AX8600S・AX8300S 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.2

Ver. 12.9 対応 Rev.1

AX86S-S002-A0

AlaxalA

■ 対象製品

このマニュアルは AX8600S および AX8300S を対象に記載しています。

■ 輸出時の注意

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

■ 商標一覧

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

■ マニュアルはよく読み，保管してください。

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

■ ご注意

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

■ 発行

２０２１年　　６月 （第１１版） ＡＸ８６Ｓ－Ｓ００２－Ａ０

■ 著作権

変更内容

【Ver. 12.9 対応 Rev.1 版】

表　変更内容

章・節・項・タイトル	追加・変更内容
1.2.1　レイヤ 2 スイッチ機能	• アグリゲート VLAN の記述を追加しました。
1.3　レイヤ 2 スイッチ機能と他機能の共存について	• アグリゲート VLAN の記述を追加しました。
4.9　アグリゲート VLAN の解説	• 本節を追加しました。
4.10　アグリゲート VLAN のコンフィグレーション	• 本節を追加しました。
4.11.3　VLAN 拡張機能の MAC アドレス学習の確認	• 本項を追加しました。
14.1.4　重要フロー保護	• 本項を追加しました。
14.2.7　重要フロー保護の設定	• 本項を追加しました。
14.3.7　重要フロー保護による最大帯域監視の確認	• 本項を追加しました。
20.1.2　キュー長変更	• 本項を追加しました。
20.2　コンフィグレーション	• 本節を追加しました。
23　トラッキング機能	• トラッキング連携機能に，ポリシーベースルーティングを追加しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver. 12.9 対応版】

表　変更内容

項目	追加・変更内容
トラッキング機能	• トラッキング連携機能に，イーサネットインタフェース，IP インタフェース，およびスタティックルーティングを追加しました。

【Ver. 12.8 対応 Rev.2 版】

表　変更内容

項目	追加・変更内容
帯域監視のオプション動作	• 本項を追加しました。
帯域制御	•「(3) 帯域制御のオプション動作」を追加しました。
帯域制御のオプション動作の設定	• 本項を追加しました。

【Ver. 12.8 対応版】

表　変更内容

項目	追加・変更内容
広域イーサネット機能	• switch-3e-qinq の記述を追加しました。
キュー数指定	• PSU-C1，PSU-C2，PSU-E1A，および PSU-E2A の記述を追加しました。
装置内キュー	• AX8304S の記述を追加しました。

【Ver. 12.7 対応 Rev.1 版】

表　変更内容

項目	追加・変更内容
MAC アドレス学習抑止	• 本項を追加しました。
MAC アドレス学習抑止の設定	• 本項を追加しました。
解説	•「図 18-1 階層化シェーパの位置づけ」を変更しました。
概要	• シェーパユーザ個別設定についての記述を追加しました。
シェーパユーザ決定	• フロー検出によるシェーパユーザ決定の記述を追加しました。
廃棄制御	• 廃棄優先度数変更の記述を追加しました。
シェーパモード	• 設定例を追加しました。
帯域制御	• 記述を変更しました。
シェーパユーザ設定機能	•「(1) シェーパユーザワンタッチ設定機能」に廃棄優先度および廃棄閾値の記述を追加しました。 •「(2) シェーパユーザ個別設定」を追加しました。
階層化シェーパ使用時の注意事項	•「(2) ユーザ帯域設定についての注意事項」の内容を一部削除しました。 •「(4) MIB および運用コマンドの統計値に関する注意事項」を追加しました。 •「(5) 運用コマンド clear shaper 実行時の MIB の注意事項」を追加しました。
フロー検出によるシェーパユーザ決定の設定	• 本項を追加しました。
シェーパユーザワンタッチ設定機能の設定	• 廃棄優先度数の記述を追加しました。
シェーパユーザ個別設定	• 本項を追加しました。
シェーパモード情報の確認	• 確認内容を一部追加しました。
シェーパユーザ情報の確認	• 確認内容を一部追加しました。
シェーパユーザ数の確認	• 本項を追加しました。
トラッキング機能	• 本章を追加しました。

【Ver. 12.7 対応版】

表　変更内容

項目	追加・変更内容
サポート仕様	• 収容条件および障害監視時間に関する記述を変更しました。
リングポートのデータ転送用 VLAN	• 本項を追加しました。
経路切り戻し抑止および解除時の動作	• 本項を追加しました。
経路切り戻し抑止および解除時の動作	• 本項を追加しました。
Ring Protocol の禁止構成	• 「(5) マスタノードの両リングポートが共有リンクとなる構成」を追加しました。
Ring Protocol 使用時の注意事項	• 「(15) 経路切り戻し抑止機能適用時のリングポートフォワーディング遷移時間の設定について」を追加しました。 • 「(16) ヘルスチェックフレームの送信について」を追加しました。
各種パラメータの設定	• 「(6) 経路切り戻し抑止機能の有効化および抑止時間」を追加しました。
階層化シェーパ	• 本章を追加しました。
装置内キュー	• 階層化シェーパの記述を追加しました。
概要	• 「(3) NIF 種別ごとの装置内キューとフレームの流れ」を追加しました。

【Ver. 12.6 対応 Rev.1 版】

表　変更内容

項目	追加・変更内容
サポート機能	• アイソレート VLAN の記述を追加しました。
レイヤ 2 スイッチ機能と他機能の共存について	• ポリシーベースミラーリングの記述を追加しました。 • アイソレート VLAN の記述を追加しました。
アイソレート VLAN の解説	• 本節を追加しました。
アイソレート VLAN のコンフィグレーション	• 本節を追加しました。
VLAN 拡張機能の確認	• アイソレート VLAN の記述を追加しました。
アクセスリストロギング	• 本章を追加しました。
ポリシーベースミラーリング	• 本章を追加しました。

【Ver. 12.6 対応版】

表　変更内容

項目	追加・変更内容
サポート機能	• QinQ 網向け機能の記述を追加しました。
レイヤ 2 スイッチ機能と他機能の共存について	• QinQ 網向け機能の記述を追加しました。
広域イーサネット機能	• 本章を追加しました。

項目	追加・変更内容
暗黙の廃棄	• 暗黙の廃棄エントリ自動生成抑止の記述を追加しました。
フロー検出使用時の注意事項	• QoS フロー検出時の注意事項を追加しました。
QoS フロー廃棄	• 本章を追加しました。
キュー数指定	• PSU-22 の記述を追加しました。
概要	• PSU-22 の記述を追加しました。 • AX8308S の記述を追加しました。
ストームコントロール	• 本章を追加しました。

【Ver. 12.4 対応 Rev.1 版】

表　変更内容

項目	追加・変更内容
レイヤ 2 スイッチ概説	• VLAN トンネリングの記述を追加しました。 • IGMP/MLD snooping の記述を追加しました。
概要	• トンネリングポートの記述を追加しました。
VLAN トンネリングの解説	• 本節を追加しました。
VLAN トンネリングのコンフィグレーション	• 本節を追加しました。
IGMP/MLD snooping	• 本章を追加しました。
IEEE802.3ah OAM	• 本章を追加しました。

はじめに

■ 対象製品およびソフトウェアバージョン

このマニュアルは AX8600S および AX8300S のソフトウェア Ver. 12.9 の機能について記載しています。ソフトウェア機能のうち，オプションライセンスで提供する機能については次のマークで示します。

【OP-SHPS】

オプションライセンス OP-SHPS についての記述です。

【OP-SHPE】

オプションライセンス OP-SHPE についての記述です。

【OP-BGP】

オプションライセンス OP-BGP についての記述です。

【OP-FLENT】

オプションライセンス OP-FLENT についての記述です。

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

■ このマニュアルの訂正について

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

■ 対象読者

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

また，次に示す知識を理解していることを前提としています。

- ネットワークシステム管理の基礎的な知識

■ このマニュアルの URL

このマニュアルの内容は下記 URL に掲載しております。

https://www.alaxala.com/

■ マニュアルの読書手順

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

●装置の開梱から，初期導入時の基本的な設定を知りたい

AX8600S クイックスタートガイド (AX86S-Q001)	AX8300S クイックスタートガイド (AX83S-Q001)

●ハードウェアの設備条件，取扱方法を調べる

AX8600S ハードウェア取扱説明書 (AX86S-H001)	AX8300S ハードウェア取扱説明書 (AX83S-H001)

●ソフトウェアの機能，コンフィグレーションの設定，運用コマンドを知りたい

▽まず，ガイドで使用する機能や収容条件についてご確認ください。

・収容条件 ・ログインなどの基本操作 ・イーサネット	・フィルタ，QoS ・ネットワークの管理	・IPパケット中継 ・ユニキャストルーティング ・マルチキャストルーティング
コンフィグレーションガイド Vol.1 (AX86S-S001)	コンフィグレーションガイド Vol.2 (AX86S-S002)	コンフィグレーションガイド Vol.3 (AX86S-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 (AX86S-S004)	コンフィグレーション コマンドレファレンス Vol.2 (AX86S-S005)	コンフィグレーション コマンドレファレンス Vol.3 (AX86S-S006)
運用コマンドレファレンス Vol.1 (AX86S-S007)	運用コマンドレファレンス Vol.2 (AX86S-S008)	運用コマンドレファレンス Vol.3 (AX86S-S009)

・システムメッセージとログについて

メッセージ・ログレファレンス (AX86S-S010)

・MIBについて

MIBレファレンス (AX86S-S011)

●トラブル発生時の対処方法について知りたい

トラブルシューティングガイド (AX86S-T001)

■ このマニュアルでの表記

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

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

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

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

■ KB（キロバイト）などの単位表記について

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

目次

第 1 編　レイヤ 2 スイッチング

1 レイヤ 2 スイッチ概説

この章では，本装置の機能のうち，OSI 階層モデルの第 2 レイヤでデータを中継するレイヤ 2 スイッチ機能の概要について説明します。

1.1　概要

本装置では，VLAN を利用した各種のレイヤ 2 スイッチ機能を使用できます。

1.1.1　スイッチポート

VLAN に所属して使用するポートをスイッチポートと呼びます。スイッチポートには，VLAN のポート種別としてアクセスモード，トランクモードまたはトンネリングモードを設定します。アクセスモードを設定したスイッチポートをアクセスポート，トランクモードを設定したスイッチポートをトランクポート，トンネリングモードを設定したスイッチポートをトンネリングポートと呼びます。本装置のデフォルトはアクセスモードです。

なお，VLAN に所属させないでスイッチポートを解除して，各ポートをイーサネットインタフェース，イーサネットサブインタフェース，ポートチャネルインタフェース，またはポートチャネルサブインタフェースとして，レイヤ 3 機能を使用できます。

1.1.2　MAC アドレス学習

レイヤ 2 スイッチ機能は，フレームを受信すると送信元 MAC アドレスを MAC アドレステーブルに登録します。MAC アドレステーブルの各エントリには，MAC アドレスとフレームを受信したポートおよびエージングタイマを記録します。フレームを受信するたびに，送信元 MAC アドレスに対応するエントリを更新します。

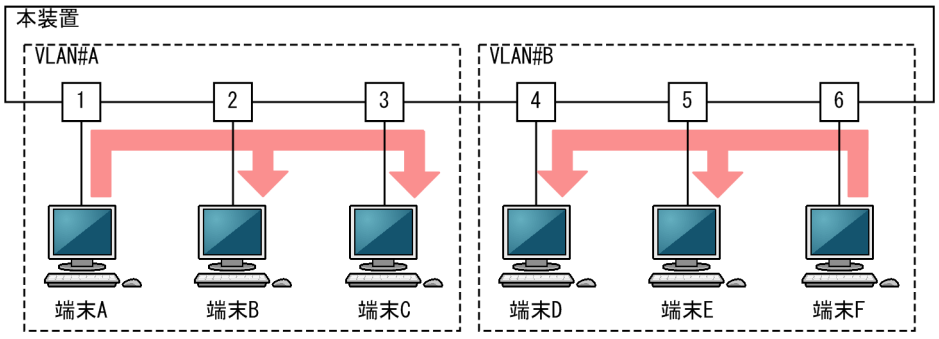
レイヤ 2 スイッチ機能は，MAC アドレステーブルのエントリに従ってフレームを中継します。フレームの宛先 MAC アドレスに一致するエントリがあると，そのエントリのポートに中継します（エントリのポートが受信したポートである場合は中継しません）。一致するエントリがない場合，受信したポート以外のすべてのポートにフレームを中継します。この中継をフラッディングと呼びます。

MAC アドレス学習では VLAN ごとに送信元 MAC アドレスを登録しますが，ハードウェアプロファイルの設定によって VLAN Tag が 2 段の場合，S-Tag と C-Tag の両方の VLAN Tag の値に基づいて MAC アドレス学習ができます。

1.1.3　VLAN

VLAN は，スイッチ内を仮想的なグループに分ける機能のことです。スイッチ内を複数の VLAN にグループ分けすることによってブロードキャストドメインを分割します。これによって，ブロードキャストフレームの抑制や，セキュリティの強化を図れます。VLAN の概要を次の図に示します。

図 1-1　VLAN の概要



この図では，VLAN#A と VLAN#B に分割したことで，VLAN#A の端末 A からのブロードキャストパケットは端末 B および C には中継されますが，VLAN#B の端末 D，E，および F には中継されません。このように，VLAN#A と VLAN#B の間ではブロードキャストドメインが分割されるため，互いのフレームが届くことはありません。

1.2　サポート機能

1.2.1　レイヤ 2 スイッチ機能

レイヤ 2 スイッチ機能として，本装置がサポートする機能を次の表に示します。

表 1-1　レイヤ 2 スイッチサポート機能

サポート機能		機能概要
MAC アドレス学習		MAC アドレステーブルに登録する MAC アドレスの学習機能
VLAN	ポート VLAN	ポート単位にスイッチ内を仮想的なグループに分ける機能
	ネイティブ VLAN	トランクポートで Untagged フレームを扱うポート VLAN の呼称
	トンネリング	複数ユーザの VLAN をほかの VLAN に集約してトンネルする機能
	Tag 変換	VLAN Tag を変換して別の VLAN に中継する機能
	アイソレート VLAN	VLAN 内で，ポート間でのレイヤ 2 中継を遮断する機能
	VLAN ごと MAC アドレス	IP インタフェースの MAC アドレスを VLAN ごとに異なるアドレスにする機能
	アグリゲート VLAN	グループ化した VLAN 間でレイヤ 2 中継をする機能
スパニングツリー	PVST+	VLAN 単位のスイッチ間のループ防止機能
	シングルスパニングツリー	装置単位のスイッチ間のループ防止機能
	マルチプルスパニングツリー	MST インスタンス単位のスイッチ間のループ防止機能
Ring Protocol		リングトポロジでのレイヤ 2 ネットワークの冗長化機能
IGMP/MLD snooping		VLAN 内のマルチキャストトラフィックを制御する機能
QinQ 網向け機能		2 段の VLAN Tag での MAC アドレス学習機能
		MAC アドレス学習の移動監視機能
		BPDU の透過機能

1.2.2　装置 MAC アドレスを使用する機能

本装置は，装置を識別するための MAC アドレスを一つ持ちます。この MAC アドレスのことを装置 MAC アドレスと呼びます。装置 MAC アドレスは，レイヤ 2 の各機能の装置識別子として使用します。

装置 MAC アドレスを使用する機能を次の表に示します。

表 1-2　装置 MAC アドレスを使用する機能

機能	用途
リンクアグリゲーションの LACP	装置識別子
スパニングツリー	装置識別子

機能	用途
Ring Protocol	装置識別子
L2 ループ検知	装置識別子
IEEE802.3ah OAM	装置識別子
LLDP	装置識別子

1.3　レイヤ 2 スイッチ機能と他機能の共存について

レイヤ 2 スイッチ機能と併用する際，共存できないまたは制限のある機能があります。機能間の共存についての制限事項を次に示します。

なお，これらの表では各機能間の共存関係で，制限のある項目だけを示しています。

表 1-3　VLAN での制限事項

使用したい機能		制限のある機能	制限の内容
VLAN 種別	ポート VLAN	ポートミラーリング（ミラーポート）	ポートミラーリング（ミラーポート）を設定したポートでは，ポート VLAN と共存できません。
		ポリシーベースミラーリング（ミラーポート）	ポリシーベースミラーリング（ミラーポート）を設定したポートでは，ポート VLAN と共存できません。
VLAN 拡張機能	VLAN トンネリング	PVST+	PVST+が動作しているポートでは，トンネリングポートと共存できません。
		シングルスパニングツリー	シングルスパニングツリーが動作しているポートでは，トンネリングポートと共存できません。
		マルチプルスパニングツリー	マルチプルスパニングツリーが動作しているポートでは，トンネリングポートと共存できません。
	Tag 変換	PVST+	PVST+が動作している VLAN では，Tag 変換と共存できません。
	アイソレート VLAN	PVST+	スパニングツリーを使用しているポートにアイソレートポートを設定すると，トポロジによっては通信不可となることがあります。
		シングルスパニングツリー	
		マルチプルスパニングツリー	
		Ring Protocol	Ring Protocol を使用しているポートにアイソレートポートを設定すると，トポロジによっては通信不可となることがあります。
		IGMP/MLD snooping	IGMP/MLD snooping を設定した VLAN では，アイソレート VLAN と共存できません。
	アグリゲート VLAN	VLAN インタフェースのレイヤ 3 機能	アグリゲート VLAN を適用した VLAN では，VLAN インタフェースに IPv4 アドレスおよび IPv6 アドレスを設定して IP インタフェースにできません。
		アイソレート VLAN	アイソレート VLAN を有効にした VLAN では，アグリゲート VLAN と共存できません。

使用したい機能		制限のある機能	制限の内容
		Ring Protocol	Ring Protocol の制御 VLAN に使用している VLAN は，アグリゲート VLAN と共存できません。
		IGMP/MLD snooping	IGMP/MLD snooping を設定した VLAN では，アグリゲート VLAN と共存できません。
		QinQ 網向け機能	アグリゲート VLAN を設定した場合，QinQ 網向け機能と共存できません。

表 1-4　スパニングツリーでの制限事項

使用したい機能	制限のある機能	制限の内容
PVST+	VLAN トンネリング	VLAN トンネリングを設定したポートでは，PVST+と共存できません。
	Tag 変換	Tag 変換を設定した VLAN では，PVST+と共存できません。
	アイソレート VLAN	アイソレートポートを設定しているポートに PVST+を設定すると，トポロジによっては通信不可となることがあります。
	マルチプルスパニングツリー	一つの装置でマルチプルスパニングツリーと PVST+は共存できません。
	Ring Protocol	一つの装置で Ring Protocol と PVST+は共存できません。
	QinQ 網向け機能	一つの装置で QinQ 網向け機能と PVST+は共存できません。
シングルスパニングツリー	VLAN トンネリング	VLAN トンネリングを設定したポートでは，シングルスパニングツリーと共存できません。
	アイソレート VLAN	アイソレートポートを設定しているポートにシングルスパニングツリーを設定すると，トポロジによっては通信不可となることがあります。
	マルチプルスパニングツリー	一つの装置でマルチプルスパニングツリーとシングルスパニングツリーは共存できません。
	Ring Protocol	一つの装置で Ring Protocol とシングルスパニングツリーは共存できません。
	QinQ 網向け機能	一つの装置で QinQ 網向け機能とシングルスパニングツリーは共存できません。
マルチプルスパニングツリー	VLAN トンネリング	VLAN トンネリングを設定したポートでは，マルチプルスパニングツリーと共存できません。

使用したい機能	制限のある機能	制限の内容
	アイソレート VLAN	アイソレートポートを設定しているポートにマルチプルスパニングツリーを設定すると，トポロジによっては通信不可となることがあります。
	PVST+	一つの装置で PVST+とマルチプルスパニングツリーは共存できません。
	シングルスパニングツリー	一つの装置でシングルスパニングツリーとマルチプルスパニングツリーは共存できません。
	Ring Protocol	一つの装置で Ring Protocol とマルチプルスパニングツリーは共存できません。
	QinQ 網向け機能	一つの装置で QinQ 網向け機能とマルチプルスパニングツリーは共存できません。

表 1-5　Ring Protocol での制限事項

使用したい機能	制限のある機能	制限の内容
Ring Protocol	アイソレート VLAN	アイソレートポートを設定しているポートに Ring Protocol を設定すると，トポロジによっては通信不可となることがあります。
	アグリゲート VLAN	アグリゲート VLAN を設定している VLAN は，Ring Protocol の制御 VLAN と共存できません。
	PVST+	一つの装置でスパニングツリーと Ring Protocol は共存できません。
	シングルスパニングツリー	
	マルチプルスパニングツリー	

表 1-6　IGMP/MLD snooping での制限事項

使用したい機能	制限のある機能	制限の内容
IGMP/MLD snooping	VLAN トンネリング	一つの装置で VLAN トンネリングと IGMP/MLD snooping は共存できません。
	アイソレート VLAN	アイソレート VLAN を有効にした VLAN では，IGMP/MLD snooping と共存できません。
	アグリゲート VLAN	アグリゲート VLAN を設定した VLAN では，IGMP/MLD snooping と共存できません。
	QinQ 網向け機能	一つの装置で QinQ 網向け機能と IGMP/MLD snooping は共存できません。

表 1-7　QinQ 網向け機能での制限事項

使用したい機能	制限のある機能	制限の内容
QinQ 網向け機能	VLAN インタフェースのレイヤ 3 機能	QinQ 網向け機能適用時は，VLAN インタフェースに IPv4 アドレスおよび IPv6 アドレスを設定して IP インタフェースにできません。
	アグリゲート VLAN	QinQ 網向け機能適用時は，アグリゲート VLAN と共存できません。
	PVST+	QinQ 網向け機能適用時は，スパニングツリーと共存できません。
	シングルスパニングツリー	
	マルチプルスパニングツリー	
	IGMP/MLD snooping	QinQ 網向け機能適用時は，IGMP/MLD snooping と共存できません。

1.4　スイッチポートで制限のある機能

本装置でサポートする機能のうち，スイッチポートで制限のある機能とその制限事項を次の表に示します。

表 1-8　スイッチポートで制限のある機能と制限事項

機能	制限事項
LLDP	IEEE802.1AB/D6.0（Draft6.0 LLDP）でサポートする TLV のうち，Organizationally Specific TLVs は送信しません。

1.5　VLAN 未所属ポートの機能について

スイッチポートを解除した VLAN 未所属ポートでは，レイヤ 2 スイッチ機能として本装置がサポートしている機能（「表 1-1　レイヤ 2 スイッチサポート機能」を参照）を使用できません。各ポートをイーサネットインタフェースもしくはイーサネットサブインタフェースとして，または各チャネルグループをポートチャネルインタフェースもしくはポートチャネルサブインタフェースとして，IP インタフェースなどに使用します。

VLAN 未所属ポートには，さまざまなイーサネットの設定ができます。また，IP インタフェースに対して，各機能を設定できます。そのほか，ポートに設定する機能のうち，いくつかの機能を使用できます。VLAN 未所属ポートでサポートする機能を次に示します。

- リンクアグリゲーション
- フィルタ
- QoS
- ポートミラーリング
- sFlow 統計
- LLDP

2 MAC アドレス学習

この章では，MAC アドレス学習機能の解説と操作方法について説明します。

2.1　解説

本装置は，フレームを宛先 MAC アドレスによって目的のポートへ中継するレイヤ 2 スイッチングをします。宛先 MAC アドレスによって特定のポートだけに中継することで, ユニキャストフレームのフラッディングによるむだなトラフィックを抑止します。

MAC アドレス学習では，チャネルグループを一つのポートとして扱います。

2.1.1　送信元 MAC アドレス学習

すべての受信フレームを MAC アドレス学習の対象として，送信元 MAC アドレスを学習して MAC アドレステーブルに登録します。登録した MAC アドレスはエージングタイムアウトまで保持します。VLAN 単位に学習して，MAC アドレステーブルは MAC アドレスと VLAN をペアにして管理します。異なる VLAN であれば，同一の MAC アドレスでも学習できます。

2.1.2　MAC アドレス学習の移動検出

学習済みの送信元 MAC アドレスを持つフレームを学習時と異なるポートから受信した場合，その MAC アドレスが移動したものと見なして MAC アドレステーブルのエントリを再登録(移動先ポートに関する上書き）します。

チャネルグループで学習した MAC アドレスについては, そのチャネルグループに含まれないポートからフレームを受信した場合に MAC アドレスが移動したものと見なします。

2.1.3　学習 MAC アドレスのエージング

学習したエントリは, エージングタイム内に同じ送信元 MAC アドレスからフレームを受信しなかった場合にエントリを削除します。これによって，不要なエントリの蓄積を防止します。エージングタイム内にフレームを受信した場合は, エージングタイマを更新してエントリを保持します。エージングタイムを設定できる範囲を次に示します。

- エージングタイムの範囲：0，10～1000000（秒）
  0 は無限を意味します（エージングしません)。
- デフォルト値：300（秒）

ポートがリンクダウンした場合は, 該当ポートから学習したエントリをすべて削除します。チャネルグループで学習したエントリは，そのチャネルグループが Down した場合に削除します。

2.1.4　MAC アドレスによるレイヤ 2 スイッチング

MAC アドレス学習の結果に基づいてレイヤ 2 スイッチングをします。宛先 MAC アドレスに対応するエントリを保持している場合，学習したポートだけに中継します。レイヤ 2 スイッチングの動作仕様を次の表に示します。

表 2-1　レイヤ 2 スイッチングの動作仕様

宛先 MAC アドレスの種類	動作概要
学習済みのユニキャスト	学習したポートへ中継します。
未学習のユニキャスト	受信した VLAN に所属する全ポートへ中継します。

宛先 MAC アドレスの種類	動作概要
ブロードキャスト	受信した VLAN に所属する全ポートへ中継します。
マルチキャスト	受信した VLAN に所属する全ポートへ中継します。

2.1.5　MAC アドレス学習抑止

受信フレームによる MAC アドレス学習に制限を設けて，使用する MAC アドレステーブルのエントリを管理できます。

(1)　VLAN 単位の MAC アドレス学習抑止

VLAN ごとに，MAC アドレス学習を抑止できます。MAC アドレス学習を抑止すると，学習抑止の対象となる VLAN で受信したフレームはフラッディングします。

すでに MAC アドレスを学習しているときに MAC アドレス学習を抑止すると，学習していた MAC アドレステーブルのエントリは削除します。

2.1.6　MAC アドレステーブルのクリア

本装置はコマンドの実行やプロトコルの動作などによって MAC アドレステーブルをクリアします。
MAC アドレステーブルをクリアする契機を次の表に示します。

表 2–2　MAC アドレステーブルをクリアする契機

契機	説明
ポートのリンクダウン※1	該当ポートから学習したエントリを削除します。
チャネルグループの Down※2	該当チャネルグループから学習したエントリを削除します。
運用コマンド clear mac-address-table の実行	パラメータに従って MAC アドレステーブルをクリアします。
MAC アドレステーブル Clear 用 MIB （プライベート MIB）	セット時に MAC アドレステーブルをクリアします。
VLAN のコンフィグレーションの削除および変更	コンフィグレーションコマンド switchport access および switchport trunk で VLAN ポートを削除した場合や，コンフィグレーションコマンド switchport mode でポート種別を変更した場合に，該当ポートの該当 VLAN の MAC アドレステーブルをクリアします。
	コンフィグレーションコマンド shutdown で VLAN をシャットダウン状態にした場合に，該当 VLAN の MAC アドレステーブルをクリアします。
	コンフィグレーションコマンド isolate-vlan でアイソレート VLAN を有効または無効にした場合に，該当 VLAN の MAC アドレステーブルをクリアします。
	コンフィグレーションコマンド switchport isolate でアイソレートポートを設定または削除した場合に，該当ポートの該当 VLAN の MAC アドレステーブルをクリアします。
スパニングツリーのトポロジ変更	トポロジ変更を検出した時に MAC アドレステーブルをクリアします。

契機	説明
Ring Protocol による経路の切り替え	[本装置がマスタノードとして動作] 経路切り替え時に MAC アドレステーブルをクリアします。
	[本装置がトランジットノードとして動作] 経路切り替え時にマスタノードから送信されるフラッシュ制御フレームを受信した場合，MAC アドレステーブルをクリアします。 リングポートフォワーディング遷移時間のタイムアウト時に MAC アドレステーブルをクリアします。
MAC アドレス学習抑止のコンフィグレーションの設定	コンフィグレーションコマンド no mac-address-table learning で MAC アドレス学習抑止を設定した場合，該当 VLAN の MAC アドレステーブルをクリアします。

注※1

回線障害，運用コマンド inactivate の実行，コンフィグレーションコマンド shutdown の設定などによるポートのリンクダウンです。

注※2

LACP，回線障害，コンフィグレーションコマンド shutdown の設定などによるチャネルグループの Down です。

2.2　コンフィグレーション

2.2.1　コンフィグレーションコマンド一覧

MAC アドレス学習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 2-3　コンフィグレーションコマンド一覧

コマンド名	説明
mac-address-table aging-time	MAC アドレス学習のエージングタイムを設定します。
mac-address-table learning	MAC アドレス学習可否を設定します。

2.2.2　エージングタイムの設定

[設定のポイント]

MAC アドレス学習のエージングタイムを変更できます。設定は装置単位および VLAN 単位です。設定しない場合，エージングタイムは 300 秒で動作します。装置単位と VLAN 単位の設定では，VLAN 単位の設定が優先されます。

[コマンドによる設定]

1. **(config)# mac-address-table aging-time 100**
   エージングタイムを 100 秒に設定します。
2. **(config)# mac-address-table aging-time 600 vlan 200**
   VLAN200 のエージングタイムを 600 秒に設定します。

2.2.3　MAC アドレス学習抑止の設定

[設定のポイント]

MAC アドレス学習を行う場合はコンフィグレーションの設定は不要です。MAC アドレス学習をしない VLAN に対してだけ，MAC アドレス学習抑止を設定します。

[コマンドによる設定]

1. **(config)# no mac-address-table learning vlan 100**
   VLAN100 では MAC アドレス学習を抑止します。

2.3　オペレーション

2.3.1　運用コマンド一覧

MAC アドレス学習の運用コマンド一覧を次の表に示します。

表 2-4　運用コマンド一覧

コマンド名	説明
show mac-address-table	MAC アドレステーブルの情報を表示します。 learning-counter パラメータを指定すると，MAC アドレス学習の学習アドレス数をポート単位に表示します。 learning-counter vlan パラメータを指定すると，MAC アドレス学習の学習アドレス数を VLAN 単位に表示します。
clear mac-address-table	MAC アドレステーブルをクリアします。
show vlan※	VLAN の MAC アドレス学習状態を表示します。

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

2.3.2　MAC アドレス学習の状態の確認

MAC アドレス学習の情報は show mac-address-table コマンドで表示します。MAC アドレステーブルに登録されている MAC アドレスとその MAC アドレスを宛先とするフレームの中継先を確認してください。このコマンドで表示されない MAC アドレスを宛先とするフレームは VLAN 全体にフラッディングされます。

show mac-address-table コマンドでは，MAC アドレス学習によって登録したエントリを表示します。

図 2-1　show mac-address-table コマンドの実行結果

```
> show mac-address-table
Date 20XX/01/11 11:16:46 UTC
MAC address        VLAN C-Tag VLAN-G    Aging-Time Type     Port-list
0012.e200.1111        2     -      -           100 Dynamic  1/5
0012.e244.f073      100     -      -           230 Dynamic  1/10-11
0012.e244.f072      100     -      -         10000 Dynamic  1/10-11
0012.e244.f070      100     -      -            10 Dynamic  1/12
0100.5e01.0102      200     -      -             - Snoop    3/1
0012.e2c0.072a     4030     -   2048           299 Dynamic  2/2,4/2
0012.e2c0.087a     4054     -   2048           299 Dynamic  2/2,4/2
0012.e2c0.073a     4031     -   2048           299 Dynamic  2/2,4/2
>
```

2.3.3　MAC アドレス学習数の確認

show mac-address-table コマンドで learning-counter パラメータを指定すると，MAC アドレス学習によって登録したダイナミックエントリの数をポート単位に表示します。このコマンドで，ポートごとの接続端末数の状態を確認できます。

show mac-address-table コマンドで learning-counter vlan パラメータを指定すると，ダイナミックエントリの数を VLAN 単位に表示できます。

なお，リンクアグリゲーションを使用している場合，同じチャネルグループのポートはすべて同じ値を表示します。表示する値はチャネルグループ上で学習したアドレス数です。

図 2–2　show mac-address-table コマンド（learning-counter パラメータ指定）の実行結果

```
> show mac-address-table learning-counter port 1/1-10
Date 20XX/01/11 20:00:57 UTC
Port counts:10
Port       Count
1/1            3
1/2         1000
1/3            0
1/4           50
1/5           45
1/6            0
1/7           22
1/8            0
1/9            0
1/10           0
```

図 2–3　show mac-address-table コマンド（learning-counter vlan パラメータ指定）の実行結果

```
> show mac-address-table learning-counter vlan
Date 20XX/01/11 20:00:57 UTC
VLAN counts:4
ID         Count
   2           3
 100        1000
 200           0
4095          90
```

3 VLAN

VLAN はスイッチ内を仮想的なグループに分ける機能です。この章では，VLAN の解説と操作方法について説明します。

3.1 解説

3.1.1 概要

この項では，VLAN の概要を説明します。

(1) VLAN の種類

本装置がサポートする VLAN の種類を次の表に示します。

表 3-1 サポートする VLAN の種類

項目	概要
ポート VLAN	ポートおよびチャネルグループで VLAN のグループを分けます。

装置の初回起動時，各ポートは VLAN に所属しません。そのため，必要に応じて VLAN のコンフィグレーションを設定してください。

(2) ポート種別

使用する VLAN の種類に応じて各ポートの種別を設定する必要があります。ポート種別を次の表に示します。

表 3-2 ポート種別

ポート種別	概要	使用する VLAN
アクセスポート	ポート VLAN で Untagged フレームを扱います。 このポートでは，すべての Untagged フレームを一つのポート VLAN で扱います。	ポート VLAN
トランクポート	すべての種類の VLAN で Tagged フレームを扱います。 このポートでは，VLAN Tag によって VLAN を決定します。	すべての種類の VLAN
トンネリングポート	VLAN トンネリングのポート VLAN で，Untagged と Tagged を区別しないでフレームを扱います。このポートでは，すべてのフレームを一つのポート VLAN で扱います。	ポート VLAN

アクセスポートは Untagged フレームを扱うポートです。このポートでは Tagged フレームを扱えません。Tagged フレームを受信したときは廃棄して，また送信もしません。

Tagged フレームはトランクポートでだけ扱えます。トランクポートの Untagged フレームはネイティブ VLAN が扱います。

トンネリングポートは，VLAN トンネリングをするポートです。このポートでは Untagged フレームと Tagged フレームを区別しません。

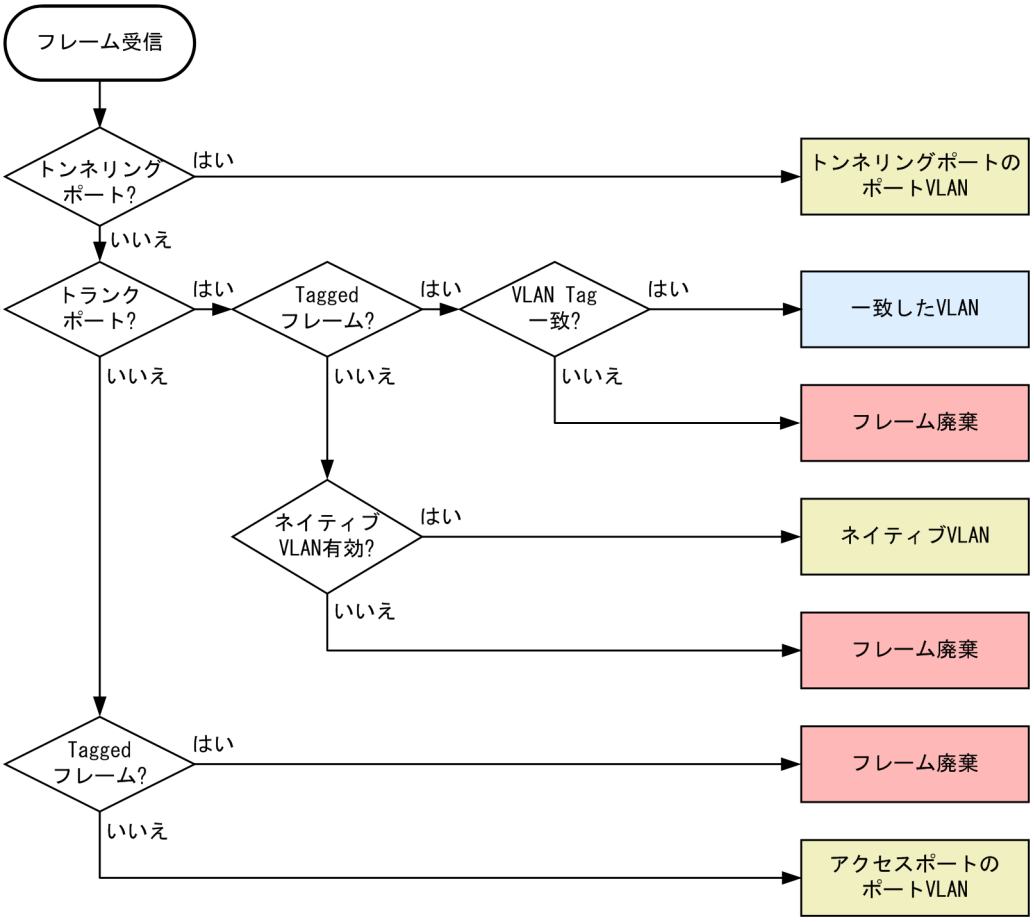
(3) ポートのネイティブ VLAN

トランクポートで Untagged フレームを受信する場合，ポートごとに作成済みのポート VLAN を一つネイティブ VLAN に設定します。この VLAN を，ポートのネイティブ VLAN と呼びます。

(4)　VLAN 判定のアルゴリズム

フレームを受信したとき，受信したフレームの VLAN を判定します。VLAN 判定のアルゴリズムを次の図に示します。

図 3-1　VLAN 判定のアルゴリズム

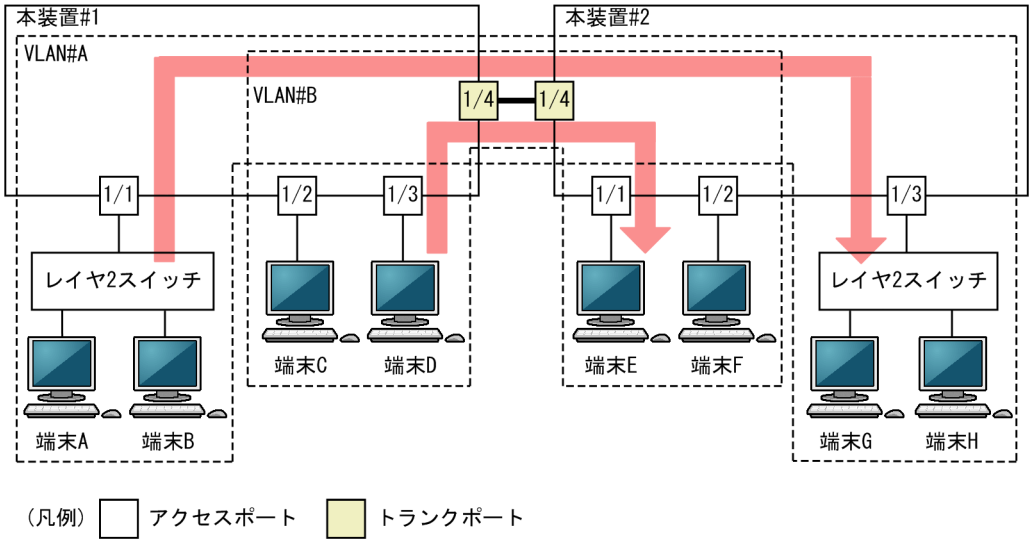


3.1.2　アクセスポートとトランクポート

ポート VLAN は一つのポートに一つの VLAN を割り当てます。ポート VLAN として使用するポートは，アクセスポートとして設定します。複数のポート VLAN をほかの LAN スイッチなどに接続するためにはトランクポートを使用します。トランクポートは VLAN Tag によって VLAN を識別するため，一つのポートに複数の VLAN を設定できます。

ポート VLAN の構成例を次の図に示します。ポート 1/1～1/3 はアクセスポートとしてポート VLAN を設定します。2 台の本装置の間はトランクポート（ポート 1/4）で接続します。トランクポートには複数の VLAN を設定します。トランクポートでは VLAN Tag を付けて中継することで，VLAN を識別します。

図 3-2　ポート VLAN の構成例



3.1.3　ネイティブ VLAN

トランクポートには，Untagged フレームを扱うネイティブ VLAN があります。例えば，「図 3-2　ポート VLAN の構成例」のトランクポートで VLAN#B をネイティブ VLAN に設定すると，VLAN#B はトランクポートでも Untagged フレームで中継します。

3.1.4　VLAN 使用時の注意事項

(1)　他機能との共存

「1.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

(2)　アクセスポートでの Tagged フレームに関する注意事項

アクセスポートは Untagged フレームを扱うポートです。Tagged フレームを受信した場合は廃棄します。ただし，VLAN Tag 値が 0 のフレームを受信した場合は，Untagged フレームと同じ扱いになります。

なお，アクセスポートは Tagged フレームおよび VLAN Tag 値が 0 のフレームを送信しません。

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

VLAN 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 3-3 コンフィグレーションコマンド一覧

コマンド名	説明
description	VLAN の補足説明を設定します。
interface vlan	VLAN を作成して，インタフェースを設定します。
shutdown	VLAN をシャットダウン状態に設定します。
switchport access	アクセスポートの VLAN を設定します。
switchport mode	VLAN でのポート種別（アクセスポートまたはトランクポート）を設定します。
switchport trunk	トランクポートの VLAN を設定します。
system vlan-statistics-mode	インタフェース統計モードを設定します。
vlan	VLAN を作成します。

3.2.2 VLAN の設定

[設定のポイント]

VLAN を作成します。新規に VLAN を作成するためには，VLAN ID を指定します。VLAN ID リストによって複数の VLAN を一括して設定することもできます。

interface vlan コマンドで VLAN ID を指定します。VLAN を作成して，VLAN インタフェースのコンフィグレーションモードに移行します。作成済みの VLAN を指定した場合は，モードだけ移行します。VLAN インタフェースのコンフィグレーションモードでは，VLAN のパラメータを設定できます。

[コマンドによる設定]

1. **(config)# interface vlan 10**

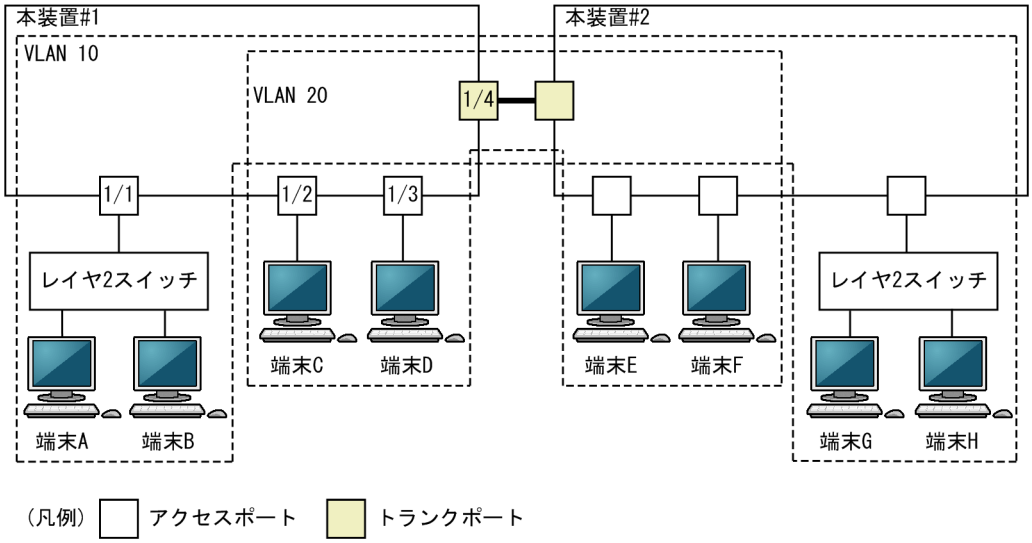
   VLAN ID 10 を指定します。VLAN 10 を作成して，VLAN インタフェース 10 のコンフィグレーションモードに移行します。

3.2.3 ポート VLAN の設定

ポート VLAN を設定する手順を次に示します。ここでは，次の図に示す本装置#1 の設定例を示します。

ポート 1/1 はポート VLAN 10 を設定します。ポート 1/2，1/3 はポート VLAN 20 を設定します。ポート 1/4 はトランクポートであり，すべての VLAN を設定します。

図 3-3 ポート VLAN の設定例



(1) ポート VLAN の作成

[設定のポイント]

ポート VLAN を作成します。

[コマンドによる設定]

1. **(config)# interface range vlan 10, vlan 20**

   VLAN 10，20 をポート VLAN として作成します。本コマンドで VLAN インタフェース 10，20 のコンフィグレーションモードに移行します。

(2) アクセスポートの設定

一つのポートに一つの VLAN を設定して Untagged フレームを扱う場合，アクセスポートとして設定します。

[設定のポイント]

ポートをアクセスポートに設定して，そのアクセスポートで扱う VLAN を設定します。

[コマンドによる設定]

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

   ポート 1/1 のコンフィグレーションモードに移行します。

2. **(config-if)# switchport mode access**
   (config-if)# switchport access vlan 10
   (config-if)# exit

   ポート 1/1 をアクセスポートに設定します。また，VLAN 10 を設定します。

3. **(config)# interface range gigabitethernet 1/2-3**

   ポート 1/2, 1/3 のコンフィグレーションモードに移行します。ポート 1/2, 1/3 は同じコンフィグレーションとなるため，一括して設定します。

4. **(config-if-range)# switchport mode access**
   (config-if-range)# switchport access vlan 20

ポート 1/2，1/3 をアクセスポートに設定します。また，VLAN 20 を設定します。

(3) トランクポートの設定

[設定のポイント]

Tagged フレームを扱うポートはトランクポートとして設定して，そのトランクポートに VLAN を設定します。トランクポートは，switchport mode コマンドを設定しただけではどの VLAN にも所属していません。このポートで扱う VLAN は，switchport trunk コマンドの allowed vlan パラメータで設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/4**
   ポート 1/4 のコンフィグレーションモードに移行します。
2. **(config-if)# switchport mode trunk**
   (config-if)# switchport trunk allowed vlan 10,20
   ポート 1/4 をトランクポートに設定します。また，VLAN 10，20 を設定します。

3.2.4 トランクポートの VLAN 追加と削除

[設定のポイント]

トランクポートへの VLAN の追加と削除は，switchport trunk コマンドの allowed vlan add パラメータおよび allowed vlan remove パラメータで設定します。

すでに switchport trunk allowed vlan コマンドを設定した状態でもう一度 switchport trunk allowed vlan コマンドを実行すると，add 指定した場合と同じように，元の設定から追加した内容が VLAN ID リストに追加されます。

[コマンドによる設定]

1. **(config)# interface range vlan 10-20,100**
   (config-if-range)# exit
   VLAN 10～20，100 を作成します。
2. **(config)# interface gigabitethernet 1/1**
   (config-if)# switchport mode trunk
   ポート 1/1 のコンフィグレーションモードに移行します。また，トランクポートとして設定します。
3. **(config-if)# switchport trunk allowed vlan 10-20**
   ポート 1/1 に VLAN 10～20 を設定します。ポート 1/1 は VLAN 10～20 の Tagged フレームを扱います。
4. **(config-if)# switchport trunk allowed vlan add 100**
   ポート 1/1 で扱う VLAN に VLAN 100 を追加します。
5. **(config-if)# switchport trunk allowed vlan remove 15,16**
   ポート 1/1 で扱う VLAN から VLAN 15 および VLAN 16 を削除します。この状態で，ポート 1/1 は VLAN 10～14，17～20，100 の Tagged フレームを扱います。

3.2.5 トランクポートのネイティブ VLAN の設定

[設定のポイント]

トランクポートで Untagged フレームを扱う場合，ネイティブ VLAN を設定します。ネイティブ VLAN にはポート VLAN だけを設定できます。

ネイティブ VLAN の VLAN ID を switchport trunk コマンドの allowed vlan パラメータで指定すると，トランクポートで Untagged フレームを扱う VLAN となります。

[コマンドによる設定]

1. **(config)# interface range vlan 10,20**
   (config-if-range)# exit
   VLAN 10，20 をポート VLAN として作成します。
2. **(config)# interface gigabitethernet 1/1**
   (config-if)# switchport mode trunk
   ポート 1/1 のコンフィグレーションモードに移行します。また，トランクポートとして設定します。
3. **(config-if)# switchport trunk native vlan 10**
   (config-if)# switchport trunk allowed vlan 10,20
   ポート 1/1（トランクポート）のネイティブ VLAN を VLAN 10 に設定します。また，VLAN 10，20 を設定します。ネイティブ VLAN である VLAN 10 が Untagged フレームを扱い，VLAN 20 は Tagged フレームを扱います。

3.3 オペレーション

3.3.1 運用コマンド一覧

VLAN の運用コマンド一覧を次の表に示します。

表 3-4 運用コマンド一覧

コマンド名	説明
show vlan	VLAN の各種情報を表示します。

3.3.2 VLAN の状態の確認

(1) VLAN の設定状態の確認

show vlan コマンドで VLAN の情報を確認できます。なお,「Untagged」はその VLAN で Untagged フレームを扱うポート,「Tagged」はその VLAN で Tagged フレームを扱うポートです。VLAN に設定されているポートの設定が正しいことを確認してください。

図 3-4 show vlan コマンドの実行結果

```
> show vlan 3,5
Date 20XX/05/23 17:01:40 UTC
VLAN counts:2
VLAN ID:3     Status:Up
  Name:VLAN0003
  Learning:On
  Isolate VLAN:
  Aggregate VLAN group:
  Spanning Tree:
  AXRP RING ID:1     AXRP VLAN group:2
  AXRP RING ID:100   AXRP VLAN group:1
  AXRP RING ID:500   AXRP VLAN group:2
  AXRP RING ID:1000  AXRP VLAN group:2
  IGMP snooping:     MLD snooping:
  Untagged(6)   :1/5-10
  Tagged(2)     :1/11-12
VLAN ID:5     Status:Up
  Name:VLAN0005
  Learning:On
  Isolate VLAN:
  Spanning Tree:
  AXRP RING ID:100   AXRP VLAN group:Control-VLAN
  IGMP snooping:     MLD snooping:
  Tagged(2)     :1/11-12
>
```

(2) VLAN の通信状態の確認

show vlan コマンドで detail パラメータを指定すると，VLAN の通信状態を確認できます。Port Information でポートの Up または Down, Forwarding または Blocking を確認してください。Blocking 状態の場合，括弧内に Blocking の要因が表示されます。

図 3-5 show vlan コマンド（detail パラメータ指定）の実行結果

```
> show vlan 3 detail
Date 20XX/05/23 17:01:40 UTC
VLAN counts:1
VLAN ID:3     Status:Up
  Name:VLAN0003
  Learning:On
  Isolate VLAN:
```

```
  Aggregate VLAN group:
  Spanning Tree:Single(802.1D)
  AXRP RING ID:      AXRP VLAN group:
  IGMP snooping:     MLD snooping:
  Port Information
   1/5          Up   Forwarding      Untagged
   1/6          Up   Blocking(STP)   Untagged
   1/7          Up   Forwarding      Untagged
   1/8          Up   Forwarding      Untagged
   1/9          Up   Forwarding      Untagged
   1/10         Up   Forwarding      Untagged
   1/11(CH:9)   Up   Forwarding      Tagged   Tag-Translation:103
   1/12(CH:9)   Up   Blocking(CH)    Tagged   Tag-Translation:103
>
```

(3) VLAN ID 一覧の確認

show vlan コマンドで summary パラメータを指定すると，設定した VLAN ポート数，VLAN 数，および VLAN ID を確認できます。

図 3-6 show vlan コマンド（summary パラメータ指定）の実行結果

```
> show vlan summary
Date 20XX/05/23 14:15:00 UTC
Number of VLAN ports:1000
Configured VLANs(10)  :2-5,8,10,12,14,16,18
>
```

(4) VLAN のリスト表示による確認

show vlan コマンドで list パラメータを指定すると，VLAN の設定状態の概要を 1 行に表示します。本コマンドで，VLAN の設定状態やレイヤ 2 冗長機能を一覧で確認できます。また，VLAN，ポートまたはチャネルグループをパラメータとして指定すると，指定したパラメータの VLAN の状態だけを一覧で確認できます。

図 3-7 show vlan コマンド（list パラメータ指定）の実行結果

```
> show vlan list
Date 20XX/05/23 17:01:40 UTC
VLAN counts:2
ID   Name             Status  Fwd/Up /Cfg Protocol
   2 VLAN0002         Up       16/ 18/ 18 STP PVST+:1D
   3 VLAN0003         Up        9/ 10/ 10 STP Single:1D
>
```

4 VLAN 拡張機能

この章では，VLAN に適用する拡張機能の解説と操作方法について説明します。

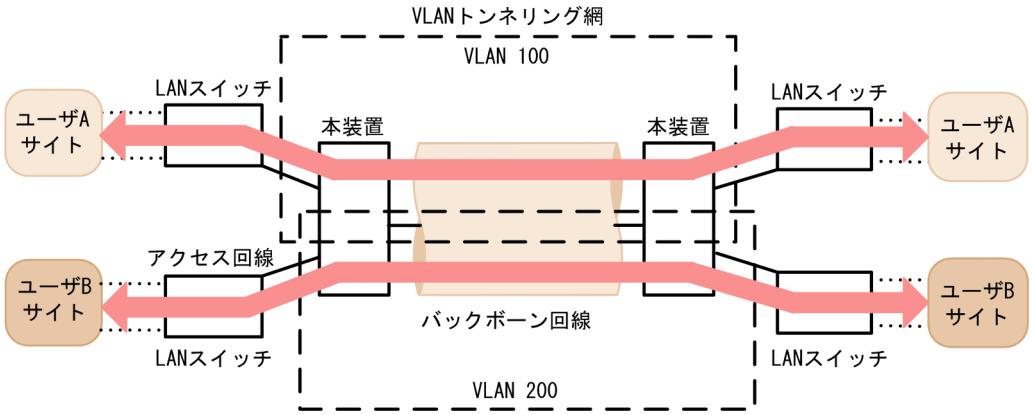
4.1　VLAN トンネリングの解説

4.1.1　概要

VLAN トンネリング機能とは，複数ユーザの VLAN をほかの VLAN の中に集約したトンネルで通信する機能です。IEEE802.1Q VLAN Tag をスタックすれば，一つの VLAN 内で，ほかの VLAN に属するフレームをトランスペアレントに通せます。トンネルは 3 か所以上のサイトを接続するマルチポイント接続ができます。

VLAN トンネリングの概要を次の図に示します。

図 4-1　VLAN トンネリングの概要



この図は，レイヤ 2 VPN サービスである広域イーサネットサービスに適用した例です。本装置に VLAN トンネリング機能を適用します。VLAN トンネリングでは，VLAN Tag をスタックすることで VLAN トンネリング網内の VLAN を識別します。ユーザサイトを収容するポートをアクセス回線，VLAN トンネリング網内に接続するポートをバックボーン回線と呼びます。アクセス回線からのフレームに VLAN Tag を追加してバックボーン回線に中継します。バックボーン回線からのフレームは VLAN Tag を外しアクセス回線へ中継します。

4.1.2　アクセス回線とバックボーン回線

VLAN トンネリング機能を適用するときは，アクセス回線をトンネリングポート，バックボーン回線をトランクポートで設定します。

トンネリングポートには，ポートごとにアクセスポート用の VLAN を一つ設定します。トランクポートには 1 ポートに複数の VLAN を設定できます。

すべてのポートをアクセス回線またはバックボーン回線に割り当てられます。ただし，バックボーン回線では VLAN Tag をスタックするため，通常より 4 バイト大きいサイズのフレームを扱える必要があります。

4.1.3　VLAN トンネリング使用時の注意事項

(1)　他機能との共存

「1.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

(2)　トランクポートのネイティブ VLAN について

VLAN トンネリングのトランクポートは VLAN Tag をスタックするポートとなりますが，ネイティブ VLAN では VLAN Tag をスタックしません。本装置からフレームを送信するときはアクセスポートと同様に動作して，フレームを受信するときは Untagged フレームだけを扱います。ほかの VLAN とは異なる動作となるため，VLAN トンネリング網のバックボーン回線の VLAN としては使用できません。

(3)　アクセス回線でリンクアグリゲーション使用時の注意事項

フレーム送信時のポート振り分けに VLAN Tag ごとのポート振り分けを選択しても，チャネルグループを構成するどれか一つのポートから送信するため，ポート振り分けをしたい場合は VLAN Tag ごとのポート振り分け以外の方法を選択してください。

4.2　VLAN トンネリングの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

VLAN トンネ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 4-1　コンフィグレーションコマンド一覧

コマンド名	説明
switchport access	アクセス回線を設定します。
switchport mode	アクセス回線，バックボーン回線を設定するためにポートの種類を設定します。
switchport trunk	バックボーン回線を設定します。
mtu※	バックボーン回線でジャンボフレームを設定します。

注※
「コンフィグレーションコマンドレファレンス Vol.1」「16　イーサネット」を参照してください。

4.2.2　VLAN トンネリングの設定

(1)　アクセス回線，バックボーン回線の設定

[設定のポイント]

VLAN トンネリング機能はポート VLAN を使用し，アクセス回線をトンネリングポート，バックボーン回線をトランクポートで設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   ポート 1/1 のコンフィグレーションモードに移行します。
2. **(config-if)# switchport mode dot1q-tunnel**
   (config-if)# switchport access vlan 10
   (config-if)# exit
   ポート 1/1 をトンネリングポートに設定します。また，VLAN 10 を設定します。
3. **(config)# interface gigabitethernet 2/1**
   ポート 2/1 のコンフィグレーションモードに移行します。
4. **(config-if)# switchport mode trunk**
   (config-if)# switchport trunk allowed vlan 10
   ポート 2/1 をトランクポートに設定します。また，VLAN 10 を設定します。
   ポート 2/1 は VLAN 10 の Tagged フレームを扱うバックボーン回線となります。

(2)　バックボーン回線のジャンボフレームの設定

[設定のポイント]

バックボーン回線は VLAN Tag をスタックするため通常より 4 バイト以上大きいサイズのフレームを扱います。そのため，ジャンボフレームを設定する必要があります。

［コマンドによる設定］

ジャンボフレームのコンフィグレーションについては，「コンフィグレーションガイド Vol.1」「18.3.8　ジャンボフレームの設定」を参照してください。

4.3　Tag 変換の解説

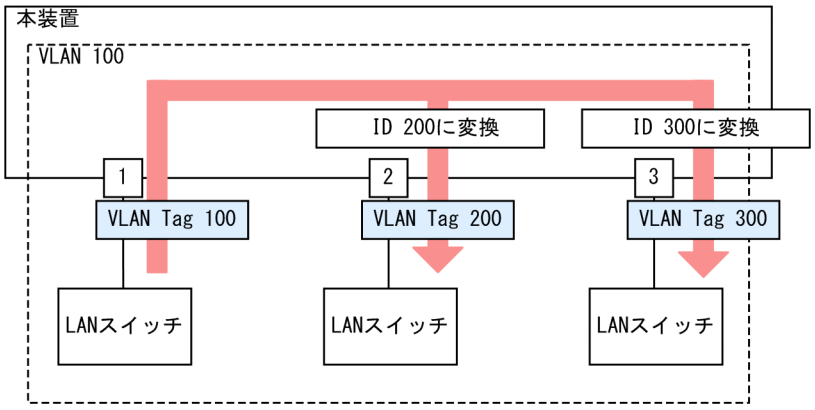
4.3.1　概要

Tag 変換は，Tagged フレームをレイヤ 2 中継する際に，フレームの VLAN Tag の VLAN ID フィールドを別の値に変換する機能です。この機能によって，異なる VLAN ID で設定した既設の VLAN を一つの VLAN として接続できるようになります。

Tag 変換は，トランクポートで指定します。Tag 変換を使用しない場合は，VLAN Tag の VLAN ID フィールドにその VLAN の VLAN ID を使用します。Tag 変換を指定した場合はその ID を使用します。

Tag 変換の構成例を次の図に示します。図では，ポート 1 で Tag 変換が未指定であり，ポート 2 およびポート 3 にそれぞれ Tag 変換を設定して，VLAN Tag の VLAN ID フィールドを変換して中継します。また，フレームを受信するときにも，各ポートで設定した ID の VLAN Tag のフレームを VLAN 100 で扱います。

図 4-2　Tag 変換の構成例



4.3.2　Tag 変換使用時の注意事項

(1)　他機能との共存

「1.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

4.4　Tag 変換のコンフィグレーション

4.4.1　コンフィグレーションコマンド一覧

Tag 変換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 4-2　コンフィグレーションコマンド一覧

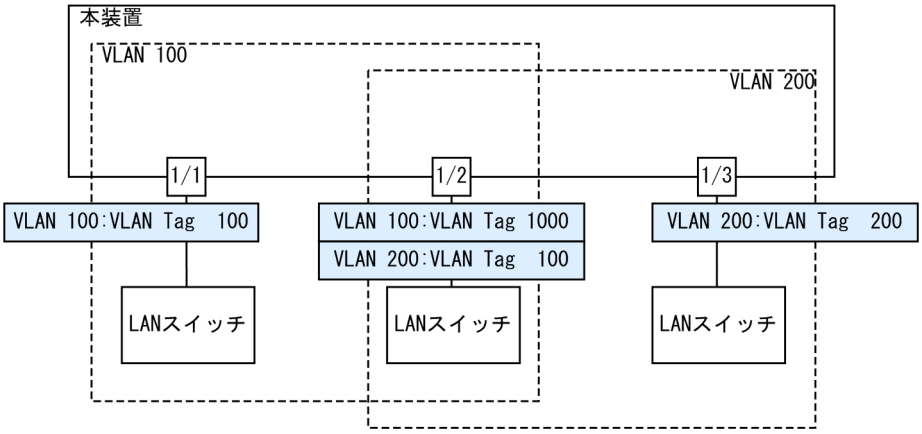
コマンド名	説明
switchport vlan mapping	変換する ID を設定します。
switchport vlan mapping enable	指定したポートで Tag 変換を有効にします。

4.4.2　Tag 変換の設定

Tag 変換を設定する手順を次に示します。ここでは，図に示す構成のポート 1/2 の設定例を示します。

この例では，ポート 1/2 に Tag 変換を適用します。ポート 1/2 では，VLAN 100 のフレームの送受信は VLAN Tag 1000 で，VLAN 200 のフレームの送受信は VLAN Tag 100 でします。このように，VLAN 100 で Tag 変換をした場合，ほかの VLAN でも VLAN Tag 100 を使用できます。また，ポート 1/2 では VLAN Tag 200 のフレームを VLAN 200 として扱わないで，未設定の VLAN Tag として廃棄します。

図 4-3　Tag 変換の設定例



[設定のポイント]

Tag 変換は，Tag 変換を有効にする設定と，変換する ID を設定することによって動作します。Tag 変換の設定はトランクポートだけ有効です。

Tag 変換は switchport vlan mapping コマンドで設定します。設定した変換を有効にするためには，switchport vlan mapping enable コマンドを設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/2**
   (config-if)# switchport mode trunk
   (config-if)# switchport trunk allowed vlan 100,200
   ポート 1/2 をトランクポートに設定して，VLAN 100，200 を設定します。

2. **(config-if)# switchport vlan mapping 1000 100**

   (config-if)# switchport vlan mapping 100 200

   ポート 1/2 で VLAN 100，200 に Tag 変換を設定します。VLAN 100 では VLAN Tag 1000 でフレームを送受信して，VLAN 200 では VLAN Tag 100 でフレームを送受信するように設定します。

3. **(config-if)# switchport vlan mapping enable**

   ポート 1/2 で Tag 変換を有効にします。本コマンドを設定するまでは Tag 変換は動作しません。

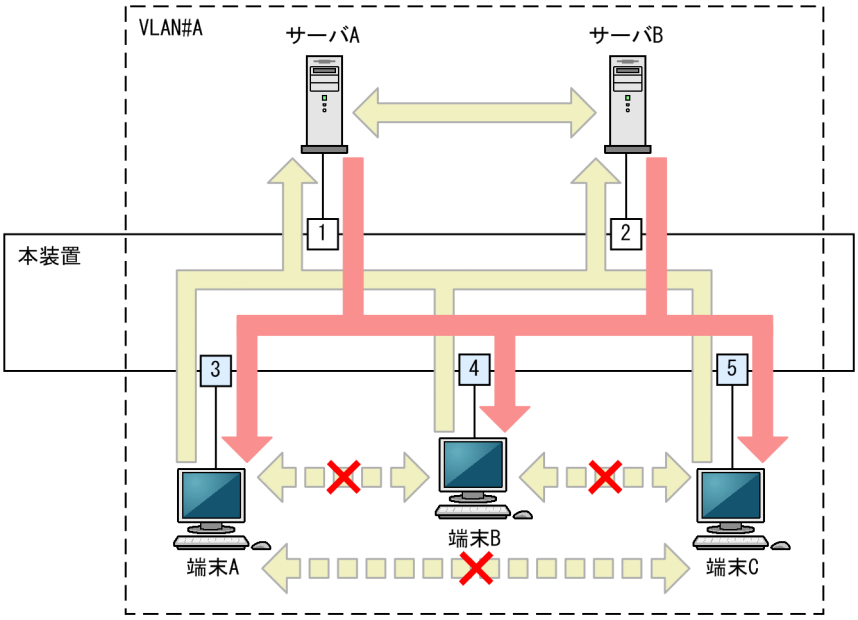
4.5　アイソレート VLAN の解説

4.5.1　概要

アイソレート VLAN とは，VLAN 内で，ポート間でのレイヤ 2 中継を遮断する機能です。サーバとの接続は許可しても端末同士の直接通信を遮断して，セキュリティを確保したい場合などに適用します。なお，この遮断対象のポートをアイソレートポートと呼びます。

アイソレート VLAN の構成例を次の図に示します。

図 4-4　アイソレート VLAN の構成例



この構成例では，VLAN 内で端末を接続しているポート 3~5 にアイソレートポートを設定して，共有サーバなどを接続しているポート 1 および 2 にはアイソレートポートを設定しません。これによって，端末間での通信は遮断されますが，端末から各サーバへ，サーバから各端末へ，およびサーバ間では通信できます。

4.5.2　アイソレート VLAN 使用時の注意事項

(1)　他機能との共存

「1.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

4.6　アイソレート VLAN のコンフィグレーション

4.6.1　コンフィグレーションコマンド一覧

アイソレート VLAN 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 4-3　コンフィグレーションコマンド一覧

コマンド名	説明
isolate-vlan	アイソレート VLAN を設定します。
switchport isolate	アイソレートポートの情報を設定します。

4.6.2　アイソレート VLAN の設定

アイソレート VLAN を設定する手順を次に示します。

[設定のポイント]

アイソレート VLAN は，VLAN ごとに設定します。また，レイヤ 2 中継を遮断したいポートにアイソレートポートを設定します。

[コマンドによる設定]

1. **(config)# interface vlan 10**
   (config-if)# isolate-vlan
   (config-if)# exit
   VLAN 10 でアイソレート VLAN を有効にします。
2. **(config)# interface range gigabitethernet 1/1-2**
   (config-if-range)# switchport mode access
   (config-if-range)# switchport access vlan 10
   (config-if)# exit
   ポート 1/1 および 1/2 を，レイヤ 2 中継を遮断しないポートとして設定します。
3. **(config)# interface range gigabitethernet 1/3-5**
   (config-if-range)# switchport mode access
   (config-if-range)# switchport access vlan 10
   (config-if-range)# switchport isolate vlan 10
   ポート 1/3，1/4，および 1/5 を，アイソレートポートとして設定します。

4.7　VLAN debounce 機能の解説

4.7.1　概要

VLAN は，VLAN 内のポートのどれかが通信できる状態になったときにアップし，VLAN 内のすべてのポートがダウンしたときや，スパニングツリーなどの機能でブロッキング状態になり通信できなくなったときなどにダウンします。

VLAN debounce 機能は，VLAN のアップまたはダウンを遅延させて，ネットワークトポロジの変更，システムメッセージ，SNMP 通知などを削減するための機能です。

スパニングツリーや Ring Protocol など，レイヤ 2 での冗長構成を使用したときに障害が発生した場合，通常レイヤ 3 のトポロジ変更と比べて短い時間で代替経路へ切り替わります。VLAN debounce 機能によってレイヤ 2 での代替経路への切替時間まで VLAN のダウンを遅延させると，レイヤ 3 のトポロジを変化させないですみ，通信の可用性を確保できます。

4.7.2　VLAN debounce 機能の動作契機

(1)　VLAN のダウンに対する動作契機

VLAN で通信できるポートがなくなった場合に，VLAN のダウンに対する VLAN debounce 機能が動作します。VLAN のダウンに対する VLAN debounce 機能の動作契機を次の表に示します。

表 4-4　VLAN のダウンに対する VLAN debounce 機能の動作契機

契機	備考
ポートのリンクダウン	－
VLAN ポートのブロッキング状態への変更※	－
リンクアップしているポートを VLAN から削除（コンフィグレーションの変更）	VLAN に所属するポートが 0 になった場合は，すぐに VLAN もダウンします

（凡例）－：該当なし

注※　スパニングツリー，Ring Protocol などによります

(2)　VLAN のアップに対する動作契機

VLAN で通信できるポートが一つできた場合に，VLAN のアップに対する VLAN debounce 機能が動作します。ただし，コンフィグレーションコマンド up-debounce の extend パラメータの有無によって動作契機が異なります。VLAN のアップに対する VLAN debounce 機能の動作契機を次の表に示します。

表 4-5　VLAN のアップに対する VLAN debounce 機能の動作契機

契機	extend パラメータあり	extend パラメータなし
装置起動および再起動	○	×
ポートのリンクアップ	○	○
VLAN ポートのフォワーディング状態への変更※	○	○
コンフィグレーションコマンド no shutdown で VLAN をシャットダウン状態解除へ変更	○	×

契機	extend パラメータあり	extend パラメータなし
リンクアップしているポートを VLAN に追加（コンフィグレーションの変更）	○	○

（凡例）○：VLAN debounce 機能が動作する　×：VLAN debounce 機能が動作しない

注※　スパニングツリー，Ring Protocol などによります

4.7.3　VLAN debounce 機能と他機能との関係

(1)　スパニングツリー

スパニングツリーでは，ポートに障害が発生して代替経路へ変更されるまでに，スパニングツリーのトポロジ変更に必要な時間が掛かります。この間に VLAN をダウンさせたくない場合は，VLAN のダウン遅延時間をトポロジ変更に必要な時間以上に設定してください。

(2)　Ring Protocol

Ring Protocol を使用する場合，マスタノードではプライマリポートがフォワーディング状態，セカンダリポートがブロッキング状態となっています。VLAN debounce 機能を使用しない場合，プライマリポートで障害が発生するといったん VLAN がダウンして，セカンダリポートのブロッキング状態が解除されると再び VLAN がアップします。

このようなときに VLAN がいったんダウンすることを防ぐためには，VLAN のダウン遅延時間を設定してください。なお，ダウン遅延時間はコンフィグレーションコマンド health-check holdtime で設定する保護時間以上に設定してください。

(3)　その他の冗長化機能

スパニングツリーや Ring Protocol 以外の冗長化を使用する場合でも，VLAN が短時間にアップやダウンを繰り返すときには，VLAN debounce 機能を使用するとアップやダウンを抑止できます。

4.7.4　VLAN debounce 機能使用時の注意事項

(1)　ダウン遅延時間の注意事項

ダウン遅延時間を設定すると，回復しない障害が発生した場合でも VLAN のダウンが遅延します。VLAN debounce 機能でダウンが遅延している間は，通信できない状態です。ダウン遅延時間は，ネットワークの構成や運用に応じて必要な値を設定してください。

VLAN にコンフィグレーションコマンド shutdown を設定したときや VLAN のポートをすべて削除したときなど，コンフィグレーションを変更しないとその VLAN が通信可能とならない場合には，ダウン遅延時間を設定していても VLAN のダウンは遅延しません。

(2)　アップ遅延時間の注意事項

アップ遅延時間を設定すると，いったんアップした VLAN がダウンしたあと，再度アップするときにアップが遅延します。装置を再起動すると，VLAN は初期状態になるため，アップ遅延時間を設定していても VLAN のアップは遅延しません。

4.8　VLAN debounce 機能のコンフィグレーション

4.8.1　コンフィグレーションコマンド一覧

VLAN debounce 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 4-6　コンフィグレーションコマンド一覧

コマンド名	説明
down-debounce	VLAN がダウンするまでの遅延時間を設定します。
up-debounce	VLAN がアップするまでの遅延時間を設定します。

4.8.2　VLAN debounce 機能の設定

VLAN debounce 機能を設定する手順を次に示します。

[設定のポイント]

VLAN debounce 機能の遅延時間は，ネットワーク構成および運用に合わせて最適な値を設定します。

[コマンドによる設定]

1. **(config)# interface vlan 100**
   VLAN インタフェース 100 のコンフィグレーションモードに移行します。
2. **(config-if)# down-debounce 2**
   (config-if)# exit
   VLAN 100 のダウン遅延時間を 2 秒に設定します。
3. **(config)# interface range vlan 201-300**
   VLAN インタフェース 201～300 のコンフィグレーションモードに移行します。
4. **(config-if-range)# down-debounce 3**
   (config-if-range)# exit
   VLAN 201～300 のダウン遅延時間を 3 秒に設定します。

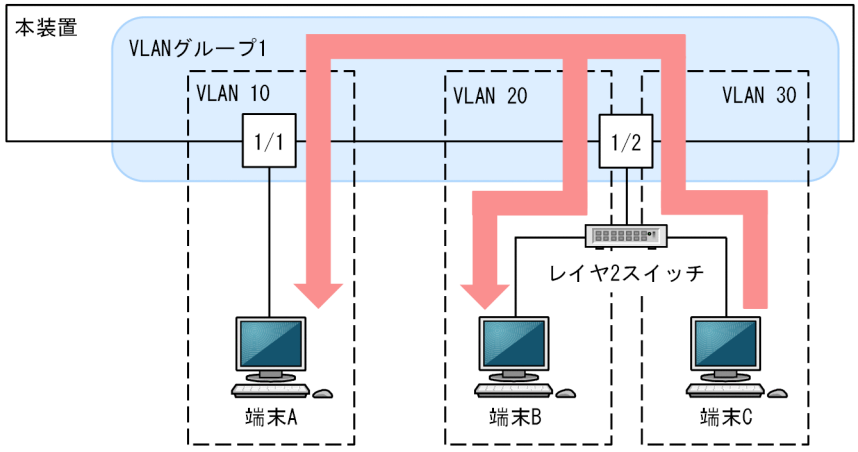
4.9　アグリゲート VLAN の解説

4.9.1　概要

アグリゲート VLAN は，複数の VLAN をグループ化し，グループ内の VLAN から受信したフレームをグループ内の全 VLAN に中継できる機能です。このグループを VLAN グループと呼びます。通常の VLAN は異なる VLAN へ中継できませんが，本機能を使用すると，異なる VLAN 間で中継できるようになります。

アグリゲート VLAN の構成例を次の図に示します。

図 4-5　アグリゲート VLAN の構成例



この例では，VLAN 10，VLAN 20，および VLAN 30 を VLAN グループ 1 に設定したことで，VLAN 30 の端末 C が送信するブロードキャストフレームは，同じ VLAN グループ 1 内の，VLAN 10 の端末 A と VLAN 20 の端末 B へ中継されます。このように，ブロードキャストドメインが VLAN グループとなるため，異なる VLAN 間でフレームを送受信できます。

また，通常の VLAN では，フレームを受信したポートから送信しません。しかし，アグリゲート VLAN では，グループ内の VLAN から受信したフレームを，同じグループ内のほかの VLAN へ，同じポートでも送信できます。この例では，ポート 1/2 の VLAN 30 で受信したフレームを，同じポートの VLAN 20 に送信しています。

4.9.2　アグリゲート VLAN の MAC アドレス学習

通常の MAC アドレス学習では，MAC アドレステーブルに，受信したフレームの送信元 MAC アドレスと VLAN をペアにして管理します。しかし，アグリゲート VLAN を設定すると，同じ VLAN グループの VLAN も管理対象となります。異なる VLAN であっても，VLAN グループが同じであれば，同一の MAC アドレスと扱います。VLAN グループが同じで異なる VLAN であっても，フレームの宛先 MAC アドレスが一致すれば，MAC アドレステーブルに従って，フレームを中継します。この場合，MAC アドレスを学習したときの VLAN でフレームを中継します。MAC アドレスのエージングや，MAC アドレス学習抑止は，VLAN グループ内の VLAN 単位に行います。

4.9.3　アグリゲート VLAN の MAC アドレス学習の移動検出

学習済みの送信元 MAC アドレスを持つフレームを，VLAN グループ内の学習時と異なる VLAN，またはポートから受信した場合，その MAC アドレスが移動したものと見なして MAC アドレステーブルのエントリを再登録（移動先 VLAN またはポートに関する上書き）します。

4.9.4　アグリゲート VLAN 使用時の注意事項

(1)　他機能との共存

「1.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

4.10　アグリゲート VLAN のコンフィグレーション

4.10.1　コンフィグレーションコマンド一覧

アグリゲート VLAN 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 4-7　コンフィグレーションコマンド一覧

コマンド名	説明
aggregate-vlan	VLAN をアグリゲート VLAN の VLAN グループに設定します。
aggregate-vlan-group	アグリゲート VLAN の VLAN グループを設定します。

4.10.2　アグリゲート VLAN の設定

アグリゲート VLAN を設定する手順を次に示します。

[設定のポイント]

アグリゲート VLAN の VLAN グループを設定します。VLAN グループに所属する VLAN を設定します。

[コマンドによる設定]

1. **(config)# aggregate-vlan-group 1**
   VLAN グループ 1 を設定します。
2. **(config)# interface vlan 100**
   (config-if)# aggregate-vlan group 1
   (config-if)# exit
   VLAN100 を VLAN グループ 1 に設定します。
3. **(config)# interface range vlan 200-202**
   (config-if-range)# aggregate-vlan group 1
   (config-if-range)# exit
   VLAN200～202 を VLAN グループ 1 に設定します。

4.11　VLAN 拡張機能のオペレーション

4.11.1　運用コマンド一覧

VLAN 拡張機能の運用コマンド一覧を次の表に示します。

表 4-8　運用コマンド一覧

コマンド名	説明
show vlan	VLAN 拡張機能の設定状態を確認します。
show mac-address-table※	VLAN 拡張機能の MAC アドレス学習の状態を確認します。

注※

「運用コマンドレファレンス Vol.2」「2　MAC アドレステーブル」を参照してください。

4.11.2　VLAN 拡張機能の確認

(1)　VLAN トンネリングの確認

show vlan コマンドで, VLAN トンネリングの設定状態を確認できます。VLAN トンネリングが設定されているポートは，Port Information に「Tunnel」が表示されます。

図 4-6　VLAN トンネリングの確認

```
> show vlan 10 detail
Date 20XX/03/08 14:04:49 UTC
VLAN counts:1
VLAN ID:10    Status:Up
  Name:VLAN0010
  Learning:ON
  Isolate VLAN:
  Aggregate VLAN group:
  Spanning Tree:
  AXRP RING ID:      AXRP VLAN group:
  IGMP snooping:     MLD snooping:
  Port Information
   1/1          Up   Forwarding      Untagged Tunnel                 <-1
   2/1          Up   Forwarding      Tagged
>
```

1. このポートに VLAN トンネリングが設定されていることを示します。

(2)　Tag 変換の確認

show vlan コマンドで，Tag 変換の設定状態を確認できます。Tag 変換が設定されているポートは，Port Information に「Tag-Translation」が表示されます。

図 4-7　Tag 変換の確認

```
> show vlan 3 detail
Date 20XX/05/23 17:01:40 UTC
VLAN counts:1
VLAN ID:3     Status:Up
  Name:VLAN0003
  Learning:ON
  Isolate VLAN:
  Aggregate VLAN group:
  Spanning Tree:Single(802.1D)
  AXRP RING ID:      AXRP VLAN group:
  Port Information
   1/5          Up   Forwarding      Untagged
```

```
  1/6          Up   Blocking(STP)   Untagged
  1/7          Up   Forwarding      Untagged
  1/8          Up   Forwarding      Untagged
  1/9          Up   Forwarding      Untagged
  1/10         Up   Forwarding      Untagged
  1/11(CH:9)   Up   Forwarding      Tagged   Tag-Translation:103     <-1
  1/12(CH:9)   Up   Blocking(CH)    Tagged   Tag-Translation:103     <-1
>
```

1.このポートに Tag 変換が設定されていることを示します。

(3) アイソレート VLAN の確認

show vlan コマンドで，アイソレート VLAN の設定状態を確認できます。アイソレート VLAN が設定されている VLAN は，Isolate VLAN に「On」が表示されます。また，アイソレートポートが設定されているポートは，Port Information に「Isolate」が表示されます。

図 4-8 アイソレート VLAN の確認

```
> show vlan 10 detail
Date 20XX/03/07 17:45:47 UTC
VLAN counts:1
VLAN ID:10    Status:Up
  Name:VLAN0010
  Learning:ON
  Isolate VLAN:On                                                  <-1
  Aggregate VLAN group:
  Spanning Tree:
  AXRP RING ID:      AXRP VLAN group:
  IGMP snooping:     MLD snooping:
  Port Information
   1/1          Up   Forwarding      Untagged
   1/2          Up   Forwarding      Untagged
   1/3          Up   Forwarding      Untagged Isolate                <-2
   1/4          Up   Forwarding      Untagged Isolate                <-2
   1/5          Up   Forwarding      Untagged Isolate                <-2
>
```

1.アイソレート VLAN が設定されていることを示します。

2.このポートにアイソレートポートが設定されていることを示します。

(4) アグリゲート VLAN の確認

show vlan コマンドで，アグリゲート VLAN の設定状態を確認できます。アグリゲート VLAN が設定されている VLAN は，Aggregate VLAN group に VLAN グループ ID が表示されます。

図 4-9 アグリゲート VLAN の確認

```
> show vlan 100 detail
Date 20XX/12/15 17:12:48 UTC
VLAN counts:1
VLAN ID:100   Status:Up
  Name:VLAN0100
  Learning:On
  Isolate VLAN:
  Aggregate VLAN group:1                                           <-1
  Spanning Tree:
  AXRP RING ID:      AXRP VLAN group:
  IGMP snooping:     MLD snooping:
  Port Information
   1/1          Up   Forwarding      Tagged
   1/2          Up   Forwarding      Tagged
   1/10         Up   Forwarding      Tagged
>
```

1.アグリゲート VLAN の VLAN グループが設定されていることを示します。

4.11.3　VLAN 拡張機能の MAC アドレス学習の確認

(1)　アグリゲート VLAN の VLAN グループが学習した MAC アドレス

show mac-address-table コマンドで，学習した MAC アドレスの，アグリゲート VLAN の VLAN グループを確認できます。アグリゲート VLAN の VLAN グループに属する VLAN で学習した MAC アドレスには，VLAN グループ ID が表示されます。

図 4-10　show mac-address-table コマンドの実行結果

```
>show mac-address-table
Date 20XX/01/11 11:16:46 UTC
MAC address        VLAN C-Tag VLAN-G    Aging-Time Type     Port-list
0012.e200.1111        2     -      -           100 Dynamic  1/5
0012.e211.82ad     2746     -    717            92 Dynamic  2/1,4/1
0012.e2c0.04aa     3986     -   2048           299 Dynamic  2/2,4/2
0012.e2c0.090a     4071     -   2048           299 Dynamic  2/2,4/2
0012.e2c0.04da     3997     -   2048           299 Dynamic  2/2,4/2
0012.e2c0.091a     4072     -   2048           299 Dynamic  2/2,4/2
0012.e211.8c7d     2934     -    811            92 Dynamic  2/1,4/1
>
```

5 広域イーサネット機能

この章では，広域イーサネット機能の解説と操作方法について説明します。

5.1　解説

広域イーサネットとは，ユーザ VLAN を透過して転送するキャリアサービスです。

広域イーサネット網のサービス提供形態はいろいろありますが，そのうちの一つに QinQ という方式があります。この方式では，エッジ装置で VLAN トンネリングすることによって，バックボーン網でユーザ VLAN を透過して転送できます。なお，VLAN トンネリング機能については，「4.1　VLAN トンネリングの解説」を参照してください。

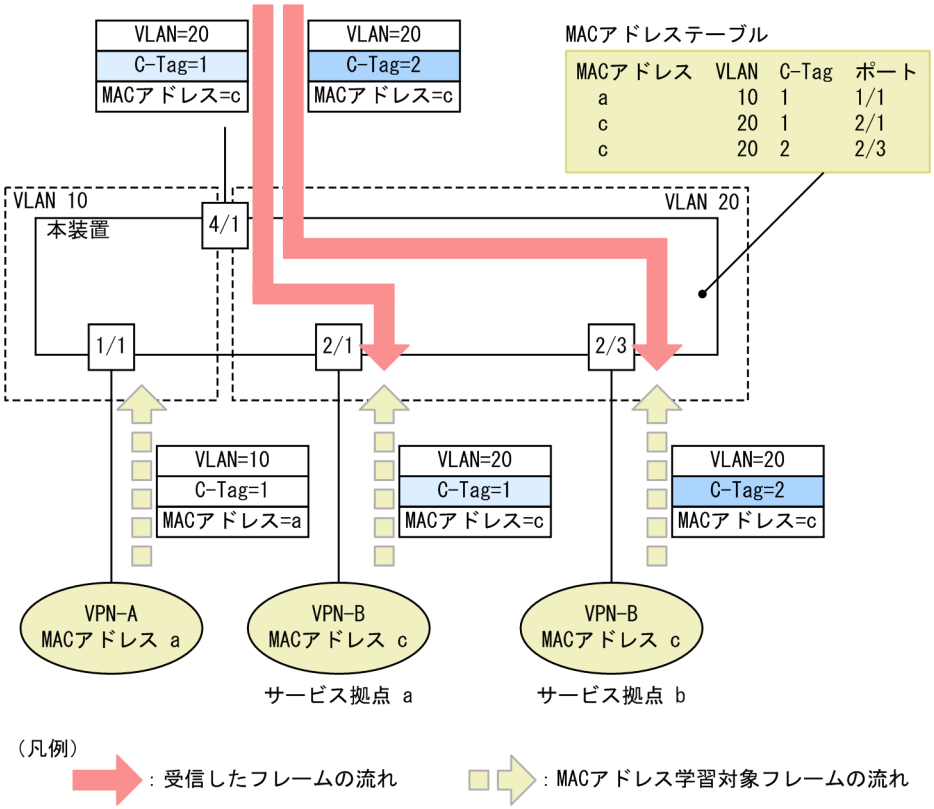
本装置では，QinQ 網のコア装置向けの機能を提供します。QinQ 網向け機能は，コンフィグレーションで QinQ 網向け機能に対応したハードウェアプロファイルを設定すると動作します。

5.1.1　2 段の VLAN Tag での MAC アドレス学習

通常の MAC アドレス学習では Tag なしまたは 1 段の VLAN Tag を扱いますが，QinQ 網向け機能のハードウェアプロファイルを設定すると，2 段の VLAN Tag を扱う MAC アドレス学習ができるようになります。

2 段の VLAN Tag での MAC アドレス学習によって，同一 VLAN（S-Tag）でも C-Tag 値が異なる場合，別のエントリとして MAC アドレステーブルへ登録されるため，別々に通信できます。複数 VPN を集約する VLAN 上で，2 段の VLAN Tag での MAC アドレス学習を使用した例を次の図に示します。

図 5-1　2 段の VLAN Tag での MAC アドレス学習



VPN-B の VLAN 20 内では，二つのサービス拠点を接続しています。VRRP の設定などによって両拠点が同一の送信元 MAC アドレスになった場合でも，C-Tag 値が異なっていると，本装置の MAC アドレステー

ブルには別のエントリとして登録されます。登録後は，受信したフレームの C-Tag 値に基づいて，該当するポートへ中継できます。

5.1.2　MAC アドレス学習の移動監視

MAC アドレス学習の移動検出では，学習済みの送信元 MAC アドレスを持つフレームを学習時と異なるポートから受信した場合，その MAC アドレスが移動したものと見なして MAC アドレステーブルのエントリを再登録（移動先ポートに関する上書き）します。

QinQ 網向け機能のハードウェアプロファイルを設定すると，MAC アドレス学習の移動を監視します。単位時間当たりに閾値を超えると，システムメッセージで MAC アドレス学習の移動の過多を通知します。この動作は，ネットワーク間でフレームのループが発生したときなどの検知に利用できます。

5.1.3　BPDU の透過機能

QinQ 網向け機能のハードウェアプロファイルを設定すると，すべてのポートでスパニングツリーの BPDU を中継します。通常，これらレイヤ 2 のプロトコル制御フレームは中継しません。本装置では，中継するフレームをマルチキャストフレームとして扱います。

5.1.4　QinQ 網向け機能使用時の注意事項

(1)　他機能との共存

「1.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

5.2　コンフィグレーション

5.2.1　コンフィグレーションコマンド一覧

QinQ 網向け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 5-1　コンフィグレーションコマンド一覧

コマンド名	説明
hardware profile※	ハードウェアプロファイルを設定します。

注※

「コンフィグレーションコマンドレファレンス Vol.1」「10　装置とソフトウェアの管理」を参照してください。

5.2.2　QinQ 網向け機能の設定

[設定のポイント]

本装置で QinQ 網向け機能を有効にするには，対応するハードウェアプロファイルを設定する必要があります。

装置および VLAN インタフェースの IGMP snooping と MLD snooping を無効にしてから，QinQ 網向け機能に対応したハードウェアプロファイルを設定してください。また，設定したハードウェアプロファイルを反映するために，装置を再起動してください。

[コマンドによる設定]

1. **(config)# hardware profile switch-2-qinq**

   グローバルコンフィグレーションモードで，ハードウェアプロファイルを switch-2-qinq に設定します。

5.3　オペレーション

5.3.1　運用コマンド一覧

QinQ 網向け機能の運用コマンド一覧を次の表に示します。

表 5-2　運用コマンド一覧

コマンド名	説明
show mac-address-table※	MAC アドレステーブルの情報を表示します。
clear mac-address-table※	MAC アドレステーブルをクリアします。

注※

「運用コマンドレファレンス Vol.2」「2　MAC アドレステーブル」を参照してください。

5.3.2　MAC アドレス学習の状態の確認

MAC アドレステーブルの情報は show mac-address-table コマンドで表示します。MAC アドレステーブルに登録されている MAC アドレスと，その MAC アドレスを宛先とする S-Tag（VLAN），C-Tag，およびポートが表示されます。

図 5-2　show mac-address-table コマンドの実行結果

```
> show mac-address-table
Date 20XX/01/11 11:16:46 UTC
MAC address        VLAN C-Tag VLAN-G    Aging-Time Type     Port-list
0012.e200.1111        2     1      -           100 Dynamic  1/5
0012.e244.f070      100    10      -            10 Dynamic  1/12
0012.e244.f070      100    20      -            10 Dynamic  2/12
```

6 スパニングツリー

この章では，スパニングツリー機能の解説と操作方法について説明します。

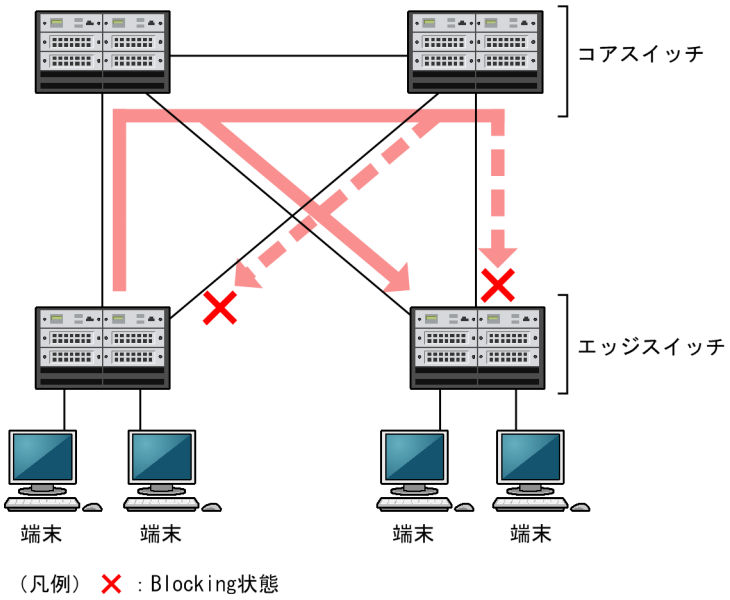
6.1　スパニングツリーの概説

6.1.1　概要

スパニングツリープロトコルは，レイヤ２のループ防止プロトコルです。スパニングツリープロトコルを使用することで，レイヤ２ネットワークを冗長化し，ループを防止できます。

スパニングツリーを適用したネットワークの概要を次の図に示します。

図 6-1　スパニングツリーを適用したネットワークの概要



図の構成は，ネットワークのコアを担うスイッチを冗長化し，また，端末を収容するエッジスイッチからの通信経路を冗長化しています。装置および通信経路を冗長化することで，通常の通信経路に障害が発生しても代替の経路で通信を継続できます。

レイヤ２ネットワークを冗長化するとレイヤ２ループの構成になります。レイヤ２のループはブロードキャストストームの発生や MAC アドレス学習が安定しないなどの問題を引き起こします。スパニングツリーは，冗長化してループ構成になったレイヤ２ネットワークで，通信を止める場所を選択して Blocking 状態とすることでループを防止するプロトコルです。

6.1.2　スパニングツリーの種類

本装置では，PVST+，シングルスパニングツリー，およびマルチプルスパニングツリーの３種類のスパニングツリーをサポートします。各スパニングツリーは構築の単位が異なります。スパニングツリーの種類と概要について次の表に示します。

表 6-1　スパニングツリーの種類

名称	構築単位	概要
PVST+	VLAN 単位	VLAN 単位にツリーを構築します。一つのポートに複数の VLAN が所属している場合，VLAN ごとに異なるツリー構築結果を適用します。

名称	構築単位	概要
シングルスパニングツリー	装置単位	装置全体のポートを対象としてツリーを構築します。VLAN 構成とは無関係に装置のすべてのポートにツリー構築結果を適用します。
マルチプルスパニングツリー	MST インスタンス単位	複数の VLAN をまとめた MST インスタンスというグループごとにスパニングツリーを構築します。一つのポートに複数の VLAN が所属している場合，MST インスタンス単位に異なるツリー構築結果を適用します。

本装置では，上記で記述したスパニングツリーを単独または組み合わせて使用できます。スパニングツリーの組み合わせと適用範囲を次の表に示します。

表 6-2　スパニングツリーの組み合わせと適用範囲

ツリー構築条件	トポロジ計算結果の適用範囲
PVST+単独	PVST+が動作している VLAN には VLAN ごとのスパニングツリーを適用します。そのほかの VLAN はスパニングツリーを適用しません。
シングルスパニングツリー単独	全 VLAN にシングルスパニングツリーを適用します。 PVST+をすべて停止した構成です。
PVST+とシングルスパニングツリーの組み合わせ	PVST+が動作している VLAN には VLAN ごとのスパニングツリーを適用します。そのほかの VLAN にはシングルスパニングツリーを適用します。
マルチプルスパニングツリー単独	全 VLAN にマルチプルスパニングツリーを適用します。

注　マルチプルスパニングツリーはほかのツリーと組み合わせて使用できません。

6.1.3　スパニングツリーと高速スパニングツリー

PVST+，シングルスパニングツリーには IEEE802.1D のスパニングツリーと IEEE802.1w の高速スパニングツリーの 2 種類があります。それぞれ，PVST+と Rapid PVST+，STP と Rapid STP と呼びます。

スパニングツリープロトコルのトポロジ計算は，通信経路を変更する際にいったんポートを通信不可状態（Blocking 状態）にしてから複数の状態を遷移して通信可能状態（Forwarding 状態）になります。IEEE 802.1D のスパニングツリーはこの状態遷移でタイマによる状態遷移をするため，通信可能となるまでに一定の時間が掛かります。IEEE 802.1w の高速スパニングツリーはこの状態遷移でタイマによる待ち時間を省略して高速な状態遷移をすることで，トポロジ変更によって通信が途絶える時間を最小限にします。

なお，マルチプルスパニングツリーは IEEE802.1s として規格化されたもので，状態遷移の時間は IEEE802.1w と同等です。それぞれのプロトコルの状態遷移とそれに必要な時間を次に示します。

表 6-3　PVST+，STP（シングルスパニングツリー）の状態遷移

状態	状態の概要	次の状態への遷移
Disable	ポートが使用できない状態です。使用可能となると，すぐに Blocking に遷移します。	−

状態	状態の概要	次の状態への遷移
Blocking	通信不可の状態で，MAC アドレス学習もしません。リンクアップ直後またはトポロジが安定して Blocking になるポートもこの状態になります。	20 秒（変更可能）または BPDU を受信
Listening	通信不可の状態で，MAC アドレス学習もしません。該当ポートが Learning になる前に，トポロジが安定するまで待つ期間です。	15 秒（変更可能）
Learning	通信不可の状態です。しかし，MAC アドレス学習はします。該当ポートが Forwarding になる前に，事前に MAC アドレス学習をする期間です。	15 秒（変更可能）
Forwarding	通信可能の状態です。トポロジが安定した状態です。	－

（凡例）－：該当なし

表 6-4　Rapid PVST+，Rapid STP（シングルスパニングツリー）の状態遷移

状態	状態の概要	次の状態への遷移
Disable	ポートが使用できない状態です。使用可能となると，すぐに Discarding に遷移します。	－
Discarding	通信不可の状態で，MAC アドレス学習もしません。該当ポートが Learning になる前に，トポロジが安定するまで待つ期間です。	省略または 15 秒（変更可能）
Learning	通信不可の状態です。しかし，MAC アドレス学習はします。該当ポートが Forwarding になる前に，事前に MAC アドレス学習をする期間です。	省略または 15 秒（変更可能）
Forwarding	通信可能の状態です。トポロジが安定した状態です。	－

（凡例）－：該当なし

Rapid PVST+，Rapid STP では，対向装置からの BPDU 受信によって Discarding と Learning 状態を省略します。この省略によって，高速なトポロジ変更をします。

