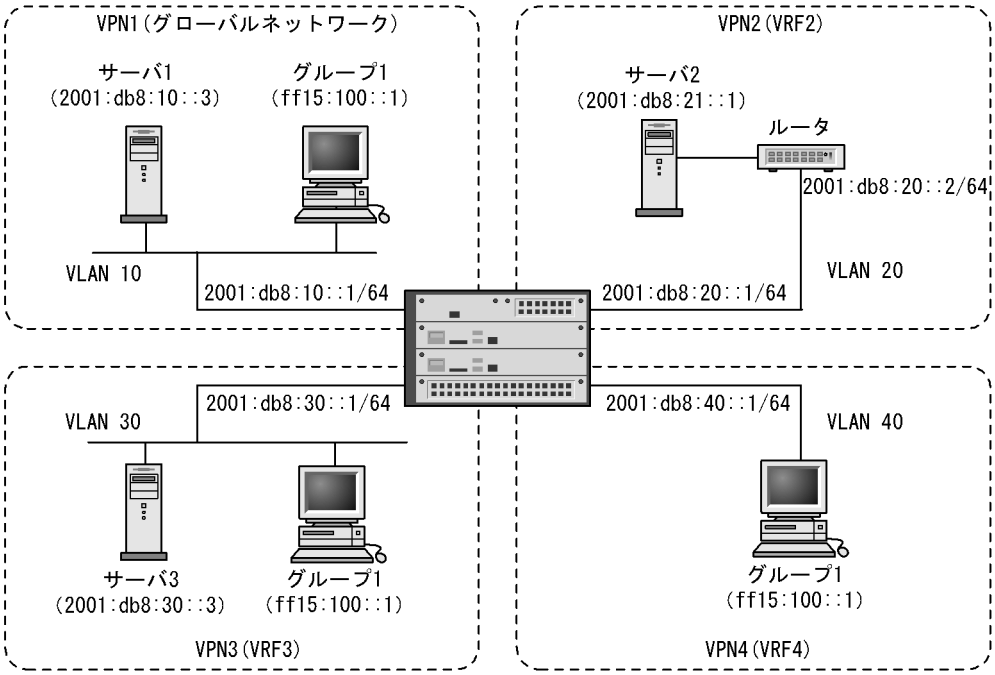
注※ 3
「コンフィグレーションコマンドレファレンス Vol.3　30. VRF【OP-NPAR】」を参照してください。

33.2.2 IPv6 マルチキャストエクストラネット

次の図のようなネットワーク構成で，IPv6 マルチキャストエクストラネットを設定します。

IPv6 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 33-2 IPv6 マルチキャストエクストラネットの構成例



(1) すべての VRF からの要求を許可する設定

VRF 2 が，すべての VRF およびグローバルネットワークからの IPv6 マルチキャスト中継要求を許可す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，中継先 VRF およびグローバルネットワークから IPv6 マルチキャスト送信元への経路が 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 IPv6 マルチキャスト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 IPv6 マルチキャスト中継要求を許可するように設定します。

(2) 特定 VRF だけ許可する設定

VRF 2 が VRF 3 および VRF 4 からの IPv6 マルチキャスト中継要求を許可す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，VRF3 および VRF4 から IPv6 マルチキャスト送信元への経路が VRF2 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 IPv6 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 IPv6 マルチキャスト中継要求だけ許可にします。

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 IPv6 マルチキャストエクストラネットに適用して，VRF 3 および VRF 4 からの IPv6 マルチキャスト中継要求を許可するように設定します。

(3) 特定グループアドレスだけ許可する設定

ff15:100::/32 の範囲内のグループアドレスだけ IPv6 マルチキャスト中継要求を許可す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，中継先 VRF およびグローバルネットワークから IPv6 マルチキャスト送信元への経路が VRF2 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 ff15:100::/32 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を ff15:100::/32 に設定します。

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 IPv6 マルチキャスト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 ff15:100::/32 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，IPv6 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 IPv6 マルチキャスト送信元への経路が，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 ff15:100::/32 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 ff15:100::/32 に対する IPv6 マルチキャスト中継要求を許可にします。

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 IPv6 マルチキャストエクストラネットに適用して，相互に IPv6 マルチキャスト中継要求を許可するように設定します。

33.3 オペレーション

33.3.1 運用コマンド一覧

IPv6 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 33-5 運用コマンド一覧

コマンド名	説明
show ipv6 mcache ※	IPv6 マルチキャスト中継エントリを一覧表示します。
show ipv6 mroute ※	IPv6 マルチキャスト経路情報を一覧表示します。
show ipv6 multicast resources ※	IPv6 マルチキャストルーティングで使用している各エントリ数を表示します。

注※
「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。

33.3.2 IPv6 マルチキャストエクストラネットの確認

show ipv6 mroute 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によって VRF 間中継するエントリを参照できます。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。