高速スパニングツリーを使用する際は，次の条件に従って設定してください。条件を満たさない場合，Discarding，Learning を省略しないで高速な状態遷移をしないことがあります。

- トポロジの全体を同じプロトコル（Rapid PVST+または Rapid STP）で構築する（Rapid PVST+と Rapid STP の相互接続は，「6.3.2　アクセスポートの PVST+」を参照してください）。
- スパニングツリーが動作する装置間は Point-to-Point 接続する。
- スパニングツリーが動作する装置を接続しないポートでは PortFast を設定する。

6.1.4　スパニングツリートポロジの構成要素

スパニングツリーのトポロジを設計するためには，ブリッジやポートの役割およびそれらの役割を決定するために使用する識別子などのパラメータがあります。これらの構成要素とトポロジ設計での利用方法を次に示します。

(1)　ブリッジの役割

ブリッジの役割を次の表に示します。スパニングツリーのトポロジ設計は，ルートブリッジを決定することから始まります。

表 6-5　ブリッジの役割

ブリッジの役割	概要
ルートブリッジ	トポロジを構築する上で論理的な中心となるスイッチです。トポロジ内に一つだけ存在します。
指定ブリッジ	ルートブリッジ以外のスイッチです。ルートブリッジの方向からのフレームを転送する役割を担います。

(2)　ポートの役割

ポートの役割を次の表に示します。指定ブリッジは 3 種類のポートの役割を持ちます。ルートブリッジは，次の役割のうち，すべてのポートが指定ポートとなります。

表 6-6　ポートの役割

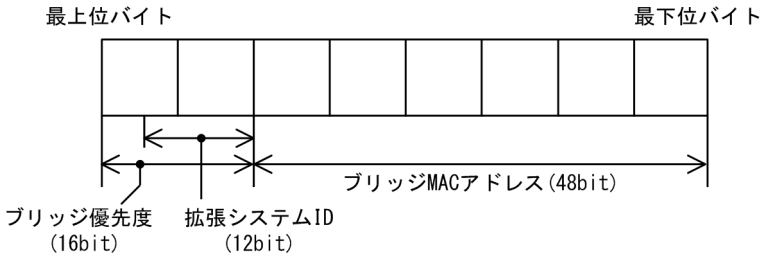
ポートの役割	概要
ルートポート	指定ブリッジからルートブリッジへ向かう通信経路のポートです。通信可能なポートとなります。
指定ポート	ルートポート以外の通信可能なポートです。ルートブリッジからの通信経路でトポロジの下流へ接続するポートです。
非指定ポート	ルートポート，指定ポート以外のポートで，通信不可の状態のポートです。障害が発生した際に通信可能になり代替経路として使用します。

(3)　ブリッジ識別子

トポロジ内の装置を識別するパラメータをブリッジ識別子と呼びます。ブリッジ識別子が最も小さい装置が優先度が高く，ルートブリッジとして選択されます。

ブリッジ識別子はブリッジ優先度（16bit）とブリッジ MAC アドレス（48bit）で構成されます。ブリッジ優先度の下位 12bit は拡張システム ID です。拡張システム ID には，シングルスパニングツリー，マルチプルスパニングツリーの場合は 0 が設定され，PVST+の場合は VLAN ID が設定されます。ブリッジ識別子を次の図に示します。

図 6-2　ブリッジ識別子



(4)　パスコスト

スイッチ上の各ポートの通信速度に対応するコスト値をパスコストと呼びます。指定ブリッジからルートブリッジへ到達するために経由するすべてのポートのコストを累積した値をルートパスコストと呼びます。ルートブリッジへ到達するための経路が 2 種類以上ある場合，ルートパスコストが最も小さい経路を使用します。

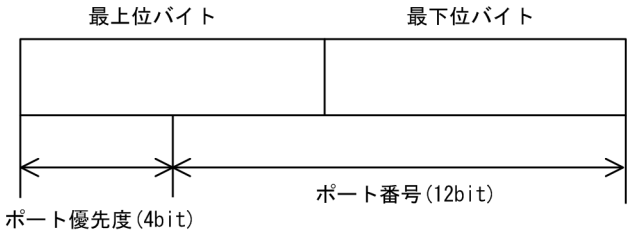
速度が速いポートほどパスコストを低くすることをお勧めします。パスコストはデフォルト値がポートの速度に応じた値となっていて，コンフィグレーションで変更することもできます。

(5)　ポート識別子

スイッチ内の各ポートを識別するパラメータをポート識別子と呼びます。ポート識別子は 2 台のスイッチ間で 2 本以上の冗長接続をし，かつ各ポートでパスコストを変更できない場合に通信経路の選択に使用します。ただし，2 台のスイッチ間の冗長接続はリンクアグリゲーションを使用することをお勧めします。リンクアグリゲーションをサポートしていない装置と冗長接続するためにはスパニングツリーを使用してください。

ポート識別子はポート優先度（4bit）とポート番号（12bit）によって構成されます。ポート識別子を次の図に示します。

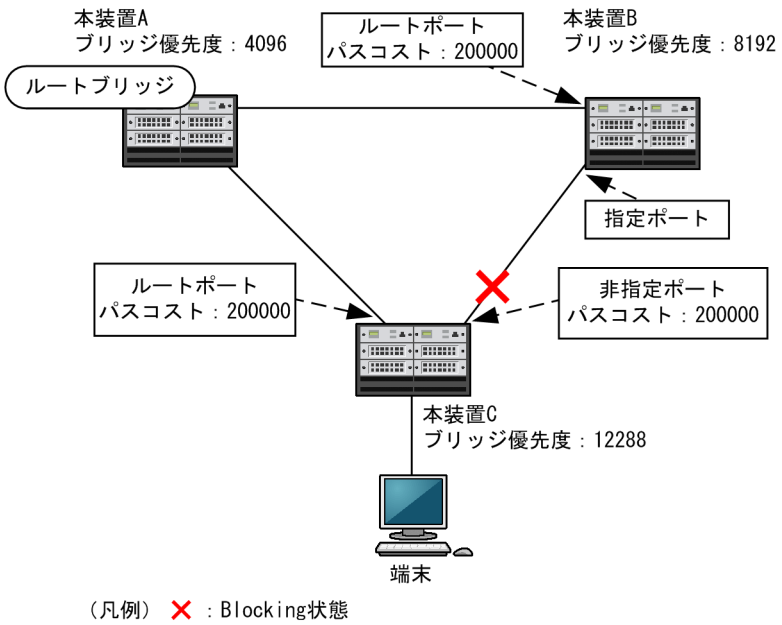
図 6-3　ポート識別子



6.1.5　スパニングツリーのトポロジ設計

スパニングツリーは，ブリッジ識別子，パスコストによってトポロジを構築します。次の図に，トポロジ設計の基本的な手順を示します。図の構成は，コアスイッチとして 2 台を冗長化して，エッジスイッチとして端末を収容するスイッチを配置する例です。

図 6-4　スパニングツリーのトポロジ設計



(1)　ブリッジ識別子によるルートブリッジの選出

ルートブリッジは，ブリッジ識別子の最も小さい装置を選出します。通常，ルートブリッジにしたい装置のブリッジ優先度を最も小さい値（最高優先度）に設定します。図の例では，本装置 A がルートブリッジになるように設定します。本装置 B，本装置 C は指定ブリッジとなります。

また，ルートブリッジに障害が発生した場合に代替のルートブリッジとして動作するスイッチを本装置 B になるように設定します。本装置 C は最も低い優先度として設定します。

スパニングツリーのトポロジ設計では，図の例のようにネットワークのコアを担う装置をルートブリッジとし，代替のルートブリッジとしてコアを冗長化する構成をお勧めします。

(2)　通信経路の設計

ルートブリッジを選出したあと，各指定ブリッジからルートブリッジに到達するための通信経路を決定します。

(a)　パスコストによるルートポートの選出

本装置 B，本装置 C では，ルートブリッジに到達するための経路を最も小さいルートパスコスト値になるよう決定します。図の例は，すべてのポートがパスコスト 200000 としています。それぞれ直接接続したポートが最もルートパスコストが小さく，ルートポートとして選出します。

ルートパスコストの計算は，指定ブリッジからルートブリッジへ向かう経路で，各装置がルートブリッジの方向で送信するポートのパスコストの総和で比較します。例えば，本装置 C の本装置 B を経由する経路はパスコストが 400000 となりルートポートには選択されません。

パスコストは，ポートの速度が速いほど小さい値をデフォルト値に持ちます。また，ルートポートの選択にはルートブリッジまでのコストの総和で比較します。そのため，速度の速いポートや経由する装置の段数が少ない経路を優先して使用したい場合，通常はパスコスト値を変更する必要はありません。速度の遅いポートを速いポートより優先して経路として使用したい場合はコンフィグレーションで変更することによって通信したい経路を設計します。

(b)　指定ポート，非指定ポートの選出

本装置 B，本装置 C 間の接続はルートポート以外のポートでの接続になります。このようなポートではどれかのポートが非指定ポートとなって Blocking 状態になります。スパニングツリーは，このように片側が Blocking 状態となることでループを防止します。

指定ポート，非指定ポートは次のように選出します。

- 装置間でルートパスコストが小さい装置が指定ポート，大きい装置が非指定ポートになります。
- ルートパスコストが同一の場合，ブリッジ識別子の小さい装置が指定ポート，大きい装置が非指定ポートになります。

図の例では，ルートパスコストは同一です。ブリッジ優先度によって本装置 B が指定ポート，本装置 C が非指定ポートとなり，本装置 C が Blocking 状態となります。Blocking 状態になるポートを本装置 B にしたい場合は，パスコストを調整して本装置 B のルートパスコストが大きくなるように設定します。

6.1.6　STP 互換モード

(1)　概要

Rapid PVST+，Rapid STP，およびマルチプルスパニングツリーで，対向装置が PVST+または STP の場合，該当するポートは STP 互換モードで動作します。

STP 互換モードで動作すると，該当するポートで高速遷移をしなくなり，通信復旧に時間が掛かるようになります。

対向装置が Rapid PVST+，Rapid STP，およびマルチプルスパニングツリーに変わった場合，STP 互換モードから復旧し，再び高速遷移をするようになりますが，タイミングによって該当するポートと対向装置が STP 互換モードで動作し続けることがあります。

STP 互換モード復旧機能は，STP 互換モードで動作しているポートを強制的に復旧させ，正常に高速遷移ができるようにします。

(2)　復旧機能

運用コマンド clear spanning-tree detected-protocol を実行することで，STP 互換モードから強制的に復旧します。該当するポートのリンクタイプが point-to-point，shared のどちらの場合でも動作します。

(3)　自動復旧機能

該当するポートのリンクタイプが point-to-point の場合，STP 互換モード復旧機能が自動で動作します。

該当するポートが非指定ポートで STP 互換モードで動作した場合，該当するポートから RST BPDU または MST BPDU を送信することで，STP 互換モードを解除します。

該当するポートのリンクタイプが shared の場合，自動復旧モードが正しく動作できないため，自動復旧モードは動作しません。

6.1.7　スパニングツリー共通の注意事項

(1)　BCU 二重化構成で BPDU ガード機能を使用する場合について

BPDU ガード機能によってポートがダウンした場合，系切替が発生すると新運用系 BCU でそのポートがダウンしたままになります。この状態でコマンドによってスパニングツリーの状態を出力すると，BPDU ガードでポートがダウンしたのではなく，最初からポートがダウンしていたように出力されます。

(2)　他機能との共存

「1.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

6.2　スパニングツリー動作モードのコンフィグレーション

スパニングツリーの動作モードを設定します。

コンフィグレーションを設定しない状態で本装置を起動すると，スパニングツリーは停止状態です。

6.2.1　コンフィグレーションコマンド一覧

スパニングツリー動作モード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 6-7　コンフィグレーションコマンド一覧

コマンド名	説明
spanning-tree enable	スパニングツリーの動作を開始します。
spanning-tree mode	スパニングツリー機能の動作モードを設定します。
spanning-tree single mode	シングルスパニングツリーの STP と Rapid STP を選択します。
spanning-tree vlan mode	VLAN ごとに PVST+と Rapid PVST+を選択します。

6.2.2　動作モードの設定

スパニングツリーは装置の動作モードを設定することで各種スパニングツリーを使用できます。装置の動作モードに関するコマンドを次の表に示します。動作モードを設定しない場合，pvst モードで動作します。

動作モードに rapid-pvst を指定しても，シングルスパニングツリーのデフォルトは STP であることに注意してください。

表 6-8　スパニングツリー動作モードに関するコマンド

コマンド名	説明
spanning-tree enable	スパニングツリーの動作を開始します。
spanning-tree mode pvst	PVST+とシングルスパニングツリーを使用できます。デフォルトで PVST+が動作します。シングルスパニングツリーはデフォルトでは動作しません。
spanning-tree mode rapid-pvst	PVST+とシングルスパニングツリーを使用できます。デフォルトで高速スパニングツリーの Rapid PVST+が動作します。シングルスパニングツリーはデフォルトでは動作しません。
spanning-tree mode mst	マルチプルスパニングツリーが動作します。

(1)　スパニングツリーを動作させる設定

[設定のポイント]

スパニングツリーの動作を開始する場合に設定します。

[コマンドによる設定]

1.**(config)# spanning-tree enable**

スパニングツリーの動作を開始します。

(2) 動作モード pvst の設定

[設定のポイント]

装置の動作モードを pvst に設定します。ポート VLAN を作成すると，その VLAN で自動的に PVST+が動作します。VLAN ごとに Rapid PVST+に変更することもできます。

シングルスパニングツリーは spanning-tree single コマンドを設定すると動作します。その際, デフォルトでは STP で動作し，Rapid STP に変更することもできます。

[コマンドによる設定]

1. **(config)# spanning-tree mode pvst**

   スパニングツリーの動作モードを pvst に設定します。ポート VLAN で自動的に PVST+が動作します。

2. **(config)# spanning-tree vlan 10 mode rapid-pvst**

   VLAN 10 の動作モードを Rapid PVST+に変更します。ほかのポート VLAN は PVST+で動作し，VLAN 10 は Rapid PVST+で動作します。

3. **(config)# spanning-tree single**

   シングルスパニングツリーを動作させます。PVST+を使用していない VLAN に適用します。デフォルトでは STP で動作します。

4. **(config)# spanning-tree single mode rapid-stp**

   シングルスパニングツリーを Rapid STP に変更します。

(3) 動作モード rapid-pvst の設定

[設定のポイント]

装置の動作モードを rapid-pvst に設定します。ポート VLAN を作成すると，その VLAN で自動的に Rapid PVST+が動作します。VLAN ごとに PVST+に変更することもできます。

シングルスパニングツリーはデフォルトでは動作しないで，設定することで動作します。動作モードに rapid-pvst を指定しても，シングルスパニングツリーのデフォルトは STP であることに注意してください。

[コマンドによる設定]

1. **(config)# spanning-tree mode rapid-pvst**

   スパニングツリーの動作モードを rapid-pvst に設定します。ポート VLAN で自動的に Rapid PVST+が動作します。

2. **(config)# spanning-tree vlan 10 mode pvst**

   VLAN 10 の動作モードを PVST+に変更します。ほかのポート VLAN は Rapid PVST+で動作し，VLAN 10 は PVST+で動作します。

3. **(config)# spanning-tree single**

   シングルスパニングツリーを動作させます。PVST+を使用していない VLAN に適用します。デフォルトでは STP で動作します。

4. **(config)# spanning-tree single mode rapid-stp**

   シングルスパニングツリーを Rapid STP に変更します。

(4)　動作モード mst の設定

[設定のポイント]

マルチプルスパニングツリーを使用する場合，装置の動作モードを mst に設定します。マルチプルスパニングツリーはすべての VLAN に適用します。PVST+やシングルスパニングツリーとは併用できません。

[コマンドによる設定]

1. **(config)# spanning-tree mode mst**

マルチプルスパニングツリーを動作させます。

6.3　PVST+解説

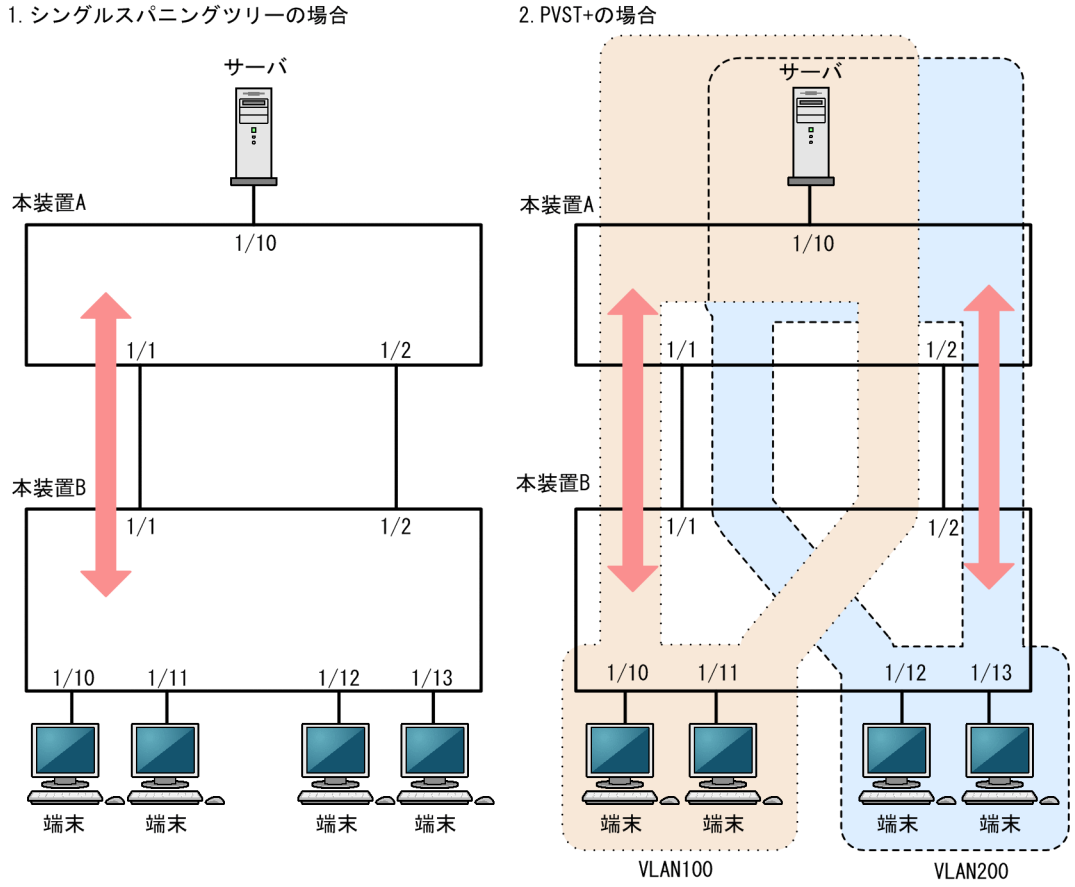
PVST+は，VLAN 単位にツリーを構築します。VLAN 単位にツリーを構築できるため，ロードバランシングが可能です。また，アクセスポートでは，シングルスパニングツリーで動作しているスイッチと接続できます。

6.3.1　PVST+によるロードバランシング

次の図に示すような本装置 A, B 間で冗長パスを組んだネットワークでシングルスパニングツリーを組んだ場合，各端末からサーバへのアクセスは本装置 A，B 間のポート 1 に集中します。そこで，複数の VLAN を組み，PVST+によって VLAN ごとに別々のトポロジとなるように設定することで冗長パスとして使用できるようになり，さらに負荷分散を図れます。ポート優先度によるロードバランシングの例を次の図に示します。

この例では，VLAN 100 に対してはポート 1/1 のポート優先度をポート 1/2 より高く設定し，逆に VLAN 200 に対しては 1/2 のポート優先度をポート 1/1 より高く設定することで，各端末からサーバに対するアクセスを VLAN ごとに負荷分散をしています。

図 6-5　PVST+によるロードバランシング



1. シングルスパニングツリーでは，ポート 1/2 は冗長パスとして通常は未使用のため，ポート 1/1 に負荷が集中します。
2. PVST+では，VLAN ごとに別々のトポロジとすることで本装置 A，B 間の負荷を分散できます。

6.3.2　アクセスポートの PVST+

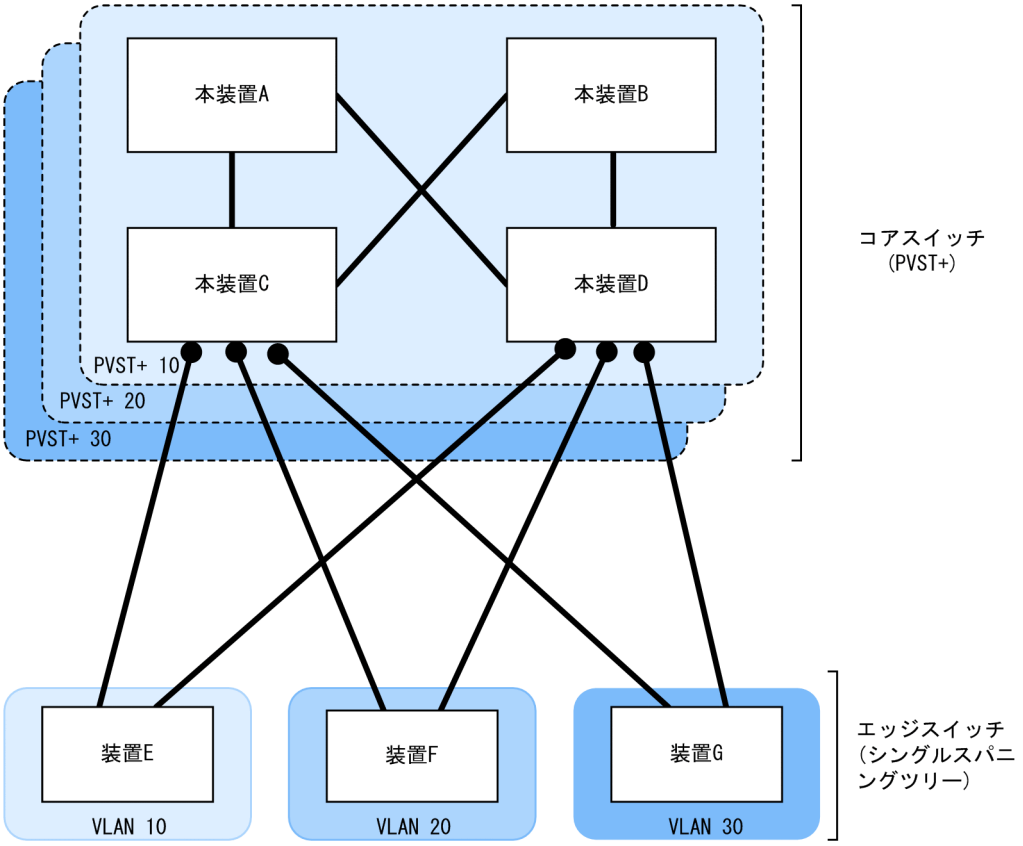
(1)　解説

シングルスパニングツリーを使用している装置，または装置で一つのツリーを持つシングルスパニングツリーに相当する機能をサポートしている装置（以降，単にシングルスパニングツリーと表記します）とPVST+を使用してネットワークを構築できます。シングルスパニングツリーで運用している装置をエッジスイッチ，本装置をコアスイッチに配置して使用します。このようなネットワークを構築することで，次のメリットがあります。

- エッジスイッチに障害が発生しても，ほかのエッジスイッチにトポロジ変更の影響が及ばない。
- コアスイッチ間でロードバランスができる。

シングルスパニングツリーとは，アクセスポートで接続できます。構成例を次の図に示します。この例では，エッジスイッチでシングルスパニングツリーを動作させ，コアスイッチで PVST+を動作させています。コアスイッチではエッジスイッチと接続するポートをアクセスポートとしています。各エッジスイッチはそれぞれ単一の VLAN を設定しています。

図 6-6　シングルスパニングツリーとの接続



（凡例）　●：アクセスポート

この例では，装置 E で障害が発生しても，コアスイッチ側を PVST+で動作させているため，装置 F および装置 G にトポロジ変更通知が波及しません。

(2)　アクセスポートでシングルスパニングツリーを混在させた場合

PVST+とシングルスパニングツリーを混在して設定している場合，アクセスポートでは，シングルスパニングツリーは停止状態（Disable）になります。

6.3.3　PVST+使用時の注意事項

(1)　他機能との共存

「1.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

(2)　VLAN 1 の PVST+とシングルスパニングツリーについて

シングルスパニングツリーと VLAN 1 の PVST+は同時に動作できません。シングルスパニングツリーを動作させると，VLAN 1 の PVST+は停止します。

また，シングルスパニングツリーを停止した場合に次の条件をどちらも満たすとき，VLAN 1 の PVST+が自動で動作を開始します。

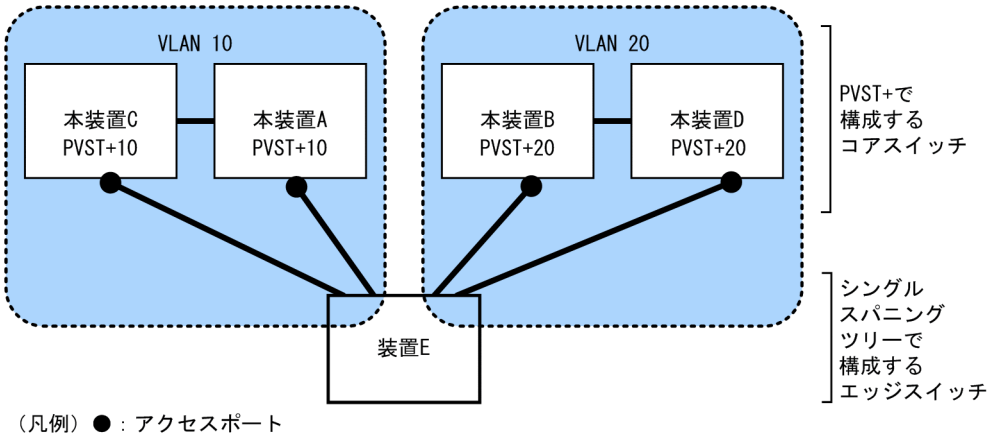
- VLAN 1 の PVST+を停止に設定していない
- PVST+の動作ツリー数が 250 未満である

(3)　禁止構成

本装置とシングルスパニングツリーで動作する装置は，単一のスパニングツリーで構成してください。複数のスパニングツリーで構成すると正しいトポロジになりません。

禁止構成の例を次の図に示します。この例では，装置 E のシングルスパニングツリーが複数の PVST+スパニングツリーとトポロジを構成している（装置 E は単一のスパニングツリーで構成されていない）ため，正しいトポロジになりません。

図 6-7　シングルスパニングツリーとの禁止構成例



（凡例）●：アクセスポート

6.4　PVST+のコンフィグレーション

6.4.1　コンフィグレーションコマンド一覧

PVST+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 6-9　コンフィグレーションコマンド一覧

コマンド名	説明
spanning-tree cost	ポートごとにパスコストのデフォルト値を設定します。
spanning-tree pathcost method	ポートごとにパスコストに使用する値の幅のデフォルト値を設定します。
spanning-tree port-priority	ポートごとにポート優先度のデフォルト値を設定します。
spanning-tree vlan	PVST+の動作，停止を設定します。
spanning-tree vlan cost	VLAN ごとにパスコスト値を設定します。
spanning-tree vlan forward-time	ポートの状態遷移に必要な時間を設定します。
spanning-tree vlan hello-time	BPDU の送信間隔を設定します。
spanning-tree vlan max-age	送信 BPDU の最大有効時間を設定します。
spanning-tree vlan pathcost method	VLAN ごとにパスコストに使用する値の幅を設定します。
spanning-tree vlan port-priority	VLAN ごとにポート優先度を設定します。
spanning-tree vlan priority	ブリッジ優先度を設定します。
spanning-tree vlan transmission-limit	hello-time 当たりに送信できる最大 BPDU 数を設定します。

6.4.2　PVST+の設定

[設定のポイント]

動作モード pvst，rapid-pvst を設定するとポート VLAN で自動的に PVST+が動作しますが，VLAN ごとにモードの変更や PVST+の動作，停止を設定できます。停止する場合は，no spanning-tree vlan コマンドを使用します。

VLAN を作成するときにその VLAN で PVST+を動作させたくない場合，no spanning-tree vlan コマンドを VLAN 作成前にあらかじめ設定しておくことができます。

[コマンドによる設定]

1. **(config)# no spanning-tree vlan 20**

   VLAN 20 の PVST+の動作を停止します。

2. **(config)# spanning-tree vlan 20**

   停止した VLAN 20 の PVST+を動作させます。

[注意事項]

- PVST+はコンフィグレーションに表示がないときは自動的に動作しています。no spanning-tree vlan コマンドで停止すると，停止状態であることがコンフィグレーションで確認できます。

- PVST+は最大 250 個のポート VLAN まで動作します。それ以上のポート VLAN を作成しても自動的には動作しません。

6.4.3 PVST+のトポロジ設定

(1) ブリッジ優先度の設定

ブリッジ優先度は，ルートブリッジを決定するためのパラメータです。トポロジを設計する際に，ルートブリッジにしたい装置を最高の優先度に設定し，ルートブリッジに障害が発生したときのために，次にルートブリッジにしたい装置を 2 番目の優先度に設定します。

[設定のポイント]

ブリッジ優先度は値が小さいほど高い優先度となり，最も小さい値を設定した装置がルートブリッジになります。ルートブリッジはブリッジ優先度と装置の MAC アドレスから成るブリッジ識別子で判定するため，本パラメータを設定しない場合は装置の MAC アドレスが最も小さい装置がルートブリッジになります。

[コマンドによる設定]

1. **(config)# spanning-tree vlan 10 priority 4096**

   VLAN 10 の PVST+のブリッジ優先度を 4096 に設定します。

(2) パスコストの設定

パスコストは通信経路を決定するためのパラメータです。スパニングツリーのトポロジ設計では，ブリッジ優先度の決定後に，指定ブリッジのルートポート（指定ブリッジからルートブリッジへの通信経路）を本パラメータで設計します。

[設定のポイント]

パスコスト値は指定ブリッジの各ポートに設定します。小さい値で設定することによってルートポートに選択されやすくなります。設定しない場合，ポートの速度ごとに異なるデフォルト値になり，高速なポートほどルートポートに選択されやすくなります。

パスコストは，速度の遅いポートを速いポートより優先して経路として使用したい場合に設定します。速いポートを優先したトポロジとする場合は設定する必要はありません。

パスコスト値には short（16bit 値），long（32bit 値）の 2 種類があり，トポロジの全体で合わせる必要があります。10 ギガビットイーサネット以上の回線速度を使用する場合は long（32bit 値）を使用することをお勧めします。デフォルトでは short（16bit 値）で動作します。イーサネットインタフェースの速度による自動的な設定は，short（16bit 値）か long（32bit 値）かで設定内容が異なります。パスコストのデフォルト値を次の表に示します。

表 6-10 パスコストのデフォルト値

ポートの速度	パスコストのデフォルト値	
	short（16bit 値）	long（32bit 値）
10Mbit/s	100	2000000
100Mbit/s	19	200000
1Gbit/s	4	20000
10Gbit/s	2	2000

ポートの速度	パスコストのデフォルト値	
	short（16bit 値）	long（32bit 値）
40Gbit/s	2	500
100Gbit/s	2	200

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   (config-if)# spanning-tree cost 100
   (config-if)# exit
   ポート 1/1 のパスコストを 100 に設定します。
2. **(config)# spanning-tree pathcost method long**
   (config)# interface gigabitethernet 1/1
   (config-if)# spanning-tree vlan 10 cost 200000
   long（32bit 値）のパスコストを使用するように設定したあとで，ポート 1/1 の VLAN 10 をコスト値 200000 に変更します。ポート 1/1 では VLAN 10 だけパスコスト 200000 となり，そのほかの VLAN は 100 で動作します。

[注意事項]

リンクアグリゲーションを使用する場合，チャネルグループのパスコストは，チャネルグループ内の全集約ポートの合計ではなく，チャネルグループ内の集約ポートのうち最低速度の回線の値となります。

(3)　ポート優先度の設定

ポート優先度は 2 台の装置間での接続をスパニングツリーで冗長化し，パスコストも同じ値とする場合に，どちらのポートを使用するかを決定するために設定します。

2 台の装置間の接続を冗長化する機能にはリンクアグリゲーションがあり，通常はリンクアグリゲーションを使用することをお勧めします。接続する対向の装置がリンクアグリゲーションをサポートしていないで，スパニングツリーで冗長化する必要がある場合に本機能を使用してください。

[設定のポイント]

ポート優先度は値が小さいほど高い優先度となります。2 台の装置間で冗長化している場合に，ルートブリッジに近い側の装置でポート優先度の高いポートが通信経路として使われます。本パラメータを設定しない場合はポート番号の小さいポートが優先されます。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   (config-if)# spanning-tree port-priority 64
   (config-if)# exit
   ポート 1/1 のポート優先度を 64 に設定します。
2. **(config)# interface gigabitethernet 1/1**
   (config-if)# spanning-tree vlan 10 port-priority 144
   ポート 1/1 の VLAN 10 をポート優先度 144 に変更します。ポート 1/1 では VLAN 10 だけポート優先度 144 となり，そのほかの VLAN は 64 で動作します。

6.4.4 PVST+のパラメータ設定

各パラメータは「2×（forward-time－1）≧max-age≧2×（hello-time + 1)」という関係を満たすように設定する必要があります。パラメータを変える場合は，スパニングツリーを構築するすべての装置でパラメータを合わせる必要があります。

(1) BPDU の送信間隔の設定

BPDU の送信間隔は，短くした場合はトポロジ変更を検知しやすくなります。長くした場合はトポロジ変更の検知までに時間が掛かるようになる一方で，BPDU トラフィックや本装置のスパニングツリープログラムの負荷を軽減できます。

[設定のポイント]

設定しない場合，2 秒間隔で BPDU を送信します。通常は設定する必要はありません。

[コマンドによる設定]

1. **(config)# spanning-tree vlan 10 hello-time 3**

   VLAN 10 の PVST+の BPDU 送信間隔を 3 秒に設定します。

[注意事項]

BPDU の送信間隔を短くすると，トポロジ変更を検知しやすくなる一方で BPDU トラフィックが増加することによってスパニングツリープログラムの負荷が増加します。本パラメータをデフォルト値（2 秒）より短くすることでタイムアウトのメッセージ出力やトポロジ変更が頻発する場合は，デフォルト値に戻して使用してください。

(2) 送信する最大 BPDU 数の設定

スパニングツリーでは，CPU 負荷の増大を抑えるために，hello-time（BPDU 送信間隔）当たりに送信する最大 BPDU 数を決められます。トポロジ変更が連続的に発生すると，トポロジ変更を通知，収束するために大量の BPDU が送信され，BPDU トラフィックの増加，CPU 負荷の増大につながります。送信する BPDU の最大数を制限することでこれらを抑えます。

[設定のポイント]

設定しない場合，hello-time（BPDU 送信間隔）当たりの最大 BPDU 数は 3 で動作します。本パラメータのコンフィグレーションは Rapid PVST+だけ有効であり，PVST+は 3（固定）で動作します。通常は設定する必要はありません。

[コマンドによる設定]

1. **(config)# spanning-tree vlan 10 transmission-limit 5**

   VLAN 10 の Rapid PVST+の hello-time 当たりの最大送信 BPDU 数を 5 に設定します。

(3) BPDU の最大有効時間の設定

ルートブリッジから送信する BPDU の最大有効時間を設定します。BPDU のカウンタは装置を経由するたびに増加して，最大有効時間を超えた BPDU は無効な BPDU となって無視されます。

[設定のポイント]

最大有効時間を大きく設定することで，多くの装置に BPDU が届くようになります。設定しない場合，最大有効時間は 20 で動作します。

[コマンドによる設定]

1.(config)# spanning-tree vlan 10 max-age 25

VLAN 10 の PVST+の BPDU の最大有効時間を 25 に設定します。

(4)　状態遷移時間の設定

PVST+モードまたは Rapid PVST+モードでタイマによる動作となる場合，ポートの状態が一定時間ごとに遷移します。PVST+モードの場合は Blocking から Listening, Learning, Forwarding と遷移し, Rapid PVST+モードの場合は Discarding から Learning，Forwarding と遷移します。この状態遷移に必要な時間を設定できます。小さい値を設定すると，より早く Forwarding 状態に遷移できます。

[設定のポイント]

設定しない場合, 状態遷移時間は 15 秒で動作します。本パラメータを短い時間に変更する場合, BPDU の最大有効時間（max-age），送信間隔（hello-time）との関係が「2×（forward-time－1）≧max-age≧2×（hello-time ＋ 1)」を満たすように設定してください。

[コマンドによる設定]

1.(config)# spanning-tree vlan 10 forward-time 10

VLAN 10 の PVST+の状態遷移時間を 10 に設定します。

6.5　PVST+のオペレーション

6.5.1　運用コマンド一覧

PVST+の運用コマンド一覧を次の表に示します。

表 6-11　運用コマンド一覧

コマンド名	説明
show spanning-tree	スパニングツリー情報を表示します。
show spanning-tree statistics	スパニングツリーの統計情報を表示します。
clear spanning-tree statistics	スパニングツリーの統計情報をクリアします。
clear spanning-tree detected-protocol	スパニングツリーの STP 互換モードを強制回復します。
show spanning-tree port-count	スパニングツリーの収容数を表示します。
restart spanning-tree	スパニングツリープログラムを再起動します。
dump protocols spanning-tree	スパニングツリーで採取している詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。

6.5.2　PVST+の状態の確認

PVST+の情報は show spanning-tree コマンドで確認してください。Mode で PVST+，Rapid PVST+の動作モードを確認できます。トポロジが正しく構築されていることを確認するためには，次の項目を確認してください。

- Root Bridge ID の内容が正しいこと
- Port Information の Status，Role が正しいこと

show spanning-tree コマンドの実行結果を次の図に示します。

図 6-8　show spanning-tree コマンドの実行結果（PVST+の情報）

```
> show spanning-tree vlan 1
Date 20XX/03/04 11:39:43 UTC
VLAN 1              PVST+ Spanning Tree:Enabled  Mode:PVST+
  Bridge ID        Priority:32769       MAC Address:0012.e205.0900
    Bridge Status:Designated
  Root Bridge ID   Priority:32769       MAC Address:0012.e201.0900
    Root Cost:1000
    Root Port:1/1
  Port Information
    1/1        Up    Status:Forwarding  Role:Root
    1/2        Up    Status:Forwarding  Role:Designated
    1/3        Up    Status:Blocking    Role:Alternate
    1/4        Down  Status:Disabled    Role:-
    1/10       Up    Status:Forwarding  Role:Designated PortFast
    1/11       Up    Status:Forwarding  Role:Designated PortFast
    1/12       Up    Status:Forwarding  Role:Designated PortFast
>
```

6.6　シングルスパニングツリー解説

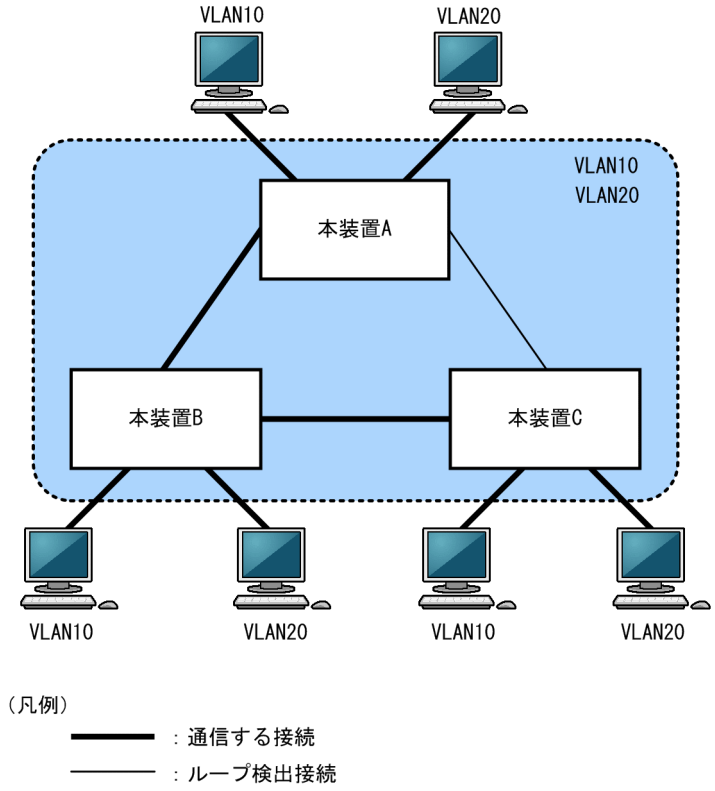
シングルスパニングツリーは装置全体を対象としてトポロジを構築します。

6.6.1　概要

シングルスパニングツリーは，一つのスパニングツリーですべての VLAN のループを回避できます。VLAN ごとに制御する PVST+よりも多くの VLAN を扱えます。

シングルスパニングツリーによるネットワーク構成を次の図に示します。この図では，本装置 A，B，C に対して，VLAN 10 および VLAN 20 を設定し，すべての VLAN で PVST+を停止しシングルスパニングツリーを適用しています。すべての VLAN で一つのトポロジを使用して通信します。

図 6-9　シングルスパニングツリーによるネットワーク構成



6.6.2　PVST+との併用

PVST+が動作できる VLAN 数は 250 個であり，それ以上の VLAN では使用できません。シングルスパニングツリーを使用することで，PVST+を使用しながらこれらの VLAN にもスパニングツリーを適用できます。

シングルスパニングツリーは，PVST+が動作していないすべての VLAN に対して適用します。シングルスパニングツリーを PVST+と併用したときに，シングルスパニングツリーの対象になる VLAN を次の表に示します。

表 6-12　シングルスパニングツリー対象の VLAN

項目	VLAN
PVST+対象の VLAN	• PVST+が動作している VLAN 最大 250 個のポート VLAN は自動的に PVST+が動作します。
シングルスパニングツリー対象の VLAN	• 251 個目以上のポート VLAN • PVST+を停止（コンフィグレーションコマンド no spanning-tree vlan で指定）している VLAN

6.6.3　シングルスパニングツリー使用時の注意事項

(1)　他機能との共存

「1.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

(2)　VLAN 1 の PVST+とシングルスパニングツリーについて

シングルスパニングツリーと VLAN 1 の PVST+は同時に動作できません。シングルスパニングツリーを動作させると，VLAN 1 の PVST+は停止します。

また，シングルスパニングツリーを停止した場合に次の条件をどちらも満たすとき，VLAN 1 の PVST+が自動で動作を開始します。

- VLAN 1 の PVST+を停止に設定していない
- PVST+の動作ツリー数が 250 未満である

6.7　シングルスパニングツリーのコンフィグレーション

6.7.1　コンフィグレーションコマンド一覧

シングルスパニングツリ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 6-13　コンフィグレーションコマンド一覧

コマンド名	説明
spanning-tree cost	ポートごとにパスコストのデフォルト値を設定します。
spanning-tree pathcost method	ポートごとにパスコストに使用する値の幅のデフォルト値を設定します。
spanning-tree port-priority	ポートごとにポート優先度のデフォルト値を設定します。
spanning-tree single	シングルスパニングツリーの動作，停止を設定します。
spanning-tree single cost	シングルスパニングツリーのパスコストを設定します。
spanning-tree single forward-time	ポートの状態遷移に必要な時間を設定します。
spanning-tree single hello-time	BPDU の送信間隔を設定します。
spanning-tree single max-age	送信 BPDU の最大有効時間を設定します。
spanning-tree single pathcost method	シングルスパニングツリーのパスコストに使用する値の幅を設定します。
spanning-tree single port-priority	シングルスパニングツリーのポート優先度を設定します。
spanning-tree single priority	ブリッジ優先度を設定します。
spanning-tree single transmission-limit	hello-time 当たりに送信できる最大 BPDU 数を設定します。

6.7.2　シングルスパニングツリーの設定

[設定のポイント]

シングルスパニングツリーの動作，停止を設定します。シングルスパニングツリーは，動作モード pvst, rapid-pvst を設定しただけでは動作しません。spanning-tree single コマンドを設定すると動作を開始します。

VLAN 1 の PVST+とシングルスパニングツリーは同時に使用できません。シングルスパニングツリーを設定すると VLAN 1 の PVST+は停止します。

[コマンドによる設定]

1. **(config)# spanning-tree single**

シングルスパニングツリーを動作させます。この設定によって，VLAN 1 の PVST+が動作している場合は動作を停止して，VLAN 1 はシングルスパニングツリーの対象となります。

6.7.3　シングルスパニングツリーのトポロジ設定

(1)　ブリッジ優先度の設定

ブリッジ優先度は，ルートブリッジを決定するためのパラメータです。トポロジを設計する際に，ルートブリッジにしたい装置を最高の優先度に設定し，ルートブリッジに障害が発生したときのために，次にルートブリッジにしたい装置を 2 番目の優先度に設定します。

[設定のポイント]

ブリッジ優先度は値が小さいほど高い優先度となり，最も小さい値を設定した装置がルートブリッジになります。ルートブリッジはブリッジ優先度と装置の MAC アドレスから成るブリッジ識別子で判定するため，本パラメータを設定しない場合は装置の MAC アドレスが最も小さい装置がルートブリッジになります。

[コマンドによる設定]

1. **(config)# spanning-tree single priority 4096**

   シングルスパニングツリーのブリッジ優先度を 4096 に設定します。

(2)　パスコストの設定

パスコストは通信経路を決定するためのパラメータです。スパニングツリーのトポロジ設計では，ブリッジ優先度の決定後に，指定ブリッジのルートポート（指定ブリッジからルートブリッジへの通信経路）を本パラメータで設計します。

[設定のポイント]

パスコスト値は指定ブリッジの各ポートに設定します。小さい値で設定することによってルートポートに選択されやすくなります。設定しない場合，ポートの速度ごとに異なるデフォルト値になり，高速なポートほどルートポートに選択されやすくなります。

パスコストは，速度の遅いポートを速いポートより優先して経路として使用したい場合に設定します。速いポートを優先したトポロジとする場合は設定する必要はありません。

パスコスト値には short（16bit 値），long（32bit 値）の 2 種類があり，トポロジの全体で合わせる必要があります。10 ギガビットイーサネット以上の回線速度を使用する場合は long（32bit 値）を使用することをお勧めします。デフォルトでは short（16bit 値）で動作します。イーサネットインタフェースの速度による自動的な設定は，short（16bit 値）か long（32bit 値）かで設定内容が異なります。パスコストのデフォルト値を次の表に示します。

表 6-14　パスコストのデフォルト値

ポートの速度	パスコストのデフォルト値	
	short（16bit 値）	long（32bit 値）
10Mbit/s	100	2000000
100Mbit/s	19	200000
1Gbit/s	4	20000
10Gbit/s	2	2000
40Gbit/s	2	500
100Gbit/s	2	200

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   (config-if)# spanning-tree cost 100
   (config-if)# exit
   ポート 1/1 のパスコストを 100 に設定します。
2. **(config)# spanning-tree pathcost method long**
   (config)# interface gigabitethernet 1/1
   (config-if)# spanning-tree single cost 200000
   long（32bit 値）のパスコストを使用するように設定したあとで，シングルスパニングツリーのポート 1/1 のパスコストを 200000 に変更します。ポート 1/1 ではシングルスパニングツリーだけパスコスト 200000 となり，同じポートで使用している PVST+は 100 で動作します。

[注意事項]

リンクアグリゲーションを使用する場合，チャネルグループのパスコストは，チャネルグループ内の全集約ポートの合計ではなく，チャネルグループ内の集約ポートのうち最低速度の回線の値となります。

(3)　ポート優先度の設定

ポート優先度は 2 台の装置間での接続をスパニングツリーで冗長化し，パスコストも同じ値とする場合に，どちらのポートを使用するかを決定するために設定します。

2 台の装置間の接続を冗長化する機能にはリンクアグリゲーションがあり，通常はリンクアグリゲーションを使用することをお勧めします。接続する対向の装置がリンクアグリゲーションをサポートしていないで，スパニングツリーで冗長化する必要がある場合に本機能を使用してください。

[設定のポイント]

ポート優先度は値が小さいほど高い優先度となります。2 台の装置間で冗長化している場合に，ルートブリッジに近い側の装置でポート優先度の高いポートが通信経路として使われます。本パラメータを設定しない場合はポート番号の小さいポートが優先されます。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   (config-if)# spanning-tree port-priority 64
   (config-if)# exit
   ポート 1/1 のポート優先度を 64 に設定します。
2. **(config)# interface gigabitethernet 1/1**
   (config-if)# spanning-tree single port-priority 144
   シングルスパニングツリーのポート 1/1 のポート優先度を 144 に変更します。ポート 1/1 ではシングルスパニングツリーだけポート優先度 144 となり，同じポートで使用している PVST+は 64 で動作します。

6.7.4　シングルスパニングツリーのパラメータ設定

各パラメータは「2×（forward-time－1）≧max-age≧2×（hello-time ＋ 1)」という関係を満たすように設定する必要があります。パラメータを変える場合は，トポロジ全体でパラメータを合わせる必要があります。

(1) BPDU の送信間隔の設定

BPDU の送信間隔は，短くした場合はトポロジ変更を検知しやすくなります。長くした場合はトポロジ変更の検知までに時間が掛かるようになる一方で，BPDU トラフィックや本装置のスパニングツリープログラムの負荷を軽減できます。

[設定のポイント]

設定しない場合，2 秒間隔で BPDU を送信します。通常は設定する必要はありません。

[コマンドによる設定]

1. **(config)# spanning-tree single hello-time 3**
   シングルスパニングツリーの BPDU 送信間隔を 3 秒に設定します。

[注意事項]

BPDU の送信間隔を短くすると，トポロジ変更を検知しやすくなる一方で BPDU トラフィックが増加することによってスパニングツリープログラムの負荷が増加します。本パラメータをデフォルト値（2 秒）より短くすることでタイムアウトのメッセージ出力やトポロジ変更が頻発する場合は，デフォルト値に戻して使用してください。

(2) 送信する最大 BPDU 数の設定

スパニングツリーでは，CPU 負荷の増大を抑えるために，hello-time（BPDU 送信間隔）当たりに送信する最大 BPDU 数を決められます。トポロジ変更が連続的に発生すると，トポロジ変更を通知，収束するために大量の BPDU が送信され，BPDU トラフィックの増加，CPU 負荷の増大につながります。送信する BPDU の最大数を制限することでこれらを抑えます。

[設定のポイント]

設定しない場合，hello-time（BPDU 送信間隔）当たりの最大 BPDU 数は 3 で動作します。本パラメータのコンフィグレーションは Rapid STP だけ有効であり，STP は 3（固定）で動作します。通常は設定する必要はありません。

[コマンドによる設定]

1. **(config)# spanning-tree single transmission-limit 5**
   シングルスパニングツリーの hello-time 当たりの最大送信 BPDU 数を 5 に設定します。

(3) BPDU の最大有効時間

ルートブリッジから送信する BPDU の最大有効時間を設定します。BPDU のカウンタは装置を経由するたびに増加して，最大有効時間を超えた BPDU は無効な BPDU となって無視されます。

[設定のポイント]

最大有効時間を大きく設定することで，多くの装置に BPDU が届くようになります。設定しない場合，最大有効時間は 20 で動作します。

[コマンドによる設定]

1. **(config)# spanning-tree single max-age 25**
   シングルスパニングツリーの BPDU の最大有効時間を 25 に設定します。

(4)　状態遷移時間の設定

STP モードまたは Rapid STP モードでタイマによる動作となる場合，ポートの状態が一定時間ごとに遷移します。STP モードの場合は Blocking から Listening，Learning，Forwarding と遷移し，Rapid STP モードの場合は Discarding から Learning，Forwarding と遷移します。この状態遷移に必要な時間を設定できます。小さい値を設定すると，より早く Forwarding 状態に遷移できます。

[設定のポイント]

設定しない場合，状態遷移時間は 15 秒で動作します。本パラメータを短い時間に変更する場合，BPDU の最大有効時間（max-age），送信間隔（hello-time）との関係が「2×（forward-time－1）≧max-age≧2×（hello-time ＋ 1)」を満たすように設定してください。

[コマンドによる設定]

1. **(config)# spanning-tree single forward-time 10**
   シングルスパニングツリーの状態遷移時間を 10 に設定します。

6.8　シングルスパニングツリーのオペレーション

6.8.1　運用コマンド一覧

シングルスパニングツリーの運用コマンド一覧を次の表に示します。

表 6-15　運用コマンド一覧

コマンド名	説明
show spanning-tree	スパニングツリー情報を表示します。
show spanning-tree statistics	スパニングツリーの統計情報を表示します。
clear spanning-tree statistics	スパニングツリーの統計情報をクリアします。
clear spanning-tree detected-protocol	スパニングツリーの STP 互換モードを強制回復します。
show spanning-tree port-count	スパニングツリーの収容数を表示します。
restart spanning-tree	スパニングツリープログラムを再起動します。
dump protocols spanning-tree	スパニングツリーで採取している詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。

6.8.2　シングルスパニングツリーの状態の確認

シングルスパニングツリーの情報は show spanning-tree コマンドで確認してください。Mode で STP，Rapid STP の動作モードを確認できます。トポロジが正しく構築されていることを確認するためには，次の項目を確認してください。

- Root Bridge ID の内容が正しいこと
- Port Information の Status，Role が正しいこと

show spanning-tree コマンドの実行結果を次の図に示します。

図 6-10　show spanning-tree コマンドの実行結果（シングルスパニングツリーの情報）

```
> show spanning-tree single
Date 20XX/03/04 11:42:06 UTC
Single Spanning Tree:Enabled  Mode:Rapid STP
  Bridge ID        Priority:32768       MAC Address:0012.e205.0900
    Bridge Status:Designated
  Root Bridge ID   Priority:32768       MAC Address:0012.e205.0900
    Root Cost:0
    Root Port:-
  Port Information
    1/1        Up    Status:Forwarding  Role:Root
    1/2        Up    Status:Forwarding  Role:Designated
    1/3        Up    Status:Blocking    Role:Alternate
    1/4        Down  Status:Disabled    Role:-
    1/10       Up    Status:Forwarding  Role:Designated PortFast
    1/11       Up    Status:Forwarding  Role:Designated PortFast
    1/12       Up    Status:Forwarding  Role:Designated PortFast
>
```

6.9　マルチプルスパニングツリー解説

6.9.1　概要

マルチプルスパニングツリーには，次に示す特長があります。

- MST インスタンスによって，ロードバランシングを可能にしています。
- MST リージョンによって，大規模なネットワーク構成を中小構成に分割することでネットワーク設計が容易になります。

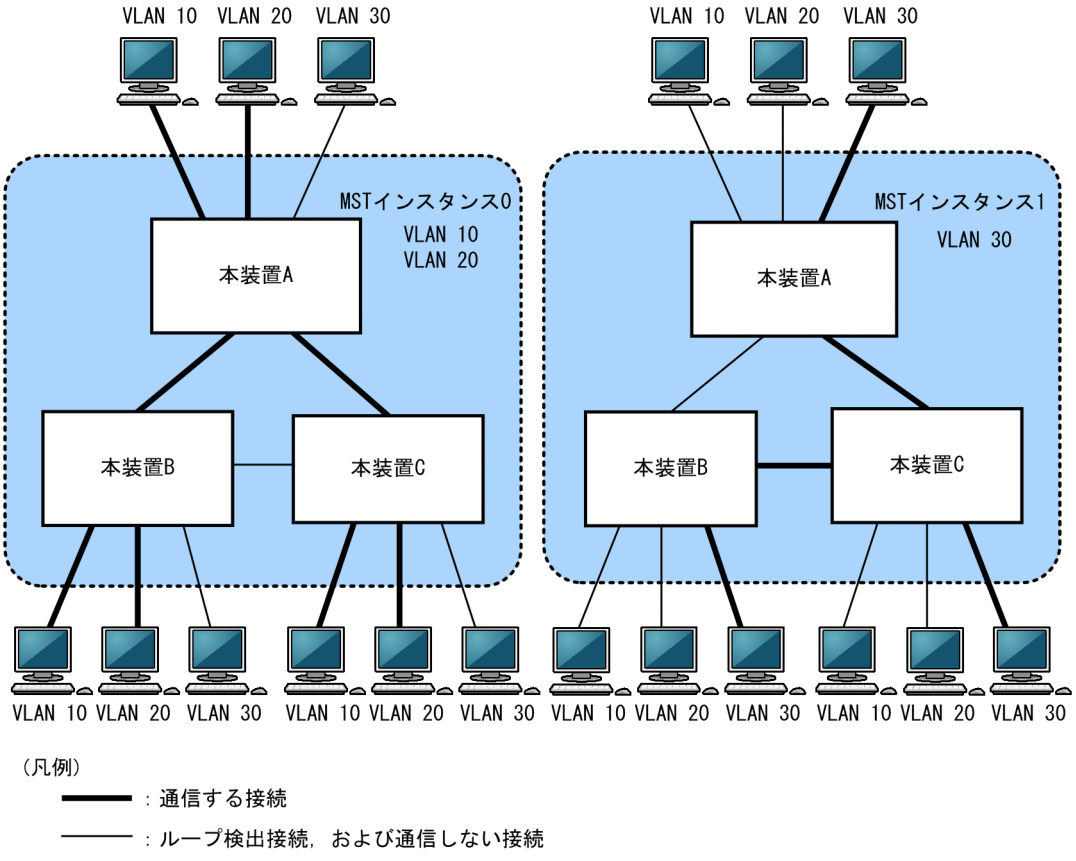
以降，これらを実現するためのマルチプルスパニングツリーの機能概要を説明します。

(1)　MST インスタンス

マルチプルスパニングツリーは，複数の VLAN をまとめた MST インスタンス（MSTI：Multiple Spanning Tree Instance）というグループごとにスパニングツリーを構築でき，MST インスタンスごとにロードバランシングができます。PVST+によるロードバランシングでは，VLAN 数分のツリーが必要でしたが，マルチプルスパニングツリーでは MST インスタンスによって，計画したロードバランシングに従ったツリーだけで済みます。その結果，PVST+とは異なり VLAN 数の増加に比例した CPU 負荷およびネットワーク負荷の増加を抑えられます。本装置では最大 16 個の MST インスタンスが設定できます。

MST インスタンスイメージを次の図に示します。

図 6-11　MST インスタンスイメージ



この例では，ネットワーク上に二つのインスタンスを設定して，ロードバランシングをしています。インスタンス 0 には，VLAN 10 および VLAN 20 を，インスタンス 1 には VLAN 30 を所属させています。

(2) MST リージョン

マルチプルスパニングツリーでは，複数の装置をグルーピングして MST リージョンとして扱えます。同一の MST リージョンに所属させるには，リージョン名，リビジョン番号，MST インスタンス ID と VLAN の対応を同じにする必要があります。これらはコンフィグレーションで設定します。ツリーの構築は MST リージョン間と MST リージョン内で別々に行い，MST リージョン内のトポロジは MST インスタンス単位に構築できます。

次に，MST リージョン間や MST リージョン内で動作するスパニングツリーについて説明します。

- CST

  CST（Common Spanning Tree）は，MST リージョン間や，シングルスパニングツリーを使用しているブリッジ間の接続を制御するスパニングツリーです。このトポロジはシングルスパニングツリーと同様で物理ポートごとに計算するので，ロードバランシングはできません。

- IST

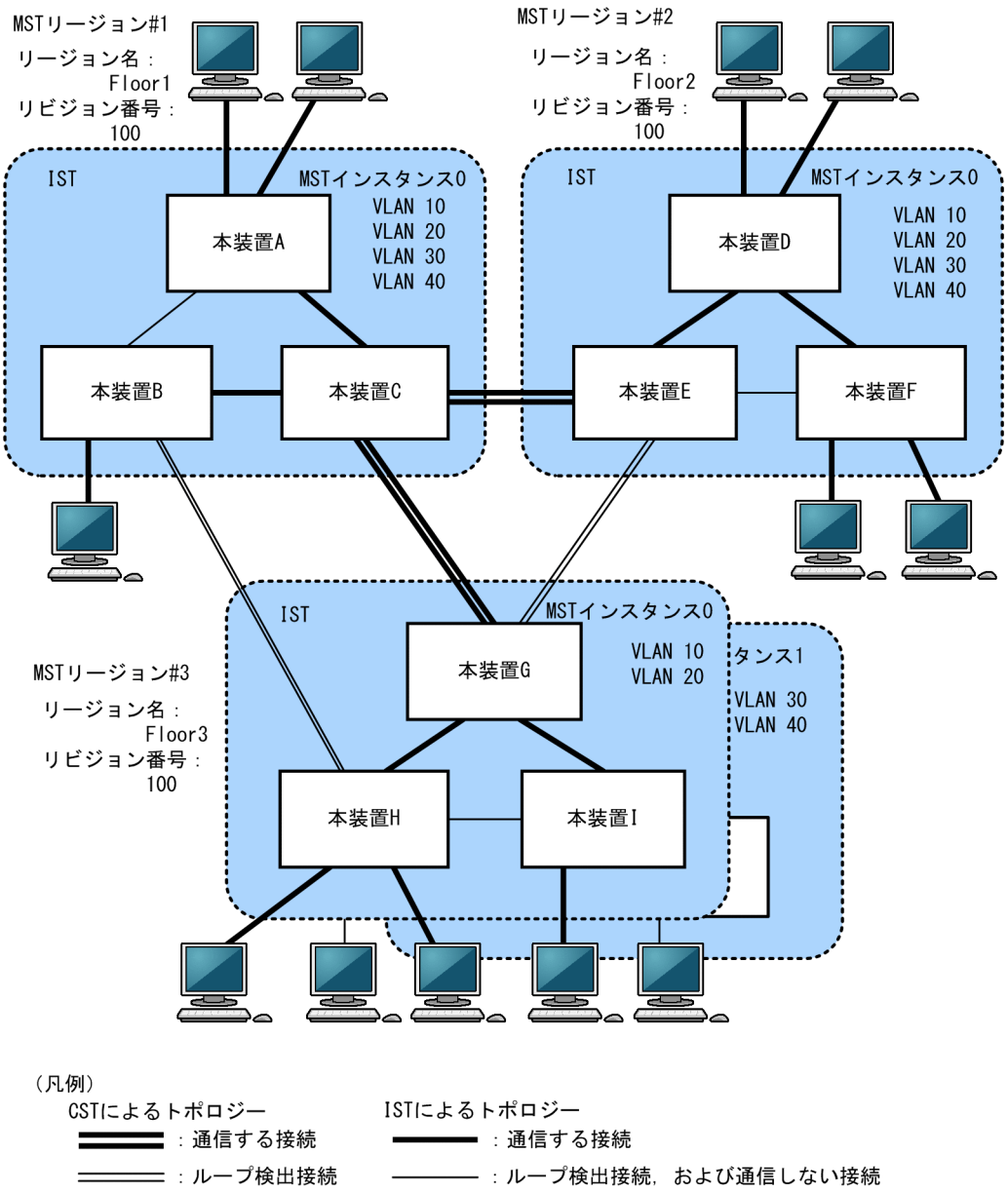
  IST（Internal Spanning Tree）は，MST リージョン外と接続するために，MST リージョン内で Default 動作するトポロジのことを指し，MST インスタンス ID 0 が割り当てられます。MST リージョン外と接続しているポートを境界ポートと呼びます。また，リージョン内，リージョン間で MST BPDU を送受信する唯一の MST インスタンスとなります。全 MST インスタンスのトポロジ情報は，MST BPDU にカプセル化して通知します。

- CIST

  CIST（Common and Internal Spanning Tree）は，IST と CST とを合わせたトポロジを指します。

マルチプルスパニングツリー概要を次の図に示します。

図 6-12　マルチプルスパニングツリー概要

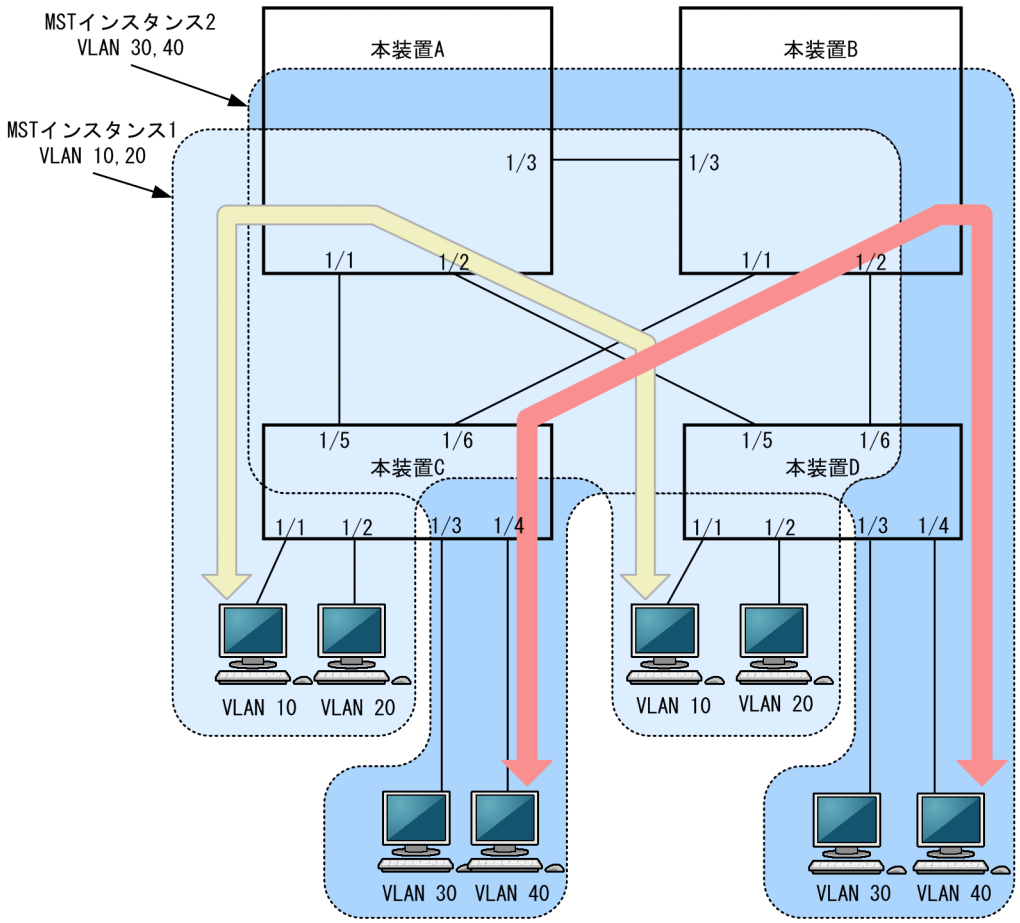


6.9.2　マルチプルスパニングツリーのネットワーク設計

(1)　MST インスタンス単位のロードバランシング構成

マルチプルスパニングツリーでは，MST インスタンス単位にロードバランシングができます。ロードバランシング構成の例を次の図に示します。この例では，VLAN 10，20 を MST インスタンス 1 に，VLAN 30，40 を MST インスタンス 2 に設定して，本装置 C と本装置 D に接続している VLAN 10 の端末の通信経路と VLAN 40 の端末の通信経路の二つでロードバランシングをしています。マルチプルスパニングツリーでは，この例のように四つの VLAN であっても二つのツリーだけを管理することでロードバランシングができます。

図 6-13　マルチプルスパニングツリーのロードバランシング構成

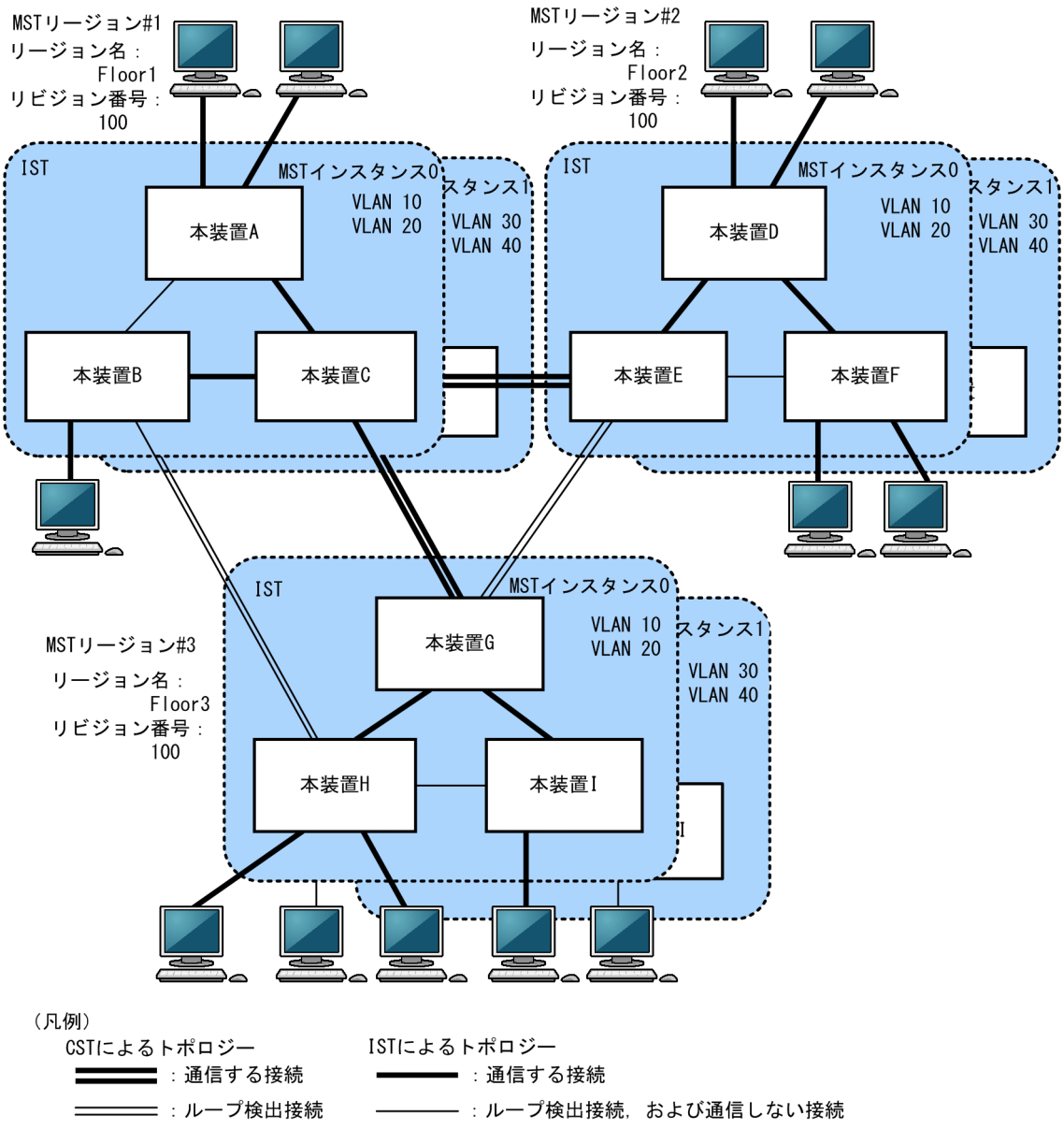


(2)　MST リージョンによるネットワーク設計

ネットワーク構成が大規模になるに従ってネットワーク設計は複雑になりますが，MST リージョンによって中小規模構成に分割することで，例えば，ロードバランシングを MST リージョン単位に実施できるため，ネットワーク設計が容易になります。

MST リージョンによるネットワーク設計例を次の図に示します。この例では，装置 A，B，C を MST リージョン#1，装置 D，E，F を MST リージョン#2，本装置 G，H，I を MST リージョン#3 に設定して，ネットワークを三つの MST リージョンに分割しています。

図 6-14　MST リージョンによるネットワーク構成



6.9.3　ほかのスパニングツリーとの互換性

(1)　シングルスパニングツリーとの互換性

マルチプルスパニングツリーは，シングルスパニングツリーで動作する STP，Rapid STP と互換性があります。これらと接続した場合，別の MST リージョンと判断して接続します。Rapid STP と接続した場合は高速な状態遷移をします。

(2)　PVST+との互換性

マルチプルスパニングツリーは，PVST+と互換性はありません。ただし，PVST+が動作している装置のアクセスポートはシングルスパニングツリーと同等の動作をするため，マルチプルスパニングツリーと接続できます。

6.9.4　マルチプルスパニングツリー使用時の注意事項

(1)　他機能との共存

「1.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

(2)　MST リージョンについて

本装置と他装置で扱える VLAN の範囲が異なることがあります。そのような装置を同じ MST リージョンとして扱いたい場合は，該当 VLAN を MST インスタンス 0 に所属させてください。

(3)　トポロジの収束に時間が掛かる場合について

CIST のルートブリッジまたは MST インスタンスのルートブリッジで，次の表に示すイベントが発生すると，トポロジが落ち着くまでに時間が掛かる場合があります。その間，通信が途絶えたり，MAC アドレステーブルのクリアが発生したりします。

表 6-16　ルートブリッジでのイベント発生

イベント	内容	イベントの発生したルートブリッジ種別	影響トポロジ
コンフィグレーション変更	リージョン名※1，リビジョン番号※2，またはインスタンス番号と VLAN の対応※3 をコンフィグレーションで変更し，リージョンを分割または同じにする場合	CIST のルートブリッジ	CIST
		MST インスタンス 0（IST）でのルートブリッジ	CIST
		MST インスタンス 1 以降でのルートブリッジ	該当 MST インスタンス
	ブリッジ優先度をコンフィグレーションコマンド spanning-tree mst root priority で下げた（現状より大きな値を設定した）場合	CIST のルートブリッジ	CIST
		MST インスタンス 1 以降でのルートブリッジ	該当 MST インスタンス
その他	本装置が停止した場合	CIST のルートブリッジ	CIST
		MST インスタンス 0（IST）でのルートブリッジ	CIST
		MST インスタンス 1 以降でのルートブリッジ	該当 MST インスタンス
	本装置と接続している対向装置で，ループ構成となっている本装置の全ポートがダウンした場合（本装置が該当ループ構成上ルートブリッジではなくなった場合）	CIST のルートブリッジ	CIST
		MST インスタンス 0（IST）でのルートブリッジ	CIST
		MST インスタンス 1 以降でのルートブリッジ	該当 MST インスタンス

注※1

MST コンフィグレーションモードのコンフィグレーションコマンド name

注※2

MST コンフィグレーションモードのコンフィグレーションコマンド revision

注※3

MST コンフィグレーションモードのコンフィグレーションコマンド instance

6.10　マルチプルスパニングツリーのコンフィグレーション

6.10.1　コンフィグレーションコマンド一覧

マルチプルスパニングツリ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 6-17　コンフィグレーションコマンド一覧

コマンド名	説明
instance	マルチプルスパニングツリーの MST インスタンスに所属する VLAN を設定します。
name	マルチプルスパニングツリーのリージョンを識別するための文字列を設定します。
revision	マルチプルスパニングツリーのリージョンを識別するためのリビジョン番号を設定します。
spanning-tree cost	ポートごとにパスコストのデフォルト値を設定します。
spanning-tree mode	スパニングツリー機能の動作モードを設定します。
spanning-tree mst configuration	マルチプルスパニングツリーの MST リージョンの形成に必要な情報を設定します。
spanning-tree mst cost	マルチプルスパニングツリーの MST インスタンスごとのパスコストを設定します。
spanning-tree mst forward-time	ポートの状態遷移に必要な時間を設定します。
spanning-tree mst hello-time	BPDU の送信間隔を設定します。
spanning-tree mst max-age	送信 BPDU の最大有効時間を設定します。
spanning-tree mst max-hops	MST リージョン内での最大ホップ数を設定します。
spanning-tree mst port-priority	マルチプルスパニングツリーの MST インスタンスごとのポート優先度を設定します。
spanning-tree mst root priority	MST インスタンスごとのブリッジ優先度を設定します。
spanning-tree mst transmission-limit	hello-time 当たりに送信できる最大 BPDU 数を設定します。
spanning-tree port-priority	ポートごとにポート優先度のデフォルト値を設定します。

6.10.2　マルチプルスパニングツリーの設定

(1)　マルチプルスパニングツリーの設定

[設定のポイント]

スパニングツリーの動作モードをマルチプルスパニングツリーに設定すると，PVST+，シングルスパニングツリーはすべて停止し，マルチプルスパニングツリーの動作を開始します。

[コマンドによる設定]

1. **(config)# spanning-tree mode mst**

   マルチプルスパニングツリーを使用するように設定し，CIST が動作を開始します。

[注意事項]

no spanning-tree mode コマンドでマルチプルスパニングツリーの動作モード設定を削除すると，デフォルトの動作モードである pvst になります。その際，ポート VLAN で自動的に PVST+が動作を開始します。

(2) リージョン，インスタンスの設定

[設定のポイント]

MST リージョンは，同じリージョンに所属させたい装置はリージョン名，リビジョン番号，MST インスタンスのすべてを同じ設定にする必要があります。

MST インスタンスは，インスタンス番号と所属する VLAN を同時に設定します。リージョンを一致させるために，本装置に未設定の VLAN ID もインスタンスに所属させられます。インスタンスに所属することを指定しない VLAN は自動的に CIST（インスタンス 0）に所属します。

MST インスタンスは，CIST（インスタンス 0）を含め 16 個まで設定できます。

[コマンドによる設定]

1. **(config)# spanning-tree mst configuration**
   (config-mst)# name "REGION TOKYO"
   (config-mst)# revision 1

   マルチプルスパニングツリーコンフィグレーションモードに移行して，name（リージョン名），revision（リビジョン番号）を設定します。

2. **(config-mst)# instance 10 vlans 100-150**
   (config-mst)# instance 20 vlans 200-250
   (config-mst)# instance 30 vlans 300-350

   インスタンス 10，20，30 を設定し，各インスタンスに所属する VLAN を設定します。インスタンス 10 に VLAN 100～150，インスタンス 20 に VLAN 200～250，インスタンス 30 に VLAN 300～350 を設定します。指定していないそのほかの VLAN は CIST（インスタンス 0）に所属します。

6.10.3 マルチプルスパニングツリーのトポロジ設定

(1) インスタンスごとのブリッジ優先度の設定

ブリッジ優先度は，ルートブリッジを決定するためのパラメータです。トポロジを設計する際に，ルートブリッジにしたい装置を最高の優先度に設定し，ルートブリッジに障害が発生したときのために，次にルートブリッジにしたい装置を 2 番目の優先度に設定します。

[設定のポイント]

ブリッジ優先度は値が小さいほど高い優先度になり，最も小さい値を設定した装置がルートブリッジになります。ルートブリッジはブリッジ優先度と装置の MAC アドレスから成るブリッジ識別子で判定するため，本パラメータを設定しない場合は装置の MAC アドレスが最も小さい装置がルートブリッジになります。

マルチプルスパニングツリーのブリッジ優先度はインスタンスごとに設定します。インスタンスごとに値を変えた場合，インスタンスごとのロードバランシング（異なるトポロジの構築）ができます。

[コマンドによる設定]

1. **(config)# spanning-tree mst 0 root priority 4096**
   (config)# spanning-tree mst 20 root priority 61440
   CIST（インスタンス 0）のブリッジ優先度を 4096 に，インスタンス 20 のブリッジ優先度を 61440 に設定します。

(2)　インスタンスごとのパスコストの設定

パスコストは通信経路を決定するためのパラメータです。スパニングツリーのトポロジ設計では，ブリッジ優先度の決定後に，指定ブリッジのルートポート（指定ブリッジからルートブリッジへの通信経路）を本パラメータで設計します。

[設定のポイント]

パスコスト値は指定ブリッジの各ポートに設定します。小さい値で設定することによってルートポートに選択されやすくなります。設定しない場合，ポートの速度ごとに異なるデフォルト値になり，高速なポートほどルートポートに選択されやすくなります。

パスコストは，速度の遅いポートを速いポートより優先して経路として使用したい場合に設定します。速いポートを優先したトポロジとする場合は設定する必要はありません。

パスコストのデフォルト値を次の表に示します。

表 6-18　パスコストのデフォルト値

ポートの速度	パスコストのデフォルト値
10Mbit/s	2000000
100Mbit/s	200000
1Gbit/s	20000
10Gbit/s	2000
40Gbit/s	500
100Gbit/s	200

[コマンドによる設定]

1. **(config)# spanning-tree mst configuration**
   (config-mst)# instance 10 vlans 100-150
   (config-mst)# instance 20 vlans 200-250
   (config-mst)# instance 30 vlans 300-350
   (config-mst)# exit
   (config)# interface gigabitethernet 1/1
   (config-if)# spanning-tree cost 2000
   MST インスタンス 10，20，30 を設定し，ポート 1/1 のパスコストを 2000 に設定します。CIST（インスタンス 0），MST インスタンス 10，20，30 のポート 1/1 のパスコストは 2000 になります。
2. **(config-if)# spanning-tree mst 20 cost 500**
   MST インスタンス 20 のポート 1/1 のパスコストを 500 に変更します。インスタンス 20 以外は 2000 で動作します。

[注意事項]

リンクアグリゲーションを使用する場合，チャネルグループのパスコストは，チャネルグループ内の全集約ポートの合計ではなく，チャネルグループ内の集約ポートのうち最低速度の回線の値となります。

(3) インスタンスごとのポート優先度の設定

ポート優先度は 2 台の装置間での接続をスパニングツリーで冗長化し，パスコストも同じ値とする場合に，どちらのポートを使用するかを決定するために設定します。

2 台の装置間の接続を冗長化する機能にはリンクアグリゲーションがあり，通常はリンクアグリゲーションを使用することをお勧めします。接続する対向の装置がリンクアグリゲーションをサポートしていないで，スパニングツリーで冗長化する必要がある場合に本機能を使用してください。

[設定のポイント]

ポート優先度は値が小さいほど高い優先度となります。2 台の装置間で冗長化している場合に，ルートブリッジに近い側の装置でポート優先度の高いポートが通信経路として使われます。本パラメータを設定しない場合はポート番号の小さいポートが優先されます。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   (config-if)# spanning-tree port-priority 64
   (config-if)# exit
   ポート 1/1 のポート優先度を 64 に設定します。
2. **(config)# interface gigabitethernet 1/1**
   (config-if)# spanning-tree mst 20 port-priority 144
   インスタンス 20 のポート 1/1 にポート優先度 144 を設定します。ポート 1/1 ではインスタンス 20 だけポート優先度 144 となり，そのほかのインスタンスは 64 で動作します。

6.10.4 マルチプルスパニングツリーのパラメータ設定

各パラメータは「2×（forward-time－1）≧max-age≧2×（hello-time ＋ 1)」という関係を満たすように設定する必要があります。パラメータを変える場合は，トポロジ全体でパラメータを合わせる必要があります。

(1) BPDU の送信間隔の設定

BPDU の送信間隔は，短くした場合はトポロジ変更を検知しやすくなります。長くした場合はトポロジ変更の検知までに時間が掛かるようになる一方で，BPDU トラフィックや本装置のスパニングツリープログラムの負荷を軽減できます。

[設定のポイント]

設定しない場合，2 秒間隔で BPDU を送信します。通常は設定する必要はありません。

[コマンドによる設定]

1. **(config)# spanning-tree mst hello-time 3**
   マルチプルスパニングツリーの BPDU 送信間隔を 3 秒に設定します。

[注意事項]

BPDU の送信間隔を短くすると，トポロジ変更を検知しやすくなる一方で BPDU トラフィックが増加することによってスパニングツリープログラムの負荷が増加します。本パラメータをデフォルト値（2 秒）より短くすることでタイムアウトのメッセージ出力やトポロジ変更が頻発する場合は，デフォルト値に戻して使用してください。

(2)　送信する最大 BPDU 数の設定

スパニングツリーでは，CPU 負荷の増大を抑えるために，hello-time（BPDU 送信間隔）当たりに送信する最大 BPDU 数を決められます。トポロジ変更が連続的に発生すると，トポロジ変更を通知，収束するために大量の BPDU が送信され，BPDU トラフィックの増加，CPU 負荷の増大につながります。送信する BPDU の最大数を制限することでこれらを抑えます。

[設定のポイント]

設定しない場合，hello-time（BPDU 送信間隔）当たりの最大 BPDU 数は 3 で動作します。通常は設定する必要はありません。

[コマンドによる設定]

1. **(config)# spanning-tree mst transmission-limit 5**
   マルチプルスパニングツリーの hello-time 当たりの最大送信 BPDU 数を 5 に設定します。

(3)　最大ホップ数の設定

ルートブリッジから送信する BPDU の最大ホップ数を設定します。BPDU のカウンタは装置を経由するたびに増加して，最大ホップ数を超えた BPDU は無効な BPDU となって無視されます。

シングルスパニングツリーの装置と接続しているポートは，最大ホップ数（max-hops）ではなく最大有効時間（max-age）のパラメータを使用します。ホップ数のカウントはマルチプルスパニングツリーの装置間で有効なパラメータです。

[設定のポイント]

最大ホップ数を大きく設定することで，多くの装置に BPDU が届くようになります。設定しない場合，最大ホップ数は 20 で動作します。

[コマンドによる設定]

1. **(config)# spanning-tree mst max-hops 10**
   マルチプルスパニングツリーの BPDU の最大ホップ数を 10 に設定します。

(4)　BPDU の最大有効時間の設定

マルチプルスパニングツリーでは，最大有効時間（max-age）はシングルスパニングツリーの装置と接続しているポートでだけ有効なパラメータです。トポロジ全体をマルチプルスパニングツリーが動作している装置で構成する場合は設定する必要はありません。

最大有効時間は，ルートブリッジから送信する BPDU の最大有効時間を設定します。BPDU のカウンタは装置を経由するたびに増加して，最大有効時間を超えた BPDU は無効な BPDU となって無視されます。

[設定のポイント]

最大有効時間を大きく設定することで，多くの装置に BPDU が届くようになります。設定しない場合，最大有効時間は 20 で動作します。

[コマンドによる設定]

1.(config)# spanning-tree mst max-age 25
マルチプルスパニングツリーの BPDU の最大有効時間を 25 に設定します。

(5) 状態遷移時間の設定

タイマによる動作となる場合，ポートの状態が Discarding から Learning，Forwarding へ一定時間ごとに遷移します。この状態遷移に必要な時間を設定できます。小さい値を設定すると，より早く Forwarding 状態に遷移できます。

[設定のポイント]

設定しない場合，状態遷移時間は 15 秒で動作します。本パラメータを短い時間に変更する場合，BPDU の最大有効時間（max-age），送信間隔（hello-time）との関係が「2×（forward-time－1）≧max-age≧2×（hello-time ＋ 1)」を満たすように設定してください。

[コマンドによる設定]

1.(config)# spanning-tree mst forward-time 10
マルチプルスパニングツリーの BPDU の最大有効時間を 10 に設定します。

6.11　マルチプルスパニングツリーのオペレーション

6.11.1　運用コマンド一覧

マルチプルスパニングツリーの運用コマンド一覧を次の表に示します。

表 6-19　運用コマンド一覧

コマンド名	説明
show spanning-tree	スパニングツリー情報を表示します。
show spanning-tree statistics	スパニングツリーの統計情報を表示します。
clear spanning-tree statistics	スパニングツリーの統計情報をクリアします。
clear spanning-tree detected-protocol	スパニングツリーの STP 互換モードを強制回復します。
show spanning-tree port-count	スパニングツリーの収容数を表示します。
restart spanning-tree	スパニングツリープログラムを再起動します。
dump protocols spanning-tree	スパニングツリーで採取している詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。

6.11.2　マルチプルスパニングツリーの状態の確認

マルチプルスパニングツリーの情報は show spanning-tree コマンドで確認してください。トポロジが正しく構築されていることを確認するためには，次の項目を確認してください。

- リージョンの設定（Revision Level，Configuration Name，MST Instance の VLAN Mapped）が正しいこと
- Regional Root の内容が正しいこと
- Port Information の Status，Role が正しいこと

show spanning-tree コマンドの実行結果を次の図に示します。

図 6-15　show spanning-tree コマンドの実行結果（マルチプルスパニングツリーの情報）

```
> show spanning-tree mst instance 10
Date 20XX/03/04 11:41:03 UTC
Multiple Spanning Tree: Enabled
Revision Level: 65535  Configuration Name: MSTP001
MST Instance 10
  VLAN Mapped: 100-150
  Regional Root  Priority: 32778       MAC      : 0012.e207.7200
  Internal Root Cost     : 2000        Root Port: 1/1
  Bridge ID      Priority: 32778       MAC      : 0012.e205.0900
  Regional Bridge Status : Designated
  Port Information
    1/1        Up   Status:Forwarding  Role:Root
    1/2        Up   Status:Discarding  Role:Backup
    1/3        Up   Status:Discarding  Role:Alternate
    1/4        Up   Status:Forwarding  Role:Designated
>
```

6.12 スパニングツリー共通機能解説

6.12.1 PortFast

(1) 概要

PortFast は，端末が接続されループが発生しないことがあらかじめわかっているポートのための機能です。PortFast はスパニングツリーのトポロジ計算対象外となり，リンクアップ後すぐに通信できる状態になります。

(2) PortFast 適用時の BPDU 受信

PortFast を設定したポートは BPDU を受信しないことを想定したポートですが，もし，PortFast を設定したポートで BPDU を受信した場合は，その先にスイッチが存在しループの可能性があることになります。そのため，PortFast 機能を停止し，トポロジ計算や BPDU の送受信など，通常のスパニングツリー対象のポートとしての動作を開始します。

いったんスパニングツリー対象のポートとして動作を開始したあと，リンクのダウン／アップによって再び PortFast 機能が有効になります。

なお，BPDU を受信したときに PortFast 機能を停止しないようにする場合は，BPDU フィルタ機能を併用してください。

(3) PortFast 適用時の BPDU 送信

PortFast を設定したポートではスパニングツリーを動作させないため，BPDU を送信しません。

ただし，PortFast を設定したポート同士を誤って接続した状態を検出するために，PortFast 機能によってすぐに通信できる状態になった時点から 10 フレームだけ BPDU を送信します。

(4) BPDU ガード

PortFast に適用する機能として，BPDU ガード機能があります。BPDU ガード機能を適用したポートでは，BPDU 受信時に，スパニングツリー対象のポートとして動作するのではなくポートを inactive 状態にします。

inactive 状態にしたポートを activate コマンドで解放することによって，再び BPDU ガード機能を適用した PortFast としてリンクアップして通信を開始します。

6.12.2 BPDU フィルタ

(1) 概要

BPDU フィルタ機能を適用したポートでは，BPDU の送受信を停止します。BPDU フィルタ機能は，端末が接続されループが発生しないことがあらかじめわかっている，PortFast を設定したポートに適用します。

(2) BPDU フィルタに関する注意事項

PortFast を適用したポート以外に BPDU フィルタ機能を設定した場合，BPDU の送受信を停止するため，タイマによるポートの状態遷移が終了するまで通信断になります。

6.12.3　ループガード

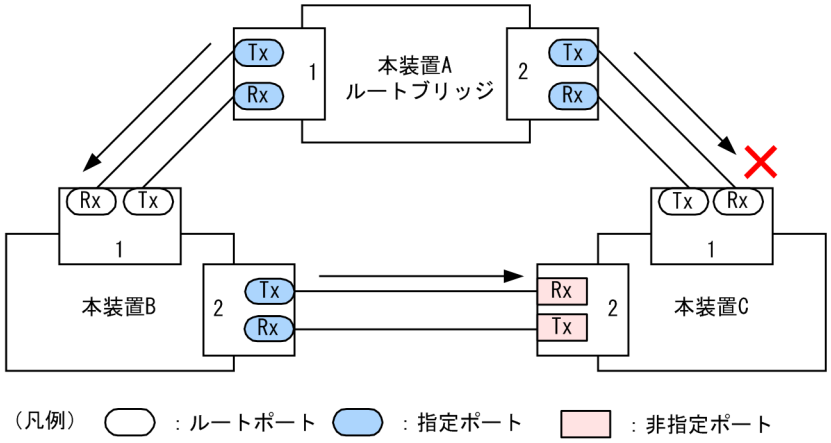
(1)　概要

片線切れなどの単一方向のリンク障害が発生し，BPDU の受信が途絶えた場合，ループが発生することがあります。ループガード機能は，このような場合にループの発生を防止する機能です。

単一方向のリンク障害時に閉ループが発生する例を示します。

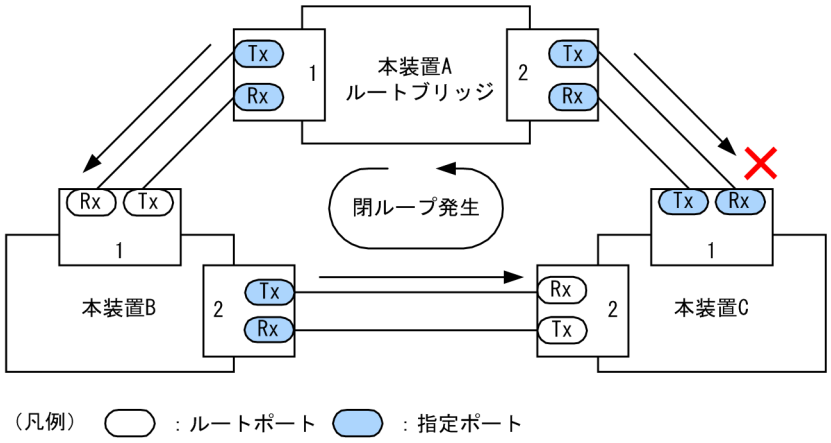
1. 本装置 C のポート 1 にリンク障害が発生すると，BPDU の受信が途絶えます。

図 6-16　単一方向のリンク障害時の閉ループ発生例 1



2. 本装置 C では，ルートポートがポート 2 に切り替わります。このとき，ポート 1 は指定ポートとなって通信可能状態を維持するため，閉ループが発生します。

図 6-17　単一方向のリンク障害時の閉ループ発生例 2



ループガード機能とは BPDU の受信が途絶えたポートの状態を，再度 BPDU を受信するまで転送不可状態に遷移させる機能です。BPDU 受信を開始した場合は，通常のスパニングツリー対象のポートとしての動作を開始します。

ループガード機能は，端末を接続するポートを指定する機能である PortFast を設定したポート，またはルートガード機能を設定したポートには設定できません。

(2)　ループガードに関する注意事項

ループガードはマルチプルスパニングツリーでは使用できません。

ループガード機能を設定したあと，次に示すイベントが発生すると，ループガードが動作してポートをブロックします。その後，BPDU を受信するまで，ループガードは解除されません。

- 装置起動
- 系切替
- ポートのアップ（リンクアグリゲーションのアップも含む）
- スパニングツリープログラムの再起動
- スパニングツリープロトコルの種別変更（STP／高速 STP，PVST+／高速 PVST+）

なお，ループガード機能は，指定ポートだけでなく対向装置にも設定してください。指定ポートだけに設定すると，上記のイベントが発生しても，指定ポートは BPDU を受信しないことがあります。このような場合，ループガードの解除に時間が掛かります。ループガードを解除するには，対向装置のポートで BPDU 受信タイムアウトを検出したあとの BPDU の送信を待つ必要があるためです。

また，両ポートにループガードを設定した場合でも，指定ポートで BPDU を一度も受信しないで，ループガードの解除に時間が掛かることがあります。具体的には，対向ポートが指定ポートとなるようにブリッジやポートの優先度，パスコストを変更した場合です。対向ポートで BPDU タイムアウトを検出し，ループガードが動作します。このポートが指定ポートになった場合，BPDU を受信しないことがあり，ループガードの解除に時間が掛かることがあります。

運用中にループガード機能を設定した場合，その時点では，ループガードは動作しません。運用中に設定したループガードは，BPDU の受信タイムアウトが発生した時に動作します。

本装置と対向装置のポート間に BPDU を中継しない装置が存在し，かつポートの両端にループガード機能を設定した状態でポートがリンクアップした場合，両端のポートはループガードが動作したままになります。復旧するには，ポート間に存在する装置の BPDU 中継機能を有効にし，再度ポートをリンクアップさせる必要があります。

6.12.4 ルートガード

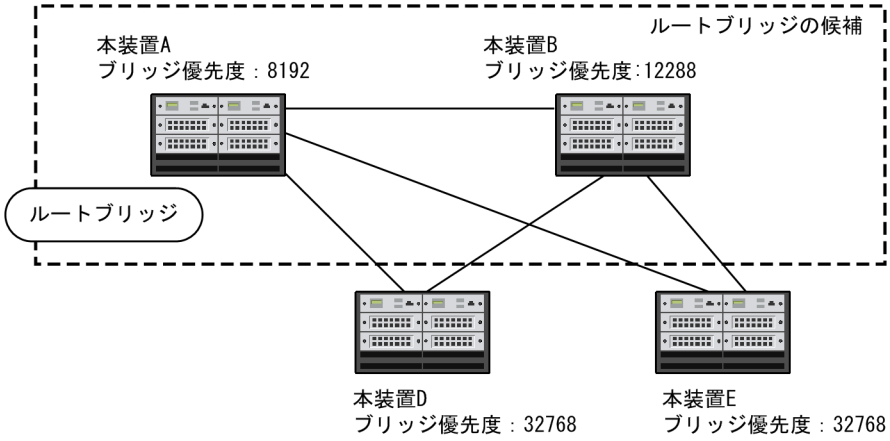
(1) 概要

ネットワークの管理の届かない個所で誤って装置が接続された場合や設定が変更された場合，意図しないトポロジになることがあります。意図しないトポロジのルートブリッジの性能が低い場合，トラフィックが集中するとネットワーク障害のおそれがあります。ルートガード機能は，このようなときのためにルートブリッジの候補を特定しておくことによって，ネットワーク障害を回避する機能です。