図 33-3 show ipv6 mroute コマンドの実行結果

```
> show ipv6 mroute vrf all group ff15:100::1 source 2001:db8:21::1
Date 2010/04/15 12:40:30 UTC
Total: 4 routes
VRF: global  Total: 1 route, 1 group, 1 source

(S,G) 1 route  ------------------------------------------------
Group Address                       Source Address
ff15:100::1                         2001:db8:21::1
    uptime: 02:00    expires: 02:30    assert: 00:00    flags: FL  protocol SM
    incoming: VRF 2          upstream: Extra  reg-sup: 0s
    outgoing: VLAN0010  uptime 02:30    expires --:--

VRF: 2  Total: 1 routes, 1 groups, 1 sources

(S,G) 1 route  ------------------------------------------------
Group Address                       Source Address
ff15:100::1                         2001:db8:21::1
    uptime: 02:00    expires: 02:30    assert: 00:00    flags: LV  protocol SM
    incoming: VLAN0020       upstream: 2001:db8:20::2  reg-sup: 0s
    outgoing: global    uptime 02:30
    outgoing: VRF 3     uptime 02:30
    outgoing: VRF 4     uptime 02:30

VRF: 3  Total: 1 route, 1 group, 1 source

(S,G) 1 route  ------------------------------------------------
Group Address                       Source Address
ff15:100::1                         2001:db8:21::1
    uptime: 02:00    expires: 02:30    assert: 00:00    flags: FL  protocol SM
    incoming: VRF 2          upstream: Extra  reg-sup: 0s
    outgoing: VLAN0030  uptime 02:30    expires --:--

VRF: 4  Total: 1 route, 1 group, 1 source

(S,G) 1 route  ------------------------------------------------
Group Address                       Source Address
ff15:100::1                         2001:db8:21::1
    uptime: 02:00    expires: 02:30    assert: 00:00    flags: FL  protocol SM
    incoming: VRF 2          upstream: Extra  reg-sup: 0s
    outgoing: VLAN0040  uptime 02:30    expires --:--

>
```

図 33-4　show ipv6 mcache コマンドの実行結果

```
> show ipv6 mcache vrf all group ff15:100::1 source 2001:db8:21::1
Date 2010/04/15 12:42:30 UTC
Total: 4 routes
VRF: global  Total: 1 route
- Forwarding entry  ----------------------------------------------------------
Group Address                            Source Address
ff15:100::1                              2001:db8:21::1
    uptime: 00:20    expires: 02:40    flags: U
    incoming:
        VRF 2
    outgoing:
        VLAN0010

VRF: 2  Total: 1 route
- Forwarding entry  ----------------------------------------------------------
Group Address                            Source Address
ff15:100::1                              2001:db8:21::1
    uptime: 00:20    expires: 02:40    flags: U
    incoming:
        VLAN0020
    outgoing:
        VLAN0010      global
        VLAN0030      VRF 3
        VLAN0040      VRF 4

VRF: 3  Total: 1 route
- Forwarding entry  ----------------------------------------------------------
Group Address                            Source Address
ff15:100::1                              2001:db8:21::1
    uptime: 00:20    expires: 02:40    flags:D
    incoming:
        VRF 2
    outgoing:
        VLAN0030

VRF: 4  Total: 1 route
- Forwarding entry  ----------------------------------------------------------
Group Address                            Source Address
ff15:100::1                              2001:db8:21::1
    uptime: 00:20    expires: 02:40    flags:D
    incoming:
        VRF 2
    outgoing:
        VLAN0040

>
```

34 ネットワーク・パーティション【OP-NPAR】

この章では，ネットワーク・パーティションの解説，ネットワーク構築例および VRF 機能に必要な操作方法について説明します。

34.1 解説

34.1.1 ネットワーク・パーティションの概要

ネットワーク・パーティションは，部門ごとや業務ごとに構築されているネットワークを一つのネットワークに統合するネットワークコンソリデーションを可能にします。ネットワーク・パーティションで実現するネットワークコンソリデーションを次の表および図に示します。

表 34-1 ネットワークコンソリデーションの分類

分類	説明
物理的コンソリデーション	ネットワークを論理的に分離したままで，装置や回線を物理的に統合します。
運用管理コンソリデーション	ネットワーク上に分散していたレイヤ 3 機能を 1 拠点で集中管理することで，運用管理を統合します。

図 34-1 物理的コンソリデーション

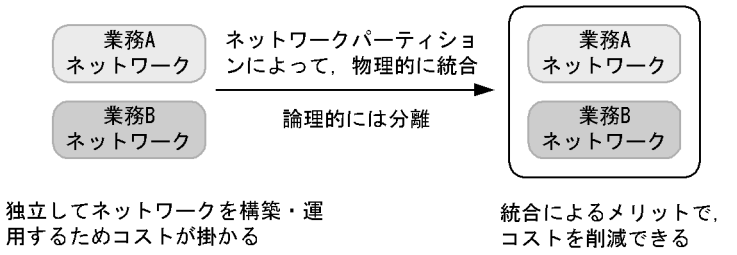
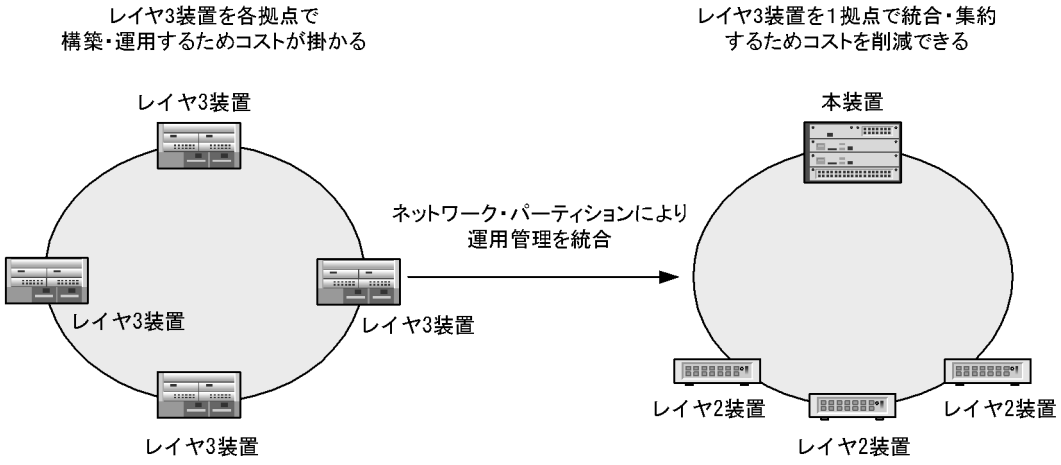


図 34-2 運用管理コンソリデーション



ネットワーク・パーティションは，VRF および VLAN によってネットワークを論理的に分割し，VPN を構成します。ネットワーク・パーティションを導入すると，次の表に示すような利点があります。

表 34-2 ネットワーク・パーティションの利点

利点	説明
低コスト	• 装置，回線の物理的統合によって，少ない装置や回線数でネットワーク構築し，初期導入コストを低減できます。 • レイヤ 3 機能を 1 拠点で集中管理することで，ランニングコストを低減できます。

利点	説明
強固なセキュリティ	• ネットワークを論理的に分離できます。
ネットワーク統合が容易	• 複数のネットワークを一つのネットワークに物理的に統合できます。 • 論理的には分離されているため，IP アドレスが重複していても IP アドレスの変更が不要です。
省電力	• 装置，回線の物理的統合によって，環境配慮型のネットワークを構築できます。

34.1.2 VRF

ネットワーク・パーティションを実現する機能の一つとして VRF があります。VRF とは，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，各ルーティングテーブルに従い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。そのため，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は VRF インスタンスごとに独立して動作します。

VLAN 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。

各機能の VRF のサポート状況を次の表に示します。

表 34-3 VRF サポート状況

項目		サポート状況	備考
VLAN 機能	ポート VLAN	○	なし
	プロトコル VLAN	○	
	MAC VLAN	○	
	Tag 変換	○	
	VLAN トンネリング	○	
レイヤ 2 プロトコル	スパニングツリー	－	VRF と装置単位で排他
	Ring Protocol	○	VRF との同時動作については，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 22.6 Ring Protocol 使用時の注意事項
IGMP snooping/MLD snooping		○	なし
ポリシーベーススイッチング		○	なし
フィルタ	フィルタ	○	なし
	uRPF	○	
QoS		○	なし
レイヤ 2 認証	IEEE 802.1X	－	VRF と装置単位で排他
	Web 認証	－	VRF と装置単位で排他
	MAC 認証	－	VRF と装置単位で排他
	認証 VLAN	－	VRF と装置単位で排他
DHCP snooping		○	なし
高信頼化機能	GSRP	○	なし

項目		サポート状況	備考
	VRRP	○	
障害検出機能	IEEE802.3ah/UDLD	○	なし
	ストームコントロール	○	
	L2 ループ検知	○	
	CFM	○	
リモートネットワーク管理	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。 • コンフィグレーションガイド Vol.2 28.2 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
	トラップ	△	一部のトラップ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. サポート MIB トラップ
	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.2 29.2.3 ログの VRF への 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
	sFlow 統計	△	VRF も統計対象に含みます。ただし，VRF 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。 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。
隣接装置情報管理	LLDP	△	Organizationally-defined TLV extensions 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 31.1.3 LLDP 使用時の注意事項
	OADP	△	VRF の VLAN では，OADP 中に Address 情報は含まれません。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 32.1.3 OADP 使用時の注意事項
ポートミラーリング		○	なし

項目		サポート状況	備考
レイヤ 3 中継	IPv4 ユニキャスト中継	○	本章のほかに次を参照してください。 • 7.13 VRF の解説【OP-NPAR】 • 7.14 VRF のコンフィグレーション【OP-NPAR】 • 7.15 VRF のオペレーション【OP-NPAR】
	IPv4 ユニキャスト VRF 間中継	○	詳細は次を参照してください。 • 7.13.3 エクストラネット • 8.2.7 VRF 間にわたるスタティック経路の設定【OP-NPAR】 • 13.1.6 エクストラネット【OP-NPAR】 • 13.2.8 エクストラネット【OP-NPAR】 • 13.3.10 エクストラネットの確認【OP-NPAR】
	IPv4 マルチキャスト中継	○	詳細は次を参照してください。 • 14.4.6 VRF での IPv4 マルチキャスト【OP-NPAR】 • 15.1 コンフィグレーション • 16 IPv4 マルチキャスト経路フィルタリング【OP-NPAR】
	IPv4 マルチキャスト VRF 間中継	○	
	IPv6 ユニキャスト中継	○	本章のほかに次を参照してください。 • 24.13 VRF の解説【OP-NPAR】 • 24.14 VRF のコンフィグレーション【OP-NPAR】 • 24.15 VRF のオペレーション【OP-NPAR】
	IPv6 ユニキャスト VRF 間中継	○	詳細は次を参照してください。 • 24.13.3 エクストラネット • 25.2.7 VRF 間にわたるスタティック経路の設定【OP-NPAR】 • 30.1.6 エクストラネット【OP-NPAR】 • 30.2.8 エクストラネット【OP-NPAR】 • 30.3.9 エクストラネットの確認【OP-NPAR】
	IPv6 マルチキャスト中継	○	IPv6 マルチキャストを VRF で動作させた場合，グローバルネットワークを含む全 VRF で IPv6 PIM-SSM の系切替時の通信無停止対応機能が動作しません。 VRF での IPv6 マルチキャスト中継については，次を参照してください。 • 31.4.11 VRF での IPv6 マルチキャスト【OP-NPAR】 • 32.1 コンフィグレーション • 33 IPv6 マルチキャスト経路フィルタリング【OP-NPAR】
	IPv6 マルチキャスト VRF 間中継	○	

項目		サポート状況	備考
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。
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。 • 4.2.3 ポリシーベースルーティングでのエクストラネットの設定【OP-NPAR】 • 20.2.3 ポリシーベースルーティングでのエクストラネットの設定【OP-NPAR】
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。 • 5.2.4 VRF 構成での設定【OP-NPAR】 • 5.2.5 エクストラネット構成での設定【OP-NPAR】
DHCP サーバ機能		－	グローバルネットワークだけが対象
IPv6 DHCP リレー		－	グローバルネットワークだけが対象
IPv6 DHCP サーバ機能		－	グローバルネットワークだけが対象
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。 • 8.2.6 VRF でのスタティック経路の設定【OP-NPAR】 • 8.2.7 VRF 間にわたるスタティック経路の設定【OP-NPAR】
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。 • 25.2.6 VRF でのスタティック経路の設定【OP-NPAR】 • 25.2.7 VRF 間にわたるスタティック経路の設定【OP-NPAR】 • 25.2.8 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【OP-NPAR】
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。 • 9.2.8 VRF での RIP の適用【OP-NPAR】 • 10.2.7 VRF での OSPF の適用【OP-NPAR】
	OSPF	○	