誤って装置が接続されたときの問題点を次の図に示します。

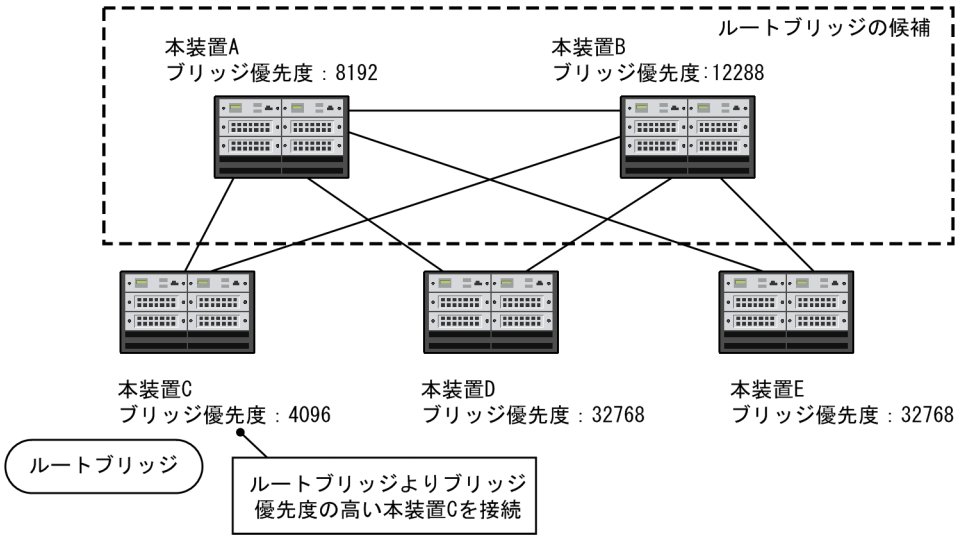
- 本装置 A，本装置 B をルートブリッジの候補として運用

図 6-18　本装置 A，本装置 B をルートブリッジの候補として運用



- 本装置 A，本装置 B よりブリッジ優先度の高い本装置 C を接続すると，本装置 C がルートブリッジになり，本装置 C にトラフィックが集中するようになる

図 6-19　本装置 A，本装置 B よりブリッジ優先度の高い本装置 C を接続



ルートガード機能は，現在のルートブリッジよりも優先度の高いブリッジを検出し，BPDU を廃棄することによってトポロジを保護します。また，該当するポートをブロック状態に設定することでループを回避します。ルートガード機能は，ループガード機能を設定したポートには設定できません。

6.13　スパニングツリー共通機能のコンフィグレーション

6.13.1　コンフィグレーションコマンド一覧

スパニングツリー共通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 6-20　コンフィグレーションコマンド一覧

コマンド名	説明
spanning-tree bpdufilter	ポートごとに BPDU フィルタ機能を設定します。
spanning-tree bpduguard	ポートごとに BPDU ガード機能を設定します。
spanning-tree guard	ポートごとにループガード機能，ルートガード機能を設定します。
spanning-tree link-type	ポートのリンクタイプを設定します。
spanning-tree loopguard default	ループガード機能をデフォルトで使用するように設定します。
spanning-tree portfast	ポートごとに PortFast 機能を設定します。
spanning-tree portfast bpduguard default	BPDU ガード機能をデフォルトで使用するように設定します。
spanning-tree portfast default	PortFast 機能をデフォルトで使用するように設定します。

6.13.2　PortFast の設定

(1)　PortFast の設定

PortFast は，端末を接続するポートなど，ループが発生しないことがあらかじめわかっているポートをすぐに通信できる状態にしたい場合に適用します。

[設定のポイント]

spanning-tree portfast default コマンドを設定すると，アクセスポートにデフォルトで PortFast 機能を適用します。デフォルトで適用してポートごとに無効にしたい場合は，spanning-tree portfast コマンドで disable を設定します。

トランクポートでは，ポートごとの指定で適用できます。

[コマンドによる設定]

1. **(config)# spanning-tree portfast default**

   すべてのアクセスポートに対して PortFast 機能を適用するように設定します。

2. **(config)# interface gigabitethernet 1/1**
   (config-if)# switchport mode access
   (config-if)# spanning-tree portfast disable
   (config-if)# exit

   ポート 1/1（アクセスポート）で PortFast 機能を使用しないように設定します。

3. **(config)# interface gigabitethernet 1/3**
   (config-if)# switchport mode trunk

(config-if)# spanning-tree portfast trunk

ポート 1/3 をトランクポートに指定して，PortFast 機能を適用します。トランクポートはデフォルトでは適用されません。ポートごとに指定するためには trunk パラメータを指定する必要があります。

(2)　BPDU ガードの設定

BPDU ガード機能は，PortFast を適用したポートで BPDU を受信した場合にそのポートを inactive 状態にします。通常，PortFast 機能は冗長経路ではないポートを指定し，ポートの先にはスパニングツリー装置がないことを前提とします。BPDU を受信したことによる意図しないトポロジ変更を回避したい場合に設定します。

[設定のポイント]

BPDU ガード機能を設定するためには，PortFast 機能を同時に設定する必要があります。spanning-tree portfast bpduguard default コマンドは PortFast 機能を適用しているすべてのポートにデフォルトで BPDU ガードを適用します。デフォルトで適用するときに BPDU ガード機能を無効にしたい場合は，spanning-tree bpduguard コマンドで disable を設定します。

[コマンドによる設定]

1. **(config)# spanning-tree portfast default**
   (config)# spanning-tree portfast bpduguard default
   すべてのアクセスポートに対して PortFast 機能を設定します。また，PortFast 機能を適用したすべてのポートに対して BPDU ガード機能を設定します。
2. **(config)# interface gigabitethernet 1/1**
   (config-if)# spanning-tree bpduguard disable
   (config-if)# exit
   ポート 1/1（アクセスポート）で BPDU ガード機能を使用しないように設定します。ポート 1/1 は通常の PortFast 機能を適用します。
3. **(config)# interface gigabitethernet 1/2**
   (config-if)# switchport mode trunk
   (config-if)# spanning-tree portfast trunk
   ポート 1/2（トランクポート）に PortFast 機能を設定します。また，BPDU ガード機能を設定します。トランクポートはデフォルトでは PortFast 機能を適用しないためポートごとに設定します。デフォルトで BPDU ガード機能を設定している場合は, PortFast 機能を設定すると自動的に BPDU ガードも適用します。デフォルトで設定していない場合は, spanning-tree bpduguard コマンドで enable を設定します。

6.13.3　BPDU フィルタの設定

BPDU フィルタ機能は，BPDU を受信した場合にその BPDU を廃棄します。また，BPDU を一切送信しなくなります。通常は冗長経路ではないポートを指定することを前提とします。

[設定のポイント]

インタフェース単位に BPDU フィルタ機能を設定できます。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   (config-if)# spanning-tree bpdufilter enable

ポート 1/1 で BPDU フィルタ機能を設定します。

6.13.4 ループガードの設定

片線切れなどの単一方向のリンク障害が発生し，BPDU の受信が途絶えた場合，ループが発生することがあります。ループガードは，このようにループの発生を防止したい場合に設定します。

[設定のポイント]

ループガードは，PortFast 機能を設定していないポートで動作します。

spanning-tree loopguard default コマンドを設定すると，PortFast を設定したポート以外のすべてのポートにループガードを適用します。デフォルトで適用する場合に，ループガードを無効にしたい場合は spanning-tree guard コマンドで none を設定します。

[コマンドによる設定]

1. **(config)# spanning-tree loopguard default**

   PortFast を設定したポート以外のすべてのポートに対してループガード機能を適用するように設定します。

2. **(config)# interface gigabitethernet 1/1**
   (config-if)# spanning-tree guard none
   (config-if)# exit

   デフォルトでループガードを適用するように設定した状態で，ポート 1/1 はループガードを無効にするように設定します。

3. **(config)# no spanning-tree loopguard default**
   (config)# interface gigabitethernet 1/2
   (config-if)# spanning-tree guard loop

   デフォルトでループガードを適用する設定を削除します。また，ポート 1/2 に対してポートごとの設定でループガードを適用します。

6.13.5 ルートガードの設定

ネットワークに誤って装置が接続された場合や設定が変更された場合，ルートブリッジが替わり，意図しないトポロジになることがあります。ルートガードは，このような意図しないトポロジ変更を防止したい場合に設定します。

[設定のポイント]

ルートガードは指定ポートに対して設定します。ルートブリッジの候補となる装置以外の装置と接続する個所すべてに適用します。

ルートガード動作時，PVST+が動作している場合は，該当する VLAN のポートだけブロック状態に設定します。マルチプルスパニングツリーが動作している場合，該当するインスタンスのポートだけブロック状態に設定しますが，該当するポートが境界ポートの場合は，全インスタンスのポートをブロック状態に設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   (config-if)# spanning-tree guard root

   ポート 1/1 でルートガード機能を設定します。

6.13.6　リンクタイプの設定

リンクタイプはポートの接続状態を表します。Rapid PVST+，シングルスパニングツリーの Rapid STP，マルチプルスパニングツリーで高速な状態遷移をするためには，スイッチ間の接続が point-to-point である必要があります。shared の場合は高速な状態遷移はしないで，PVST+，シングルスパニングツリーの STP と同様にタイマによる状態遷移となります。

[設定のポイント]

ポートごとに接続状態を設定できます。設定しない場合，ポートが全二重の接続のときは point-to-point，半二重の接続のときは shared となります。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/1**
   (config-if)# spanning-tree link-type point-to-point
   ポート 1/1 を point-to-point 接続と見なして動作させます。

[注意事項]

実際のネットワークの接続形態が 1 対 1 接続ではない構成では，本コマンドで point-to-point を指定しないでください。1 対 1 接続ではない構成とは，一つのポートに隣接するスパニングツリー装置が 2 台以上存在する構成です。

6.14 スパニングツリー共通機能のオペレーション

6.14.1 運用コマンド一覧

スパニングツリー共通機能の運用コマンド一覧を次の表に示します。

表 6-21 運用コマンド一覧

コマンド名	説明
show spanning-tree	スパニングツリー情報を表示します。

6.14.2 スパニングツリー共通機能の状態の確認

スパニングツリーの情報は,show spanning-tree コマンドで detail パラメータを指定して確認してください。VLAN 10 の PVST+の例を次の図に示します。

PortFast はポート 1/3，1/4，1/5 に設定していることを PortFast の項目で確認できます。ポート 1/3 は PortFast を設定していて，ポート 1/4 は PortFast に加えて BPDU ガードを設定しています。どちらのポートも意図しない BPDU を受信しないで正常に動作していることを示しています。ポート 1/5 は BPDU フィルタを設定しています。

ループガードはポート 1/2 に設定していることを Loop Guard の項目で確認できます。ルートガードはポート 1/6 に設定していることを Root Guard の項目で確認できます。リンクタイプは各ポートの Link Type の項目で確認できます。すべてのポートが point-to-point で動作しています。

図 6-20 スパニングツリーの情報

```
> show spanning-tree vlan 10 detail
Date 20XX/03/21 18:13:59 UTC
VLAN 10             PVST+ Spanning Tree:Enabled  Mode:Rapid PVST+
  Bridge ID
    Priority:32778                  MAC Address:0012.e210.3004
    Bridge Status:Designated        Path Cost Method:Short
    Max Age:20                      Hello Time:2
    Forward Delay:15
  Root Bridge ID
    Priority:32778                  MAC Address:0012.e210.1004
    Root Cost:4
    Root Port:1/1
    Max Age:20                      Hello Time:2
    Forward Delay:15
  Port Information
  Port:1/1 Up
    Status:Forwarding               Role:Root
    Priority:128                    Cost:4
    Link Type:point-to-point        Compatible Mode:-
    Loop Guard:OFF                  PortFast:OFF
    BpduFilter:OFF                  Root Guard:OFF
    BPDU Parameters(20XX/03/21 18:13:59):
      Designated Root
        Priority:32778              MAC address:0012.e210.1004
      Designated Bridge
        Priority:32778              MAC address:0012.e210.1004
        Root Path Cost:0
      Port ID
        Priority:128                Number:1
      Message Age Time:0(3)/20
  Port:1/2 Up
    Status:Discarding               Role:Alternate
    Priority:128                    Cost:4
    Link Type:point-to-point        Compatible Mode:-
    Loop Guard:ON                   PortFast:OFF
```

```
  BpduFilter:OFF                  Root Guard:OFF
  BPDU Parameters(20XX/03/21 18:13:58):
    Designated Root
      Priority:32778              MAC address:0012.e210.1004
    Designated Bridge
      Priority:32778              MAC address:0012.e210.2004
      Root Path Cost:4
    Port ID
      Priority:128                Number:1
    Message Age Time:1(3)/20
Port:1/3 Up
  Status:Forwarding               Role:Designated
  Priority:128                    Cost:4
  Link Type:point-to-point        Compatible Mode:-
  Loop Guard:OFF                  PortFast:ON (BPDU not received)
  BpduFilter:OFF                  Root Guard:OFF
Port:1/4 Up
  Status:Forwarding               Role:Designated
  Priority:128                    Cost:4
  Link Type:point-to-point        Compatible Mode:-
  Loop Guard:OFF                  PortFast:BPDU Guard(BPDU not received)
  BpduFilter:OFF                  Root Guard:OFF
Port:1/5 Up
  Status:Forwarding               Role:Designated
  Priority:128                    Cost:4
  Link Type:point-to-point        Compatible Mode:-
  Loop Guard:OFF                  PortFast:ON(BPDU not received)
  BpduFilter:ON                   Root Guard:OFF
Port:1/6 Up
  Status:Forwarding               Role:Designated
  Priority:128                    Cost:4
  Link Type:point-to-point        Compatible Mode:-
  Loop Guard:OFF                  PortFast:OFF
  BpduFilter:OFF                  Root Guard:ON
```

7 Ring Protocol の解説

この章は，Autonomous Extensible Ring Protocol について説明します。
Autonomous Extensible Ring Protocol は，リングトポロジでのレイヤ 2 ネットワークの冗長化プロトコルで，以降，Ring Protocol と呼びます。

7.1　Ring Protocol の概要

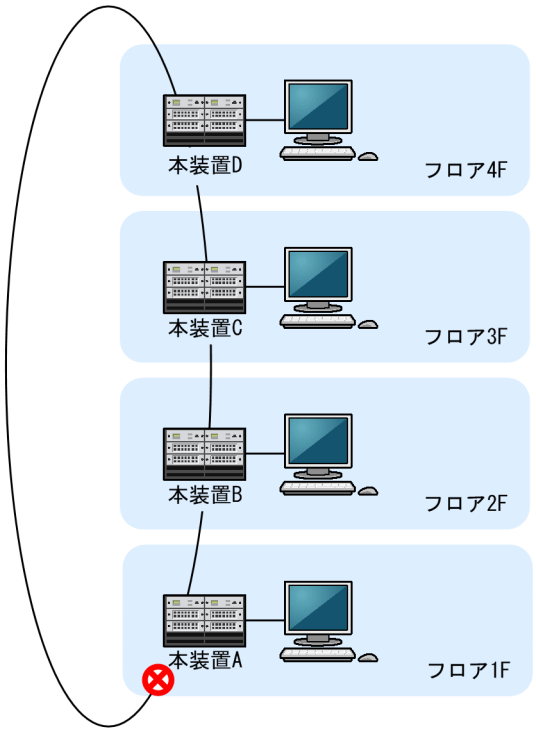
7.1.1　概要

Ring Protocol とは，スイッチをリング状に接続したネットワークでの障害の検出と，それに伴う経路切り替えを高速に行うレイヤ 2 ネットワークの冗長化プロトコルです。

レイヤ 2 ネットワークの冗長化プロトコルとして，スパニングツリーが利用されますが，障害発生に伴う切り替えの収束時間が遅いなどの欠点があります。Ring Protocol を使用すると，障害発生に伴う経路切り替えを高速にできるようになります。また，リングトポロジを利用することで，メッシュトポロジよりも伝送路やインタフェースの必要量が少なくて済むという利点もあります。

Ring Protocol の適用例を次の図に示します。

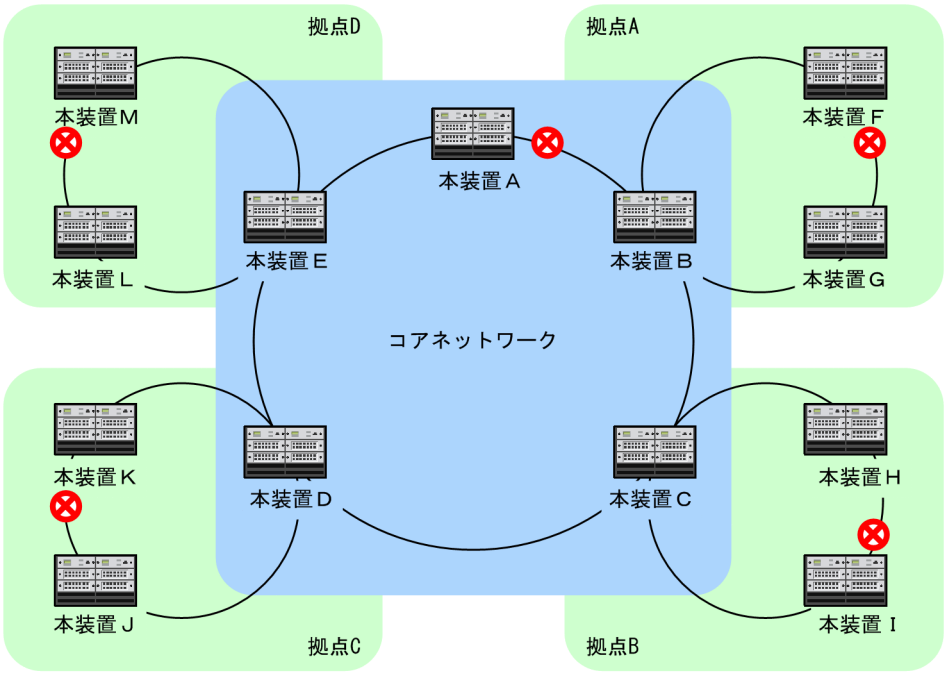
図 7-1　Ring Protocol の適用例（その 1）



（凡例）

：ブロッキング状態

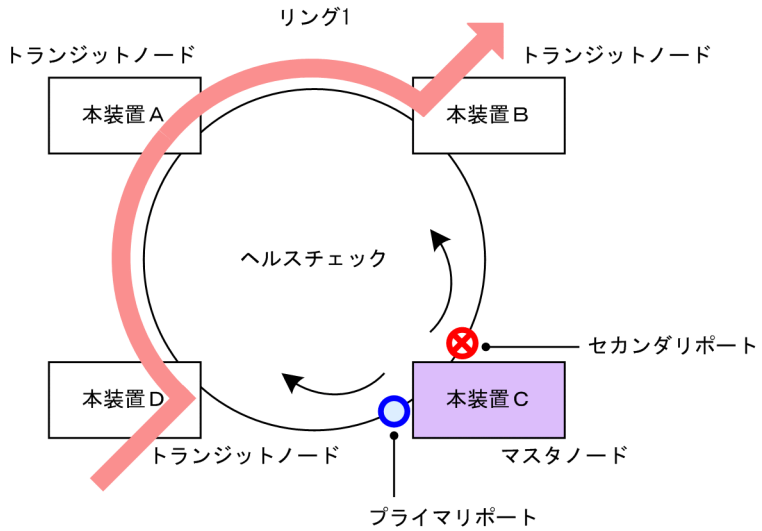
図 7-2　Ring Protocol の適用例（その 2）



（凡例）
：ブロッキング状態

Ring Protocol によるリングネットワークの概要を次の図に示します。

図 7-3　Ring Protocol の概要



（凡例）
：フォワーディング状態　：ブロッキング状態
：データの流れ

リングを構成するノードのうち一つをマスタノードとして，ほかのリング構成ノードをトランジットノードとします。各ノード間を接続する二つのポートをリングポートと呼び，マスタノードのリングポートにはプ

ライマリポートとセカンダリポートがあります。マスタノードはセカンダリポートをブロッキング状態にすることでリング構成を分断します。これによって，データフレームのループを防止しています。マスタノードはリング内の状態監視を目的とした制御フレーム（ヘルスチェックフレーム）を定期的に送信します。マスタノードは，巡回したヘルスチェックフレームの受信，未受信によって，リング内で障害が発生していないかどうかを判断します。障害または障害復旧を検出したマスタノードは，セカンダリポートのブロッキング状態を設定または解除することで経路を切り替え，通信を復旧させます。

7.1.2　特長

(1)　イーサネットベースのリングネットワーク

Ring Protocol はイーサネットベースのネットワーク冗長化プロトコルです。従来のリングネットワークでは FDDI のように二重リンクの光ファイバを利用したネットワークが主流でしたが, Ring Protocol を使用することでイーサネットを利用したリングネットワークが構築できます。

(2)　シンプルな動作方式

Ring Protocol を使用したネットワークは, マスタノード 1 台とそのほかのトランジットノードで構成したシンプルな構成となります。リング状態（障害や障害復旧）の監視や経路の切り替え動作は，主にマスタノードが行い, そのほかのトランジットノードはマスタノードからの指示によって経路の切り替え動作を行います。

(3)　制御フレーム

Ring Protocol では，本プロトコル独自の制御フレームを使用します。制御フレームは，マスタノードによるリング状態の監視やマスタノードからトランジットノードへの経路の切り替え指示に使われます。制御フレームの送受信は，専用の VLAN 上で行われるため，スパニングツリーのようにデータフレームと制御フレームが同じ VLAN 内に流れることはありません。

(4)　負荷分散方式

リング内で使用する複数の VLAN を論理的なグループ単位にまとめ，マスタノードを基点としてデータの流れを右回りと左回りに分散させる設定ができます。負荷分散や VLAN ごとに経路を分けたい場合に有効です。

7.1.3　サポート仕様

Ring Protocol でサポートする項目と仕様を次の表に示します。

表 7-1　Ring Protocol でサポートする項目と仕様

項目		内容
適用レイヤ	レイヤ 2	○
	レイヤ 3	×
リング構成	シングルリング	○
	マルチリング	○（共有リンクありマルチリング構成含む）
装置当たりのリング ID 最大数		192
リングポート（1 リング ID 当たりのポート数）		2（物理ポートまたはリンクアグリゲーション）

項目		内容
VLAN 数	1 リング ID 当たりの制御 VLAN 数	1
	1 リング ID 当たりのデータ転送用 VLAN グループ最大数	2
	1 データ転送用 VLAN グループ当たりの VLAN マッピング最大数	384
	1VLAN マッピング当たりの VLAN 最大数	4094
ヘルスチェックフレーム送信間隔		5～60000 ミリ秒の範囲で 1 ミリ秒単位
障害監視時間		15～300000 ミリ秒の範囲で 1 ミリ秒単位
負荷分散方式		二つのデータ転送用 VLAN グループを使用することで可能

（凡例）　○：サポート　×：未サポート

7.2　Ring Protocol の基本原理

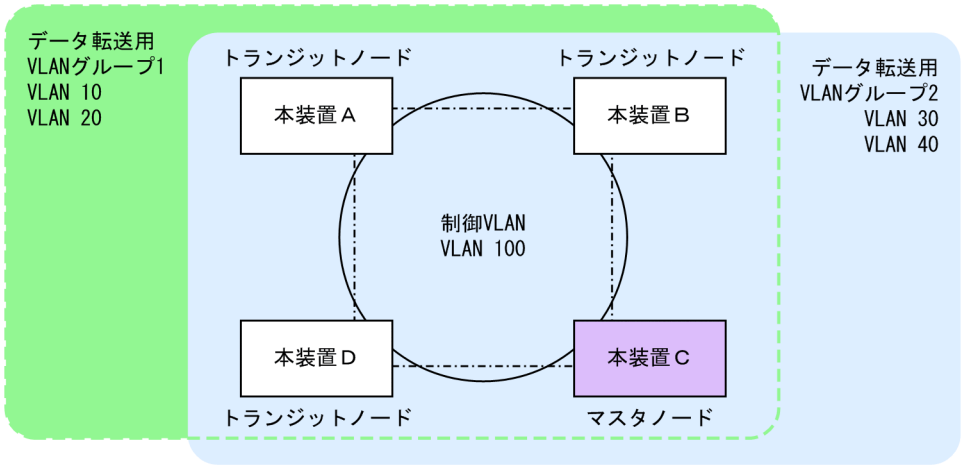
7.2.1　ネットワーク構成

Ring Protocol を使用する場合の基本的なネットワーク構成を次に示します。

(1)　シングルリング構成

シングルリング構成について，次の図に示します。

図 7-4　シングルリング構成

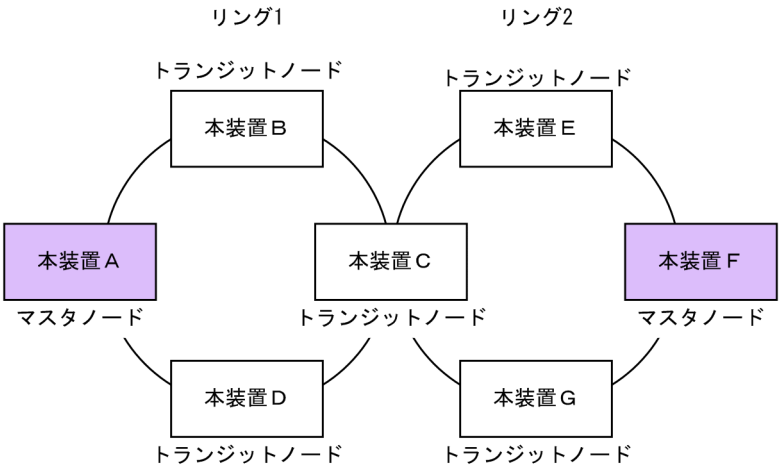


マスタノード 1 台とトランジットノード数台から成る一つのリング構成をシングルリング構成と呼びます。リングを構成するノード間は，リングポートとして，物理ポートまたはリンクアグリゲーションで接続されます。また，リングを構成するすべてのノードに，制御 VLAN として同一の VLAN，およびデータフレームの転送用として共通の VLAN を使用する必要があります。マスタノードから送信した制御フレームは，制御 VLAN 内を巡回します。データフレームの送受信に使用する VLAN は，VLAN グループと呼ばれる一つの論理的なグループに束ねて使用します。VLAN グループは複数の VLAN をまとめることができ，一つのリングにマスタノードを基点とした右回り用と左回り用の最大 2 グループを設定できます。

(2)　マルチリング構成

マルチリング構成のうち，隣接するリングの接点となるノードが一つの場合の構成について次の図に示します。

図 7-5　マルチリング構成

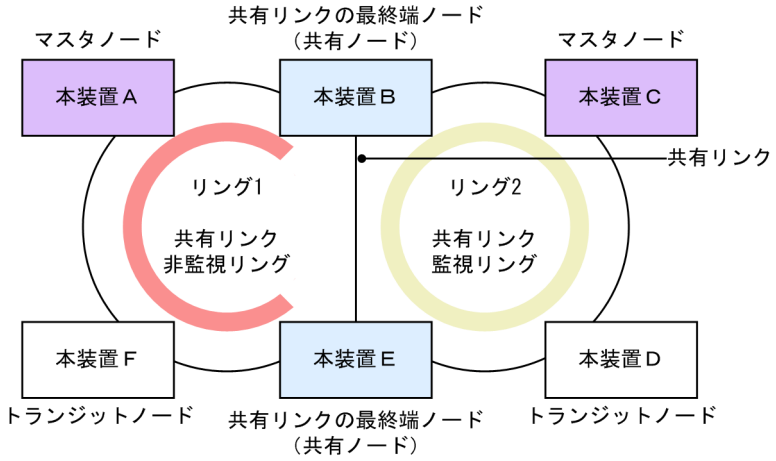


それぞれのリングを構成しているノードは独立したシングルリングとして動作します。このため，リング障害の検出および復旧の検出はそれぞれのリングで独立して行われます。

(3)　共有リンクありのマルチリング構成

マルチリング構成のうち，隣接するリングの接点となるノードが二つ以上の場合の構成について次の図に示します。

図 7-6　共有リンクありのマルチリング構成



（凡例）　：リング1の監視経路　：リング2の監視経路

複数のシングルリングが，二つ以上のノードで接続されている場合，複数のリングでリンクを共有することになります。このリンクを共有リンクと呼び，共有リンクのあるマルチリング構成を，共有リンクありのマルチリング構成と呼びます。これに対し，（2）のように，複数のシングルリングが一つのノードで接続されている場合には，共有リンクがありませんので，共有リンクなしのマルチリング構成と呼びます。

共有リンクありのマルチリング構成では，隣接するリングで共通の VLAN をデータ転送用の VLAN グループとして使用した場合に，共有リンクで障害が発生すると隣接するリングそれぞれのマスタノードが障害を検出し，複数のリングをまたいだループ（いわゆるスーパーループ）が発生します。このため，本構成ではシングルリング構成とは異なる障害検出，および切り替え動作を行う必要があります。

Ring Protocol では，共有リンクをリングの一部とする複数のリングのうち，一つを共有リンクの障害および復旧を監視するリング（共有リンク監視リング）とし，それ以外のリングを，共有リンクの障害および復旧を監視しないリング（共有リンク非監視リング）とします。また，共有リンクの両端に位置するノードを共有リンク非監視リングの最終端ノード（または，共有ノード）と呼びます。このように，各リングのマスタノードで監視対象リングを重複させないことによって，共有リンク間の障害によるループの発生を防止します。

7.2.2 制御 VLAN

Ring Protocol を利用するネットワークでは，制御フレームの送信範囲を限定するために，制御フレームの送受信に専用の VLAN を使用します。この VLAN を制御 VLAN と呼び，リングを構成するすべてのノードで同一の VLAN を使用します。制御 VLAN は，リングごとに共通な一つの VLAN を使用しますので，マルチリング構成時には，隣接するリングで異なる VLAN を使用する必要があります。

7.2.3 障害監視方法

Ring Protocol のリング障害の監視は，マスタノードがヘルスチェックフレームと呼ぶ制御フレームを定期的に送信し，マスタノードがこのヘルスチェックフレームの受信可否を監視することで実現します。マスタノードでは，ヘルスチェックフレームが一定時間到達しないとリング障害が発生したと判断し，障害動作を行います。また，リング障害中に再度ヘルスチェックフレームを受信すると，リング障害が復旧したと判断し，復旧動作を行います。

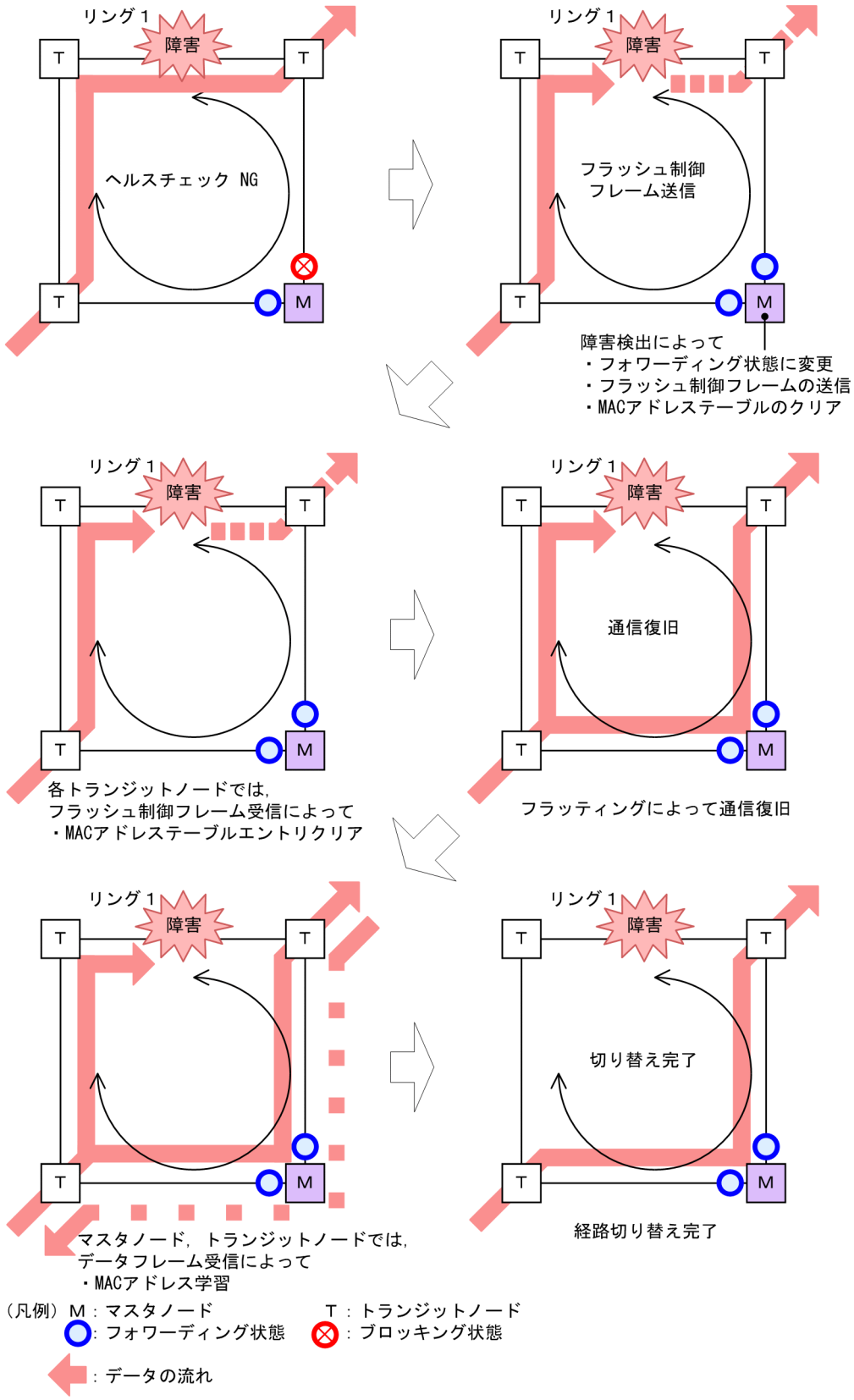
マスタノードでは，片方向リンク障害での障害の検出および通信経路の切り替え動作を実施しません。片方向リンク障害の発生時にも切り替え動作を実施したい場合は，UDLD を併用してください。UDLD では，片方向リンク障害が検出された場合に該当ポートを inactive 状態にします。これによって，該当するリングを監視するマスタノードはリング障害を検出し，通信経路を切り替えます。

7.2.4 通信経路の切り替え

マスタノードは，リング障害の検出による迂回経路への切り替えのために，セカンダリポートをブロッキング状態からフォワーディング状態に変更します。また，リング障害の復旧検出による経路の切り戻しのために，セカンダリポートをフォワーディング状態からブロッキング状態に変更します。これに併せて，早急な通信の復旧を行うために，リング内のすべてのノードで，MAC アドレステーブルエントリのクリアが必要です。MAC アドレステーブルエントリのクリアが実施されないと，切り替え（または切り戻し）前の情報に従ってデータフレームの転送が行われるため，正しくデータが届かないおそれがあります。したがって，通信を復旧させるために，リングを構成するすべてのノードで MAC アドレステーブルエントリのクリアを実施します。

マスタノードおよびトランジットノードそれぞれの場合の切り替え動作について次に説明します。

図 7-7　Ring Protocol の経路切り替え動作概要



(1)　マスタノードの経路切り替え

マスタノードでは，リング障害を検出するとセカンダリポートのブロッキング状態を解除します。また，リングポートで MAC アドレステーブルエントリのクリアを行います。これによって，MAC アドレスの学習が行われるまでフラッディングを行います。セカンダリポートを経由したフレームの送受信によって MAC アドレス学習を行い，新しい経路への切り替えが完了します。

(2)　トランジットノードの経路切り替え

マスタノードがリングの障害を検出すると，同一の制御 VLAN を持つリング内の，そのほかのトランジットノードに対して MAC アドレステーブルエントリのクリアを要求するために，フラッシュ制御フレームと呼ぶ制御フレームを送信します。トランジットノードでは，このフラッシュ制御フレームを受信すると，リングポートでの MAC アドレステーブルエントリのクリアを行います。これによって，MAC アドレスの学習が行われるまでフラッディングを行います。新しい経路でのフレームの送受信によって MAC アドレス学習が行われ，通信経路の切り替えが完了します。

7.2.5　リングポートのデータ転送用 VLAN

Ring Protocol では，装置，Ring Protocol プログラム，またはリングポートが障害となった場合に，障害復旧時のループの発生を防ぐために，リングポートのデータ転送用 VLAN 状態をブロッキング状態にします。このブロッキング状態は，次の契機で解除します。

- マスタノードが送信するフラッシュ制御フレームをトランジットノードで受信したとき
- リングポートフォワーディング遷移時間（forwarding-shift-time）がタイムアウトしたとき

リングネットワーク内で複数の障害が同時に発生し，一部の障害が復旧した場合，リングネットワークは障害状態であるため，マスタノードはリングの復旧を検知しないで，フラッシュ制御フレームを送信しません。リングポートフォワーディング遷移時間を設定すると，このような場合に，設定した時間の経過後，障害から復旧したノードでリングポートのデータ転送用 VLAN のブロッキング状態を解除して，一部の通信を復旧できます。

リングポートフォワーディング遷移時間は，装置，Ring Protocol プログラム，またはリングポートの障害が復旧したときに設定されます。なお，マスタノードでは，リングポートフォワーディング遷移時間がタイムアウトしたときに，リング状態が障害状態の場合だけ，該当ポートのデータ転送用 VLAN をフォワーディング状態に変更します。

リングポートフォワーディング遷移時間中にリング状態が障害状態以外の状態に遷移した場合，リングポートフォワーディング遷移時間のタイマは解除され，該当ポートのデータ転送用 VLAN 状態はリング状態の遷移に応じて次に示す状態に変更されます。

リング状態が障害状態から経路切り戻し抑止状態に遷移した場合

　ブロッキング状態を維持します。

リング状態が障害状態から正常状態に遷移した場合

　「表 7–3　復旧検出時のデータ転送用リング VLAN 状態」を参照してください。

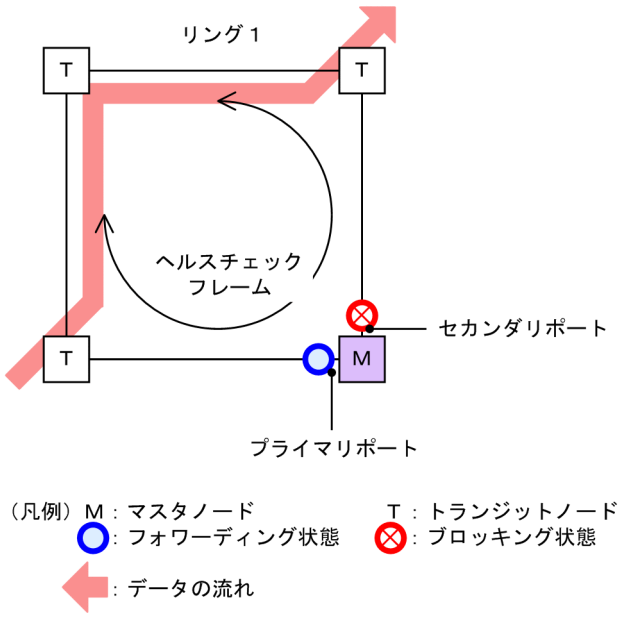
リングポートフォワーディング遷移時間中に系切替が発生した場合，新運用系 BCU でリングポートフォワーディング遷移時間のタイマを再設定します。このため，データ転送用 VLAN 状態は，リングポートフォワーディング遷移時間の設定値より長い時間ブロッキング状態となります。また，リングポートフォワーディング遷移時間中にコンフィグレーションコマンド forwarding-shift-time で設定値を変更した場合，変更後の設定値は，次回のリンク障害復旧時および系切替時に反映されます。

7.3　シングルリングの動作概要

7.3.1　リング正常時の動作

シングルリングでのリング正常時の動作について次の図に示します。

図 7-8　リング正常時の動作



(1)　マスタノード動作

片方向リンク障害による障害誤検出を防止するために，二つのリングポートからヘルスチェックフレームを送信します。あらかじめ設定された時間内に，両方向のヘルスチェックフレームを受信するか監視します。データフレームの転送は，プライマリポートで行います。セカンダリポートはブロッキング状態になっているため，データフレームの転送および MAC アドレス学習は行いません。

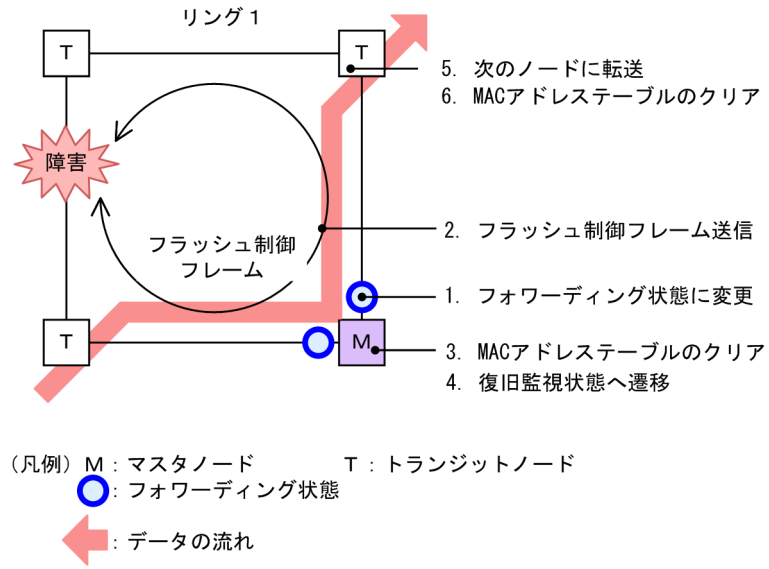
(2)　トランジットノード動作

トランジットノードでは，マスタノードが送信するヘルスチェックフレームの監視は行いません。ヘルスチェックフレームを受信すると，リング内の次ノードに転送します。データフレームの転送は，両リングポートで行います。

7.3.2　障害検出時の動作

シングルリングでのリング障害検出時の動作について次の図に示します。

図 7-9　リング障害時の動作



(1)　マスタノード動作

あらかじめ設定された時間内に，両方向のヘルスチェックフレームを受信しなければ障害と判断します。障害を検出したマスタノードは，次に示す手順で切り替え動作を行います。

1. データ転送用リング VLAN 状態の変更

セカンダリポートのリング VLAN 状態をブロッキング状態からフォワーディング状態に変更します。障害検出時のリング VLAN 状態は次の表のように変更します。

表 7-2　障害検出時のデータ転送用リング VLAN 状態

リングポート	変更前（正常時）	変更後（障害時）
プライマリポート	フォワーディング状態	フォワーディング状態
セカンダリポート	ブロッキング状態	フォワーディング状態

2. フラッシュ制御フレームの送信

マスタノードのプライマリポートおよびセカンダリポートからフラッシュ制御フレームを送信します。

3. MAC アドレステーブルのクリア

リングポートに関する MAC アドレステーブルエントリのクリアを行います。MAC アドレステーブルエントリをクリアすることで，迂回経路へ切り替えられます。

4. 監視状態の変更

リング障害を検出すると，マスタノードは障害監視状態から復旧監視状態に遷移します。

(2)　トランジットノード動作

障害を検出したマスタノードから送信されるフラッシュ制御フレームを受信すると，トランジットノードでは次に示す動作を行います。

5. フラッシュ制御フレームの転送

受信したフラッシュ制御フレームを次のノードに転送します。

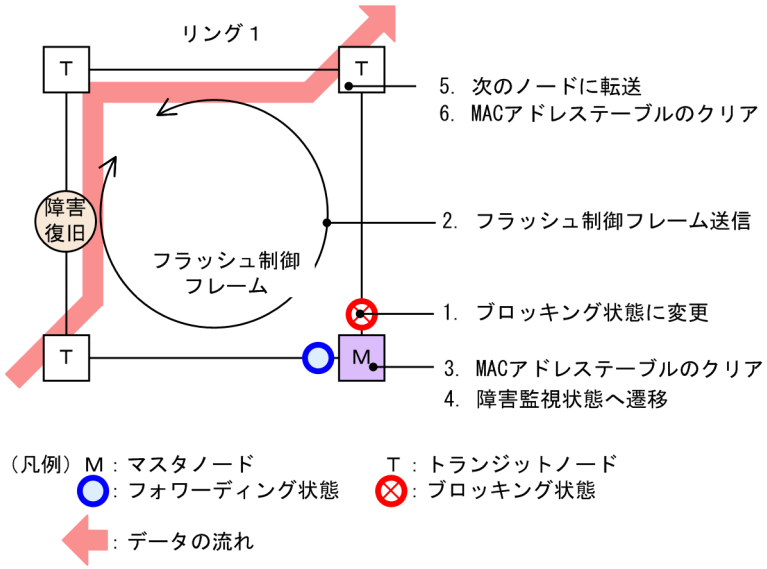
6. MAC アドレステーブルのクリア

リングポートに関する MAC アドレステーブルエントリのクリアを行います。MAC アドレステーブルエントリをクリアすることで，迂回経路へ切り替えられます。

7.3.3　復旧検出時の動作

シングルリングでのリング障害復旧時の動作について次の図に示します。

図 7-10　障害復旧時の動作



(1)　マスタノード動作

リング障害を検出している状態で，自身が送出したヘルスチェックフレームを受信すると，リング障害が復旧したと判断し，次に示す復旧動作を行います。

1. データ転送用リング VLAN 状態の変更

セカンダリポートのリング VLAN 状態をフォワーディング状態からブロッキング状態に変更します。復旧検出時のリング VLAN 状態は次の表のように変更します。

表 7-3　復旧検出時のデータ転送用リング VLAN 状態

リングポート	変更前（障害時）	変更後（復旧時）
プライマリポート	フォワーディング状態	フォワーディング状態
セカンダリポート	フォワーディング状態	ブロッキング状態

2. フラッシュ制御フレームの送信

マスタノードのプライマリポートおよびセカンダリポートからフラッシュ制御フレームを送信します。なお，リング障害復旧時は，各トランジットノードが転送したフラッシュ制御フレームがマスタノードへ戻ってきますが，マスタノードでは受信しても廃棄します。

3. MAC アドレステーブルのクリア

リングポートに関する MAC アドレステーブルエントリのクリアを行います。

4. 監視状態の変更

リング障害の復旧を検出すると，マスタノードは復旧監視状態から障害監視状態に遷移します。

(2) トランジットノード動作

マスタノードから送信されるフラッシュ制御フレームを受信すると，次に示す動作を行います。

5. フラッシュ制御フレームの転送
   受信したフラッシュ制御フレームを次のノードに転送します。
6. MAC アドレステーブルクリア
   リングポートに関する MAC アドレステーブルエントリのクリアを行います。

7.3.4 経路切り戻し抑止および解除時の動作

マスタノードに経路切り戻し抑止機能を適用すると，リングの障害復旧を検出した場合に，マスタノードは復旧抑止状態になり，すぐには復旧動作を行いません。本機能を有効にするには，マスタノードにコンフィグレーションコマンド preempt-delay の設定が必要です。

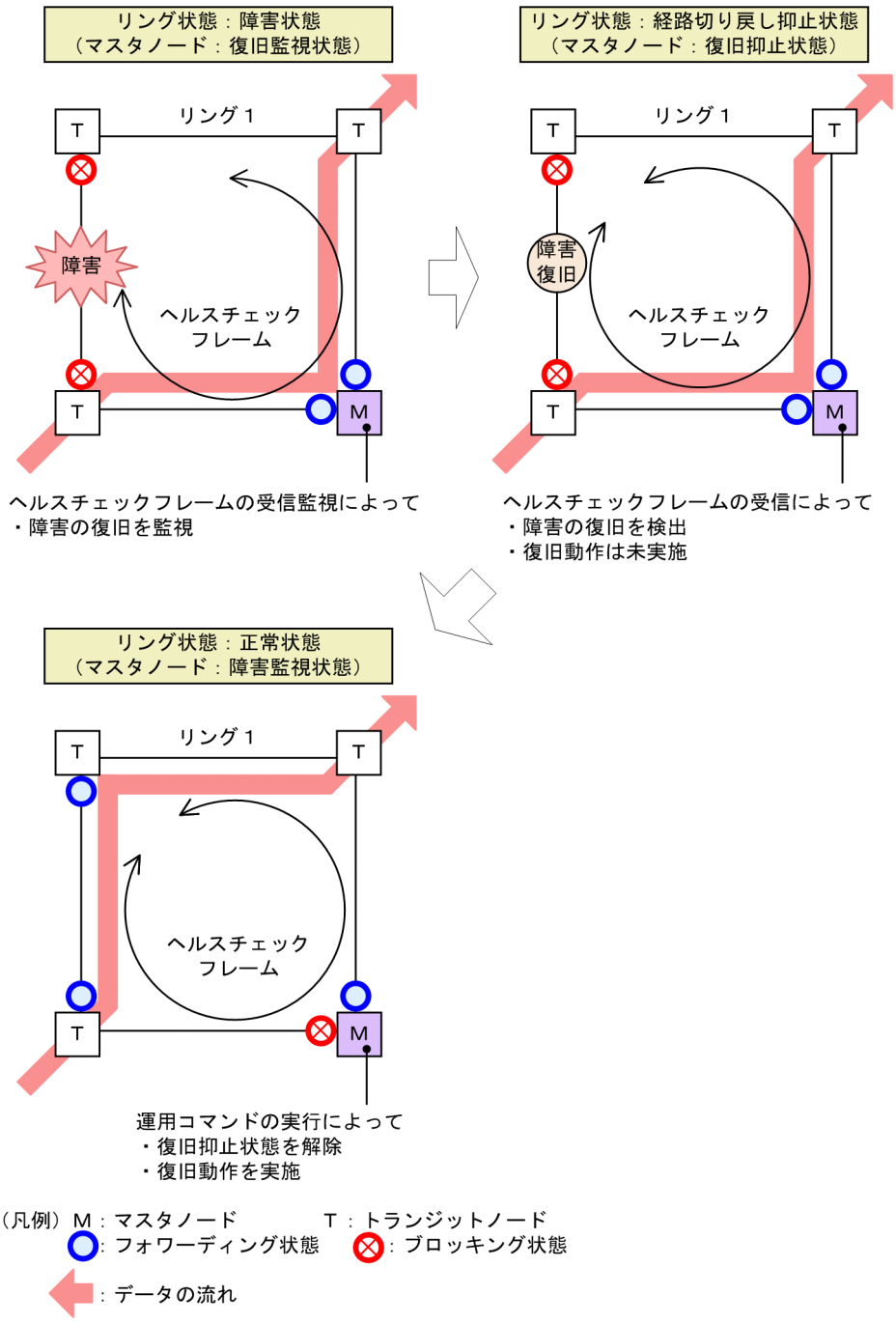
なお，復旧抑止状態は，次の契機で解除します。

- 運用コマンド clear axrp preempt-delay の実行によって，経路切り戻し抑止が解除された場合
- コンフィグレーションコマンド preempt-delay で指定した，経路切り戻し抑止時間が経過した場合
- 経路切り戻し抑止機能を有効にするコンフィグレーションコマンド preempt-delay を削除した場合

復旧抑止状態が解除されると，復旧動作を行います。復旧が完了すると，マスタノードは障害監視状態に遷移します。また，復旧抑止状態でリングの障害を検出すると，マスタノードは復旧監視状態に遷移します。

運用コマンド clear axrp preempt-delay の実行によって経路切り戻し抑止を解除した場合の動作を次の図に示します。その他の契機で解除した場合も，同様の動作となります。

図 7-11　運用コマンドの実行によって経路切り戻し抑止を解除した場合の動作



また，次に示すイベントが発生した場合は経路の切り戻し抑止を解除して，マスタノードが復旧監視状態に遷移します。

- 装置起動（運用コマンド reload および update software の実行を含む）
- Ring Protocol プログラムの再起動（運用コマンド restart axrp の実行を含む）

復旧抑止状態で系切替が発生した場合，新運用系 BCU で経路切り戻し抑止時間のタイマを再設定します。このため，経路切り戻し抑止時間の設定値より長い時間復旧抑止状態となります。また，復旧抑止状態でコ

ンフィグレーションコマンド preempt-delay で設定値を変更した場合，変更後の設定値は，次回のリング障害復旧時および系切替時に反映されます。

7.4　マルチリングの動作概要

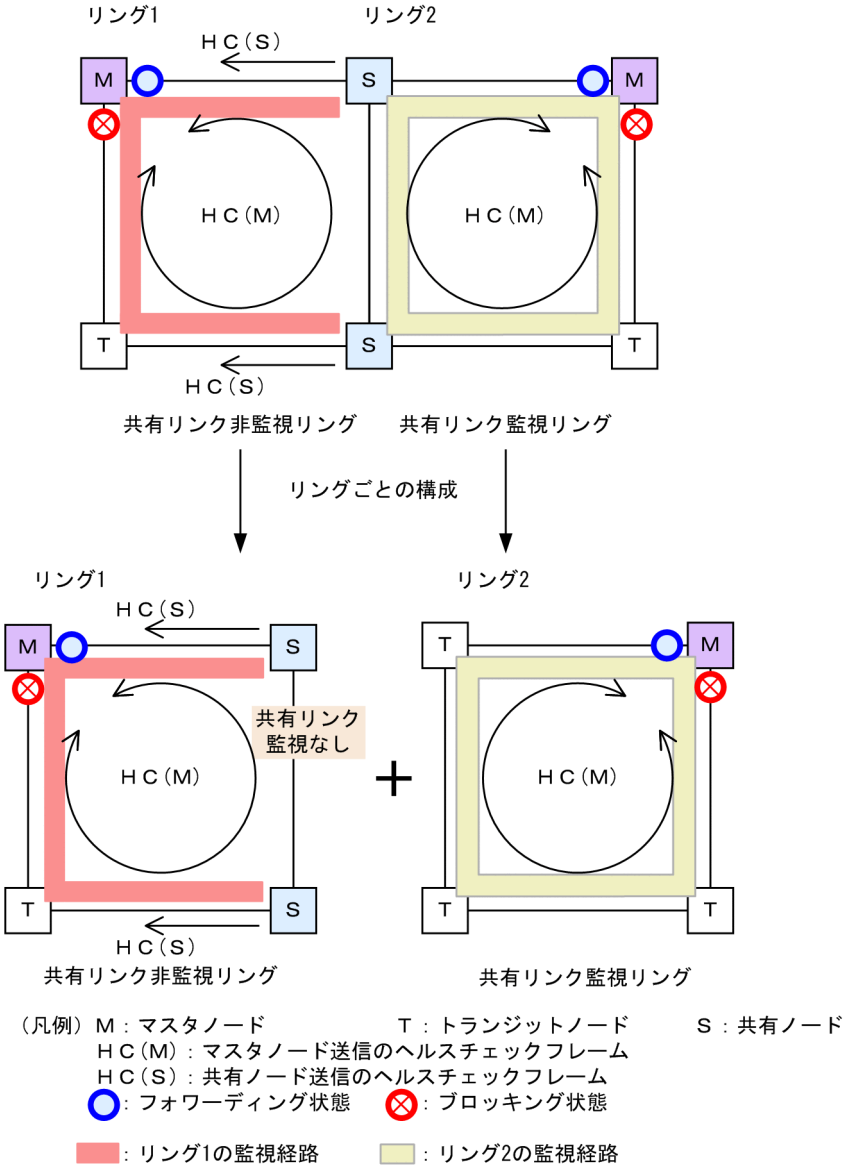
マルチリング構成のうち，共有リンクありのマルチリング構成について説明します。共有リンクなしのマルチリング構成については，シングルリング時の動作と同様ですので，「7.3　シングルリングの動作概要」を参照してください。

なお，この節では，HC はヘルスチェックフレームを意味し，HC(M)はマスタノードが送信するヘルスチェックフレーム，HC(S)は共有ノードが送信するヘルスチェックフレームを表します。

7.4.1　リング正常時の動作

共有リンクありのマルチリング構成でのリング正常時の状態について次の図に示します。

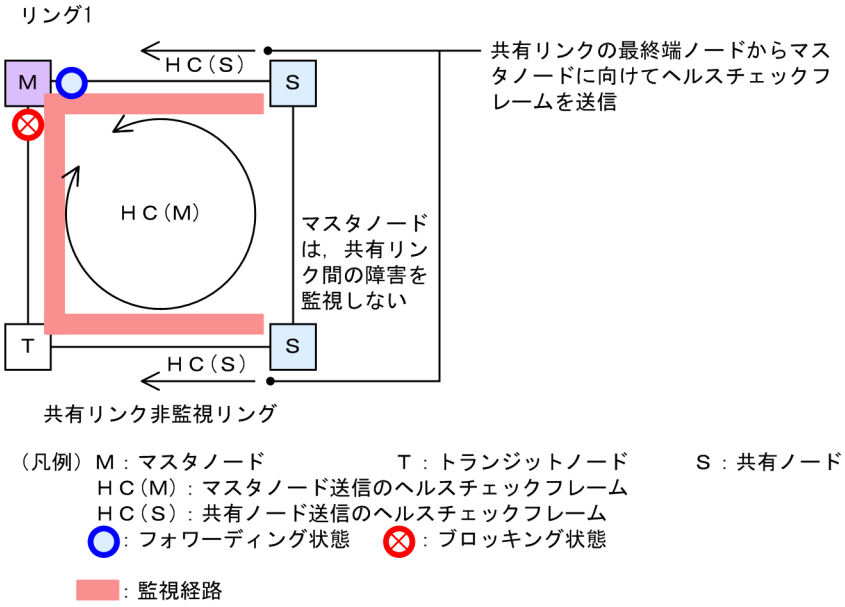
図 7-12　リング正常時の状態



(1)　共有リンク非監視リング

共有リンク非監視リングは，マスタノード 1 台とトランジットノード数台で構成します。しかし，共有リンクの障害を監視しないため，補助的な役割として，共有リンクの両端に位置する共有リンク非監視リングの最終端ノード（共有ノード）から，ヘルスチェックフレームをマスタノードに向けて送信します。このヘルスチェックフレームは，二つのリングポートのうち，共有リンクではない方のリングポートから送信します。これによって，共有リンク非監視リングのマスタノードは，共有リンクで障害が発生した場合に，自身が送信したヘルスチェックフレームが受信できなくなっても，共有リンク非監視リングの最終端ノード（共有ノード）からのヘルスチェックフレームが受信できている間は障害を検出しないようにできます。

図 7-13　共有リンク非監視リングでの正常時の動作



(a)　マスタノード動作

片方向リンク障害による障害誤検出を防止するために，二つのリングポートからヘルスチェックフレーム（HC(M)）を送信します。あらかじめ設定した時間内に，両方向の HC(M)を受信するか監視します。マスタノードが送信した HC(M)とは別に，共有リンクの両端に位置する共有リンク非監視リングの最終端ノード（共有ノード）から送信したヘルスチェックフレーム（HC(S)）についても合わせて受信を監視します。データフレームの転送は，プライマリポートで行います。セカンダリポートはブロッキング状態になっているため，データフレームの転送および MAC アドレス学習は行いません。

(b)　トランジットノード動作

トランジットノードの動作は，シングルリング時と同様です。トランジットノードは，HC(M)および HC(S)を監視しません。HC(M)や HC(S)を受信すると，リング内の次ノードに転送します。データフレームの転送は，両リングポートで行います。

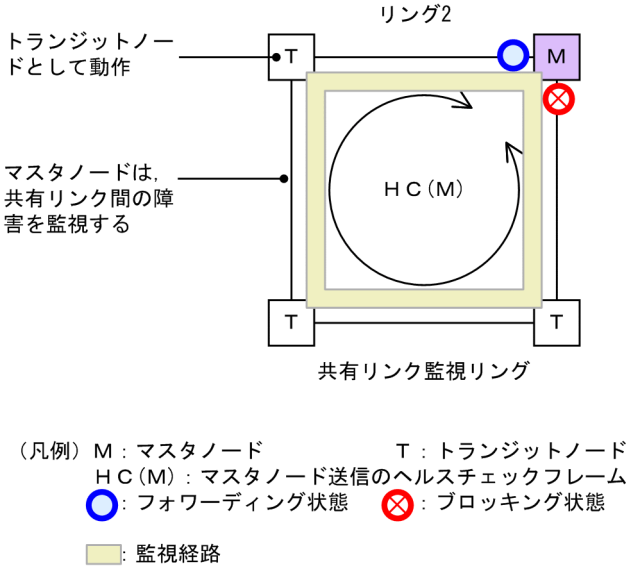
(c)　共有リンク非監視リングの最終端ノード動作

共有リンク非監視リングの最終端ノード（共有ノード）は，共有リンク非監視リングのマスタノードに向けて HC(S)の送信を行います。HC(S)の送信は，二つのリングポートのうち，共有リンクではない方のリングポートから送信します。マスタノードが送信する HC(M)や，データフレームの転送については，トランジットノードの場合と同様となります。

(2)　共有リンク監視リング

共有リンク監視リングは，シングルリング時と同様に，マスタノード 1 台と，そのほか数台のトランジットノードとの構成となります。共有リンクの両端に位置するノードは，シングルリング時と同様にマスタノードまたはトランジットノードとして動作します。

図 7-14　共有リンク監視リングでの正常時の動作



(a)　マスタノード動作

片方向リンク障害による障害誤検出を防止するために，二つのリングポートからヘルスチェックフレーム（HC(M)）を送信します。あらかじめ設定された時間内に，両方向の HC(M)を受信するかを監視します。データフレームの転送は，プライマリポートで行います。セカンダリポートはブロッキング状態になっているため，データフレームの転送および MAC アドレス学習は行いません。

(b)　トランジットノード動作

トランジットノードの動作は，シングルリング時と同様です。トランジットノードは，マスタノードが送信した HC(M)を監視しません。HC(M)を受信すると，リング内の次ノードに転送します。データフレームの転送は，両リングポートで行います。

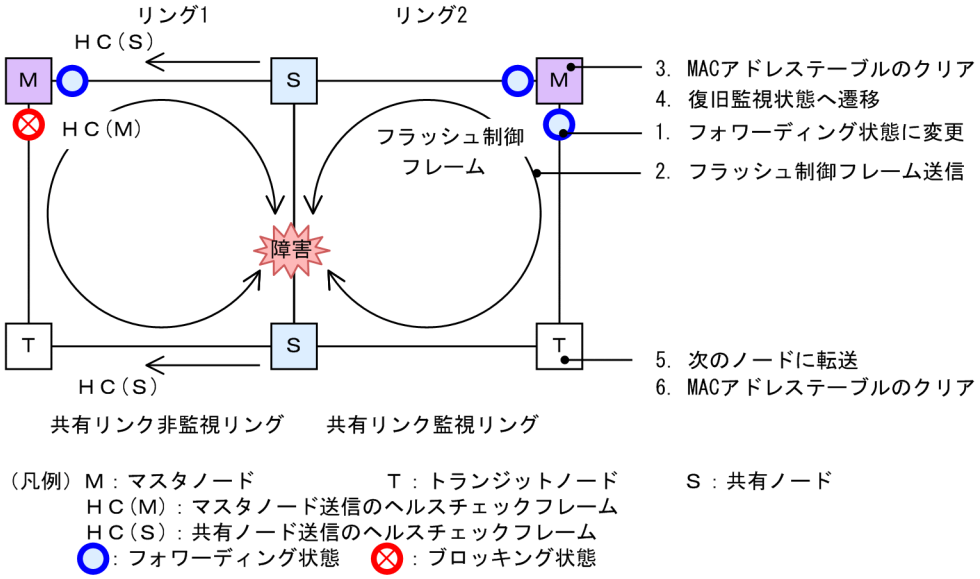
7.4.2　共有リンク障害・復旧時の動作

共有リンクありのマルチリング構成時に，共有リンク間で障害が発生した際の障害および復旧動作について説明します。

(1)　障害検出時の動作

共有リンクの障害を検出した際の動作について次の図に示します。

図 7-15　共有リング障害時の動作



(a)　共有リンク監視リングのマスタノード動作

共有リンクで障害が発生すると，マスタノードは両方向の HC(M)を受信できなくなり，リング障害を検出します。障害を検出したマスタノードはシングルリング時と同様に，次に示す手順で障害動作を行います。

1. データ転送用リング VLAN 状態の変更
2. フラッシュ制御フレームの送信
3. MAC アドレステーブルのクリア
4. 監視状態の変更

(b)　共有リンク監視リングのトランジットノード動作

シングルリング時と同様に，マスタノードから送信されるフラッシュ制御フレームを受信すると次に示す動作を行います。

5. フラッシュ制御フレームの転送
6. MAC アドレステーブルのクリア

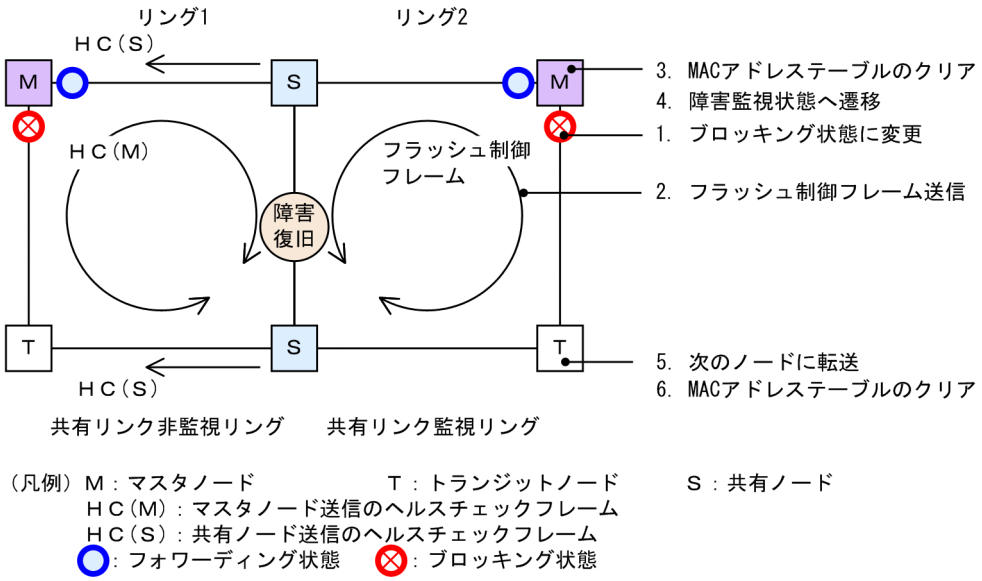
(c)　共有リンク非監視リングのマスタノードおよびトランジットノード動作

共有リンク非監視リングのマスタノードは，共有リンクでのリング障害を検出しないため，障害動作は行いません。このため，トランジットノードについても経路の切り替えは発生しません。

(2)　復旧検出時の動作

共有リンクの障害復旧を検出した際の動作について次の図に示します。

図 7-16　共有リンク復旧時の動作



(a)　共有リンク監視リングのマスタノード動作

リング障害を検出している状態で，自身が送信した HC(M)を受信すると，リング障害が復旧したと判断し，シングルリング時と同様に，次に示す手順で復旧動作を行います。

1. データ転送用リング VLAN 状態の変更
2. フラッシュ制御フレームの送信
3. MAC アドレステーブルのクリア
4. 監視状態の変更

(b)　共有リンク監視リングのトランジットノード動作

シングルリング時と同様に，マスタノードから送信されるフラッシュ制御フレームを受信すると次に示す動作を行います。

5. フラッシュ制御フレームの転送
6. MAC アドレステーブルのクリア

(c)　共有リンク非監視リングのマスタノードおよびトランジットノード動作

共有リンク非監視リングのマスタノードは，リング障害を検出していないため，トランジットノードを含め，復旧動作は行いません。

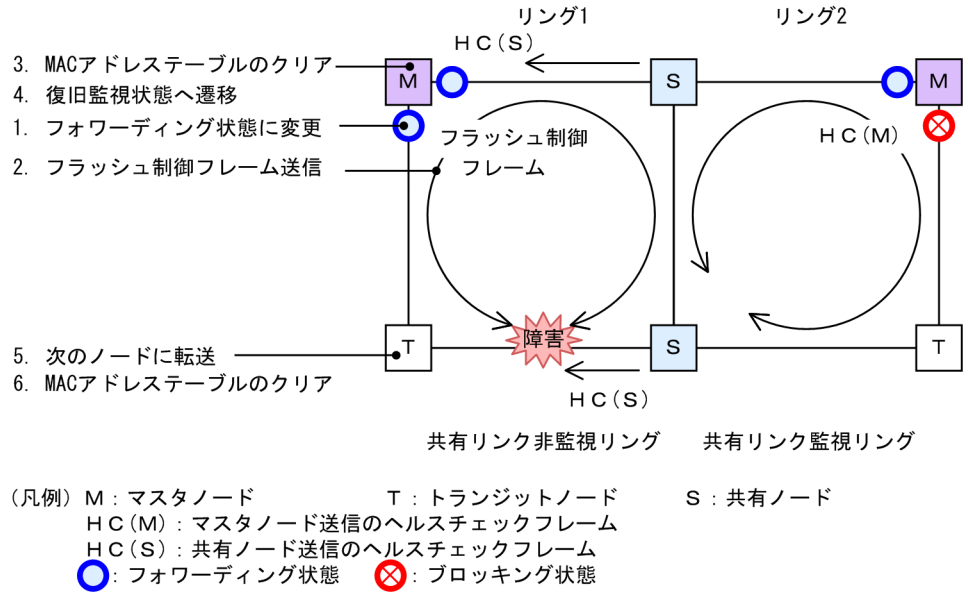
7.4.3　共有リンク非監視リングでの共有リンク以外の障害・復旧時の動作

共有リンク非監視リングでの，共有リンク以外のリング障害および復旧時の動作について説明します。

(1)　障害検出時の動作

共有リンク非監視リングでの共有リンク以外の障害を検出した際の動作について次の図に示します。

図 7-17　共有リンク非監視リングにおける共有リンク以外のリング障害時の動作



（凡例）Ｍ：マスタノード　　Ｔ：トランジットノード　　Ｓ：共有ノード
ＨＣ（Ｍ）：マスタノード送信のヘルスチェックフレーム
ＨＣ（Ｓ）：共有ノード送信のヘルスチェックフレーム
：フォワーディング状態　：ブロッキング状態

(a)　共有リンク非監視リングのマスタノード動作

共有リンク非監視リングのマスタノードは，自身が送信した両方向の HC(M)と共有ノードが送信した HC(S)が共に未受信となりリング障害を検出します。障害を検出したマスタノードの動作はシングルリング時と同様に，次に示す手順で障害動作を行います。

1. データ転送用リング VLAN 状態の変更
2. フラッシュ制御フレームの送信
3. MAC アドレステーブルのクリア
4. 監視状態の変更

(b)　共有リンク非監視リングのトランジットノードおよび共有ノード動作

シングルリング時と同様に，マスタノードから送信されるフラッシュ制御フレームを受信すると次に示す動作を行います。

5. フラッシュ制御フレームの転送
6. MAC アドレステーブルのクリア

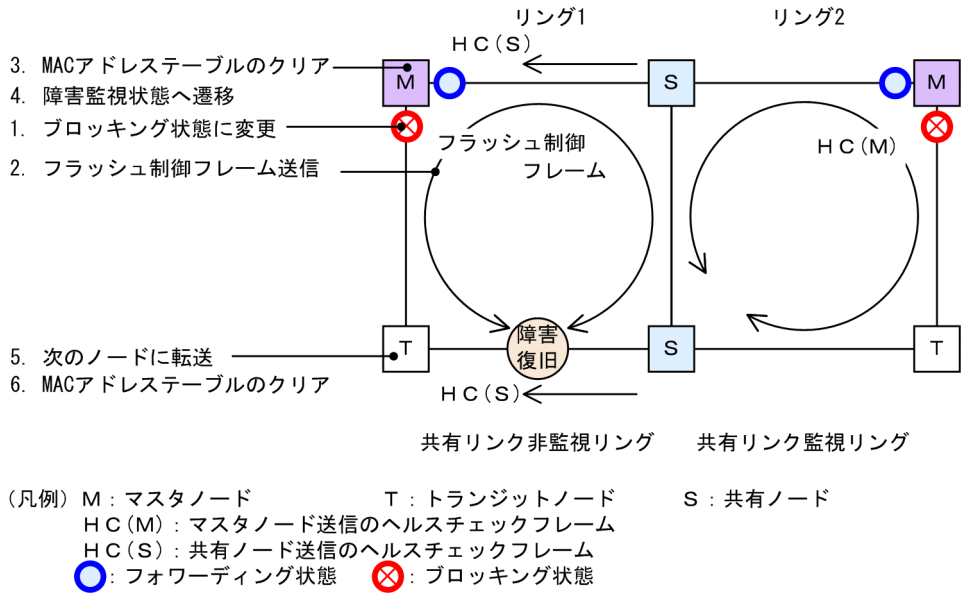
(c)　共有リンク監視リングのマスタノードおよびトランジットノード動作

共有リンク監視リング内では障害が発生していないため，障害動作は行いません。

(2)　復旧検出時の動作

共有リンク非監視リングでの共有リンク以外の障害が復旧した際の動作について次の図に示します。

図 7-18　共有リンク非監視リングでの共有リンク以外のリング障害復旧時の動作



（凡例）Ｍ：マスタノード　　Ｔ：トランジットノード　　Ｓ：共有ノード
ＨＣ（M）：マスタノード送信のヘルスチェックフレーム
ＨＣ（Ｓ）：共有ノード送信のヘルスチェックフレーム
：フォワーディング状態　：ブロッキング状態

(a)　共有リンク非監視リングのマスタノード動作

リング障害を検出している状態で，自身が送信した HC(M)を受信するか，または共有ノードが送信した HC(S)を両方向から受信すると，リング障害が復旧したと判断し，シングルリング時と同様に，次に示す手順で復旧動作を行います。

1. データ転送用リング VLAN 状態の変更
2. フラッシュ制御フレームの送信
3. MAC アドレステーブルのクリア
4. 監視状態の変更

(b)　共有リンク非監視リングのトランジットノードおよび共有ノード動作

シングルリング時と同様に，マスタノードから送信されるフラッシュ制御フレームを受信すると次に示す動作を行います。

5. フラッシュ制御フレームの転送
6. MAC アドレステーブルのクリア

(c)　共有リンク監視リングのマスタノードおよびトランジットノード動作

共有リンク監視リング内では障害が発生していないため，復旧動作は行いません。

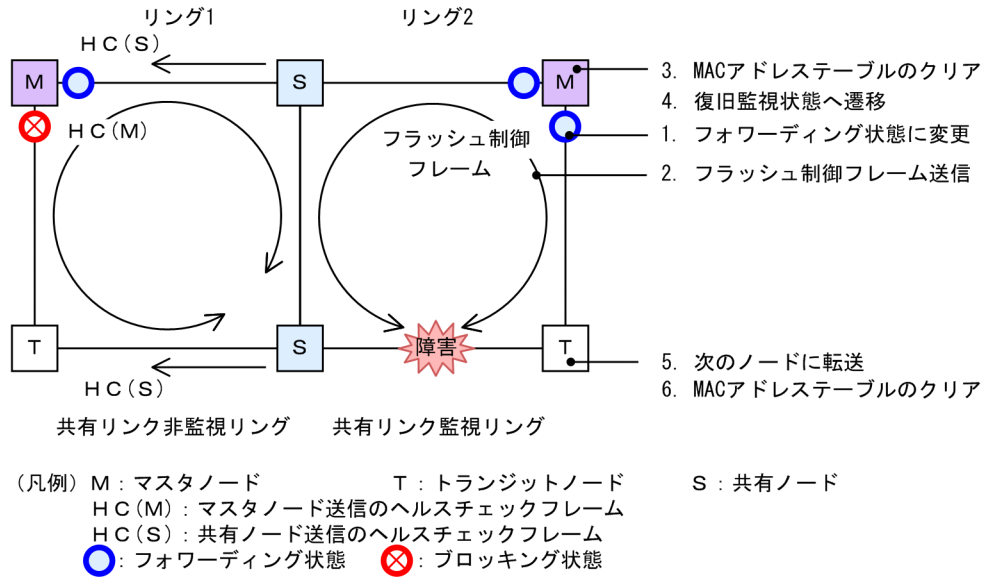
7.4.4　共有リンク監視リングでの共有リンク以外の障害・復旧時の動作

共有リンク監視リングでの共有リンク以外のリング障害および復旧時の動作について説明します。

(1)　障害検出時の動作

共有リンク監視リングでの共有リンク以外の障害を検出した際の動作について次の図に示します。

図 7-19　共有リンク監視リングでの共有リンク以外のリング障害時の動作



(a)　共有リンク監視リングのマスタノード動作

共有リンク監視リング内で障害が発生すると，マスタノードは両方向の HC(M)を受信できなくなり，リング障害を検出します。障害を検出したマスタノードはシングルリング時と同様に，次に示す手順で障害動作を行います。

1. データ転送用リング VLAN 状態の変更
2. フラッシュ制御フレームの送信
3. MAC アドレステーブルのクリア
4. 監視状態の変更

(b)　共有リンク監視リングのトランジットノード動作

シングルリング時と同様に，マスタノードから送信されるフラッシュ制御フレームを受信すると次に示す動作を行います。

5. フラッシュ制御フレームの転送
6. MAC アドレステーブルのクリア

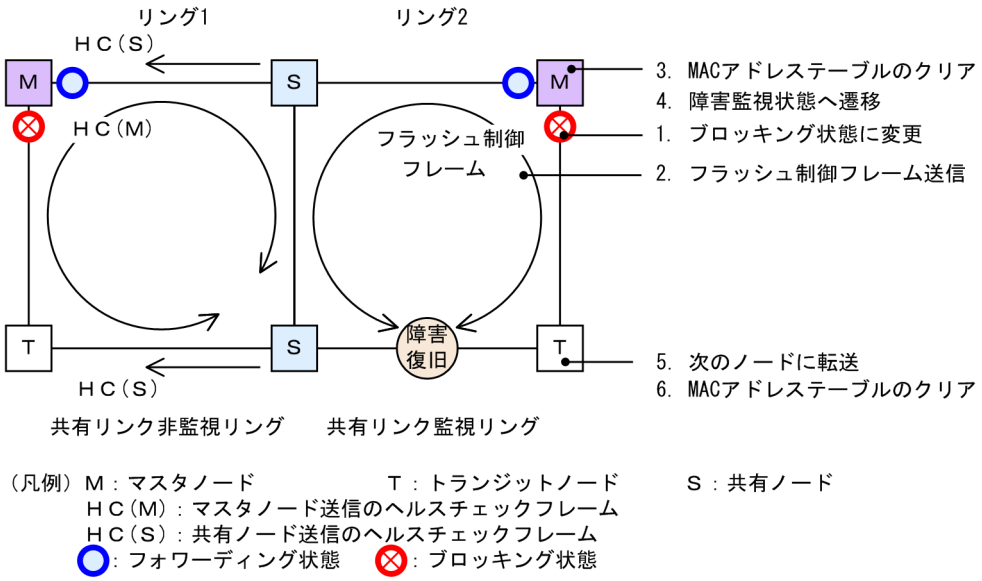
(c)　共有リンク非監視リングのマスタノードおよびトランジットノード（共有ノード）動作

共有リンク非監視リング内では障害が発生していないため，障害動作は行いません。

(2)　復旧検出時の動作

共有リンク監視リングでの共有リンク以外の障害が復旧した際の動作について次の図に示します。

図 7-20　共有リンク監視リングでの共有リンク以外のリング障害復旧時の動作



(a)　共有リンク監視リングのマスタノード動作

リング障害を検出している状態で，自身が送信した HC(M)を受信すると，リング障害が復旧したと判断し，シングルリング時と同様に，次に示す手順で復旧動作を行います。

1. データ転送用リング VLAN 状態の変更
2. フラッシュ制御フレームの送信
3. MAC アドレステーブルのクリア
4. 監視状態の変更

(b)　共有リンク監視リングのトランジットノード動作

シングルリング時と同様に，マスタノードから送信されるフラッシュ制御フレームを受信すると次に示す動作を行います。

5. フラッシュ制御フレームの転送
6. MAC アドレステーブルのクリア

(c)　共有リンク非監視リングのマスタノードおよびトランジットノード（共有ノード）動作

共有リンク非監視リング内では障害が発生していないため，復旧動作は行いません。

7.4.5　経路切り戻し抑止および解除時の動作

マルチリング構成での経路切り戻し抑止および解除時の動作については，シングルリング時の動作と同様ですので，「7.3　シングルリングの動作概要」を参照してください。

7.5　Ring Protocol のネットワーク設計

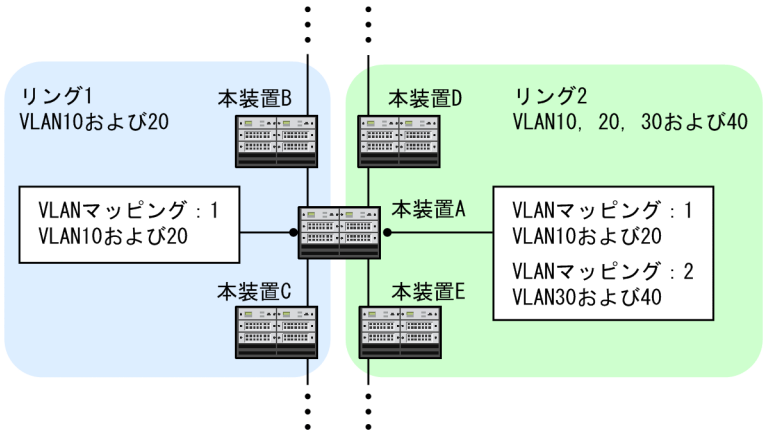
7.5.1　VLAN マッピングの使用方法

(1)　VLAN マッピングとデータ転送用 VLAN

マルチリング構成などで，一つの装置に複数のリング ID を設定するような場合，それぞれのリング ID に複数の同一 VLAN を設定する必要があります。このとき，データ転送用 VLAN として使用する VLAN のリスト（これを **VLAN マッピング**と呼びます）をあらかじめ設定しておくと，マルチリング構成時のデータ転送用 VLAN の設定を簡略できたり，コンフィグレーションの設定誤りによるループなどを防止できたりします。

VLAN マッピングは，データ転送用に使用する VLAN を VLAN マッピング ID に割り当てて使用します。この VLAN マッピング ID を VLAN グループに設定して，データ転送用 VLAN として管理します。

図 7-21　リングごとの VLAN マッピングの割り当て例



7.5.2　制御 VLAN の forwarding-delay-time の使用方法

トランジットノードの装置起動やプログラム再起動（運用コマンド restart axrp）など，Ring Protocol が初期状態から動作する場合，データ転送用 VLAN はブロッキング状態になっています。トランジットノードは，マスタノードが送信するフラッシュ制御フレームを受信することでこのブロッキング状態を解除します。しかし，プログラム再起動時は，マスタノードの障害監視時間（health-check holdtime）が長いと，リングネットワークの状態変化を認識できないおそれがあります。この場合，リングポートフォワーディング遷移時間（forwarding-shift-time）がタイムアウトするまでブロッキング状態は解除されないため，トランジットノードのデータ転送用 VLAN は通信できない状態になります。制御 VLAN のフォワーディング遷移時間（forwarding-delay-time）を設定すると次に示す手順で動作するため，このようなケースを回避できます。

1. トランジットノードは，装置起動，プログラム再起動後に，制御 VLAN をいったんブロッキング状態にします。
2. トランジットノードの制御 VLAN がブロッキング状態になったため，マスタノードで障害を検出します（ただし，装置起動時はこれ以前に障害を検出しています）。このため，通信は迂回経路に切り替わります。
3. トランジットノードは，制御 VLAN のフォワーディング遷移時間（forwarding-delay-time）のタイムアウトによって制御 VLAN のブロッキング状態を解除します。

4. マスタノードはヘルスチェックフレームを受信することで復旧を検出して，フラッシュ制御フレームを送信します。
5. トランジットノードは，このフラッシュ制御フレームを受信することでデータ転送用 VLAN のブロッキング状態を解除します。これによってデータ転送用 VLAN での通信が再開され，リングネットワーク全体でも通常の通信経路に復旧します。

(1)　制御 VLAN のフォワーディング遷移時間（forwarding-delay-time）と障害監視時間（health-check holdtime）の関係について

制御 VLAN のフォワーディング遷移時間（forwarding-delay-time）は，障害監視時間（health-check holdtime）より大きな値を設定してください。制御 VLAN のフォワーディング遷移時間（forwarding-delay-time）は，障害監視時間（health-check holdtime）の 2 倍程度を目安として設定することを推奨します。障害監視時間（health-check holdtime）より小さな値を設定した場合，マスタノードで障害を検出できません。したがって，迂回経路への切り替えが行われないため，通信断の時間が長くなるおそれがあります。

7.5.3　プライマリポートの自動決定

マスタノードのプライマリポートは，ユーザが設定した二つのリングポートの情報に従って，自動で決定します。次の表に示すように，優先度の高い方がプライマリポートとして動作します。また，VLAN グループごとに優先度を逆にすることで，ユーザが特に意識することなく，経路の振り分けができるようになります。

表 7-4　プライマリポートの選択方式（VLAN グループ＃1）

リングポート＃1	リングポート＃2	優先ポート
物理ポート	物理ポート	• NIF 番号の小さい方がプライマリポートとして動作 • NIF 番号が同一の場合は，ポート番号の小さい方がプライマリポートとして動作
物理ポート	チャネルグループ	物理ポート側がプライマリポートとして動作
チャネルグループ	物理ポート	物理ポート側がプライマリポートとして動作
チャネルグループ	チャネルグループ	チャネルグループ番号の小さい方がプライマリポートとして動作

表 7-5　プライマリポートの選択方式（VLAN グループ＃2）

リングポート＃1	リングポート＃2	優先ポート
物理ポート	物理ポート	• NIF 番号が大きい方がプライマリポートとして動作 • NIF 番号が同一の場合は，ポート番号の大きい方がプライマリポートとして動作
物理ポート	チャネルグループ	チャネルグループ側がプライマリポートとして動作
チャネルグループ	物理ポート	チャネルグループ側がプライマリポートとして動作
チャネルグループ	チャネルグループ	チャネルグループ番号の大きい方がプライマリポートとして動作

また，上記の決定方式以外に，コンフィグレーションコマンド axrp-primary-port を使って，ユーザが VLAN グループごとにプライマリポートを設定することもできます。

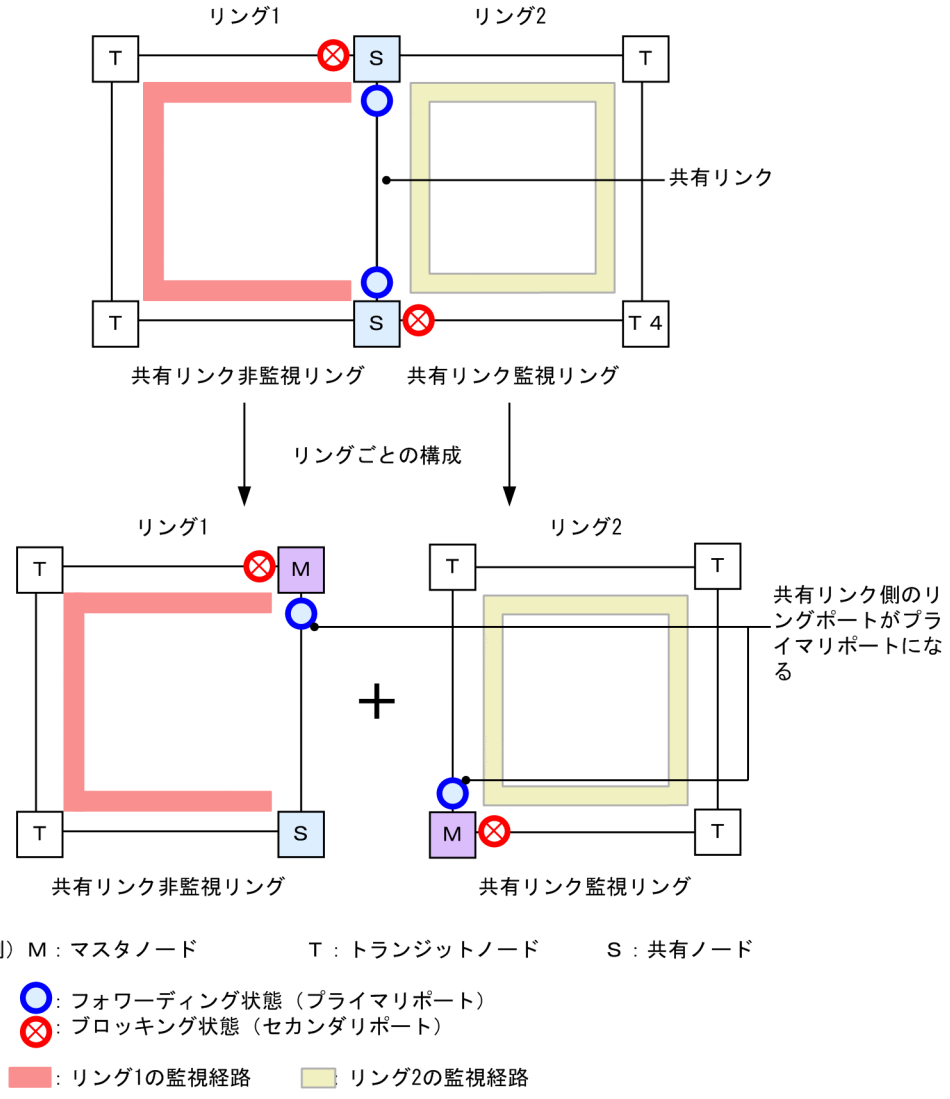
7.5.4　同一装置内でのノード種別混在構成

本装置が，二つの異なるリングに属している場合に，一方のリングではマスタノードとして，もう一方のリングではトランジットノードとして動作させられます。

7.5.5　共有ノードでのノード種別混在構成

共有リンクありのマルチリング構成で，共有リンクの両端に位置するノードをマスタノードとして動作させられます。この場合，マスタノードのプライマリポートは，データ転送用の VLAN グループに関係なく，必ず共有リンク側のリングポートになります。このため，本構成では，データ転送用の VLAN グループを二つ設定したことによる負荷分散は実現できません。

図 7-22　共有ノードをマスタノードとした場合のポート状態



7.5.6　リンクアグリゲーションを用いた場合の障害監視時間の設定

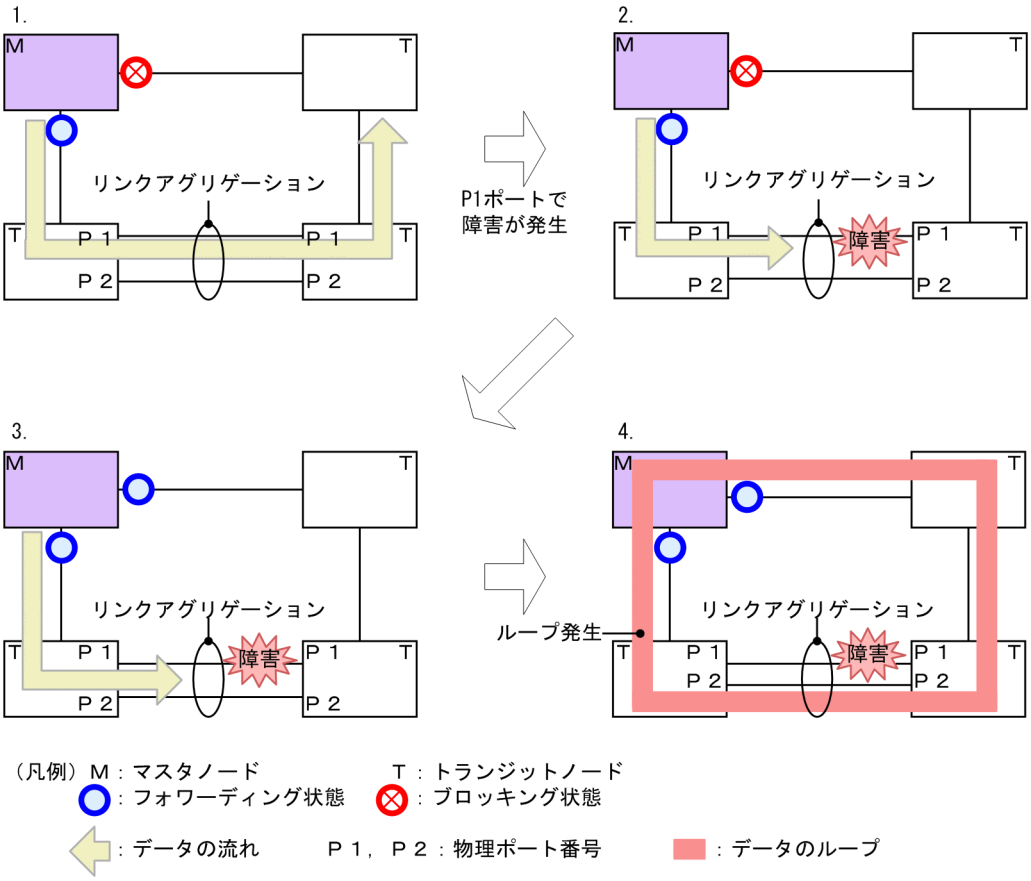
リングポートをリンクアグリゲーションで構成した場合に，ヘルスチェックフレームが転送されているリンクアグリゲーション内のポートに障害が発生すると，リンクアグリゲーションの切り替えまたは縮退動作が完了するまでの間，制御フレームが廃棄されます。このため，マスタノードの障害監視時間（health-check

holdtime）がリンクアグリゲーションの切り替えまたは縮退動作が完了する時間よりも短いと，マスタノードがリングの障害を誤検出し，経路の切り替えを行います。この結果，ループが発生するおそれがあります。

リングポートをリンクアグリゲーションで構成した場合は，マスタノードの障害監視時間をリンクアグリゲーションによる切り替えまたは縮退動作が完了する時間よりも大きくする必要があります。マスタノードの障害監視時間は 30 ミリ秒以上を目安として設定してください。

なお，LACP によるリンクアグリゲーションを使用する場合は，LACPDU の送信間隔の初期値が long（30 秒）となっているため，初期値を変更しないまま運用すると，ループが発生するおそれがあります。LACP によるリンクアグリゲーションを使用する際は，LACPDU の送信間隔を short（1 秒）に設定して，マスタノードの障害監視時間には 4 秒より大きい値を設定してください。

図 7-23　リンクアグリゲーション使用時の障害検出



1. マスタノードが送信するヘルスチェックフレームは，リンクアグリゲーション内の P1 を経由して通信しています。
2. P1 で障害が発生したため，リンクアグリゲーションとして縮退動作を実施します。縮退動作が完了するまで，フレームを廃棄します。
3. 縮退動作が完了するまではヘルスチェックフレームも廃棄されるため，マスタノードはヘルスチェックフレームのタイムアウトによって障害を検出して，障害動作を実施します。
4. リンクアグリゲーションの縮退動作が完了して，P2 を経由して通信することでループが発生します。

7.5.7　リンクダウン検出タイマおよびリンクアップ検出タイマとの併用

リングポートに使用しているポート（物理ポートまたはリンクアグリゲーションに属する物理ポート）のリンク状態が不安定な場合，マスタノードがリング障害やリング障害復旧を連続で検出してリングネットワークが不安定な状態になり，ループや長時間の通信断が発生するおそれがあります。このような状態を防ぐには，リングポートに使用しているポートに対して，リンクダウン検出タイマおよびリンクアップ検出タイマを設定します。リンクダウン検出タイマおよびリンクアップ検出タイマの設定については，「コンフィグレーションガイド Vol.1」「18.3.9　リンクダウン検出タイマの設定」および「コンフィグレーションガイド Vol.1」「18.3.10　リンクアップ検出タイマの設定」を参照してください。

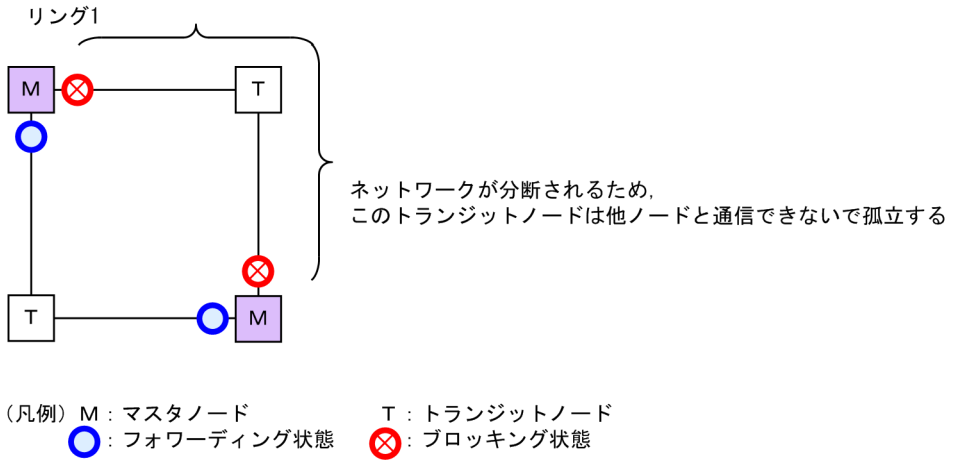
7.5.8　Ring Protocol の禁止構成

Ring Protocol を使用したネットワークでの禁止構成を次の図に示します。

(1)　同一リング内に複数のマスタノードを設定

同一のリング内に 2 台以上のマスタノードを設定しないでください。同一リング内に複数のマスタノードがあると，セカンダリポートがブロッキング状態になっているためにネットワークが分断されてしまい，適切な通信ができなくなります。

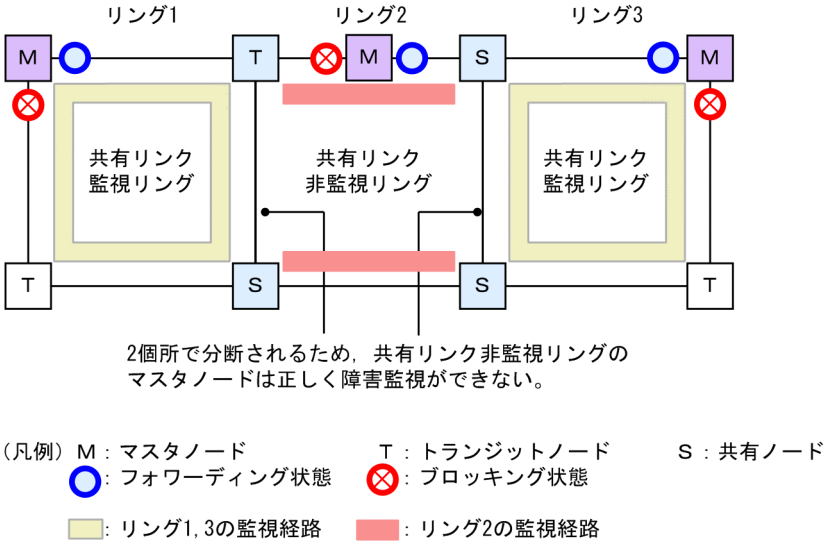
図 7-24　同一リング内に複数のマスタノードを設定



(2)　共有リンク監視リングが複数ある構成

共有リンクありのマルチリング構成では，共有リンク監視リングはネットワーク内で必ず一つとなるように構成してください。共有リンク監視リングが複数あると，共有リンク非監視リングでの障害監視が分断されるため，正しい障害監視ができなくなります。