項目		サポート状況	備考
	BGP4	○	詳細は次を参照してください。 • 12.1.4 VRF での BGP4 の機能【OP-NPAR】 • 12.2.11 VRF での BGP4 の設定【OP-NPAR】
	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。 • 26.2.5 VRF での RIPng の適用【OP-NPAR】 • 27.2.7 VRF での OSPFv3 の適用【OP-NPAR】
	OSPFv3	○	
	BGP4+	○	詳細は次を参照してください。 • 29.1.4 VRF での BGP4+ の機能【OP-NPAR】 • 29.2.11 VRF での BGP4+ の設定【OP-NPAR】
	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。 • 14.4.6 VRF での IPv4 マルチキャスト【OP-NPAR】 • 15.1 コンフィグレーション • 16 IPv4 マルチキャスト経路フィルタリング【OP-NPAR】
	PIM-SM	○	
	PIM-SSM	○	
	PIM-DM	―	グローバルネットワークだけが対象
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。 • 31.4.11 VRF での IPv6 マルチキャスト【OP-NPAR】 • 32.1 コンフィグレーション • 33 IPv6 マルチキャスト経路フィルタリング【OP-NPAR】
	PIM-SM	○	
	PIM-SSM	○	
運用・保守	ping	○	なし
	traceroute	○	
	telnet	○	
	ftp	○	
	tftp	○	

項目		サポート状況	備考
	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 8.1.9 VRF でのリモート運用端末からのログインの許可【OP-NPAR】 • 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を許可する IP アドレスの設定【OP-NPAR】
	ftp によるログイン	○	
	DNS リゾルバ	―	グローバルネットワークだけが対象
	NTP	○	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 9.1.6 VRF での NTP による時刻同期の設定【OP-NPAR】

（凡例）○：サポート　△：一部サポート　―：未サポート

本装置では，VRF インスタンスで IPv6 を使用するかどうか，および Ring Protocol や GSRP を VRF と同時動作させるかどうかを，動作モードとして設定します。本装置でサポートする VRF の動作モード，動作対象となる通信プロトコル，値の範囲および説明を次の表に示します。

表 34-4　VRF の動作モード，値の範囲および説明

VRF 動作モード	VRF 動作対象プロトコル	VRF の値の範囲	説明
設定なし	なし	設定不可	• VRF は動作しません
axrp-enable	IPv4	2 ～ 64	• IPv4 だけが VRF インスタンスで動作します • Ring Protocol が動作します
l2protocol-disable	IPv4	2 ～ 250	• IPv4 だけが VRF インスタンスで動作します • レイヤ 2 プロトコルが動作しません
axrp-enable-ipv4-ipv6	IPv4 IPv6	2 ～ 64	• IPv4 と IPv6 のどちらも VRF インスタンスで動作します • Ring Protocol が動作します
gsrp-enable-ipv4-ipv6	IPv4 IPv6	2 ～ 125	• IPv4 と IPv6 のどちらも VRF インスタンスで動作します • GSRP が動作します
l2protocol-disable-ipv4-ipv6	IPv4 IPv6	2 ～ 250	• IPv4 と IPv6 のどちらも VRF インスタンスで動作します • レイヤ 2 プロトコルが動作しません

なお，VRF を使用するためには，オプションライセンス OP-NPAR が必要です。MSU-1A，MSU-1A1，および CSU-1A では未サポートです。

34.1.3　ネットワーク構築例

ネットワーク・パーティションでは様々なネットワークを構築できます。本項では，代表的なネットワー

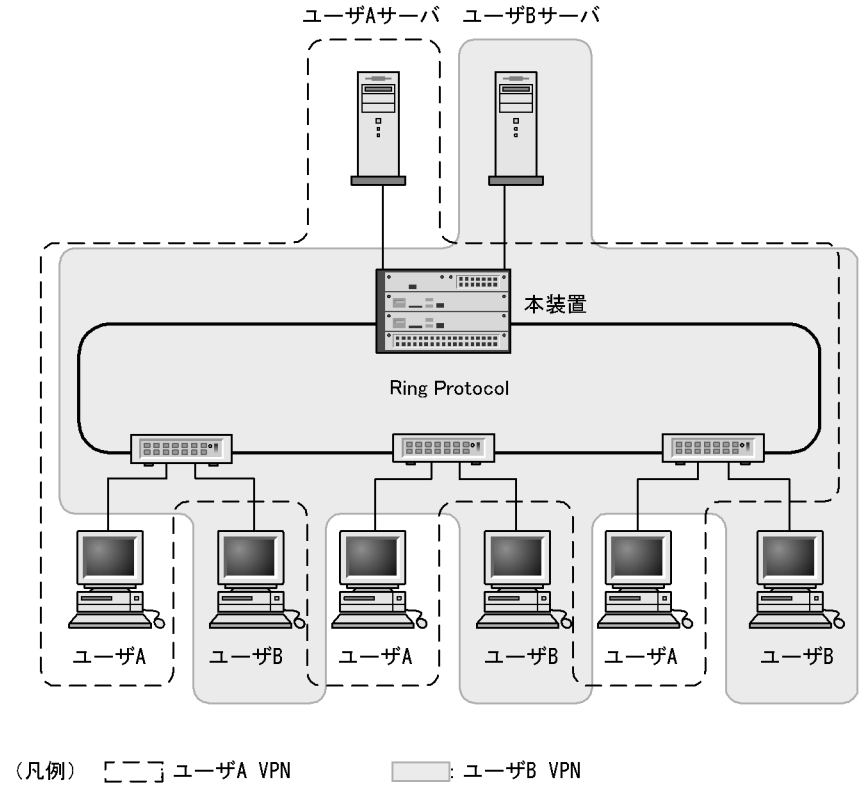
ク・パーティションの適用事例を基にネットワークの構築方法を説明します。

(1) Ring Protocol を使用したネットワーク・パーティション

ネットワーク・パーティションに最も適した構築方法の一つとして，Ring Protocol を使用した構成があります。Ring Protocol を使用することで，障害発生に伴う経路切り替えを高速に行うことができ，信頼性の高いネットワークを構築できます。また，レイヤ 3 機能を一つの拠点に集中させることでネットワーク運用が容易になる利点もあります。

Ring Protocol を使用したネットワーク・パーティションの構築例を次の図に示します。図中のユーザ A とユーザ B は異なる VPN で，互いに通信できないようにする例です。

図 34-3　Ring Protocol を使用したネットワーク・パーティション

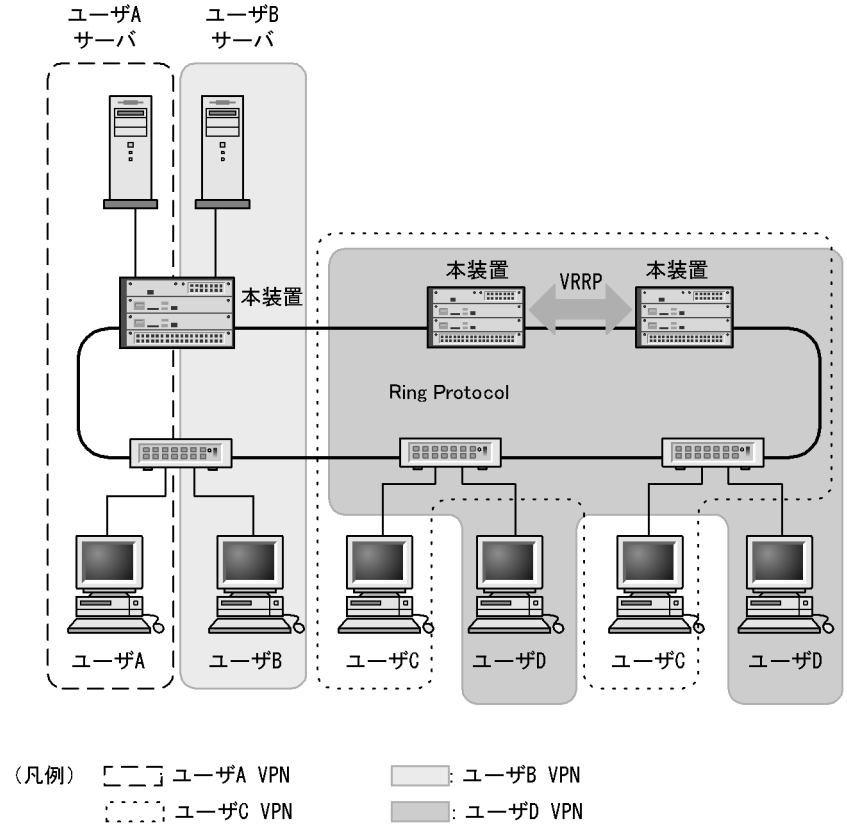


(2) レイヤ 3 集約装置の増設

ネットワーク全体で扱う VRF 数や拠点数が多くなった場合，レイヤ 3 機能を持つ装置を増設することで分散して収容できます。また，信頼性が要求される装置では VRRP を動作させることで，さらに信頼性を向上できます。

レイヤ 3 集約装置を増設する構築例を次の図に示します。

図 34-4　レイヤ 3 集約装置の増設

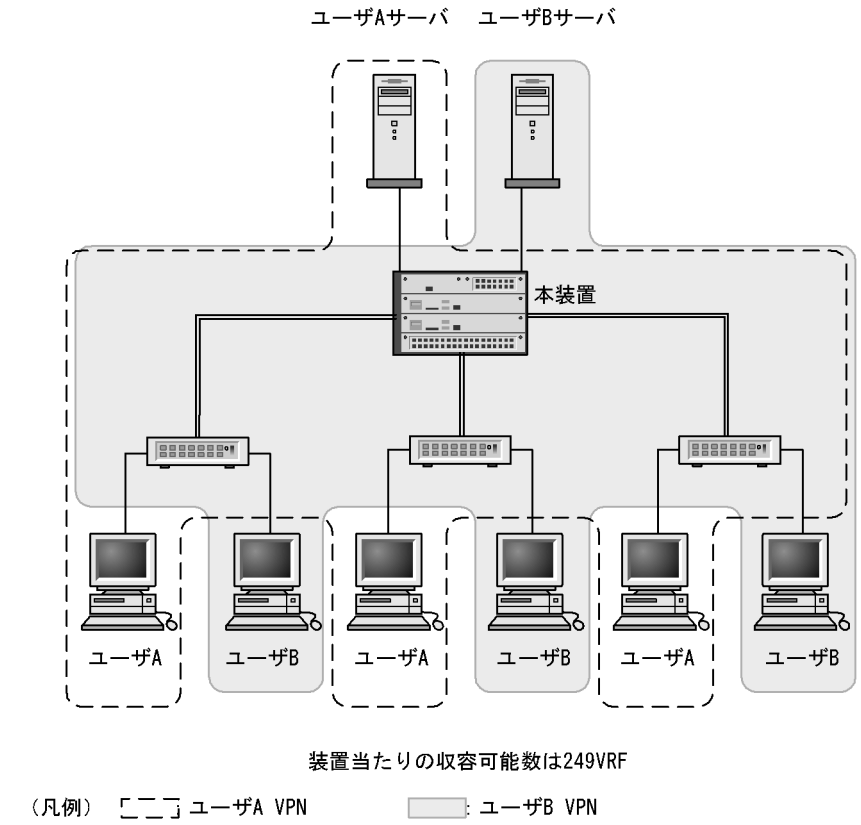


(3) レイヤ 2 プロトコルを使用しない構築

レイヤ 2 プロトコルを使用しないネットワークでも，VRF 機能は使用できます。Ring Protocol を使用する場合と比較すると，多くの VRF を同時に動作させられます。