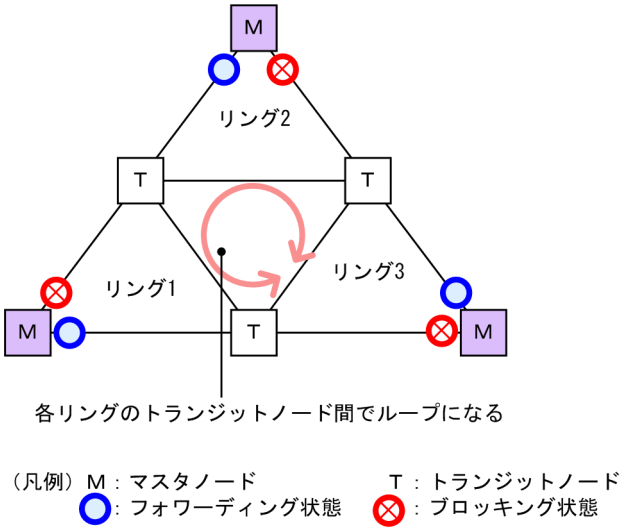
図 7-25　共有リンク監視リングが複数ある構成



(3)　ループになるマルチリング構成例

次に示す図のようなマルチリング構成を組むとトランジットノード間でループ構成となります。

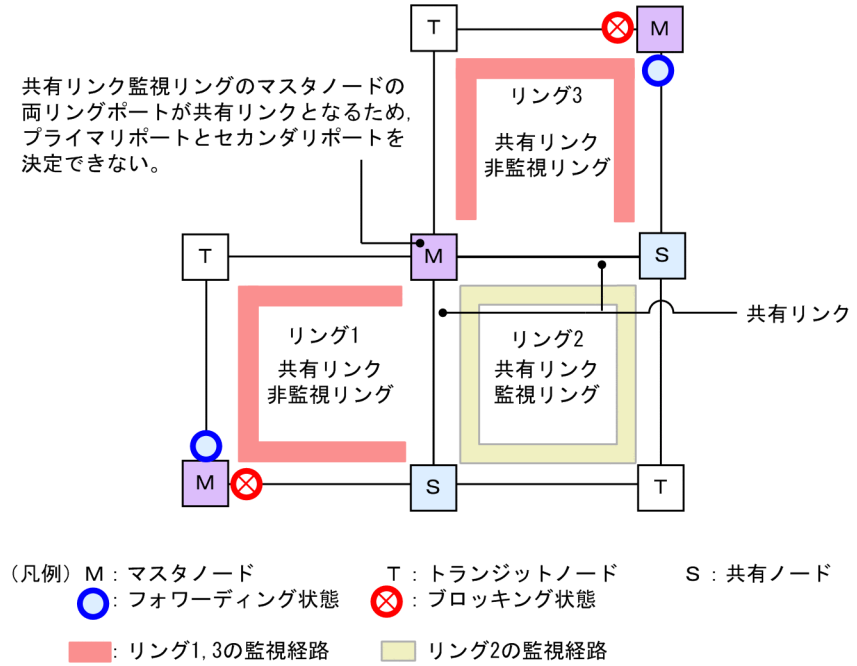
図 7-26　ループになるマルチリング構成



(4)　マスタノードのプライマリポートが決定できない構成

次の図のように，二つの共有リンク非監視リングの最終端に位置するノードにマスタノードを設定しないでください。このような構成の場合，マスタノードの両リングポートが共有リンクとなるため，プライマリポートを正しく決定できません。

図 7-27　マスタノードのプライマリポートが決定できない構成

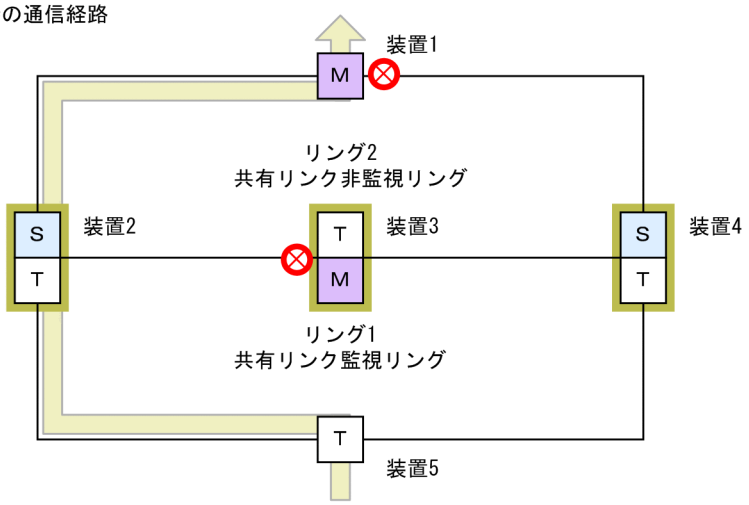


(5)　マスタノードの両リングポートが共有リンクとなる構成

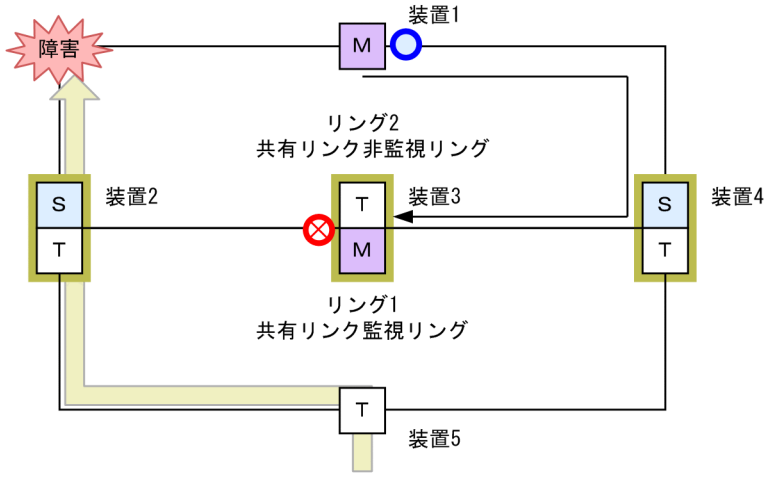
次の図のように，共有リンク上に共有リンク監視リングのマスタノードが存在するマルチリングを構成しないでください。このような構成では，共有リンク非監視リングで障害が発生した場合，共有リンク非監視リングでは経路が切り替わりますが，隣接する共有リンク監視リングでは経路が切り替わりません。この結果，共有リンク監視リングを構成する装置では古い MAC アドレス学習の情報が残るため，すぐに新しい通信経路に切り替わらないおそれがあります。また，共有リンク非監視リングのリング障害が復旧した場合も同様になります。

図 7-28　マスタノードの両リングポートが共有リンクとなる構成

●正常時の通信経路



●リング2　共有リンク非監視リング障害時の通信経路



（凡例）M：マスタノード　　T：トランジットノード
S：共有リンクの最終端ノード（トランジットノード）　：共有ノード
：フォワーディング状態　：ブロッキング状態　：フラッシュ制御フレーム
：データの流れ

7.6　Ring Protocol 使用時の注意事項

(1)　運用中のコンフィグレーション変更について

運用中に，Ring Protocol の次に示すコンフィグレーションを変更する場合は，ループ構成にならないように注意が必要です。

- Ring Protocol 機能の停止（disable コマンド）
- 動作モード（mode コマンド）の変更および属性（ring-attribute パラメータ）の変更
- 制御 VLAN（control-vlan コマンド）の変更および制御 VLAN に使用している VLAN ID（interface vlan コマンド，switchport trunk コマンド）の変更
- データ転送用 VLAN（axrp vlan-mapping コマンド，vlan-group コマンド）の変更
- プライマリポート（axrp-primary-port コマンド）の変更
- 共有リンク監視リングのマスタノードが動作している装置に，共有リンク非監視リングの最終端ノードを追加（動作モードの属性に rift-ring-edge パラメータ指定のあるリングを追加）

これらのコンフィグレーションは，次の手順で変更することを推奨します。

1. コンフィグレーションを変更する装置のリングポート，またはマスタノードのセカンダリポートを shutdown コマンドなどでダウン状態にします。
2. コンフィグレーションを変更する装置の Ring Protocol 機能を停止（disable コマンド）します。
3. コンフィグレーションを変更します。
4. Ring Protocol 機能の停止を解除（no disable コマンド）します。
5. 事前にダウン状態としたリングポートをアップ（shutdown コマンドなどの解除）します。

(2)　他機能との共存

「1.3　レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

(3)　リングポートフォワーディング遷移時間の設定について

リングポートフォワーディング遷移時間（forwarding-shift-time）がマスタノードのヘルスチェック送信間隔（health-check interval）よりも短い場合，マスタノードがリング障害の復旧を検出して，セカンダリポートをブロッキング状態に変更するよりも先に，障害が復旧したノードのリングポートがフォワーディング状態となることがあり，ループが発生するおそれがあります。したがって，リングポートフォワーディング遷移時間（forwarding-shift-time）はヘルスチェック送信間隔（health-check interval）より大きい値を設定してください。

(4)　共有リンクありのマルチリングでの VLAN 構成について

複数のリングで共通に使用する共有リンクでは，それぞれのリングで同じ VLAN を使用する必要があります。共有リンク間での VLAN のポート状態（フォワーディング状態またはブロッキング状態）は共有リンク監視リングで制御します。このため，共有リンク監視／非監視リングで異なる VLAN を使用すると，共有リンク非監視リングで使用している VLAN はブロッキング状態のままとなり，通信ができなくなります。

(5)　Ring Protocol 使用時のネットワーク構築について

(a)　リングネットワークを構築してから，Ring Protocol を動作させる場合

Ring Protocol を利用するネットワークはループ構成となります。ネットワークの構築時は，次に示すような対応をしてループを防止してください。

- 事前に，リング構成ノードのリングポート（物理ポートまたはチャネルグループ）を shutdown コマンドなどでダウン状態にしてください。
- Ring Protocol のコンフィグレーションを設定して，Ring Protocol を有効にしてください。
- ネットワーク内のすべての装置に Ring Protocol の設定が完了した時点でリングポートをアップ（shutdown コマンドなどの解除）してください。

(b)　Ring Protocol が動作している装置を順次接続して，リングネットワークを構築する場合

リングネットワークの構築が完了していない状態，かつコンフィグレーションコマンド forwarding-shift-time で「infinity」をマスタノードに設定している状態で，マスタノードのセカンダリポートを他装置と接続した場合，セカンダリポートがリンクアップしてもブロッキング状態を維持するため，該当ポートを使用した通信はできません。このため，次に示すどれかの方法でリングネットワークを構築してください。

- リングネットワークを構成するすべてのトランジットノードの接続が完了したあと，マスタノードを接続してください。
- リングネットワークを構築するときに，最初にマスタノードを接続する場合は，プライマリポート側からトランジットノードを接続してください。そして，すべてのトランジットノードの接続が完了したあと，マスタノードのセカンダリポートを接続してください。
- リングポートがフォワーディング状態に遷移するまでの保護時間として，コンフィグレーションコマンド forwarding-shift-time で「infinity」以外の値をマスタノードに設定してください。また，リングネットワークの構築が完了したあと，この保護時間（forwarding-shift-time コマンドでの設定値）は，マスタノードでのヘルスチェックフレームの送信間隔（health-check interval コマンドでの設定値）よりも大きい値を設定してください。小さい場合，一時的にループの発生するおそれがあるため，設定値は十分に考慮してください。
- リングネットワークを構築するときに，最初にマスタノードを接続して，セカンダリポート側からトランジットノードを接続する場合は，次の手順で実施してください。
  1. マスタノードのプライマリポートでは，接続時にダウン状態となるように，shutdown コマンドを実行します。
  2. マスタノードの Ring Protocol 機能を停止（disable コマンド）します。
  3. すべてのトランジットノードを接続します。
  4. マスタノードの Ring Protocol 機能の停止を解除（no disable コマンド）します。
  5. ダウン状態としていたマスタノードのプライマリポートをアップ（no shutdown コマンド）します。

(6)　ヘルスチェックフレームの送信間隔と障害監視時間について

障害監視時間（health-check holdtime）は送信間隔（health-check interval）より大きな値を設定してください。送信間隔よりも小さな値を設定すると，受信タイムアウトとなって障害を誤検出します。また，障害監視時間と送信間隔はネットワーク構成などを十分に考慮した値を設定してください。障害監視時間は送信間隔の 2 倍以上を目安として設定することを推奨します。2 倍未満に設定すると，ヘルスチェックフレームの受信が 1 回失敗した状態で障害を検出することがあるため，ネットワークの負荷などによって遅延が発生した場合に障害を誤検出するおそれがあります。

(7) 相互運用

Ring Protocol は，本装置独自仕様の機能です。他社スイッチとは相互運用できません。

(8) リングを構成する装置について

Ring Protocol を使用したネットワーク内で，本装置間に Ring Protocol をサポートしていない他社スイッチや伝送装置などを設置した場合，本装置のマスタノードが送信するフラッシュ制御フレームを解釈できないため，すぐに MAC アドレステーブルエントリがクリアされません。その結果，通信経路の切り替え（もしくは切り戻し）前の情報に従ってデータフレームの転送が行われるため，正しくデータが届かないおそれがあります。

(9) マスタノード障害時について

マスタノードが装置障害などによって通信できない状態になると，リングネットワークの障害監視が行われなくなります。このため，迂回経路への切り替えは行われないで，マスタノード以外のトランジットノード間の通信はそのまま継続されます。また，マスタノードが装置障害から復旧する際には，フラッシュ制御フレームをリング内のトランジットノードに向けて送信します。このため，一時的に通信が停止するおそれがあります。

(10) ネットワーク内の多重障害時について

同一リング内の異なるノード間で 2 個所以上の障害が起きた場合（多重障害），マスタノードはすでに 1 個所目の障害で障害検出を行っているため，2 個所目以降の障害を検出しません。また，多重障害での復旧検出についても，最後の障害が復旧するまでマスタノードが送信しているヘルスチェックフレームを受信できないため，復旧を検出できません。その結果，多重障害のうち，一部の障害が復旧した（リングとして障害が残っている状態）ときには一時的に通信できないことがあります。

(11) VLAN のダウンを伴う障害発生時の経路の切り替えについて

マスタノードのプライマリポートでリンクダウンなどの障害が発生すると，データ転送用の VLAN グループに設定されている VLAN が一時的にダウンする場合があります。このような場合，経路の切り替えによる通信の復旧に時間がかかることがあります。

なお，VLAN debounce 機能を使用することで VLAN のダウンを回避できる場合があります。VLAN debounce 機能の詳細については，「4.7 VLAN debounce 機能の解説」を参照してください。

(12) ネットワーク負荷の高い環境での運用について

トランジットノードで，定常的またはバースト的に，リングポートに高負荷のトラフィックが流れると，Ring Protocol の制御フレームの破棄または遅延が発生し，マスタノードで障害を誤検出するおそれがあります。上記の環境に当てはまる場合には，次の対応を行ってください。

- Ring Protocol のパラメータ値の調整による対応の場合
  ヘルスチェックフレームの送信間隔（health-check interval），および障害監視時間（health-check holdtime）を環境に合わせて調整して運用してください。
- フロー制御の設定による対応の場合
  次のどちらかを条件とした QoS フローリストを使用して，Ring Protocol の制御フレームに対する優先制御を設定して運用してください。詳細は，「13 QoS フロー」を参照してください。
  - Ring Protocol の制御フレームに使用している EtherType 値（0x88f3）または EtherType 名称（axp）を条件とする。
  - Ring Protocol の制御 VLAN に使用している VLAN ID を条件とする。

(13)　VLAN のダウンを伴うコンフィグレーションコマンドの設定について

Ring Protocol に関するコンフィグレーションコマンドが設定されていない状態で，一つ目の Ring Protocol に関するコンフィグレーションコマンド（次に示すどれかのコマンド）を設定した場合に，すべての VLAN が一時的にダウンします。そのため，Ring Protocol を使用したリングネットワークを構築する場合には，あらかじめ次に示すコンフィグレーションコマンドを設定しておくことを推奨します。

- axrp
- axrp vlan-mapping
- axrp-primary-port
- axrp-ring-port

なお，VLAN マッピング（axrp vlan-mapping コマンド）については，新たに追加設定した場合でも，その VLAN マッピングに関連づけられる VLAN が一時的にダウンします。すでに設定されている VLAN マッピング，およびその VLAN マッピングに関連づけられているその他の VLAN には影響ありません。

(14)　経路切り戻し抑止機能適用時のリングポートフォワーディング遷移時間の設定について

経路切り戻し抑止機能を動作させる場合，トランジットノードでのリングポートフォワーディング遷移時間（forwarding-shift-time）には infinity を指定するか，または経路切り戻し抑止時間（preempt-delay）よりも大きな値を指定してください。経路切り戻し抑止中，トランジットノードでのリングポートフォワーディング遷移時間がタイムアウトして該当リングポートのブロッキング状態を解除してしまうと，マスタノードはセカンダリポートのブロッキング状態を解除しているため，ループが発生するおそれがあります。

(15)　ヘルスチェックフレームの送信について

本装置では，リングポートの状態に関係なく，ヘルスチェックフレームの送信処理をします。このため，リングポートがダウン状態の場合，ヘルスチェックフレームは送信されませんが，該当ポートのヘルスチェックフレームの送信統計はカウントされます。ヘルスチェックフレームの統計情報を確認するときは注意してください。

8 Ring Protocol の設定と運用

この章では，Ring Protocol の設定例について説明します。

8.1　コンフィグレーション

Ring Protocol 機能が動作するためには，axrp，axrp vlan-mapping，mode，control-vlan，vlan-group，axrp-ring-port の設定が必要です。すべてのノードについて，構成に合ったコンフィグレーションを設定してください。

8.1.1　コンフィグレーションコマンド一覧

Ring Protocol 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 8-1　コンフィグレーションコマンド一覧

コマンド名	説明
axrp	リング ID を設定します。
axrp vlan-mapping	VLAN マッピング，およびそのマッピングに参加する VLAN を設定します。
axrp-primary-port	プライマリポートを設定します。
axrp-ring-port	リングポートを設定します。
control-vlan	制御 VLAN として使用する VLAN を設定します。
disable	Ring Protocol 機能を無効にします。
flush-request-count	フラッシュ制御フレームを送信する回数を設定します。
forwarding-shift-time	リングポートをフォワーディング状態に変更するまでの時間を設定します。
health-check holdtime	ヘルスチェックフレームの保護時間を設定します。
health-check interval	ヘルスチェックフレームの送信間隔を設定します。
mode	リングでの動作モードを設定します。
name	リングを識別するための名称を設定します。
preempt-delay	経路切り戻し抑止機能を有効にして抑止時間を設定します。
vlan-group	Ring Protocol 機能で運用する VLAN グループ，および VLAN マッピング ID を設定します。

8.1.2　Ring Protocol 設定の流れ

Ring Protocol 機能を正常に動作させるには，構成に合った設定が必要です。設定の流れを次に示します。

(1)　Ring Protocol 共通の設定

リングの構成，またはリングでの本装置の位置づけに依存しない共通の設定をします。

- リング ID
- 制御 VLAN
- VLAN マッピング
- VLAN グループ

(2)　モードとポートの設定

リングの構成，またはリングでの本装置の位置づけに応じた設定をします。設定の組み合わせに矛盾がある場合，Ring Protocol 機能は正常に動作しません。

- モード
- リングポート

(3)　各種パラメータ設定

Ring Protocol 機能は，次に示すコンフィグレーションの設定がない場合，初期値で動作します。値を変更したい場合はコマンドで設定してください。

- 機能の無効化
- ヘルスチェックフレーム送信間隔
- ヘルスチェックフレーム受信待ち保護時間
- リングポートフォワーディング遷移時間
- フラッシュ制御フレーム送信回数
- プライマリポート
- 経路切り戻し抑止機能の有効化および抑止時間

8.1.3　リング ID の設定

[設定のポイント]

リング ID を設定します。同じリングに属する装置にはすべて同じリング ID を設定する必要があります。

[コマンドによる設定]

1. **(config)# axrp 1**
   リング ID 1 を設定します。

8.1.4　制御 VLAN の設定

(1)　制御 VLAN の設定

[設定のポイント]

制御 VLAN として使用する VLAN を指定します。データ転送用 VLAN に使われている VLAN は使用できません。また，異なるリングで使われている VLAN ID と同じ値の VLAN ID は使用できません。

[コマンドによる設定]

1. **(config)# axrp 1**
   リング ID 1 の axrp コンフィグレーションモードに移行します。
2. **(config-axrp)# control-vlan 2**
   制御 VLAN として VLAN 2 を指定します。

(2) 制御 VLAN のフォワーディング遷移時間の設定

[設定のポイント]

Ring Protocol が初期状態の場合に，トランジットノードでの制御 VLAN のフォワーディング遷移時間を設定します。それ以外のノードでは，本設定を実施しても無効となります。トランジットノードでの制御 VLAN のフォワーディング遷移時間（forwarding-delay-time パラメータでの設定値）は，マスタノードでのヘルスチェックフレームの保護時間（health-check holdtime コマンドでの設定値）よりも大きな値を設定してください。

[コマンドによる設定]

1. **(config)# axrp 1**
   (config-axrp)# control-vlan 2 forwarding-delay-time 10
   制御 VLAN のフォワーディング遷移時間を 10 秒に設定します。

8.1.5 VLAN マッピングの設定

(1) VLAN 新規設定

[設定のポイント]

データ転送用に使用する VLAN を VLAN マッピングに括り付けます。一つの VLAN マッピングを共通定義として複数のリングで使用できます。設定できる VLAN マッピングの最大数は 128 個です。VLAN マッピングに設定する VLAN はリストで複数指定できます。

リングネットワーク内で使用するデータ転送用 VLAN は，すべてのノードで同じにする必要があります。ただし，VLAN グループに指定した VLAN マッピングの VLAN が一致していればよいため，リングネットワーク内のすべてのノードで VLAN マッピング ID を一致させる必要はありません。

[コマンドによる設定]

1. **(config)# axrp vlan-mapping 1 vlan 5-7**
   VLAN マッピング ID 1 に，VLAN ID 5，6，7 を設定します。

(2) VLAN 追加

[設定のポイント]

設定済みの VLAN マッピングに対して，VLAN ID を追加します。追加した VLAN マッピングを適用したリングが動作中の場合には，すぐに反映されます。また，複数のリングで適用されている場合には，同時に反映されます。リング運用中に VLAN マッピングを変更すると，ループが発生することがあります。

[コマンドによる設定]

1. **(config)# axrp vlan-mapping 1 vlan add 8-10**
   VLAN マッピング ID 1 に VLAN ID 8，9，10 を追加します。

(3) VLAN 削除

[設定のポイント]

設定済みの VLAN マッピングから，VLAN ID を削除します。削除した VLAN マッピングを適用したリングが動作中の場合には，すぐに反映されます。また，複数のリングで適用されている場合には，同

時に反映されます。リング運用中に VLAN マッピングを変更すると，ループが発生することがあります。

[コマンドによる設定]

1. **(config)# axrp vlan-mapping 1 vlan remove 8-9**
   VLAN マッピング ID 1 から VLAN ID 8，9 を削除します。

8.1.6　VLAN グループの設定

[設定のポイント]

VLAN グループに VLAN マッピングを割り当てることによって，VLAN ID を Ring Protocol で使用する VLAN グループに所属させます。VLAN グループは一つのリングに最大二つ設定できます。
VLAN グループには，リスト指定によって最大 128 個の VLAN マッピング ID を設定できます。

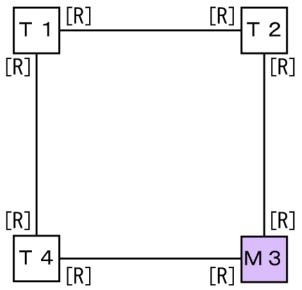
[コマンドによる設定]

1. **(config)# axrp 1**
   (config-axrp)# vlan-group 1 vlan-mapping 1
   VLAN グループ 1 に，VLAN マッピング ID 1 を設定します。

8.1.7　モードとリングポートに関する設定（シングルリングと共有リンクなしマルチリング構成）

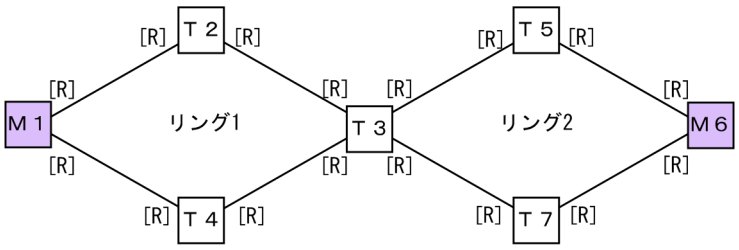
シングルリング構成を「図 8-1　シングルリング構成」に，共有リンクなしマルチリング構成を「図 8-2 共有リンクなしマルチリング構成」に示します。

図 8-1　シングルリング構成



（凡例）　M：マスタノード　　T：トランジットノード
　　[R]：リングポート

図 8-2　共有リンクなしマルチリング構成



（凡例）　M：マスタノード　　T：トランジットノード
　　[R]：リングポート

シングルリング構成と共有リンクなしマルチリング構成での，マスタノード，およびトランジットノードに関するモードとリングポートの設定は同様になります。

(1)　マスタノード

[設定のポイント]

リングでの本装置の動作モードをマスタモードに設定します。イーサネットインタフェースまたはポートチャネルインタフェースをリングポートとして指定します。リングポートは一つのリングに対して二つ設定してください。「図 8-1　シングルリング構成」では M3 ノード，「図 8-2　共有リンクなしマルチリング構成」では M1 および M6 ノードがこれに該当します。

[コマンドによる設定]

1. **(config)# axrp 2**
   (config-axrp)# mode master
   リング ID 2 の動作モードをマスタモードに設定します。
2. **(config)# interface gigabitethernet 1/1**
   (config-if)# axrp-ring-port 2
   (config-if)# interface gigabitethernet 1/2
   (config-if)# axrp-ring-port 2
   ポート 1/1 および 1/2 のインタフェースモードに移行して，該当するインタフェースをリング ID 2 のリングポートとして設定します。

(2)　トランジットノード

[設定のポイント]

リングでの本装置の動作モードをトランジットモードに設定します。イーサネットインタフェースまたはポートチャネルインタフェースをリングポートとして指定します。リングポートは一つのリングに対して二つ設定してください。「図 8-1　シングルリング構成」では T1，T2 および T4 ノード，「図 8-2　共有リンクなしマルチリング構成」では T2，T3，T4，T5 および T7 ノードがこれに該当します。

[コマンドによる設定]

1. **(config)# axrp 2**
   (config-axrp)# mode transit
   リング ID 2 の動作モードをトランジットモードに設定します。

2.(config)# interface gigabitethernet 1/1
(config-if)# axrp-ring-port 2
(config-if)# interface gigabitethernet 1/2
(config-if)# axrp-ring-port 2

ポート 1/1 および 1/2 のインタフェースモードに移行して，該当するインタフェースをリング ID 2 のリングポートとして設定します。

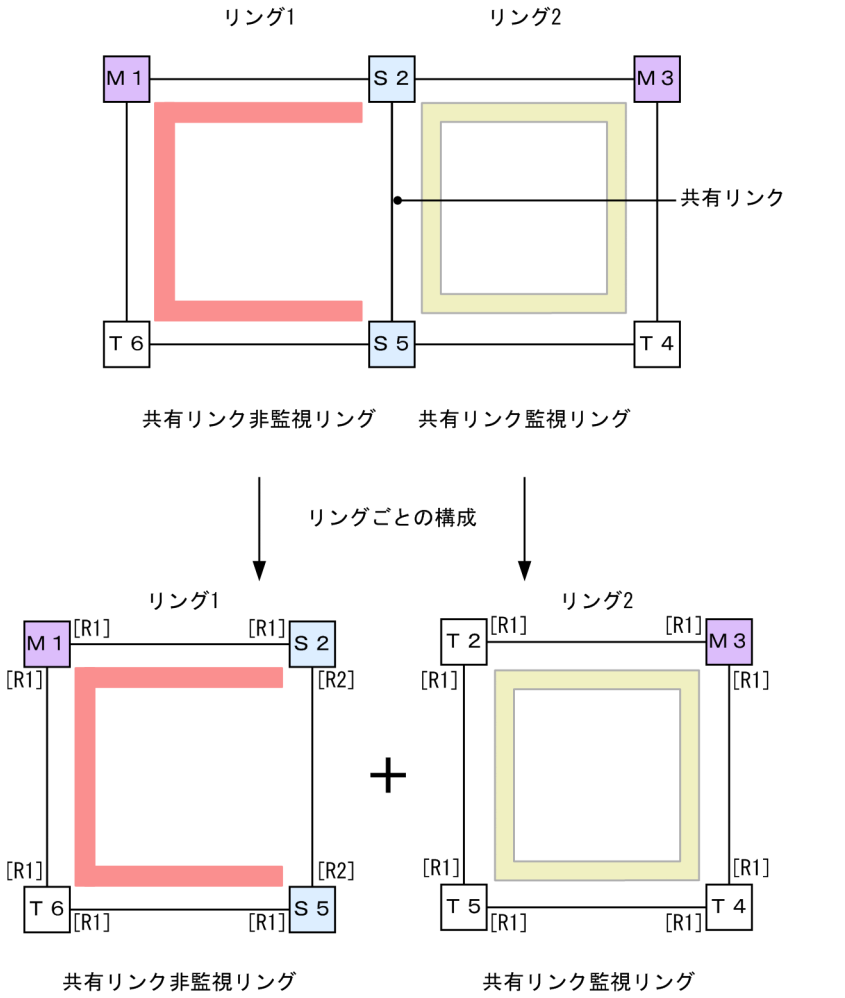
8.1.8　モードとリングポートに関する設定（共有リンクありマルチリング構成）

共有リンクありマルチリング構成について，モードとリングポートのパラメータ設定パターンを示します。

(1)　共有リンクありマルチリング構成（基本構成）

共有リンクありマルチリング構成（基本構成）を次の図に示します。

図 8-3　共有リンクありマルチリング構成（基本構成）



（凡例）　M：マスタノード　　T：トランジットノード　　S：共有ノード
[R1]：リングポート
[R2]：リングポート（共有リンク非監視リング最終端ノードの共有リンク側ポート）
：リング1の監視経路　　：リング2の監視経路

(a)　共有リンク監視リングのマスタノード

シングルリングのマスタノード設定と同様です。「8.1.7　モードとリングポートに関する設定（シングルリングと共有リンクなしマルチリング構成）(1)　マスタノード」を参照してください。「図 8-3　共有リンクありマルチリング構成（基本構成）」では M3 ノードがこれに該当します。

(b)　共有リンク監視リングのトランジットノード

シングルリングのトランジットノード設定と同様です。「8.1.7　モードとリングポートに関する設定（シングルリングと共有リンクなしマルチリング構成）(2)　トランジットノード」を参照してください。「図 8-3　共有リンクありマルチリング構成（基本構成）」では T2，T4 および T5 ノードがこれに該当します。

(c)　共有リンク非監視リングのマスタノード

[設定のポイント]

リングでの本装置の動作モードをマスタモードに設定します。また，本装置が構成しているリングの属性，およびそのリングでの本装置の位置づけを共有リンク非監視リングに設定します。イーサネットインタフェースまたはポートチャネルインタフェースをリングポートとして指定します。リングポートは一つのリングに対して二つ設定してください。「図 8-3　共有リンクありマルチリング構成（基本構成）」では M1 ノードがこれに該当します。

[コマンドによる設定]

1. **(config)# axrp 1**
   (config-axrp)# mode master ring-attribute rift-ring
   リング ID 1 の動作モードをマスタモード，リング属性を共有リンク非監視リングに設定します。
2. **(config)# interface gigabitethernet 1/1**
   (config-if)# axrp-ring-port 1
   (config-if)# interface gigabitethernet 1/2
   (config-if)# axrp-ring-port 1
   ポート 1/1 および 1/2 のインタフェースモードに移行して，該当するインタフェースをリング ID 1 のリングポートとして設定します。

(d)　共有リンク非監視リングのトランジットノード

シングルリングのトランジットノード設定と同様です。「8.1.7　モードとリングポートに関する設定（シングルリングと共有リンクなしマルチリング構成）(2)　トランジットノード」を参照してください。「図 8-3　共有リンクありマルチリング構成（基本構成）」では T6 ノードがこれに該当します。

(e)　共有リンク非監視リングの最終端ノード（トランジット）

[設定のポイント]

リングでの本装置の動作モードをトランジットモードに設定します。また，本装置が構成しているリングの属性，およびそのリングでの本装置の位置づけを共有リンク非監視リングの最終端ノードに設定します。構成上二つ存在する共有リンク非監視リングの最終端ノードの区別にはエッジノード ID（1 または 2）を指定します。「図 8-3　共有リンクありマルチリング構成（基本構成）」では S2 および S5 ノードがこれに該当します。リングポート設定は共有リンク側のポートにだけ shared-edge を指定します。「図 8-3　共有リンクありマルチリング構成（基本構成）」では S2 および S5 ノードのリングポート［R2］がこれに該当します。

[コマンドによる設定]

1. **(config)# axrp 1**
   (config-axrp)# mode transit ring-attribute rift-ring-edge 1
   リング ID 1 での動作モードをトランジットモード，リング属性を共有リンク非監視リングの最終端ノード，エッジノード ID を 1 に設定します。
2. **(config)# interface gigabitethernet 1/1**
   (config-if)# axrp-ring-port 1
   (config-if)# interface gigabitethernet 1/2
   (config-if)# axrp-ring-port 1 shared-edge

ポート 1/1 および 1/2 のインタフェースモードに移行して，該当するインタフェースをリング ID 1 のリングポートとして設定します。このとき，ポート 1/2 を共有リンクとして shared-edge パラメータも設定します。

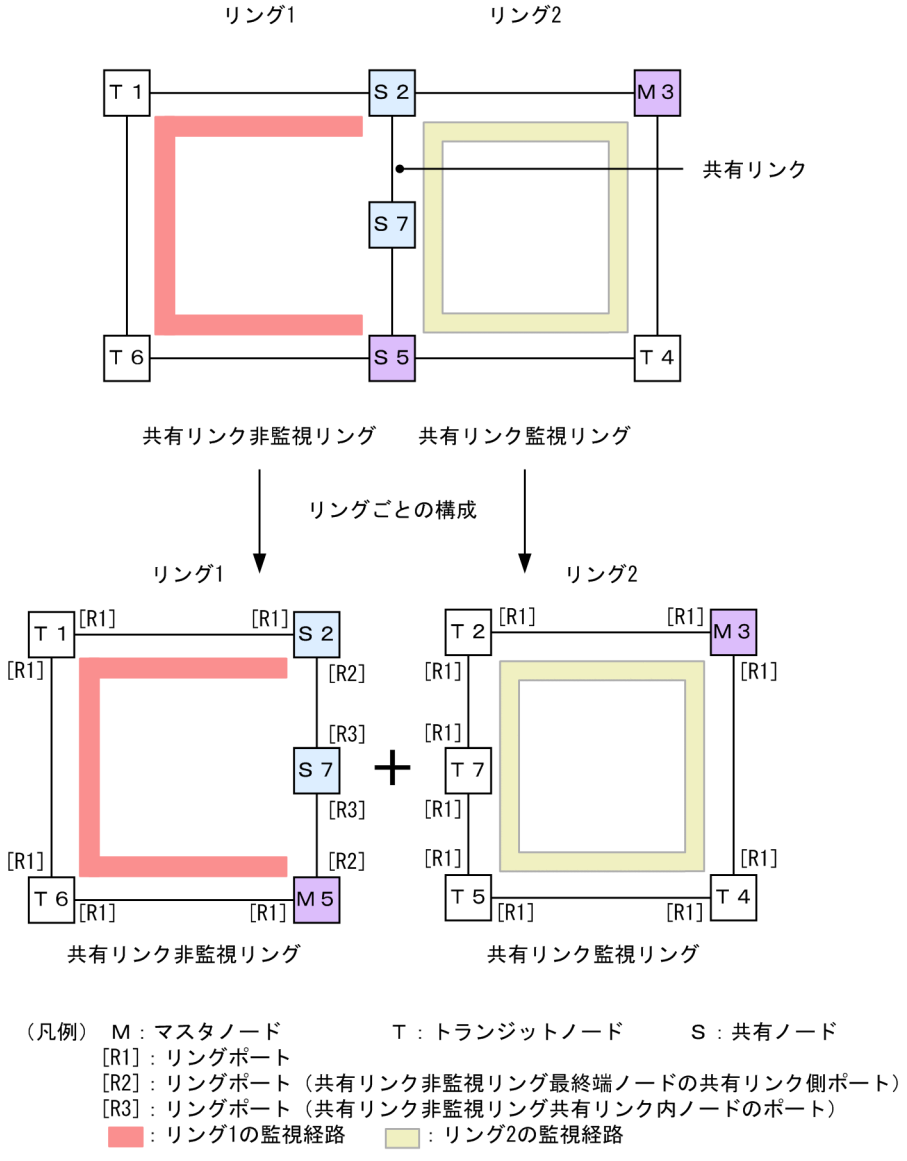
［注意事項］

エッジノード ID は，二つある共有リンク非監視リングの最終端ノードで他方と異なる ID を設定してください。

(2)　共有リンクありのマルチリング構成（拡張構成）

共有リンクありマルチリング構成（拡張構成）を次の図に示します。共有リンク非監視リングの最終端ノード（マスタノード）および共有リンク非監視リングの共有リンク内ノード（トランジット）以外の設定については，「(1)　共有リンクありマルチリング構成（基本構成）」を参照してください。

図 8-4　共有リンクありのマルチリング構成（拡張構成）



（凡例）　M：マスタノード　　T：トランジットノード　　S：共有ノード
[R1]：リングポート
[R2]：リングポート（共有リンク非監視リング最終端ノードの共有リンク側ポート）
[R3]：リングポート（共有リンク非監視リング共有リンク内ノードのポート）
：リング1の監視経路　　：リング2の監視経路

(a)　共有リンク非監視リングの最終端ノード（マスタノード）

[設定のポイント]

リングでの本装置の動作モードをマスタモードに設定します。また，本装置が構成しているリングの属性，およびそのリングでの本装置の位置づけを共有リンク非監視リングの最終端ノードに設定します。構成上二つ存在する共有リンク非監視リングの最終端ノードの区別にはエッジノード ID（1 または 2）を指定します。「図 8-4　共有リンクありのマルチリング構成（拡張構成）」では M5 ノードがこれに該当します。リングポート設定は共有リンク側のポートにだけ shared-edge を指定します。「図 8-4　共有リンクありのマルチリング構成（拡張構成）」では M5 ノードのリングポート［R2］がこれに該当します。

[コマンドによる設定]

1. **(config)# axrp 1**
   (config-axrp)# mode master ring-attribute rift-ring-edge 2
   リング ID 1 での動作モードをマスタモード，リング属性を共有リンク非監視リングの最終端ノード，エッジノード ID を 2 に設定します。
2. **(config)# interface gigabitethernet 1/1**
   (config-if)# axrp-ring-port 1
   (config-if)# interface gigabitethernet 1/2
   (config-if)# axrp-ring-port 1 shared-edge
   ポート 1/1 および 1/2 のインタフェースモードに移行して，該当するインタフェースをリング ID 1 のリングポートとして設定します。このとき，ポート 1/2 を共有リンクとして shared-edge パラメータも設定します。

[注意事項]

エッジノード ID は,二つある共有リンク非監視リングの最終端ノードで他方と異なる ID を設定してください。

(b)　共有リンク非監視リングの共有リンク内ノード（トランジット）

[設定のポイント]

リングでの本装置の動作モードをトランジットモードに設定します。「図 8-4　共有リンクありのマルチリング構成（拡張構成）」では S7 ノードがこれに該当します。リングポートは両ポート共に shared パラメータを指定し，共有ポートとして設定します。「図 8-4　共有リンクありのマルチリング構成（拡張構成）」では S7 ノードのリングポート［R3］がこれに該当します。

[コマンドによる設定]

1. **(config)# axrp 1**
   (config-axrp)# mode transit
   リング ID 1 の動作モードをトランジットモードに設定します。
2. **(config)# interface gigabitethernet 1/1**
   (config-if)# axrp-ring-port 1 shared
   (config-if)# interface gigabitethernet 1/2
   (config-if)# axrp-ring-port 1 shared
   ポート 1/1 および 1/2 のインタフェースモードに移行して，該当するインタフェースをリング ID 1 の共有リンクポートに設定します。

[注意事項]

- 共有リンク監視リングの共有リンク内トランジットノードに shared 指定でポート設定をした場合，Ring Protocol 機能は正常に動作しません。
- 共有リンク非監視リングの共有リンク内で shared 指定したノードにマスタモードは指定できません。

8.1.9　各種パラメータの設定

(1)　Ring Protocol 機能の無効

[設定のポイント]

コマンドを指定して Ring Protocol 機能を無効にします。ただし，運用中に Ring Protocol 機能を無効にすると，ネットワークの構成上，ループが発生するおそれがあります。このため，先に Ring Protocol 機能を動作させているインタフェースを shutdown コマンドなどで停止させてから，Ring Protocol 機能を無効にしてください。

[コマンドによる設定]

1. **(config)# axrp 1**
   (config-axrp)# disable
   該当するリング ID 1 の axrp コンフィグレーションモードに移行します。disable コマンドを実行することで，Ring Protocol 機能が無効となります。

(2)　ヘルスチェックフレーム送信間隔

[設定のポイント]

マスタノード，または共有リンク非監視リングの最終端ノードでのヘルスチェックフレームの送信間隔を設定します。それ以外のノードでは，本設定を実施しても，無効となります。

[コマンドによる設定]

1. **(config)# axrp 1**
   (config-axrp)# health-check interval 500
   ヘルスチェックフレームの送信間隔を 500 ミリ秒に設定します。

[注意事項]

マルチリングの構成をとる場合，同一リング内のマスタノードと共有リンク非監視リングの最終端ノードでのヘルスチェックフレーム送信間隔は同じ値を設定してください。値が異なる場合，障害検出処理が正常に行われません。

(3)　ヘルスチェックフレーム受信待ち保護時間

[設定のポイント]

マスタノードでのヘルスチェックフレームの受信待ち保護時間を設定します。それ以外のノードでは，本設定を実施しても，無効となります。受信待ち保護時間を変更することで，障害検出時間を調節できます。

受信待ち保護時間（health-check holdtime コマンドでの設定値）は，送信間隔（health-check interval コマンドでの設定値）よりも大きい値を設定してください。

[コマンドによる設定]

1.(config)# axrp 1
(config-axrp)# health-check holdtime 1500
ヘルスチェックフレームの受信待ち保護時間を 1500 ミリ秒に設定します。

(4)　リングポートフォワーディング遷移時間

[設定のポイント]

リンク障害が復旧した場合に，リングポートのデータ VLAN の状態をフォワーディング状態に変更するまでの時間を設定します。なお，リングポートフォワーディング遷移時間中にリング状態が障害状態以外の状態に遷移した場合は，マスタノードでは本設定によるデータ転送用 VLAN の状態変更は実施しません。

リングポートフォワーディング遷移時間（forwarding-shift-time コマンドでの設定値）は，マスタノードでのヘルスチェックフレームの送信間隔（health-check interval コマンドでの設定値）よりも大きい値を設定してください。設定誤りからマスタノードが復旧を検出するよりも先にマスタノードおよびトランジットノードのリングポートがフォワーディング状態になってしまった場合，一時的にループが発生するおそれがあります。

[コマンドによる設定]

1.(config)# axrp 1
(config-axrp)# forwarding-shift-time 100
リングポートフォワーディング遷移時間を 100 秒に設定します。

(5)　プライマリポートの設定

[設定のポイント]

マスタノードでプライマリポートを設定できます。マスタノードでリングポート（axrp-ring-port コマンド）指定のあるインタフェースに設定してください。本装置が共有リンク非監視リングの最終端となっている場合は設定されても動作しません。通常，プライマリポートは自動で割り振られますので，axrp-primary-port コマンドの設定または変更によってプライマリポートを切り替える場合は，リング動作がいったん停止します。

[コマンドによる設定]

1.(config)# interface port-channel 10
(config-if)# axrp-primary-port 1 vlan-group 1
ポートチャネルインタフェースコンフィグレーションモードに移行して，該当するインタフェースをリング ID 1，VLAN グループ ID 1 のプライマリポートに設定します。

(6)　経路切り戻し抑止機能の有効化および抑止時間

[設定のポイント]

マスタノードで障害復旧検出後，経路切り戻し動作を抑止する時間を設定します。なお，抑止時間として infinity を指定した場合，運用コマンド clear axrp preempt-delay が入力されるまで経路切り戻し動作を抑止します。

[コマンドによる設定]

1.(config)# axrp 1
(config-axrp)# preempt-delay infinity

リング ID 1 のコンフィグレーションモードに移行して，経路切り戻し抑止時間を infinity に設定します。

8.2　オペレーション

8.2.1　運用コマンド一覧

Ring Protocol の運用コマンド一覧を次の表に示します。

表 8-2　運用コマンド一覧

コマンド名	説明
show axrp	Ring Protocol 情報を表示します。
clear axrp	Ring Protocol の統計情報をクリアします。
clear axrp preempt-delay	リングの経路切り戻し抑止状態を解除します。
restart axrp	Ring Protocol プログラムを再起動します。
dump protocols axrp	Ring Protocol プログラムで採取している詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。
show vlan※	VLAN の Ring Protocol 使用状態を表示します。

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

8.2.2　Ring Protocol の状態確認

show axrp コマンドで Ring Protocol の設定と運用状態を確認できます。コンフィグレーションコマンドで設定した Ring Protocol 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。リング単位の状態情報確認には，show axrp コマンドでリング ID を指定してください。

表示される情報は，Oper State の内容によって異なります。

Oper State に「enable」が表示されている場合
　Ring Protocol 機能が動作しています。このとき，表示内容は全項目について運用の状態を示しています。

Oper State に「-」が表示されている場合
　必須のコンフィグレーションコマンドがそろっていない状態です。

Oper State に「Not Operating」が表示されている場合
　コンフィグレーションに矛盾があるなどの理由で，Ring Protocol 機能が動作できていない状態です。

Oper State に「-」または「Not Operating」が表示されているときには，コンフィグレーションを確認してください。show axrp コマンドの表示例を次に示します。

図 8-5　show axrp コマンドの実行結果

```
> show axrp
Date 20XX/01/27 12:00:00 UTC

Total Ring Counts:4

Ring ID:1
 Name:RING#1
 Oper State:enable           Mode:Master     Attribute:-

 VLAN Group ID  Ring Port  Role/State            Ring Port  Role/State
```

```
 1              1/1         primary/forwarding    1/2         secondary/blocking
 2              1/1         secondary/blocking    1/2         primary/forwarding

Ring ID:2
 Name:RING#2
 Oper State:enable           Mode:Transit    Attribute:-

 VLAN Group ID  Ring Port  Role/State            Ring Port  Role/State
 1              1(ChGr)    -/forwarding          2(ChGr)    -/forwarding
 2              1(ChGr)    -/forwarding          2(ChGr)    -/forwarding
   :
   :
   :
>
```

show axrp detail コマンドを使用すると，統計情報やマスタノードのリング状態などについての詳細情報を確認できます。統計情報については，Ring Protocol 機能が有効（Oper State が「enable」）でない限り 0 を表示します。show axrp detail コマンドの表示例を次に示します。

図 8-6　show axrp detail のコマンド実行結果

```
> show axrp detail
Date 20XX/01/27 12:00:00 UTC

Total Ring Counts:4

Ring ID:1
 Name:RING#1
 Oper State:enable           Mode:Master     Attribute:-
 Control VLAN ID:5           Ring State:normal
 Health Check Interval  (msec):1000
 Health Check Hold Time (msec):3000
 Forwarding Shift Time   (sec):10
 Flush Request Counts:3
 Health Check Counts:
  Ring Port:1/1
   HC(M) Tx:              256203  Rx:              116115
   HC(S) Tx:                   0  Rx:                   0
  Ring Port:1/2
   HC(M) Tx:              256203  Rx:              116115
   HC(S) Tx:                   0  Rx:                   0

 VLAN Group ID:1
  VLAN ID:6-10,12
  Ring Port:1/1         Role:primary      State:forwarding
  Ring Port:1/2         Role:secondary    State:blocking

 VLAN Group ID:2
  VLAN ID:16-20,22
  Ring Port:1/1         Role:secondary    State:blocking
  Ring Port:1/2         Role:primary      State:forwarding

Last Transition Time:20XX/01/24 10:00:00
Fault Counts    Recovery Counts    Total Flush Request Counts
1               1                  12

Ring ID:2
 Name:RING#2
 Oper State:enable           Mode : Transit    Attribute : -
 Control VLAN ID:15
 Forwarding Shift Time (sec):10
 Last Forwarding:flush request receive

 VLAN Group ID:1
  VLAN ID  :26-30,32
  Ring Port:1(ChGr)     Role:-            State:forwarding
  Ring Port:2(ChGr)     Role:-            State:forwarding

 VLAN Group ID:2
  VLAN ID:36-40,42
  Ring Port:1(ChGr)     Role:-            State:forwarding
  Ring Port:2(ChGr)     Role:-            State:forwarding
   :
```

⋮
⋮
>

9 IGMP/MLD snooping

IGMP/MLD snooping はレイヤ 2 スイッチで VLAN 内のマルチキャストトラフィックを制御する機能です。この章では，IGMP/MLD snooping について説明します。

9.1　IGMP/MLD snooping の概要

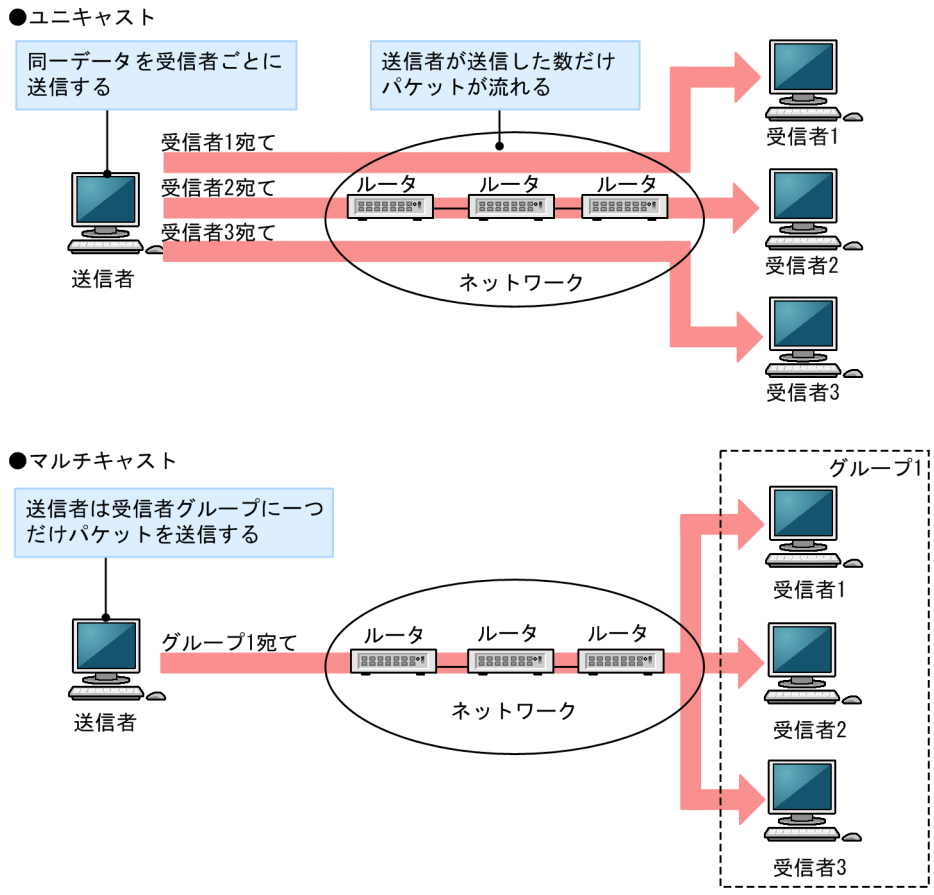
この節では，マルチキャスト，IGMP snooping および MLD snooping の概要について説明します。

9.1.1　概要

(1)　マルチキャストの概要

同一の情報を複数の受信者に送信する場合，ユニキャストでは送信者が受信者の数だけユニキャストパケットを複製して送信するため，送信者とネットワークの負荷が高くなります。マルチキャストでは送信者がネットワーク内で選択されたグループに対してマルチキャストパケットを送信します。送信者は受信者ごとにマルチキャストパケットを複製する必要はなく，受信者が増えたときのネットワークの負荷を軽減できます。マルチキャストの概要を次の図に示します。

図 9-1　マルチキャストの概要



マルチキャストで送信する場合，宛先アドレスにはグループアドレス（マルチキャストアドレス）を使用します。グループアドレスを次の表に示します。

表 9-1　グループアドレス

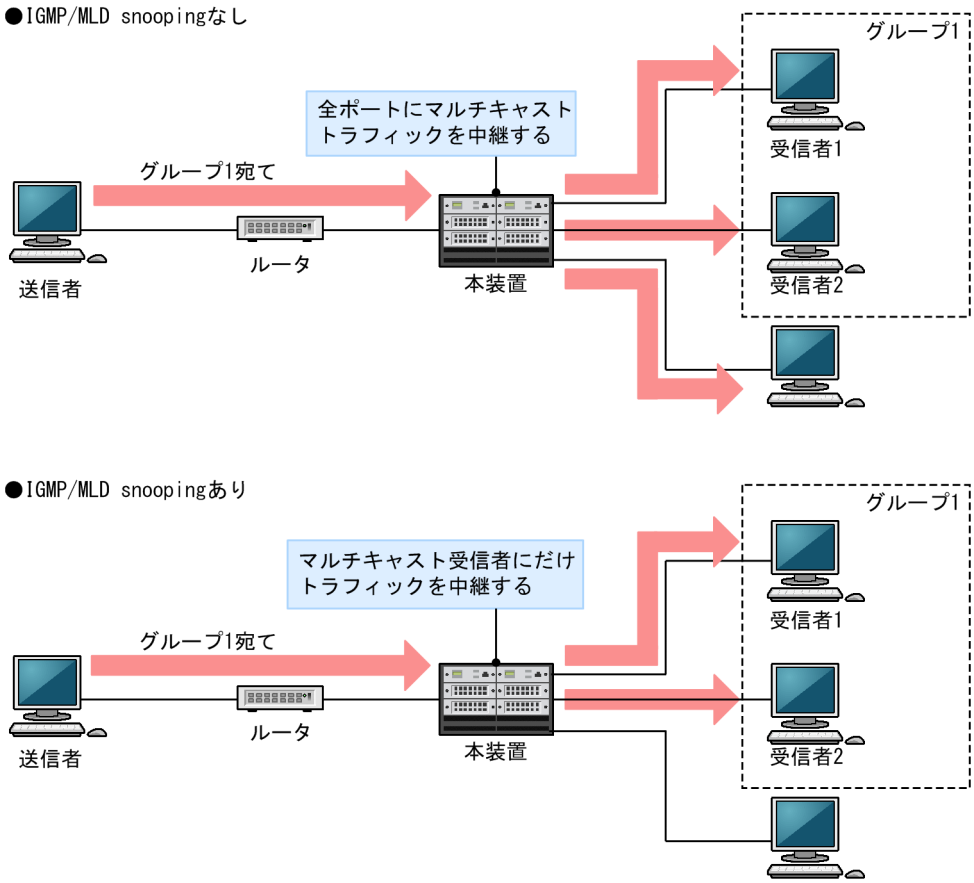
プロトコル	アドレス範囲
IPv4	224.0.0.0～239.255.255.255
IPv6	上位 8 ビットが ff（16 進数）となる IPv6 アドレス

(2)　IGMP snooping および MLD snooping の概要

レイヤ 2 スイッチはマルチキャストトラフィックを VLAN 内の全ポートに中継します。そのため，レイヤ 2 スイッチが接続されているネットワークでマルチキャストを使用すると，マルチキャストトラフィックの受信者がいないポートに不要なマルチキャストトラフィックが流れます。

IGMP snooping および MLD snooping は，IGMP メッセージもしくは MLD メッセージを監視して，受信者が接続しているポートにだけマルチキャストトラフィックを中継します。この機能を利用することで，不要なマルチキャストトラフィックの中継を抑止し，ネットワークを効率的に利用できます。IGMP/MLD snooping の概要を次の図に示します。

図 9-2　IGMP/MLD snooping の概要



本装置はマルチキャストグループ管理プロトコルのパケットを監視して，マルチキャストトラフィックの受信者が接続しているポートを検出します。マルチキャストグループ管理プロトコルは，ルータと受信者間でマルチキャストグループメンバシップ情報を送受信するプロトコルで，IPv4 ネットワークでは IGMP，IPv6 ネットワークでは MLD をサポートしています。本装置は，受信者から送信されるマルチキャストグループ参加および離脱要求を示すパケットを検出することで，どの接続ポートへマルチキャストトラフィックを中継すればよいかを学習します。

9.1.2　サポート機能

本装置がサポートする IGMP snooping の機能を次の表に示します。

表 9-2 サポートする IGMP snooping の機能

項目	サポート内容
フレームフォーマット	Ethernet V2 フレーム
インタフェースの種類	VLAN インタフェース
サポートバージョン	IGMP Version 1 IGMP Version 2 IGMP Version 3 以降，それぞれ IGMPv1，IGMPv2，IGMPv3 と呼びます。
学習する MAC アドレスの範囲	0100.5e00.0000～0100.5e7f.ffff （RFC1112 による）
マルチキャストルータ接続ポートの設定	コンフィグレーションによる設定
IGMP クエリア機能	IGMPv2 および IGMPv3 の仕様に従う
IGMP 即時離脱機能	次に示すメッセージの受信による即時離脱 • IGMPv2 Leave メッセージ • IGMPv3 Report（離脱要求）メッセージ

本装置がサポートする MLD snooping の機能を次の表に示します。

表 9-3 サポートする MLD snooping の機能

項目	サポート内容
フレームフォーマット	Ethernet V2 フレーム
インタフェースの種類	VLAN インタフェース
サポートバージョン	MLD Version 1 MLD Version 2 以降，それぞれ MLDv1，MLDv2 と呼びます。
学習する MAC アドレスの範囲	3333.0000.0000～3333.ffff.ffff （RFC2464 による）
マルチキャストルータ接続ポートの設定	コンフィグレーションによる設定
MLD クエリア機能	MLDv1 および MLDv2 の仕様に従う
MLD 即時離脱機能	次に示すメッセージの受信による即時離脱 • MLDv1 Done メッセージ • MLDv2 Report（離脱要求）メッセージ

9.2　IGMP snooping の解説

ここでは，IGMP snooping の機能と動作について説明します。本装置が送受信する IGMP メッセージのフォーマットおよびタイマは 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。

9.2.1　MAC アドレスの学習

IGMP snooping が設定された VLAN で IGMP メッセージを受信することによってマルチキャスト MAC アドレスをダイナミックに学習します。学習したマルチキャスト MAC アドレスは MAC アドレステーブルに登録します。

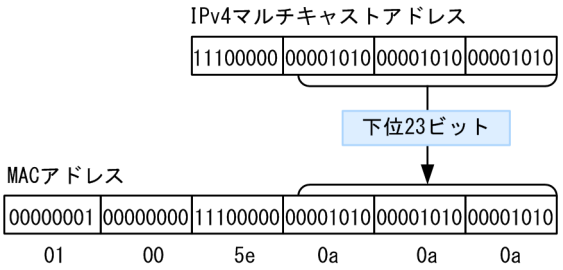
(1)　エントリの登録

次に示す IGMP メッセージを受信すると，メッセージに含まれるグループアドレスからマルチキャスト MAC アドレスを学習し，受信したポートにだけマルチキャストグループ宛てのトラフィックを中継するエントリを作成します。以降，これらのメッセージを IGMP Report（参加要求）メッセージと呼びます。

- IGMPv1 Report メッセージ
- IGMPv2 Report メッセージ
- IGMPv3 Report（参加要求）メッセージ

IPv4 マルチキャストパケットの宛先 MAC アドレスは IPv4 アドレスの下位 23 ビットを MAC アドレスにコピーして生成します。そのため，下位 23 ビットが同じ IPv4 アドレスは MAC アドレスが重複します。例えば，224.10.10.10 と 225.10.10.10 はどちらもマルチキャスト MAC アドレスは 0100.5E0A.0A0A となります。これらのアドレスについては，レイヤ 2 中継で同一 MAC アドレス宛てのパケットとして取り扱います。IPv4 マルチキャストアドレスと MAC アドレスの対応を次の図に示します。

図 9-3　IPv4 マルチキャストアドレスと MAC アドレスの対応



(2)　IGMPv2 メッセージ受信によるエントリの削除

IGMPv2 Leave メッセージを受信すると，受信したポートだけエントリから削除し，このポートへのマルチキャストトラフィックの中継を停止します。VLAN 内のすべてのポートにグループメンバが存在しなくなった時点で，エントリを削除します。

(a)　IGMP クエリア機能設定時の動作

本装置は，IGMPv2 Leave メッセージを受信したポートから Group-Specific Query メッセージを 1 秒間隔で 2 回送信します。応答がない場合にエントリからこのポートだけを削除します。

(b) IGMP 即時離脱機能設定時の動作

本装置は，IGMPv2 Leave メッセージを受信したポートをエントリからすぐに削除します。IGMP クエリア機能を設定していても，Group-Specific Query メッセージは送信しません。

(3) IGMPv3 メッセージ受信によるエントリの削除

IGMPv3 Report（離脱要求）メッセージを受信すると，受信したポートだけエントリから削除し，このポートへのマルチキャストトラフィックの中継を停止します。VLAN 内のすべてのポートにグループメンバが存在しなくなった時点で，エントリを削除します。

(a) IGMP クエリア機能設定時の動作

本装置は，IGMPv3 Report（離脱要求）メッセージを受信したポートから Group-Specific Query メッセージを 1 秒間隔で 2 回送信します。応答がない場合にエントリからこのポートだけを削除します。

ただし，受信した IGMPv3 Report（離脱要求）メッセージのマルチキャストアドレスレコードタイプが BLOCK_OLD_SOURCES の場合，これらの削除処理が実行されるのは，該当する VLAN に IPv4 マルチキャストを使用していないときだけです。

(b) IGMP 即時離脱機能設定時の動作

本装置は，マルチキャストアドレスレコードタイプが CHANGE_TO_INCLUDE_MODE の IGMPv3 Report（離脱要求）メッセージを受信したポートをエントリからすぐに削除します。

IGMP クエリア機能を設定していても，Group-Specific Query メッセージは送信しません。

(4) エントリのエージング

IGMP Report（参加要求）メッセージを受信してから一定時間経過すると，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グループメンバが存在するかを確認するため，定期的に IGMP Query メッセージを送信します。本装置はルータからの IGMP Query メッセージを受信した場合, VLAN 内の全ポートに中継します。IGMP Query メッセージへの応答である IGMP Report（参加要求）メッセージを受信しない場合，エントリからこのポートだけを削除します。すべてのポートから応答がない場合は，エントリ自体を削除します。

本装置では，ポートへの中継を停止するタイムアウト時間は 260 秒（コンフィグレーションコマンド ip igmp query-interval のデフォルト値から算出）であり，この間に IGMP Report（参加要求）メッセージを受信しない場合，該当するポートへの中継を停止します。

次の場合，タイムアウト時間は動的に設定します。

- 他装置が代表クエリア（IGMPv3 での運用）
  代表クエリアからの IGMPv3 Query メッセージ（QQIC フィールド）から算出します。
- 自装置が代表クエリアで IPv4 マルチキャストを使用
  IGMPv2/IGMPv3 に関係なく，自装置に設定した Query Interval で算出します。ただし，Query Interval を設定していないときは，デフォルト値での運用となります。
- 他装置が代表クエリア（IGMPv2 での運用）で IPv4 マルチキャストを使用
  該当する VLAN に IPv4 マルチキャストを使用しているときは，自装置に設定した Query Interval で算出します。ただし，Query Interval を設定していないときは，デフォルト値での運用となります。

また，次の場合，タイムアウト時間はデフォルト値での運用となります。

- 自装置が代表クエリアで IPv4 マルチキャストは未使用
  IGMPv2/IGMPv3 に関係なく，デフォルト値での運用となります。
- 他装置が代表クエリア（IGMPv2 での運用）で IPv4 マルチキャストは未使用
  該当する VLAN に IPv4 マルチキャストを使用していないときは，デフォルト値での運用となります。この場合，該当する VLAN では Query Interval を 125 秒で運用してください。

注　タイムアウト時間は，Query Interval（QQIC フィールドの値）×2+Query Response Interval で算出します。

9.2.2　マルチキャストパケットの中継制御

(1)　MAC アドレス学習によるマルチキャストパケット中継

本装置は VLAN インタフェースに IGMP snooping を設定した場合，受信者からの IGMP Report（参加要求）メッセージの収集が完了するまで，マルチキャストパケットの VLAN 内フラッディングを継続します。IGMP Report（参加要求）メッセージの収集が完了したあと，MAC アドレスの学習結果に従い，該当する受信者だけにマルチキャストパケット中継を開始します。マルチキャストパケットは，同一の MAC アドレスに対応する IPv4 マルチキャストアドレスの IGMP Report（参加要求）メッセージを受信したすべてのポートに中継します。

「9.2.1　MAC アドレスの学習　(1)　エントリの登録」の例で述べた 224.10.10.10 と 225.10.10.10 のマルチキャスト MAC アドレスはどちらも 0100.5E0A.0A0A となるため，224.10.10.10 宛てのマルチキャストパケットをレイヤ 2 中継する際に，225.10.10.10 への IGMP Report（参加要求）メッセージを受信したポートへも中継します。

(2)　中継制御対象外のマルチキャストパケット

IGMP snooping がポート単位の中継制御をするマルチキャストパケットはデータトラフィックであり，ルーティングプロトコルなどの制御パケットは VLAN 内の全ルータや全受信者が受信できるように VLAN 内にフラッディングする必要があります。そのため，本装置では，次の表に示すアドレス範囲に含まれる宛先 IP アドレスを持つマルチキャストパケットは，VLAN 内の全ポートに中継し，アドレス範囲外の宛先 IP アドレスを持つマルチキャストパケットは，マルチキャスト MAC アドレスの学習結果に従って中継します。

表 9-4　VLAN 内にフラッディングする IP アドレス範囲

プロトコル	IP アドレス範囲
IGMP snooping	224.0.0.0/24

9.2.3　マルチキャストルータとの接続

マルチキャストパケットの中継先は，マルチキャストグループ参加済みの受信者だけでなく，隣接するマルチキャストルータも対象とします。本装置とマルチキャストルータを接続して IGMP snooping を使用する場合，マルチキャストルータへマルチキャストパケットを中継するためにマルチキャストルータと接続するポート（以降，マルチキャストルータポートとします）をコンフィグレーションで設定します。

(1) マルチキャストルータポートの設定

(a) 冗長構成時

スパニングツリーによる冗長構成時，スパニングツリーのトポロジ変更でルータとの接続が変わる可能性がある場合は，ルータと接続する可能性のある全ポートをマルチキャストルータポートに設定しておく必要があります。

(b) レイヤ 2 スイッチ間の接続時

複数のレイヤ 2 スイッチだけで構成される VLAN で，マルチキャストトラフィックの送信者を収容するレイヤ 2 スイッチと接続するポートをマルチキャストルータポートに設定しておく必要があります。

冗長構成にする場合は，送信者を収容するレイヤ 2 スイッチと接続する可能性のある全ポートをマルチキャストルータポートに設定しておく必要があります。

(2) IGMP メッセージの中継動作

本装置は設定したマルチキャストルータポートに全マルチキャストパケットを中継します。

また，IGMP はルータと受信者間で送受信するプロトコルであるため，IGMP メッセージはルータおよび受信者が受け取ります。本装置は IGMP メッセージを次の表に示すように中継します。

表 9-5 IGMPv1 メッセージごとの動作

IGMPv1 メッセージの種類	VLAN 内転送ポート
IGMPv1 Query	全ポートへ中継します。
IGMPv1 Report	マルチキャストルータポートにだけ中継します。

表 9-6 IGMPv2 メッセージごとの動作

IGMPv2 メッセージの種類	VLAN 内転送ポート
IGMPv2 Query	全ポートへ中継します。
IGMPv2 Report	マルチキャストルータポートにだけ中継します。
IGMPv2 Leave※	ほかのポートにまだグループメンバが存在する場合はどのポートにも中継しません。 ほかのポートにグループメンバが存在しない場合はマルチキャストルータポートに中継します。

注※

自装置にクエリアを設定している場合の中継動作です。クエリアを設定していない場合は，常にマルチキャストルータポートに中継します。

表 9-7 IGMPv3 メッセージごとの動作

IGMPv3 メッセージの種類	VLAN 内転送ポート
IGMPv3 Query	全ポートへ中継します。
IGMPv3 Report（参加要求）	マルチキャストルータポートにだけ中継します。
IGMPv3 Report（離脱要求） (CHANGE_TO_INCLUDE_MODE)※	ほかのポートにまだグループメンバが存在する場合はどのポートにも中継しません。

IGMPv3 メッセージの種類	VLAN 内転送ポート
	ほかのポートにグループメンバが存在しない場合はマルチキャストルータポートに中継します。
IGMPv3 Report（離脱要求） (BLOCK_OLD_SOURCES)	マルチキャストルータポートにだけ中継します。

注※

自装置にクエリアを設定している場合の中継動作です。クエリアを設定していない場合は，常にマルチキャストルータポートに中継します。

9.2.4 IGMP クエリア機能

IGMP クエリア機能は，VLAN 内にマルチキャストルータがなく，マルチキャストパケットの送信者と受信者だけが存在する環境で，本装置が受信者に IGMP Query メッセージを代理で送信する機能です。

マルチキャストルータは定期的に IGMP Query メッセージを送信し，受信者からの応答を受け取ることでグループメンバの存在を確認します。マルチキャストルータがない場合，受信者からの応答がなくなるため，グループメンバを監視できません。このような場合，IGMP クエリア機能を使用すれば，VLAN 内にマルチキャストルータがなくてもグループメンバを監視できるため，IGMP snooping が利用できるようになります。本装置では IGMP Query メッセージを 125 秒間隔で送信します。

IGMP クエリア機能を動作させるには，IGMP snooping を利用する VLAN に IPv4 アドレスを設定する必要があります。

VLAN 内に IGMP Query メッセージを送信する装置がある場合，IGMP Query メッセージの送信元 IPv4 アドレスの小さい方が代表クエリアとなって IGMP Query メッセージを送信します。VLAN 内のほかの装置が代表クエリアの場合，本装置は IGMP クエリア機能による Query メッセージの送信を停止します。

代表クエリアが障害などで停止すると新たに代表クエリアを選定します。VLAN 内の他装置が障害などで本装置が代表クエリアに決定すると Query メッセージの送信を開始します。本装置の代表クエリアの監視時間は 255 秒です。

本装置で送信する IGMP Query のバージョンのデフォルト値は，IGMPv2 です。装置起動以降，IGMP Query のバージョンは，代表クエリアの IGMP バージョンに従います。

9.2.5 IGMP 即時離脱機能

IGMP 即時離脱機能は，IGMPv2 Leave および IGMPv3 Report（離脱要求）メッセージを受信したときに，該当ポートへのマルチキャスト通信をすぐに停止する機能です。

IGMPv3 Report（離脱要求）メッセージのうち，マルチキャストアドレスレコードタイプが CHANGE_TO_INCLUDE_MODE の IGMPv3 Report（離脱要求）メッセージだけを，本機能のサポート対象とします。

9.2.6 同一 VLAN 上での IPv4 マルチキャストが動作する場合

本装置では，IPv4 マルチキャストと IGMP snooping の両方を同一の VLAN 上で同時に動作させることができます。この場合の動作を次に示します。

- IPv4 マルチキャストによる VLAN 間のレイヤ 3 中継時に，中継先の VLAN で IGMP snooping が動作している場合，レイヤ 3 中継されたマルチキャストトラフィックは，中継先の VLAN 内で IGMP snooping の学習結果に従って受信者の存在するポートにだけ中継されます。
- IPv4 マルチキャストが動作することで本装置が VLAN 内の代表クエリアである場合，IGMPv2 Leave メッセージまたは IGMPv3 Report（離脱要求）メッセージ受信による，Group-Specific Query または Group-and-Source-Specific Query は受信ポートだけでなく VLAN 内の全ポートに送信します。

9.2.7 IGMP バージョン 3 受信者との接続

本装置に IGMPv3 受信者を接続する場合，次のどちらかの対応が必要です。

- 該当する VLAN に IPv4 マルチキャストを使用して，IGMP バージョンを 3 に設定してください。
- IGMPv3 ルータを接続して該当するルータが代表クエリアになるように IPv4 アドレスを設定してください。

また，IGMPv3 受信者からの IGMPv3 メッセージがフラグメント化されない構成で運用してください。

9.2.8 IGMP snooping 使用時の注意事項

(1) 他機能との共存

「1.3 レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

(2) IPv4 マルチキャストの静的グループ参加機能との併用

IPv4 マルチキャストの静的グループ参加機能を使用している VLAN では，受信者から IGMP Report（参加要求）が送信されないおそれがあります。IGMP snooping と同時使用する場合，IGMP Report（参加要求）が送信されないとマルチキャスト通信ができないため，静的グループ参加機能を使用している VLAN でマルチキャスト通信が必要なポートには，マルチキャストルータポートを設定してください。

(3) IGMP 即時離脱機能

IGMP 即時離脱機能を使用した場合，IGMPv2 Leave および IGMPv3 Report（離脱要求）メッセージを受信すると，該当ポートへのマルチキャスト通信をすぐに停止します。このため，本機能を使用する場合は，接続ポートに各マルチキャストグループの受信者の端末を 1 台だけ設置することを推奨します。

接続ポートに同一マルチキャストグループの受信者の端末を複数台設置した場合は，一時的にほかの受信者へのマルチキャスト通信が停止します。この場合，受信者からの IGMP Report（参加要求）メッセージを再度受信することで，マルチキャスト通信は再開します。

(4) IPv4 マルチキャストの Last Member Query Time 値について

IPv4 マルチキャストと IGMP snooping を併用する場合は，IPv4 マルチキャストの Last Member Query Time 値が 3 秒以下になるように設定してください。

Last Member Query Time は，各コンフィグレーションコマンドの設定値から次に示す計算式で算出される時間です。

Last Member Query Time ＝
　ip igmp last-member-query-interval コマンドの設定値×
　（ip igmp last-member-query-count コマンドの設定値－1）＋
　ip igmp last-member-query-max-response-time コマンドの設定値

Last Member Query Time 値が 3 秒より長く，かつ一つの接続ポートに同一マルチキャストグループの受信者が複数存在する状態で併用すると，一方の受信者の IGMPv2 Leave または IGMPv3 Report（離脱要求）メッセージによって，他方の受信者へのマルチキャスト通信が停止することがあります。

9.3 IGMP snooping のコンフィグレーション

9.3.1 コンフィグレーションコマンド一覧

IGMP snooping 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 9-8 コンフィグレーションコマンド一覧

コマンド名	説明
ip igmp snooping（global）	no ip igmp snooping によって，本装置で IGMP snooping を無効にします。
ip igmp snooping（VLAN インタフェース）	VLAN インタフェースで IGMP snooping を有効にします。
ip igmp snooping fast-leave	IGMP 即時離脱機能を有効にします。
ip igmp snooping mrouter	VLAN インタフェースにマルチキャストルータポートを設定します。
ip igmp snooping querier	VLAN インタフェースで IGMP クエリア機能を有効にします。

9.3.2 IGMP snooping の設定

[設定のポイント]

VLAN インタフェースのコンフィグレーションモードで設定します。ここでは，VLAN2 で IGMP snooping を有効にする例を示します。

[コマンドによる設定]

1. **(config)# interface vlan 2**
   (config-if)# ip igmp snooping
   VLAN2 のコンフィグレーションモードに移行して，IGMP snooping を有効にします。

9.3.3 IGMP クエリア機能の設定

[設定のポイント]

IGMP snooping を設定した VLAN 内にマルチキャストルータがない場合,IGMP クエリア機能を動作させる必要があります。VLAN インタフェースのコンフィグレーションモードで設定します。

[コマンドによる設定]

1. **(config-if)# ip igmp snooping querier**
   IGMP クエリア機能を有効にします。

[注意事項]

本設定は該当するインタフェースに IPv4 アドレスの設定がないと有効になりません。

9.3.4 マルチキャストルータポートの設定

[設定のポイント]

IGMP snooping を設定した VLAN 内にマルチキャストルータを接続している場合，VLAN インタフェースのコンフィグレーションモードで設定します。ここでは，該当する VLAN 内のギガビットイーサネットのインタフェース 1/1 にマルチキャストルータを接続している場合の例を示します。

[コマンドによる設定]

1. **(config-if)# ip igmp snooping mrouter interface gigabitethernet 1/1**
   該当するインタフェースで，マルチキャストルータポートを設定します。

9.4 MLD snooping の解説

ここでは，MLD snooping の機能と動作について説明します。本装置が送受信する MLD メッセージのフォーマットおよび既定値は RFC2710 に従います。また，MLD バージョン 2（以降，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。

9.4.1 MAC アドレスの学習

MLD snooping が設定された VLAN で MLD メッセージを受信することによってマルチキャスト MAC アドレスをダイナミックに学習します。学習したマルチキャスト MAC アドレスは MAC アドレステーブルに登録します。

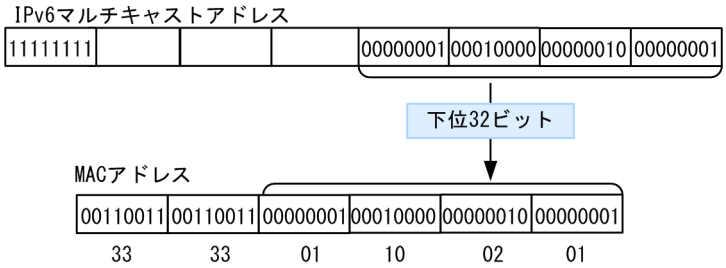
(1) エントリの登録

次に示す MLD メッセージを受信すると，メッセージに含まれるグループアドレスからマルチキャスト MAC アドレスを学習し，受信したポートにだけマルチキャストグループ宛てのトラフィックを中継するエントリを作成します。以降，これらのメッセージを MLD Report（参加要求）メッセージと呼びます。

- MLDv1 Report メッセージ
- MLDv2 Report（参加要求）メッセージ

IPv6 マルチキャストパケットの宛先 MAC アドレスは IPv6 アドレスの下位 32 ビットを MAC アドレスにコピーして生成します。IPv6 マルチキャストアドレスは，マルチキャストグループを識別するグループ ID フィールドが 112 ビット長のフォーマットと，32 ビット長のフォーマットの 2 種類が規定されています。グループ ID フィールドが 112 ビット長のアドレスフォーマットを使用する場合は，IPv4 マルチキャストアドレスと同様に MAC アドレスの重複が発生します。IPv6 マルチキャストアドレスと MAC アドレスの対応を次の図に示します。

図 9-4 IPv6 マルチキャストアドレスと MAC アドレスの対応



(2) MLDv1 メッセージ受信によるエントリの削除

MLDv1 Done メッセージを受信すると，受信したポートだけエントリから削除し，このポートへのマルチキャストトラフィックの中継を停止します。VLAN 内のすべてのポートにグループメンバが存在しなくなった時点で，エントリを削除します。

(a) MLD クエリア機能設定時の動作

本装置は，MLDv1 Done メッセージを受信したポートから Group-Specific Query メッセージを 1 秒間隔で 2 回送信します。応答がない場合にエントリからこのポートだけを削除します。

(b) MLD 即時離脱機能設定時の動作

本装置は，MLDv1 Done メッセージを受信したポートをエントリからすぐに削除します。MLD クエリア機能を設定していても，Group-Specific Query メッセージは送信しません。

(3) MLDv2 メッセージ受信によるエントリの削除

MLDv2 Report（離脱要求）メッセージを受信すると，受信したポートだけエントリから削除し，このポートへのマルチキャストトラフィックの中継を停止します。VLAN 内のすべてのポートにグループメンバが存在しなくなった時点で，エントリを削除します。

(a) MLD クエリア機能設定時の動作

本装置は，MLDv2 Report（離脱要求）メッセージを受信したポートから Group-Specific Query メッセージを 1 秒間隔で 2 回送信します。応答がない場合にエントリからこのポートだけを削除します。

ただし，受信した MLDv2 Report（離脱要求）メッセージのマルチキャストアドレスレコードタイプが BLOCK_OLD_SOURCES の場合，これらの削除処理が実行されるのは，該当する VLAN に IPv6 マルチキャストを使用していないときだけです。

(b) MLD 即時離脱機能設定時の動作

本装置は，マルチキャストアドレスレコードタイプが CHANGE_TO_INCLUDE_MODE の MLDv2 Report（離脱要求）メッセージを受信したポートをエントリからすぐに削除します。

MLD クエリア機能を設定していても，Group-Specific Query メッセージは送信しません。

(4) エントリのエージング

MLD Report（参加要求）メッセージを受信してから一定時間経過すると，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グループメンバが存在するかを確認するため，定期的に MLD Query メッセージを送信します。本装置はルータからの MLD Query メッセージを受信した場合，VLAN 内の全ポートに中継します。MLD Query メッセージへの応答である MLD Report（参加要求）メッセージを受信しない場合，エントリからこのポートだけを削除します。すべてのポートから応答がない場合は，エントリ自体を削除します。

本装置では，ポートへの中継を停止するタイムアウト時間は 260 秒（コンフィグレーションコマンド ipv6 mld query-interval のデフォルト値から算出）であり，この間に MLD Report（参加要求）メッセージを受信しない場合，該当するポートへの中継を停止します。

次の場合，タイムアウト時間は動的に設定します。

- 他装置が代表クエリア（MLDv2 での運用）
  代表クエリアからの MLDv2 Query メッセージ（QQIC フィールド）から算出します。
- 自装置が代表クエリアで IPv6 マルチキャストを使用
  MLDv1/MLDv2 に関係なく，自装置に設定した Query Interval で算出します。ただし，Query Interval を設定していないときは，デフォルト値での運用となります。
- 他装置が代表クエリア（MLDv1 での運用）で IPv6 マルチキャストを使用
  該当する VLAN に IPv6 マルチキャストを使用しているときは，自装置に設定した Query Interval で算出します。ただし，Query Interval を設定していないときは，デフォルト値での運用となります。

また，次の場合，タイムアウト時間はデフォルト値での運用となります。

- 自装置が代表クエリアで IPv6 マルチキャストは未使用
  MLDv1/MLDv2 に関係なく，デフォルト値での運用となります。
- 他装置が代表クエリア（MLDv1 での運用）で IPv6 マルチキャストは未使用
  該当する VLAN に IPv6 マルチキャストを使用していないときは，デフォルト値での運用となります。この場合，該当する VLAN では Query Interval を 125 秒で運用してください。

注　タイムアウト時間は，Query Interval（QQIC フィールドの値）×2+Query Response Interval で算出します。

9.4.2　マルチキャストパケットの中継制御

(1)　MAC アドレス学習によるマルチキャストパケット中継

本装置は VLAN インタフェースに MLD snooping を設定した場合，受信者からの MLD Report（参加要求）メッセージの収集が完了するまで，マルチキャストパケットの VLAN 内フラッディングを継続します。MLD Report（参加要求）メッセージの収集が完了したあと，MAC アドレスの学習結果に従い，該当する受信者だけにマルチキャストパケット中継を開始します。マルチキャストパケットは，同一の MAC アドレスに対応する IPv6 マルチキャストアドレスの MLD Report（参加要求）メッセージを受信したすべてのポートに中継します。

(2)　中継制御対象外のマルチキャストパケット

MLD snooping がポート単位の中継制御をするマルチキャストパケットはデータトラフィックであり，ルーティングプロトコルなどの制御パケットは VLAN 内の全ルータや全受信者が受信できるように VLAN 内にフラッディングする必要があります。そのため，本装置では，次の表に示すアドレス範囲に含まれる宛先 IP アドレスを持つマルチキャストパケットは，VLAN 内の全ポートに中継し，アドレス範囲外の宛先 IP アドレスを持つマルチキャストパケットは，マルチキャスト MAC アドレスの学習結果に従って中継します。

表 9-9　VLAN 内にフラッディングする IP アドレス範囲

プロトコル	IP アドレス範囲
MLD snooping	ff*2::/16（*は任意）

9.4.3　マルチキャストルータとの接続

マルチキャストパケットの中継先は，マルチキャストグループ参加済みの受信者だけでなく，隣接するマルチキャストルータも対象とします。本装置とマルチキャストルータを接続して MLD snooping を使用する場合，マルチキャストルータへマルチキャストパケットを中継するためにマルチキャストルータと接続するポート（以降，マルチキャストルータポートとします）をコンフィグレーションで設定します。

(1)　マルチキャストルータポートの設定

(a)　冗長構成時

スパニングツリーによる冗長構成時，スパニングツリーのトポロジ変更でルータとの接続が変わる可能性がある場合は，ルータと接続する可能性のある全ポートをマルチキャストルータポートに設定しておく必要があります。

(b)　レイヤ 2 スイッチ間の接続時

複数のレイヤ 2 スイッチだけで構成される VLAN で，マルチキャストトラフィックの送信者を収容するレイヤ 2 スイッチと接続するポートをマルチキャストルータポートに設定しておく必要があります。

冗長構成にする場合は，送信者を収容するレイヤ 2 スイッチと接続する可能性のある全ポートをマルチキャストルータポートに設定しておく必要があります。

(2)　MLD メッセージの中継動作

本装置は設定したマルチキャストルータポートに全マルチキャストパケットを中継します。

また，MLD はルータと受信者間で送受信するプロトコルであるため，MLD メッセージはルータおよび受信者が受け取ります。本装置は MLD メッセージを次の表に示すように中継します。

表 9-10　MLDv1 メッセージごとの動作

MLDv1 メッセージの種類	VLAN 内転送ポート
MLDv1 Query	全ポートへ中継します。
MLDv1 Report	マルチキャストルータポートにだけ中継します。
MLDv1 Done※	ほかのポートにまだグループメンバが存在する場合はどのポートにも中継しません。 ほかのポートにグループメンバが存在しない場合はマルチキャストルータポートに中継します。

注※

自装置にクエリアを設定している場合の中継動作です。クエリアを設定していない場合は，常にマルチキャストルータポートに中継します。

表 9-11　MLDv2 メッセージごとの動作

MLDv2 メッセージの種類	VLAN 内転送ポート
MLDv2 Query	全ポートへ中継します。
MLDv2 Report（参加要求）	マルチキャストルータポートにだけ中継します。
MLDv2 Report（離脱要求） (CHANGE_TO_INCLUDE_MODE)※	ほかのポートにまだグループメンバが存在する場合はどのポートにも中継しません。 ほかのポートにグループメンバが存在しない場合はマルチキャストルータポートに中継します。
MLDv2 Report（離脱要求） (BLOCK_OLD_SOURCES)	マルチキャストルータポートにだけ中継します。

注※

自装置にクエリアを設定している場合の中継動作です。クエリアを設定していない場合は，常にマルチキャストルータポートに中継します。

9.4.4　MLD クエリア機能

MLD クエリア機能は，VLAN 内にマルチキャストルータがなく，マルチキャストパケットの送信者と受信者だけが存在する環境で，本装置が受信者に MLD Query メッセージを代理で送信する機能です。

マルチキャストルータは定期的に MLD Query メッセージを送信し，受信者からの応答を受け取ることでグループメンバの存在を確認します。マルチキャストルータがない場合，受信者からの応答がなくなるため，グループメンバを監視できません。このような場合，MLD クエリア機能を使用すれば，VLAN 内にマルチキャストルータがなくてもグループメンバを監視できるため，MLD snooping が利用できるようになります。本装置では Query メッセージを 125 秒間隔で送信します。

MLD クエリア機能を動作させるには，MLD snooping を利用する VLAN に IPv6 アドレスを設定する必要があります。

VLAN 内に MLD Query メッセージを送信する装置がある場合，MLD Query メッセージの送信元 IPv6 アドレスの小さい方が代表クエリアとなって MLD Query メッセージを送信します。VLAN 内のほかの装置が代表クエリアの場合，本装置は MLD クエリア機能による MLD Query メッセージの送信を停止します。

代表クエリアが障害などで停止すると新たに代表クエリアを選定します。VLAN 内の他装置が障害などで本装置が代表クエリアに決定すると MLD Query メッセージの送信を開始します。本装置の代表クエリアの監視時間は 255 秒です。

本装置で送信する MLD Query のバージョンのデフォルト値は，MLDv1 です。装置起動以降，MLD Query のバージョンは，代表クエリアの MLD バージョンに従います。

9.4.5 MLD 即時離脱機能

MLD 即時離脱機能は，MLDv1 Done および MLDv2 Report（離脱要求）メッセージを受信したときに，該当ポートへのマルチキャスト通信をすぐに停止する機能です。

MLDv2 Report（離脱要求）メッセージのうち，マルチキャストアドレスレコードタイプが CHANGE_TO_INCLUDE_MODE の MLDv2 Report（離脱要求）メッセージだけを，本機能のサポート対象とします。

9.4.6 同一 VLAN 上での IPv6 マルチキャストが動作する場合

本装置では，IPv6 マルチキャストと MLD snooping の両方を同一の VLAN 上で同時に動作させることができます。この場合の動作を次に示します。

- IPv6 マルチキャストによる VLAN 間のレイヤ 3 中継時に，中継先の VLAN で MLD snooping が動作している場合，レイヤ 3 中継されたマルチキャストトラフィックは，中継先の VLAN 内で MLD snooping の学習結果に従って受信者の存在するポートにだけ中継されます。
- IPv6 マルチキャストが動作することで本装置が VLAN 内の代表クエリアである場合，MLDv1 Done メッセージまたは MLDv2 Report（離脱要求）メッセージ受信による，Group-Specific Query または Group-and-Source-Specific Query は受信ポートだけでなく VLAN 内の全ポートに送信します。

9.4.7 MLD バージョン 2 受信者との接続

本装置に MLDv2 受信者を接続する場合，次のどちらかの対応が必要です。

- 該当する VLAN に IPv6 マルチキャストを使用して，MLD バージョンを 2 に設定してください。
- MLDv2 ルータを接続して該当するルータが代表クエリアになるように IPv6 アドレスを設定してください。

また，MLDv2 受信者からの MLDv2 メッセージがフラグメント化されない構成で運用してください。

9.4.8 MLD snooping 使用時の注意事項

(1) 他機能との共存

「1.3 レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

(2) IPv6 マルチキャストの静的グループ参加機能との併用

IPv6 マルチキャストの静的グループ参加機能を使用している VLAN では，受信者から MLD Report（参加要求）が送信されないおそれがあります。MLD snooping と同時使用する場合，MLD Report（参加要求）が送信されないとマルチキャスト通信ができないため，静的グループ参加機能を使用している VLAN でマルチキャスト通信が必要なポートには，マルチキャストルータポートを設定してください。

(3) MLD 即時離脱機能

MLD 即時離脱機能を使用した場合，MLDv1 Done および MLDv2 Report（離脱要求）メッセージを受信すると，該当ポートへのマルチキャスト通信をすぐに停止します。このため，本機能を使用する場合は，接続ポートに各マルチキャストグループの受信者の端末を 1 台だけ設置することを推奨します。

接続ポートに同一マルチキャストグループの受信者の端末を複数台設置した場合は，一時的にほかの受信者へのマルチキャスト通信が停止します。この場合，受信者からの MLD Report（参加要求）メッセージを再度受信することで，マルチキャスト通信は再開します。

9.5 MLD snooping のコンフィグレーション

9.5.1 コンフィグレーションコマンド一覧

MLD snooping 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 9-12 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 snooping（global）	no ipv6 mld snooping によって，本装置で MLD snooping を無効にします。
ipv6 mld snooping（VLAN インタフェース）	VLAN インタフェースで MLD snooping を有効にします。
ipv6 mld snooping fast-leave	MLD 即時離脱機能を有効にします。
ipv6 mld snooping mrouter	VLAN インタフェースにマルチキャストルータポートを設定します。
ipv6 mld snooping querier	VLAN インタフェースで MLD クエリア機能を有効にします。

9.5.2 MLD snooping の設定

[設定のポイント]

VLAN インタフェースのコンフィグレーションモードで設定します。ここでは，VLAN2 で MLD snooping を有効にする例を示します。

[コマンドによる設定]

1. **(config)# interface vlan 2**
   (config-if)# ipv6 mld snooping
   VLAN2 のコンフィグレーションモードに移行して，MLD snooping を有効にします。

9.5.3 MLD クエリア機能の設定

[設定のポイント]

MLD snooping を設定した VLAN 内にマルチキャストルータがない場合，MLD クエリア機能を動作させる必要があります。VLAN インタフェースのコンフィグレーションモードで設定します。

[コマンドによる設定]

1. **(config-if)# ipv6 mld snooping querier**
   MLD クエリア機能を有効にします。

[注意事項]

本設定は該当するインタフェースに IPv6 アドレスの設定がないと有効になりません。

9.5.4 マルチキャストルータポートの設定

[設定のポイント]

MLD snooping を設定した VLAN 内にマルチキャストルータを接続している場合，VLAN インタフェースのコンフィグレーションモードで設定します。ここでは，該当する VLAN 内のギガビットイーサネットのインタフェース 1/1 にマルチキャストルータを接続している場合の例を示します。

[コマンドによる設定]

1. **(config-if)# ipv6 mld snooping mrouter interface gigabitethernet 1/1**
   該当するインタフェースで，マルチキャストルータポートを設定します。

9.6 IGMP/MLD snooping のオペレーション

9.6.1 運用コマンド一覧

IGMP snooping の運用コマンド一覧を次の表に示します。

表 9-13 IGMP snooping の運用コマンド一覧

コマンド名	説明
show igmp-snooping	IGMP snooping 情報を表示します。
clear igmp-snooping	IGMP snooping 情報をクリアします。

MLD snooping の運用コマンド一覧を次の表に示します。

表 9-14 MLD snooping の運用コマンド一覧

コマンド名	説明
show mld-snooping	MLD snooping 情報を表示します。
clear mld-snooping	MLD snooping 情報をクリアします。

9.6.2 IGMP snooping の確認

IGMP snooping に関する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

show igmp-snooping コマンドを実行し，IGMP snooping に関する設定が正しいことを確認してください。

図 9-5 IGMP snooping の設定状態表示

```
> show igmp-snooping 100
Date 20XX/10/01 15:20:00 UTC
VLAN: 100
  IP address: 192.168.11.20    Querier: enable
  IGMP querying system: 192.168.11.20
  Querier version: V2
  IPv4 Multicast routing: Off
  Fast-leave: On
  Port(5): 1/1-5
  Mrouter-port: 1/1,3
  Group Counts: 3
```

(2) 運用中の確認

次のコマンドで，IGMP snooping の運用中の状態を確認してください。

- 学習した MAC アドレス，VLAN 内に中継される IPv4 マルチキャストアドレスと中継先のポートは，show igmp-snooping コマンドに group パラメータを指定して確認してください。

  図 9-6 show igmp-snooping group コマンドの実行結果

  ```
  > show igmp-snooping group 100
  Date 20XX/02/01 15:20:00 UTC
  VLAN counts: 1
  VLAN: 100  Group counts: 3 IPv4 Multicast routing: Off
    Group Address     MAC Address             Version        Mode
  ```

```
  224.10.10.10      0100.5e0a.0a0a          V2              -
    Port-list:1/1-3
  225.10.10.10      0100.5e0a.0a0a          V3              INCLUDE
    Port-list:1/1-2
  239.192.1.1       0100.5e40.0101          V2,V3           EXCLUDE
    Port-list:1/1
```

- ポートごとのマルチキャストグループ参加状態は show igmp-snooping コマンドに port パラメータを指定して確認してください。

図 9-7 show igmp-snooping port コマンドの実行結果

```
> show igmp-snooping port 1/1
Date 20XX/10/01 15:20:00 UTC
Port 1/1  VLAN counts: 2
  VLAN: 100  Group counts: 2
    Group Address     Last Reporter      Uptime     Expires
    224.10.10.10      192.168.1.3        00:10      04:10
    239.192.1.1       192.168.1.3        02:10      03:00
  VLAN: 150  Group counts: 1
    Group Address     Last Reporter      Uptime     Expires
    239.10.120.1      192.168.15.10      01:10      02:30
```

9.6.3 MLD snooping の確認

MLD snooping に関する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

show mld-snooping コマンドを実行し，MLD snooping に関する設定が正しいことを確認してください。

図 9-8 MLD snooping の設定状態表示

```
> show mld-snooping 100
Date 20XX/02/01 15:20:00 UTC
VLAN: 100
  IP address: fe80::b1    Querier: enable
  MLD querying system: fe80::b1
  Querier version: V1
  IPv6 Multicast routing: Off
  Fast-leave: On
  Port(5): 1/1-5
  Mrouter-port: 1/1,3
  Group Counts: 3
```

(2) 運用中の確認

以下のコマンドで，MLD snooping の運用中の状態を確認してください。

- 学習した MAC アドレス，VLAN 内に中継される IPv6 マルチキャストアドレスと中継先のポートは，show mld-snooping コマンドに group パラメータを指定して確認してください。

図 9-9 show mld-snooping group コマンドの実行結果

```
> show mld-snooping group 100
Date 20XX/02/01 15:20:00 UTC
VLAN counts: 1
VLAN: 100  Group counts: 2 IPv6 Multicast routing: Off
  Group Address     MAC Address             Version      Mode
  ff35::1           3333.0000.0001          V1,V2        EXCLUDE
    Port-list:1/1-3
  ff35::2           3333.0000.0002          V2           EXCLUDE
    Port-list:1/1-2
```

- ポートごとのマルチキャストグループ参加状態は show mld-snooping コマンドに port パラメータを指定して確認してください。

図 9-10 show mld-snooping port コマンドの実行結果

```
> show mld-snooping port 1/1
Date 20XX/10/01 15:20:00 UTC
Port  1/1  VLAN counts: 1
  VLAN: 100  Group counts: 2
    Group Address      Last Reporter      Uptime     Expires
    ff35::1            fe80::b2           00:10      04:10
    ff35::2            fe80::b3           02:10      03:00
```

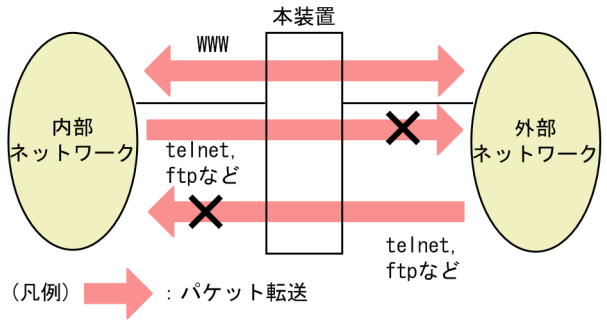
10 フィルタ

フィルタは，受信フレームや送信フレームを中継したり，廃棄したりする機能です。この章では，フィルタ機能の解説と操作方法について説明します。

10.1　解説

フィルタは，受信フレームや送信フレームのうち特定のフレームを中継または廃棄する機能です。フィルタはネットワークのセキュリティを確保するために使用します。フィルタを使用すると，ユーザごとやプロトコルごとにネットワークへのアクセスを制限できます。例えば，内部ネットワークと外部ネットワーク間でWWW は中継しても，telnet や ftp は廃棄したいなどの運用ができます。外部ネットワークからの不正なアクセスを防ぎ，また，内部ネットワークから外部ネットワークへ不要な情報の漏洩を防ぐことができます。フィルタを使用したネットワーク構成例を次に示します。