レイヤ 2 プロトコルを使用しない構築例を次の図に示します。

図 34-5 レイヤ 2 プロトコルを使用しない構築



(4) エクストラネットの実現

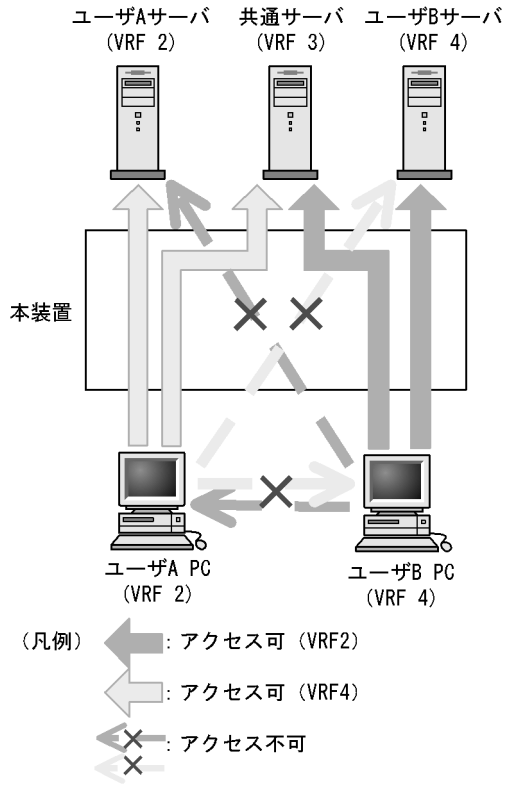
エクストラネットでは，VRF 間の通信を遮断しながら，特定の VRF 間だけ通信できるようにします。これによって，ユーザ間のセキュリティを保った状態で共通サーバへのアクセスを許可するネットワークが構築できます。

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います。

- 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。

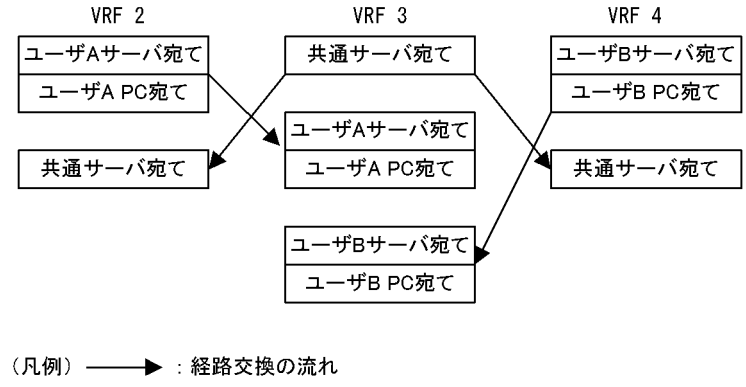
図 34-6 経路交換によるエクストラネット



- 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。

上記の場合，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 34-7 本装置の経路情報



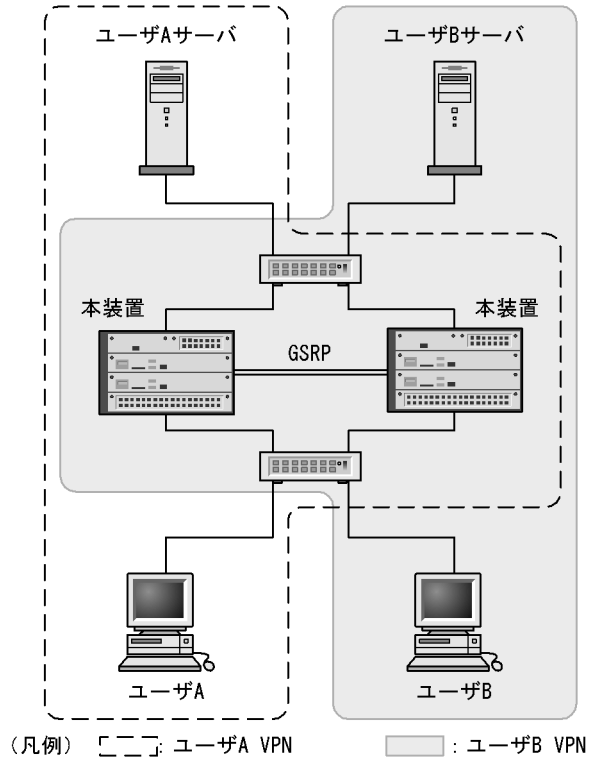
(5) GSRP を使用したネットワーク・パーティション

VRF では冗長化機能として GSRP を使用できます。GSRP を使用すると，障害発生に伴う装置切り替えを高速に行うことができ，信頼性の高いネットワークを構築できます。また，レイヤ 2 とレイヤ 3 の冗長化を一つの機能で実現できる利点もあります。

GSRP を使用したネットワーク・パーティションの構築例を次の図に示します。図中のユーザ A とユーザ

B は異なる VPN で，互いに通信できないようにする例です。

図 34-8　GSRP を使用したネットワーク・パーティション



34.2 コンフィグレーション

34.2.1 コンフィグレーションコマンド一覧

ネットワーク・パーティ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 34-5 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	VRF の IPv6 最大経路数と警告の運用メッセージ出力閾値を設定します。
maximum routes	VRF の IPv4 最大経路数と警告の運用メッセージ出力閾値を設定します。
vrf definition	VRF を設定します。
vrf mode	VRF と Ring Protocol の同時動作や排他動作などのモードを設定します。
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　16. IPv6・NDP・ICMPv6」を参照してください。