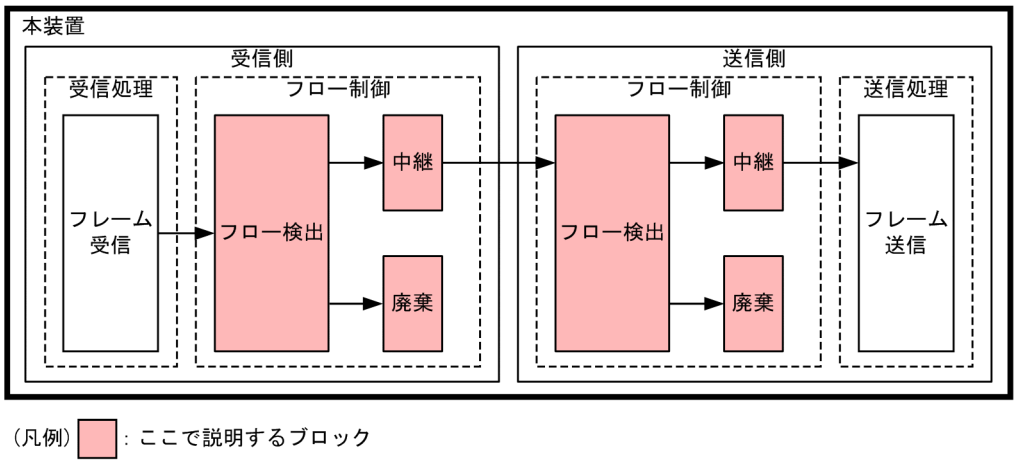
図 10-1　フィルタを使用したネットワーク構成例



10.1.1　フィルタの概要

本装置のフィルタの機能ブロックを次の図に示します。

図 10-2　本装置のフィルタの機能ブロック



この図に示したフィルタの各機能ブロックの概要を次の表に示します。

表 10-1　フィルタの各機能ブロックの概要

機能部位		機能概要
フロー制御	フロー検出	MAC アドレスやプロトコル種別，IP アドレス，TCP/UDP のポート番号などの条件に一致するフロー（特定フレーム）を検出します。
	中継・廃棄	フロー検出したフレームに対し，中継または廃棄します。

本装置では，MAC アドレス，プロトコル種別，IP アドレス，TCP/UDP のポート番号などのフロー検出と，中継や廃棄という動作を組み合わせたフィルタエントリを作成して，フィルタを実施します。

本装置のフィルタの仕組みを次に示します。

1. 各インタフェースに設定したフィルタエントリをユーザが設定した優先順に検索します。
2. 一致したフィルタエントリが見つかった時点で検索を終了します。
3. 該当したフレームはフィルタエントリで設定した動作に従って，中継や廃棄が実行されます。
4. すべてのフィルタエントリに一致しなかった場合は，そのフレームを廃棄します。廃棄動作の詳細は，「10.1.6　暗黙の廃棄」を参照してください。

10.1.2　フロー検出

フロー検出とは，フレームの一連の流れであるフローを MAC ヘッダ，IP ヘッダ，TCP ヘッダなどの条件に基づいて検出する機能です。アクセスリストで設定します。アクセスリストの詳細は，「10.1.5　アクセスリスト」を参照してください。

本装置の各インタフェースに対するフロー検出およびアクセスリストの設定可否を次の表に示します。

表 10-2　インタフェースに対するフロー検出およびアクセスリストの設定可否

インタフェース	フロー検出	アクセスリストの設定
イーサネットインタフェース	○	○
イーサネットサブインタフェース	○	○
ポートチャネルインタフェース	○※	－
ポートチャネルサブインタフェース	○	○
VLAN インタフェース	○	○
ループバックインタフェース	－	－
Null インタフェース	－	－
マネージメントポート	－	－
AUX ポート	－	－

（凡例）　○：検出または設定できる　－：検出または設定できない

注※

チャネルグループを構成するイーサネットインタフェースにアクセスリストを設定すると，フロー検出ができます。

10.1.3　フロー検出モード

本装置では，フロー検出動作を決めるモードとしてフロー検出モードを用意しています。フロー検出モードごとの特徴を次に示します。

エントリ数重視モード

エントリ数が多くなりますが，検出条件が次のように限定されます。

- 非 IP パケットおよびレイヤ 2 中継する IP パケットを，MAC ヘッダでフロー検出します。
- レイヤ 3 中継する IP パケットを，IP ヘッダとレイヤ 4 ヘッダの組み合わせでフロー検出します。

検出条件数重視モード

エントリ数は少なくなりますが，エントリ当たりの検出条件数が多いためきめ細かい検出ができます。非 IP パケット，IP パケットのすべてをフロー検出の対象として，MAC ヘッダ，IP ヘッダ，およびレイヤ 4 ヘッダを組み合わせた Advance 条件でフロー検出します。

フロー検出モードはコンフィグレーションコマンド flow detection mode で設定します。デフォルトでは，エントリ数重視モードです。フロー検出モードとフロー検出動作については，「10.1.5　アクセスリスト」を参照してください。

10.1.4　フロー検出条件

フロー検出するためには，コンフィグレーションでフローを識別するための条件を指定します。フロー検出条件は MAC 条件，IPv4 条件，IPv6 条件，および Advance 条件に分類されます。フロー検出条件と検出できるヘッダ種別の対応を次の表に示します。

表 10-3　フロー検出条件と検出できるヘッダ種別の対応

フロー検出条件	MAC ヘッダ	VLAN Tag ヘッダ	IPv4 ヘッダ	IPv6 ヘッダ	レイヤ 4 ヘッダ
MAC 条件	○	○	－	－	－
IPv4 条件	－	○	○	－	○
IPv6 条件	－	○	－	○	○
Advance 条件	○	○	○	○	○

（凡例）　○：検出できる　－：検出できない

指定できるフロー検出条件の詳細項目を次の表に示します。

表 10-4　指定できるフロー検出条件の詳細項目

種別		設定項目
MAC 条件	コンフィグレーション	インタフェース※1
	MAC ヘッダ	送信元 MAC アドレス
		宛先 MAC アドレス
		イーサネットタイプ
	VLAN Tag ヘッダ※2	Tag の VLAN ID
		ユーザ優先度
		Tag なし
	2 段目の VLAN Tag ヘッダ※3	Tag の VLAN ID
		ユーザ優先度
		Tag なし
IPv4 条件	コンフィグレーション	インタフェース※1
	VLAN Tag ヘッダ※2	ユーザ優先度

種別		設定項目	
		Tag なし	
	IPv4 ヘッダ	上位プロトコル※4	
		送信元 IP アドレス	
		宛先 IP アドレス	
		ToS※5	
		DSCP※5	
		Precedence※5	
		フラグメント※6	FO
			MF
		IP レングス	
	IPv4-TCP ヘッダ	送信元ポート番号	
		宛先ポート番号	
		TCP 制御フラグ※7	
	IPv4-UDP ヘッダ	送信元ポート番号	
		宛先ポート番号	
	IPv4-ICMP ヘッダ	ICMP タイプ	
		ICMP コード	
	IPv4-IGMP ヘッダ	IGMP タイプ	
IPv6 条件	コンフィグレーション	インタフェース※1	
	VLAN Tag ヘッダ※2	ユーザ優先度	
		Tag なし	
	IPv6 ヘッダ	上位プロトコル※8	
		送信元 IP アドレス※9	
		宛先 IP アドレス	
		トラフィッククラス※10	
		DSCP※10	
		フラグメント※6	FO
			MF
		IP レングス	
	IPv6-TCP ヘッダ	送信元ポート番号	
		宛先ポート番号	

種別		設定項目	
		TCP 制御フラグ※7	
	IPv6-UDP ヘッダ	送信元ポート番号	
		宛先ポート番号	
	IPv6-ICMP ヘッダ	ICMP タイプ	
		ICMP コード	
Advance 条件	コンフィグレーション	インタフェース※1	
	MAC ヘッダ	送信元 MAC アドレス※11	
		宛先 MAC アドレス	
		イーサネットタイプ	
	VLAN Tag ヘッダ※2	Tag の VLAN ID	
		ユーザ優先度	
		Tag なし	
	2 段目の VLAN Tag ヘッダ※3	Tag の VLAN ID	
		ユーザ優先度	
		Tag なし	
	IPv4 ヘッダ	上位プロトコル※4	
		送信元 IP アドレス	
		宛先 IP アドレス	
		ToS※5	
		DSCP※5	
		Precedence※5	
		フラグメント※6	FO
			MF
		IP レングス	
	IPv4-TCP ヘッダ	送信元ポート番号	
		宛先ポート番号	
		TCP 制御フラグ※7	
	IPv4-UDP ヘッダ	送信元ポート番号	
		宛先ポート番号	
	IPv4-ICMP ヘッダ	ICMP タイプ	
		ICMP コード	

種別		設定項目	
	IPv4-IGMP ヘッダ	IGMP タイプ	
	IPv6 ヘッダ	上位プロトコル※8	
		送信元 IP アドレス	
		宛先 IP アドレス	
		トラフィッククラス※10	
		DSCP※10	
		フラグメント※6	FO
			MF
		IP レングス	
	IPv6-TCP ヘッダ	送信元ポート番号	
		宛先ポート番号	
		TCP 制御フラグ※7	
	IPv6-UDP ヘッダ	送信元ポート番号	
		宛先ポート番号	
	IPv6-ICMP ヘッダ	ICMP タイプ	
		ICMP コード	
	中継種別※12	パケット中継種別	

注※1

インタフェースのコンフィグレーションで設定した，インタフェース名およびインタフェース番号です。指定できるインタフェース名を次に示します。

- イーサネットサブインタフェース
- ポートチャネルサブインタフェース
- VLAN インタフェース

注※2

VLAN Tag ヘッダを指定したときの検出を次に示します。

Tag の VLAN ID

VLAN Tag ヘッダの VLAN ID です。Untagged フレームは検出しません。

ユーザ優先度

VLAN Tag ヘッダのユーザ優先度です。Untagged フレームは検出しません。

Tag なし

Untagged フレームです。Tagged フレームは検出しません。

注※3

2 段目の VLAN Tag ヘッダを指定したときの検出を次に示します。

Tag の VLAN ID

2 段目の VLAN Tag ヘッダの VLAN ID です。VLAN Tag ヘッダが 1 段以下のフレームは検出しません。

ユーザ優先度

2 段目の VLAN Tag ヘッダのユーザ優先度です。VLAN Tag ヘッダが 1 段以下のフレームは検出しません。

Tag なし

2 段目の VLAN Tag ヘッダがないフレームです。VLAN Tag ヘッダが 2 段以上のフレームは検出しません。

注※4

IPv4 ヘッダのプロトコルフィールドで示される値を検出します。

注※5

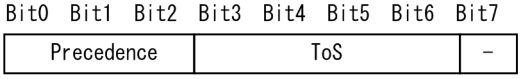
ToS フィールドを指定したときの検出を次に示します。

ToS

ToS フィールドの 3 ビット～6 ビットの値です。

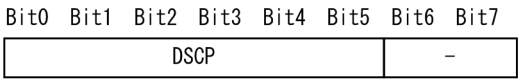
Precedence

ToS フィールドの上位 3 ビットの値です。



DSCP

ToS フィールドの上位 6 ビットの値です。



注※6

フラグメントパラメータを指定したときの検出を次に示します。+fo を指定した場合は，VLAN Tag ヘッダと IP ヘッダだけをフロー検出条件として指定できます。

+fo 指定

フラグメントパケットの途中と最後のパケットを検出します。

-fo 指定

非フラグメントパケット，およびフラグメントパケットの最初のパケットを検出します。

+mf 指定

フラグメントパケットの最初と途中のパケットを検出します。

-mf 指定

非フラグメントパケット，およびフラグメントパケットの最後のパケットを検出します。

フラグメントパラメータの組み合わせと検出するパケットの関係を次の表に示します。

表 10-5　フラグメントパラメータの組み合わせと検出するパケットの関係

フラグメントパラメータ		非フラグメントパケット	フラグメントパケット		
FO	MF		最初	途中	最後
指定なし	指定なし	○	○	○	○

フラグメントパラメータ		非フラグメントパケット	フラグメントパケット		
FO	MF		最初	途中	最後
	-mf 指定	○	－	－	○
	+mf 指定	－	○	○	－
-fo 指定	指定なし	○	○	－	－
	-mf 指定	○	－	－	－
	+mf 指定	－	○	－	－
+fo 指定	指定なし	－	－	○	○
	-mf 指定	－	－	－	○
	+mf 指定	－	－	○	－

（凡例）　○：検出する　－：検出しない

注※7

ack/fin/psh/rst/syn/urg フラグを検出します。

注※8

IPv6 ヘッダまたは IPv6 拡張ヘッダの NextHeader フィールドで示される拡張ヘッダ以外の値を検出します。

注※9

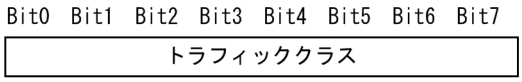
上位 64bit だけ設定できます。

注※10

トラフィッククラスフィールドを指定したときの検出を次に示します。

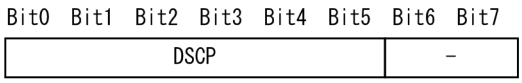
トラフィッククラス

トラフィッククラスフィールドの値です。



DSCP

トラフィッククラスフィールドの上位 6 ビットの値です。



注※11

送信側インタフェースで送信元 MAC アドレスを指定した場合，本装置がレイヤ 3 中継するパケットは受信時の送信元 MAC アドレスで検出します。

注※12

中継種別を指定したときの検出を次に示します。

レイヤ 2 中継

レイヤ 2 中継するフレームを検出します。

レイヤ 3 中継

レイヤ 3 中継するパケットを検出します。

10.1.5 アクセスリスト

フィルタのフロー検出を実施するためにはコンフィグレーションでアクセスリストを設定します。フロー検出条件に応じて設定するアクセスリストが異なります。また，フロー検出条件ごとに検出できるフレーム種別が異なります。フロー検出条件とアクセスリスト，および検出するフレーム種別の関係を次の表に示します。

表 10-6 フロー検出条件とアクセスリスト，検出するフレーム種別の関係

フロー検出条件	アクセスリスト	検出するフレーム種別					
		エントリ数重視モード			検出条件数重視モード		
		非 IP	IPv4	IPv6	非 IP	IPv4	IPv6
MAC 条件	mac access-list	○	○※1	○※1	○	○※1	○※1
IPv4 条件	ip access-list	－	○※2	－	－	○※2	－
IPv6 条件	ipv6 access-list	－	－	○※2	－	－	○※2
Advance 条件	advance access-list	－※3	－※3	－※3	○	○※4	○※4

（凡例） ○：検出する －：検出しない

注※1

レイヤ 2 中継するフレームを検出します。

注※2

レイヤ 3 中継するパケットを検出します。

注※3

エントリ数重視モードの場合，Advance 条件をインタフェースに適用できません。

注※4

レイヤ 2 中継およびレイヤ 3 中継するフレームの両方を検出します。

アクセスリストのインタフェースへの適用は，アクセスリストグループコマンドおよび IPv6 トラフィックフィルタコマンドで設定します。

なお，アクセスリストは設定条件によってフロー検出順序が決まります。設定条件ごとのフロー検出順序を次に示します。

(1) アクセスリスト内での順序

アクセスリストに複数のフィルタエントリを設定した場合，フィルタエントリのシーケンス番号の昇順でフレームを検出します。

(2) 同一インタフェース内での順序

同一インタフェースに複数のアクセスリストを設定した場合，次の順序でフレームを検出します。

1. MAC アクセスリスト，IPv4 アクセスリスト，または IPv6 アクセスリスト
2. Advance アクセスリスト

例えば，MAC アクセスリストでフロー検出したフレームは，Advance アクセスリストではフロー検出されません。また，統計情報もカウントされません。

(3)　複数のインタフェースでの順序

イーサネットインタフェースと，該当するイーサネットインタフェースのイーサネットサブインタフェース，ポートチャネルサブインタフェース，または VLAN インタフェースにアクセスリストを設定した場合，次の順序でフレームを検出します。

1. イーサネットインタフェース
2. イーサネットサブインタフェース，ポートチャネルサブインタフェース，または VLAN インタフェース

10.1.6　暗黙の廃棄

フィルタを設定したインタフェースでは，フロー検出条件に一致しないフレームは廃棄できます。これを暗黙の廃棄と呼びます。

暗黙の廃棄エントリは，デフォルトではアクセスリスト単位で自動生成されます。ただし，コンフィグレーションで暗黙の廃棄エントリの自動生成抑止を設定すると，暗黙の廃棄エントリは生成されません。暗黙の廃棄エントリが生成されない場合，フロー検出条件に一致しないフレームは中継されます。

暗黙の廃棄エントリがあるアクセスリストでは，フロー検出順序が先のアクセスリストで検出されるフレームは，フィルタエントリまたは暗黙の廃棄エントリのどちらかに必ず一致します。このため，フロー検出順序が後ろになるアクセスリストではフロー検出されません。

アクセスリストを一つも設定しない場合は，すべてのフレームを中継します。

(1)　同一インタフェース内での順序

同一インタフェースでのフロー検出順序を次に示します。

1. MAC アクセスリスト，IPv4 アクセスリスト，または IPv6 アクセスリスト
2. Advance アクセスリスト

暗黙の廃棄エントリがある MAC アクセスリストと Advance アクセスリストを同一インタフェースに設定した場合，MAC アクセスリストで検出されるフレームはフィルタエントリまたは暗黙の廃棄エントリのどちらかに必ず一致します。このため，Advance アクセスリストではフロー検出されません。

(2)　複数のインタフェースでの順序

複数のインタフェースでのフロー検出順序を次に示します。

1. イーサネットインタフェース
2. イーサネットサブインタフェース，ポートチャネルサブインタフェース，または VLAN インタフェース

イーサネットインタフェースと，該当するイーサネットインタフェースのイーサネットサブインタフェースに暗黙の廃棄エントリがあるアクセスリストを設定した場合，イーサネットインタフェースに設定したアクセスリストで検出されるフレームはフィルタエントリまたは暗黙の廃棄エントリのどちらかに必ず一致します。このため，イーサネットサブインタフェースに設定したアクセスリストではフロー検出されません。

10.1.7 フィルタ使用時の注意事項

(1) ESP 拡張ヘッダのある IPv6 パケットに対するフィルタ

拡張ヘッダである ESP ヘッダのある IPv6 パケットをフロー検出する場合は，フロー検出条件に次の条件を指定してください。

- コンフィグレーション
- MAC ヘッダ
- VLAN Tag ヘッダ
- IPv6 ヘッダ
- 中継種別

上位プロトコルおよび TCP/UDP/ICMP ヘッダをフロー検出条件に指定しても，フロー検出しません。

(2) オプションヘッダのある IPv4 パケットに対するフィルタ

Advance 条件でレイヤ 2 中継かつオプションヘッダのある IPv4 パケットをフロー検出する場合は，フロー検出条件に次の条件を指定してください。

- コンフィグレーション
- MAC ヘッダ
- VLAN Tag ヘッダ
- IPv4 ヘッダ
- 中継種別

TCP/UDP/ICMP/IGMP ヘッダをフロー検出条件に指定しても，フロー検出しません。

(3) 拡張ヘッダのある IPv6 パケットに対するフィルタ

Advance 条件でレイヤ 2 中継かつ拡張ヘッダのある IPv6 パケットをフロー検出する場合は，フロー検出条件に次の条件を指定してください。

- コンフィグレーション
- MAC ヘッダ
- VLAN Tag ヘッダ
- IPv6 ヘッダ
- 中継種別

上位プロトコルおよび TCP/UDP/ICMP ヘッダをフロー検出条件に指定した場合の，フロー検出可否を次に示します。

表 10-7　受信側インタフェースでのフロー検出可否

パケット				フロー検出条件		
レイヤ 3 ヘッダ			パケット受信時のレイヤ 2 ヘッダサイズ	上位プロトコル	TCP/UDP/ICMP ヘッダ	TCP 制御フラグ
拡張ヘッダ段数	拡張ヘッダ種別	拡張ヘッダサイズ				
2 段以上	−	−	−	×	×	×
1 段	−	28byte 以上	−	○	×	×
	AH	16byte	30byte 以上	○	○	×
		20byte	26byte 以上	○	○	×
		24byte	22byte 以上	○	○	×
			30byte 以上	○	×	×
	上記以外	16byte	30byte 以上	○	○	×
		24byte	22byte 以上	○	○	×
			30byte 以上	○	×	×

（凡例）○：検出できる　×：検出できない　−：条件によらない

表 10-8　送信側インタフェースでのフロー検出可否

パケット				フロー検出条件		
レイヤ 3 ヘッダ			パケット受信時のレイヤ 2 ヘッダサイズ	上位プロトコル	TCP/UDP/ICMP ヘッダ	TCP 制御フラグ
拡張ヘッダ段数	拡張ヘッダ種別	拡張ヘッダサイズ				
2 段以上	−	−	−	×	×	×
1 段	−	28byte 以上	−	○	×	×
	AH	12byte	30byte 以上	○	○	×
		16byte	26byte 以上	○	○	×
		20byte	22byte 以上	○	○	×
			30byte 以上	○	×	×
		24byte	18byte 以上	○	○	×
			26byte 以上	○	×	×
	上記以外	16byte	26byte 以上	○	○	×
		24byte 以上	18byte 以上	○	○	×
			26byte 以上	○	×	×

（凡例）○：検出できる　×：検出できない　−：条件によらない

(4) 拡張ヘッダが 2 段以上ある IPv6 パケットに対するフィルタ

レイヤ 2 中継かつ拡張ヘッダが 2 段以上ある IPv6 パケットをフロー検出する場合は，フラグメント条件（FO および MF）以外の条件を指定してください。

(5) フラグメントパケットに対するフィルタ

フラグメントパケットの 2 番目以降のパケットは TCP/UDP/ICMP/IGMP ヘッダがパケット内にありません。フラグメントパケットを受信した際のフィルタを次の表に示します。

表 10-9 フラグメントパケットとフィルタの関係

フロー検出条件	フロー検出条件とパケットの一致/不一致	動作	先頭パケット	2 番目以降のパケット
IP ヘッダだけ	IP ヘッダ一致	中継	中継	中継
		廃棄	廃棄	廃棄
	IP ヘッダ不一致	中継	次のエントリを検索	次のエントリを検索
		廃棄	次のエントリを検索	次のエントリを検索
IP ヘッダ＋ TCP/UDP/ICMP/ IGMP ヘッダ	IP ヘッダ一致，TCP/UDP/ICMP/ IGMP ヘッダ一致	中継	中継	－
		廃棄	廃棄	－
	IP ヘッダ一致，TCP/UDP/ICMP/ IGMP ヘッダ不一致	中継	次のエントリを検索	次のエントリを検索
		廃棄	次のエントリを検索	次のエントリを検索
	IP ヘッダ不一致，TCP/UDP/ICMP/ IGMP ヘッダ不一致	中継	次のエントリを検索	次のエントリを検索
		廃棄	次のエントリを検索	次のエントリを検索

（凡例）

－：TCP/UDP/ICMP/IGMP ヘッダがパケットにないため，常に TCP/UDP/ICMP/IGMP ヘッダ不一致として扱うので該当しない

(6) フィルタで検出しないフレーム

本装置では，受信側に設定したフィルタで次に示すフレームをフロー検出しません。

- uRPF によって廃棄したフレーム

また，送信側に設定したフィルタで次に示すフレームをフロー検出しません。

- ポートミラーリングでコピーしたフレーム

(7) 自発パケットに対するフィルタ

特定自発パケットを送信側でフロー検出する場合は，検出できるアクセスリスト種別や中継種別で設定してください。

対象となる特定自発 IPv4 パケットを次に示します。

- 宛先 IP アドレスがブロードキャストアドレスのパケット

- 宛先 IP アドレスがマルチキャストアドレスのパケット
- 次のプロトコル制御パケット
  - DHCP/BOOTP クライアント宛てのメッセージ
  - スタティック経路のポーリングによる ICMP パケット
  - 直結経路との BGP4 メッセージ

対象となる特定自発 IPv6 パケットを次に示します。

- 宛先 IP アドレスがリンクローカルアドレスのパケット
- 宛先 IP アドレスがマルチキャストアドレスのパケット
- 次のプロトコル制御パケット
  - スタティック経路のポーリングによる ICMPv6 パケット
  - 直結経路との BGP4+メッセージ

これらの特定自発パケットに対するフロー検出可否を次の表に示します。

表 10-10　特定自発パケットのフロー検出可否

フロー検出モード	アクセスリスト種別	検出条件の中継種別	検出可否
エントリ数重視モード	MAC アクセスリスト	－	×
	IPv4 アクセスリスト	－	○
	IPv6 アクセスリスト	－	○
検出条件数重視モード	MAC アクセスリスト	－	○
	IPv4 アクセスリスト	－	×
	IPv6 アクセスリスト	－	×
	Advance アクセスリスト	指定なし	○
		レイヤ 2 中継	○
		レイヤ 3 中継	×

（凡例）　○：検出できる　×：検出できない　－：指定できない

(8)　IP マルチキャストパケットおよび IP ブロードキャストパケットに対するフィルタ

IP マルチキャストパケットおよび IP ブロードキャストパケットには，レイヤ 2 中継とレイヤ 3 中継が共に実施されます。IP マルチキャストパケットおよび IP ブロードキャストパケットをフロー検出する場合は，該当するインタフェースに対して次のどちらかの方法を適用してください。

- 次に示す 2 種類のフィルタエントリを同時に指定する
  - IPv4 条件または IPv6 条件のフィルタエントリ
  - MAC 条件のフィルタエントリ
- Advance 条件で，中継種別を指定しないフィルタエントリを指定する
  この場合，統計情報は 2 回カウントされます。

(9) フィルタエントリ削除時の動作

次に示すコンフィグレーションの変更でフィルタエントリを削除した場合，一時的に暗黙の廃棄エントリによってフレームが廃棄されます。

- アクセスグループコマンドで 1 エントリ以上を設定したアクセスリストを，インタフェースから削除する場合
- アクセスグループコマンドでインタフェースに適用済みのアクセスリストから，最後のフィルタエントリを削除する場合

(10) フィルタエントリ変更時の動作

本装置では，インタフェースに適用済みのフィルタエントリを変更すると，変更が反映されるまでの間，検出の対象となるフレームをほかのフィルタエントリまたは暗黙の廃棄エントリで検出します。

また，変更後のフィルタエントリが複数のエントリを使用するフロー検出条件の場合，すべてのフィルタエントリを装置に反映してから統計情報の採取を開始します。

(11) 自宛パケットを廃棄するフィルタの設定

次に示す条件を満たす場合は，ポリシーベースルーティングを動作に指定しているフィルタエントリのシーケンス番号よりも小さい番号に，自宛パケットを廃棄するフィルタエントリを設定してください。

- 自宛パケットを廃棄するフィルタを設定するインタフェースに，ポリシーベースルーティングを動作に指定しているフィルタを設定している場合
- 廃棄したい自宛パケットのフロー検出条件が，ポリシーベースルーティングを動作に指定しているフィルタのフロー検出条件に含まれる場合

10.2　コンフィグレーション

10.2.1　コンフィグレーションコマンド一覧

フィル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 10-11　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	インタフェースに対して Advance 条件による Advance フィルタを設定して，Advance フィルタ機能を適用します。
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。
advance access-list resequence	Advance 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。
deny	フィルタで廃棄する条件を指定します。
flow filter implicit-deny	暗黙の廃棄エントリの自動生成を抑止します。
ip access-group	インタフェースに対して IPv4 フィルタを設定して，IPv4 フィルタ機能を適用します。
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。
ip access-list resequence	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	IPv4 アドレスフィルタとして動作するアクセスリストを設定します。
ipv6 access-list	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	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。
ipv6 traffic-filter	インタフェースに対して IPv6 フィルタを設定して，IPv6 フィルタ機能を適用します。
mac access-group	インタフェースに対して MAC フィルタを設定して，MAC フィルタ機能を適用します。
mac access-list extended	MAC フィルタとして動作するアクセスリストを設定します。
mac access-list resequence	MAC 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	フィルタで中継する条件を指定します。
remark	フィルタの補足説明を指定します。
flow detection mode※	フィルタ・QoS フローのフロー検出モードを設定します。
flow max-configuration※	フィルタ・QoS フローのコンフィグレーション最大数を設定します。
flow max-entry extended※	フローエントリ数拡張機能を有効にします。
flow-table allocation※	フィルタ・QoS フローの配分パターンを設定します。

注※

「コンフィグレーションコマンドレファレンス Vol.1」「10　装置とソフトウェアの管理」を参照してください。

10.2.2 フロー検出モードの設定

フロー検出モードを検出条件数重視モードに指定する例を次に示します。

[設定のポイント]

フロー検出モードはデフォルトではエントリ数重視モードです。設定したフロー検出モードを反映させるために，すべての PSU を再起動してください。

[コマンドによる設定]

1. **(config)# flow detection mode condition-oriented**
   グローバルコンフィグレーションモードでフロー検出モードを検出条件数重視モードに設定します。

[注意事項]

- エントリ数重視モードには，すべてのインタフェースに Advance アクセスリストおよび Advance QoS フローリストが適用されていないときに変更できます。
- 検出条件数重視モードには，フィルタ・QoS フローのエントリ数が収容条件以内のときに変更できます。

10.2.3 暗黙の廃棄エントリの自動生成を抑止する設定

暗黙の廃棄エントリの自動生成を抑止する例を次に示します。

[設定のポイント]

暗黙の廃棄エントリは，デフォルトでは自動生成されます。暗黙の廃棄エントリの自動生成抑止を設定すると，暗黙の廃棄エントリを自動生成しません。暗黙の廃棄エントリの自動生成抑止は，どのインタフェースにもアクセスリストが適用されていないときに設定できます。

[コマンドによる設定]

1. **(config)# no flow filter implicit-deny**
   グローバルコンフィグレーションモードで暗黙の廃棄エントリの自動生成抑止を設定します。

10.2.4 MAC ヘッダで中継・廃棄をする設定

MAC ヘッダをフロー検出条件として，フレームの中継または廃棄を指定する例を次に示します。

[設定のポイント]

フレーム受信時に MAC ヘッダによってフロー検出をして，フィルタエントリに一致したフレームを中継または廃棄します。

[コマンドによる設定]

1. **(config)# mac access-list extended IPX_DENY**
   mac access-list（IPX_DENY）を作成します。本リストを作成すると，MAC フィルタの動作モードに移行します。
2. **(config-ext-macl)# deny any any ipx**
   イーサネットタイプが IPX のフレームを廃棄する MAC フィルタを設定します。
3. **(config-ext-macl)# permit any any**
   すべてのフレームを中継する MAC フィルタを設定します。

4. **(config-ext-macl)# exit**
   MAC 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 gigabitethernet 1/1**
   イーサネットインタフェース 1/1 のコンフィグレーションモードに移行します。
6. **(config-if)# mac access-group IPX_DENY in**
   受信側に MAC フィルタを適用します。

10.2.5　IP ヘッダ・TCP/UDP ヘッダで中継・廃棄をする設定

(1)　IPv4 アドレスをフロー検出条件とする設定

IPv4 アドレスだけをフロー検出条件として，フレームの中継または廃棄を指定する例を次に示します。

[設定のポイント]

フレーム受信時に送信元 IPv4 アドレスによってだけフロー検出をして，フィルタエントリに一致したフレームを中継します。フィルタエントリに一致しない IP パケットはすべて廃棄します。

[コマンドによる設定]

1. **(config)# ip access-list standard FLOOR_A_PERMIT**
   ip access-list（FLOOR_A_PERMIT）を作成します。本リストを作成すると，IPv4 アドレスフィルタの動作モードに移行します。
2. **(config-std-nacl)# permit 192.0.2.0 0.0.0.255**
   送信元 IP アドレス 192.0.2.0/24　ネットワークからのフレームを中継する IPv4 アドレスフィルタを設定します。
3. **(config-std-nacl)# exit**
   IPv4 アドレス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 gigabitethernet 1/1.10**
   イーサネットサブインタフェース 1/1.10 のコンフィグレーションモードに移行します。
5. **(config-subif)# ip access-group FLOOR_A_PERMIT in**
   受信側に IPv4 アドレスフィルタを適用します。

(2)　IPv4 パケットをフロー検出条件とする設定

IPv4 HTTP パケットをフロー検出条件として，フレームの中継または廃棄を指定する例を次に示します。

[設定のポイント]

フレーム受信時に IP ヘッダおよび TCP/UDP ヘッダによってフロー検出をして，フィルタエントリに一致したフレームを廃棄します。

[コマンドによる設定]

1. **(config)# ip access-list extended HTTP_DENY**
   ip access-list（HTTP_DENY）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)# deny tcp any any eq http**
   HTTP パケットを廃棄する IPv4 パケットフィルタを設定します。

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 アドレス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 port-channel 10.10**
   ポートチャネルサブインタフェース 10.10 のコンフィグレーションモードに移行します。
6. **(config-subif)# ip access-group HTTP_DENY in**
   受信側に IPv4 パケットフィルタを適用します。

(3) IPv6 パケットをフロー検出条件とする設定

IPv6 パケットをフロー検出条件として，フレームの中継または廃棄を指定する例を次に示します。

[設定のポイント]

フレーム受信時に IPv6 アドレスによってフロー検出をして，フィルタエントリに一致したフレームを中継します。フィルタエントリに一致しない IPv6 パケットはすべて廃棄します。

[コマンドによる設定]

1. **(config)# ipv6 access-list FLOOR_B_PERMIT**
   ipv6 access-list（FLOOR_B_PERMIT）を作成します。本リストを作成すると，IPv6 フィルタの動作モードに移行します。
2. **(config-ipv6-acl)# permit ipv6 2001:db8::/32 any**
   送信元 IP アドレス 2001:db8::/32 からのフレームを中継する IPv6 フィルタを設定します。
3. **(config-ipv6-acl)# exit**
   IPv6 フィルタの動作モードからグローバルコンフィグレーションモードに戻ります。
4. **(config)# interface gigabitethernet 1/1**
   イーサネットインタフェース 1/1 のコンフィグレーションモードに移行します。
5. **(config-if)# ipv6 traffic-filter FLOOR_B_PERMIT in**
   受信側に IPv6 フィルタを適用します。

10.2.6 MAC ヘッダ・IP ヘッダ・TCP/UDP ヘッダで中継・廃棄をする設定

(1) MAC ヘッダ・IPv4 ヘッダ・TCP ヘッダをフロー検出条件とする設定

MAC ヘッダ，IPv4 ヘッダ，および TCP ヘッダをフロー検出条件として，フレームの中継または廃棄を指定する例を次に示します。

[設定のポイント]

フレーム受信時に送信元 MAC アドレス，送信元 IPv4 アドレス，および TCP ヘッダによってフロー検出をして，フィルタエントリに一致したフレームを中継します。フィルタエントリに一致しないすべてのフレームを廃棄します。

[コマンドによる設定]

1. **(config)# advance access-list ADVANCE_ACL_A_PERMIT**

advance access-list（ADVANCE_ACL_A_PERMIT）を作成します。本リストを作成すると，Advance フィルタの動作モードに移行します。

2. **(config-adv-acl)# permit mac-ip host 0012.e200.0001 any tcp 192.0.2.0 0.0.0.255 any eq http**

   送信元 MAC アドレス 0012.e200.0001，送信元 IP アドレス 192.0.2.0/24 の HTTP パケットを中継する Advance フィルタを設定します。

3. **(config-adv-acl)# exit**

   Advance 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 gigabitethernet 1/1.10**

   イーサネットサブインタフェース 1/1.10 のコンフィグレーションモードに移行します。

5. **(config-subif)# advance access-group ADVANCE_ACL_A_PERMIT in**

   受信側に Advance フィルタを適用します。

(2)　MAC ヘッダ・IPv6 ヘッダ・UDP ヘッダをフロー検出条件とする設定

MAC ヘッダ，IPv6 ヘッダ，および UDP ヘッダをフロー検出条件として，フレームの中継または廃棄を指定する例を次に示します。

[設定のポイント]

フレーム受信時に送信元 MAC アドレス，送信元 IPv6 アドレス，および UDP ヘッダによってフロー検出をして，フィルタエントリに一致したフレームを中継します。フィルタエントリに一致しないすべてのフレームを廃棄します。

[コマンドによる設定]

1. **(config)# advance access-list ADVANCE_ACL_B_PERMIT**

   advance access-list（ADVANCE_ACL_B_PERMIT）を作成します。本リストを作成すると，Advance フィルタの動作モードに移行します。

2. **(config-adv-acl)# permit mac-ipv6 host 0012.e200.0001 any udp 2001:db8::/32 any eq ntp**

   送信元 MAC アドレス 0012.e200.0001，送信元 IP アドレス 2001:db8::/32 の NTP パケットを中継する Advance フィルタを設定します。

3. **(config-adv-acl)# exit**

   Advance 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 port-channel 10.10**

   ポートチャネルサブインタフェース 10.10 のコンフィグレーションモードに移行します。

5. **(config-subif)# advance access-group ADVANCE_ACL_B_PERMIT in**

   受信側に Advance フィルタを適用します。

10.2.7　複数インタフェースに対するフィルタの設定

複数のイーサネットインタフェースにフィルタを設定する例を次に示します。

[設定のポイント]

config-if-range モードで複数のイーサネットインタフェースにフィルタを設定できます。

[コマンドによる設定]

1. **(config)# ip access-list standard FLOOR_C_PERMIT**

ip access-list（FLOOR_C_PERMIT）を作成します。本リストを作成すると，IPv4 アドレスフィルタの動作モードに移行します。

2. **(config-std-nacl)# permit 192.0.2.0 0.0.0.255**

   送信元 IP アドレス 192.0.2.0/24　ネットワークからのフレームを中継する IPv4 アドレスフィルタを設定します。

3. **(config-std-nacl)# exit**

   IPv4 アドレス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 range gigabitethernet 1/1-4**

   イーサネットインタフェース 1/1-4 のコンフィグレーションモードに移行します。

5. **(config-if-range)# ip access-group FLOOR_C_PERMIT in**

   受信側に IPv4 アドレスフィルタを適用します。

10.2.8　VLAN インタフェースに対するフィルタの設定

VLAN インタフェースにフィルタを設定する例を次に示します。

[設定のポイント]

VLAN インタフェースで MAC ヘッダおよび IPv6 ヘッダによってフロー検出をして，フィルタエントリに一致したフレームを中継します。フィルタエントリに一致しないすべてのフレームを廃棄します。

[コマンドによる設定]

1. **(config)# advance access-list ADVANCE_FLOOR_V6_PERMIT**

   advance access-list（ADVANCE_FLOOR_V6_PERMIT）を作成します。本リストを作成すると，Advance フィルタの動作モードに移行します。

2. **(config-adv-acl)# permit mac-ipv6 0012.e200.1234 0000.0000.ffff any ipv6 any any**

   送信元 MAC アドレスの上位 4 バイトが 0012.e200，下位 2 バイトが任意の IPv6 パケットを中継する Advance フィルタを設定します。

3. **(config-adv-acl)# exit**

   Advance 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 10**

   VLAN インタフェース 10 のコンフィグレーションモードに移行します。

5. **(config-if)# advance access-group ADVANCE_FLOOR_V6_PERMIT in**

   受信側に Advance フィルタを適用します。

10.3　オペレーション

10.3.1　運用コマンド一覧

フィルタの運用コマンド一覧を次の表に示します。

表 10-12　運用コマンド一覧

コマンド名	説明
show access-filter	フィルタの設定内容と統計情報を表示します。
clear access-filter	フィルタの統計情報を 0 クリアします。
restart filter-qosflow※	フィルタ・QoS フロー制御プログラムを再起動します。
dump filter-qosflow※	フィルタ・QoS フロー制御プログラムで採取している制御情報をファイルへ出力します。

注※

「運用コマンドレファレンス Vol.2」「10　フィルタ・QoS 共通」を参照してください。

10.3.2　フィルタの確認

show access-filter コマンドでフィルタの動作を確認できます。インタフェースを範囲指定すると，複数インタフェースのフィルタの動作を確認できます。

(1)　イーサネットインタフェースに設定されたエントリの確認

イーサネットインタフェースにフィルタを設定した場合の動作確認を次の図に示します。

図 10-3　イーサネットインタフェースにフィルタを設定した場合の動作確認

```
> show access-filter interface gigabitethernet 1/1 IPX_DENY in
Date 20XX/01/01 12:00:00 UTC
Using interface : gigabitethernet 1/1 in
Extended MAC access-list : IPX_DENY
      10 deny any any ipx(0x8137)
                      Matched packets        Matched bytes
         Total  :             74699826           4780788864
         PSU 1  :             74699826           4780788864
      20 permit any any
                      Matched packets        Matched bytes
         Total  :               718235             45967040
         PSU 1  :               718235             45967040
      Implicit-deny
                      Matched packets        Matched bytes
         Total  :                    0                    0
         PSU 1  :                    0                    0
```

指定したイーサネットインタフェースのフィルタに「Extended MAC access-list」が表示されることを確認します。フロー検出条件に一致したフレームは Matched packets および Matched bytes で確認します。また，暗黙の廃棄に一致したフレームは Implicit-deny の Matched packets および Matched bytes で確認します。

(2)　ポートチャネルサブインタフェースに設定されたエントリの確認

ポートチャネルサブインタフェースにフィルタを設定した場合の動作確認を次の図に示します。

図 10-4 ポートチャネルサブインタフェースにフィルタを設定した場合の動作確認

```
> show access-filter interface port-channel 10.10 HTTP_DENY in
Date 20XX/01/01 12:00:00 UTC
Using interface : port-channel 10.10 in
Extended IP access-list : HTTP_DENY
      10 deny tcp(6) any any eq http(80)
                        Matched packets        Matched bytes
         Total  :              1052789            161801506
         PSU 1  :               894321            151659506
         PSU 3  :               158468             10142000
      20 permit ip any any
                        Matched packets        Matched bytes
         Total  :            100535750          15476889608
         PSU 1  :             74699826          11653172856
         PSU 3  :             25835924           3823716752
      Implicit-deny
                        Matched packets        Matched bytes
         Total  :                    0                    0
         PSU 1  :                    0                    0
         PSU 3  :                    0                    0
```

指定したポートチャネルサブインタフェースのフィルタに「Extended IP access-list」が表示されることを確認します。フロー検出条件に一致したフレームは Matched packets および Matched bytes で確認します。また，暗黙の廃棄に一致したフレームは Implicit-deny の Matched packets および Matched bytes で確認します。

(3) VLAN インタフェースに設定されたエントリの確認

VLAN インタフェースにフィルタを設定した場合の動作確認を次の図に示します。

図 10-5 VLAN インタフェースにフィルタを設定した場合の動作確認

```
> show access-filter interface vlan 10 ADVANCE_FLOOR_V6_PERMIT in
Date 20XX/01/01 12:00:00 UTC
Using interface : vlan 10 in
Advance access-list : ADVANCE_FLOOR_V6_PERMIT
   remark "permit only Floor-A"
      10 permit mac-ipv6 0012.e200.1234 0000.0000.ffff any ipv6 any any
                        Matched packets        Matched bytes
         Total  :              2999899            475262518
         PSU 1  :              2682963            454978518
         PSU 3  :               316936             20284000
      Implicit-deny
                        Matched packets        Matched bytes
         Total  :                    0                    0
         PSU 1  :                    0                    0
         PSU 3  :                    0                    0
```

指定した VLAN インタフェースのフィルタに「Advance access-list」が表示されることを確認します。フロー検出条件に一致したフレームは Matched packets および Matched bytes で確認します。また，暗黙の廃棄に一致したフレームは Implicit-deny の Matched packets および Matched bytes で確認します。

11 アクセスリストロギング

この章では，アクセスリストロギングの解説と操作方法について説明します。

11.1　解説

11.1.1　概要

アクセスリストロギングは，フィルタで検出したパケットの情報とその統計情報を収集して，システムメッセージで運用端末に表示したり，syslog サーバに送信したりする機能です。これによって，不正アクセスや不正パケットを監視したり，フィルタの設定誤りによる意図しないパケットの廃棄を確認したりできます。

アクセスリストロギングを動作に指定できるアクセスリストを次の表に示します。

表 11-1　アクセスリストロギングの対象アクセスリスト

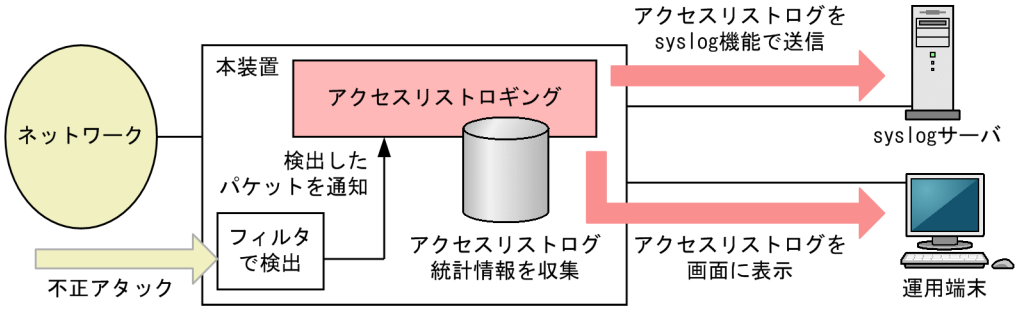
アクセスリスト種別	フィルタアクション	
	通過	廃棄
MAC アクセスリスト	−	○
IPv4 アクセスリスト	−	○
IPv6 アクセスリスト	−	○
Advance アクセスリスト	−	○

（凡例）　○：対象　　−：対象外

アクセスリストロギングが出力するシステムメッセージを**アクセスリストログ**と呼びます。また，アクセスリストロギングが収集するパケットの情報とその統計情報を**アクセスリストログ統計情報**と呼びます。アクセスリストロギングでは，パケット情報の内容ごとに，検出したパケット数をカウントします。

アクセスリストロギングの動作概要を次の図に示します。

図 11-1　アクセスリストロギングの動作概要



出力するアクセスリストログの例を次の図に示します。

図 11-2　出力するアクセスリストログの例

```
>
20XX/01/01 12:00:00 UTC 1-1(A) S6 ACLLOG 2d000003 00 000000000001 denied:0012.e25a.9839(4095)(E
thernet1/1) -> 0012.e25a.7840, 2 packets
20XX/01/01 12:00:00 UTC 1-1(A) S6 ACLLOG 2d000004 00 000000000001 denied:(4095)tcp 192.168.1.3(
1)(Ethernet1/1) -> 192.168.2.1(12), 1 packet
20XX/01/01 12:00:00 UTC 1-1(A) S6 ACLLOG 2d000005 00 000000000001 denied:(4095)255 fe80::39fe:9
a30:53dd:1234(1)(Ethernet1/1) -> fe80::39fe:9a30:53dd:5678(12), 1 packet
>
```

11.1.2　アクセスリストログの表示内容

アクセスリストロギングでは，フィルタで検出したパケット内のレイヤ 2，レイヤ 3，およびレイヤ 4 ヘッダを解析して，アクセスリストログに表示します。なお，アクセスリストログ統計情報もアクセスリストログと同等の表示内容となります。アクセスリストログの表示内容を次の表に示します。

表 11-2　アクセスリストログの表示内容

分類	表示項目	内容
パケット内の情報	<source mac>	送信元 MAC アドレス
	<destination mac>	宛先 MAC アドレス
	<tag vlan id>	VLAN ID※1
	<ethernet type>	イーサネットタイプ
	<protocol no.>	上位プロトコル番号
	<next header>	次ヘッダ番号
	<source ip address>	送信元 IPv4/IPv6 アドレス
	<destination ip address>	宛先 IPv4/IPv6 アドレス
	<source port>	送信元ポート番号※2
	<destination port>	宛先ポート番号※2
付与情報	<received interface>	表示パケットの受信インタフェース※3
パケット数	<packets>	出力したアクセスリストログのうち，次の内容が同じフローのパケット数 • パケット内の情報 • 付与情報

注※1

検出したフレームの本装置受信時の 1 段目の VLAN ID だけを表示します。Tag 変換や VLAN トンネリングを設定したインタフェースの場合は，各処理を適用する前の VLAN ID を表示します。

注※2

上位プロトコルが TCP と UDP の場合だけ表示します。

注※3

受信インタフェースにはイーサネットインタフェースを表示します。なお，フィルタで検出したパケットの中継種別およびフィルタの適用方向（Inbound または Outbound）によって，表示内容が異なります。受信インタフェースの表示内容を次の表に示します。

表 11-3　受信インタフェースの表示内容

中継種別	Inbound フィルタで検出	Outbound フィルタで検出
中継	○	○
自宛	○	－
自発	－	－

（凡例）　○：表示する　－：表示しない

フィルタで検出したパケット種別および VLAN Tag の段数によって，表示するアクセスリストログの内容が異なります。アクセスリストログで表示する内容を，VLAN Tag の段数別に示します。

(1)　VLAN Tag なしの場合

VLAN Tag なしの場合にアクセスリストログで表示する内容を，パケット種別ごとに次に示します。

表 11-4　アクセスリストログの表示内容（非 IP パケット）

表示項目	表示可否
<source mac>	○
<destination mac>	○
<tag vlan id>	－
<ethernet type>	○
<protocol no.>	－
<next header>	－
<source ip address>	－
<destination ip address>	－
<source port>	－
<destination port>	－
<received interface>	○
<packets>	○

（凡例）　○：表示する　－：表示しない

表 11-5　アクセスリストログの表示内容（IPv4 パケット）

表示項目	IP オプションなし		IP オプションあり
	レイヤ 4 が TCP, UDP	レイヤ 4 なし，またはレイヤ 4 が TCP，UDP 以外	
<source mac>	－	－	－
<destination mac>	－	－	－
<tag vlan id>	－	－	－
<ethernet type>	－	－	－
<protocol no.>	○	○	○
<next header>	－	－	－
<source ip address>	○	○	○
<destination ip address>	○	○	○
<source port>	○※	－	－

表示項目	IP オプションなし		IP オプションあり
	レイヤ 4 が TCP, UDP	レイヤ 4 なし，またはレイヤ 4 が TCP，UDP 以外	
<destination port>	○※	−	−
<received interface>	○	○	○
<packets>	○	○	○

（凡例）　○：表示する　−：表示しない

注※

フラグメントされていないパケットの場合に表示します。本装置でフラグメントする場合は，フラグメントする前のパケットの内容を表示します。

フラグメントされたパケットの場合は表示しません。

表 11-6　アクセスリストログの表示内容（IPv6 パケット）

表示項目	IPv6 拡張ヘッダなし		IPv6 拡張ヘッダあり
	レイヤ 4 が TCP，UDP	レイヤ 4 なし，またはレイヤ 4 が TCP，UDP 以外	
<source mac>	−	−	−
<destination mac>	−	−	−
<tag vlan id>	−	−	−
<ethernet type>	−	−	−
<protocol no.>	−	−	−
<next header>	○	○	○
<source ip address>	○	○	○
<destination ip address>	○	○	○
<source port>	○	−	−
<destination port>	○	−	−
<received interface>	○	○	○
<packets>	○	○	○

（凡例）　○：表示する　−：表示しない

(2)　VLAN Tag が 1 段または 2 段の場合

VLAN Tag が 1 段または 2 段の場合にアクセスリストログで表示する内容を，パケット種別ごとに次に示します。

表 11-7　アクセスリストログの表示内容（非 IP パケット）

表示項目	表示可否
<source mac>	○

表示項目	表示可否
<destination mac>	○
<tag vlan id>	○
<ethernet type>	○
<protocol no.>	－
<next header>	－
<source ip address>	－
<destination ip address>	－
<source port>	－
<destination port>	－
<received interface>	○
<packets>	○

（凡例）　○：表示する　－：表示しない

表 11-8　アクセスリストログの表示内容（IPv4 パケット）

表示項目	IP オプションなし		IP オプションあり
	レイヤ 4 が TCP, UDP	レイヤ 4 なし，またはレイヤ 4 が TCP，UDP 以外	
<source mac>	－	－	－
<destination mac>	－	－	－
<tag vlan id>	○	○	○
<ethernet type>	－	－	－
<protocol no.>	○	○	○
<next header>	－	－	－
<source ip address>	○	○	○
<destination ip address>	○	○	○
<source port>	○※	－	－
<destination port>	○※	－	－
<received interface>	○	○	○
<packets>	○	○	○

（凡例）　○：表示する　－：表示しない

注※

フラグメントされていないパケットの場合に表示します。本装置でフラグメントする場合は，フラグメントする前のパケットの内容を表示します。

フラグメントされたパケットの場合は表示しません。

表 11-9　アクセスリストログの表示内容（IPv6 パケット）

表示項目	IPv6 拡張ヘッダなし		IPv6 拡張ヘッダあり
	レイヤ 4 が TCP，UDP	レイヤ 4 なし，またはレイヤ 4 が TCP，UDP 以外	
<source mac>	−	−	−
<destination mac>	−	−	−
<tag vlan id>	○	○	○
<ethernet type>	−	−	−
<protocol no.>	−	−	−
<next header>	○	○	○
<source ip address>	○	○	○
<destination ip address>	○	○	○
<source port>	○	−	−
<destination port>	○	−	−
<received interface>	○	○	○
<packets>	○	○	○

（凡例）　○：表示する　−：表示しない

(3)　VLAN Tag が 3 段以上の場合

VLAN Tag が 3 段以上の場合にアクセスリストログで表示する内容を次の表に示します。なお，パケット種別による表示項目や表示可否の差はありません。

表 11-10　アクセスリストログの表示内容

表示項目	表示可否
<source mac>	○
<destination mac>	○
<tag vlan id>	○
<ethernet type>	−
<protocol no.>	−
<next header>	−
<source ip address>	−
<destination ip address>	−
<source port>	−
<destination port>	−
<received interface>	○

表示項目	表示可否
<packets>	○

（凡例）　○：表示する　－：表示しない

11.1.3　アクセスリストログを出力する契機

アクセスリストログを出力する契機は次のとおりです。

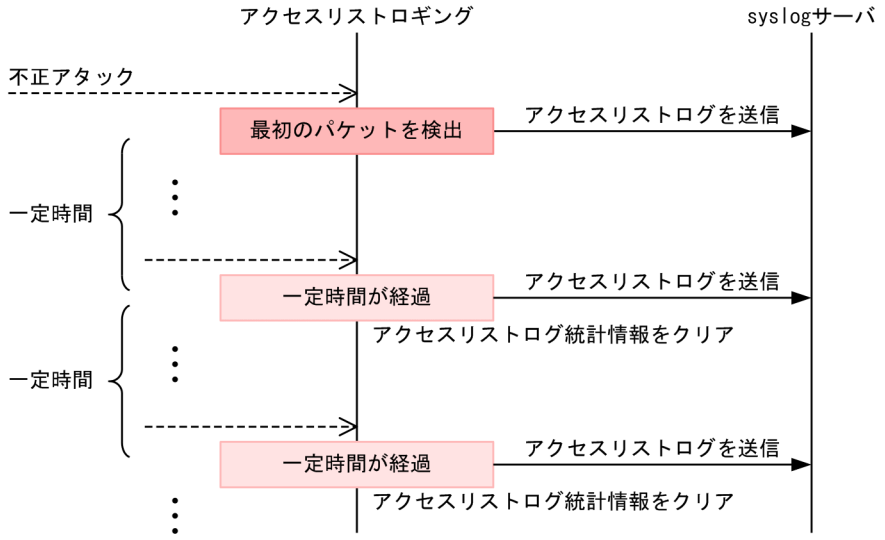
- フィルタで最初のパケットを検出したとき
- パケットを検出してから一定時間が経過したとき（ログ出力インターバル契機）
- 一定数のパケットを検出したとき（スレッシュホールド契機）

(1)　ログ出力インターバル契機での出力

指定した時間間隔（インターバル）で，アクセスリストログを出力します。時間間隔は，コンフィグレーションコマンド access-log interval で設定します。

フィルタで最初のパケットを検出してアクセスリストログを出力してから，時間を計り始めます。指定した時間が経過するまでの間は，複数のパケットを検出してもアクセスリストログを出力しません。指定した時間が経過すると，その間にフィルタで検出したパケット数も合わせてアクセスリストログを出力して，アクセスリストログ統計情報をクリアします。このように，一定時間間隔で監視ができます。ログ出力インターバル契機の動作を次の図に示します。

図 11-3　ログ出力インターバル契機の動作

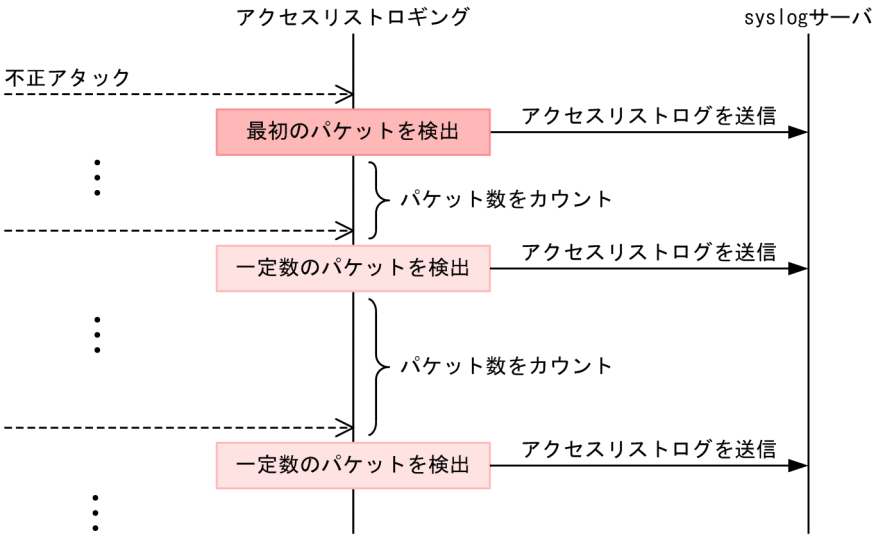


なお，アクセスリストロギングの動作中に，出力する時間間隔を変更した場合は，いったんアクセスリストログ統計情報をすべてクリアして，再度監視を開始します。

(2)　スレッシュホールド契機での出力

アクセスリストログで表示するパケット内の情報および付与情報が同じパケットの検出数が，指定したスレッシュホールド（パケット数）の N 倍に一致したときに，アクセスリストログを出力します。スレッシュホールドは，コンフィグレーションコマンド access-log threshold で設定します。このように，フィルタで検出したパケット数による監視ができます。スレッシュホールド契機の動作を次の図に示します。

図 11-4　スレッシュホールド契機の動作



なお，アクセスリストロギングの動作中に，スレッシュホールドを変更した場合は，直前に出力したアクセスリストログを基点として，変更後のスレッシュホールドの N 倍に一致したときかつ現時点以降に，アクセスリストログを出力します。

11.1.4　アクセスリストロギングの注意事項

- 暗黙の廃棄で検出したパケットは，アクセスリストロギングの対象としません。
- アクセスリストロギングの収容数を超えた場合は，アクセスリストログ統計情報を新たに登録しません。そのため，アクセスリストログを出力しません。
- 系切替後，および運用コマンド restart flow-log-control の実行後は，それまで収集していたアクセスリストログ統計情報をクリアします。
- アクセスリストログの出力を抑止する場合は，コンフィグレーションコマンド message-type でメッセージ種別 ACLLOG の出力抑止を設定してください。
- フィルタで検出したパケットの CPU への通知速度は 1000pps 固定です。1000pps を超えて通知されるアクセスリストログ統計情報は登録されません。

11.2　コンフィグレーション

11.2.1　コンフィグレーションコマンド一覧

アクセスリストロギ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 11-11　コンフィグレーションコマンド一覧

コマンド名	説明
access-log enable	アクセスリストロギングを有効にします。
access-log interval	アクセスリストログの出力の契機とする時間間隔を指定します。
access-log threshold	アクセスリストログの出力の契機とするスレッシュホールドを指定します。

11.2.2　アクセスリストロギングの設定

アクセスリストロギングを設定する例を次に示します。

[設定のポイント]

指定したアクセスリストで検出したパケットを，アクセスリストロギングの対象にします。

[コマンドによる設定]

1. **(config)# ip access-list extended ACLLOG_DENY**
   (config-ext-nacl)# 10 deny ip any any action log
   (config-ext-nacl)# exit
   ip access-list（ACLLOG_DENY）を作成して，IPv4 パケットをアクセスリストロギングの対象に設定します。
2. **(config)# interface gigabitethernet 1/1**
   (config-if)# ip access-group ACLLOG_DENY in
   (config-if)# exit
   イーサネットインタフェース 1/1 の受信側に IPv4 フィルタ（ACLLOG_DENY）を適用します。
3. **(config)# access-log enable**
   アクセスリストロギングの動作を開始します。

11.2.3　アクセスリストログを syslog サーバへ送信する設定

アクセスリストログを syslog サーバへ送信する設定例を次に示します。

[設定のポイント]

アクセスリストロギングの対象フィルタで検出されたパケット情報を，syslog サーバへ送信します。

[コマンドによる設定]

1. **(config)# logging syslog-host 192.0.2.1**
   送信先の syslog サーバとして IPv4 アドレス 192.0.2.1 を指定します。
2. **(config)# ip access-list extended ACLLOG_DENY**
   (config-ext-nacl)# 10 deny ip any any action log

(config-ext-nacl)# exit

ip access-list（ACLLOG_DENY）を作成して，IPv4 パケットをアクセスリストロギングの対象に設定します。

3. **(config)# interface gigabitethernet 1/1**
   (config-if)# ip access-group ACLLOG_DENY in
   (config-if)# exit
   イーサネットインタフェース 1/1 の受信側に IPv4 フィルタ（ACLLOG_DENY）を適用します。
4. **(config)# access-log threshold 100**
   スレッシュホールドに 100 を設定します。
5. **(config)# access-log enable**
   アクセスリストロギングの動作を開始します。

11.2.4　アクセスリストログ統計情報を長期間保持する設定

アクセスリストログ統計情報を長期間保持する設定例を次に示します。

[設定のポイント]

ログ出力インターバルを契機としたアクセスリストログの出力をしないように設定します。

[コマンドによる設定]

1. **(config)# ipv6 access-list ACLLOG_DENY**
   (config-ipv6-acl)# 10 deny ipv6 any any action log
   (config-ipv6-acl)# exit
   ipv6 access-list（ACLLOG_DENY）を作成して，IPv6 パケットをアクセスリストロギングの対象に設定します。
2. **(config)# interface gigabitethernet 1/1**
   (config-if)# ipv6 traffic-filter ACLLOG_DENY
   (config-if)# exit
   イーサネットインタフェース 1/1 の受信側に IPv6 フィルタ（ACLLOG_DENY）を適用します。
3. **(config)# access-log interval unlimit**
   ログ出力インターバルを契機としたアクセスリストログの出力をしないように設定します。
4. **(config)# access-log enable**
   アクセスリストロギングの動作を開始します。

11.3　オペレーション

11.3.1　運用コマンド一覧

アクセスリストロギングの運用コマンド一覧を次の表に示します。

表 11-12　運用コマンド一覧

コマンド名	説明
show access-log	アクセスリストロギングの情報を表示します。
clear access-log	アクセスリストログ情報テーブルに空きがなく廃棄したパケット数をクリアします。
show access-log flow	アクセスリストログ統計情報を表示します。
clear access-log flow	アクセスリストログ統計情報をクリアします。

11.3.2　アクセスリストロギングの情報の確認

アクセスリストロギングの情報は，show access-log コマンドで表示します。アクセスリストログの設定状態やアクセスリストログ統計情報数などが確認できます。

図 11-5　アクセスリストロギングの情報の確認

```
> show access-log
Date 20XX/01/01 12:00:00 UTC
Access list logging Information:
  interval(minutes)  :                    5       <-1
  threshold(packets) :                    -       <-1
Access list logging Logged:
  Max                :                10000       <-2
  Used               :                 1001       <-2
    NonIP            :                  950
    IPv4             :                    0
    IPv6             :                   51
Access list logging Statistics:
  flow table full    :               17295
>
```

1. アクセスリストロギングが設定したとおりであることを確認します。
2. アクセスリストログ統計情報数が最大収容数を超えていないことを確認します。

11.3.3　アクセスリストログ統計情報の確認

アクセスリストロギングで保持しているアクセスリストログ統計情報は，show access-log flow コマンドで表示します。検出したパケットの情報と検出したパケット数を確認できます。

図 11-6　アクセスリストログ統計情報の確認

```
> show access-log flow
Date 20XX/01/01 12:00:00 UTC
denied:0012.e25a.9839(4095)(Ethernet1/1) -> 0012.e25a.7840, 2 packets
denied:(4095)tcp 192.168.1.3(1)(Ethernet1/1) -> 192.168.2.1(12), 1 packet
denied:(4095)255 fe80::39fe:9a30:53dd:1234(1)(Ethernet1/1) -> fe80::39fe:9a30:53dd:5678(12), 1
packet
>
```

12 QoS の概要

QoS は，ポリサー・マーカー・優先度変更・帯域制御によって通信品質を制御し, 回線の帯域やキューのバッファ容量などの限られたネットワーク資源を有効に利用するための機能です。この章では，本装置の QoS 制御について説明します。

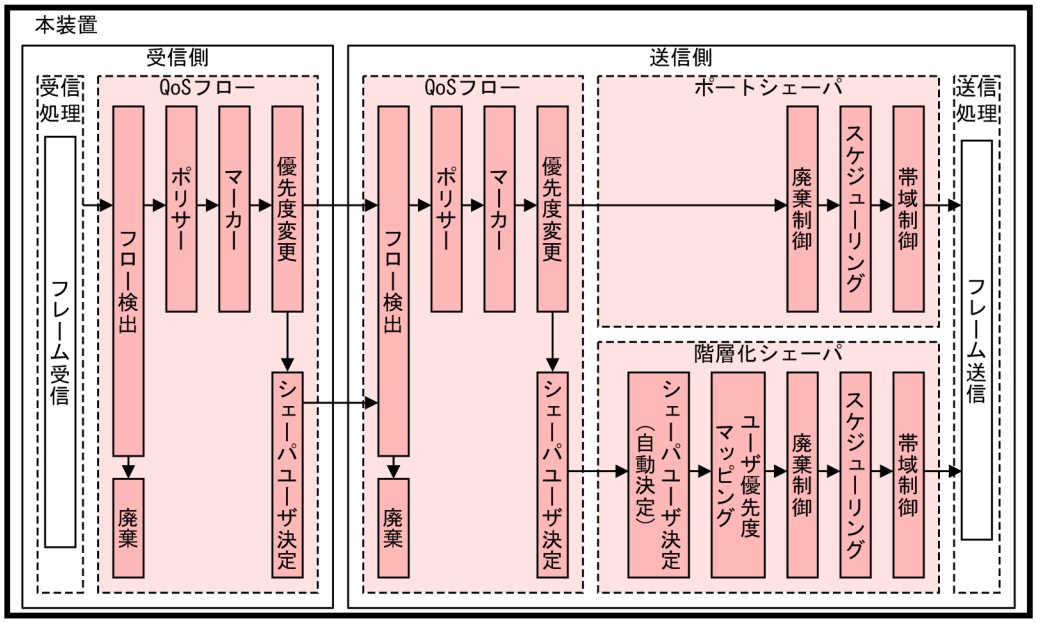
12.1　QoS 制御構造

ネットワークを利用したサービスの多様化に伴って，通信品質を保証しないベストエフォート型のトラフィックに加え，実時間型・帯域保証型のトラフィックが増加しています。本装置の QoS 制御を使用することによって，トラフィック種別に応じた通信品質を提供できます。

本装置の QoS 制御は，回線の帯域やキューのバッファ容量などの限られたネットワーク資源を有効に使用できます。アプリケーションごとに要求されるさまざまな通信品質を満たすために，QoS 制御を使用してネットワーク資源を適切に分配します。

本装置の QoS 制御の機能ブロックを次の図に示します。

図 12-1　本装置の QoS 制御の機能ブロック



（凡例）：ここで説明するブロック

図に示した QoS 制御の各機能ブロックの概要を次の表に示します。

表 12-1　QoS 制御の各機能ブロックの概要

機能部位		機能概要
QoS フロー	フロー検出	MAC ヘッダやプロトコル種別，IP アドレス，ポート番号などの条件に一致するフローを検出します。
	ポリサー	フローごとに帯域を監視して，帯域を超えたフローに対してペナルティを与えます。
	マーカー	VLAN Tag ヘッダのユーザ優先度や IP ヘッダの DSCP を書き換えます。
	優先度変更	フローに対して優先クラスや，廃棄されやすさを示す廃棄クラスを変更します。
	廃棄	フロー検出したフローを廃棄します。
	シェーパユーザ決定	フローごとに階層化シェーパユーザを決定します。

機能部位		機能概要
ポートシェーパ	廃棄制御	フレームの優先度とキューの状態に応じて，該当フレームをキューイングするか廃棄するかを制御します。
	スケジューリング	各キューからのフレームの出力順序を制御します。
	帯域制御	各ポートの出力帯域を制御します。
階層化シェーパ【OP-SHPS】	シェーパユーザ決定（自動決定）	ランダム振り分けや VLAN ID マッピングによって，シェーパユーザを自動で決定します。
	ユーザ優先度マッピング	ユーザ優先度によってキュー番号を決定します。
	廃棄制御	フレームの優先度とキューの状態に応じて，該当フレームをキューイングするか廃棄するかを制御します。
	スケジューリング	各キューからのフレームの出力順序を制御します。
	帯域制御	各ポートの出力帯域を制御します。さらに，シェーパユーザごとに出力帯域を制御します。

QoS フローでは，フロー検出したフローに対してポリサー，マーカー，優先度変更，シェーパユーザ決定，または廃棄を実施します。

ポートシェーパでは，フレームの優先度に基づいて廃棄制御，スケジューリングおよび送信時の帯域制御を実施します。

階層化シェーパでは，上記の動作に加えて，シェーパユーザ決定，およびユーザ優先度マッピングを実施します。【OP-SHPS】

13 QoS フロー

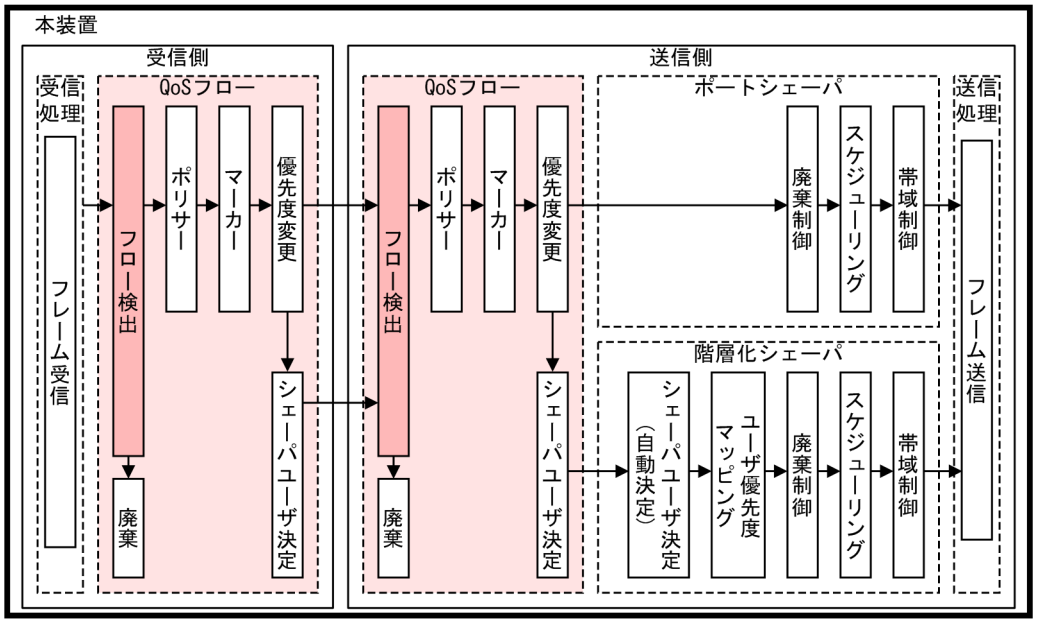
QoS フローは，フロー検出したフレームに対してポリサー，マーカー，優先度変更，または廃棄をする機能です。この章では，QoS フローでのフロー検出の解説と操作方法について説明します。

13.1　解説

13.1.1　概要

QoS フローは，受信フレームや送信フレームのうち特定のフレームに対してポリサー，マーカー，優先度変更，または廃棄をする機能です。本装置の QoS フローの機能ブロックとフロー検出の位置づけを次の図に示します。

図 13-1　本装置の QoS フローの機能ブロックとフロー検出の位置づけ



（凡例）　：ここで説明するブロック

13.1.2　フロー検出

フロー検出とは，フレームの一連の流れであるフローを MAC ヘッダ，IP ヘッダ，TCP ヘッダなどの条件に基づいてフレームを検出する機能です。QoS フローリストで設定します。QoS フローリストの詳細は，「13.1.5　QoS フローリスト」を参照してください。

本装置の各インタフェースに対するフロー検出および QoS フローリストの設定可否を次の表に示します。

表 13-1　インタフェースに対するフロー検出および QoS フローリストの設定可否

インタフェース	フロー検出	QoS フローリストの設定
イーサネットインタフェース	○	○
イーサネットサブインタフェース	○	○
ポートチャネルインタフェース	○※	－
ポートチャネルサブインタフェース	○	○
VLAN インタフェース	○	○
ループバックインタフェース	－	－

インタフェース	フロー検出	QoS フローリストの設定
Null インタフェース	－	－
マネージメントポート	－	－
AUX ポート	－	－

（凡例）　○：検出または設定できる　－：検出または設定できない

注※

チャネルグループを構成するイーサネットインタフェースに QoS フローリストを設定すると，フロー検出ができます。

13.1.3　フロー検出モード

本装置では，フロー検出動作を決めるモードとしてフロー検出モードを用意しています。フロー検出モードごとの特徴を次に示します。

エントリ数重視モード

エントリ数が多くなりますが，検出条件が次のように限定されます。

- 非 IP パケットおよびレイヤ 2 中継する IP パケットを，MAC ヘッダでフロー検出します。
- レイヤ 3 中継する IP パケットを，IP ヘッダとレイヤ 4 ヘッダの組み合わせでフロー検出します。

検出条件数重視モード

エントリ数は少なくなりますが，エントリ当たりの検出条件数が多いためきめ細かい検出ができます。非 IP パケット，IP パケットのすべてをフロー検出の対象として，MAC ヘッダ，IP ヘッダ，およびレイヤ 4 ヘッダを組み合わせた Advance 条件でフロー検出します。

フロー検出モードはコンフィグレーションコマンド flow detection mode で設定します。デフォルトでは，エントリ数重視モードです。フロー検出モードとフロー検出動作については，「13.1.5　QoS フローリスト」を参照してください。

13.1.4　フロー検出条件

フロー検出するためには，コンフィグレーションでフローを識別するための条件を指定します。フロー検出条件は MAC 条件，IPv4 条件，IPv6 条件，および Advance 条件に分類されます。フロー検出条件と検出できるヘッダ種別の対応を次の表に示します。

表 13-2　フロー検出条件と検出できるヘッダ種別の対応

フロー検出条件	MAC ヘッダ	VLAN Tag ヘッダ	IPv4 ヘッダ	IPv6 ヘッダ	レイヤ 4 ヘッダ
MAC 条件	○	○	－	－	－
IPv4 条件	－	○	○	－	○
IPv6 条件	－	○	－	○	○
Advance 条件	○	○	○	○	○

（凡例）　○：検出できる　－：検出できない

指定できるフロー検出条件の詳細項目を次の表に示します。

表 13-3 指定できるフロー検出条件の詳細項目

種別		設定項目	
MAC 条件	コンフィグレーション	インタフェース※1	
	MAC ヘッダ	送信元 MAC アドレス	
		宛先 MAC アドレス	
		イーサネットタイプ	
	VLAN Tag ヘッダ※2	Tag の VLAN ID	
		ユーザ優先度	
		Tag なし	
	2 段目の VLAN Tag ヘッダ※3	Tag の VLAN ID	
		ユーザ優先度	
		Tag なし	
IPv4 条件	コンフィグレーション	インタフェース※1	
	VLAN Tag ヘッダ※2	ユーザ優先度	
		Tag なし	
	IPv4 ヘッダ	上位プロトコル※4	
		送信元 IP アドレス	
		宛先 IP アドレス	
		ToS※5	
		DSCP※5	
		Precedence※5	
		フラグメント※6	FO
			MF
		IP レングス	
	IPv4-TCP ヘッダ	送信元ポート番号	
		宛先ポート番号	
		TCP 制御フラグ※7	
	IPv4-UDP ヘッダ	送信元ポート番号	
		宛先ポート番号	
	IPv4-ICMP ヘッダ	ICMP タイプ	
		ICMP コード	
	IPv4-IGMP ヘッダ	IGMP タイプ	

種別		設定項目	
IPv6 条件	コンフィグレーション	インタフェース※1	
	VLAN Tag ヘッダ※2	ユーザ優先度	
		Tag なし	
	IPv6 ヘッダ	上位プロトコル※8	
		送信元 IP アドレス※9	
		宛先 IP アドレス	
		トラフィッククラス※10	
		DSCP※10	
		フラグメント※6	FO
			MF
		IP レングス	
	IPv6-TCP ヘッダ	送信元ポート番号	
		宛先ポート番号	
		TCP 制御フラグ※7	
	IPv6-UDP ヘッダ	送信元ポート番号	
		宛先ポート番号	
	IPv6-ICMP ヘッダ	ICMP タイプ	
		ICMP コード	
Advance 条件	コンフィグレーション	インタフェース※1	
	MAC ヘッダ	送信元 MAC アドレス※11	
		宛先 MAC アドレス	
		イーサネットタイプ	
	VLAN Tag ヘッダ※2	Tag の VLAN ID	
		ユーザ優先度	
		Tag なし	
	2 段目の VLAN Tag ヘッダ※3	Tag の VLAN ID	
		ユーザ優先度	
		Tag なし	
	IPv4 ヘッダ	上位プロトコル※4	
		送信元 IP アドレス	
		宛先 IP アドレス	

種別		設定項目	
		ToS※5	
		DSCP※5	
		Precedence※5	
		フラグメント※6	FO
			MF
		IP レングス	
	IPv4-TCP ヘッダ	送信元ポート番号	
		宛先ポート番号	
		TCP 制御フラグ※7	
	IPv4-UDP ヘッダ	送信元ポート番号	
		宛先ポート番号	
	IPv4-ICMP ヘッダ	ICMP タイプ	
		ICMP コード	
	IPv4-IGMP ヘッダ	IGMP タイプ	
	IPv6 ヘッダ	上位プロトコル※8	
		送信元 IP アドレス	
		宛先 IP アドレス	
		トラフィッククラス※10	
		DSCP※10	
		フラグメント※6	FO
			MF
		IP レングス	
	IPv6-TCP ヘッダ	送信元ポート番号	
		宛先ポート番号	
		TCP 制御フラグ※7	
	IPv6-UDP ヘッダ	送信元ポート番号	
		宛先ポート番号	
	IPv6-ICMP ヘッダ	ICMP タイプ	
		ICMP コード	
	中継種別※12	パケット中継種別	

注※1

インタフェースのコンフィグレーションで設定した，インタフェース名およびインタフェース番号です。指定できるインタフェース名を次に示します。

- イーサネットサブインタフェース
- ポートチャネルサブインタフェース
- VLAN インタフェース

注※2

VLAN Tag ヘッダを指定したときの検出を次に示します。

Tag の VLAN ID

VLAN Tag ヘッダの VLAN ID です。Untagged フレームは検出しません。

ユーザ優先度

VLAN Tag ヘッダのユーザ優先度です。Untagged フレームは検出しません。

Tag なし

Untagged フレームです。Tagged フレームは検出しません。

注※3

2 段目の VLAN Tag ヘッダを指定したときの検出を次に示します。

Tag の VLAN ID

2 段目の VLAN Tag ヘッダの VLAN ID です。VLAN Tag ヘッダが 1 段以下のフレームは検出しません。

ユーザ優先度

2 段目の VLAN Tag ヘッダのユーザ優先度です。VLAN Tag ヘッダが 1 段以下のフレームは検出しません。

Tag なし

2 段目の VLAN Tag ヘッダがないフレームです。VLAN Tag ヘッダが 2 段以上のフレームは検出しません。

注※4

IPv4 ヘッダのプロトコルフィールドで示される値を検出します。

注※5

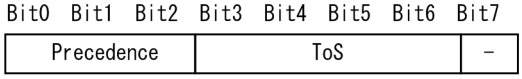
ToS フィールドを指定したときの検出を次に示します。

ToS

ToS フィールドの 3 ビット～6 ビットの値です。

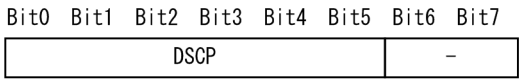
Precedence

ToS フィールドの上位 3 ビットの値です。



DSCP

ToS フィールドの上位 6 ビットの値です。



注※6

フラグメントパラメータを指定したときの検出を次に示します。+fo を指定した場合は，VLAN Tag ヘッダと IP ヘッダだけをフロー検出条件として指定できます。

+fo 指定

フラグメントパケットの途中と最後のパケットを検出します。

-fo 指定

非フラグメントパケット，およびフラグメントパケットの最初のパケットを検出します。

+mf 指定

フラグメントパケットの最初と途中のパケットを検出します。

-mf 指定

非フラグメントパケット，およびフラグメントパケットの最後のパケットを検出します。

フラグメントパラメータの組み合わせと検出するパケットの関係を次の表に示します。

表 13-4　フラグメントパラメータの組み合わせと検出するパケットの関係

フラグメントパラメータ		非フラグメントパケット	フラグメントパケット		
FO	MF		最初	途中	最後
指定なし	指定なし	○	○	○	○
	-mf 指定	○	－	－	○
	+mf 指定	－	○	○	－
-fo 指定	指定なし	○	○	－	－
	-mf 指定	○	－	－	－
	+mf 指定	－	○	－	－
+fo 指定	指定なし	－	－	○	○
	-mf 指定	－	－	－	○
	+mf 指定	－	－	○	－

（凡例）　○：検出する　－：検出しない

注※7

ack/fin/psh/rst/syn/urg フラグを検出します。

注※8

IPv6 ヘッダまたは IPv6 拡張ヘッダの NextHeader フィールドで示される拡張ヘッダ以外の値を検出します。

注※9

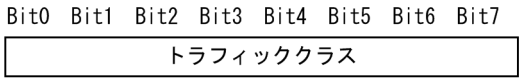
上位 64bit だけ設定できます。

注※10

トラフィッククラスフィールドを指定したときの検出を次に示します。

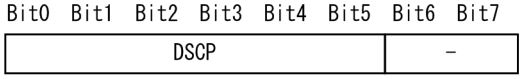
トラフィッククラス

トラフィッククラスフィールドの値です。



DSCP

トラフィッククラスフィールドの上位 6 ビットの値です。



注※11

送信側インタフェースで送信元 MAC アドレスを指定した場合，本装置がレイヤ 3 中継するパケットは受信時の送信元 MAC アドレスで検出します。

注※12

中継種別を指定したときの検出を次に示します。

レイヤ 2 中継

レイヤ 2 中継するフレームを検出します。

レイヤ 3 中継

レイヤ 3 中継するパケットを検出します。

13.1.5　QoS フローリスト

QoS のフロー検出を実施するためにはコンフィグレーションで QoS フローリストを設定します。フロー検出条件に応じて設定する QoS フローリストが異なります。また，フロー検出条件ごとに検出できるフレーム種別が異なります。フロー検出条件と QoS フローリスト，および検出するフレーム種別の関係を次の表に示します。

表 13-5　フロー検出条件と QoS フローリスト，検出するフレーム種別の関係

フロー検出条件	QoS フローリスト	検出するフレーム種別					
		エントリ数重視モード			検出条件数重視モード		
		非 IP	IPv4	IPv6	非 IP	IPv4	IPv6
MAC 条件	mac qos-flow-list	○	○※1	○※1	○	○※1	○※1
IPv4 条件	ip qos-flow-list	－	○※2	－	－	○※2	－
IPv6 条件	ipv6 qos-flow-list	－	－	○※2	－	－	○※2
Advance 条件	advance qos-flow-list	－※3	－※3	－※3	○	○※4	○※4

（凡例）　○：検出する　－：検出しない

注※1

レイヤ 2 中継するフレームを検出します。

注※2

レイヤ 3 中継するパケットを検出します。

注※3

エントリ数重視モードの場合，Advance 条件をインタフェースに適用できません。

注※4

レイヤ 2 中継およびレイヤ 3 中継するフレームの両方を検出します。

QoS フローリストのインタフェースへの適用は，QoS フローグループコマンドで実施します。

なお，QoS フローリストは設定条件によってフロー検出順序が決まります。設定条件ごとのフロー検出順序を次に示します。

(1) QoS フローリスト内での順序

QoS フローリストに複数の QoS フローエントリを設定した場合，QoS フローエントリのシーケンス番号の昇順でフレームを検出します。

(2) 同一インタフェース内での順序

同一インタフェースに複数の QoS フローリストを設定した場合，次の順序でフレームを検出します。

1. MAC QoS フローリスト，IPv4 QoS フローリスト，または IPv6 QoS フローリスト
2. Advance QoS フローリスト

例えば，MAC QoS フローリストでフロー検出したフレームは，Advance QoS フローリストではフロー検出されません。また，統計情報もカウントされません。

(3) 複数のインタフェースでの順序

イーサネットインタフェースと，該当するイーサネットインタフェースのイーサネットサブインタフェース，ポートチャネルサブインタフェース，または VLAN インタフェースに QoS フローリストを設定した場合，次の順序でフレームを検出します。

1. イーサネットインタフェース
2. イーサネットサブインタフェース，ポートチャネルサブインタフェース，または VLAN インタフェース

13.1.6 フロー検出使用時の注意事項

(1) ESP 拡張ヘッダのある IPv6 パケットに対する QoS フロー検出

拡張ヘッダである ESP ヘッダのある IPv6 パケットを QoS フロー検出する場合は，フロー検出条件に次の条件を指定してください。

- コンフィグレーション
- MAC ヘッダ
- VLAN Tag ヘッダ
- IPv6 ヘッダ
- 中継種別

上位プロトコルおよび TCP/UDP/ICMP ヘッダをフロー検出条件に指定しても，QoS フロー検出しません。

(2) オプションヘッダのある IPv4 パケットに対する QoS フロー検出

Advance 条件でレイヤ 2 中継かつオプションヘッダのある IPv4 パケットを QoS フロー検出する場合は，フロー検出条件に次の条件を指定してください。

- コンフィグレーション

- MAC ヘッダ
- VLAN Tag ヘッダ
- IPv4 ヘッダ
- 中継種別

TCP/UDP/ICMP/IGMP ヘッダをフロー検出条件に指定しても，QoS フロー検出しません。

(3)　拡張ヘッダのある IPv6 パケットに対する QoS フロー検出

Advance 条件でレイヤ 2 中継かつ拡張ヘッダのある IPv6 パケットを QoS フロー検出する場合は，フロー検出条件に次の条件を指定してください。

- コンフィグレーション
- MAC ヘッダ
- VLAN Tag ヘッダ
- IPv6 ヘッダ
- 中継種別

上位プロトコルおよび TCP/UDP/ICMP ヘッダをフロー検出条件に指定した場合の，QoS フロー検出可否を次に示します。

表 13-6　受信側インタフェースでの QoS フロー検出可否

パケット				フロー検出条件		
レイヤ 3 ヘッダ			パケット受信時のレイヤ 2 ヘッダサイズ	上位プロトコル	TCP/UDP/ICMP ヘッダ	TCP 制御フラグ
拡張ヘッダ段数	拡張ヘッダ種別	拡張ヘッダサイズ				
2 段以上	−	−	−	×	×	×
1 段	−	28byte 以上	−	○	×	×
	AH	16byte	30byte 以上	○	○	×
		20byte	26byte 以上	○	○	×
		24byte	22byte 以上	○	○	×
			30byte 以上	○	×	×
	上記以外	16byte	30byte 以上	○	○	×
		24byte	22byte 以上	○	○	×
			30byte 以上	○	×	×

（凡例）　○：検出できる　×：検出できない　−：条件によらない

表 13-7　送信側インタフェースでの QoS フロー検出可否

パケット				フロー検出条件		
レイヤ 3 ヘッダ			パケット受信時のレイヤ 2 ヘッダサイズ	上位プロトコル	TCP/UDP/ICMP ヘッダ	TCP 制御フラグ
拡張ヘッダ段数	拡張ヘッダ種別	拡張ヘッダサイズ				
2 段以上	−	−	−	×	×	×
1 段	−	25byte 以上	−	○	×	×
	AH	12byte	30byte 以上	○	○	×
		16byte	26byte 以上	○	○	×
		20byte	22byte 以上	○	○	×
			30byte 以上	○	×	×
		24byte	18byte 以上	○	○	×
			26byte 以上	○	×	×
	上記以外	16byte	26byte 以上	○	○	×
		24byte 以上	18byte 以上	○	○	×
			26byte 以上	○	×	×

（凡例）○：検出できる　×：検出できない　−：条件によらない

(4)　拡張ヘッダが 2 段以上ある IPv6 パケットに対する QoS フロー検出

レイヤ 2 中継かつ拡張ヘッダが 2 段以上ある IPv6 パケットを QoS フロー検出する場合は，フラグメント条件（FO および MF）以外の条件を指定してください。

(5)　フラグメントパケットに対する QoS フロー検出

フラグメントパケットの 2 番目以降のパケットは TCP/UDP/ICMP/IGMP ヘッダがパケット内にありません。フラグメントパケットを受信した際の QoS フロー検出を次の表に示します。

表 13-8　フラグメントパケットと QoS フロー検出の関係

フロー検出条件	フロー検出条件とパケットの一致/不一致	先頭パケット	2 番目以降のパケット
IP ヘッダだけ	IP ヘッダ一致	一致したエントリの動作	一致したエントリの動作
	IP ヘッダ不一致	次のエントリを検索	次のエントリを検索
IP ヘッダ+ TCP/UDP/ICMP/IGMP ヘッダ	IP ヘッダ一致，TCP/UDP/ICMP/IGMP ヘッダ一致	一致したエントリの動作	−
	IP ヘッダ一致，	次のエントリを検索	次のエントリを検索

フロー検出条件	フロー検出条件とパケットの一致/不一致	先頭パケット	2 番目以降のパケット
	TCP/UDP/ICMP/IGMP ヘッダ不一致		
	IP ヘッダ不一致， TCP/UDP/ICMP/IGMP ヘッダ不一致	次のエントリを検索	次のエントリを検索

（凡例）

－：TCP/UDP/ICMP/IGMP ヘッダがパケットにないため，常に TCP/UDP/ICMP/IGMP ヘッダ不一致として扱うので該当しない

(6)　QoS フロー廃棄以外の QoS フローで検出しないフレーム

本装置では，受信側に設定した QoS フロー廃棄以外の QoS フローで，次に示すフレームをフロー検出しません。

- uRPF によって廃棄したフレーム
- 受信側に設定したフィルタによって廃棄したフレーム
- Null インタフェースによって廃棄したパケット
- ダイレクトブロードキャスト中継が無効なため廃棄したパケット
- パケット受信時のユニキャスト中継機能によって廃棄したパケット
- パケット受信時のマルチキャスト中継機能によって廃棄したパケット
- 本装置宛てのフレーム
- TTL が 1 の IPv4 パケット
- ホップリミットが 1 の IPv6 パケット
- ストームコントロールによって廃棄したフレーム

また，送信側に設定した QoS フロー廃棄以外の QoS フローで，次に示すフレームをフロー検出しません。

- 送信側に設定したフィルタによって廃棄したフレーム
- ポートミラーリングでコピーしたフレーム

(7)　QoS フロー廃棄の QoS フローで検出しないフレーム

本装置では，次のどちらの条件も満たすフレームに対して，QoS フロー廃棄の QoS フローエントリによるフロー検出をしません。

- QoS フロー廃棄以外の QoS フローで検出しないフレーム
- フロー検出順序が先になる QoS フロー廃棄以外の QoS フローエントリで，検出条件に一致するフレーム

受信側に設定した QoS フロー廃棄の QoS フローでは，次に示すフレームをフロー検出しません。

- uRPF によって廃棄したフレーム
- 受信側に設定したフィルタによって廃棄したフレーム

また，送信側に設定した QoS フロー廃棄の QoS フローでは，次に示すフレームをフロー検出しません。

- 送信側に設定したフィルタによって廃棄したフレーム
- ポートミラーリングでコピーしたフレーム

(8)　自発パケットに対する QoS フロー検出

特定自発パケットを送信側で QoS フロー検出する場合は，検出できる QoS フローリスト種別や中継種別で設定してください。

対象となる特定自発 IPv4 パケットを次に示します。

- 宛先 IP アドレスがブロードキャストアドレスのパケット
- 宛先 IP アドレスがマルチキャストアドレスのパケット
- 次のプロトコル制御パケット
  - DHCP/BOOTP クライアント宛てのメッセージ
  - スタティック経路のポーリングによる ICMP パケット
  - 直結経路との BGP4 メッセージ

対象となる特定自発 IPv6 パケットを次に示します。

- 宛先 IP アドレスがリンクローカルアドレスのパケット
- 宛先 IP アドレスがマルチキャストアドレスのパケット
- 次のプロトコル制御パケット
  - スタティック経路のポーリングによる ICMPv6 パケット
  - 直結経路との BGP4+メッセージ

これらの特定自発パケットに対する QoS フロー検出可否を次の表に示します。

表 13-9　特定自発パケットの QoS フロー検出可否

フロー検出モード	QoS フローリスト種別	検出条件の中継種別	検出可否
エントリ数重視モード	MAC QoS フローリスト	－	×
	IPv4 QoS フローリスト	－	○
	IPv6 QoS フローリスト	－	○
検出条件数重視モード	MAC QoS フローリスト	－	○
	IPv4 QoS フローリスト	－	×
	IPv6 QoS フローリスト	－	×
	Advance QoS フローリスト	指定なし	○
		レイヤ 2 中継	○
		レイヤ 3 中継	×

（凡例）　○：検出できる　×：検出できない　－：指定できない

(9)　IP マルチキャストパケットおよび IP ブロードキャストパケットに対する QoS フロー検出

IP マルチキャストパケットおよび IP ブロードキャストパケットには，レイヤ 2 中継とレイヤ 3 中継が共に実施されます。IP マルチキャストパケットおよび IP ブロードキャストパケットを QoS フロー検出する場合は，該当するインタフェースに対して次のどちらかを適用してください。

- 次に示す 2 種類の QoS フローエントリを同時に指定する
  - IPv4 条件または IPv6 条件の QoS フローエントリ
  - MAC 条件の QoS フローエントリ
- Advance 条件で，中継種別を指定しない QoS フローエントリを指定する
  この場合，統計情報は 2 回カウントされます。

(10)　DSCP マッピングでの QoS フロー検出

DSCP マッピングを指定した QoS フローでは，IP パケットをフロー検出します。

(11)　QoS フローエントリ変更時の動作

本装置では，インタフェースに適用済みの QoS フローエントリを変更すると，変更が反映されるまでの間，検出の対象となるフレームをほかの QoS フローエントリで検出することがあります。

また，変更後の QoS フローエントリが複数のエントリを使用するフロー検出条件の場合，すべての QoS フローエントリを装置に反映してから統計情報の採取を開始します。

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

QoS フロ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 13-10　コンフィグレーションコマンド一覧

コマンド名	説明
advance qos-flow-group	インタフェースに対して Advance QoS フローリストを設定して，Advance 条件による QoS 制御を適用します。
advance qos-flow-list	Advance 条件でフロー検出を行う Advance QoS フローリストを設定します。
advance qos-flow-list resequence	Advance QoS フローリストの条件適用順序のシーケンス番号を再設定します。
ip qos-flow-group	インタフェースに対して IPv4 QoS フローリストを設定して，IPv4 QoS 制御を適用します。
ip qos-flow-list	IPv4 QoS フロー検出として動作する QoS フローリストを設定します。
ip qos-flow-list resequence	IPv4 QoS フローリストの条件適用順序のシーケンス番号を再設定します。
ipv6 qos-flow-group	インタフェースに対して IPv6 QoS フローリストを設定して，IPv6 QoS 制御を適用します。
ipv6 qos-flow-list	IPv6 QoS フロー検出として動作する QoS フローリストを設定します。
ipv6 qos-flow-list resequence	IPv6 QoS フローリストの条件適用順序のシーケンス番号を再設定します。
mac qos-flow-group	インタフェースに対して MAC QoS フローリストを設定して，MAC QoS 制御を適用します。
mac qos-flow-list	MAC QoS フロー検出として動作する QoS フローリストを設定します。
mac qos-flow-list resequence	MAC QoS フローリストの条件適用順序のシーケンス番号を再設定します。
qos	QoS フローリストのフロー検出条件および動作を指定します。
remark	QoS の補足説明を記述します。
flow detection mode※	フィルタ・QoS フローのフロー検出モードを設定します。
flow max-configuration※	フィルタ・QoS フローのコンフィグレーション最大数を設定します。
flow max-entry extended※	フローエントリ数拡張機能を有効にします。
flow-table allocation※	フィルタ・QoS フローの配分パターンを設定します。

注※

「コンフィグレーションコマンドレファレンス Vol.1」「10　装置とソフトウェアの管理」を参照してください。

13.2.2　フロー検出モードの設定

フロー検出モードを検出条件数重視モードに指定する例を次に示します。

[設定のポイント]

フロー検出モードはデフォルトではエントリ数重視モードです。設定したフロー検出モードを反映させるために，すべての PSU を再起動してください。

[コマンドによる設定]

1. **(config)# flow detection mode condition-oriented**
   グローバルコンフィグレーションモードでフロー検出モードを検出条件数重視モードに設定します。

[注意事項]

- エントリ数重視モードには，すべてのインタフェースに Advance アクセスリストおよび Advance QoS フローリストが適用されていないときに変更できます。
- 検出条件数重視モードには，フィルタ・QoS フローのエントリ数が収容条件以内のときに変更できます。

13.2.3　複数インタフェースに対する QoS フローの設定

複数のイーサネットインタフェースに QoS フローを設定する例を示します。

[設定のポイント]

config-if-range モードで，複数のイーサネットインタフェースに QoS フローを設定できます。

[コマンドによる設定]

1. **(config)# ip qos-flow-list QOS-LIST1**
   IPv4 QoS フローリスト（QOS-LIST1）を作成します。本リストを作成すると，IPv4 QoS フローリストモードに移行します。
2. **(config-ip-qos)# qos ip any host 192.0.2.10 action priority-class 6**
   192.0.2.10 の IP アドレスを宛先として，優先クラスを 6 に変更する IPv4 QoS フローリストを設定します。
3. **(config-ip-qos)# exit**
   IPv4 QoS フローリスト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 range gigabitethernet 1/1-4**
   イーサネットインタフェース 1/1-4 のコンフィグレーションモードに移行します。
5. **(config-if-range)# ip qos-flow-group QOS-LIST1 out**
   送信側に IPv4 QoS フローリストを適用します。

13.3　オペレーション

13.3.1　運用コマンド一覧

QoS フローの運用コマンド一覧を次の表に示します。

表 13-11　運用コマンド一覧

コマンド名	説明
show qos-flow	QoS フローの設定内容と統計情報を表示します。
clear qos-flow	QoS フローの統計情報を 0 クリアします。
restart filter-qosflow※	QoS フローを設定するフィルタ・QoS フロー制御プログラムを再起動します。
dump filter-qosflow※	QoS フローを設定するフィルタ・QoS フロー制御プログラムで採取している制御情報をファイルへ出力します。

注※

「運用コマンドレファレンス Vol.2」「10　フィルタ・QoS 共通」を参照してください。

13.3.2　IPv4 パケットをフロー検出条件とした QoS フローの動作確認

show qos-flow コマンドで QoS フローの動作を確認できます。インタフェースを範囲指定すると, 複数インタフェースの QoS フローの動作を確認できます。

IPv4 パケットをフロー検出条件とした QoS フローの動作確認を次の図に示します。

図 13-2　IPv4 パケットをフロー検出条件とした QoS フローの動作確認

```
> show qos-flow interface gigabitethernet 1/1 QOS-LIST1 out
Date 20XX/01/01 12:00:00 UTC
Using interface : gigabitethernet 1/1 out
IP qos-flow-list : QOS-LIST1
      10 ip any host 192.0.2.10 action priority-class 6
                      Matched packets        Matched bytes
         Total  :                 5642               222540
         PSU 1  :                 5642               222540
>
```

指定したイーサネットインタフェースの QoS フローに「IP qos-flow-list」が表示されることを確認します。また, フロー検出条件に一致したフレームは Matched packets および Matched bytes で確認します。

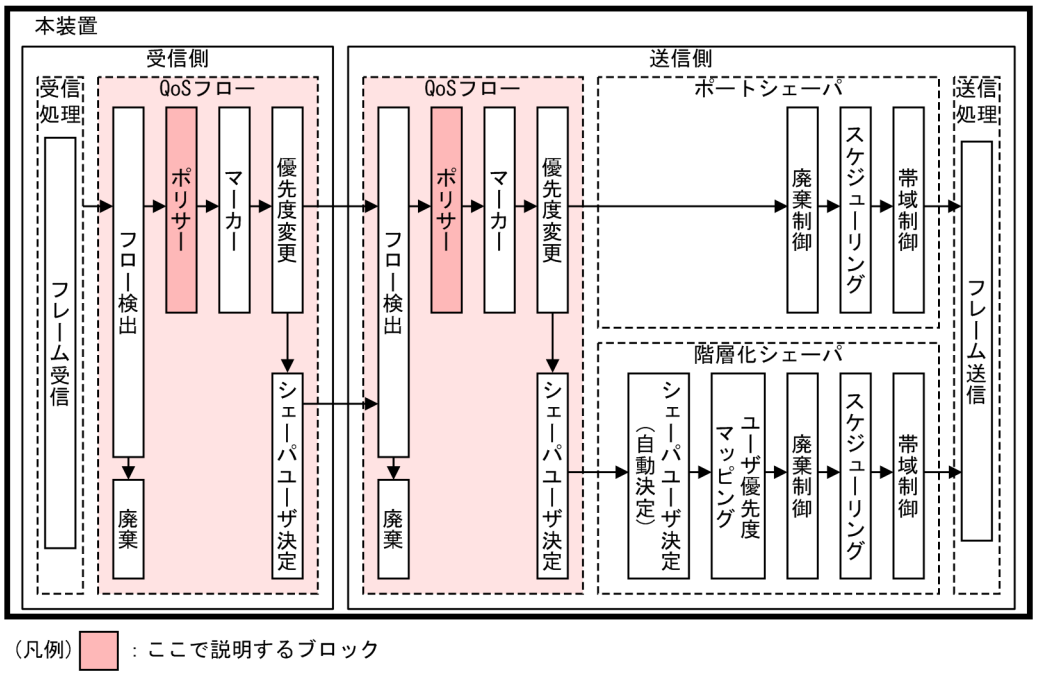
14 ポリサー

ポリサーは，QoS フローでフロー検出したフレームの帯域を監視する機能です。この章では，ポリサーの解説と操作方法について説明します。

14.1　解説

ポリサーは，フロー検出で検出したフローの帯域を監視する機能です。ここで説明するポリサーの位置づけを次の図に示します。

図 14-1　ポリサーの位置づけ



14.1.1　概要

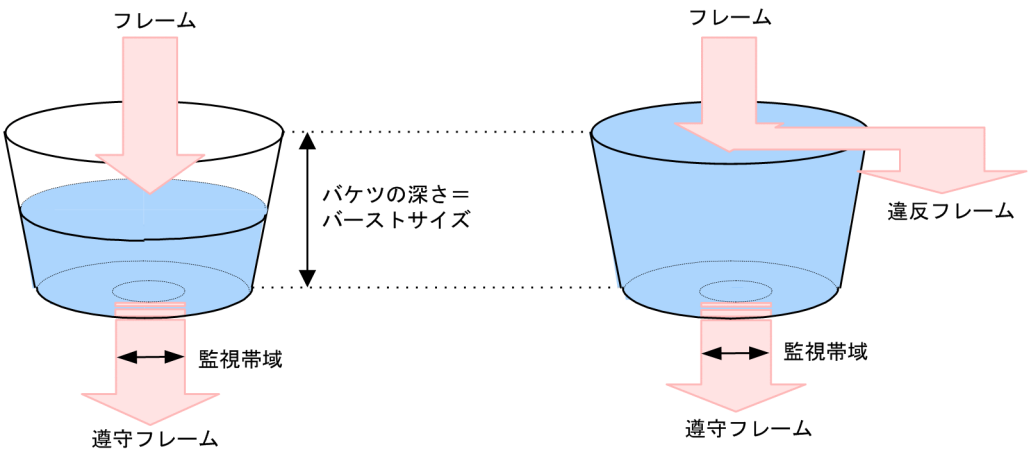
ポリサーでは，フロー検出で検出したフレームのフレーム長（フレーム間ギャップ※から FCS まで）を基に帯域を監視します。指定した監視帯域内として中継するフレームを**遵守フレーム**，監視帯域以上としてペナルティを科すフレームを**違反フレーム**と呼びます。

注※　フレーム間ギャップは，12byte とします。

フロー検出で検出したフレームが監視帯域を遵守しているか，または違反しているかの判定には，水の入った穴の開いたバケツをモデルとする，Leaky Bucket アルゴリズムを使用しています。

Leaky Bucket アルゴリズムのモデルを次の図に示します。

図 14-2　Leaky Bucket アルゴリズムのモデル



バケツからは監視帯域分の水が流れ，フレーム送受信時にはフレーム間ギャップから FCS までのサイズの水が注ぎ込まれます。水が注ぎ込まれる際にバケツがあふれていなければ，遵守フレームとして中継されます（上図の左側の例）。水が注ぎ込まれる際にバケツがあふれている場合は，フロー検出で検出したフレームを違反フレームとしてペナルティを科します（上図の右側の例）。水が一時的に大量に注ぎこまれたときに許容できる量，すなわちバケツの深さがバーストサイズに対応します。

本機能は，最低帯域監視と最大帯域監視から成ります。最低帯域監視は，違反フレームに対してマーカーや優先度変更によって優先度や DSCP を書き換え，ペナルティを科します。最大帯域監視は違反フレームを廃棄します。最低帯域監視と最大帯域監視で使用できるペナルティの種類を次の表に示します。

表 14-1　最低帯域監視と最大帯域監視で使用できるペナルティの種類

違反フレームに対するペナルティ	帯域監視種別	
	最低帯域監視	最大帯域監視
廃棄	－	○
廃棄クラス変更	○	－
DSCP 書き換え	○	－
ユーザ優先度書き換え	○	－

（凡例）○：使用できるペナルティ　－：使用できないペナルティ

ポリサーで最低帯域監視と最大帯域監視を同時に使用した場合，監視帯域値やバーストサイズの組み合わせによって，2 レート 3 カラーのポリシングおよびシングルレート 3 カラーのポリシングができます。

(1)　2 レート 3 カラーのポリシング

2 レート 3 カラーのポリシングでは，帯域使用量に応じてフレームを分類して，マーキングします。フレームの分類を次の表に示します。

表 14-2　フレームの分類（2 レート 3 カラーのポリシング）

分類	カラー	内容
違反フレーム	レッド	最大帯域監視の監視帯域値を超過したフレーム

分類	カラー	内容
超過フレーム	イエロー	最低帯域監視の監視帯域値を超過したフレーム
遵守フレーム	グリーン	最低帯域監視の監視帯域値以下のフレーム

このうち，違反フレーム（レッド）は廃棄します。超過フレーム（イエロー）には，最低帯域監視の違反フレームに対するペナルティを科します。

2 レート 3 カラーのポリシングをする場合は，最大帯域監視の監視帯域値に，最低帯域監視の監視帯域値より大きい値を設定してください。

(2)　シングルレート 3 カラーのポリシング

シングルレート 3 カラーのポリシングでは，特定の帯域でバースト性に応じてフレームを分類して，マーキングします。フレームの分類を次の表に示します。

表 14-3　フレームの分類（シングルレート 3 カラーのポリシング）

分類	カラー	内容
違反フレーム	レッド	監視帯域値を超過かつ最大帯域監視のバーストサイズを超過したフレーム
超過フレーム	イエロー	監視帯域値を超過かつ最低帯域監視のバーストサイズを超過したフレーム
遵守フレーム	グリーン	監視帯域値以下のフレーム

このうち，違反フレーム（レッド）は廃棄します。超過フレーム（イエロー）には，最低帯域監視の違反フレームに対するペナルティを科します。

シングルレート 3 カラーのポリシングをする場合は，最大帯域監視の監視帯域値と最低帯域監視の監視帯域値に同じ値を設定して，最大帯域監視のバーストサイズに最低帯域監視のバーストサイズより大きい値を設定してください。

14.1.2　集約ポリサー

集約ポリサーとは，複数のフローをまとめて帯域を監視する機能です。本機能は，受信側インタフェースと送信側インタフェースでそれぞれ使用できます。

集約ポリサーを使用するには，同じポリサーエントリを複数の QoS フローエントリに指定する方法や，ポリサーエントリを指定した QoS フローエントリを複数のインタフェースに適用する方法などがあります。

14.1.3　帯域監視のオプション動作

ポリサーでは，コンフィグレーションコマンド policer rate-option によって，帯域を監視するオプション動作を設定できます。帯域監視のオプション動作で設定できるパラメータと，その動作内容を次の表に示します。

表 14-4　帯域監視のオプション動作のパラメータおよび動作

パラメータ	動作	用途
exclude-4-byte	フレーム長から 4 バイトを差し引いた値を基に帯域を監視します※。	エッジスイッチで，VLAN Tag が 2 段以上付いたフレームの 1 段目の VLAN Tag（4 バイト）を差し引いて帯域を監視します。

注※

運用コマンドで表示する統計情報（バイト数統計）は，実際のフレーム長で表示します。

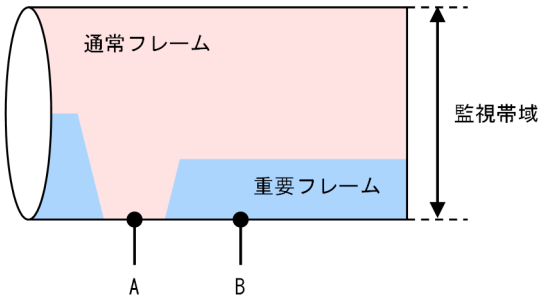
14.1.4　重要フロー保護

重要フロー保護は，ポリサーで設定した監視帯域内で，より重要なフレームを優先的に転送する機能です。この優先的に転送するフレームを重要フレームと呼びます。これに対し，重要フレームが使用していない監視帯域（余剰帯域）を使用して転送するフレームを通常フレームと呼びます。

重要フレームは，重要フロー保護で設定するフロー検出条件（重要フロー検出条件）で検出します。通常フレームは，ポリサーを設定したフロー検出条件（通常フロー検出条件）で検出します。

重要フロー保護使用時の帯域使用状態の例を次の図に示します。

図 14-3　重要フロー保護使用時の帯域使用状態



A 時点

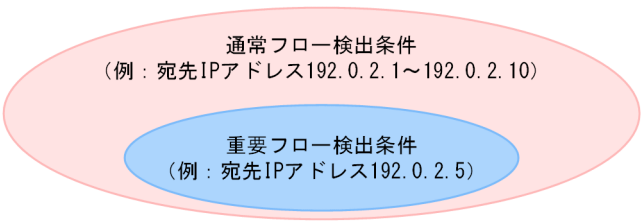
重要フレームの中継がないため，通常フレームが全監視帯域を使用しています。

B 時点

重要フレームは優先的に監視帯域を使用しています。通常フレームは余剰帯域を使用しています。

重要フロー保護を使用する場合は，次の図に示すように，通常フロー検出条件の中で特に重要なフレームの検出条件を，重要フロー検出条件に指定してください。

図 14-4　フロー検出条件指定の概念



14.1.5　ポリサー使用時の注意事項

(1)　バーストサイズの設定

帯域の揺らぎが大きいトラフィックの遵守パケットを中継する場合には，バーストサイズを大きく設定して使用してください。

なお，バーストサイズにはフロー検出で検出するフレームのフレーム長より大きい値を設定してください。注入されるフレーム長より小さい値をバーストサイズに設定した場合は，設定した帯域以下で違反となることがあります。

(2) 最大帯域監視と最低帯域監視の設定値

ポリサーで最大帯域監視と最低帯域監視を同時に設定して，監視帯域値およびバーストサイズを同じ値で設定した場合は，最大帯域監視だけ指定したときと同等の動作になります。

(3) ポリサーとほかの QoS フロー機能を同時に使用したときの動作

ポリサーと，マーカーおよび優先度変更を同時に使用した場合は，次の順で動作を優先してフレームを送信します。

1. 送信インタフェースに設定した，DSCP マッピング
2. 送信インタフェースに設定した，最低帯域監視に違反したフレームに対するペナルティ
3. 送信インタフェースに設定した，優先度変更またはマーカー
4. 受信インタフェースに設定した，DSCP マッピング
5. 受信インタフェースに設定した，最低帯域監視に違反したフレームに対するペナルティ
6. 受信インタフェースに設定した，優先度変更またはマーカー

(4) ポリサーと送信イーサネットインタフェース・送信キューの関係

次のような場合に，送信イーサネットインタフェースまたは送信キューで遵守フレームを廃棄するおそれがあります。

- ポリサーで指定する監視帯域値を，該当フローの送信イーサネットインタフェースまたは送信キューの帯域値より大きい値とした場合
- 帯域監視を使用しないフローと使用するフローを，同じ送信イーサネットインタフェースまたは送信キューに送信した場合

特に，複数のフローで複数のポリサーを使用する場合は，各ポリサーの監視帯域値の合計に注意してください。

(5) プロトコル制御パケットのポリサー

ポリサーではプロトコル制御フレームも監視対象になります。したがって，プロトコル制御フレームにも帯域違反としてペナルティを科します。そのため，プロトコル制御フレームを考慮した帯域を確保する必要があります。

(6) TCP フレームに対する最大帯域監視の使用

最大帯域監視を使用した場合は，TCP のスロースタートが繰り返されデータ転送速度が極端に遅くなることがあります。

上記動作を防ぐために，最低帯域監視を使用して「フレームが廃棄されやすくなるように廃棄クラスを下げる」動作を実施するようにしてください。本設定によって，契約帯域を超えてもすぐに廃棄されないようになります。

(7) 複数の FE にわたるポリサー設定時の動作

次に示すような複数の FE にわたるポリサーを設定した場合，PSU 内の FE ごとに帯域を監視します。

- ポリサーを指定した QoS フローを，複数の FE にわたるインタフェースで構成するポートチャネル（サブインタフェース）に適用した場合
- ポリサーを指定した QoS フローを，FE が異なる複数のインタフェースに適用した場合

PSU の種別によって，実装される FE の数や，FE と NIF のつながりが異なるため，設定する際は注意してください。PSU 内の FE と NIF のつながりについては，「20.1.1　概要」を参照してください。

14.2　コンフィグレーション

14.2.1　コンフィグレーションコマンド一覧

ポリサ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 14-5　コンフィグレーションコマンド一覧

コマンド名	説明
advance qos-flow-group	インタフェースに対して Advance QoS フローリストを設定して，Advance 条件による QoS 制御を適用します。
advance qos-flow-list	Advance 条件でフロー検出を行う Advance QoS フローリストを設定します。
advance qos-flow-list resequence	Advance QoS フローリストの条件適用順序のシーケンス番号を再設定します。
ip qos-flow-group	インタフェースに対して IPv4 QoS フローリストを設定して，IPv4 QoS 制御を適用します。
ip qos-flow-list	IPv4 QoS フロー検出として動作する QoS フローリストを設定します。
ip qos-flow-list resequence	IPv4 QoS フローリストの条件適用順序のシーケンス番号を再設定します。
ipv6 qos-flow-group	インタフェースに対して IPv6 QoS フローリストを設定して，IPv6 QoS 制御を適用します。
ipv6 qos-flow-list	IPv6 QoS フロー検出として動作する QoS フローリストを設定します。
ipv6 qos-flow-list resequence	IPv6 QoS フローリストの条件適用順序のシーケンス番号を再設定します。
mac qos-flow-group	インタフェースに対して MAC QoS フローリストを設定して，MAC QoS 制御を適用します。
mac qos-flow-list	MAC QoS フロー検出として動作する QoS フローリストを設定します。
mac qos-flow-list resequence	MAC QoS フローリストの条件適用順序のシーケンス番号を再設定します。
policer	QoS フローリストで指定するポリサーエントリを設定します。
policer rate-option	ポリサーで帯域を監視するオプション動作を設定します。
premium	QoS フローリストの重要フロー検出条件を指定します。
qos	QoS フローリストのフロー検出条件および動作を指定します。
remark	QoS の補足説明を記述します。
system policer-statistics-mode	ポリサーの統計情報の取得単位を設定します。

14.2.2　最大帯域監視の設定

特定のフローに対して最大帯域監視をする場合の例を次に示します。

[設定のポイント]

フレーム受信時に宛先 IP アドレスによってフロー検出をして，最大帯域監視をする設定をします。

[コマンドによる設定]

1. **(config)# policer POLICER-1 in max-rate 500M max-burst 100k**
   ポリサーエントリ（POLICER-1）を作成して，次に示す設定をします。
   - 最大帯域監視の監視帯域：500Mbit/s
   - 最大帯域監視のバーストサイズ：100kbyte
2. **(config)# ip qos-flow-list QOS-LIST1**
   IPv4 QoS フローリスト（QOS-LIST1）を作成します。本リストを作成すると，IPv4 QoS フローリストモードに移行します。
3. **(config-ip-qos)# qos ip any host 192.0.2.10 action policer POLICER-1**
   宛先 IP アドレスが 192.0.2.10 のフローに対してポリサーエントリ（POLICER-1）を指定した IPv4 QoS フローリストを設定します。
4. **(config-ip-qos)# exit**
   IPv4 QoS フローリスト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 gigabitethernet 1/1**
   イーサネットインタフェース 1/1 のコンフィグレーションモードに移行します。
6. **(config-if)# ip qos-flow-group QOS-LIST1 in**
   受信側に IPv4 QoS フローリスト（QOS-LIST1）を適用します。

14.2.3　最低帯域監視違反時の廃棄クラスの設定

特定のフローに対して最低帯域監視をして，違反フレームの廃棄クラスを変更する場合の例を次に示します。

[設定のポイント]

フレーム送信時に宛先 IP アドレスによってフロー検出をして，最低帯域監視をする設定をします。最低帯域監視を違反したフレームに対しては，廃棄クラスを変更する設定をします。

[コマンドによる設定]

1. **(config)# policer POLICER-2 out min-rate 300M min-burst 80k penalty-discard-class 2**
   ポリサーエントリ（POLICER-2）を作成して，次に示す設定をします。
   - 最低帯域監視の監視帯域：300Mbit/s
   - 最低帯域監視のバーストサイズ：80kbyte
   - 最低帯域監視の違反フレームの廃棄クラス：2
2. **(config)# ip qos-flow-list QOS-LIST2**
   IPv4 QoS フローリスト（QOS-LIST2）を作成します。本リストを作成すると，IPv4 QoS フローリストモードに移行します。
3. **(config-ip-qos)# qos ip any host 192.0.2.10 action policer POLICER-2**
   宛先 IP アドレスが 192.0.2.10 のフローに対してポリサーエントリ（POLICER-2）を指定した IPv4 QoS フローリストを設定します。
4. **(config-ip-qos)# exit**

IPv4 QoS フローリスト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 gigabitethernet 1/3**
   イーサネットインタフェース 1/3 のコンフィグレーションモードに移行します。
6. **(config-if)# ip qos-flow-group QOS-LIST2 out**
   送信側に IPv4 QoS フローリスト（QOS-LIST2）を適用します。

14.2.4　最低帯域監視違反時の DSCP 書き換えの設定

特定のフローに対して最低帯域監視をして，違反フレームの DSCP を書き換える場合の例を次に示します。

[設定のポイント]

フレーム受信時に宛先 IP アドレスによってフロー検出をして，最低帯域監視をする設定をします。最低帯域監視を違反したフレームに対しては，DSCP 値を変更する設定をします。

[コマンドによる設定]

1. **(config)# policer POLICER-3 in min-rate 200M min-burst 70k penalty-dscp 11**
   ポリサーエントリ（POLICER-3）を作成して，次に示す設定をします。
   - 最低帯域監視の監視帯域：200Mbit/s
   - 最低帯域監視のバーストサイズ：70kbyte
   - 最低帯域監視の違反フレームの DSCP 値：11
2. **(config)# ip qos-flow-list QOS-LIST3**
   IPv4 QoS フローリスト（QOS-LIST3）を作成します。本リストを作成すると，IPv4 QoS フローリストモードに移行します。
3. **(config-ip-qos)# qos ip any host 192.0.2.10 action policer POLICER-3**
   宛先 IP アドレスが 192.0.2.10 のフローに対してポリサーエントリ（POLICER-3）を指定した IPv4 QoS フローリストを設定します。
4. **(config-ip-qos)# exit**
   IPv4 QoS フローリスト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 gigabitethernet 1/3.100**
   イーサネットサブインタフェース 1/3.100 のコンフィグレーションモードに移行します。
6. **(config-subif)# ip qos-flow-group QOS-LIST3 in**
   受信側に IPv4 QoS フローリスト（QOS-LIST3）を適用します。

14.2.5　最大帯域監視と最低帯域監視の組み合わせの設定

特定のフローに対して最大帯域監視と最低帯域監視をして，違反フレームの DSCP を書き換える場合の例を次に示します。

[設定のポイント]

フレーム受信時に宛先 IP アドレスによってフロー検出をして，最大帯域監視と最低帯域監視をする設定をします。最低帯域監視を違反したフレームに対しては，DSCP 値を変更する設定をします。

[コマンドによる設定]

1. **(config)# policer POLICER-4 in max-rate 800M max-burst 120k min-rate 300M min-burst 70k penalty-dscp 22**

   ポリサーエントリ（POLICER-4）を作成して，次に示す設定をします。

   - 最大帯域監視の監視帯域：800Mbit/s
   - 最大帯域監視のバーストサイズ：120kbyte
   - 最低帯域監視の監視帯域：300Mbit/s
   - 最低帯域監視のバーストサイズ：70kbyte
   - 最低帯域監視の違反フレームの DSCP 値：22

2. **(config)# ip qos-flow-list QOS-LIST4**

   IPv4 QoS フローリスト（QOS-LIST4）を作成します。本リストを作成すると，IPv4 QoS フローリストモードに移行します。

3. **(config-ip-qos)# qos ip any host 192.0.2.10 action policer POLICER-4**

   宛先 IP アドレスが 192.0.2.10 のフローに対してポリサーエントリ（POLICER-4）を指定した IPv4 QoS フローリストを設定します。

4. **(config-ip-qos)# exit**

   IPv4 QoS フローリスト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 port-channel 20.200**

   ポートチャネルサブインタフェース 20.200 のコンフィグレーションモードに移行します。

6. **(config-subif)# ip qos-flow-group QOS-LIST4 in**

   受信側に IPv4 QoS フローリスト（QOS-LIST4）を適用します。

14.2.6 集約ポリサーによる最大帯域監視の設定

一つのポリサーエントリを複数の QoS フローエントリや複数のインタフェースに適用して，複数のフローをまとめて帯域を監視する場合の例を次に示します。

[設定のポイント]

最大帯域監視を設定したポリサーエントリを，異なる TCP ポート番号でフロー検出する二つの QoS フローエントリに設定します。この QoS フローエントリを二つのインタフェースに設定することで，四つのフローをまとめて帯域を監視します。

[コマンドによる設定]

1. **(config)# policer POLICER-5 in max-rate 800M max-burst 200k**

   ポリサーエントリ（POLICER-5）を作成して，次に示す設定をします。

   - 最大帯域監視の監視帯域：800Mbit/s
   - 最大帯域監視のバーストサイズ：200kbyte

2. **(config)# ip qos-flow-list QOS-LIST5**

   IPv4 QoS フローリスト（QOS-LIST5）を作成します。本リストを作成すると，IPv4 QoS フローリストモードに移行します。

3. **(config-ip-qos)# qos tcp any any eq http action policer POLICER-5**

   宛先ポート番号が http の tcp フローに対してポリサーエントリ（POLICER-5）を指定した IPv4 QoS フローリストを設定します。

4. **(config-ip-qos)# qos tcp any any eq ftp action policer POLICER-5**

宛先ポート番号が ftp の tcp フローに対してポリサーエントリ（POLICER-5）を指定した IPv4 QoS フローリストを設定します。

5. **(config-ip-qos)# exit**
   IPv4 QoS フローリスト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)# interface gigabitethernet 1/3**
   イーサネットインタフェース 1/3 のコンフィグレーションモードに移行します。
7. **(config-if)# ip qos-flow-group QOS-LIST5 in**
   受信側に IPv4 QoS フローリスト（QOS-LIST5）を適用します。
8. **(config-if)# exit**
   イーサネットインタフェース 1/3 の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に戻ります。
9. **(config)# interface gigabitethernet 1/4**
   イーサネットインタフェース 1/4 のコンフィグレーションモードに移行します。
10. **(config-if)# ip qos-flow-group QOS-LIST5 in**
    受信側に IPv4 QoS フローリスト（QOS-LIST5）を適用します。

14.2.7 重要フロー保護の設定

重要フロー保護を使用する場合の設定例を次に示します。

[設定のポイント]

フレーム受信時に，宛先 IP アドレス（192.0.2.1～192.0.2.10）で通常フロー検出を，特定の宛先 IP アドレス（192.0.2.5）で重要フロー検出をして，最大帯域監視を行います。

[コマンドによる設定]

1. **(config)# policer POLICER-6 in max-rate 500M max-burst 100k**
   ポリサーエントリ（POLICER-6）を作成して，次に示す設定をします。
   - 最大帯域監視の監視帯域：500Mbit/s
   - 最大帯域監視のバーストサイズ：100kbyte
2. **(config)# ip qos-flow-list PREMIUM-LIST**
   IPv4 QoS フローリスト（PREMIUM-LIST）を作成します。本リストを作成すると，IPv4 QoS フローリストモードに移行します。
3. **(config-ip-qos)# 10 qos ip any range-address 192.0.2.1 192.0.2.10 action policer POLICER-6**
   宛先 IP アドレスが 192.0.2.1～192.0.2.10 のフローに対して，ポリサーエントリ（POLICER-6）を指定した IPv4 QoS フローリストを設定します。
4. **(config-ip-qos)# 10 premium ip any host 192.0.2.5**
   重要フロー検出条件では，通常フロー検出条件と同じシーケンス番号 10 を指定し，宛先 IP アドレス 192.0.2.5 をフロー検出条件とする IPv4 QoS フローリストを設定します。
5. **(config-ip-qos)# exit**
   IPv4 QoS フローリスト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)# interface gigabitethernet 1/5**
   イーサネットインタフェース 1/5 のコンフィグレーションモードに移行します。
7. **(config-if)# ip qos-flow-group PREMIUM-LIST in**

受信側に IPv4 QoS フローリスト（PREMIUM-LIST）を適用します。

14.3　オペレーション

14.3.1　運用コマンド一覧

ポリサーの運用コマンド一覧を次の表に示します。

表 14-6　運用コマンド一覧

コマンド名	説明
show qos-flow	QoS フローの設定内容と統計情報を表示します。
show policer	ポリサーの設定内容と統計情報を表示します。
clear policer	ポリサーの統計情報を 0 クリアします。
restart filter-qosflow※	QoS フローを設定するフィルタ・QoS フロー制御プログラムを再起動します。
dump filter-qosflow※	QoS フローを設定するフィルタ・QoS フロー制御プログラムで採取している制御情報をファイルへ出力します。

注※

「運用コマンドレファレンス Vol.2」「10　フィルタ・QoS 共通」を参照してください。

14.3.2　最大帯域監視の確認

最大帯域監視は show qos-flow コマンドと show policer コマンドで確認できます。show qos-flow コマンドを実行して，QoS フローの統計情報に「refer to policer statistics」が表示されることを確認します。そのあと，show policer コマンドを実行してポリサーの統計情報を確認します。

図 14-5　show qos-flow コマンドの実行結果

```
> show qos-flow interface gigabitethernet 1/1 in
Date 20XX/01/01 12:00:00 UTC
Using interface : gigabitethernet 1/1 in
IP qos-flow-list : QOS-LIST1
      10 ip any host 192.0.2.10 action policer POLICER-1
         refer to policer statistics
```

QOS-LIST1 のリスト情報にポリサーエントリ（POLICER-1）と「refer to policer statistics」が表示されることを確認します。

図 14-6　show policer コマンドの実行結果

```
> show policer POLICER-1
Date 20XX/01/01 12:00:00 UTC
policer POLICER-1 in
   max-rate 500M max-burst 100k
      Total                    Matched packets
         Max-rate over  :              146723
         Max-rate under :          2118673486
      PSU 1                    Matched packets
         Max-rate over  :              146723
         Max-rate under :          2118673486
```

POLICER-1 の情報に次の項目が表示されることを確認します。

- 最大帯域監視の監視帯域：max-rate 500M
- 最大帯域監視のバーストサイズ：max-burst 100k

違反フレームは Max-rate over の Matched packets で確認します。遵守フレームは Max-rate under の Matched packets で確認します。

14.3.3　最低帯域監視違反時の廃棄クラスの確認

最低帯域監視違反時の廃棄クラスは show qos-flow コマンドと show policer コマンドで確認できます。show qos-flow コマンドを実行して，QoS フローの統計情報に「refer to policer statistics」が表示されることを確認します。そのあと，show policer コマンドを実行してポリサーの統計情報を確認します。

図 14-7　show qos-flow コマンドの実行結果

```
> show qos-flow interface gigabitethernet 1/3 out
Date 20XX/01/01 12:00:00 UTC
Using interface : gigabitethernet 1/3 out
IP qos-flow-list : QOS-LIST2
      10 ip any host 192.0.2.10 action policer POLICER-2
         refer to policer statistics
```

QOS-LIST2 のリスト情報にポリサーエントリ（POLICER-2）と「refer to policer statistics」が表示されることを確認します。

図 14-8　show policer コマンドの実行結果

```
> show policer POLICER-2
Date 20XX/01/01 12:00:00 UTC
policer POLICER-2 out
   min-rate 300M min-burst 80k penalty-discard-class 2
      Total                  Matched packets
         Min-rate over  :              146723
         Min-rate under :          2118673486
      PSU 1                  Matched packets
         Min-rate over  :              146723
         Min-rate under :          2118673486
```

POLICER-2 の情報に次の項目が表示されることを確認します。

- 最低帯域監視の監視帯域：min-rate 300M
- 最低帯域監視のバーストサイズ：min-burst 80k
- 違反フレームの廃棄クラス：penalty-discard-class 2

違反フレームは Min-rate over の Matched packets で確認します。遵守フレームは Min-rate under の Matched packets で確認します。

14.3.4　最低帯域監視違反時の DSCP 書き換えの確認

最低帯域監視違反時の DSCP 書き換えは show qos-flow コマンドと show policer コマンドで確認できます。show qos-flow コマンドを実行して，QoS フローの統計情報に「refer to policer statistics」が表示されることを確認します。そのあと，show policer コマンドを実行してポリサーの統計情報を確認します。

図 14-9　show qos-flow コマンドの実行結果

```
> show qos-flow interface gigabitethernet 1/3.100 in
Date 20XX/01/01 12:00:00 UTC
Using interface : gigabitethernet 1/3.100 in
IP qos-flow-list : QOS-LIST3
      10 ip any host 192.0.2.10 action policer POLICER-3
         refer to policer statistics
```

QOS-LIST3 のリスト情報にポリサーエントリ（POLICER-3）と「refer to policer statistics」が表示されることを確認します。

図 14-10 show policer コマンドの実行結果

```
> show policer POLICER-3
Date 20XX/01/01 12:00:00 UTC
policer POLICER-3 in
   min-rate 200M min-burst 70k penalty-dscp 11
      Total                    Matched packets
         Min-rate over  :              146723
         Min-rate under :          2118673486
      PSU 1                    Matched packets
         Min-rate over  :              146723
         Min-rate under :          2118673486
```

POLICER-3 の情報に次の項目が表示されることを確認します。

- 最低帯域監視の監視帯域：min-rate 200M
- 最低帯域監視のバーストサイズ：min-burst 70k
- 違反フレームの DSCP 値：penalty-dscp 11

違反フレームは Min-rate over の Matched packets で確認します。遵守フレームは Min-rate under の Matched packets で確認します。

14.3.5 最大帯域監視と最低帯域監視の組み合わせの確認

最大帯域監視と最低帯域監視の組み合わせは show qos-flow コマンドと show policer コマンドで確認できます。show qos-flow コマンドを実行して，QoS フローの統計情報に「refer to policer statistics」が表示されることを確認します。そのあと，show policer コマンドを実行してポリサーの統計情報を確認します。

図 14-11 show qos-flow コマンドの実行結果

```
> show qos-flow interface port-channel 20.200 in
Date 20XX/01/01 12:00:00 UTC
Using interface : port-channel 20.200 in
IP qos-flow-list : QOS-LIST4
      10 ip any host 192.0.2.10 action policer POLICER-4
         refer to policer statistics
```

QOS-LIST4 のリスト情報にポリサーエントリ（POLICER-4）と「refer to policer statistics」が表示されることを確認します。

図 14-12 show policer コマンドの実行結果

```
> show policer POLICER-4
Date 20XX/01/01 12:00:00 UTC
policer POLICER-4 in
   max-rate 800M max-burst 120k min-rate 300M min-burst 70k penalty-dscp af23(22)
      Total                    Matched packets
         Max-rate over  :              502491
         Min-rate over  :            64729081
         Min-rate under :          2883808952
      PSU 1                    Matched packets
         Max-rate over  :               26834
         Min-rate over  :              146723
         Min-rate under :          2118673486
      PSU 3                    Matched packets
         Max-rate over  :              475657
         Min-rate over  :            64582358
         Min-rate under :           765135484
```

POLICER-4 の情報に次の項目が表示されることを確認します。

- 最大帯域監視の監視帯域：max-rate 800M
- 最大帯域監視のバーストサイズ：max-burst 120k

- 最低帯域監視の監視帯域：min-rate 300M
- 最低帯域監視のバーストサイズ：min-burst 70k
- 違反フレームの DSCP 値：penalty-dscp 22

最大帯域監視の違反フレームは Max-rate over の Matched packets で確認します。また，最低帯域監視の違反フレームは Min-rate over の Matched packets，最低帯域監視の遵守フレームは Min-rate under の Matched packets で確認します。

14.3.6　集約ポリサーによる最大帯域監視の確認

集約ポリサーによる最大帯域監視は show qos-flow コマンドと show policer コマンドで確認できます。show qos-flow コマンドを実行して，QoS フローの統計情報に「refer to policer statistics」が表示されることを確認します。そのあと，show policer コマンドを実行してポリサーの統計情報を確認します。

図 14-13　show qos-flow コマンドの実行結果

```
> show qos-flow interface gigabitethernet 1/3 in
Date 20XX/01/01 12:00:00 UTC
Using interface : gigabitethernet 1/3 in
IP qos-flow-list : QOS-LIST5
      10 tcp(6) any any eq http(80) action policer POLICER-5
         refer to policer statistics
      20 tcp(6) any any eq ftp(21) action policer POLICER-5
         refer to policer statistics

> show qos-flow interface gigabitethernet 1/4 in
Date 20XX/01/01 12:00:00 UTC
Using interface : gigabitethernet 1/4 in
IP qos-flow-list : QOS-LIST5
      10 tcp(6) any any eq http(80) action policer POLICER-5
         refer to policer statistics
      20 tcp(6) any any eq ftp(21) action policer POLICER-5
         refer to policer statistics
```

QOS-LIST5 のリスト情報にポリサーエントリ（POLICER-5）と「refer to policer statistics」が表示されることを確認します。

図 14-14　show policer コマンドの実行結果

```
> show policer POLICER-5
Date 20XX/01/01 12:00:00 UTC
policer POLICER-5 in
   max-rate 800M max-burst 200k
      Total                    Matched packets
         Max-rate over  :              2745392
         Max-rate under :            125343477
      PSU 1                    Matched packets
         Max-rate over  :              2745392
         Max-rate under :            125343477
```

POLICER-5 の情報に次の項目が表示されることを確認します。

- 最大帯域監視の監視帯域：max-rate 800M
- 最大帯域監視のバーストサイズ：max-burst 200k

ポリサーエントリ（POLICER-5）を指定した複数フローの違反フレームは Max-rate over の Matched packets で確認します。遵守フレームは Max-rate under の Matched packets で確認します。

14.3.7　重要フロー保護による最大帯域監視の確認

重要フロー保護による最大帯域監視は，show qos-flow コマンドと show policer コマンドで確認できます。show qos-flow コマンドを実行して，QoS フローの統計情報に「refer to policer statistics」が表示されることを確認します。そのあと, show policer コマンドを実行してポリサーの統計情報を確認します。

図 14-15　show qos-flow コマンドの実行結果

```
> show qos-flow interface gigabitethernet 1/5 in
Date 20XX/01/01 12:00:00 UTC
Using interface : gigabitethernet 1/5 in
IP qos-flow-list : PREMIUM-LIST
      10 ip any range-address 192.0.2.1 192.0.2.10 action policer POLICER-6
         refer to policer statistics
      10 premium ip any host 192.0.2.5
         refer to policer statistics
```

PREMIUM-LIST のリスト情報に，通常フロー検出条件でポリサーエントリ（POLICER-6）が表示されること，同じシーケンス番号で重要フロー検出条件が表示されること，それぞれに「refer to policer statistics」が表示されることを確認します。

図 14-16　show policer コマンドの実行結果

```
> show policer POLICER-6
Date 20XX/01/01 12:00:00 UTC
policer POLICER-6 in
   max-rate 500M max-burst 100k
      Total                    Matched packets
         Max-rate over  :              146723
         Max-rate under :          2118673486
      PSU 1                    Matched packets
         Max-rate over  :              146723
         Max-rate under :          2118673486
   premium
      Total                    Matched packets
         Max-rate over  :               35271
         Max-rate under :           161129543
      PSU 1                    Matched packets
         Max-rate over  :               35271
         Max-rate under :           161129543
```

POLICER-6 の情報に次の項目が表示されることを確認します。

- 最大帯域監視の監視帯域：max-rate 500M
- 最大帯域監視のバーストサイズ：max-burst 100k
- 重要フロー項目：premium

違反フレームは Max-rate over の Matched packets で確認します。遵守フレームは Max-rate under の Matched packets で確認します。

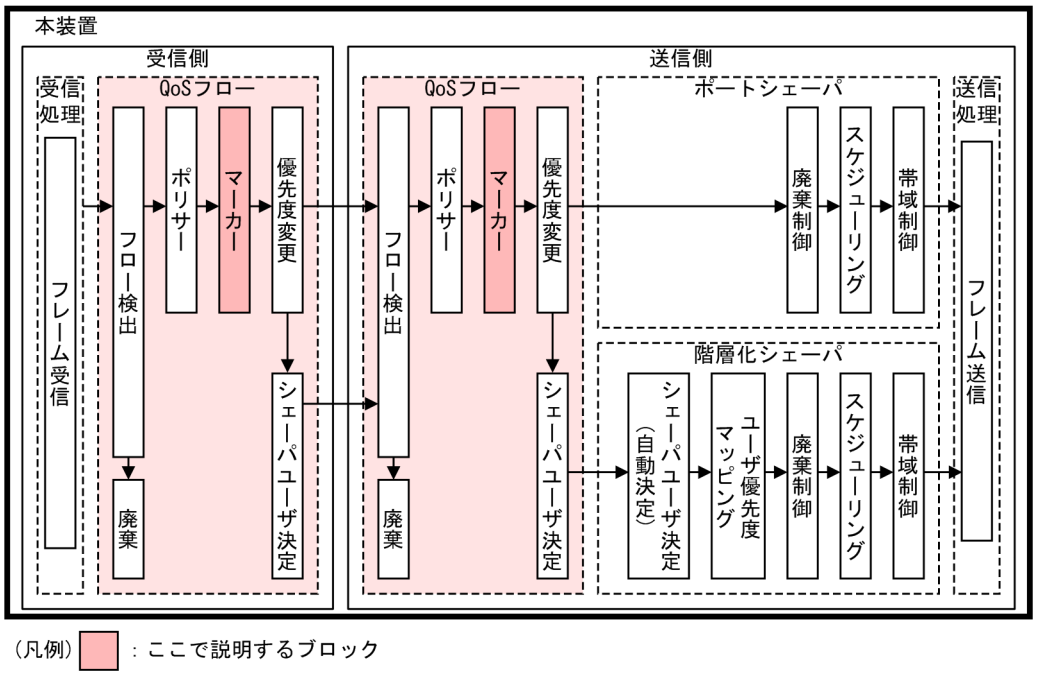
15 マーカー

マーカーは，QoS フローでフロー検出したフレームのユーザ優先度や DSCP を書き換える機能です。この章では, マーカーの解説と操作方法について説明します。

15.1　解説

マーカーは，フロー検出で検出したフレームの VLAN Tag ヘッダのユーザ優先度および IP ヘッダの DSCP 値を書き換える機能です。ここで説明するマーカーの位置づけを次の図に示します。

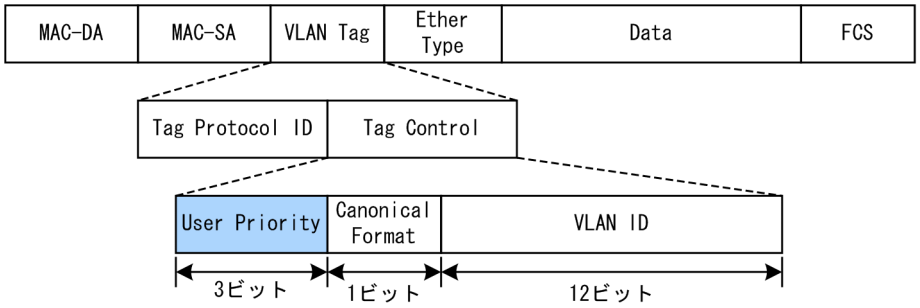
図 15-1　マーカーの位置づけ



15.1.1　ユーザ優先度書き換え

フロー検出で検出したフレームの VLAN Tag ヘッダのユーザ優先度（User Priority）を書き換える機能です。ユーザ優先度は，次の図に示す Tag Control フィールドの先頭 3 ビットを指します。

図 15-2　VLAN Tag のヘッダフォーマット



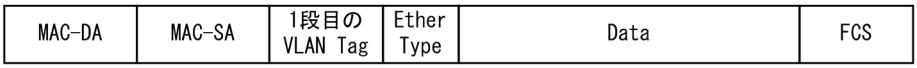
本装置がフレームを中継する場合，ユーザ優先度書き換えを使用するとユーザ優先度は書き換えた値になります。ユーザ優先度書き換えを使用しないとユーザ優先度は次のとおりです。

- レイヤ 2 中継するフレームは受信フレームの値を引き継ぎます。ただし，新規に Tag が付けられる場合は 0 になります。
- レイヤ 3 中継するパケットは 0 になります。

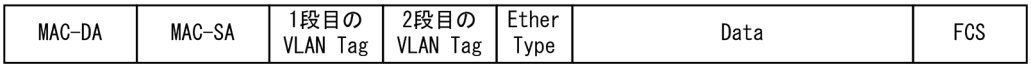
VLAN トンネリングの使用時にユーザ優先度書き換えをする，対象フレームのフレームフォーマットを次の図に示します。

図 15-3　VLAN トンネリング使用時のフレームフォーマット

（i）VLAN Tag 1段のフォーマット



（ii）VLAN Tag 2段のフォーマット



VLAN トンネリングおよびユーザ優先度書き換えを同時に実施する場合の書き換え対象について，次の表に示します。

表 15-1　VLAN トンネリングおよびユーザ優先度書き換えを同時に実施する場合の書き換え対象

中継の種類		ユーザ優先度書き換え対象の VLAN Tag
受信（VLAN Tag 数）	送信（VLAN Tag 数）	
Tag なし	1	1 段目の VLAN Tag
1	1	1 段目の VLAN Tag
1	2	1 段目の VLAN Tag
1	Tag なし	書き換え不可
2	1	1 段目の VLAN Tag

15.1.2　DSCP 書き換え

IPv4 ヘッダの TOS フィールドまたは IPv6 ヘッダのトラフィッククラスフィールドの上位 6 ビットである DSCP 値を書き換える機能です。TOS フィールドのフォーマットおよびトラフィッククラスフィールドのフォーマットの図を次に示します。

図 15-4　TOS フィールドのフォーマット

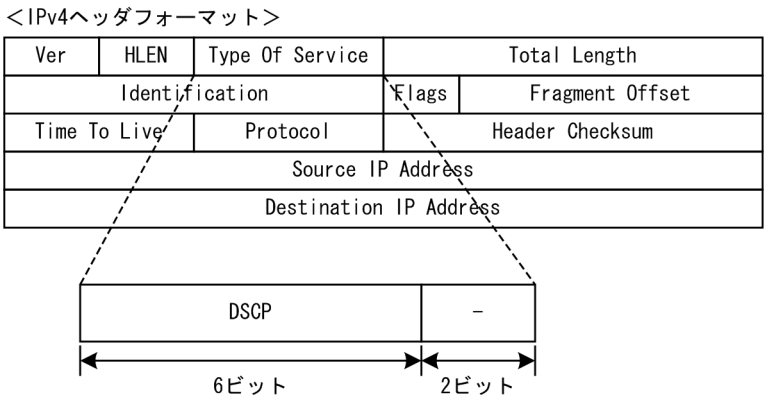
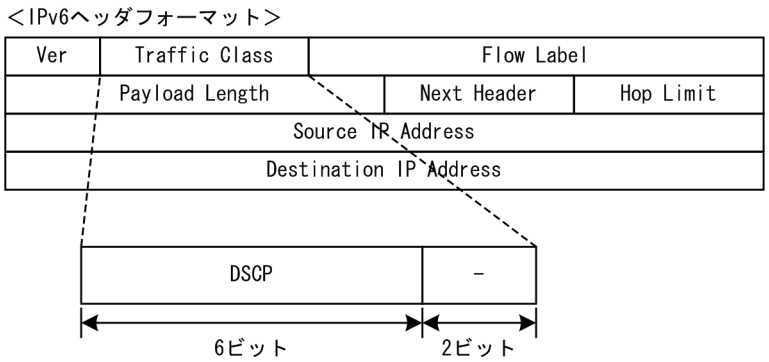


図 15-5　トラフィッククラスフィールドのフォーマット



15.1.3　マーカー使用時の注意事項

(1)　受信インタフェースおよび送信インタフェースにマーカーを指定したときの動作

送受信インタフェースにマーカーを実施するフロー検出を設定して,送受信インタフェースそれぞれに一致した場合は，送信側インタフェースのマーカーを適用して，フレームを送信します。

15.2　コンフィグレーション

15.2.1　コンフィグレーションコマンド一覧

マーカ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 15-2　コンフィグレーションコマンド一覧

コマンド名	説明
advance qos-flow-group	インタフェースに対して Advance QoS フローリストを設定して，Advance 条件による QoS 制御を適用します。
advance qos-flow-list	Advance 条件でフロー検出を行う Advance QoS フローリストを設定します。
advance qos-flow-list resequence	Advance QoS フローリストの条件適用順序のシーケンス番号を再設定します。
ip qos-flow-group	インタフェースに対して IPv4 QoS フローリストを設定して，IPv4 QoS 制御を適用します。
ip qos-flow-list	IPv4 QoS フロー検出として動作する QoS フローリストを設定します。
ip qos-flow-list resequence	IPv4 QoS フローリストの条件適用順序のシーケンス番号を再設定します。
ipv6 qos-flow-group	インタフェースに対して IPv6 QoS フローリストを設定して，IPv6 QoS 制御を適用します。
ipv6 qos-flow-list	IPv6 QoS フロー検出として動作する QoS フローリストを設定します。
ipv6 qos-flow-list resequence	IPv6 QoS フローリストの条件適用順序のシーケンス番号を再設定します。
mac qos-flow-group	インタフェースに対して MAC QoS フローリストを設定して，MAC QoS 制御を適用します。
mac qos-flow-list	MAC QoS フロー検出として動作する QoS フローリストを設定します。
mac qos-flow-list resequence	MAC QoS フローリストの条件適用順序のシーケンス番号を再設定します。
qos	QoS フローリストのフロー検出条件および動作を指定します。

15.2.2　ユーザ優先度書き換えの設定

特定のフローに対してユーザ優先度を書き換える場合の例を次に示します。

[設定のポイント]

フレーム送信時に宛先 IP アドレスによってフロー検出をして，ユーザ優先度を書き換える設定をします。

[コマンドによる設定]

1.**(config)# ip qos-flow-list QOS-LIST1**

IPv4 QoS フローリスト（QOS-LIST1）を作成します。本リストを作成すると，IPv4 QoS フローリストモードに移行します。

2. **(config-ip-qos)# qos ip any host 192.0.2.10 action replace-user-priority 6**

   192.0.2.10 の IP アドレスを宛先として，ユーザ優先度を 6 に書き換える IPv4 QoS フローリストを設定します。

3. **(config-ip-qos)# exit**

   IPv4 QoS フローリスト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 gigabitethernet 1/2.30**

   イーサネットサブインタフェース 1/2.30 のコンフィグレーションモードに移行します。

5. **(config-subif)# ip qos-flow-group QOS-LIST1 out**

   送信側に IPv4 QoS フローリスト（QOS-LIST1）を適用します。

15.2.3 DSCP 書き換えの設定

特定のフローに対して DSCP を書き換える場合の例を次に示します。

[設定のポイント]

フレーム受信時に宛先 IP アドレスによってフロー検出をして，DSCP 値を書き換える設定をします。

[コマンドによる設定]

1. **(config)# ip qos-flow-list QOS-LIST2**

   IPv4 QoS フローリスト（QOS-LIST2）を作成します。本リストを作成すると，IPv4 QoS フローリストモードに移行します。

2. **(config-ip-qos)# qos ip any host 192.0.2.10 action replace-dscp 63**

   192.0.2.10 の IP アドレスを宛先として，DSCP 値を 63 に書き換える IPv4 QoS フローリストを設定します。

3. **(config-ip-qos)# exit**

   IPv4 QoS フローリスト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 port-channel 10.30**

   ポートチャネルサブインタフェース 10.30 のコンフィグレーションモードに移行します。

5. **(config-subif)# ip qos-flow-group QOS-LIST2 in**

   受信側に IPv4 QoS フローリスト（QOS-LIST2）を適用します。

15.3　オペレーション

15.3.1　運用コマンド一覧

マーカーの運用コマンド一覧を次の表に示します。

表 15-3　運用コマンド一覧

コマンド名	説明
show qos-flow	QoS フローの設定内容と統計情報を表示します。
clear qos-flow	QoS フローの統計情報を 0 クリアします。
restart filter-qosflow※	QoS フローを設定するフィルタ・QoS フロー制御プログラムを再起動します。
dump filter-qosflow※	QoS フローを設定するフィルタ・QoS フロー制御プログラムで採取している制御情報をファイルへ出力します。

注※

「運用コマンドレファレンス Vol.2」「10　フィルタ・QoS 共通」を参照してください。

15.3.2　ユーザ優先度書き換えの確認

ユーザ優先度書き換えの確認を次の図に示します。

図 15-6　ユーザ優先度書き換えの確認

```
> show qos-flow interface gigabitethernet 1/2.30 QOS-LIST1 out
Date 20XX/01/01 12:00:00 UTC
Using interface : gigabitethernet 1/2.30 out
IP qos-flow-list : QOS-LIST1
      10 ip any host 192.0.2.10 action replace-user-priority 6
                      Matched packets        Matched bytes
         Total  :             74699826         100097766840
         PSU 1  :             74699826         100097766840
```

QOS-LIST1 のリスト情報に「replace-user-priority 6」が表示されることを確認します。また，フロー検出条件に一致したフレームは Matched packets および Matched bytes で確認します。

15.3.3　DSCP 書き換えの確認

DSCP 書き換えの確認を次の図に示します。

図 15-7　DSCP 書き換えの確認

```
> show qos-flow interface port-channel 10.30 QOS-LIST2 in
Date 20XX/01/01 12:00:00 UTC
Using interface : port-channel 10.30 in
IP qos-flow-list : QOS-LIST2
      10 ip any host 192.0.2.10 action replace-dscp 63
                      Matched packets        Matched bytes
         Total  :             83436032         111804282880
         PSU 1  :             74699826         100097766840
         PSU 2  :              8736206          11706516040
```

QOS-LIST2 のリスト情報に「replace-dscp 63」が表示されることを確認します。また，フロー検出条件に一致したフレームは Matched packets および Matched bytes で確認します。

16 優先度変更

優先度変更は，QoS フローでフロー検出したフレームの優先クラスおよび廃棄クラスを変更する機能です。この章では, 優先度変更の解説と操作方法について説明します。

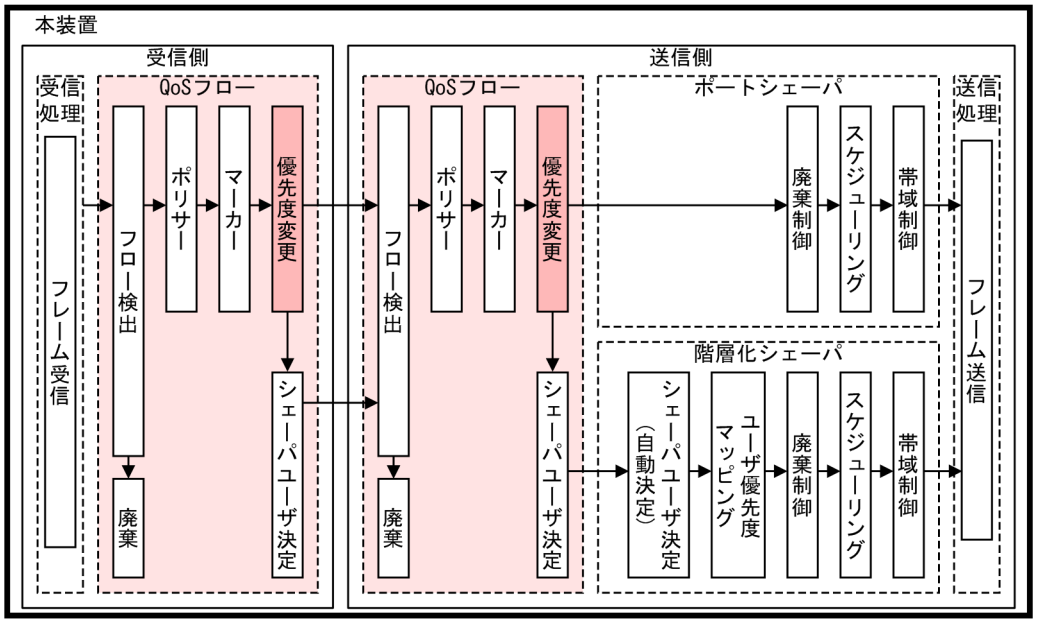
16.1　解説

優先度変更は，フロー検出で検出したフレームの優先クラスと廃棄クラスを変更する機能です。優先度変更には次に示す二つの方法があります。

- 優先クラスおよび廃棄クラスの直接指定
- DSCP マッピング

ここで説明する優先度変更の位置づけを次の図に示します。

図 16-1　優先度変更の位置づけ



（凡例）：ここで説明するブロック

優先度を変更しないフレームの優先クラスおよび廃棄クラスを次の表に示します。

表 16-1　優先度を変更しないフレームの優先クラスおよび廃棄クラス

対象フレーム	優先クラス	廃棄クラス
本装置発のフレーム（自発フレーム）	8	4
本装置を経由するフレーム（中継フレーム）	4	4

16.1.1　優先クラスおよび廃棄クラスの直接指定

検出したフローに対して，優先クラスおよび廃棄クラスを直接指定する機能です。優先クラスは，フレームをどのキューにキューイングするかを示します。廃棄クラスは，キューイングするときの廃棄されやすさの度合いを示します。優先クラスおよび廃棄クラスの指定範囲を次の表に示します。

表 16-2　優先クラスおよび廃棄クラスの指定範囲

項目	指定範囲
優先クラス	1～8

項目	指定範囲
廃棄クラス	1～4

優先クラスとキューのマッピングの関係，および廃棄クラスと廃棄優先度の関係は，「18.1　解説」を参照してください。

16.1.2　DSCP マッピング

DSCP マッピングは，フレームの DSCP 値に応じて優先クラスおよび廃棄クラスを固定的に決定する機能です。DSCP 値は，TOS フィールドまたはトラフィッククラスフィールドの上位 6 ビットを意味します。

DSCP 値に対応する優先クラスおよび廃棄クラスを次の表に示します。

表 16-3　DSCP 値に対応する優先クラスおよび廃棄クラス

DSCP 値	優先クラス	廃棄クラス
0～7	1	4
8～9	2	1
10～11		4
12～13		3
14～15		2
16～17	3	1
18～19		4
20～21		3
22～23		2
24～25	4	1
26～27		4
28～29		3
30～31		2
32～33	5	1
34～35		4
36～37		3
38～39		2
40～47	6	1
48～55	7	1
56～63	8	1

16.1.3　優先度変更使用時の注意事項

(1)　優先度変更での動作の優先順位

優先クラスおよび廃棄クラスは，直接指定または DSCP マッピングで決定します。優先度変更での優先順位を次に示します。優先順位が高いのは，数字が小さい方です。

1. 送信インタフェースに設定した，DSCP マッピング
2. 送信インタフェースに設定した，優先クラスおよび廃棄クラスの直接指定
3. 受信インタフェースに設定した，DSCP マッピング
4. 受信インタフェースに設定した，優先クラスおよび廃棄クラスの直接指定

(2)　直接指定と DSCP マッピングの併用

一つの QoS フローエントリに対して，優先クラスの直接指定と DSCP マッピングは併用できません。

(3)　DSCP 書き換えと DSCP マッピングを併用した場合の動作

一つのフローに DSCP 書き換えと DSCP マッピングを併用した場合，DSCP 書き換え後の DSCP 値に従って優先クラスおよび廃棄クラスを変更します。

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

優先度変更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
advance qos-flow-group	インタフェースに対して Advance QoS フローリストを設定して，Advance 条件による QoS 制御を適用します。
advance qos-flow-list	Advance 条件でフロー検出を行う Advance QoS フローリストを設定します。
advance qos-flow-list resequence	Advance QoS フローリストの条件適用順序のシーケンス番号を再設定します。
ip qos-flow-group	インタフェースに対して IPv4 QoS フローリストを設定して，IPv4 QoS 制御を適用します。
ip qos-flow-list	IPv4 QoS フロー検出として動作する QoS フローリストを設定します。
ip qos-flow-list resequence	IPv4 QoS フローリストの条件適用順序のシーケンス番号を再設定します。
ipv6 qos-flow-group	インタフェースに対して IPv6 QoS フローリストを設定して，IPv6 QoS 制御を適用します。
ipv6 qos-flow-list	IPv6 QoS フロー検出として動作する QoS フローリストを設定します。
ipv6 qos-flow-list resequence	IPv6 QoS フローリストの条件適用順序のシーケンス番号を再設定します。
mac qos-flow-group	インタフェースに対して MAC QoS フローリストを設定して，MAC QoS 制御を適用します。
mac qos-flow-list	MAC QoS フロー検出として動作する QoS フローリストを設定します。
mac qos-flow-list resequence	MAC QoS フローリストの条件適用順序のシーケンス番号を再設定します。
qos	QoS フローリストのフロー検出条件および動作を指定します。
remark	QoS の補足説明を記述します。

16.2.2　優先クラス変更の設定

特定のフローに対して優先クラスを変更する場合の例を次に示します。

[設定のポイント]

フレーム送信時に宛先 IP アドレスによってフロー検出をして，優先クラスを変更する設定をします。

[コマンドによる設定]

1.**(config)# ip qos-flow-list QOS-LIST1**

IPv4 QoS フローリスト（QOS-LIST1）を作成します。本リストを作成すると，IPv4 QoS フローリストモードに移行します。

2. **(config-ip-qos)# qos ip any host 192.0.2.10 action priority-class 6**

   192.0.2.10 の IP アドレスを宛先として，優先クラスを 6 に変更する IPv4 QoS フローリストを設定します。

3. **(config-ip-qos)# exit**

   IPv4 QoS フローリスト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 gigabitethernet 1/3**

   イーサネットインタフェース 1/3 のコンフィグレーションモードに移行します。

5. **(config-if)# ip qos-flow-group QOS-LIST1 out**

   送信側に IPv4 QoS フローリスト（QOS-LIST1）を適用します。

16.2.3 DSCP マッピングの設定

特定のフローに対して DSCP マッピングによって優先クラスおよび廃棄クラスを変更する場合の例を次に示します。

[設定のポイント]

フレーム受信時に宛先 IP アドレスによってフロー検出をして，DSCP マッピングによって優先クラスおよび廃棄クラスを変更する設定をします。

[コマンドによる設定]

1. **(config)# ip qos-flow-list QOS-LIST2**

   IPv4 QoS フローリスト（QOS-LIST2）を作成します。本リストを作成すると，IPv4 QoS フローリストモードに移行します。

2. **(config-ip-qos)# qos ip any host 192.0.2.10 action dscp-map**

   192.0.2.10 の IP アドレスを宛先として，DSCP マッピングによって優先クラスおよび廃棄クラスを変更する IPv4 QoS フローリストを設定します。

3. **(config-ip-qos)# exit**

   IPv4 QoS フローリスト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 gigabitethernet 1/3.50**

   イーサネットサブインタフェース 1/3.50 のコンフィグレーションモードに移行します。

5. **(config-subif)# ip qos-flow-group QOS-LIST2 in**

   受信側に IPv4 QoS フローリスト（QOS-LIST2）を適用します。

16.3　オペレーション

16.3.1　運用コマンド一覧

優先度変更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 qos-flow	QoS フローの設定内容と統計情報を表示します。
clear qos-flow	QoS フローの統計情報を 0 クリアします。
restart filter-qosflow※	QoS フローを設定するフィルタ・QoS フロー制御プログラムを再起動します。
dump filter-qosflow※	QoS フローを設定するフィルタ・QoS フロー制御プログラムで採取している制御情報をファイルへ出力します。

注※

「運用コマンドレファレンス Vol.2」「10　フィルタ・QoS 共通」を参照してください。

16.3.2　優先度変更の確認

show qos queueing port コマンドで優先度変更の内容を確認できます。優先クラスの変更は, キューイングされているキュー番号で確認します。コマンドの実行結果を次に示します。

図 16-2　優先度変更の確認

```
> show qos queueing port 1/3 out
Date 20XX/01/01 12:00:00 UTC
NIF1/Port3 (Out)
 Max-queue=8
  Queue1   : Qlen=0, Peak-Qlen=0, Limit-Qlen=1023
             Drop-mode=tail-drop
   Discard           Send packet        Discard packet          Send byte
   1                           0                     0                  -
   2                           0                     0                  -
   3                           0                     0                  -
   4                           0                     0                  -
   Total                       0                     0                  0
                               :
  Queue6   : Qlen=0, Peak-Qlen=51, Limit-Qlen=1023
             Drop-mode=tail-drop
   Discard           Send packet        Discard packet          Send byte
   1                       3203665                   0                  -
   2                           0                     0                  -
   3                           0                     0                  -
   4                           0                     0                  -
   Total                   3203665                   0         4850293146
                               :
  Queue8   : Qlen=0, Peak-Qlen=0, Limit-Qlen=1023
             Drop-mode=tail-drop
   Discard           Send packet        Discard packet          Send byte
   1                           0                     0                  -
   2                           0                     0                  -
   3                           0                     0                  -
   4                           0                     0                  -
   Total                       0                     0                  0
>
```

Queue6 の値がカウントされていることを確認します。

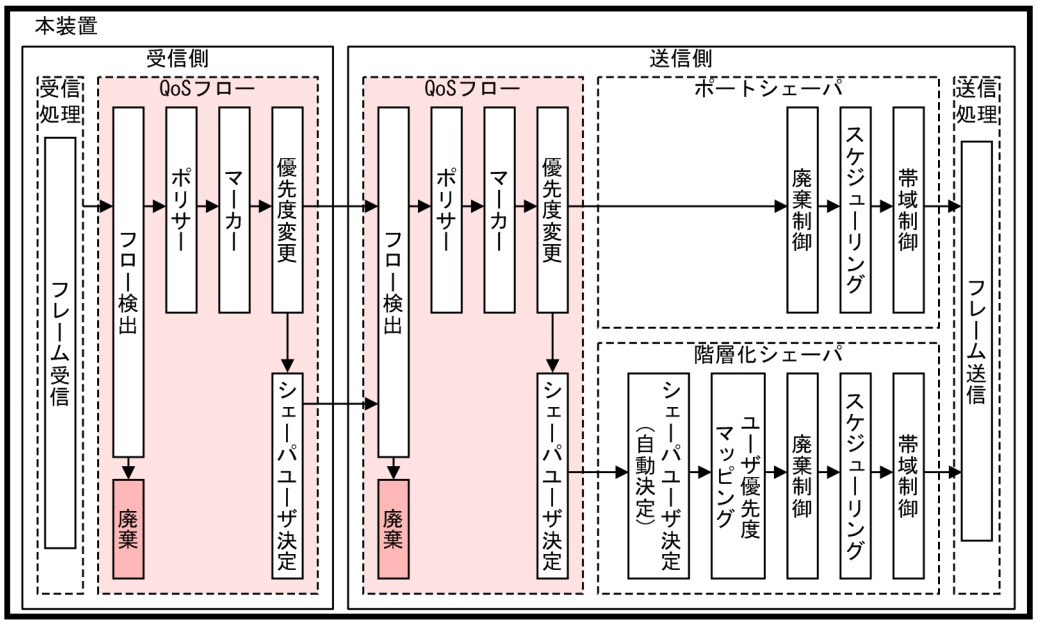
17 QoS フロー廃棄

QoS フロー廃棄は，QoS フローでフロー検出したフレームを廃棄する機能です。この章では，QoS フロー廃棄の解説と操作方法について説明します。

17.1　解説

QoS フロー廃棄は，フロー検出で検出したフローを廃棄する機能です。ここで説明する QoS フロー廃棄の位置づけを次の図に示します。

図 17-1　QoS フロー廃棄の位置づけ



17.1.1　概要

QoS フロー廃棄では，フロー検出で検出したフレームを廃棄します。廃棄したフレームに対してはポリサー，マーカー，および優先度変更をしません。

17.1.2　特徴

QoS フロー廃棄には，次に示す三つの特徴があります。

- QoS フロー専用のフロー配分パターンでもフレームを廃棄できる
- 使用するエントリ数を抑えられる
- フレームの廃棄条件を簡単に指定できる

それぞれの特徴について，具体的に説明します。

(1)　QoS フロー専用のフロー配分パターンでもフレームを廃棄できる

QoS フロー廃棄を使用すると，フィルタを使用しないでフロー検出によってフレームを廃棄します。そのため，フロー配分パターンを QoS フロー専用で運用しているときでも，フロー検出でフレームを廃棄できます。

(2)　使用するエントリ数を抑えられる

QoS 制御と，フレームの廃棄を併用する場合，フィルタではなく QoS フロー廃棄でフレームの廃棄を設定すると，使用するエントリ数を抑えられます。次の条件を適用する場合の，フィルタとの組み合わせによる設定と QoS フロー廃棄による設定での違いを示します。

- 宛先 IP アドレスが 192.0.2.0 のフローを DSCP マッピングで優先度変更
- 宛先 IP アドレスが 192.0.2.1 のフローをマーカーで DSCP 書き換え
- その他のフローを廃棄

(a)　フィルタとの組み合わせによる設定

フィルタと組み合わせて設定する場合は，パケットの中継および廃棄をフィルタで設定して，優先度変更および DSCP 書き換えを QoS フローで設定します。フィルタと組み合わせて設定する場合の例を次の図に示します

図 17-2　フィルタと組み合わせて設定する場合の例

```
(config)# ip access-list extended FILTER1                              <-1
(config-ext-nacl)# 10 permit ip any host 192.0.2.0                     <-2
(config-ext-nacl)# 20 permit ip any host 192.0.2.1                     <-3
(config-ext-nacl)# 30 deny ip any any                                  <-4
(config-ext-nacl)# exit
(config)# ip qos-flow-list QOS-LIST1                                   <-5
(config-ip-qos)# 10 qos ip any host 192.0.2.0 action dscp-map          <-6
(config-ip-qos)# 20 qos ip any host 192.0.2.1 action replace-dscp 63   <-7
(config-ip-qos)# exit
```

1. IPv4 パケットフィルタの動作モードに移行します。
2. 宛先 IP アドレスが 192.0.2.0 のパケットを中継する IPv4 パケットフィルタを設定します。
3. 宛先 IP アドレスが 192.0.2.1 のパケットを中継する IPv4 パケットフィルタを設定します。
4. すべてのパケットを廃棄する IPv4 パケットフィルタを設定します。
5. IPv4 QoS フローリストモードに移行します。
6. 宛先 IP アドレスが 192.0.2.0 のパケットを DSCP マッピングで優先クラスおよび廃棄クラスを変更する，IPv4 QoS フローリストを設定します。
7. 宛先 IP アドレスが 192.0.2.1 のパケットの DSCP 値を 63 に書き換える，IPv4 QoS フローリストを設定します。

この FILTER1 および QOS-LIST1 をインタフェースに適用した場合，フィルタ 3 エントリ，QoS フロー 2 エントリで合計 5 エントリが必要です。

(b)　QoS フロー廃棄による設定

QoS フロー廃棄でフレームの廃棄を設定する場合は，すべての条件を QoS フローで設定します。QoS フロー廃棄で設定する場合の例を次の図に示します。

図 17-3　QoS フロー廃棄で設定する場合の例

```
(config)# ip qos-flow-list QOS-LIST2                                   <-1
(config-ip-qos)# 10 qos ip any host 192.0.2.0 action dscp-map          <-2
(config-ip-qos)# 20 qos ip any host 192.0.2.1 action replace-dscp 63   <-3
(config-ip-qos)# 30 qos ip any any action drop                         <-4
(config-ip-qos)# exit
```

1. IPv4 QoS フローリストモードに移行します。

2. 宛先 IP アドレスが 192.0.2.0 のパケットを DSCP マッピングで優先クラスおよび廃棄クラスを変更する，IPv4 QoS フローリストを設定します。
3. 宛先 IP アドレスが 192.0.2.1 のパケットの DSCP 値を 63 に書き換える，IPv4 QoS フローリストを設定します。
4. すべてのパケットを廃棄する IPv4 QoS フローリストを設定します。

この QOS-LIST2 をインタフェースに適用した場合，QoS フロー 3 エントリに抑えられます。

(3)　フレームの廃棄条件を簡単に指定できる

複合条件でフレームを廃棄する場合，フィルタによる廃棄と QoS フロー廃棄を組み合わせると，フレームの廃棄条件を簡単に指定できます。次の条件を適用する場合の，フレームの廃棄にフィルタだけを使用する設定，QoS フロー廃棄だけを使用する設定，フィルタと QoS フロー廃棄を併用する設定での違いを示します。

- 宛先 IP アドレスが 192.0.2.0～192.0.2.2 かつ TCP の送信元ポート番号が 1～4 のフローを中継しつつ，送信元ポート番号に応じて優先クラスを 1～4 に変更
- その他のフローを廃棄

(a)　フレームの廃棄にフィルタだけを使用する設定

フレームの廃棄にフィルタだけを使用する場合は，フィルタのフロー検出条件に IPv4 ヘッダの送信元 IP アドレスと IPv4-TCP ヘッダの送信元ポート番号を設定します。フレームの廃棄をフィルタだけで設定する場合の例を次の図に示します。

図 17-4　フレームの廃棄をフィルタだけで設定する場合の例

```
(config)# ip access-list extended FILTER1                              <-1
(config-ext-nacl)# 10 permit tcp host 192.0.2.0 eq 1 any              ┐
(config-ext-nacl)# 20 permit tcp host 192.0.2.0 eq 2 any              │
(config-ext-nacl)# 30 permit tcp host 192.0.2.0 eq 3 any              │
(config-ext-nacl)# 40 permit tcp host 192.0.2.0 eq 4 any              │
(config-ext-nacl)# 50 permit tcp host 192.0.2.1 eq 1 any              │
(config-ext-nacl)# 60 permit tcp host 192.0.2.1 eq 2 any              │ <-2
(config-ext-nacl)# 70 permit tcp host 192.0.2.1 eq 3 any              │
(config-ext-nacl)# 80 permit tcp host 192.0.2.1 eq 4 any              │
(config-ext-nacl)# 90 permit tcp host 192.0.2.2 eq 1 any              │
(config-ext-nacl)# 100 permit tcp host 192.0.2.2 eq 2 any             │
(config-ext-nacl)# 110 permit tcp host 192.0.2.2 eq 3 any             │
(config-ext-nacl)# 120 permit tcp host 192.0.2.2 eq 4 any             ┘
(config-ext-nacl)# 130 deny ip any any                                 <-3
(config-ext-nacl)# exit
(config)# ip qos-flow-list QOS-LIST1                                   <-4
(config-ip-qos)# 10 qos tcp any eq 1 any action priority-class 1      ┐
(config-ip-qos)# 20 qos tcp any eq 2 any action priority-class 2      │ <-5
(config-ip-qos)# 30 qos tcp any eq 3 any action priority-class 3      │
(config-ip-qos)# 40 qos tcp any eq 4 any action priority-class 4      ┘
(config-ip-qos)# exit
```

1. IPv4 パケットフィルタの動作モードに移行します。
2. 送信元 IP アドレスと送信元ポート番号に応じた IPv4 パケットフィルタを設定します。
3. すべてのパケットを廃棄する IPv4 パケットフィルタを設定します。
4. IPv4 QoS フローリストモードに移行します。
5. 送信元ポート番号に応じてパケットの優先クラスを変更する，IPv4 QoS フローリストを設定します。

この FILTER1 および QOS-LIST1 を同じインタフェースに適用すると動作します。

(b)　フレームの廃棄に QoS フロー廃棄だけを使用する設定

フレームの廃棄に QoS フロー廃棄だけを使用する場合は，QoS フローのフロー検出条件に IPv4 ヘッダの送信元 IP アドレスと IPv4-TCP ヘッダの送信元ポート番号を設定します。フレームの廃棄を QoS フロー廃棄だけで設定する場合の例を次の図に示します。

図 17-5　フレームの廃棄を QoS フロー廃棄だけで設定する場合の例

```
(config)# ip qos-flow-list QOS-LIST2                                          <-1
(config-ip-qos)# 10 qos tcp host 192.0.2.0 eq 1 any action priority-class 1   ┐
(config-ip-qos)# 20 qos tcp host 192.0.2.0 eq 2 any action priority-class 2   │
(config-ip-qos)# 30 qos tcp host 192.0.2.0 eq 3 any action priority-class 3   │
(config-ip-qos)# 40 qos tcp host 192.0.2.0 eq 4 any action priority-class 4   │
(config-ip-qos)# 50 qos tcp host 192.0.2.1 eq 1 any action priority-class 1   │
(config-ip-qos)# 60 qos tcp host 192.0.2.1 eq 2 any action priority-class 2   │ <-2
(config-ip-qos)# 70 qos tcp host 192.0.2.1 eq 3 any action priority-class 3   │
(config-ip-qos)# 80 qos tcp host 192.0.2.1 eq 4 any action priority-class 4   │
(config-ip-qos)# 90 qos tcp host 192.0.2.2 eq 1 any action priority-class 1   │
(config-ip-qos)# 100 qos tcp host 192.0.2.2 eq 2 any action priority-class 2  │
(config-ip-qos)# 110 qos tcp host 192.0.2.2 eq 3 any action priority-class 3  │
(config-ip-qos)# 120 qos tcp host 192.0.2.2 eq 4 any action priority-class 4  ┘
(config-ip-qos)# 130 qos ip any any action drop                                <-3
(config-ip-qos)# exit
```

1. IPv4 QoS フローリストモードに移行します。
2. 送信元 IP アドレスと送信元ポート番号に応じてパケットの優先クラスを変更する，IPv4 QoS フローリストを設定します。
3. すべてのパケットを廃棄する IPv4 QoS フローリストを設定します。

この QOS-LIST2 をインタフェースに適用すると動作します。

(c)　フレームの廃棄にフィルタと QoS フロー廃棄を併用する設定

フレームの廃棄にフィルタと QoS フロー廃棄を併用する場合は，フィルタのフロー検出条件には IPv4 ヘッダの送信元 IP アドレスを，QoS フローのフロー検出条件には IPv4-TCP ヘッダの送信元ポート番号を設定します。フレームの廃棄をフィルタと QoS フロー廃棄の併用で設定する場合の例を次の図に示します。

図 17-6　フレームの廃棄をフィルタと QoS フロー廃棄の併用で設定する場合の例

```
(config)# ip access-list extended FILTER2                                 <-1
(config-ext-nacl)# 10 permit ip host 192.0.2.0 any                        ┐
(config-ext-nacl)# 20 permit ip host 192.0.2.1 any                        │ <-2
(config-ext-nacl)# 30 permit ip host 192.0.2.2 any                        ┘
(config-ext-nacl)# 40 deny ip any any                                     <-3
(config-ext-nacl)# exit
(config)# ip qos-flow-list QOS-LIST3                                      <-4
(config-ip-qos)# 10 qos tcp any eq 1 any action priority-class 1          ┐
(config-ip-qos)# 20 qos tcp any eq 2 any action priority-class 2          │ <-5
(config-ip-qos)# 30 qos tcp any eq 3 any action priority-class 3          │
(config-ip-qos)# 40 qos tcp any eq 4 any action priority-class 4          ┘
(config-ip-qos)# 50 qos ip any any action drop                            <-6
(config-ip-qos)# exit
```

1. IPv4 パケットフィルタの動作モードに移行します。
2. 送信元 IP アドレスが 192.0.2.0～192.0.2.2 のパケットを中継する，IPv4 パケットフィルタを設定します。
3. すべてのパケットを廃棄する IPv4 パケットフィルタを設定します。
4. IPv4 QoS フローリストモードに移行します。
5. 送信元ポート番号に応じてパケットの優先クラスを変更する，IPv4 QoS フローリストを設定します。

6. すべてのパケットを廃棄する IPv4 QoS フローリストを設定します。

この FILTER2 および QOS-LIST3 を同じインタフェースに適用すると動作します。

このように，フィルタと QoS フロー廃棄を併用すると，簡単なフロー検出条件で設定できます。

17.2　コンフィグレーション

17.2.1　コンフィグレーションコマンド一覧

QoS フロー廃棄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 17-1　コンフィグレーションコマンド一覧

コマンド名	説明
advance qos-flow-group	インタフェースに対して Advance QoS フローリストを設定して，Advance 条件による QoS 制御を適用します。
advance qos-flow-list	Advance 条件でフロー検出を行う Advance QoS フローリストを設定します。
advance qos-flow-list resequence	Advance QoS フローリストの条件適用順序のシーケンス番号を再設定します。
ip qos-flow-group	インタフェースに対して IPv4 QoS フローリストを設定して，IPv4 QoS 制御を適用します。
ip qos-flow-list	IPv4 QoS フロー検出として動作する QoS フローリストを設定します。
ip qos-flow-list resequence	IPv4 QoS フローリストの条件適用順序のシーケンス番号を再設定します。
ipv6 qos-flow-group	インタフェースに対して IPv6 QoS フローリストを設定して，IPv6 QoS 制御を適用します。
ipv6 qos-flow-list	IPv6 QoS フロー検出として動作する QoS フローリストを設定します。
ipv6 qos-flow-list resequence	IPv6 QoS フローリストの条件適用順序のシーケンス番号を再設定します。
mac qos-flow-group	インタフェースに対して MAC QoS フローリストを設定して，MAC QoS 制御を適用します。
mac qos-flow-list	MAC QoS フロー検出として動作する QoS フローリストを設定します。
mac qos-flow-list resequence	MAC QoS フローリストの条件適用順序のシーケンス番号を再設定します。
qos	QoS フローリストのフロー検出条件および動作を指定します。
remark	QoS の補足説明を記述します。

17.2.2　QoS フロー廃棄の設定

特定のフローに対して QoS フロー廃棄をする場合の例を次に示します。

[設定のポイント]

フレーム受信時に宛先 IP アドレスによってフロー検出をして，QoS フロー廃棄をする設定をします。

[コマンドによる設定]

1.**(config)# ip qos-flow-list QOS-LIST1**

IPv4 QoS フローリスト（QOS-LIST1）を作成します。本リストを作成すると，IPv4 QoS フローリストモードに移行します。

2. **(config-ip-qos)# qos ip any host 192.0.2.10 action drop**

   宛先 IP アドレスが 192.0.2.10 のフローに対して QoS フロー廃棄を指定した，IPv4 QoS フローリストを設定します。

3. **(config-ip-qos)# exit**

   IPv4 QoS フローリスト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 gigabitethernet 1/1**

   イーサネットインタフェース 1/1 のコンフィグレーションモードに移行します。

5. **(config-if)# ip qos-flow-group QOS-LIST1 in**

   受信側に IPv4 QoS フローリスト（QOS-LIST1）を適用します。

17.3　オペレーション

17.3.1　運用コマンド一覧

QoS フロー廃棄の運用コマンド一覧を次の表に示します。

表 17-2　運用コマンド一覧

コマンド名	説明
show qos-flow	QoS フローの設定内容と統計情報を表示します。
clear qos-flow	QoS フローの統計情報を 0 クリアします。
restart filter-qosflow※	QoS フローを設定するフィルタ・QoS フロー制御プログラムを再起動します。
dump filter-qosflow※	QoS フローを設定するフィルタ・QoS フロー制御プログラムで採取している制御情報をファイルへ出力します。

注※

「運用コマンドレファレンス Vol.2」「10　フィルタ・QoS 共通」を参照してください。

17.3.2　QoS フロー廃棄の確認

QoS フロー廃棄の確認を次の図に示します。

図 17-7　QoS フロー廃棄の確認

```
> show qos-flow interface gigabitethernet 1/1 QOS-LIST1 in
Date 20XX/01/01 12:00:00 UTC
Using interface : gigabitethernet 1/1 in
IP qos-flow-list : QOS-LIST1
      10 ip any host 192.0.2.10 action drop
                      Matched packets        Matched bytes
         Total  :             74699826         100097766840
         PSU 1  :             74699826         100097766840
```

QOS-LIST1 のリスト情報に「drop」が表示されることを確認します。また，フロー検出条件に一致したフレームは Matched packets および Matched bytes で確認します。

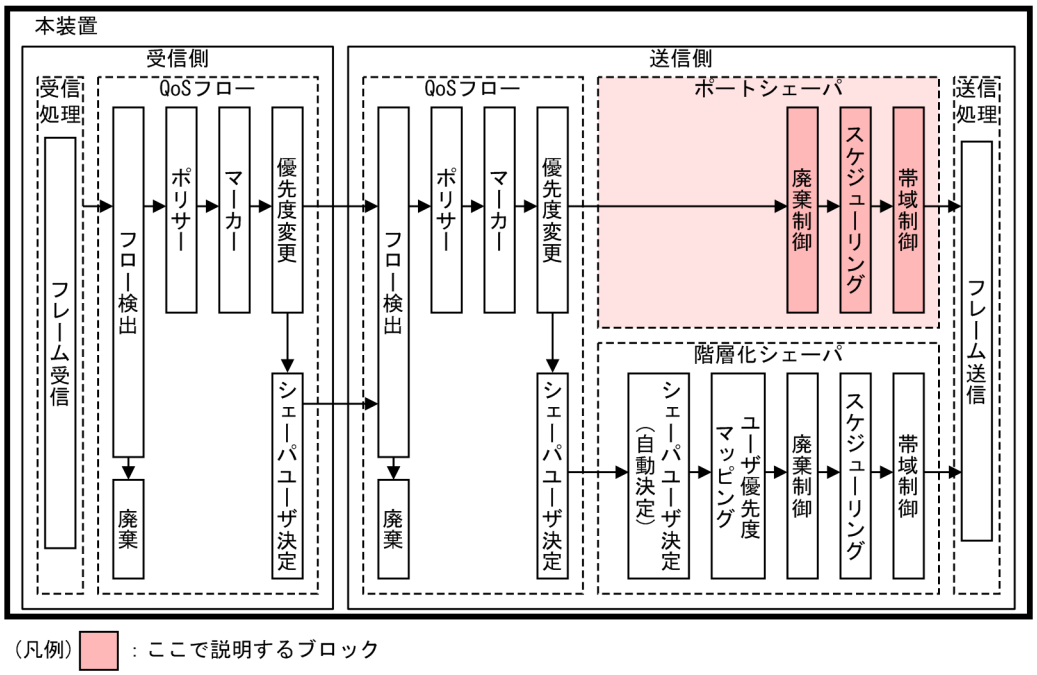
18 ポートシェーパ

ポートシェーパは，キューイング時の優先順序，各キューからのフレームの出力順序，および各ポートの出力帯域をポート単位で制御する機能です。この章では，ポートシェーパの解説と操作方法について説明します。

18.1　解説

シェーパは，キューイング時の優先順序，各キューからのフレームの出力順序，および各ポートの出力帯域を制御する機能です。シェーパには，ポートシェーパと階層化シェーパの 2 種類があります。ここではポートシェーパについて解説します。ここで説明するポートシェーパの位置づけを次の図に示します。

図 18-1　ポートシェーパの位置づけ

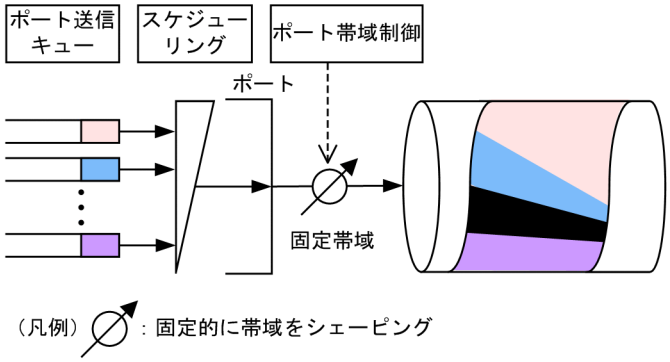


18.1.1　概要

ポートシェーパはポート送信キューで動作するシェーパ機能です。本機能はキューイングするか廃棄するかを決定する廃棄制御，どのキューにあるフレームを次に送信するかを決めるスケジューリング，およびイーサネットインタフェースの帯域をシェーピングするポート帯域制御から構成されます。

ポートシェーパの概念を次の図に示します。

図 18-2　ポートシェーパ（ポート送信キューに実装）の概念



18.1.2　廃棄制御

廃棄制御は，キューイングする各キューに対して廃棄されやすさの度合いを示す廃棄優先度と，キューにフレームが滞留している量に応じて，該当フレームをキューイングするか廃棄するかを制御する機能です。廃棄優先度は，フロー制御またはポリサーで決定した廃棄クラスによってマッピングされます。キューにフレームが滞留している状態では，廃棄優先度を適切に設定すると，さらにきめ細かな QoS を実現できます。本装置は，テールドロップ方式で廃棄制御を行います。

(1)　廃棄クラスと廃棄優先度のマッピング

廃棄優先度は，フロー制御またはポリサーで決定した廃棄クラスによってマッピングされます。廃棄クラスと廃棄優先度の関係を次の表に示します。

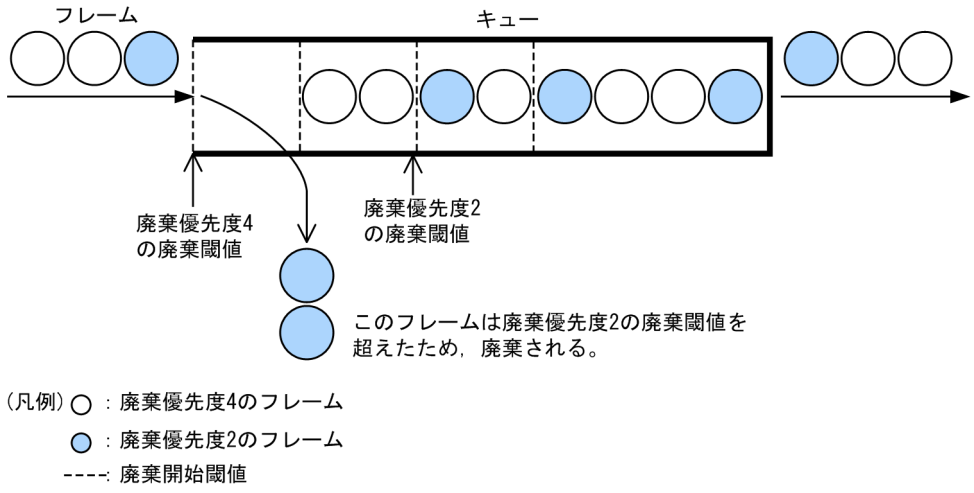
表 18-1　廃棄クラスと廃棄優先度の関係

廃棄クラス	廃棄優先度
1	1
2	2
3	3
4	4

(2)　テールドロップ

キュー長が廃棄閾値を超えると，フレームを廃棄する機能です。廃棄閾値は廃棄優先度ごとに異なり，廃棄優先度値が高いほどフレームが廃棄されにくくなります。テールドロップの概念を次の図に示します。廃棄優先度 2 の廃棄閾値を超えると，廃棄優先度 2 のフレームをすべて廃棄します。

図 18-3　テールドロップの概念



テールドロップでの廃棄優先度ごとの廃棄閾値を次の表に示します。廃棄閾値は，キュー長に対するキューのたまり具合を百分率で表します。

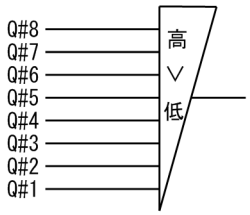
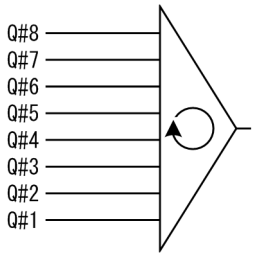
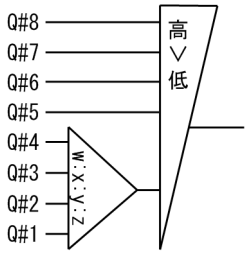
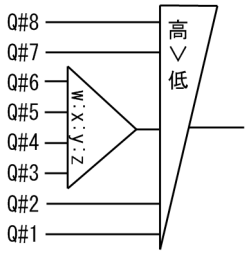
表 18-2　廃棄優先度ごとの廃棄閾値

廃棄優先度	廃棄閾値（%）
1	40
2	60
3	85
4	100

18.1.3　スケジューリング

スケジューリングは，各キューに積まれたフレームをどのような順序で送信するかを制御する機能です。本装置では，次に示すスケジューリング種別があります。スケジューリングの動作説明を次の表に示します。

表 18-3　スケジューリングの動作説明

スケジューリング種別	概念図	動作説明	適用例
PQ		完全優先制御。複数のキューにフレームがキューイングされている場合，優先度の高いキューから常にフレームを送信します。	トラフィック優先順を完全に遵守する場合
RR		ラウンドロビン。複数のキューにフレームが存在する場合，順番にキューを見ながら 1 フレームずつ送信します。フレーム長に関係なく，フレーム数が均等になるように制御します。 NL1GA-12S，NLXGA-12RS，および NLXLG-4Q では，フレーム長によって，バイト数が均等になるように制御します。	フレーム数を元に全トラフィックを均等にする場合
4PQ + 4WFQ		4 高優先キュー＋ 4 重み付き帯域均等制御。キュー 8，7，6，5（左図 Q#8，Q#7，Q#6，Q#5）までを完全優先制御します。キュー 8 から 5 にフレームが存在しない場合，あらかじめ設定した帯域の比（w：x：y：z）に応じてキュー 4，3，2，1（左図 Q#4，Q#3，Q#2，Q#1）からフレームを送信します。	PQ に優先順を完全に遵守するトラフィック WFQ に PQ の余剰帯域を使用して，帯域の比を適用するトラフィック
2PQ+4WFQ+2BEQ		2 高優先キュー＋ 4 重み付き帯域均等制御＋ 2Best Effort。キュー 8，7（左図 Q#8，Q#7）を完全優先制御します。キュー 8，7 にフレームが存在しない場合，あらかじめ設定した帯域の比（w：x：y：z）に応じてキュー 6，5，4，3（左図 Q#6，Q#5，Q#4，Q#3）からフレームを送信します。	PQ に優先順を完全に遵守するトラフィック WFQ に PQ の余剰帯域を使用して，帯域の比を適用するトラフィック

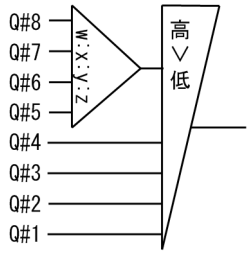
スケジューリング種別	概念図	動作説明	適用例
		キュー 8 から 3 までにフレームが存在しない場合，キュー 2，1（左図 Q#2，Q#1）で完全優先制御をします。	BEQ に PQ，WFQ の余剰帯域を使用するトラフィック
4WFQ+4BEQ		4 重み付き帯域均等制御＋ 4Best Effort。キュー 8，7，6，5（左図 Q#8，Q#7，Q#6，Q#5）であらかじめ設定した帯域の比（w：x：y：z）に応じてフレームを送信します。 キュー 8 から 5 にフレームが存在しない場合，キュー 4，3，2，1（左図 Q#4，Q#3，Q#2，Q#1）で完全優先制御をします。	WFQ に帯域の比を適用したトラフィック BEQ に WFQ の余剰帯域を使用するトラフィック

表 18-4　スケジューリングの仕様

項目		仕様	内容
キュー数	PQ RR	1，2，4，8 キュー	1，2，4，8 キューのキュー数を指定できます。キュー数を変更して，キュー長を拡張します。
	4PQ+4WFQ 2PQ+4WFQ+2BEQ 4WFQ+4BEQ	8 キュー	8 キュー固定。
4WFQ の重み	4PQ+4WFQ 2PQ+4WFQ+2BEQ 4WFQ+4BEQ	1～97%	4WFQ の重みとして帯域の比（w：x：y：z）を次の条件を満たすように設定してください。 w≧x≧y≧z かつ w+x+y+z=100

選択できるスケジューリング種別は NIF によって異なります。NIF との対応については，「18.1.6　NIF とポートシェーパとの対応」を参照してください。なお，デフォルトのスケジューリング種別は PQ です。

18.1.4　キュー数指定

キュー数指定は，ポート送信キューのキュー数を変更する機能です。デフォルトでは 8 キューです。

8 キューから 4 キュー，2 キュー，1 キューに変更すると，1 キューに割り当てるキュー長を拡張します。キュー長とは，一つのキューで使用できるパケットバッファの数です。

(1)　キュー数とキュー長の関係

キュー長は，ポート当たりのキュー数と使用する NIF によって異なります。ポート当たりのキュー数と使用する NIF による，1 キュー当たりのキュー長を次に示します。

表 18-5　1 キュー当たりのキュー長（PSU-11 または PSU-12 の場合）

NIF 型名略称	ポート当たりのキュー数			
	8 キュー時	4 キュー時	2 キュー時	1 キュー時
NL1G-12T	511	1023	2047	4095
NL1G-12S	511	1023	2047	4095

NIF 型名略称	ポート当たりのキュー数			
	8 キュー時	4 キュー時	2 キュー時	1 キュー時
NL1GA-12S	64000	128000	256000	512000
NLXG-6RS	1023	2047	4095	8191
NLXGA-12RS	64000	128000	256000	512000
NLXLG-4Q	4000	8000	16000	32000
NLCG-1Q	2047	4095	8191	16383
NMCG-1C	4095	8191	16383	32767

表 18–6　1 キュー当たりのキュー長（PSU-21 または PSU-22 の場合）

NIF 型名略称	ポート当たりのキュー数			
	8 キュー時	4 キュー時	2 キュー時	1 キュー時
NL1G-12T	1023	2047	4095	8191
NL1G-12S	1023	2047	4095	8191
NL1GA-12S	64000	128000	256000	512000
NLXG-6RS	2047	4095	8191	16383
NLXGA-12RS	64000	128000	256000	512000
NLXLG-4Q	8000	16000	32000	64000
NLCG-1Q	4095	8191	16383	32767
NMCG-1C	8191	16383	32767	65535

表 18–7　1 キュー当たりのキュー長（PSU-C1/PSU-C2/PSU-E1A/PSU-E2A/PSU-E1/PSU-E2 の場合）

NIF 型名略称	ポート当たりのキュー数			
	8 キュー時	4 キュー時	2 キュー時	1 キュー時
NL1G-12T	511	1023	2047	4095
NL1G-12S	511	1023	2047	4095
NL1GA-12S	64000	128000	256000	512000
NL1G-24T	511	1023	2047	4095
NL1G-24S	511	1023	2047	4095
NLXG-6RS	1023	2047	4095	8191
NLXGA-12RS	64000	128000	256000	512000
NLXLG-4Q	4000	8000	16000	32000
NLCG-1Q	2047	4095	8191	16383