34.2.2 VRF の設定

本装置で VRF 機能を動作させるには，VRF 動作モードの設定，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。本節では，VRF 動作モードの設定からインタフェースの 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 動作モードの設定はハードウェアの再起動を伴うため，運用を開始する時点で設定してください。VRF 動作モードは，VRF インスタンスで IPv6 を使用するかどうか，および Ring Protocol や GSRP を VRF と同時動作させるかどうかから決定してください。
なお，VRF を設定する前に，スパニングツリーを停止してください。

[コマンドによる設定]

1. **(config)# spanning-tree disable**
   スパニングツリーを停止します。

2. **(config)# vrf mode axrp-enable-ipv4-ipv6**
   PSP will be restarted automatically when the selected mode differs from current mode.
   Do you wish to change mode (y/n):
   VRF インスタンスで IPv4 と IPv6 のどちらも使用でき，かつ Ring Protocol を使用できる VRF 動作モードを設定します。
   コンフィグレーションの変更を確認して y を入力すると，AX6700S ではすべての BSU を，AX6600S

およびAX6300Sではpspを自動的に再起動します。nを入力した場合，コンフィグレーションを変更しません。

3. **(config)# vrf definition 2**
   (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 2を設定します。IPv4最大経路数を500，警告の運用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，警告の運用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。

4. **(config)# interface loopback 2**
   (config-if)# vrf forwarding 2
   (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にVRFを指定します。ループバックインタフェース2にVRF 2を指定して，IPv4アドレスとして192.168.0.2を，IPv6アドレスとして2001:db8::2を設定します。

5. **(config)# interface vlan 10**
   (config-if)# vrf forwarding 2
   (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
   VLANインタフェースにVRFを指定します。VLAN ID 10にVRF 2とIPv4アドレス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。

34.3 オペレーション

34.3.1 運用コマンド一覧

ネットワーク・パーティションの運用コマンド一覧を次の表に示します。

表 34-6 運用コマンド一覧

コマンド名	説明
show vlan ※1	VLAN の情報を表示します。
show ip vrf ※2	VRF の IPv4 情報を表示します。
show ipv6 vrf ※3	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.1 20. VLAN」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 6. 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 13. IPv6 ルーティングプロトコル」を参照してください。

34.3.2 VRF 情報の確認

show ip vrf コマンドで，VRF の IPv4 経路情報や IPv4 インタフェースの状態を確認できます。また，show ipv6 vrf コマンドで，VRF の IPv6 経路情報や IPv6 インタフェースの状態を確認できます。

図 34-9 show ip vrf コマンドの実行結果

```
> show ip vrf 2
Date 2009/03/20 12:00:00 UTC
VRF              Routes        ARP
2                270/500       7/50
>
```

図 34-10 show ip vrf detail コマンドの実行結果

```
> show ip vrf 2 detail
Date 2009/03/20 12:00:00 UTC
VRF 2
  Maximum routes: 500, Warn threshold: 70%, Current routes: 270
  Maximum ARP entries: 50, Current ARP entries: 7
  Import inter-vrf: -
Interface
Name           Local              Remote          Status
VLAN0010       192.168.10.1/24    192.168.10.255  Up
loopback2      127.0.0.1/8        127.0.0.1       Up
loopback2      192.168.0.2/32     192.168.0.2     Up
>
```

図 34-11 show ipv6 vrf コマンドの実行結果

```
> show ipv6 vrf 2
Date 2009/03/20 12:00:00 UTC
VRF              Routes          Neighbor
2                200/400         7/50
>
```

図 34-12 show ipv6 vrf detail コマンドの実行結果

```
> show ipv6 vrf 2 detail
Date 2009/03/20 12:00:00 UTC
VRF 2
  Maximum routes: 400, Warn threshold: 70%, Current routes: 200
  Maximum Neighbor entries: 50, Current Neighbor entries: 7
  Import inter-vrf: -
Interface
Name            Address                                       Status
VLAN0010        2001:db8:10::1/64                             Up
VLAN0010        fe80::212:e2ff:fe20:b000%VLAN0010/64          Up
loopback2       ::1/128                                       Up
loopback2       2001:db8::2/128                               Up
loopback2       fe80::1%loopback2/64                          Up
>
```

show vlan コマンドで，VLAN が所属する VRF を確認できます。

図 34-13 show vlan コマンドの実行結果

```
> show vlan 10
Date 2009/03/20 12:00:00 UTC
VLAN counts:1
VLAN ID:10     Type:Port based      Status:Up
  Learning:On            Tag-Translation:Off
  BPDU Forwarding:       EAPOL Forwarding:
  Router Interface Name:VLAN0010
  VRF:2
  IP Address: 192.168.10.1/24
              2001:db8:10::1/64
  Source MAC address: 0012.e205.0800(System)
  Description:VLAN0010
  Spanning Tree:
  AXRP RING ID:     AXRP VLAN group:
  GSRP ID:      GSRP VLAN group:    L3:
  IGMP snooping:     MLD snooping:
  Flow mode:
  Untagged(8)   :1/5-12
  Tagged(2)     :1/25-26
  Tag-Trans(0)  :
>
```

付録

付録 A　準拠規格

付録 A　準拠規格

付録 A.1　IP・ARP・ICMP

表 A-1　IP バージョン 4 の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC791(1981 年 9 月)	Internet Protocol
RFC792(1981 年 9 月)	Internet Control Message Protocol
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
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
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