(2)　優先クラスとキュー番号のマッピング

キューイングするキュー番号は，フロー制御で決定した優先クラスによってマッピングされます。また，キューイングするキュー番号はキュー数によって異なります。優先クラスとキューイングするキュー番号の関係を次の表に示します。

表 18-8　優先クラスとキューイングするキュー番号の関係

優先クラス	キュー数ごとのキューイングするキュー番号			
	8 キュー時	4 キュー時	2 キュー時	1 キュー時
1	1	1	1	1
2	2			
3	3	2		
4	4			
5	5	3	2	
6	6			
7	7	4		
8	8			

18.1.5　ポート帯域制御

ポート帯域制御は，スケジューリングを実施したあとに該当ポートに指定した送信帯域にシェーピングする機能です。この制御を使用して，広域イーサネットサービスなどへ接続できます。

例えば，ポート帯域が 1Gbit/s で ISP との契約帯域が 400Mbit/s の場合，ポート帯域制御を使用してあらかじめ帯域を 400Mbit/s 以下に抑えてフレームを送信できます。

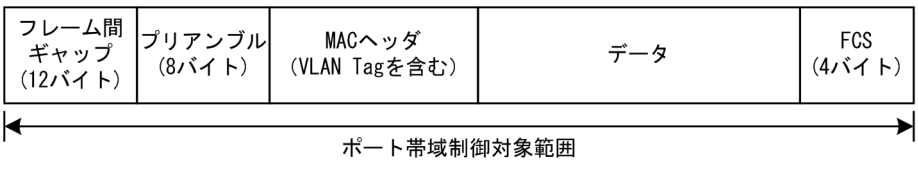
ポート帯域制御の仕様を次の表に示します。

表 18-9　ポート帯域制御の仕様

設定単位	設定範囲	刻み値
G 単位	1G～100Gbit/s	1Gbit/s
M 単位	1M～100000Mbit/s	1Mbit/s
k 単位	10k～100000000kbit/s	10kbit/s

ポート帯域制御の対象となるフレームの範囲は，フレーム間ギャップから FCS までです。ポート帯域制御の対象範囲を次の図に示します。

図 18-4　ポート帯域制御の対象範囲



18.1.6　NIF とポートシェーパとの対応

NIF とポートシェーパの各機能との対応を次の表に示します。

表 18–10　NIF とポートシェーパとの対応（1/2）

NIF 型名略称	スケジューリング				
	PQ	RR	4PQ+4WFQ	2PQ+4WFQ+2BEQ	4WFQ+4BEQ
NL1G-12T	○	○	○	○	○
NL1G-12S	○	○	○	○	○
NL1GA-12S	○	○	○	○	○
NL1G-24T	○	○	○	○	○
NL1G-24S	○	○	○	○	○
NLXG-6RS	○	○	○	○	○
NLXGA-12RS	○	○	○	○	○
NLXLG-4Q	○	○	○	○	○
NLCG-1Q	○	○	－	－	－
NMCG-1C	○	○	－	－	－

表 18–11　NIF とポートシェーパとの対応（2/2）

NIF 型名略称	キュー数指定	ポート帯域制御	廃棄制御	
			テールドロップ	廃棄優先度
NL1G-12T	○	○	○	4
NL1G-12S	○	○	○	4
NL1GA-12S	○	○	○	4
NL1G-24T	○	○	○	4
NL1G-24S	○	○	○	4
NLXG-6RS	○	○	○	4
NLXGA-12RS	○	○	○	4
NLXLG-4Q	○	○	○	4
NLCG-1Q	○	○	○	4
NMCG-1C	○	○	○	4

（凡例）　○：サポート　－：未サポート

18.1.7　ポートシェーパ使用時の注意事項

(1)　スケジューリング種別変更時の注意事項

現在のスケジューリング種別から別のスケジューリング種別に変更すると, 変更する前にキューに滞留していたフレームを廃棄します。

(2)　キュー数指定時の注意事項

キュー数指定で，現在のキュー数から別のキュー数に変更すると，変更する前にキューに滞留していたフレームを廃棄します。

(3)　半二重モードでのポート帯域制御使用時の注意事項

次に示すインタフェースでポート帯域制御を使用する場合, 送信帯域がポート帯域制御で指定した帯域にならないことがあります。

- 半二重固定を指定したイーサネットインタフェース
- オートネゴシエーションの結果，半二重となったイーサネットインタフェース

18.2　コンフィグレーション

18.2.1　コンフィグレーションコマンド一覧

ポートシェーパのコンフィグレーションコマンド一覧を次の表に示します。

表 18-12　コンフィグレーションコマンド一覧

コマンド名	説明
advance qos-flow-group	インタフェースに対して Advance QoS フローリストを設定して，Advance 条件による QoS 制御を適用します。
advance qos-flow-list	Advance 条件でフロー検出を行う Advance QoS フローリストを設定します。
ip qos-flow-group	インタフェースに対して IPv4 QoS フローリストを設定して，IPv4 QoS 制御を適用します。
ip qos-flow-list	IPv4 QoS フロー検出として動作する QoS フローリストを設定します。
ipv6 qos-flow-group	インタフェースに対して IPv6 QoS フローリストを設定して，IPv6 QoS 制御を適用します。
ipv6 qos-flow-list	IPv6 QoS フロー検出として動作する QoS フローリストを設定します。
mac qos-flow-group	インタフェースに対して MAC QoS フローリストを設定して，MAC QoS 制御を適用します。
mac qos-flow-list	MAC QoS フロー検出として動作する QoS フローリストを設定します。
qos	QoS フローリストのフロー検出条件および動作を指定します。
qos-queue-group	イーサネットインタフェースに対して QoS キューリストを適用して，シェーパを有効にします。
qos-queue-list	ポートシェーパの設定を格納する QoS キューリストにスケジューリングおよびキュー数指定を設定します。
traffic-shape rate	イーサネットインタフェースにポートシェーパのポート帯域制御を設定します。

18.2.2　スケジューリングの設定

[設定のポイント]

スケジューリングを設定した QoS キューリストを作成して，該当するイーサネットインタフェースの送信側に適用します。

[コマンドによる設定]

1. **(config)# qos-queue-list QLIST-PQ pq**

   QoS キューリスト（QLIST-PQ）にスケジューリング（PQ）を設定します。

2. **(config)# interface gigabitethernet 1/1**
   (config-if)# qos-queue-group QLIST-PQ out

   イーサネットインタフェース 1/1 のコンフィグレーションモードに移行したあと，送信側に QoS キューリスト（QLIST-PQ）を適用します。

18.2.3　キュー数指定の設定

[設定のポイント]

キュー数指定を設定した QoS キューリストを作成して，該当するイーサネットインタフェースの送信側に適用します。キュー数指定ができるスケジューリング種別は，PQ（完全優先制御）または RR（ラウンドロビン）です。

[コマンドによる設定]

1. **(config)# qos-queue-list QLIST-PQ-QNUM4 pq number_of_queue_4**
   QoS キューリスト（QLIST-PQ-QNUM4）にスケジューリング種別 PQ，キュー数 4 を設定します。
2. **(config)# interface gigabitethernet 1/11**
   (config-if)# qos-queue-group QLIST-PQ-QNUM4 out
   イーサネットインタフェース 1/11 のコンフィグレーションモードに移行したあと，送信側に QoS キューリスト（QLIST-PQ-QNUM4）を適用します。

18.2.4　ポート帯域制御の設定

該当するイーサネットインタフェースの出力帯域を，実回線の帯域より低くする場合に設定します。

[設定のポイント]

該当するイーサネットインタフェースに対して，ポート帯域制御による帯域（例では 20Mbit/s）を設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 1/12**
   (config-if)# traffic-shape rate 20M
   イーサネットインタフェース 1/12 のコンフィグレーションモードに移行したあと，ポート帯域を 20Mbit/s に設定します。

18.2.5　廃棄優先度の設定

特定の QoS フローに対して廃棄クラスを変更して，キューイング時の廃棄優先度を設定する場合の例を次に示します。

[設定のポイント]

フレーム受信時に宛先 IP アドレスによって QoS フロー検出をして，廃棄クラスを変更する設定をします。廃棄優先度は廃棄クラスによって決まります。

[コマンドによる設定]

1. **(config)# ip qos-flow-list QOS-LIST2**
   IPv4 QoS フローリスト（QOS-LIST2）を作成します。本リストを作成すると，IPv4 QoS フローリストモードに移行します。
2. **(config-ip-qos)# qos ip any host 192.0.2.10 action priority-class 8 discard-class 1**
   192.0.2.10 の IP アドレスを宛先として，優先クラス 8，廃棄クラス 1 の IPv4 QoS フローリストを設定します。
3. **(config-ip-qos)# exit**

IPv4 QoS フローリスト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 gigabitethernet 1/3**
   (config-if)# ip qos-flow-group QOS-LIST2 in
   イーサネットインタフェース 1/3 のコンフィグレーションモードに移行したあと，受信側に QoS フローリスト（QOS-LIST2）を適用します。

18.3　オペレーション

18.3.1　運用コマンド一覧

ポートシェーパの運用コマンド一覧を次の表に示します。

表 18-13　運用コマンド一覧

コマンド名	説明
show qos queueing port	ポート送受信キュー情報を表示します。
clear qos queueing port	show qos queueing port コマンドで表示するキュー統計情報を 0 クリアします。
restart filter-qosflow※	QoS フローを設定するフィルタ・QoS フロー制御プログラムを再起動します。
dump filter-qosflow※	QoS フローを設定するフィルタ・QoS フロー制御プログラムで採取している制御情報をファイルへ出力します。

注※

「運用コマンドレファレンス Vol.2」「10　フィルタ・QoS 共通」を参照してください。

18.3.2　スケジューリングの確認

NIF が NL1G-12T の場合を例として，show qos queueing port コマンドによるスケジューリングの確認を次の図に示します。

図 18-5　スケジューリングの確認

```
> show qos queueing port 1/1 out
Date 20XX/08/01 12:00:00 UTC
NIF1/Port1 (out)
 Max-queue=8, Schedule-mode=pq                                          <-1
 Port-rate-limit=100Mbps, Active-rate=100Mbps
  Queue1   : Qlen=0, Peak-Qlen=124, Limit-Qlen=511
             Drop-mode=tail-drop
   Discard        Send packets        Discard packets            Send bytes
   1                      2248                      0                     -
   2                         0                      0                     -
   3                         0                      0                     -
   4                         0                      0                     -
   Total                  2248                      0               3372732
                              :
                              :
  Queue8   : Qlen=0, Peak-Qlen=232, Limit-Qlen=511
             Drop-mode=tail-drop
   Discard        Send packets        Discard packets            Send bytes
   1                         0                      0                     -
   2                      1528                      0                     -
   3                         0                      0                     -
   4                         0                      0                     -
   Total                  1528                      0               2292210
```

1. Schedule-mode の内容が，設定したスケジューリング種別（この例では，PQ）になっていることを確認します。

18.3.3　キュー数指定の確認

NIF が NL1G-12T の場合を例として，show qos queueing port コマンドによるキュー数指定の確認を次の図に示します。

図 18-6 キュー数指定の確認

```
> show qos queueing port 1/11 out
Date 20XX/01/01 12:00:00 UTC
NIF1/Port11 (out)
 Max-queue=4, Schedule-mode=pq                                          <-1
 Port-rate-limit=100Mbps, Active-rate=100Mbps
  Queue1   : Qlen=0, Peak-Qlen=172, Limit-Qlen=1023
             Drop-mode=tail-drop
   Discard        Send packets        Discard packets           Send bytes
   1                      6225                      0                    -
   2                         0                      0                    -
   3                         0                      0                    -
   4                         0                      0                    -
   Total                  6225                      0              9207502
                               :
                               :
  Queue4   : Qlen=0, Peak-Qlen=32, Limit-Qlen=1023
             Drop-mode=tail-drop
   Discard        Send packets        Discard packets           Send bytes
   1                         0                      0                    -
   2                      1575                      0                    -
   3                         0                      0                    -
   4                         0                      0                    -
   Total                  1575                      0              2262576
```

1.Max-queue の内容が，指定したキュー数（この例では，4 キュー）になっていることを確認します。

18.3.4 ポート帯域制御の確認

NIF が NL1G-12T の場合を例として, show qos queueing port コマンドによるポート帯域制御の確認を次の図に示します。

図 18-7 ポート帯域制御の確認

```
> show qos queueing port 1/12 out
Date 20XX /01/01 12:00:00 UTC
NIF1/Port12 (out)
 Max-queue=8, Schedule-mode=pq
 Port-rate-limit=20Mbps, Active-rate=20Mbps                             <-1
  Queue1   : Qlen=0, Peak-Qlen=92, Limit-Qlen=511
             Drop-mode=tail_drop
   Discard        Send packets        Discard packets           Send bytes
   1                      2248                      0                    -
   2                         0                      0                    -
   3                         0                      0                    -
   4                         0                      0                    -
   Total                  2248                      0              3272162
                               :
                               :
  Queue8   : Qlen=0, Peak-Qlen=86, Limit-Qlen=511
             Drop-mode=tail-drop
   Discard        Send packets        Discard packets           Send bytes
   1                         0                      0                    -
   2                      1528                      0                    -
   3                         0                      0                    -
   4                         0                      0                    -
   Total                  1528                      0              2292186
```

1.Port-rate-limit および Active-rate の内容が，指定した帯域値（この例では，20Mbit/s）になっていることを確認します。

18.3.5 廃棄優先度の確認

ポートでトラフィック（Queue8 の Qlen が 511 程度の滞留が発生するトラフィック）を中継している状態として，キューイングされているキュー番号，廃棄優先度，および廃棄パケット数を確認します。対象の QoS フローは優先クラスが 8，廃棄クラスが 1 です。

NIF が NL1G-12T の場合を例として，show qos queueing port コマンドによる廃棄優先度の確認を次の図に示します。

図 18-8　廃棄優先度の確認

```
> show qos queueing port 1/11 out
Date 20XX/01/01 12:00:00 UTC
NIF1/Port11 (out)
 Max-queue=8, Schedule-mode=pq
 Port-rate-limit=100Mbps, Active-rate=100Mbps
  Queue1   : Qlen=0, Peak-Qlen=0, Limit_Qlen=511
             Drop-mode=tail-drop
   Discard        Send packets        Discard packets            Send bytes
   1                         0                      0                     -
   2                         0                      0                     -
   3                         0                      0                     -
   4                         0                      0                     -
   Total                     0                      0                     0
                             :
                             :
  Queue8   : Qlen=204, Peak-Qlen=204, Limit-Qlen=511
             Drop-mode=tail-drop
   Discard        Send packets        Discard packets            Send bytes
   1                      6533                   8245                     -
   2                         0                      0                     -
   3                         0                      0                     -
   4                         0                      0                     -
   Total                  6533                   8245               9786580
```

- Queue8 の Qlen の値がカウントされていることを確認します。
- Qlen の値が Limit-Qlen の値の 40%であり，Discard1 の Discard packets の値がカウントされていることを確認します。

19 階層化シェーパ

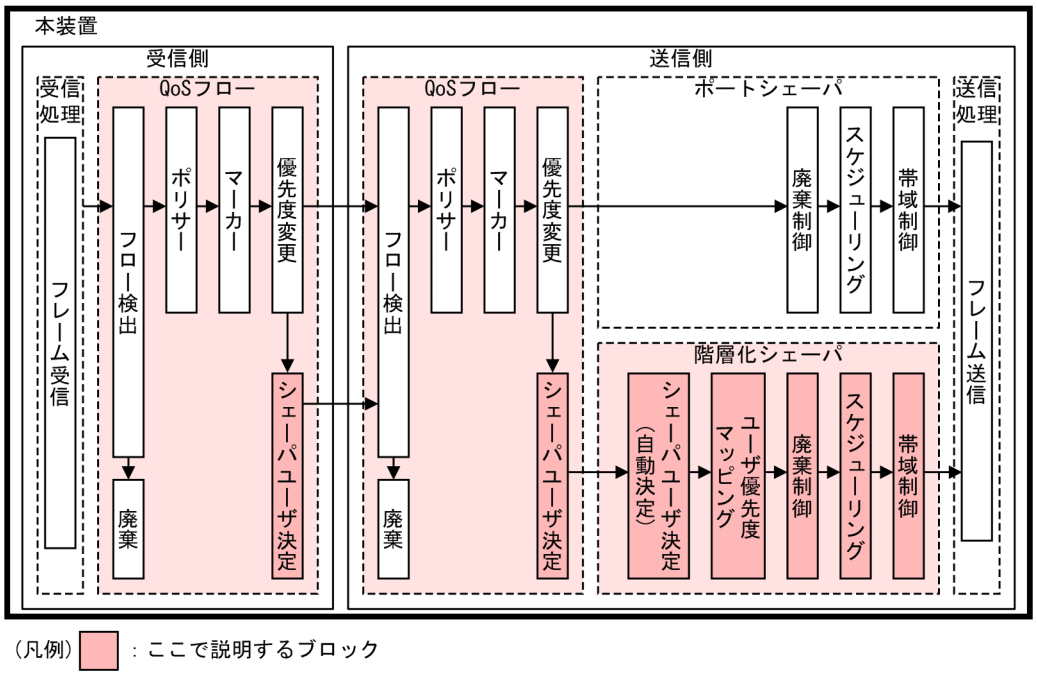
階層化シェーパは，キューイング時の優先順序，各キューからのフレームの出力順序，および出力帯域をシェーパユーザ単位ならびにポート単位で制御する機能です。この章では，階層化シェーパの解説と操作方法について説明します。

【OP-SHPS】

19.1　解説

シェーパは，キューイング時の優先順序，各キューからのフレームの出力順序，および各ポートの出力帯域を制御する機能です。シェーパには，ポートシェーパと階層化シェーパの 2 種類があります。ここでは，階層化シェーパについて解説します。階層化シェーパの位置づけを次の図に示します。

図 19-1　階層化シェーパの位置づけ



（凡例）：ここで説明するブロック

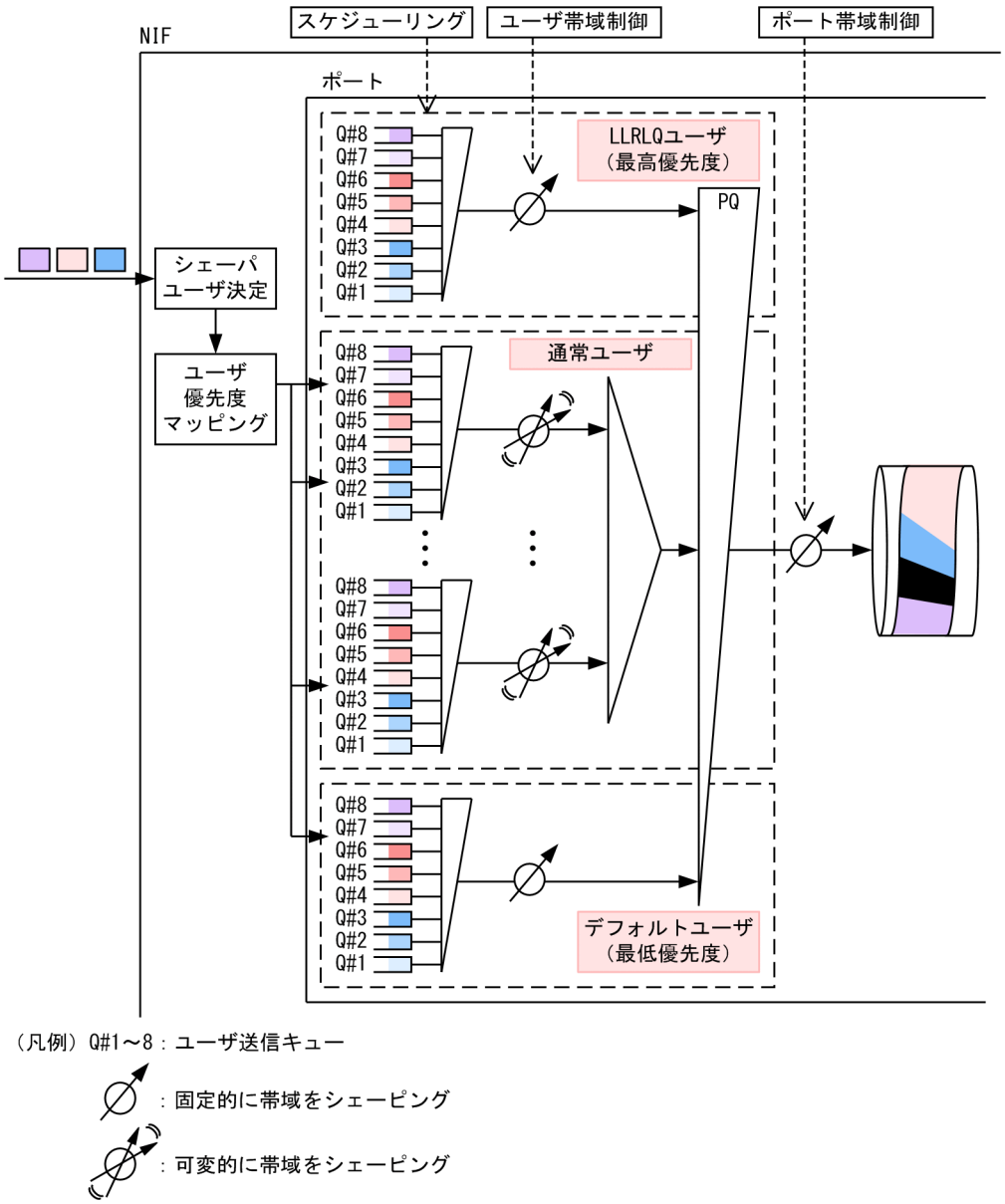
階層化シェーパは，ポート内のキューを複数まとめた単位（シェーパユーザ）と，ポート単位との 2 階層で出力帯域を制御する機能です。二つの階層で同時に制御することで，ユーザごとの帯域を守りつつ，各ユーザ内で音声パケットなどを通常パケットよりも優先的に送信するような，低遅延サービスを実現できます。

また，あらかじめ決められたルールに従って，受信フローに対応するシェーパユーザを自動的に決定します。それぞれのフローごとにシェーピングすることで，事前に予測できないバーストトラフィックを分散し，安定したデータ配信を実現できます。

19.1.1　概要

階層化シェーパは，シェーパユーザとポートとの 2 階層で出力帯域を制御します。階層化シェーパの概念を次の図に示します。

図 19-2　階層化シェーパの概念



階層化シェーパでは，キューイング時の優先順序を 2 階層で制御するために，フローをどのシェーパユーザで送信するかを決定（シェーパユーザ決定）します。さらに，シェーパユーザ内のキューイング先キュー（ユーザ送信キュー）を決定（優先度決定）し，キューイングするか廃棄するかを決定（廃棄制御）します。

各キューからのフレームの出力順序を 2 階層で制御するために，シェーパユーザ間でのフレームの送信順の制御方式（シェーパモード），各シェーパユーザのユーザ送信キューごとのフレームの送信順の制御方式（スケジューリング），およびシェーパユーザのユーザ送信キュー数やキュー長に基づいて制御します。

さらに，ポートへ送信する出力帯域を階層的にシェーピングするために，シェーパユーザごとの帯域制御（ユーザ帯域制御）とポートの合計帯域の制御（ポート帯域制御）を同時に実施しています。

階層化シェーパを動作させるためには，前述のさまざまなパラメータを設定する必要があります。本装置では，シェーパユーザワンタッチ設定機能を使用することで，階層化シェーパを簡単に使用できます。なお，シェーパユーザごとに異なる帯域やキュー長を設定したい場合は，シェーパユーザワンタッチ設定機能を使用しないで，シェーパユーザ個別設定をすることもできます。

階層化シェーパの拡張性はシェーパユーザ数に比例して高くなります。階層化シェーパ拡張モードを使用すると，NIF 単位でポート当たりの通常ユーザ数を拡張できます。【OP-SHPE】

なお，階層化シェーパ拡張モードを設定しない場合のモードを階層化シェーパ標準モードと呼びます。

階層化シェーパを動作させる NIF では，どのポートで階層化シェーパを動作させるかを設定できます。該当 NIF 内で階層化シェーパを動作させないポートではポートシェーパが動作するため，同一 NIF で階層化シェーパとポートシェーパを併用できます。

19.1.2　シェーパユーザ

シェーパユーザはポート内のキューを複数まとめたもので，階層化シェーパの帯域制御の制御単位です。本装置のシェーパユーザは 3 種類あります。シェーパユーザの種類を次の表に示します。

表 19-1　シェーパユーザの種類

シェーパユーザ	説明
LLRLQ ユーザ	最大帯域までは最優先で出力する，最高優先度のシェーパユーザです。 各ポートに一つずつ存在します。
通常ユーザ	LLRLQ ユーザの余剰帯域がある場合に，指定されたシェーパモードに従ってシェーパユーザごとに帯域を制御しながらフレームを出力するシェーパユーザです。 各ポートに複数個存在し，各通常ユーザには 1 番から始まるシェーパユーザ番号が付けられます。
デフォルトユーザ	LLRLQ ユーザおよび通常ユーザの余剰帯域がある場合にフレームを出力する，最低優先度のシェーパユーザです。 各ポートに一つずつ存在します。

19.1.3　シェーパユーザ決定

シェーパユーザ決定は，トラフィックを処理するシェーパユーザを決定する機能です。シェーパユーザ決定には，次の三つの方法があります。

- ランダム振り分け
  フレーム内情報に基づく自動計算によってシェーパユーザをランダムに決定します。
- VLAN ID マッピング
  フレームに付いた VLAN Tag の VLAN ID からシェーパユーザを一意に決定します。
- フロー検出によるシェーパユーザ決定
  QoS フローで検出したフローに対してシェーパユーザを指定することで，シェーパユーザを一意に決定します。

ランダム振り分けおよび VLAN ID マッピングについては，NIF 単位に異なるシェーパユーザ決定方法を指定できます。指定しない NIF では，すべての中継フレームがデフォルトユーザで処理されます。

フロー検出によるシェーパユーザ決定については，QoS フロー単位に指定できます。指定しない QoS フローは，すべての中継フレームがデフォルトユーザで処理されます。また，フロー検出によるシェーパユーザ決定は，ランダム振り分けおよび VLAN ID マッピングと併用できます。併用した場合は，フロー検出で決定したシェーパユーザが優先されます。

なお，本装置が自発送信する制御フレームは，ランダム振り分けおよびVLAN IDマッピングによる振り分けの対象外となり，常にLLRLQユーザに割り当てられます。フロー検出によるシェーパユーザ決定では，本装置が自発送信する制御フレームもシェーパユーザを決定できます。

(1)　ランダム振り分け

ランダム振り分けでは，指定したフレーム内の情報をキー情報として，通常ユーザをランダムに決定します。不特定多数のフローに対してマイクロバーストを抑止したい場合などに使用できます。

ランダム振り分けのキー情報として使用できるフレーム情報を次の表に示します。キー情報には，複数のフレーム情報を選択できます。

表19-2　ランダム振り分けのキー情報として使用できるフレーム情報

フレーム情報	キー情報
MACヘッダ	宛先MACアドレス
	送信元MACアドレス
VLAN Tag※	1段目のVLAN ID
	2段目のVLAN ID
IPヘッダ	宛先IPアドレス
	送信元IPアドレス
	上位プロトコル
TCP/UDPヘッダ	宛先ポート番号
	送信元ポート番号

注※
Tag変換やVLANトンネリングをする場合は，回線に送信するVLAN Tagが対象となります。

ランダム振り分けの対象となる通常ユーザの範囲は，使用するシェーパモードおよびシェーパユーザ当たりのキュー数によって異なります。シェーパモードおよびシェーパユーザ当たりのキュー数とランダム振り分けするシェーパユーザ番号の対応を次の表に示します。

表19-3　ランダム振り分け対象のシェーパユーザ番号

シェーパモード	ユーザキュー数	対象のシェーパユーザ番号の範囲	
		標準モード	拡張モード【OP-SHPE】
RGQ	8キュー	1～128	1～256
	4キュー	1～256	1～2048
LLPQ4	8キュー	1～128	1～256
LLPQ1	4キュー	1～256	1～2048

この表に示すとおり，拡張モードでシェーパユーザ数を拡張した場合，標準モードに比べてフローを同一シェーパユーザに割り当てる可能性を低くできます。【OP-SHPE】

(2)　VLAN ID マッピング

VLAN ID マッピングでは，フレームに付いた VLAN Tag の VLAN ID と同じシェーパユーザ番号の通常ユーザをマッピングします。ランダム振り分けで VLAN ID をキー情報として使った場合に比べて，一つの VLAN に一つの通常ユーザを割り当てやすい方式です。

VLAN ID マッピングに使用する VLAN ID として，1 段目の VLAN ID または 2 段目の VLAN ID のどちらかを選択できます。Tag 変換や VLAN トンネリングをする場合は，回線に送信する VLAN Tag が対象となります。該当する VLAN Tag の付いていないフレームや，シェーパユーザ番号の範囲外の VLAN ID を持つフレームは，デフォルトユーザに割り当てられます。

VLAN ID マッピングの対象となる通常ユーザの範囲は，使用するシェーパモードおよびシェーパユーザ当たりのキュー数によって異なります。シェーパモードおよびシェーパユーザ当たりのキュー数と VLAN ID マッピングするシェーパユーザ番号の対応を次の表に示します。

表 19-4　VLAN ID マッピング対象のシェーパユーザ番号

シェーパモード	ユーザキュー数	対象のシェーパユーザ番号の範囲	
		標準モード	拡張モード【OP-SHPE】
RGQ	8 キュー	1～128	1～382
	4 キュー	1～256	1～3056
LLPQ4	8 キュー	1～128	1～382
LLPQ1	4 キュー	1～256	1～3056

(3)　フロー検出によるシェーパユーザ決定

フロー検出によるシェーパユーザ決定では，QoS フローでフロー検出したフレームの送信先シェーパユーザを指定することで，シェーパユーザを決定します。QoS フローでのフロー検出については，「13　QoS フロー」を参照してください。

フロー検出によるシェーパユーザ決定は，ランダム振り分けおよび VLAN ID マッピングとは異なり，通常ユーザに加えて，LLRLQ ユーザおよびデフォルトユーザを明示的に指定することで，該当するシェーパユーザから送信できます。指定できるシェーパユーザ番号は，ほかのシェーパユーザ決定方法と同様に，使用するシェーパモードおよびシェーパユーザ当たりのキュー数によって異なります。フロー検出によるシェーパユーザ決定で指定できるシェーパユーザ番号は，VLAN ID マッピングの場合と同じです。なお，指定したシェーパユーザ番号のシェーパユーザが未設定の場合，デフォルトユーザで送信されます。

19.1.4　優先度決定

優先度決定は，どのシェーパユーザ内のユーザ送信キューからフレームを出力するかを決定する機能です。本装置では，次の 2 種類の方法で優先度を決定します。

- ユーザ優先度マッピング
  VLAN Tag の付いたフレームのユーザ優先度によって自動でキュー番号を決定します。
- フロー検出による優先度決定
  QoS フローの優先度変更によってユーザ送信キューを決定します。

(1)　ユーザ優先度マッピング

VLAN Tag の付いたフレームのユーザ優先度によって，自動でユーザ送信キュー番号を決定する方式です。

ユーザ優先度に使用する VLAN Tag として，1 段目の VLAN Tag または 2 段目の VLAN Tag のどちらかを選択できます。VLAN Tag の付いていないフレームに対してはユーザ優先度マッピングをしないで，フロー検出で決定した優先度またはデフォルトの優先度によって，ユーザ送信キュー番号を決定します。

ユーザ優先度マッピングするユーザ送信キューの番号は，使用するキュー数によって異なります。ユーザ優先度とユーザ送信キュー番号の対応を次の表に示します。

表 19-5　ユーザ優先度とユーザ送信キュー番号の対応

ユーザ優先度	ユーザ優先度で決定するユーザ送信キュー番号	
	8 キュー時	4 キュー時
0	1	1
1	2	
2	3	2
3	4	
4	5	3
5	6	
6	7	4
7	8	

(2)　フロー検出による優先度決定

QoS フローの優先度変更によってユーザ送信キューを決定します。優先度変更については，「16　優先度変更」を参照してください。

19.1.5　廃棄制御

廃棄制御は，キューイングする各フレームの廃棄優先度と，ユーザ送信キューにフレームが滞留している量に応じて，該当フレームをキューイングするか廃棄するかを制御する機能です。ユーザ送信キューにフレームが滞留している状態では，廃棄優先度を適切に設定すると，さらにきめ細かな QoS を実現できます。本装置は，テールドロップ方式で廃棄制御をします。

フレームにどの廃棄優先度が適用されるかは，フロー制御またはポリサーで決定した廃棄クラスによって決定します。廃棄優先度数は，4 または 2 のどちらかを NIF 単位に指定できます。廃棄優先度数 2 を選択した場合は，テールドロップの廃棄閾値を三つのパターンから選択できます。テールドロップの概念については，「18.1.2　廃棄制御」を参照してください。

(1)　廃棄クラスと廃棄優先度のマッピング

廃棄優先度は，フロー制御またはポリサーで決定した廃棄クラスによってマッピングされます。階層化シェーパでは，廃棄優先度数によってマッピングが異なります。廃棄クラスと廃棄優先度の関係を次の表に示します。

表 19-6　階層化シェーパでの廃棄クラスと廃棄優先度の関係

廃棄クラス	廃棄優先度	
	廃棄優先度数 4	廃棄優先度数 2
1	1	1
2	2	
3	3	2
4	4	

(2)　廃棄優先度数と廃棄閾値

階層化シェーパでの廃棄閾値は，廃棄優先度数と，廃棄優先度数 2 の場合に選択した閾値パターンによって決定します。テールドロップの廃棄優先度ごとの廃棄閾値を次の表に示します。

表 19-7　廃棄優先度ごとの廃棄閾値

廃棄優先度	廃棄閾値（%）			
	廃棄優先度数 4	廃棄優先度数 2		
		閾値パターン 1	閾値パターン 2	閾値パターン 3
1	25	25	50	75
2	50	100	100	100
3	75	−	−	−
4	100	−	−	−

（凡例）−：該当なし

19.1.6　シェーパモード

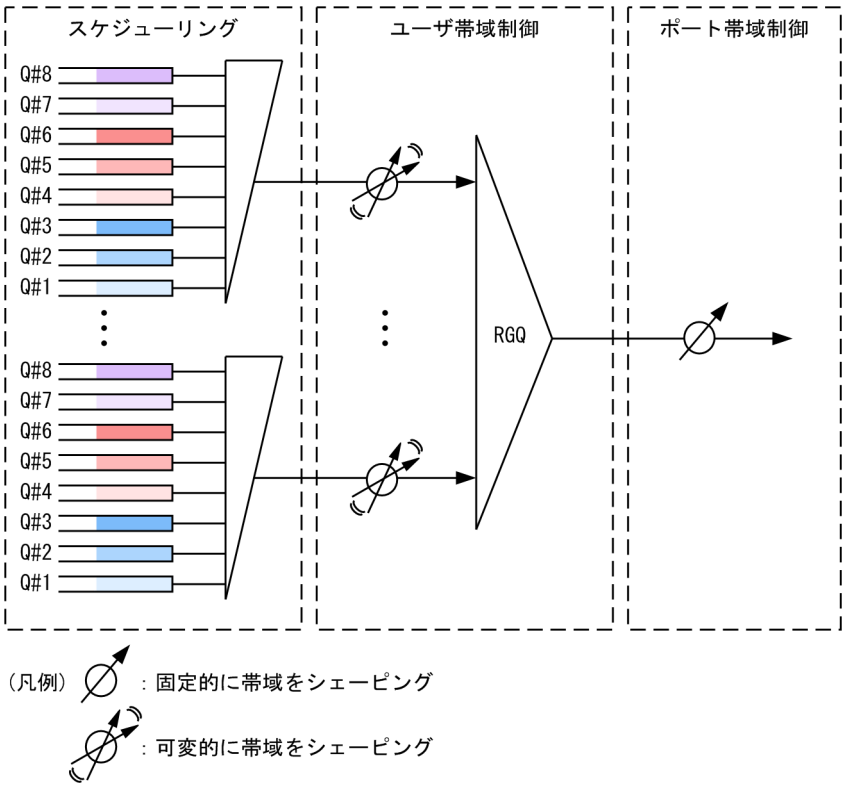
シェーパモードは，通常ユーザ間の帯域制御方式を NIF ごとに決定します。シェーパモードを設定すると，該当する NIF で階層化シェーパが有効になります。

シェーパモードには，RGQ，LLPQ1，および LLPQ4 の三つのモードがあります。シェーパモードを設定したあと，該当する NIF を再起動すると動作に反映されます。

(1)　RGQ

RGQ は通常ユーザごとの最低帯域を保証しつつ，余剰帯域がある場合は最大帯域まで使用できるようにするモードです。各通常ユーザには設定した最低帯域を分配して，さらに帯域に余剰がある場合は，重みに従った割合で各通常ユーザに帯域を最大帯域まで分配します。RGQ の概念を次の図に示します。

図 19-3　RGQ の概念



(a)　通常ユーザの重みが均等な場合

ポート帯域制御によって回線帯域を 9Gbit/s にシェーピングする場合で，重みが均等なときの帯域計算例を次の表に示します。

表 19-8　RGQ の帯域の計算例 1（回線帯域を 9Gbit/s に設定，重み均等）

シェーパユーザ	入力帯域 (Gbit/s)	最低帯域 (Gbit/s)	最大帯域 (Gbit/s)	余剰帯域※1 (Gbit/s)	余余剰帯域※2 (Gbit/s)	送信帯域※3 (Gbit/s)
通常ユーザ 1	5	2	8	1	0.25	3.25
通常ユーザ 2	3.5	2	8	1	0.25	3.25
通常ユーザ 3	2.5	2	8	0.5	0	2.5

注※1

回線内の余剰帯域＝回線帯域－各通常ユーザの最低帯域の合計＝ 9－（2 ＋ 2 ＋ 2）＝ 3（Gbit/s）

通常ユーザ 1，2，および 3 への余剰帯域の分配＝ 3×（1 ÷（1 ＋ 1 ＋ 1））＝ 1（Gbit/s）

通常ユーザ 3 への入力帯域が 2.5Gbit/s のため，余剰帯域で使用する帯域は 0.5Gbit/s だけとなります。

注※2

回線内の余剰帯域の余剰帯域（以降，余余剰帯域）＝回線帯域－各通常ユーザの最低帯域の合計－各通常ユーザの余剰帯域の合計＝ 9－（2 ＋ 2 ＋ 2）－（1 ＋ 1 ＋ 0.5）＝ 0.5（Gbit/s）

通常ユーザ 1 および 2 への余余剰帯域の分配＝ 0.5×（1 ÷（1 ＋ 1））＝ 0.25（Gbit/s）

注※3

各通常ユーザの送信帯域（最大帯域以下）＝各通常ユーザの最低帯域＋各通常ユーザに分配された余剰帯域＋各通常ユーザに分配された余余剰帯域

通常ユーザ 1 の送信帯域＝ 2 ＋ 1 ＋ 0.25 ＝ 3.25（Gbit/s）

通常ユーザ 2 の送信帯域＝ 2 ＋ 1 ＋ 0.25 ＝ 3.25（Gbit/s）
通常ユーザ 3 の送信帯域＝ 2 ＋ 0.5 ＝ 2.5（Gbit/s）

(b)　通常ユーザの重みが異なる場合

ポート帯域制御によって回線帯域を 9Gbit/s にシェーピングする場合で，ユーザ間の重みが異なり，最大帯域で制限されるときの帯域計算例を次の表に示します。

表 19-9　RGQ の帯域の計算例 2（回線帯域を 9Gbit/s に設定，重みが異なる）

シェーパユーザ	入力帯域 (Gbit/s)	最低帯域 (Gbit/s)	最大帯域 (Gbit/s)	余剰帯域※1 (Gbit/s)	余余剰帯域※2 (Gbit/s)	送信帯域※3 (Gbit/s)
通常ユーザ 1（重み 2）	5	1	8	3	0.67	4.67
通常ユーザ 2（重み 1）	3.5	1	8	1.5	0.33	2.83
通常ユーザ 3（重み 1）	2.0	1	1.5	0.5	0	1.5

注※1
回線内の余剰帯域＝回線帯域－各通常ユーザの最低帯域の合計＝ 9－（1 ＋ 1 ＋ 1）＝ 6（Gbit/s）
通常ユーザ 1 への余剰帯域の分配＝ 6×（2÷（2 ＋ 1 ＋ 1））＝ 3（Gbit/s）
通常ユーザ 2 への余剰帯域の分配＝ 6×（1÷（2 ＋ 1 ＋ 1））＝ 1.5（Gbit/s）
通常ユーザ 3 への余剰帯域の分配＝ 6×（1÷（2 ＋ 1 ＋ 1））＝ 1.5（Gbit/s）
通常ユーザ 3 への入力帯域が 2Gbit/s のため余剰帯域で使用する帯域は 1Gbit/s だけとなりますが，最大帯域が 1.5Gbit/s に制限されているため余剰帯域で使用する帯域は 0.5Gbit/s だけとなります。

注※2
回線内の余剰帯域の余剰帯域（以降，余余剰帯域）＝回線帯域－各通常ユーザの最低帯域の合計－各通常ユーザの余剰帯域の合計＝ 9－（1 ＋ 1 ＋ 1）－（3 ＋ 1.5 ＋ 0.5）＝ 1（Gbit/s）
通常ユーザ 1 への余余剰帯域の分配＝ 1×（2÷（2 ＋ 1））≒0.67（Gbit/s）
通常ユーザ 2 への余余剰帯域の分配＝ 1×（1÷（2 ＋ 1））≒0.33（Gbit/s）

注※3
各通常ユーザの送信帯域（最大帯域以下）＝各通常ユーザの最低帯域＋各通常ユーザに分配された余剰帯域＋各通常ユーザに分配された余余剰帯域
通常ユーザ 1 の送信帯域＝ 1 ＋ 3 ＋ 0.67 ＝ 4.67（Gbit/s）
通常ユーザ 2 の送信帯域＝ 1 ＋ 1.5 ＋ 0.33 ＝ 2.83（Gbit/s）
通常ユーザ 3 の送信帯域＝ 1 ＋ 0.5 ＝ 1.5（Gbit/s）

(2)　LLPQ1 および LLPQ4

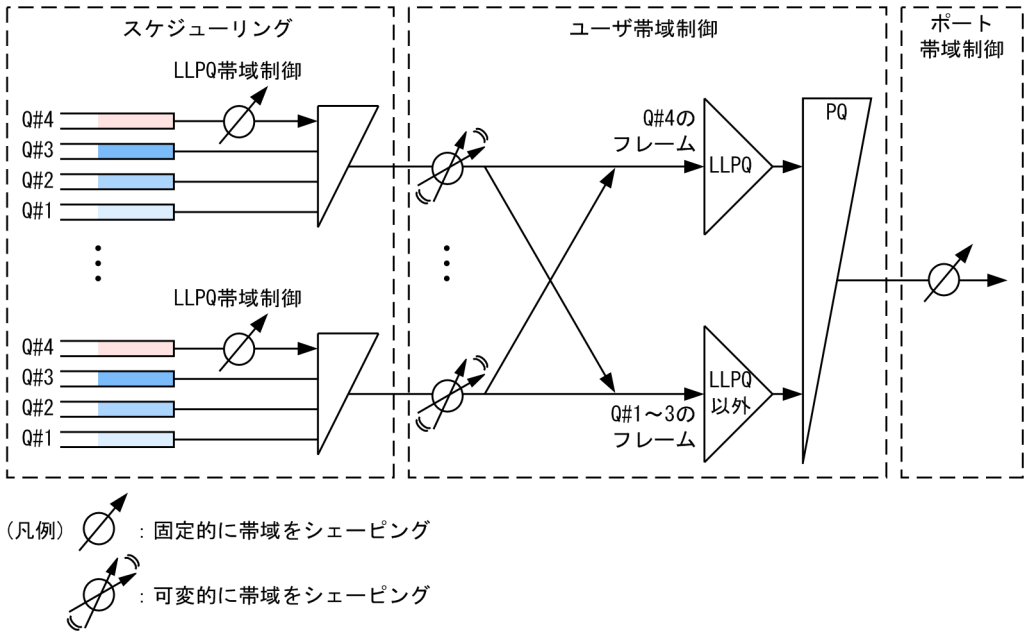
LLPQ1 および LLPQ4 の 2 モードは，LLPQ 方式で帯域を制御します。LLPQ 方式は，RGQ と同様に，通常ユーザごとの最低帯域を保証しつつ，余剰帯域がある場合は重みに従って各通常ユーザの最大帯域まで使用できるようにする方式です。RGQ との違いは次のとおりです。

- 各通常ユーザのユーザ送信キューの一部を低遅延キュー（以降 LLPQ）として，ほかの通常ユーザのユーザ送信キューより優先的に出力できる
- LLPQ に対して最大帯域を設定できる

LLPQ を使用することで，ある通常ユーザの優先したいデータが，別の通常ユーザの通常データによって遅延することを防げます。

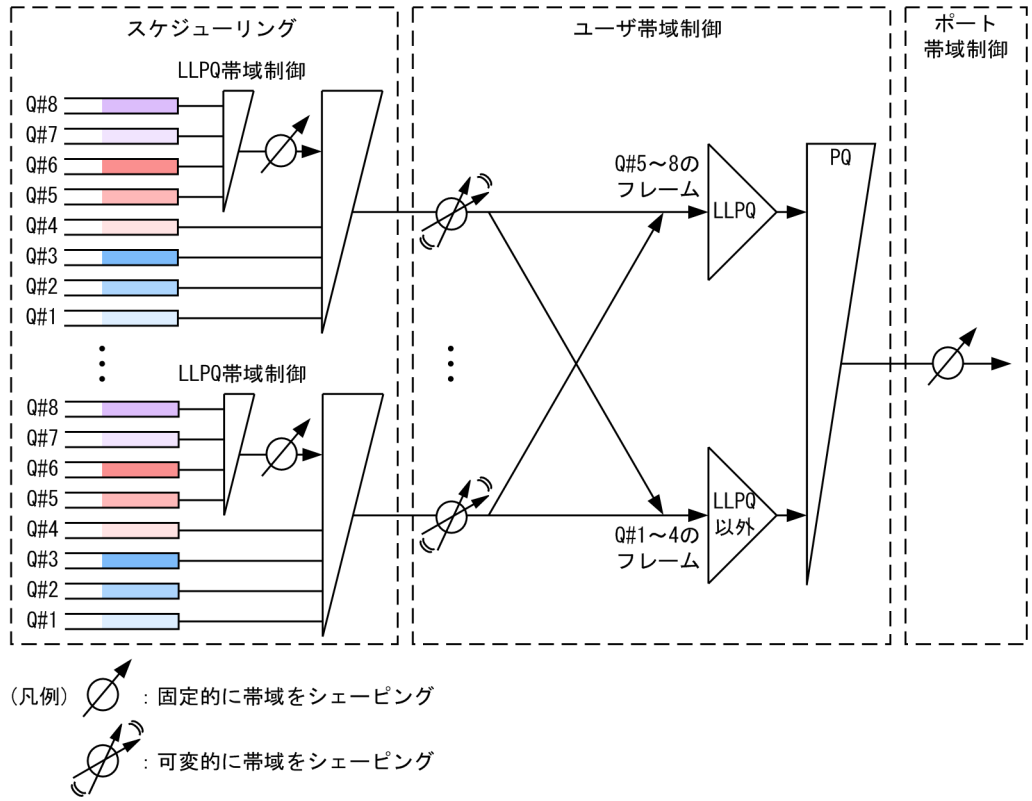
なお，LLPQ1 および LLPQ4 のシェーパモード名の数値は，LLPQ の数を示しています。LLPQ1 はユーザ当たりのキュー数が 4 キューの場合だけ使用できます。LLPQ1 の概念を次の図に示します。この図に示すとおり，Q#4 が LLPQ となります。

図 19-4　LLPQ1 の概念



LLPQ4 はユーザ当たりのキュー数が 8 キューの場合だけ使用できます。LLPQ4 の概念を次の図に示します。この図に示すとおり，Q#5～8 が LLPQ となります。

図 19-5　LLPQ4 の概念



LLPQ 方式では，各通常ユーザの LLPQ へ割り当てる帯域を分配したあと，LLPQ 以外へ割り当てる帯域を決定します。各通常ユーザの LLPQ へ割り当てる帯域は，LLPQ 最大帯域を上限とした LLPQ に対する全入力帯域になります。ただし，LLPQ へ割り当てる帯域がポート帯域を超える場合は，合計帯域がポート帯域以内になるように，各通常ユーザの LLPQ へ割り当てる帯域を均等に減らします。

LLPQ 以外のユーザ送信キューへは，次に示す 2 段階で帯域を割り当てます。

1.「各通常ユーザの最低帯域－LLPQ へ割り当てる帯域」を割り当てます。
　LLPQ へ割り当てる帯域が最低帯域より大きい場合は，この段階で帯域を割り当てません。
2. 1 段階目の帯域割り当て後に余った回線帯域を，各通常ユーザ間で均等に割り当てます。

(3)　LLRLQ ユーザ帯域がシェーパモード帯域へ与える影響

LLRLQ ユーザと組み合わせた場合の帯域計算例を次の表に示します。ここでは，通常ユーザのシェーパモードを RGQ とします。

表 19-10　LLRLQ ユーザと RGQ の帯域の計算例（回線帯域 5Gbit/s）

シェーパユーザ	入力帯域 (Gbit/s)	最低帯域 (Gbit/s)	最大帯域 (Gbit/s)	未使用帯域※1 (Gbit/s)	余剰帯域※2 (Gbit/s)	送信帯域 (Gbit/s)
LLRLQ ユーザ	1	－	2	－	－	1※3
(RGQ) 通常ユーザ 1	6.5	1	5	2	1	2

シェーパユーザ	入力帯域 (Gbit/s)	最低帯域 (Gbit/s)	最大帯域 (Gbit/s)	未使用帯域※1 (Gbit/s)	余剰帯域※2 (Gbit/s)	送信帯域 (Gbit/s)
(RGQ) 通常ユーザ 2	4	1	5		1	2

(凡例) －：対象外

注※1

通常ユーザに割り当てられる未使用帯域＝回線帯域－(LLRLQ ユーザの送信帯域) ＝ 5－1 ＝ 4 (Gbit/s)

注※2

通常ユーザの余剰帯域＝通常ユーザに割り当てられる未使用帯域－各通常ユーザの最低帯域の合計値＝ 4－(1 ＋ 1) ＝ 2 (Gbit/s)

通常ユーザ 1 および 2 の余剰帯域＝ 2×(1÷(1 ＋ 1)) ＝ 1 (Gbit/s)

注※3

LLRLQ ユーザの送信帯域は次のどちらかの値です。

・入力帯域≦最大帯域の場合，入力帯域

・入力帯域＞最大帯域の場合，最大帯域

(4)　デフォルトユーザ帯域がシェーパモード帯域へ与える影響

デフォルトユーザは，LLRLQ ユーザおよび通常ユーザの余剰帯域がある場合にフレームを出力する最低優先度のシェーパユーザで，最大帯域までフレームを送信します。

RGQ では，完全最低優先で，LLRLQ ユーザおよび通常ユーザの余剰帯域がある場合だけフレームを出力します。LLPQ4 および LLPQ1 では，LLRLQ ユーザおよび通常ユーザの LLPQ で余剰帯域がある場合に，通常ユーザの LLPQ 以外とデフォルトユーザが 999 対 1 の比率でフレームを出力します。通常ユーザのシェーパモードが RGQ と LLPQ4 の二つの場合を例に説明します。

(a)　通常ユーザのシェーパモードが RGQ の場合

LLRLQ ユーザおよびデフォルトユーザと組み合わせた場合の帯域計算例を次の表に示します。ここでは，通常ユーザのシェーパモードを RGQ とします。

表 19-11　LLRLQ ユーザ，RGQ，およびデフォルトユーザの帯域の計算例（回線帯域 6Gbit/s，重み均等)

シェーパユーザ	入力帯域 (Gbit/s)	最低帯域 (Gbit/s)	最大帯域 (Gbit/s)	未使用帯域 (Gbit/s)	余剰帯域※1 (Gbit/s)	送信帯域 (Gbit/s)
LLRLQ ユーザ	1	－	2	－	－	1
(RGQ) 通常ユーザ 1	2	1	5	5※2	1	2
(RGQ) 通常ユーザ 2	2	1	5		1	2
デフォルトユーザ	3	－	5	1※3	－	1※3

(凡例) －：対象外

注※1

通常ユーザの余剰帯域＝通常ユーザに割り当てられる未使用帯域－各通常ユーザの最低帯域の合計値＝5－（1 ＋ 1）＝3（Gbit/s）

通常ユーザ1および2の余剰帯域＝3×（1÷（1 ＋ 1））＝1.5（Gbit/s）

通常ユーザへは最低帯域＋余剰帯域を割り当てられますが，入力帯域を超えているため，送信帯域＝入力帯域となります。

注※2

通常ユーザに割り当てられる未使用帯域＝回線帯域－（LLRLQユーザの送信帯域）＝6－1＝5（Gbit/s）

注※3

デフォルトユーザに割り当てられる未使用帯域＝回線帯域－（LLRLQユーザの送信帯域）－（通常ユーザの送信帯域合計）＝6－1－（2 ＋ 2）＝1（Gbit/s）

この結果，デフォルトユーザは1（Gbit/s）の余剰帯域が使用できますが，最大帯域が0.5（Gbit/s）のため，送信帯域は0.5（Gbit/s）に制限されます。

(b)　通常ユーザのシェーパモードがLLPQ4の場合

LLRLQユーザおよびデフォルトユーザと組み合わせた場合の帯域計算例を次の表に示します。ここでは，通常ユーザのシェーパモードをLLPQ4とします。

表19-12　LLRLQユーザ，LLPQ4，およびデフォルトユーザの帯域の計算例（回線帯域6Gbit/s，重み均等）

シェーパユーザ	入力帯域(Gbit/s)	LLPQ最大帯域(Gbit/s)	最低帯域(Gbit/s)	最大帯域(Gbit/s)	未使用帯域(Gbit/s)	余剰帯域(Gbit/s)	送信帯域(Gbit/s)
LLRLQユーザ	1	－	－	2	－	－	1
（LLPQ4）通常ユーザ1	0.5（LLPQ） 1.5（LLPQ以外）	0.5	1	5	4.5※1	1.5※2（LLPQ以外）	0.5（LLPQ） 1.5（LLPQ以外）
（LLPQ4）通常ユーザ2	3（LLPQ以外）	0.5	1	5		2.24775※2	2.24775（LLPQ以外）
デフォルトユーザ	6	－	－	5		2※2	0.75225※3

（凡例）－：対象外

注※1

通常ユーザとデフォルトユーザに割り当てられる未使用帯域（A）＝回線帯域－（LLRLQユーザの送信帯域）＝6－1＝5（Gbit/s）

通常ユーザのLLPQ以外とデフォルトユーザに割り当てられる未使用帯域＝上記計算式の（A）－（LLPQユーザの送信帯域）＝5－0.5＝4.5（Gbit/s）

注※2

通常ユーザのLLPQ以外の余剰帯域＝通常ユーザとデフォルトユーザに割り当てられる未使用帯域×999÷1000－各通常ユーザの最低帯域の合計値＝4.5×999÷1000－（1 ＋ 1）＝4.4955（Gbit/s）

通常ユーザ1および2の余剰帯域＝4.4955×（1÷（1 ＋ 1））＝2.24775（Gbit/s）

通常ユーザ 1 へは LLPQ 帯域＋余剰帯域を割り当てられますが，入力帯域を超えているため，送信帯域＝入力帯域となります。

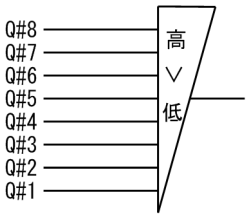
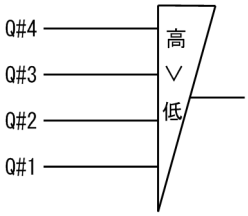
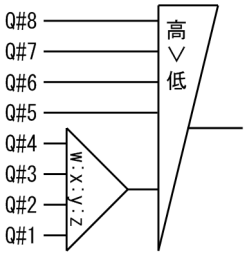
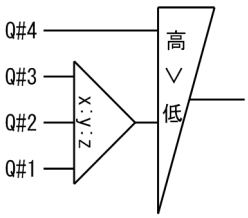
注※3

デフォルトユーザに割り当てられる余剰帯域＝回線帯域－（LLRLQ ユーザの送信帯域）－（通常ユーザの送信帯域合計）＝ 6－1－（2 + 2.24775）＝ 0.75225（Gbit/s）

19.1.7　スケジューリング

スケジューリングは，シェーパユーザ内で各キューに積まれたフレームをどのような順序で送信するかを制御する機能です。本装置では，次に示すスケジューリング種別を NIF 単位に設定できます。ただし，LLRLQ ユーザは設定に関係なく，8PQ 固定で動作します。スケジューリングの動作説明を次の表に示します。

表 19-13　スケジューリングの動作説明

スケジューリング種別	概念図	動作説明	適用例
8PQ		完全優先制御（PQ：Priority Queueing）。複数のキューにフレームがキューイングされている場合，優先度の高いキューから常にフレームを送信します。 LLPQ4 では，通常ユーザのキュー 8，7，6，5（左図 Q#8，Q#7，Q#6，Q#5）が LLPQ となります。	トラフィック優先順を完全に遵守する場合
4PQ		8PQ と同様です。 LLPQ1 では，通常ユーザのキュー 4（左図 Q#4）が LLPQ となります。	8PQ と同様
4PQ + 4WFQ		4 高優先キュー＋ 4 重み付き帯域均等制御。キュー 8，7，6，5（左図 Q#8，Q#7，Q#6，Q#5）までを完全優先制御します。キュー 8 から 5 にフレームが存在しない場合，あらかじめ設定した帯域の比（w：x：y：z）に応じてキュー 4，3，2，1（左図 Q#4，Q#3，Q#2，Q#1）からフレームを送信します。 PQ + WFQ で 8 キュー選択時に適用されます。LLPQ4 では，通常ユーザのキュー 8，7，6，5（左図 Q#8，Q#7，Q#6，Q#5）が LLPQ となります。	PQ に優先順を完全に遵守するトラフィック WFQ に PQ の余剰帯域を使用して，帯域の比を適用するトラフィック
1PQ + 3WFQ		1 高優先キュー＋ 3 重み付き帯域均等制御。キュー 4（左図 Q#4）を最優先制御します。キュー 4 にフレームが存在しない場合，あらかじめ設定した帯域の比（x：y：z）に応じてキュー 3，2，1（左図 Q#3，Q#2，Q#1）からフレームを送信します。	4PQ + 4WFQ と同様

スケジューリング種別	概念図	動作説明	適用例
		PQ ＋ WFQ で 4 キュー選択時に適用されます。LLPQ1 では，通常ユーザのキュー 4（左図 Q#4）が LLPQ となります。	

4PQ ＋ 4WFQ および 1PQ ＋ 3WFQ での，WFQ の重みの設定範囲を次の表に示します。

表 19-14　WFQ の重みの設定範囲

スケジューリング種別	仕様	内容
4PQ+4WFQ 1PQ+3WFQ	1～98（%）	WFQ の重みとして帯域の比（w：x：y：z）を次の条件を満たすように設定してください。 w≧x≧y≧z かつ w ＋ x ＋ y ＋ z≦100 （w は 4pq+4wfq 時だけ）

なお，デフォルトのスケジューリング種別は，シェーパユーザのキュー数が 4 の場合は 4PQ，シェーパユーザのキュー数が 8 の場合は 8PQ です。

19.1.8　キュー数指定

キュー数指定は，シェーパユーザ当たりのユーザ送信キュー数を NIF 単位で変更する機能です。デフォルトではシェーパユーザ当たり 8 キューです。ただし，LLRLQ ユーザはキュー数指定の設定に関係なく，8 キュー固定で動作します。

8 キューから 4 キューに変更すると，ポート当たりで収容する通常ユーザ数を拡張できます。ユーザ送信キュー数と，ポート当たりの通常ユーザ数を次の表に示します。

表 19-15　ポート当たりの通常ユーザ数

NIF 型名略称	ポート当たりの最大通常ユーザ数※			
	標準モード		拡張モード【OP-SHPE】	
	8 キュー時	4 キュー時	8 キュー時	4 キュー時
NL1GA-12S NLXGA-12RS	128	256	384	3072

注※

実際に使用する通常ユーザ数は，シェーパユーザ決定方法によって異なります。「19.1.3　シェーパユーザ決定」を参照してください。

19.1.9　キュー長変更

キュー長変更は，ユーザ送信キューのキュー長を変更する機能です。これによって，キューごとのトラフィック量に応じたキュー長に変更できます。

キュー長の設定について，シェーパユーザワンタッチ設定機能では NIF 単位に全シェーパユーザ共通の設定となり，シェーパユーザ個別設定ではシェーパユーザ単位の設定となります。また，キュー長はキュー番号ごとに 16 種類のキュー長から選択できます。選択できるキュー長を次に示します。なお，デフォルトのキュー長は 4000 です。

- 0（全廃棄）
- 250
- 500
- 1000
- 2000
- 4000
- 8000
- 12000
- 16000
- 24000
- 32000
- 64000
- 128000
- 256000
- 384000
- 512000

19.1.10　帯域制御

階層化シェーパはシェーパユーザおよびポートの 2 階層で帯域を制御する機能ですが，各階層ではユーザ帯域制御およびポート帯域制御によって帯域を制御しています。

(1)　ユーザ帯域制御

ユーザ帯域制御は，シェーパユーザ内のすべてのユーザ送信キューの送信帯域をシェーピングする機能です。ユーザ帯域制御の動作は，シェーパユーザの種類や NIF のシェーパモードによって異なります。

シェーパユーザごとのユーザ帯域制御の内容を次の表に示します。

表 19-16　シェーパユーザごとのユーザ帯域制御

シェーパユーザ種別	内容
LLRLQ ユーザ	最大帯域を制限できます。
通常ユーザ	最低帯域を保証しつつ，最大帯域を制限できます。 LLPQ の場合，LLPQ の最大帯域も制限できます。
デフォルトユーザ	最大帯域を制限できます。

シェーパモードごとのユーザ帯域制御の設定条件を次の表に示します。

表 19-17　シェーパモードごとのユーザ帯域制御の設定条件

シェーパモード	シェーパユーザ種別	帯域制御パラメータの設定条件
RGQ	LLRLQ ユーザ	最大帯域≦回線帯域※1
	通常ユーザ	最大帯域≦回線帯域※1

シェーパモード	シェーパユーザ種別	帯域制御パラメータの設定条件
		最低帯域≦最大帯域※2
	デフォルトユーザ	最大帯域≦回線帯域※1
LLPQ1，LLPQ4	LLRLQ ユーザ	最大帯域≦回線帯域※1
	通常ユーザ	最大帯域≦回線帯域※1 LLPQ 最大帯域≦最低帯域≦最大帯域※2※3
	デフォルトユーザ	最大帯域≦回線帯域※1

注※1

回線速度とポート帯域のうち，小さい方を回線帯域とします。

例えば，ポート帯域を 1Gbit/s で設定している場合，回線速度が 10Gbit/s であれば回線帯域は 1Gbit/s となりますが，回線速度が 100Mbit/s であれば回線帯域は 100Mbit/s となります。

注※2

最低帯域と最大帯域に異なる値を設定する場合は，次に示す条件をすべて満たすように設定してください。条件を満たさない場合，設定した最低帯域および最大帯域で送信しないことがあります。

・最低帯域は，最大帯域の 1／2 以下であること

・最低帯域と最大帯域の差を 256kbit/s 以上にすること

例えば，最大帯域が 10Mbit/s の場合は，最低帯域を 5Mbit/s 以下にする必要があります。また，最大帯域が 384kbit/s の場合は，最低帯域を 128kbit/s 以下にする必要があります。

注※3

LLPQ 最大帯域と最低帯域に異なる値を設定する場合は，次に示す条件をすべて満たすように設定してください。条件を満たさない場合，設定した LLPQ 最大帯域で送信しないことがあります。

・LLPQ 最大帯域は，最低帯域の 1／2 以下であること

・LLPQ 最大帯域と最低帯域の差を 256kbit/s 以上にすること

例えば，最低帯域が 6Mbit/s の場合は，LLPQ 最大帯域を 3Mbit/s 以下にする必要があります。また，最低帯域が 384kbit/s の場合は，LLPQ 最大帯域を 128kbit/s 以下にする必要があります。

帯域制御パラメータ（最大帯域，最低帯域，および LLPQ 最大帯域）の設定範囲を次の表に示します。

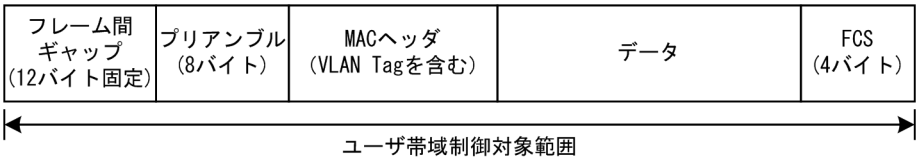
表 19-18　帯域制御パラメータの設定範囲

帯域制御パラメータ	設定単位	設定範囲	刻み値
最大帯域 最低帯域 LLPQ 最大帯域	G 単位	1G～10Gbit/s	1Gbit/s
	M 単位	1M～10000Mbit/s	1Mbit/s
	k 単位	8k～10000000kbit/s※	1kbit/s

注※　帯域値が 8kbit/s～1.6Mbit/s の場合，8kbit/s の倍数での設定を推奨します。

ユーザ帯域制御の対象となるフレームの範囲は，フレーム間ギャップから FCS までです。ユーザ帯域制御の対象範囲を次の図に示します。

図 19-6　ユーザ帯域制御の対象範囲



(2)　ポート帯域制御

ポート帯域制御は，ユーザ帯域制御を実施したあとに該当ポート内のすべてのシェーパユーザの合計帯域を，指定した送信帯域にシェーピングする機能です。この制御を使用して，広域イーサネットサービスなどへ接続できます。

例えば，ポート帯域が 10Gbit/s で ISP との契約帯域が 4Gbit/s の場合，ポート帯域制御を使用して合計帯域を 4Gbit/s 以下に抑えてフレームを送信できます。

ポート帯域制御の設定範囲を次の表に示します。

表 19-19　ポート帯域制御の設定範囲

設定単位	設定範囲	刻み値
G 単位	1G～10Gbit/s	1Gbit/s
M 単位	1M～10000Mbit/s	1Mbit/s
k 単位	8k～10000000kbit/s※	1kbit/s

注※　帯域値が 8kbit/s～1.6Mbit/s の場合，8kbit/s の倍数での設定を推奨します。

なお，ポート帯域制御の対象となるフレームの範囲は，ユーザ帯域制御と同じです。

(3)　帯域制御のオプション動作

階層化シェーパの帯域制御では，コンフィグレーションコマンド shaper port rate-option によって，帯域を制御するオプション動作を設定できます。帯域制御のオプション動作で設定できるパラメータと，その動作内容を次の表に示します。

表 19-20　帯域制御のオプション動作のパラメータおよび動作

パラメータ	動作	用途
exclude-4-byte	フレーム長から 4 バイトを差し引いた値を基に帯域を制御します。※	エッジスイッチで，VLAN Tag が 2 段以上付いたフレームの 1 段目の VLAN Tag（4 バイト）を差し引いて帯域を制御します。

注※　運用コマンドで表示する統計情報（バイト数統計）は，実際のフレーム長で表示します。

19.1.11　シェーパユーザ設定機能

階層化シェーパのシェーパユーザ設定方法には，次に示す二つの方法があります。

- シェーパユーザワンタッチ設定機能
  すべてのシェーパユーザの帯域やキュー長を，NIF 単位に一律で設定します。簡単に設定できます。
- シェーパユーザ個別設定

シェーパユーザごとに帯域やキュー長を細かく設定できます。

NIF 単位にどちらかの設定方法を選択できます。各設定方法について説明します。

(1)　シェーパユーザワンタッチ設定機能

シェーパユーザワンタッチ設定機能は，シェーパモードやキュー数などを NIF 単位に設定するだけで，シェーパユーザを自動で作成する機能です。この機能を使用すると，階層化シェーパを簡単に使用できます。

シェーパユーザワンタッチ設定機能で必要なパラメータと，パラメータごとの設定内容を次の表に示します。なお，本機能で設定した場合，シェーパユーザ間の重みは全通常ユーザで均等です。

表 19-21　シェーパユーザワンタッチ設定機能で必要なパラメータおよび設定内容

パラメータ	説明	設定できる内容	備考
シェーパモード	通常ユーザのユーザ間帯域制御方式を指定する	RGQ，LLPQ4，LLPQ1	必須（省略不可）
シェーパユーザ数	ポート内の通常ユーザ数を指定する	標準， 拡張【OP-SHPE】	省略時は標準
ユーザ送信キュー数	デフォルトユーザおよび全通常ユーザのユーザ送信キュー数を指定する	8，4	省略時は 8
廃棄優先度数	全シェーパユーザの廃棄優先度数を指定する	2	省略時は 4
廃棄閾値	廃棄優先度数 2 の場合の廃棄閾値を指定する	1～3	省略時は 2
スケジューリング種別	デフォルトユーザおよび全通常ユーザのスケジューリング種別を指定する	PQ，PQ ＋ WFQ	省略時は PQ
LLRLQ ユーザの最大帯域	LLRLQ ユーザの最大帯域を指定する	8kbit/s～10Gbit/s	省略時はポート帯域
通常ユーザの最低帯域	全通常ユーザ共通の最低帯域を指定する	8kbit/s～10Gbit/s※1	必須（省略時は自動計算※2)
通常ユーザおよびデフォルトユーザの最大帯域	デフォルトユーザおよび全通常ユーザ共通の最大帯域を指定する	8kbit/s～10Gbit/s※1	省略時は自動計算※3
LLPQ 最大帯域	全通常ユーザ共通の LLPQ 最大帯域を指定する	8kbit/s～10Gbit/s※1 ※4	シェーパモードが LLPQ4 または LLPQ1 の場合だけ有効 省略時は自動計算※5
WFQ の重み	デフォルトユーザおよび全通常ユーザ共通の各 WFQ の重みを指定する	1～98	スケジューリング種別が PQ ＋ WFQ の場合だけ有効 省略時はデフォルト値※6

パラメータ	説明	設定できる内容	備考
キュー長	デフォルトユーザおよび全通常ユーザ共通のキューごとのキュー長を指定する	0～512000 の範囲で 16 種類	省略時は全キュー 4000

注※1

ポート帯域制御の最大帯域を超える場合は，ポート帯域制御の最大帯域と同じ値になります。

注※2

各通常ユーザの最低帯域は，回線帯域÷通常ユーザ数となります。例えば，RGQ，8 キュー，標準で回線帯域を 8Gbit/s に設定した場合，次の値になります。

8Gbit/s÷128 シェーパユーザ＝ 62.5Mbit/s

ただし，計算結果が 1.6Mbit/s 以下になる場合は，8kbit/s の倍数に切り下げます。また，LLPQ4 および LLPQ1 で計算結果が 512kbit/s 以下になる場合は，512kbit/s になります。

注※3

通常ユーザの最大帯域は，最低帯域×10 となります。デフォルトユーザの最大帯域は，回線帯域と等しくなります。例えば，RGQ，8 キュー，標準で回線帯域を 8Gbit/s に設定した場合，次の値になります。

（8Gbit/s÷128 シェーパユーザ）×10 ＝ 625Mbit/s

ただし，最低帯域が 25.6kbit/s 未満の場合は，8kbit/s の倍数に切り下げた最低帯域＋ 256kbit/s となります。

注※4

LLPQ 最大帯域が最低帯域を超える場合は，送信帯域が LLPQ 最大帯域まで保証されないことがあります。

注※5

通常ユーザの LLPQ 最大帯域は，最低帯域÷2 となります。例えば，RGQ，8 キュー，標準でポート帯域を 8Gbit/s に設定した場合，次の値になります。

（8Gbit/s÷128 シェーパユーザ）÷2 ＝ 31.25Mbit/s

注※6

8 キュー（4PQ ＋ 4WFQ）時のデフォルト値は次のとおりです。

Q4：Q3：Q2：Q1 ＝ 4：3：2：1

4 キュー（1PQ ＋ 3WFQ）時のデフォルト値は次のとおりです。

Q3：Q2：Q1 ＝ 3：2：1

(2)　シェーパユーザ個別設定

シェーパユーザ個別設定では，シェーパモードやキュー数などを NIF 単位に設定したあと，シェーパユーザごとに異なる帯域やキュー長を設定できます。これによって，シェーパユーザごとにきめ細かく設定できます。

シェーパユーザ個別設定で必要なパラメータとパラメータごとの設定内容を，設定単位別に次に示します。

表 19-22　シェーパユーザ個別設定で必要なパラメータおよび設定内容（NIF 単位での設定）

パラメータ	説明	設定できる内容	備考
シェーパモード	通常ユーザのユーザ間帯域制御方式を指定する	RGQ，LLPQ4，LLPQ1	必須（省略不可）
シェーパユーザ数	ポート内の通常ユーザ数を指定する	標準，拡張【OP-SHPE】	省略時は標準
ユーザ送信キュー数	デフォルトユーザおよび全通常ユーザのユーザ送信キュー数を指定する	8，4	省略時は 8

パラメータ	説明	設定できる内容	備考
廃棄優先度数	全シェーパユーザの廃棄優先度数を指定する	2	省略時は 4
廃棄閾値	廃棄優先度数 2 の場合の廃棄閾値を指定する	1～3	省略時は 2
スケジューリング種別	デフォルトユーザおよび全通常ユーザのスケジューリング種別を指定する	PQ，PQ ＋ WFQ	省略時は PQ

表 19-23　シェーパユーザ個別設定で必要なパラメータおよび設定内容（シェーパユーザ単位での設定）

パラメータ	説明	設定できる内容	備考
最大帯域	LLRLQ ユーザ，通常ユーザ，およびデフォルトユーザの最大帯域を指定する	8kbit/s～10Gbit/s※1	－
最低帯域	通常ユーザ共通の最低帯域を指定する	8kbit/s～10Gbit/s※1	－
LLPQ 最大帯域	通常ユーザの LLPQ 最大帯域を指定する	8kbit/s～10Gbit/s※1	シェーパモードが LLPQ4 または LLPQ1 の場合に有効
WFQ の重み	デフォルトユーザおよび通常ユーザの各 WFQ の重みを指定する	1～98	スケジューリング種別が PQ ＋ WFQ の場合だけ有効 省略時はデフォルト値※2
キュー長	LLRLQ ユーザ，デフォルトユーザ，および通常ユーザのキューごとのキュー長を指定する	0～512000 の範囲で 16 種類	省略時は全キュー 4000
重み	通常ユーザの重みを指定する	1～50	省略時は 1

（凡例）－：該当なし

注※1

ポート帯域制御の最大帯域を超える場合は，ポート帯域制御の最大帯域と同じ値になります。

注※2

8 キュー（4PQ ＋ 4WFQ）時のデフォルト値は次のとおりです。

Q4：Q3：Q2：Q1 ＝ 4：3：2：1

4 キュー（1PQ ＋ 3WFQ）時のデフォルト値は次のとおりです。

Q3：Q2：Q1 ＝ 3：2：1

19.1.12　NIF と階層化シェーパとの対応

NIF と階層化シェーパの対応を次の表に示します。

表 19-24　NIF と階層化シェーパとの対応

NIF 型名略称	階層化シェーパ
NL1G-12T	－

NIF 型名略称	階層化シェーパ
NL1G-12S	－
NL1GA-12S	○
NL1G-24T	－
NL1G-24S	－
NLXG-6RS	－
NLXGA-12RS	○
NLXLG-4Q	－
NMCG-1C	－

（凡例）　○：サポート　－：未サポート

19.1.13　階層化シェーパ使用時の注意事項

(1)　優先度決定についての注意事項

ユーザ優先度マッピングを使用する場合，QoS フローの優先度変更で変更した優先度も変更されます。

(2)　ユーザ帯域設定についての注意事項

- LLRLQ ユーザの最大帯域と全シェーパユーザの最低帯域の合計が回線帯域を超えている場合，各シェーパユーザの最低帯域が保証されないことがあります。
- LLPQ で通常ユーザごとの最低帯域を常に保証する場合，回線内のすべての通常ユーザで LLPQ 最大帯域を最低帯域以下に設定する必要があります。最低帯域が保証されない例を次に示します。

表 19-25　最低帯域が保証されない例（ポート帯域および各通常ユーザの最大帯域は 10Gbit/s）

シェーパユーザ	LLPQ に対する入力帯域 (Gbit/s)	LLPQ 以外のユーザ送信キューに対する入力帯域 (Gbit/s)	LLPQ 最大帯域の設定値 (Gbit/s)	最低帯域の設定値 (Gbit/s)	送信帯域 (Gbit/s)
通常ユーザ 1	7	0	6	5	6
通常ユーザ 2	0	7			4

LLPQ に対する各通常ユーザの入力帯域は，通常ユーザ 1 が 7Gbit/s，通常ユーザ 2 が 0 です。LLPQ 以外のユーザ送信キューに対する各通常ユーザの入力帯域は，通常ユーザ 1 が 0，通常ユーザ 2 が 7Gbit/s です。

この例では，LLPQ 最大帯域の設定値が 6Gbit/s のため，LLPQ 入力のある通常ユーザ 1 の LLPQ に 6Gbit/s を割り当てます。通常ユーザ 1 は LLPQ に最低帯域を超える 6Gbit/s を割り当てているため，LLPQ 以外のユーザ送信キューに割り当てる帯域がありません。

通常ユーザ 2 は LLPQ に割り当てた帯域がないため，最低帯域の 5Gbit/s を LLPQ 以外のユーザ送信キューに割り当てようとします。しかし，未使用帯域が 4Gbit/s しかないため，ユーザ送信キューに対して割り当てられる帯域は 4Gbit/s です。このため，通常ユーザ 2 の送信帯域は，設定した最低帯域以下の 4Gbit/s になります。

(3) シェーパユーザワンタッチ設定機能使用時の注意事項

オートネゴシエーションを指定したイーサネットインタフェースに対し，階層化シェーパのユーザ帯域を省略して設定した場合は，該当するインタフェースで解決できる最大の回線速度を基にユーザ帯域を割り当てます。例えば，オートネゴシエーションだけを指定している場合は，オートネゴシエーションで解決した結果が 100Mbit/s であっても，回線帯域は 1000Mbit/s としてユーザ帯域を割り当てます。

(4) MIB および運用コマンドの統計値に関する注意事項

axShaper グループおよび運用コマンド show shaper port の統計情報は，本装置内で周期的に更新した結果で応答するため，周期時間内での再取得では更新されません。axShaper グループおよび運用コマンド show shaper port の統計情報の更新周期の目安を次の表に示します。

表 19-26 axShaper グループおよび運用コマンド show shaper port の統計情報更新目安時間

シェーパユーザ数	キュー数	廃棄優先度数	全ユーザの更新時間	
			ポート内	NIF 内
標準	8 キュー	4	10 秒	120 秒
		2	5 秒	60 秒
	4 キュー	4	10 秒	120 秒
		2	5 秒	60 秒
拡張	8 キュー	4	30 秒	360 秒
		2	15 秒	180 秒
	4 キュー	4	180 秒	36 分
		2	60 秒	12 分

(5) 運用コマンド clear shaper 実行時の MIB の注意事項

運用コマンド clear shaper を実行した場合は，axShaper グループの統計情報が少なく表示されることがあります。

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

階層化シェーパ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 19-27　コンフィグレーションコマンド一覧

コマンド名	説明
nif	シェーパユーザ決定，またはシェーパモードを適用する NIF を設定します。
qos	フロー検出によってシェーパユーザを決定します。
shaper bandwidth-profile	階層化シェーパの帯域制御プロファイルを作成します。
shaper enable	階層化シェーパの設定を許可します。
shaper flow-distribution	シェーパユーザ決定の自動決定方法を設定します。
shaper mode	シェーパワンタッチ設定機能，およびシェーパモードを設定します。 オプションライセンス OP-SHPE を使用する場合，拡張モードを有効にできます。
shaper port rate-limit	イーサネットインタフェースに階層化シェーパのポート帯域制御を設定します。
shaper port rate-option	イーサネットインタフェースに階層化シェーパの帯域制御のオプション動作を設定します。
shaper user	階層化シェーパのシェーパユーザリストにユーザごとの帯域制御プロファイルを設定します。
shaper user-priority-map	ユーザ優先度によるキュー番号の決定を設定します。
shaper users-group	階層化シェーパのシェーパユーザリストをイーサネットインタフェースに適用します。
shaper users-list	階層化シェーパのシェーパユーザリストを作成します。

19.2.2　階層化シェーパを有効にする設定

[設定のポイント]

本装置で初めて階層化シェーパを使用するときは，階層化シェーパの設定を許可して階層化シェーパを有効にします。

[コマンドによる設定]

1. **(config)# shaper enable**

階層化シェーパの設定を許可します。

19.2.3　ランダム振り分けおよび VLAN ID マッピングによるシェーパユーザ決定の設定

[設定のポイント]

シェーパユーザ決定情報を作成して，適用する NIF 番号を設定します。

[コマンドによる設定]

1. **(config)# shaper flow-distribution SIP-RANDOM random source-ip-address**
   送信元 IP アドレスによってランダム振り分けをするシェーパユーザ決定情報（SIP-RANDOM）を作成します。
2. **(config-shp-distr)# nif 1**
   作成したシェーパユーザ決定情報（SIP-RANDOM）を NIF1 に適用します。

19.2.4 フロー検出によるシェーパユーザ決定の設定

特定のフローに対してシェーパユーザを決定する場合の例を次に示します。

[設定のポイント]

フレーム送信時の宛先 IP アドレスによってフロー検出をして，シェーパユーザを決定する設定をします。

[コマンドによる設定]

1. **(config)# ip qos-flow-list QOS-LIST1**
   IPv4 QoS フローリスト（QOS-LIST1）を作成します。本リストを作成すると，IPv4 QoS フローリストモードに移行します。
2. **(config-ip-qos)# qos ip any host 192.0.2.10 action user 1**
   192.0.2.10 の IP アドレスを宛先として，シェーパユーザ（通常ユーザ 1）に変更する IPv4 QoS フローリストを設定します。
3. **(config-ip-qos)# exit**
   IPv4 QoS フローリスト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 tengigabitethernet 3/1**
   イーサネットインタフェース 3/1 のコンフィグレーションモードに移行します。
5. **(config-if)# ip qos-flow-group QOS-LIST1 out**
   送信側に IPv4 QoS フローリスト（QOS-LIST1）を適用します。

19.2.5 ユーザ優先度マッピングの設定

階層化シェーパではユーザ優先度によってユーザ送信キュー番号を決定できます。

[設定のポイント]

ユーザ優先度マッピングに使用する VLAN Tag を設定します。本機能は，階層化シェーパで動作中の全 NIF が対象です。

[コマンドによる設定]

1. **(config)# shaper user-priority-map tag-vlan**
   1 段目の VLAN Tag のユーザ優先度でユーザ送信キュー番号を決定する設定をします。
2. **(config)# end**
   コンフィグレーションモードから装置管理者モードに戻ります。
3. **# reload nif 1**
   Are you sure you want to restart nif 1? (y/n): y

装置管理者モードで，階層化シェーパとして使用しているNIFを再起動します。再起動が完了すると，ユーザ優先度マッピングで運用を開始します。

[注意事項]

ポートシェーパ同様に，QoSフローによる優先度変更もできます。優先度変更については，「16　優先度変更」を参照してください。

19.2.6　シェーパユーザワンタッチ設定機能の設定

[設定のポイント]

自動設定するシェーパモード情報を作成して，適用するNIF番号を設定することで，シェーパユーザを自動で設定します。シェーパモード情報として次に示す情報を設定します。

- シェーパモード
- スケジューリング種別
- ユーザ送信キュー数
- 廃棄優先度数
- 階層化シェーパのポート番号
- ユーザ帯域
- キュー長
- WFQの重み（スケジューリング種別がPQ + WFQの場合だけ）

[コマンドによる設定]

1. **(config)# shaper mode SHAPER-RGQ auto rgq scheduling pq max-user-queue 8 port 1-12 llrlq-peak-rate 2G peak-rate 1G min-rate 1M**

   次のとおり指定して，シェーパモード情報（SHAPER-RGQ）を作成します。

   - シェーパモード：RGQ
   - スケジューリング種別：PQ
   - ユーザ送信キュー数：8キュー
   - 廃棄優先度数：省略しているため，4
   - 階層化シェーパのポート番号：1～12
   - LLRLQユーザの最大帯域：2Gbit/s
   - 通常ユーザおよびデフォルトユーザの最大帯域：2Gbit/s
   - 通常ユーザの最低帯域：1Mbit/s

2. **(config-shp-mode)# nif 1**

   作成したシェーパモード情報（SHAPER-RGQ）をNIF1に適用します。

3. **(config-shp-mode)# end**

   コンフィグレーションモードから装置管理者モードに戻ります。

4. **# reload nif 1**

   Are you sure you want to restart nif 1? (y/n): y

   装置管理者モードで，NIF1を再起動します。再起動が完了すると，適用したシェーパモード情報で運用を開始します。

19.2.7 シェーパユーザ個別設定

[設定のポイント]

まず,個別設定するためのシェーパモード情報を作成して,適用するNIF番号を設定することで,シェーパユーザを個別で設定できるようにします。シェーパモード情報として次に示す情報を設定します。

- シェーパモード
- スケジューリング種別
- ユーザ送信キュー数
- 廃棄優先度数
- 階層化シェーパのポート番号

次に，設定するシェーパユーザ情報およびポートへ適用するシェーパユーザリストを作成して，使用するインタフェースへ適用することで，シェーパユーザを個別に作成します。

[コマンドによる設定]

1. **(config)# shaper mode SHAPER-LLPQ4 llpq4 scheduling pq max-user-queue 8 max-discard-priority 2 threshold2 port 1-12**

   次のとおり指定して，シェーパモード情報（SHAPER-LLPQ4）を作成します。

   - シェーパモード：LLPQ4
   - スケジューリング種別：PQ
   - ユーザ送信キュー数：8キュー
   - 廃棄優先度数：2，廃棄閾値はthreshold2
   - 階層化シェーパのポート番号：1～12

2. **(config-shp-mode)# nif 1**

   作成したシェーパモード情報（SHAPER-LLPQ4）をNIF1に適用します。

3. **(config-shp-mode)# top**

   (config)# shaper bandwidth-profile USER-PTN1 peak-rate 1G min-rate 100M llpq-peak-rate 50M

   グローバルコンフィグレーションモードに戻り，次のとおり指定して，階層化シェーパの帯域制御プロファイル（USER-PTN1）を作成します。

   - 最大帯域：1Gbit/s
   - 最低帯域：100Mbit/s
   - LLPQ最大帯域：50Mbit/s
   - キュー長および重み：デフォルト

4. **(config)# shaper users-list SHP-LIST1**

   階層化シェーパのシェーパユーザリスト（SHP-LIST1）を作成します。本リストを作成すると，config-shp-usersモードに移行します。

5. **(config-shp-users)# shaper user 1,100-128 USER-PTN1**

   階層化シェーパのシェーパユーザ番号と，使用する帯域制御プロファイルを設定します。この場合，通常ユーザ1および100～128に，帯域制御プロファイル（USER-PTN1）を適用します。

6. **(config-shp-users)# top**

   (config)# interface tengigabitethernet 3/1

グローバルコンフィグレーションモードに戻り，イーサネットインタフェース 3/1 のコンフィグレーションモードに移行します。

7. (config-if)# shaper users-group SHP-LIST1

   シェーパユーザリスト（SHP-LIST1）を適用します。

8. (config)# end

   # reload nif 1

   Are you sure you want to restart nif 1? (y/n): y

   装置管理者モードに移行して，NIF1 を再起動します。再起動が完了すると，適用したシェーパモードおよびシェーパユーザ情報で運用を開始します。

19.2.8　ポート帯域制御の設定

[設定のポイント]

該当するイーサネットインタフェースの出力帯域を，実回線（10Gbit/s）の帯域より低く（2Gbit/s）する場合に，ポート帯域制御を設定します。この設定には，shaper mode コマンドによる，階層化シェーパを動作させるポートの設定が必要です。

[コマンドによる設定]

1. (config)# interface tengigabitethernet 1/12

   (config-if)# shaper port rate-limit 2G

   イーサネットインタフェース 1/12 のコンフィグレーションモードに移行したあと，ポート帯域を 2Gbit/s に設定します。

19.2.9　帯域制御のオプション動作の設定

[設定のポイント]

該当するイーサネットインタフェースの帯域制御に，オプション動作が必要な場合に設定します。この設定には，shaper mode コマンドによる，階層化シェーパを動作させるポートの設定が必要です。

[コマンドによる設定]

1. (config)# interface tengigabitethernet 1/12

   (config-if)# shaper port rate-option exclude-4-byte

   イーサネットインタフェース 1/12 のコンフィグレーションモードに移行したあと，帯域制御のオプション動作として，フレーム長から 4 バイトを差し引いて帯域制御する（exclude-4-byte）設定をします。

19.2.10　廃棄優先度の設定

特定の QoS フローに対して廃棄クラスを変更して，キューイング時の廃棄優先度を設定する場合の例を次に示します。

[設定のポイント]

フレーム受信時に宛先 IP アドレスによって QoS フロー検出をして，廃棄クラスを変更する設定をします。廃棄優先度は廃棄クラスによって決まります。

[コマンドによる設定]

1. **(config)# ip qos-flow-list QOS-LIST2**

   IPv4 QoS フローリスト（QOS-LIST2）を作成します。本リストを作成すると，IPv4 QoS フローリストモードに移行します。

2. **(config-ip-qos)# qos ip any host 192.0.2.10 action priority-class 8 discard-class 1**

   192.0.2.10 の IP アドレスを宛先として，優先クラス 8，廃棄クラス 1 の IPv4 QoS フローリストを設定します。

3. **(config-ip-qos)# exit**

   IPv4 QoS フローリスト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 tengigabitethernet 1/3**

   (config-if)# ip qos-flow-group QOS-LIST2 in

   イーサネットインタフェース 1/3 のコンフィグレーションモードに移行したあと，受信側に IPv4 QoS フローリスト（QOS-LIST2）を適用します。

19.3　オペレーション

19.3.1　運用コマンド一覧

階層化シェーパの運用コマンド一覧を次の表に示します。

表 19-28　運用コマンド一覧

コマンド名	説明
show shaper	階層化シェーパの設定情報，および統計情報を表示します。
clear shaper	show shaper コマンドで表示する統計情報を 0 クリアします。
show shaper port	階層化シェーパの統計情報をポート単位の合計値で表示します。
show shaper rate	シェーパユーザの送信スループット情報を表示します。
show shaper resources	階層化シェーパのシェーパユーザ収容情報を表示します。
show shaper user	階層化シェーパの統計情報をシェーパユーザ単位の合計値で表示します。
restart shaper	階層化シェーパ制御プログラムを再起動します。
dump shaper	階層化シェーパ制御プログラムで採取している制御情報をファイルへ出力します。

19.3.2　シェーパユーザ決定の確認

show shaper コマンドでシェーパユーザ決定方法を確認できます。コマンドの実行結果を次の図に示します。

図 19-7　シェーパユーザ決定の確認

```
> show shaper 1/1
Date 20XX/01/01 12:00:00 UTC
NIF1: active
 User-priority-map
  Configuration=enable[inner-tag-vlan]
  Current      =enable[inner-tag-vlan]
 Shaper-mode            Scheduling-mode  Max-queue  Discard-priority   Extend
  Configuration=RGQ                  PQ          8                 4  disable
  Current      =RGQ                  PQ          8                 4  disable
 Auto                LLRLQ(bps) LLPQ(bps) Peak(bps)  Min(bps)   WFQ-weight
  Configuration=enable        2G         -        1G        1M   -/ -/ -/ -
  Current      =enable        2G         -        1G        1M   -/ -/ -/ -
  Queue-length       Q1     Q2     Q3     Q4     Q5     Q6     Q7     Q8
   Configuration=  4000   4000   4000   4000   4000   4000   4000   4000
   Current      =  4000   4000   4000   4000   4000   4000   4000   4000
  NIF1/Port1
   Flow-distribution=random[SIP]
   Port-rate-limit=10Gbps
   User:LLRLQ, Bandwidth-profile=-
    Peak-rate=2Gbps, Min-rate=-, Rate-weight=-
    LLPQ-peak-rate=-
    Max-queue=8
    LLPQ                                Send               Discard
              Packets                      -                     -
              Bytes                        -                     -
    Queue1 : Qlen=12, Limit-Qlen=4000
             Drop-mode=tail-drop, WFQ-weight=-
                                        Send               Discard
     Discard1  packets                312096                 58324
        :
        :
```

```
        :
>
```

- Flow-distribution の内容が，設定したシェーパユーザ決定（この例では，送信元 IP アドレスによるランダム振り分け）になっていることを確認します。

19.3.3　ユーザ優先度マッピングの確認

show shaper コマンドでユーザ優先度マッピング情報を確認できます。コマンドの実行結果を次の図に示します。

図 19-8　ユーザ優先度マッピングの確認

```
> show shaper 1/1
Date 20XX/01/01 12:00:00 UTC
NIF1: active
 User-priority-map
  Configuration=enable[inner-tag-vlan]
  Current      =enable[inner-tag-vlan]
 Shaper-mode            Scheduling-mode  Max-queue  Discard-priority   Extend
  Configuration=RGQ                  PQ          8                 4  disable
  Current      =RGQ                  PQ          8                 4  disable
 Auto                LLRLQ(bps) LLPQ(bps) Peak(bps)  Min(bps)   WFQ-weight
  Configuration=enable        2G         -        1G        1M   -/ -/ -/ -
  Current      =enable        2G         -        1G        1M   -/ -/ -/ -
  Queue-length       Q1     Q2     Q3     Q4     Q5     Q6     Q7     Q8
   Configuration=  4000   4000   4000   4000   4000   4000   4000   4000
   Current      =  4000   4000   4000   4000   4000   4000   4000   4000
  NIF1/Port1
   Flow-distribution=random[SIP]
   Port-rate-limit=10Gbps
   User:LLRLQ, Bandwidth-profile=-
    Peak-rate=2Gbps, Min-rate=-, Rate-weight=-
    LLPQ-peak-rate=-
    Max-queue=8
    LLPQ                                 Send               Discard
               Packets                      -                     -
               Bytes                        -                     -
    Queue1 : Qlen=12, Limit-Qlen=4000
             Drop-mode=tail-drop, WFQ-weight=-
                                         Send               Discard
     Discard1  packets                 312096                 58324
         :
         :
         :
>
```

- User-priority-map の Current の内容が，設定した状態（この例では，2 段目の VLAN Tag で設定）になっていることを確認します。

19.3.4　シェーパモード情報の確認

show shaper コマンドでシェーパモード情報を確認できます。コマンドの実行結果を次の図に示します。

図 19-9　シェーパモード情報の確認

```
> show shaper 1/1
Date 20XX/01/01 12:00:00 UTC
NIF1: active
 User-priority-map
  Configuration=enable[inner-tag-vlan]
  Current      =enable[inner-tag-vlan]
 Shaper-mode            Scheduling-mode  Max-queue  Discard-priority   Extend
  Configuration=RGQ                  PQ          8                 4  disable
  Current      =RGQ                  PQ          8                 4  disable
 Auto                LLRLQ(bps) LLPQ(bps) Peak(bps)  Min(bps)   WFQ-weight
  Configuration=enable        2G         -        1G        1M   -/ -/ -/ -
  Current      =enable        2G         -        1G        1M   -/ -/ -/ -
```

```
 Queue-length       Q1     Q2     Q3     Q4     Q5     Q6     Q7     Q8
  Configuration=  4000   4000   4000   4000   4000   4000   4000   4000
  Current      =  4000   4000   4000   4000   4000   4000   4000   4000
 NIF1/Port1
  Flow-distribution=random[SIP]
  Port-rate-limit=10Gbps
  User:LLRLQ, Bandwidth-profile=-
   Peak-rate=2Gbps, Min-rate=-, Rate-weight=-
   LLPQ-peak-rate=-
   Max-queue=8
   LLPQ                                 Send                Discard
             Packets                      -                      -
             Bytes                        -                      -
   Queue1 : Qlen=12, Limit-Qlen=4000
            Drop-mode=tail-drop, WFQ-weight=-
                                        Send                Discard
    Discard1  packets                 312096                  58324
       :
       :
       :
>
```

- Shaper-mode の Current の内容が，設定したシェーパモード（この例では RGQ）になっていることを確認します。
- Scheduling-mode の Current の内容が，設定したスケジューリング種別（この例では PQ）になっていることを確認します。PQ+WFQ の場合，WFQ-weight の Current の内容が，設定した重み（この例では PQ なので情報なし）になっていることを確認します。
- Max-queue の Current の内容が，設定したユーザ送信キュー数（この例では 8 キュー）になっていることを確認します。
- Discard-priority の Current の内容が，設定した廃棄優先度数（この例では 4）になっていることを確認します。
- Extend の Current の内容が，設定した階層化シェーパ拡張モード（この例では未設定）になっていることを確認します。
- Auto の Current の内容が，設定したワンタッチ設定情報（この例では enable）になっていることを確認します。
- LLRLQ(bps)，Peak(bps)，Min(bps)の Current の内容が，設定したユーザ帯域（この例では 2Gbit/s，1Gbit/s，1Mbit/s）になっていることを確認します。
- Queue-length の Current の内容が，設定したキュー長（この例ではデフォルトの 4000）になっていることを確認します。