付録 A.2　DHCP/BOOTP リレーエージェント

表 A-2　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
RFC1812(1995 年 6 月)	Requirements for IP Version 4 Routers
RFC2131(1997 年 3 月)	Dynamic Host Configuration Protocol

付録 A.3　DHCP サーバ機能

表 A-3　DHCP サーバ機能の準拠規格

規格番号 (発行年月)	規格名
RFC2131(1997 年 3 月)	Dynamic Host Configuration Protocol
RFC2132(1997 年 3 月)	DHCP Options and BOOTP Vendor Extensions
RFC2136 (1997 年 4 月)	Dynamic Updates in the Domain Name System (DNS UPDATE)
RFC3679 (2004 年 1 月)	Unused Dynamic Host Configuration Protocol (DHCP) Option Codes

付録 A.4　RIP

表 A-4　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.5　OSPF

表 A-5　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
RFC2370(1998 年 7 月)	The OSPF Opaque LSA Option
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
RFC5309(2008 年 10 月)	Point-to-Point Operation over LAN in Link State Routing Protocols

付録 A.6　BGP4【OP-BGP】

表 A-6　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
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)
RFC5065(2007 年 8 月)	Autonomous System Confederations for BGP
RFC5492(2009 年 2 月)	Capabilities Advertisement with BGP-4
draft-ietf-idr-avoid-transition-04 (2005 年 12 月)	Avoid BGP Best Path Transitions from One External to Another
draft-ietf-idr-restart-13 (2006 年 7 月)	Graceful Restart Mechanism for BGP

付録 A.7　IPv4 マルチキャスト

表 A-7　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)	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) ※ 2	Protocol Independent Multicast-Sparse Mode (PIM-SM) : Protocol Specification (Revised)
draft-ietf-pim-v2-dm-03 (1999 年 6 月)	Protocol Independent Multicast Version 2 Dense Mode Specification
draft-ietf-pim-sm-v2-new-05 (2002 年 3 月) ※ 1	Protocol Independent Multicast-Sparse Mode (PIM-SM) : Protocol Specification (Revised)
draft-ietf-pim-sm-bsr-07 (2006 年 3 月) ※ 2	Bootstrap Router(BSR) Mechanism for PIM

注※ 1　この規格は PIM-SSM 関連部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.8　IPv6・NDP・ICMPv6

表 A-8　IPv6 ネットワークの準拠規格および勧告

規格番号 (発行年月)	規格名
RFC2373(1998 年 7 月)	IP Version 6 Addressing Architecture
RFC2460(1998 年 12 月)	Internet Protocol, Version 6 (IPv6) Specification
RFC2461(1998 年 12 月)	Neighbor Discovery for IP Version 6 (IPv6)
RFC2462(1998 年 12 月)	IPv6 Stateless Address Autoconfiguration
RFC2463(1998 年 12 月)	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
RFC2710(1999 年 10 月)	Multicast Listener Discovery for IPv6
draft-ietf-ipv6-deprecate-rh0-01 (2007 年 6 月)	Deprecation of Type 0 Routing Headers in IPv6

付録 A.9　IPv6 DHCP リレー【OP-DH6R】

表 A-9　IPv6 DHCP リレー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)

付録 A.10　IPv6 DHCP サーバ

表 A-10　IPv6 DHCP サーバ機能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)
RFC3319(2003 年 7 月)	Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers
RFC3633(2003 年 12 月)	IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6
RFC3646(2003 年 12 月)	DNS Configuration Options for DHCPv6
RFC3736(2004 年 4 月)	Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6
RFC4075(2005 年 3 月)	Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6

付録 A.11　RIPng

表 A-11　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.12　OSPFv3

表 A-12　OSPFv3 の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC2740(1999 年 12 月)	OSPF for IPv6
RFC3137(2001 年 6 月)	OSPF Stub Router Advertisement
RFC5309(2008 年 10 月)	Point-to-Point Operation over LAN in Link State Routing Protocols
draft-kompella-ospf-opaquev2-00 (2002 年 10 月)	OSPFv2 Opaque LSAs in OSPFv3
draft-ietf-ospf-ospfv3-graceful-restart-04 (2006 年 5 月)	OSPFv3 Graceful Restart

付録 A.13　BGP4+【OP-BGP】

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
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)

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)
RFC4760(2007 年 1 月)	Multiprotocol Extensions for BGP-4
RFC5065(2007 年 8 月)	Autonomous System Confederations for BGP
RFC5492(2009 年 2 月)	Capabilities Advertisement with BGP-4
draft-ietf-idr-avoid-transition-04 (2005 年 12 月)	Avoid BGP Best Path Transitions from One External to Another
draft-ietf-idr-restart-13 (2006 年 7 月)	Graceful Restart Mechanism for BGP

付録 A.14　IPv6 マルチキャスト

表 A-14　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)	Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification
RFC2710(1999 年 10 月)	Multicast Listener Discovery (MLD) for IPv6
RFC3810(2004 年 6 月)	Multicast Listener Discovery Version 2 (MLDv2) for IPv6
RFC4601(2006 年 8 月) ※ 3	Protocol Independent Multicast-Sparse Mode (PIM-SM) : Protocol Specification (Revised)
draft-ietf-pim-sm-v2-new-03 (2001 年 7 月) ※ 1	Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification (Revised)
draft-ietf-pim-sm-v2-new-05 (2002 年 3 月) ※ 2	Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification (Revised)
draft-ietf-pim-sm-bsr-07 (2006 年 3 月) ※ 3	Bootstrap Router(BSR) Mechanism for PIM

注※ 1　この規格は IPv6 関連部だけ準拠しています。
注※ 2　この規格は PIM-SSM だけ準拠しています。
注※ 3　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。

索引

A

B

D

F

I

L

M

N

O

P

Q

R

T

V

あ

い

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

つ

て

と

に

ね

は

ひ

ふ

ほ

ま

み

ゆ

よ

ら

り

る

ろ