19.3.5　シェーパユーザ情報の確認

show shaper コマンドでシェーパユーザ情報を確認できます。コマンドの実行結果を次の図に示します。

図 19-10　シェーパユーザ情報の確認

```
> show shaper 1/1 user 1
Date 20XX/01/01 12:00:00 UTC
NIF1: active
 User-priority-map
  Configuration=enable[inner-tag-vlan]
  Current      =enable[inner-tag-vlan]
 Shaper-mode           Scheduling-mode  Max-queue  Discard-priority   Extend
  Configuration=RGQ                 PQ          8                 4  disable
  Current      =RGQ                 PQ          8                 4  disable
 Auto                LLRLQ(bps) LLPQ(bps) Peak(bps)  Min(bps)   WFQ-weight
  Configuration=enable        2G         -        1G        1M   -/ -/ -/ -
  Current      =enable        2G         -        1G        1M   -/ -/ -/ -
  Queue-length       Q1     Q2     Q3     Q4     Q5     Q6     Q7     Q8
   Configuration=  4000   4000   4000   4000   4000   4000   4000   4000
```

```
  Current      =  4000   4000   4000   4000   4000   4000   4000   4000
 NIF1/Port1
  Flow-distribution=random[SIP]
  Port-rate-limit=10Gbps
  User:1, Bandwidth-profile=-
   Peak-rate=1Gbps, Min-rate=1Mbps, Rate-weight=1
   LLPQ-peak-rate=-
   Max-queue=8
   LLPQ                                  Send                Discard
              Packets                       -                      -
              Bytes                         -                      -
   Queue1 : Qlen=12, Limit-Qlen=4000
            Drop-mode=tail-drop, WFQ-weight=-
                                         Send                Discard
    Discard1  packets                  312096                  58324
    Discard2  packets                  530316                  38671
    Discard3  packets                  757357                  11672
    Discard4  packets                  983613                   2473
    Total     packets                 2583382                 111140
                                         Send                Discard
    Discard1  bytes                   27464448                5132512
    Discard2  bytes                   45607176                3325706
    Discard3  bytes                   65132701                1003792
    Discard4  bytes                   84590718                 212678
    Total     bytes                  222795044                9674688
   Queue2 : Qlen=10, Limit-Qlen=4000
       :
       :
       :
>
```

- User の内容が，指定したシェーパユーザ番号（この例では，1）になっていることを確認します。
- Bandwidth-profile の内容が，指定した帯域制御プロファイル（この例ではワンタッチ設定のため，“-”）になっていることを確認します。
- Peak-rate，Min-rate の内容が，指定したレートまたは自動計算したレート（この例では，1Gbit/s，1Mbit/s）になっていることを確認します。
- Rate-weight の内容が，指定した重み（この例では，デフォルト 1）になっていることを確認します。
- LLPQ-peak-rate の内容が，指定したレートまたは自動計算したレート（この例では，RGQ なので対象外）になっていることを確認します。
- Max-queue の内容が，指定したキュー数（この例では，8 キュー）になっていることを確認します。
- Queue の表示数が，指定したキュー数（この例では，8 キュー分）になっていることを確認します。
- Discard の表示数が，指定した廃棄優先度数（この例では，四つ分）になっていることを確認します。
- Limit-Qlen の内容が，指定したキュー長（この例では，デフォルト 4000）になっていることを確認します。また Qlen の内容で，現在のキュー長（この例では，12）を確認します。

19.3.6 帯域（送信スループット）の確認

show shaper rate コマンドでユーザ帯域およびポート帯域の送信スループットを確認できます。コマンドの実行結果を次の図に示します。

図 19-11 送信スループットの確認

```
> show shaper rate 1/1 user 1
Date 20XX/01/01 12:00:00 UTC
NIF1: active
 User-priority-map
  Configuration=enable[inner-tag-vlan]
  Current      =enable[inner-tag-vlan]
 Shaper-mode            Scheduling-mode  Max-queue  Discard-priority   Extend
  Configuration=RGQ                  PQ          8                 4  disable
  Current      =RGQ                  PQ          8                 4  disable
```

```
 Auto                LLRLQ(bps) LLPQ(bps) Peak(bps)  Min(bps)   WFQ-weight
  Configuration=enable        2G         -        1G        1M   -/ -/ -/ -
  Current      =enable        2G         -        1G        1M   -/ -/ -/ -
  Queue-length       Q1     Q2     Q3     Q4     Q5     Q6     Q7     Q8
   Configuration=  4000   4000   4000   4000   4000   4000   4000   4000
   Current      =  4000   4000   4000   4000   4000   4000   4000   4000
  NIF1/Port1
   Flow-distribution=random[SIP]
   Port-rate-limit=4Gbps, Avtive-rate=3.0Gbps
   User:ID=1, Bandwidth-profile=-
    Peak-rate=1Gbps, Min-rate=1Mbps, Rate-weight=1
    LLPQ-peak-rate=-
    Max-queue=8
    LLPQ           Send packets            Send bytes       pps          bps
                              -                     -         -            -
    Queue          Send packets            Send bytes       pps          bps
    1                      6533               1672448      1.0k        98.0k
    2                      2873                735488      2.0k       258.0k
    3                   2200134             563234304     15.0k       198.0k
    4                   4781911            1224169216      3.0k      1024.0k
    5                  14890111            3811868416     10.0k       157.0k
    6                  23091811            5911503616      8.0k       283.0k
    7                  27576011            7059458816     90.0k       384.0k
    8                  37910013            9704963328     56.0k       829.0k
    Total             110459397           28277605632    185.0k      3231.0k
>
```

- Port-rate-limit および Active-rate の内容で，指定したイーサネットインタフェースのポート送信帯域（この例では，4Gbit/s），および送信スループット（この例では，3Gbit/s）を確認します。
- pps および bps の列の情報で，LLPQ 送信スループット，キューごとの送信スループット，ユーザ合計送信スループットを確認します（この例では，RGQ モードなので LLPQ 送信スループットは未表示）。

19.3.7　ユーザ送信キューの統計情報の確認

show shaper コマンドでユーザ送信キューの統計情報を確認できます。シェーパユーザ 1 に優先度 1，廃棄優先度 4 のトラフィックを中継している状態として，コマンドの実行結果を次の図に示します。

図 19-12　ユーザ送信キューの統計情報の確認

```
> show shaper 1/1 user 1
Date 20XX/01/01 12:00:00 UTC
NIF1: active
 User-priority-map
  Configuration=enable[inner-tag-vlan]
  Current      =enable[inner-tag-vlan]
 Shaper-mode            Scheduling-mode  Max-queue  Discard-priority   Extend
  Configuration=RGQ                  PQ          8                 4  disable
  Current      =RGQ                  PQ          8                 4  disable
 Auto                LLRLQ(bps) LLPQ(bps) Peak(bps)  Min(bps)   WFQ-weight
  Configuration=enable        2G         -        1G        1M   -/ -/ -/ -
  Current      =enable        2G         -        1G        1M   -/ -/ -/ -
  Queue-length       Q1     Q2     Q3     Q4     Q5     Q6     Q7     Q8
   Configuration=  4000   4000   4000   4000   4000   4000   4000   4000
   Current      =  4000   4000   4000   4000   4000   4000   4000   4000
  NIF1/Port1
   Flow-distribution=random[SIP]
   Port-rate-limit=10Gbps
   User:1, Bandwidth-profile=-
    Peak-rate=1Gbps, Min-rate=1Mbps, Rate-weight=1
    LLPQ-peak-rate=-
    Max-queue=8
    LLPQ                                Send              Discard
              Packets                      -                    -
              Bytes                        -                    -
    Queue1 : Qlen=12, Limit-Qlen=4000
             Drop-mode=tail-drop, WFQ-weight=-
                                        Send              Discard
     Discard1  packets                     0                    0
     Discard2  packets                     0                    0
```

```
     Discard3  packets                    0                    0
     Discard4  packets              2583382               111140
     Total     packets              2583382               111140
                                       Send              Discard
     Discard1  bytes                      0                    0
     Discard2  bytes                      0                    0
     Discard3  bytes                      0                    0
     Discard4  bytes                84590718               212678
     Total     bytes                84590718               212678
   Queue2 : Qlen=10, Limit-Qlen=4000
       :
       :
       :
>
```

- Queue1 の各 Discard packets 行の Send 列で，各廃棄優先度のキューに積んだパケット数を確認します。
- Queue1 の各 Discard packets 行の Discard 列で，各廃棄優先度の廃棄パケット数を確認します。
- Queue1 の各 Discard bytes 行の Send 列で，各廃棄優先度のキューに積んだバイト数を確認します。
- Queue1 の各 Discard bytes 行の Discard 列で，各廃棄優先度の廃棄バイト数を確認します。

19.3.8 シェーパユーザ数の確認

show shaper resources コマンドでシェーパユーザ数を確認できます。コマンドの実行結果を次の図に示します。

図 19-13 シェーパユーザ数の確認

```
> show shaper resources 1/1
Date 20XX/01/01 12:00:00 UTC
Hierarchical-shaper Database Management
        Shaper-users Used/Max :    500/64000
NIF1: active
 Shaper-mode=RGQ,   Max-queue=4, Extend=disable
 Port1  Shaper-users Used/Max :    250/   258
>
```

- Hierarchical-shaper Database Management の Shaper-users Used/Max の内容で，装置当たりの個別設定シェーパユーザ数の，収容できる最大シェーパユーザ数と現在設定しているシェーパユーザ数を確認します。
- 各ポートの Shaper-users Used/Max の内容で，ポートごとに収容できる最大シェーパユーザ数と現在設定しているシェーパユーザ数を確認します。

20 装置内キュー

この章では，本装置が保持するキューについて説明します。

20.1　解説

20.1.1　概要

本装置内にはいくつかのキューがあります。各キューの動作状況および統計情報は，運用コマンド show qos queueing および show shaper で確認できます。

(1)　AX8608S，AX8304S，および AX8308S の装置内キューとフレームの流れ

装置内キューとフレームの流れを次に示します。

図 20–1　AX8608S の PSU-11 および PSU-12，AX8304S および AX8308S に搭載できる PSU で BCU-CPU を経由する場合

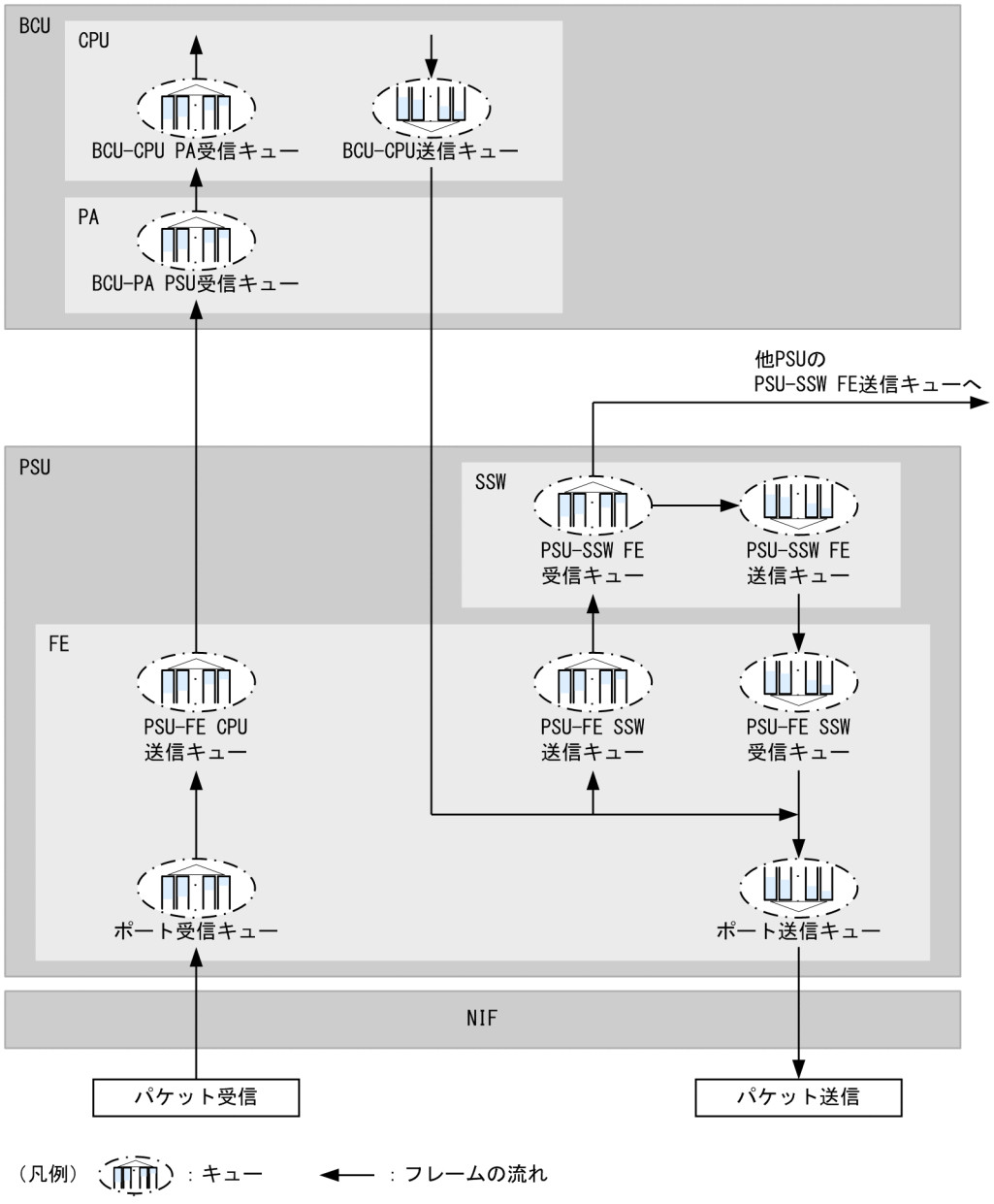


図 20-2　AX8608S の PSU-11 および PSU-12，AX8304S および AX8308S に搭載できる PSU で BCU-CPU を経由しない場合

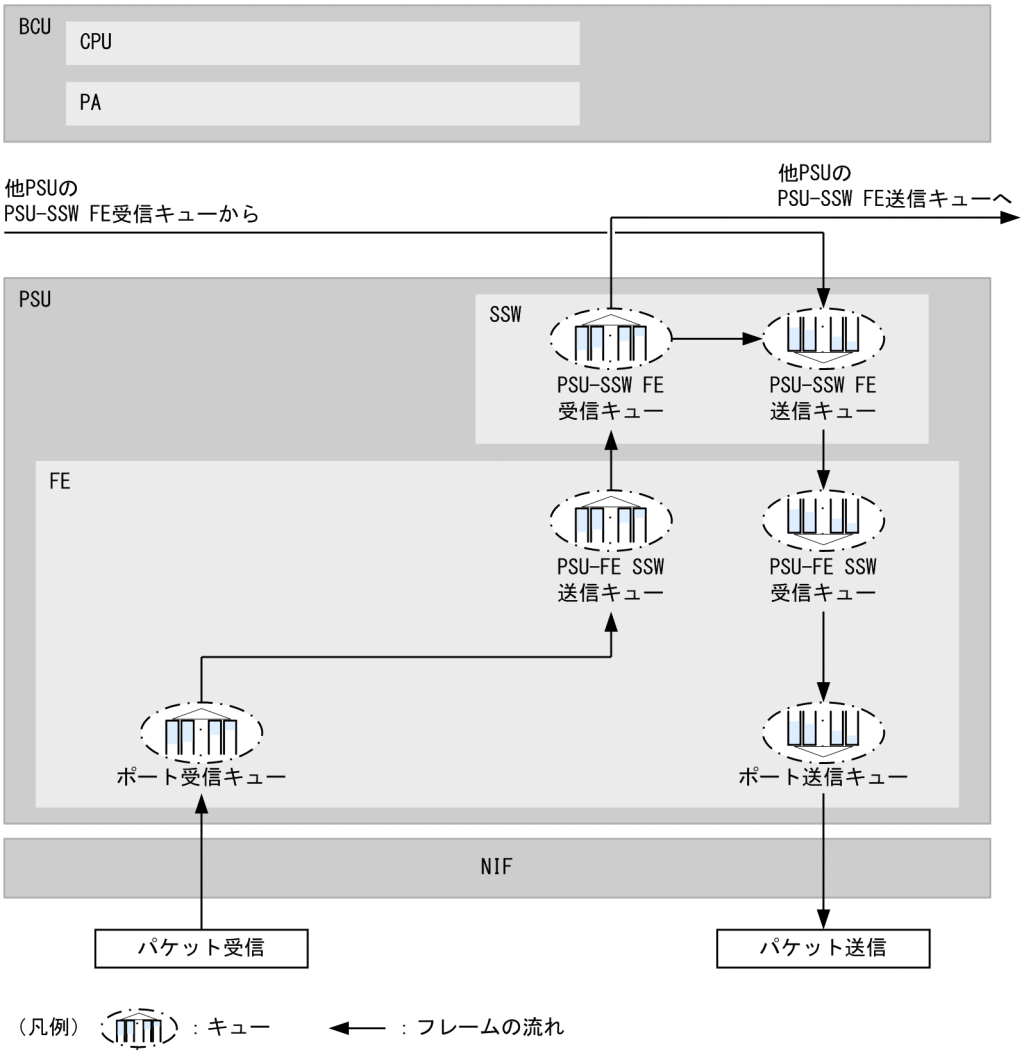


図 20-3　AX8608S の PSU-21，PSU-22，および PSU-23 で BCU-CPU を経由する場合

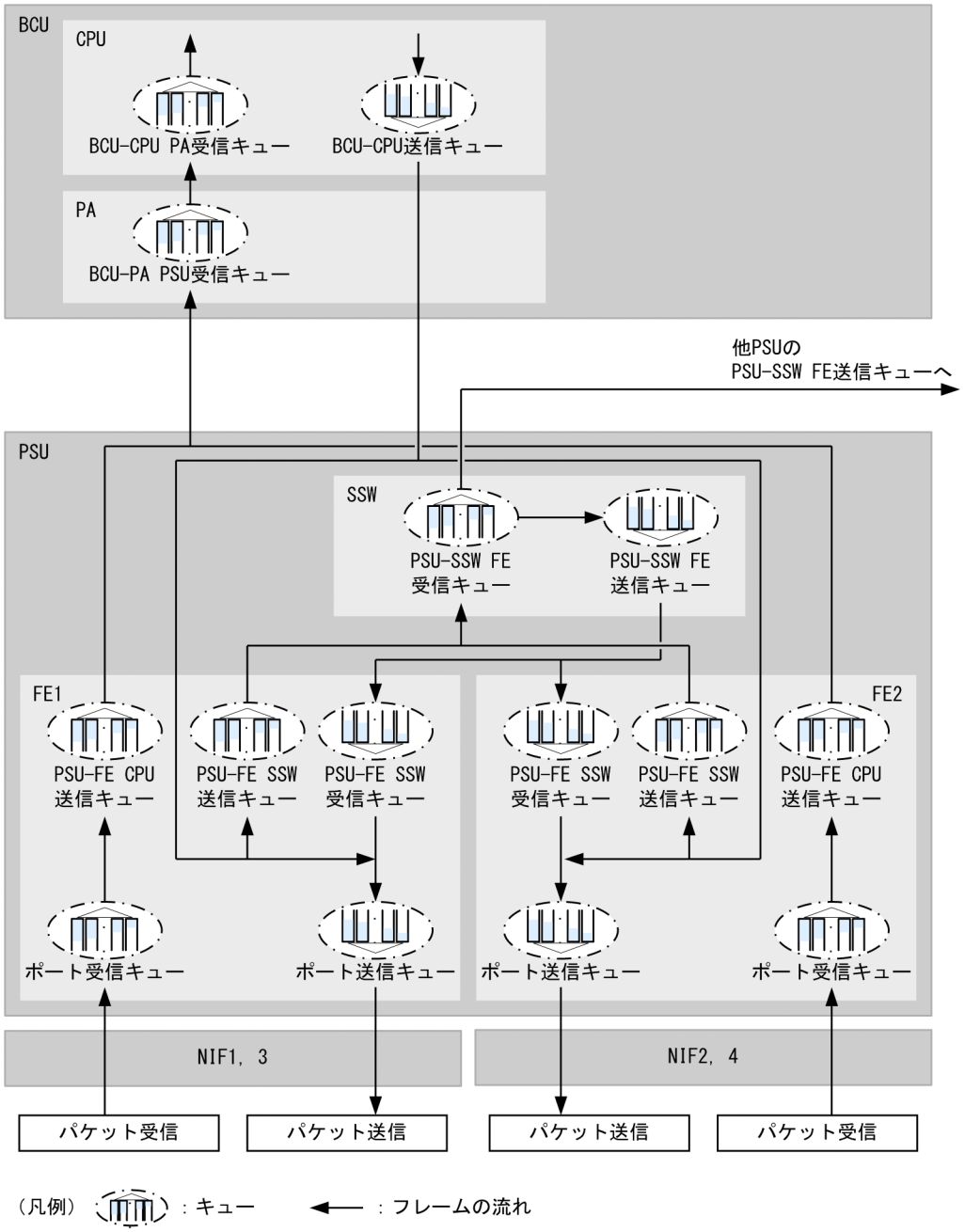
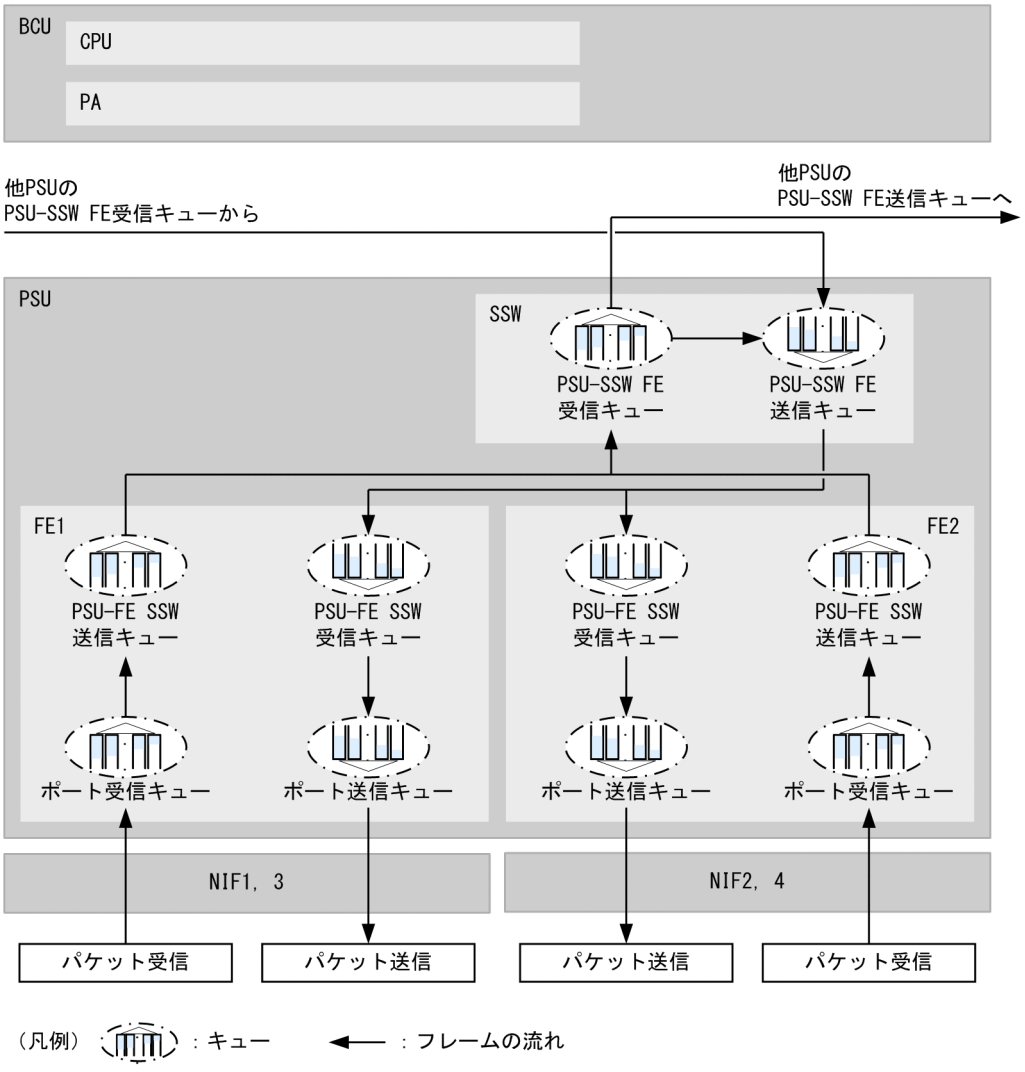


図 20–4　AX8608S の PSU-21，PSU-22，および PSU-23 で BCU-CPU を経由しない場合



(2)　AX8616S および AX8632S の装置内キューとフレームの流れ

装置内キューとフレームの流れを次に示します。

図 20-5　AX8616S および AX8632S の PSU-11 および PSU-12 で BCU-CPU を経由する場合

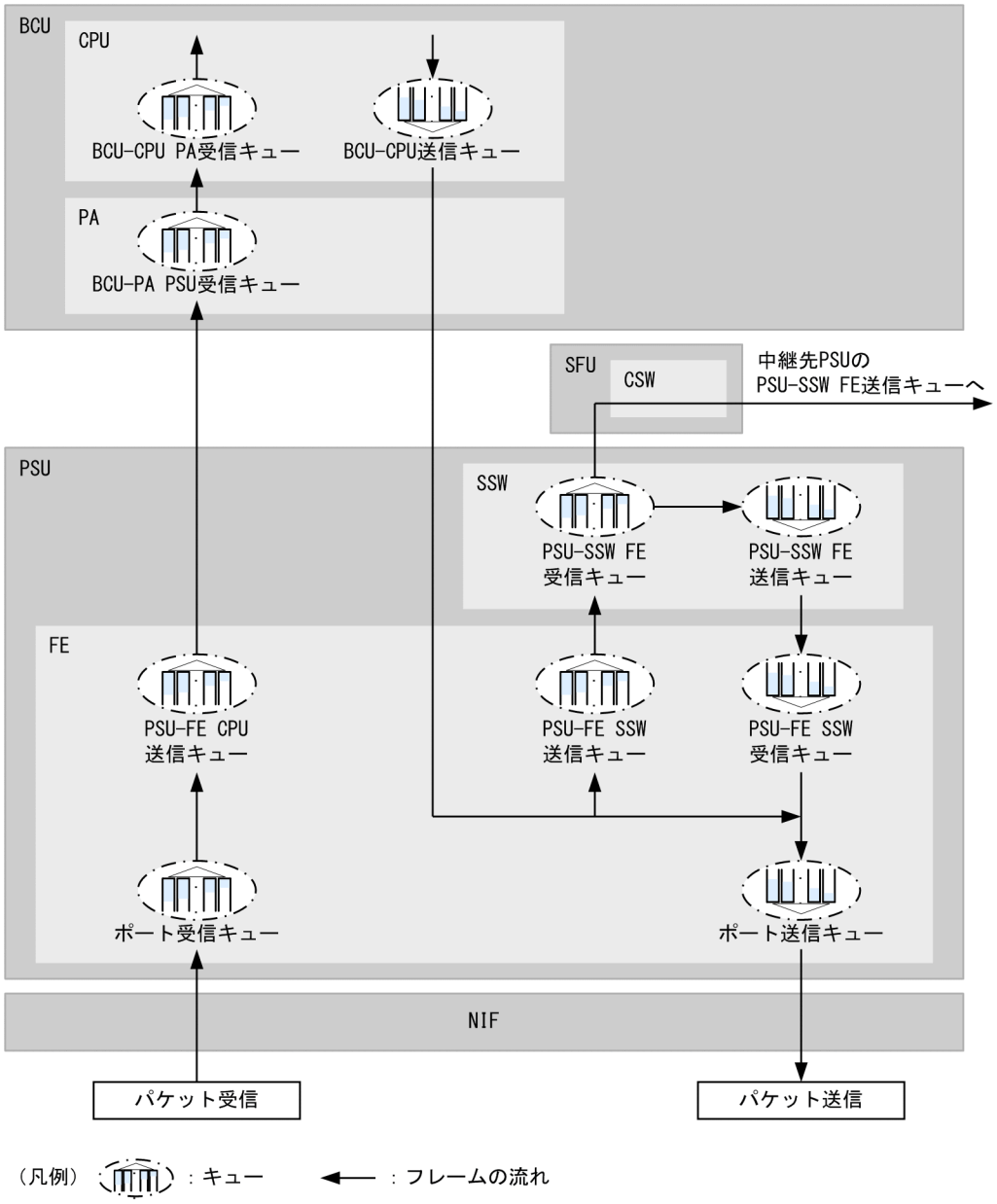


図 20-6　AX8616S および AX8632S の PSU-11 および PSU-12 で BCU-CPU を経由しない場合

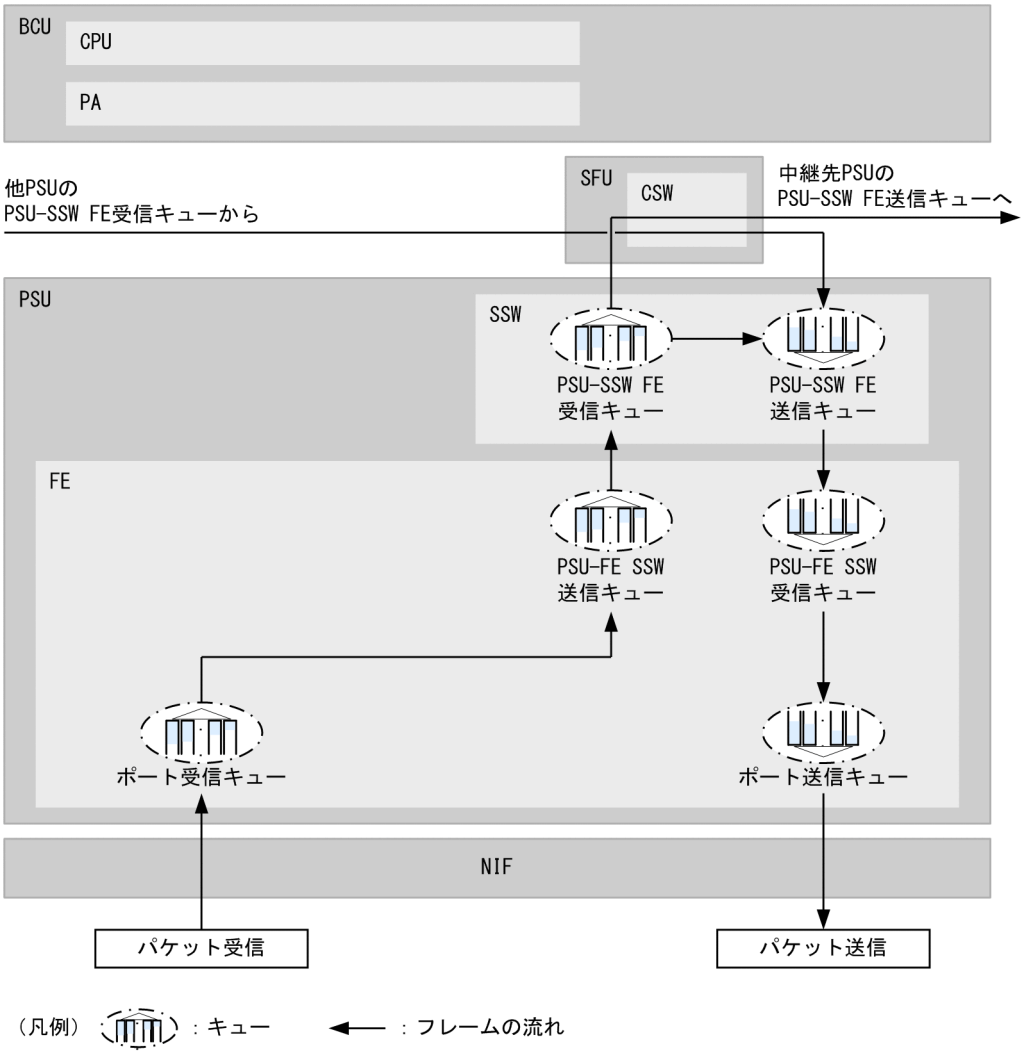


図 20-7　AX8616S および AX8632S の PSU-21，PSU-22，および PSU-23 で BCU-CPU を経由する場合

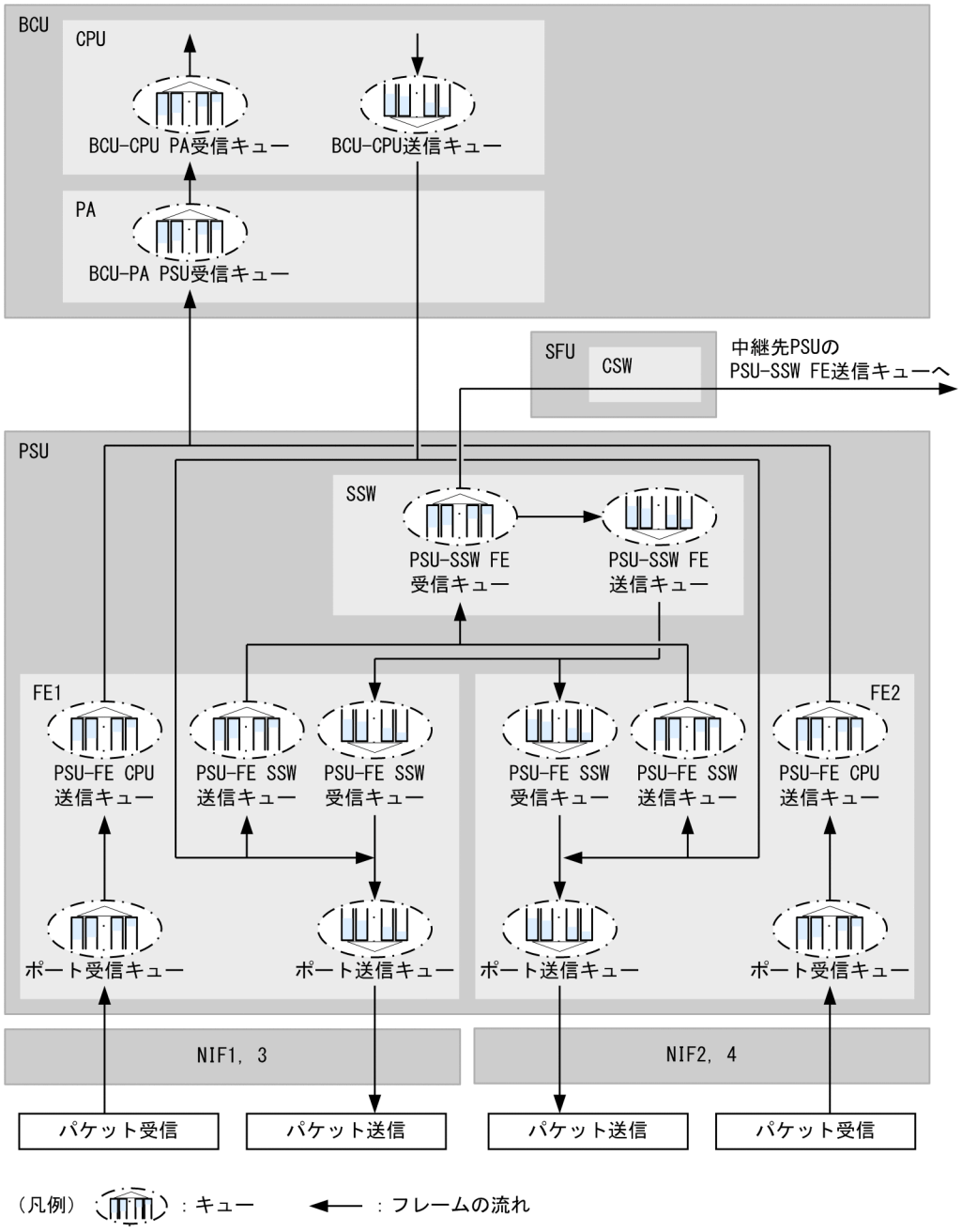
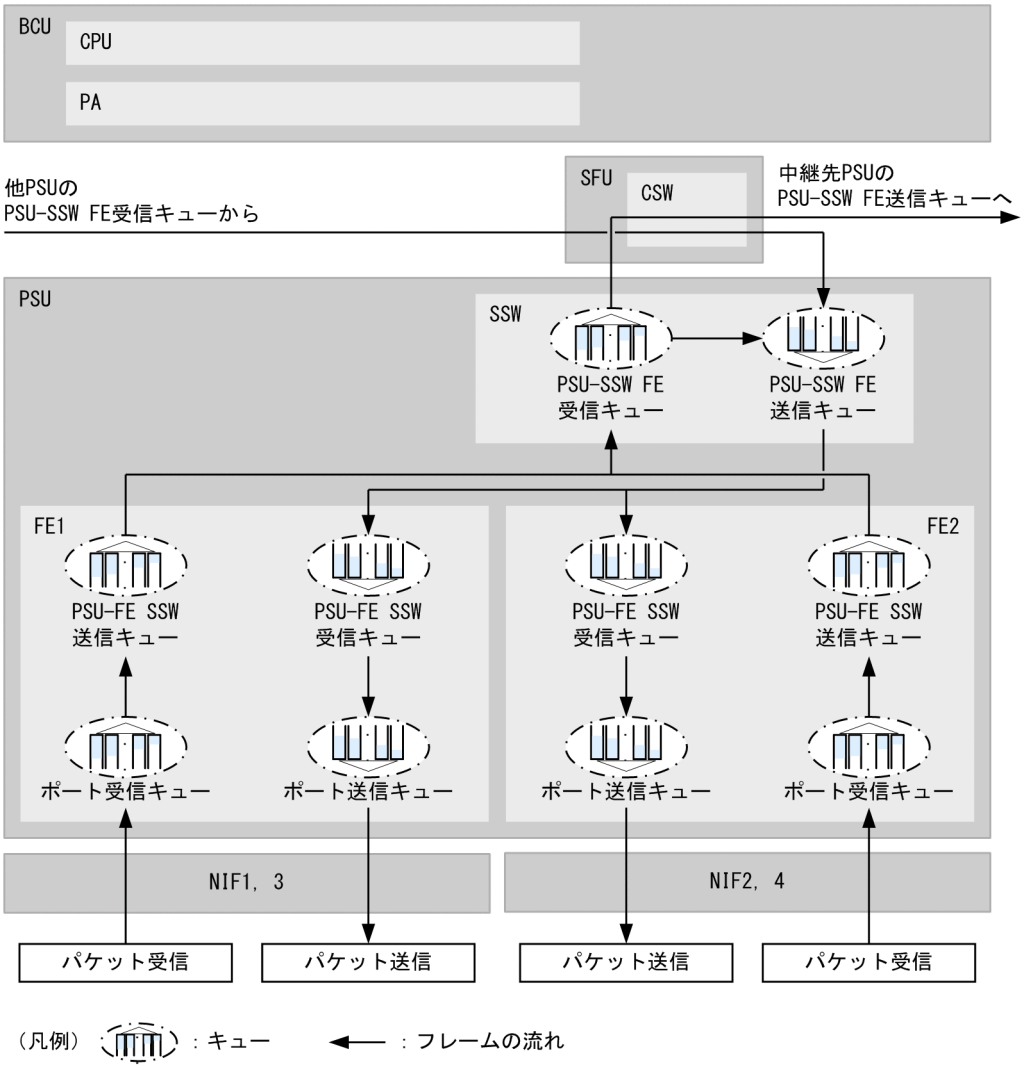


図 20-8　AX8616S および AX8632S の PSU-21，PSU-22，および PSU-23 で BCU-CPU を経由しない場合



(3)　NIF 種別ごとの装置内キューとフレームの流れ

本装置では，NIF 種別ごとに装置内キューの有無および装置内キューの実装部位が異なります。NIF 種別ごとの装置内キューの実装部位を次の表に示します。

表 20-1　NIF 種別ごとの装置内キューの実装部位（1/3）

NIF 種別	キュー種別					
	ポート受信キュー	ポート送信キュー	NIF FE 受信キュー	NIF FE 送信キュー	PSU-FE NIF 受信キュー	PSU-FE NIF 送信キュー
NL1G-12T	FE	FE	−	−	−	−
NL1G-12S	FE	FE	−	−	−	−
NL1GA-12S※	NIF	NIF	NIF	NIF	FE	FE
NL1G-24T	−	NIF	−	−	FE	FE

NIF 種別	キュー種別					
	ポート受信キュー	ポート送信キュー	NIF FE 受信キュー	NIF FE 送信キュー	PSU-FE NIF 受信キュー	PSU-FE NIF 送信キュー
NL1G-24S	−	NIF	−	−	FE	FE
NLXG-6RS	FE	FE	−	−	−	−
NLXGA-12RS※	NIF	NIF	NIF	NIF	FE	FE
NLXLG-4Q	NIF	NIF	NIF	NIF	FE	FE
NLCG-1Q	FE	FE	−	−	−	−
NMCG-1C	FE	FE	−	−	−	−

表 20–2　NIF 種別ごとの装置内キューの実装部位（2/3）

NIF 種別	キュー種別			
	PSU-FE CPU 送信キュー	PSU-FE SSW 受信キュー	PSU-FE SSW 送信キュー	PSU-SSW FE 受信キュー
NL1G-12T	FE	FE	FE	SSW
NL1G-12S	FE	FE	FE	SSW
NL1GA-12S※	FE	FE	FE	SSW
NL1G-24T	FE	FE	FE	SSW
NL1G-24S	FE	FE	FE	SSW
NLXG-6RS	FE	FE	FE	SSW
NLXGA-12RS※	FE	FE	FE	SSW
NLXLG-4Q	FE	FE	FE	SSW
NLCG-1Q	FE	FE	FE	SSW
NMCG-1C	FE	FE	FE	SSW

表 20–3　NIF 種別ごとの装置内キューの実装部位（3/3）

NIF 種別	キュー種別			
	PSU-SSW FE 送信キュー	BCU-PA PSU 受信キュー	BCU-CPU PA 受信キュー	BCU-CPU 送信キュー
NL1G-12T	SSW	PA	CPU	CPU
NL1G-12S	SSW	PA	CPU	CPU
NL1GA-12S※	SSW	PA	CPU	CPU
NL1G-24T	SSW	PA	CPU	CPU
NL1G-24S	SSW	PA	CPU	CPU
NLXG-6RS	SSW	PA	CPU	CPU

NIF 種別	キュー種別			
	PSU-SSW FE 送信キュー	BCU-PA PSU 受信キュー	BCU-CPU PA 受信キュー	BCU-CPU 送信キュー
NLXGA-12RS※	SSW	PA	CPU	CPU
NLXLG-4Q	SSW	PA	CPU	CPU
NLCG-1Q	SSW	PA	CPU	CPU
NMCG-1C	SSW	PA	CPU	CPU

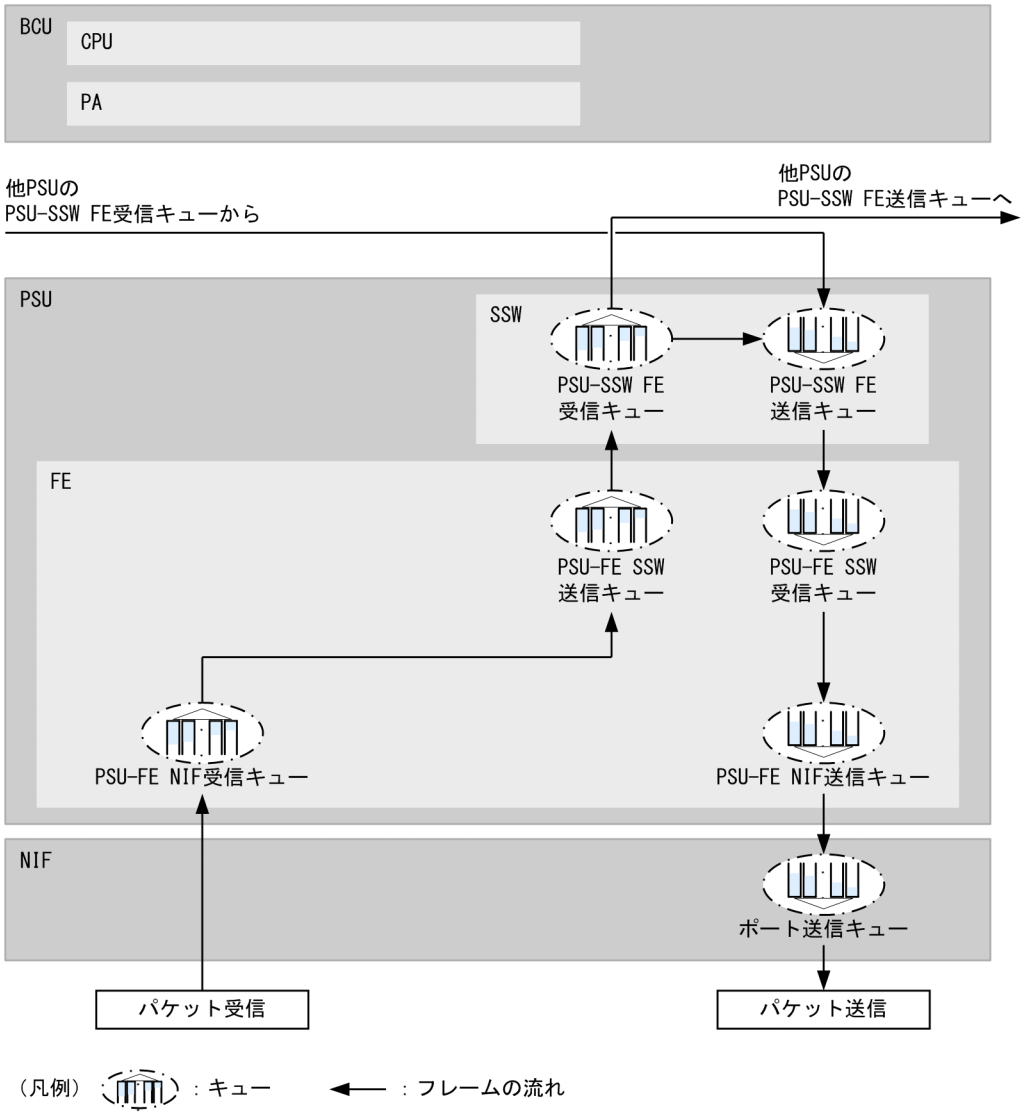
（凡例）　－：キューが存在しない

注※　この NIF は PE-NIF です。

NL1G-24T，NL1G-24S，NLXLG-4Q，および PE-NIF 以外の NIF 搭載時の装置内キューとフレームの流れについては，「(1)　AX8608S，AX8304S，および AX8308S の装置内キューとフレームの流れ」および「(2)　AX8616S および AX8632S の装置内キューとフレームの流れ」を参照してください。

AX8304S および AX8308S で NL1G-24T および NL1G-24S を使用した場合の，装置内キューと BCU-CPU を経由しないフレームの流れを次の図に示します。

図 20-9　AX8304S および AX8308S で NL1G-24T および NL1G-24S 使用時に BCU-CPU を経由しない場合



AX8616S および AX8632S で NLXLG-4Q を使用した場合の，装置内キューと BCU-CPU を経由しないフレームの流れを次に示します。

図 20-10　NLXLG-4Q 使用時に AX8616S および AX8632S の PSU-11 および PSU-12 で BCU-CPU を経由しない場合

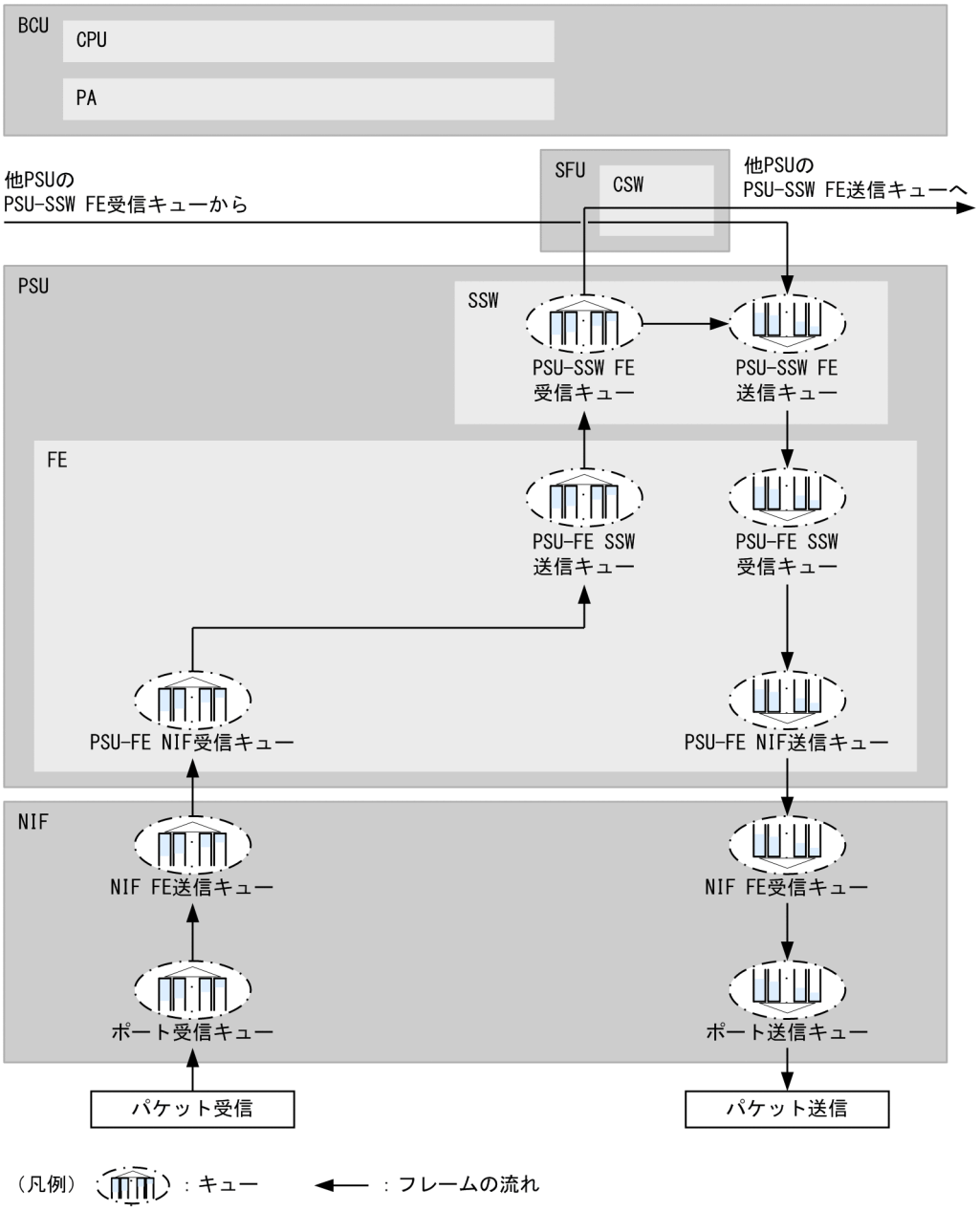
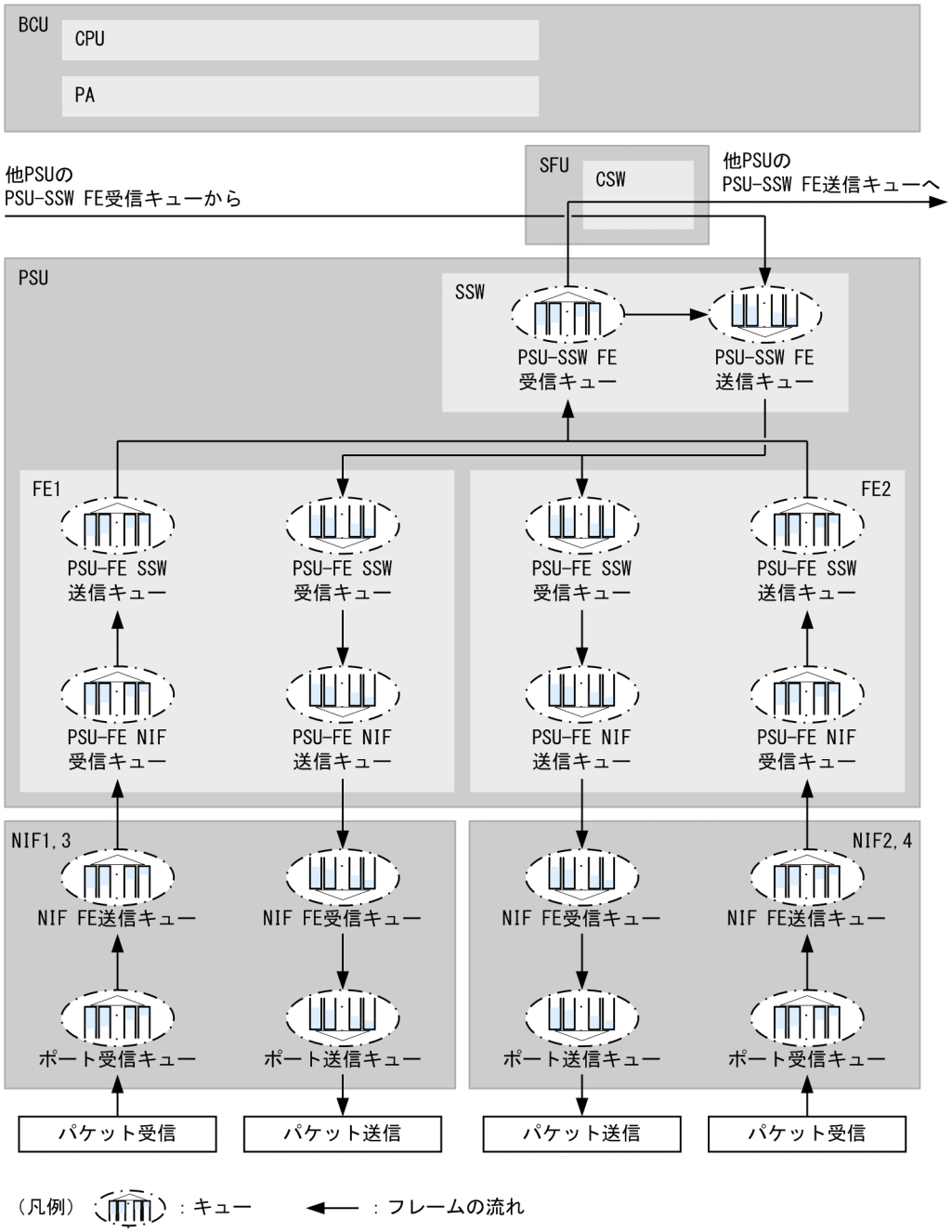


図 20-11　NLXLG-4Q 使用時に AX8616S および AX8632S の PSU-21，PSU-22，および PSU-23 で BCU-CPU を経由しない場合



AX8616S および AX8632S で PE-NIF を使用した場合の，装置内キューと BCU-CPU を経由しないフレームの流れを次に示します。

図 20-12　PE-NIF 使用時に AX8616S および AX8632S の PSU-11 および PSU-12 で BCU-CPU を経由しない場合

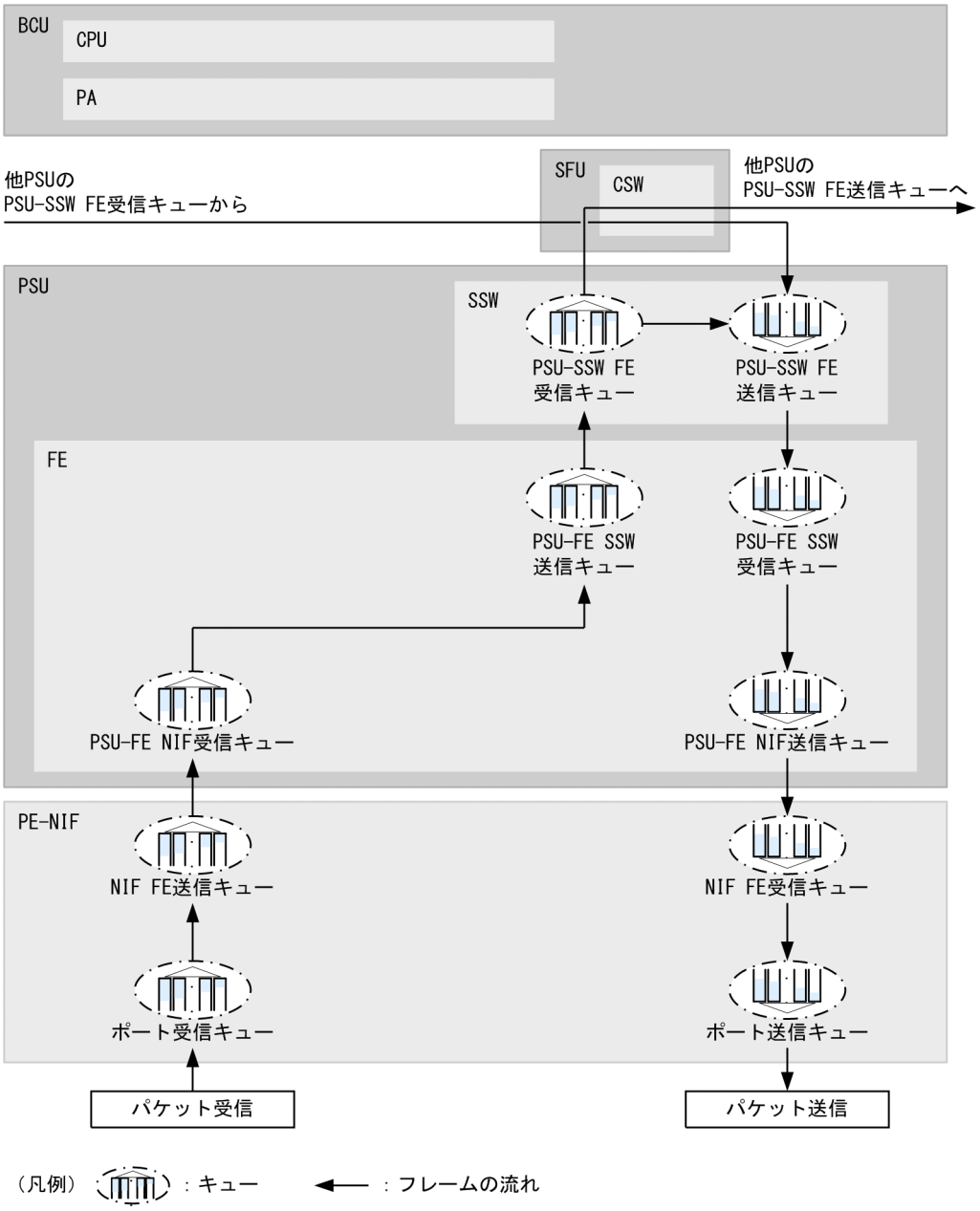
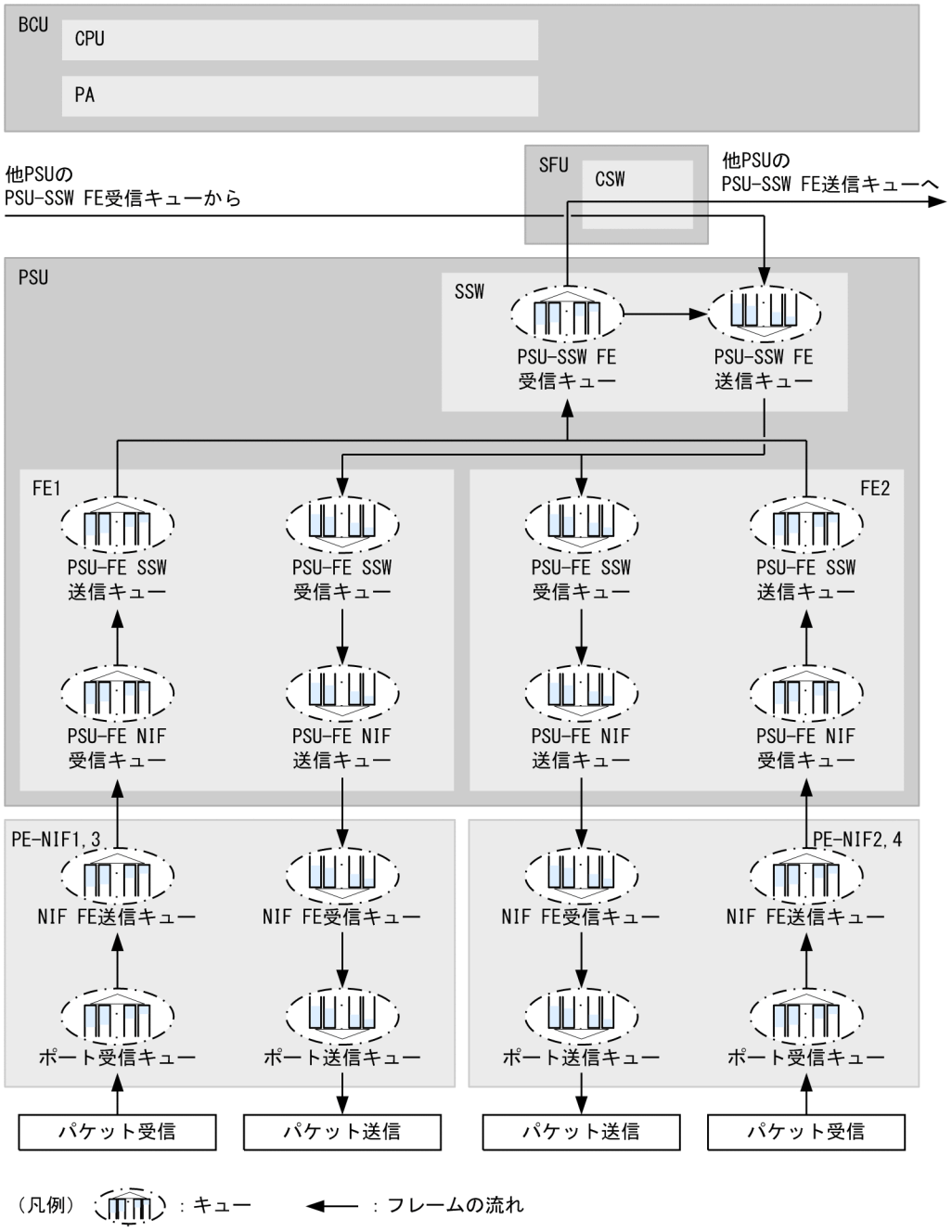


図 20-13　PE-NIF 使用時に AX8616S および AX8632S の PSU-21，PSU-22，および PSU-23 で BCU-CPU を経由しない場合



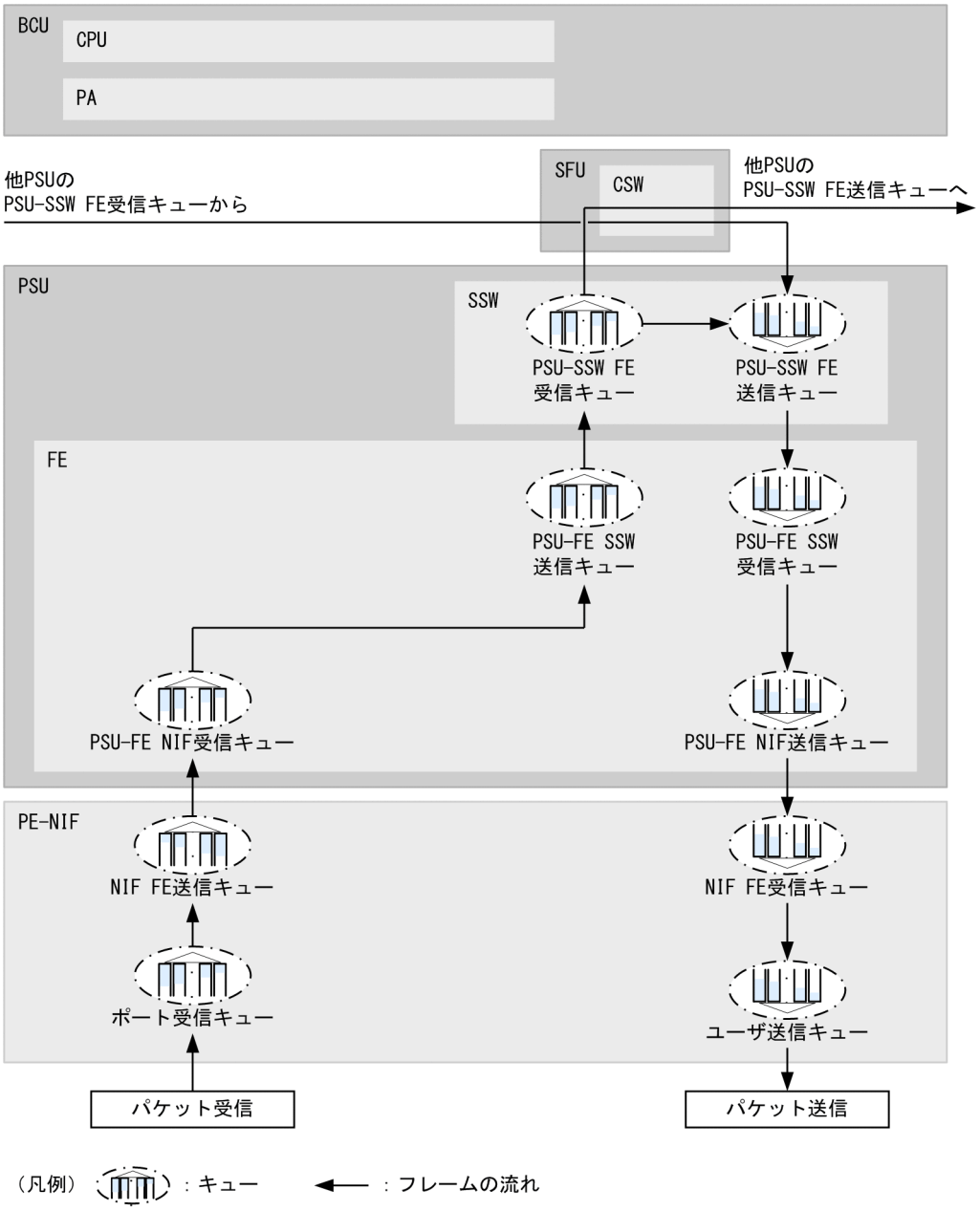
(4)　PE-NIF で階層化シェーパを使用した場合の装置内キューとフレームの流れ【OP-SHPS】

PE-NIF で階層化シェーパを使用した場合は，ポートシェーパを使用した場合と比較して，次に示す装置内キューが異なります。

- ポートシェーパ使用時のポート送信キューは，階層化シェーパ使用時はユーザ送信キューとなる

例として，AX8616S および AX8632S，PSU-11 および PSU-12 で，階層化シェーパを使用した場合の，装置内キューと BCU-CPU を経由しないフレームの流れを次に示します。

図 20-14　PE-NIF で階層化シェーパ使用時に AX8616S および AX8632S の PSU-11 および PSU-12 で BCU-CPU を経由しない場合



20.1.2　キュー長変更

装置内キューのうち，PSU-FE NIF 送信キューのキュー長（バッファ）を任意の値に変更できます。キュー長を拡張することで，該当する回線から送信されるバーストトラフィックに対して，キューあふれが起きにくくなります。

キュー長変更は，PE-NIF だけでサポートします。未サポートの NIF には変更を反映しません。

(1)　キュー長設定仕様

PSU-FE NIF 送信キューのキュー長について，デフォルト値と設定できる値を次に示します。

表 20–4　PSU-FE NIF 送信キューのキュー長（デフォルト値）

PSU の FE 数	装置のデフォルト値
1	2047
2	4095

表 20–5　PSU-FE NIF 送信キューのキュー長（設定できる値）

設定できる値	設定できるキュー長の合計値
4095※1，8191，16383，32767，65535，131071	NIF 当たりの合計値：131072 以下※2

注※1

FE 数が 2 の PSU では，運用に反映されません。設定した場合，該当する NIF のキュー長はデフォルト値になります。

注※2

コンフィグレーションコマンドで指定したキュー番号のキュー長の合計値です。キュー長の指定を省略したキュー番号のキュー長は合計値に含みません。その場合，キュー長をデフォルト値として扱います。

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

装置内キュ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 20-6　コンフィグレーションコマンド一覧

コマンド名	説明
system queue-length	装置内キューのキュー長を変更します。

20.2.2　装置内キューの設定

[設定のポイント]

装置内キューのキュー長を変更したあと，該当する NIF を再起動してください。NIF の再起動でキュー長の変更が反映されます。

[コマンドによる設定]

1. **(config)# system queue-length psu-fe to-nif 5 1 8191 2 8191 3 8191 4 8191**

   グローバルコンフィグレーションモードで，NIF 番号 5 にある PSU-FE NIF 送信キューのキュー番号 1，2，3，4 のキュー長をそれぞれ 8191 に設定します。

20.3　オペレーション

20.3.1　運用コマンド一覧

装置内キューの運用コマンド一覧を次の表に示します。

表 20-7　運用コマンド一覧

コマンド名	説明
show qos queueing	装置内のすべてのキュー情報を表示します。
clear qos queueing	show qos queueing コマンドで表示するすべてのキュー統計情報を 0 クリアします。
show qos queueing bcu	BCU のキュー情報を表示します。
clear qos queueing bcu	show qos queueing bcu コマンドで表示するキュー統計情報を 0 クリアします。
show qos queueing psu	PSU のキュー情報を表示します。
clear qos queueing psu	show qos queueing psu コマンドで表示するキュー統計情報を 0 クリアします。
show qos queueing nif	NIF のキュー情報を表示します。
clear qos queueing nif	show qos queueing nif コマンドで表示するキュー統計情報を 0 クリアします。
show qos queueing port	ポート送受信キュー情報を表示します。
clear qos queueing port	show qos queueing port コマンドで表示するキュー統計情報を 0 クリアします。
restart queue-control	シェーパを設定するキュー制御プログラムを再起動します。
dump queue-control	シェーパを設定するキュー制御プログラムで採取している制御情報をファイルへ出力します。
show shaper	階層化シェーパのユーザ送信キュー情報を表示します。
clear shaper	show shaper コマンドで表示する統計情報を 0 クリアします。

20.3.2　BCU のキュー情報の確認

show qos queueing bcu コマンドで BCU のキュー情報を確認できます。コマンドの実行結果を次の図に示します。

図 20-15　BCU のキュー情報の確認

```
> show qos queueing bcu cpu out
Date 20XX/01/01 12:00:00 UTC
BCU-CPU (Out)
 Max-queue=8
  Queue1   : Qlen=0, Limit-Qlen=256
                Send packets       Discard packets            Send bytes
   Total                 0                     0                     0
                              :
                              :
  Queue8   : Qlen=147, Limit-Qlen=256
                Send packets       Discard packets            Send bytes
   Total              8974655                     0            2297566580
>
```

BCU-CPU 送信キューでキューに積んだパケット数は Send packets，キューに積まれないで廃棄したパケット数は Discard packets，キューに積んだパケットのバイト数は Send bytes で確認します。

20.3.3　PSU のキュー情報の確認

show qos queueing psu コマンドで PSU のキュー情報を確認できます。コマンドの実行結果を次の図に示します。

図 20-16　PSU のキュー情報の確認

```
> show qos queueing psu 1 fe from-ssw control
Date 20XX/01/01 12:00:00 UTC
PSU1-FE (From-SSW Control)
 Max-queue=8
  Queue1   : Qlen=0, Peak-Qlen=0, Limit-Qlen=31
   Discard        Send packets       Discard packets            Send bytes
   1                         0                     0                     -
   2                         0                     0                     -
   3                         0                     0                     -
   4                         0                     0                     -
   Total                     0                     0                     0
                             :
                             :
  Queue8   : Qlen=0, Peak-Qlen=7, Limit-Qlen=31
   Discard        Send packets       Discard packets            Send bytes
   1                      2023                     0                     -
   2                         0                     0                     -
   3                         0                     0                     -
   4                         0                     0                     -
   Total                  2023                     0               1151320
>
```

PSU-FE SSW 受信キューでキューに積んだパケット数は Send packets，キューに積まれないで廃棄したパケット数は Discard packets，キューに積んだパケットのバイト数は Send bytes で確認します。なお，各廃棄優先度（Discard）および合計（Total）でそれぞれ値が表示されます。

20.3.4　NIF のキュー情報の確認

NLXLG-4Q または PE-NIF を使用している場合は，show qos queueing nif コマンドで NIF のキュー情報を確認できます。NIF が NLXGA-12RS の場合に NIF FE 受信キューを例として，コマンドの実行結果を次の図に示します。

図 20-17　NIF のキュー情報の確認

```
> show qos queueing nif 1 from-fe
Date 20XX/01/01 12:00:00 UTC
NIF1 (From-FE)
 Max-queue=4
                Send packets          Discard packets
  Queue1                   0                        0
  Queue2           344523416                        0
  Queue3                   0                        0
  Queue4             3573166                        0
>
```

NIF FE 受信キューでキューに積んだパケット数は Send packets，キューに積まれないで廃棄したパケット数は Discard packets で確認します。

20.3.5　イーサネットインタフェースのキュー情報の確認

show qos queueing port コマンドでイーサネットインタフェースのキュー情報を確認できます。コマンドの実行結果を次の図に示します。

図 20-18 イーサネットインタフェースのキュー情報の確認

```
> show qos queueing port 1/1 in
Date 20XX/01/01 12:00:00 UTC
NIF1/Port1 (In)
 Max-queue=1
  Queue1   : Qlen=0,  Peak-Qlen=68,  Limit-Qlen=127
   Discard        Send packets         Discard packets         Send bytes
   1                   8451361                       0                  -
   2                         0                       0                  -
   3                         0                       0                  -
   4                         0                       0                  -
   Total               8451361                       0         5813143908
>
```

ポート受信キューでキューに積んだパケット数は Send packets，キューに積まれないで廃棄したパケット数は Discard packets，キューに積んだパケットのバイト数は Send bytes で確認します。

21 L2 ループ検知

L2 ループ検知は，レイヤ 2 ネットワークでループ障害を検知して，ループの原因となるポートを inactive 状態にすることでループ障害を解消する機能です。

この章では，L2 ループ検知の解説と操作方法について説明します。

21.1　解説

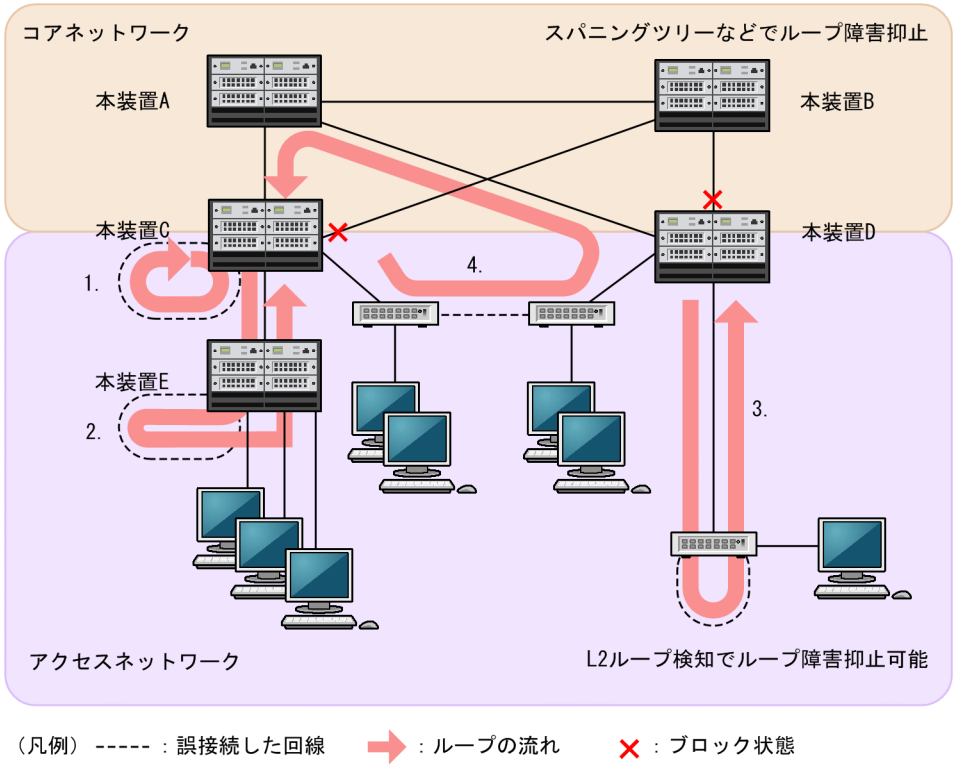
21.1.1　概要

レイヤ 2 ネットワークでは，ネットワーク内にループ障害が発生すると，MAC アドレス学習が安定しなくなったり，装置に負荷が掛かったりして正常な通信ができない状態になります。このような状態を回避するためのプロトコルとして，スパニングツリーや Ring Protocol などがありますが，L2 ループ検知は，一般的にそれらのプロトコルを動作させているコアネットワークではなく，冗長化をしていないアクセスネットワークでのループ障害を解消する機能です。

L2 ループ検知は，自装置でループ障害を検知した場合，検知したポートを inactive 状態にすることで，原因となっている個所をネットワークから切り離して，ネットワーク全体にループ障害が影響しないようにします。

ループ障害の基本パターンを次の図に示します。

図 21-1　ループ障害の基本パターン



ループ障害のパターン例

1. 本装置 C で回線を誤接続して，ループ障害が発生している。
2. 本装置 C より下位の本装置 E で回線を誤接続して，ループ障害が発生している。
3. 本装置 D より下位の装置で回線を誤接続して，ループ障害が発生している。
4. 下位装置で回線を誤接続して，コアネットワークにわたるループ障害が発生している。

L2 ループ検知は，このような自装置での誤接続や他装置での誤接続など，さまざまな場所でのループ障害を検知できます。

21.1.2　動作仕様

L2 ループ検知では，コンフィグレーションで設定したポート（物理ポートまたはチャネルグループ）から L2 ループ検知用の L2 制御フレーム（L2 ループ検知フレーム）を定期的に送信します。L2 ループ検知が有効なポートでその L2 ループ検知フレームを受信した場合，ループ障害と判断して，受信したポートまたは送信元ポートを inactive 状態にします。

inactive 状態のポートは，ループ障害の原因を解決したあと，運用コマンドで active 状態にします。また，自動復旧機能を設定しておけば，自動的に active 状態にできます。

(1)　本装置のサポート状況

L2 ループ検知は，スイッチポートでだけ動作します。

(2)　L2 ループ検知のポート種別

L2 ループ検知で使用するポートの種別を次の表に示します。

表 21-1　ポート種別

種別	機能
検知送信閉塞ポート	• ループを検知するための L2 ループ検知フレームを送信します。 • ループ障害検知時は，システムメッセージを表示して，該当ポートを inactive 状態にします。
検知送信ポート	• ループを検知するための L2 ループ検知フレームを送信します。 • ループ障害検知時は，システムメッセージを表示します。inactive 状態にはしません。
検知ポート （コンフィグレーション省略時）	• ループを検知するための L2 ループ検知フレームを送信しません。 • ループ障害検知時は，システムメッセージを表示します。inactive 状態にはしません。
検知対象外ポート	• 本機能の対象外ポートです。ループを検知するための L2 ループ検知フレームの送信やループ障害検知をしません。
アップリンクポート	• ループを検知するための L2 ループ検知フレームを送信しません。 • ループ障害検知時は，送信元ポートで，送信元のポート種別に従った動作をします。例えば，送信元が検知送信閉塞ポートの場合は，システムメッセージを表示して，送信元ポートを inactive 状態にします。

(3)　L2 ループ検知フレームの送信ポートについて

L2 ループ検知フレームは，検知送信閉塞ポートと検知送信ポートに所属しているすべての VLAN から，設定した送信間隔で送信します。本機能で送信できる最大フレーム数は決まっていて，それを超えるフレームは送信しません。フレームを送信できなかったポートや VLAN では，ループ障害を検知できなくなります。そのため，送信できる最大フレーム数は，収容条件に従って設定してください。詳細は，「コンフィグレーションガイド Vol.1」「3　収容条件」を参照してください。

(4)　ループ障害の検知方法とポートを inactive 状態にする条件

L2 ループ検知フレームを受信した場合，自装置から送信した L2 ループ検知フレームで，かつ受信ポートに設定されている VLAN であれば，異なる VLAN 間でもループ障害と見なします。L2 ループ検知フレー

ムの受信によってループ障害と判定すると，ポートごとにフレームの受信数をカウントします。この値がコンフィグレーションで設定した L2 ループ検知フレーム受信数（初期値は 1）に達すると，該当ポートを inactive 状態にします。

なお，Tag 変換などを使用して意図的に自装置に折り返すようなネットワーク構成にする場合は，対象のポートを検知対象外ポートに設定して，ループ障害を回避してください。

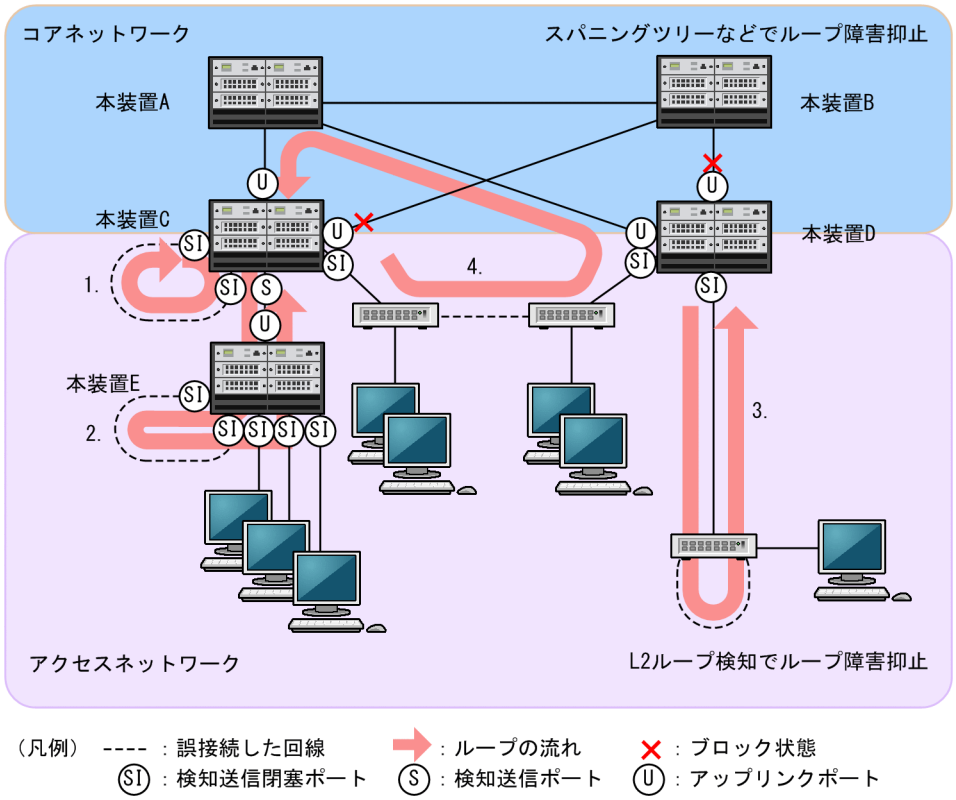
(5)　システムメッセージの表示について

L2 ループ障害検知によるシステムメッセージを一度表示したあと，同じポートで続けて L2 ループ検知フレームを受信しても，前回の表示から 1 分間は表示しません。前回の表示から 1 分間経過したあと，L2 ループ検知フレーム受信時にシステムメッセージを表示します。

21.1.3　適用例

L2 ループ検知を適用したネットワーク構成を示します。

図 21-2　L2 ループ検知を適用したネットワーク構成



(1)　検知送信閉塞ポートの適用

L2 ループ検知で一般的に設定するポート種別です。本装置 C，D，E で示すように，下位側のポートに設定しておくことで，1，2，3 のような下位側の誤接続によるループ障害に対応します。

(2)　検知送信ポートの適用

ループ障害の影響範囲を局所化するためには，できるだけ下位の装置で本機能を動作させるほうが有効です。本装置 C と本装置 E のように多段で接続している場合に，2.のような誤接続で本装置 C 側のポートを

inactive 状態にすると，本装置 E のループ障害と関係しないすべての端末で上位ネットワークへの接続ができなくなります。そのため，より下流となる本装置 E で L2 ループ検知を動作させることを推奨します。

なお，その場合は，本装置 C 側のポートには検知送信ポートを設定しておきます。この設定によって，正常運用時は本装置 E でループ障害を検知しますが，本装置 E で L2 ループ検知の設定誤りなどでループ障害を検知できないときには，本装置 C でループ障害を検知（inactive 状態にはならない）できます。

(3)　アップリンクポートの適用

上位ネットワークにつながっているポートまたはコアネットワークに接続するポートで設定します。この設定によって，4.のような誤接続となった場合，本装置 C の送信元ポートが inactive 状態になるため，コアネットワークへの接続を確保できます。

21.1.4　L2 ループ検知使用時の注意事項

(1)　L2 ループ検知の ID 設定について

同一ネットワーク内の複数の本装置で L2 ループ検知を動作させる場合，ID には各装置でユニークな値を設定してください。同一の値を設定すると，ループ障害が発生しても検知できません。

(2)　二重化構成での自動 active 状態設定について

自動的に active 状態にする設定をしていても，ループ障害検知でポートが inactive 状態のときに系切替が発生すると，新運用系 BCU ではそのポートは inactive 状態のままです。その場合は，運用コマンド activate でそのポートを active 状態にしてください。

(3)　inactive 状態にしたポートを自動的に active 状態にする機能（自動復旧機能）について

スタティックリンクアグリゲーション上で自動復旧機能を使用する場合は，次の点に注意してください。

- 回線速度を変更（ネットワーク構成の変更）する場合は，該当チャネルグループに異速度混在モードを設定してください。異速度混在モードを設定しないで回線速度を変更中にループを検知した場合，該当チャネルグループで自動復旧機能が動作しないおそれがあります。
- オートネゴシエーションで接続する場合は，回線速度を指定してください。指定しないと，回線品質の劣化などによって一時的に回線速度が異なる状態になり，低速回線が該当チャネルグループから離脱することがあります。この状態でループを検知した場合，該当チャネルグループで自動復旧機能が動作しないおそれがあります。

自動復旧機能が動作しない場合は，ループ原因を解消したあと，運用コマンド activate でポートを active 状態にしてください。

21.2　コンフィグレーション

21.2.1　コンフィグレーションコマンド一覧

L2 ループ検知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

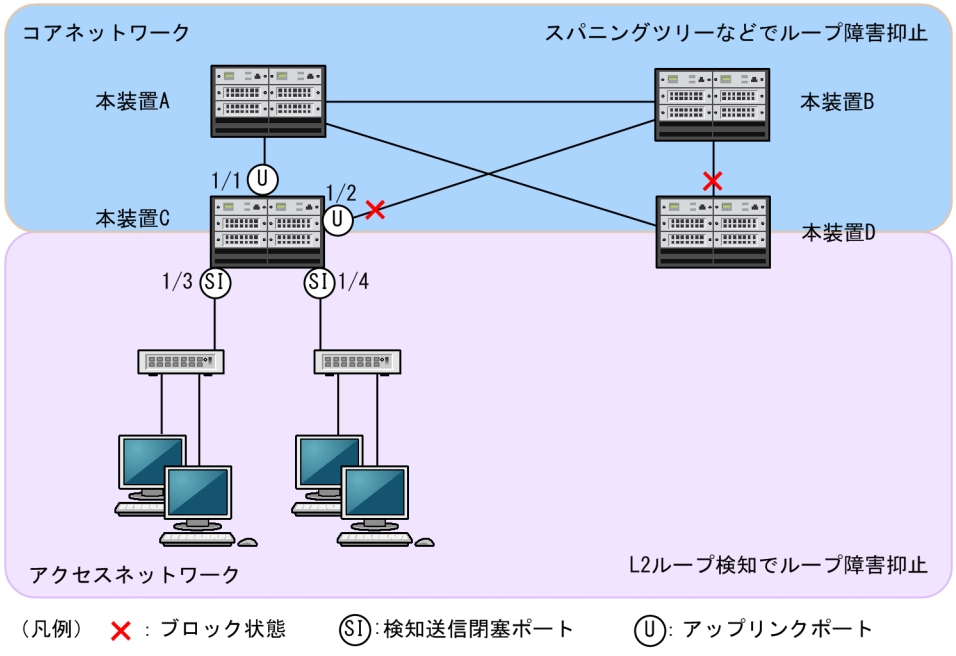
コマンド名	説明
loop-detection	L2 ループ検知でのポート種別を設定します。
loop-detection auto-restore-time	inactive 状態にしたポートを自動的に active 状態にするまでの時間を秒単位で指定します。
loop-detection enable	L2 ループ検知を有効にします。
loop-detection hold-time	inactive 状態にするまでの L2 ループ検知フレーム受信数の保持時間を秒単位で指定します。
loop-detection interval-time	L2 ループ検知フレームの送信間隔を設定します。
loop-detection threshold	ポートを inactive 状態にするまでの L2 ループ検知フレーム受信数を設定します。

21.2.2　L2 ループ検知の設定

L2 ループ検知を設定する手順を次に示します。ここでは，次の図に示す本装置 C の設定例を示します。

ポート 1/1 および 1/2 はコアネットワークと接続しているため，アップリンクポートに設定します。ポート 1/3 および 1/4 は下位装置と接続しているため，検知送信閉塞ポートに設定します。

図 21-3　L2 ループ検知の設定例



(1)　L2 ループ検知の設定

[設定のポイント]

L2 ループ検知のコンフィグレーションでは，装置全体で機能を有効にする設定と，実際に L2 ループ障害を検知するポートを設定する必要があります。

[コマンドによる設定]

1. **(config)# loop-detection enable id 64**
   本装置で L2 ループ検知を有効にします。
2. **(config)# interface range gigabitethernet 1/1-2**
   (config-if-range)# loop-detection uplink-port
   (config-if-range)# exit
   ポート 1/1 および 1/2 をアップリンクポートに設定します。この設定によって，ポート 1/1 および 1/2 で L2 ループ検知フレームを受信した場合，送信元ポートに対して送信元のポート種別に従った動作をします。
3. **(config)# interface range gigabitethernet 1/3-4**
   (config-if-range)# loop-detection send-inact-port
   (config-if-range)# exit
   ポート 1/3 および 1/4 を検知送信閉塞ポートに設定します。この設定によって，ポート 1/3 および 1/4 で L2 ループ検知フレームを送信します。また，これらのポートでループ障害を検知すると，該当ポートを inactive 状態にします。

(2)　L2 ループ検知フレームの送信間隔の設定

[設定のポイント]

L2 ループ検知フレームの最大送信レートを超えたフレームは送信しません。フレームを送信できなかったポートや VLAN では，ループ障害を検知できなくなります。L2 ループ検知フレームの最大送信レートを超える場合は，送信間隔を長く設定して最大送信レートに収まるようにする必要があります。

[コマンドによる設定]

1. **(config)# loop-detection interval-time 60**
   L2 ループ検知フレームの送信間隔を 60 秒に設定します。

(3)　inactive 状態にする条件の設定

[設定のポイント]

通常は，1 回のループ障害の検知で inactive 状態にします。この場合，初期値（1 回）のままで運用できます。しかし，瞬間的なループで inactive 状態にしたくない場合には，inactive 状態にするまでの L2 ループ検知フレーム受信数を設定できます。

[コマンドによる設定]

1. **(config)# loop-detection threshold 100**
   L2 ループ検知フレームを 100 回受信すると inactive 状態にするように設定します。
2. **(config)# loop-detection hold-time 60**
   L2 ループ検知フレームを最後に受信してからの受信数を 60 秒保持するように設定します。

(4)　自動復旧時間の設定

[設定のポイント]

inactive 状態にしたポートを自動的に active 状態にする場合に設定します。

[コマンドによる設定]

1. **(config)# loop-detection auto-restore-time 300**

300 秒後に，inactive 状態にしたポートを自動的に active 状態に戻す設定をします。

21.3　オペレーション

21.3.1　運用コマンド一覧

L2 ループ検知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 loop-detection	L2 ループ検知情報を表示します。
show loop-detection statistics	L2 ループ検知の統計情報を表示します。
show loop-detection logging	L2 ループ検知のログ情報を表示します。
clear loop-detection statistics	L2 ループ検知の統計情報をクリアします。
clear loop-detection logging	L2 ループ検知のログ情報をクリアします。
restart loop-detection	L2 ループ検知プログラムを再起動します。
dump protocols loop-detection	L2 ループ検知プログラムで採取している制御情報をファイルへ出力します。

21.3.2　L2 ループ状態の確認

show loop-detection コマンドで L2 ループ検知の設定と運用状態を確認できます。

L2 ループ検知フレームの送信レートが最大値を超えて，フレームを送信できないポートがないかを確認してください。VLAN Port Counts の Configuration が Capacity を超えていない場合は問題ありません。

ループ障害によって inactive 状態となっているポートは，Port Information の Status で確認できます。

図 21-4　L2 ループ検知の情報

```
> show loop-detection
Date 20XX/04/21 12:10:10 UTC
Loop Detection ID       :64
Interval Time           :10sec
Output Rate             :30pps
Threshold               :1
Hold Time               :infinity
Auto Restore Time       :-
VLAN Port Counts
    Configuration       :103         Capacity       :300
Port Information
  Port      Status     Type        DetectCnt RestoringTimer  SourcePort   Vlan
  1/1       Up         send-inact          0              -  -
  1/2       Down       send-inact          0              -  -
  1/3       Up         send                0              -  -
  1/4       Up         exception           0              -  -
  1/5       Down(loop) send-inact          1              -  ChGr:32(U)    100
  ChGr:1    Up         trap                0              -  -
  ChGr:32   Up         uplink              -              -  1/5           100
>
```

22 ストームコントロール

ストームコントロールは, フラッディング対象フレームの流量を制限する機能です。この章では, ストームコントロールの解説と操作方法について説明します。

22.1　解説

22.1.1　概要

レイヤ 2 ネットワークでは，ループ構成が存在すると，ブロードキャストフレームなどが装置間で無制限に中継されて，ネットワークおよび接続された機器に負荷を掛けます。この現象をブロードキャストストームと呼び，ネットワークの負荷軽減のため避ける必要があります。同様に，ユニキャストフレームが無制限に中継されるユニキャストストーム，マルチキャストフレームが無制限に中継されるマルチキャストストームも防止する必要があります。このようなフラッディング対象フレームの中継量を制限する機能がストームコントロールです。

本装置では，ストームコントロールの対象とするフレーム種別および受信帯域の閾値を設定して，ストームを監視します。閾値を超えるフレームを受信すると，ストームの発生を検出して，閾値を超えたフレームを廃棄します。同時に，あらかじめ設定しておいた動作を実施できます。

22.1.2　動作仕様

ストームコントロールの動作仕様は次のとおりです。

(1)　対象フレーム

ストームコントロールは，装置単位およびイーサネットインタフェース単位に設定できます。ストームコントロールの対象にできるフレーム種別を次に示します。

- ユニキャストフレーム
- マルチキャストフレーム
- ブロードキャストフレーム

(2)　ストームの発生

装置でストームコントロールを有効にしたあと，監視するインタフェースに閾値を設定すると，ストームの監視を開始します。インタフェースには，フレーム種別ごとに，受信帯域の閾値を設定します。

ストームの監視には，対象インタフェースの受信側で，該当フレームのフレーム間ギャップから FCS までのオクテット数で算出した値を使用します。なお，バーストサイズは 19240 オクテットであり，変更できません。

閾値を超えるフレームを受信したとき，ストームが発生したと判断します。発生時は，閾値を超えたフレームを廃棄し，コンフィグレーションコマンド storm-control action で設定した動作を実行します。このコマンドでは，次に示す動作を設定できます。

- ストーム発生のシステムメッセージを出力
- ストーム発生の SNMP 通知を送信
- 監視対象のインタフェースを inactive 状態に変更

(3)　ストームからの回復

ストームが発生したあと，受信帯域の閾値以下の状態が 30 秒間継続すると，ストームから回復したと判断します。回復時は，コンフィグレーションコマンド storm-control action で設定した動作を実行します。このコマンドでは，次に示す動作を設定できます。

- ストーム回復のシステムメッセージを出力
- ストーム回復の SNMP 通知を送信

なお，ストームの発生時または発生後に，対象インタフェースが inactive 状態の場合，回復時の動作は実行しません。また，ストーム発生時の動作で対象インタフェースが inactive 状態になった場合，ストームから回復しても自動では active 状態に戻りません。ストームから回復したことを確認したあと，運用コマンドで該当インタフェースを復旧してください。

22.1.3　ストームコントロール使用時の注意事項

(1)　ストームコントロールの対象外フレームについて

次に示すフレームは，ストームコントロールの監視対象外です。

- フィルタによって廃棄したフレーム
- QoS フロー廃棄によって廃棄したフレーム
- 本装置宛てのレイヤ 2 制御フレーム
- IGMP/MLD snooping でマルチキャストルータポートが未設定での未学習データフレーム

(2)　対象インタフェースについて

リンクアグリゲーションを構成するイーサネットインタフェースにストームコントロールを設定する場合は，すべてのイーサネットインタフェースで同じ設定にしてください。異なる設定にすると，ストームの発生およびストームからの回復を適切に検出できないおそれがあります。

(3)　受信帯域の閾値について

受信フレームが閾値を超えると，制御フレームも廃棄します。例えば，ブロードキャストフレームがストームコントロールの対象である場合，ARP や RIP などのブロードキャストで中継する制御フレームも廃棄します。

必要な制御フレームを廃棄しないように，極端に小さい値を閾値に設定しないでください。

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

ストームコントロールのコンフィグレーションコマンド一覧を次の表に示します。

表 22-1　コンフィグレーションコマンド一覧

コマンド名	説明
storm-control (global)	装置でストームコントロールの対象とするフレーム種別を設定します。
storm-control (イーサネットインタフェース)	インタフェースでストームコントロールの対象とするフレームの閾値を設定します。
storm-control action	ストームの発生時，およびストームからの回復時の動作を設定します。
storm-control enable	ストームコントロールを有効にします。

22.2.2　ストームコントロールの設定

ストームコントロールの設定例を次に示します。

[設定のポイント]

ストームコントロールを有効にして，対象とするフレーム種別および閾値を設定します。また，閾値を超えるフレームを受信したときの動作を設定します。

[コマンドによる設定]

1. **(config)# storm-control enable**

   本装置でストームコントロールを有効にします。

2. **(config)# no storm-control multicast**

   マルチキャストフレームをストームコントロールの対象外に設定します。

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

   (config-if)# storm-control action inactivate

   ストームの発生を検出したときに，イーサネットインタフェース 1/1 を inactive 状態に変更する設定をします。

4. **(config-if)# storm-control broadcast level 20**

   ブロードキャストフレームの閾値をイーサネットインタフェース 1/1 の帯域の 20%に設定します。

23 トラッキング機能

トラッキング機能は，ネットワークやネットワーク上の任意の装置を監視し，監視結果に基づいてネットワークの制御をする機能です。この章では，トラッキング機能の解説と操作方法について説明します。

23.1　解説

23.1.1　トラッキング機能の概要

トラッキング機能は，ネットワーク上の装置と通信できるかどうかを常時監視する機能です。トラッキング機能を使用すると，ネットワーク上の装置への通信状況を監視し，その状態について次に示す対応ができるようになります。

- 運用コマンドや MIB による，現在の監視状態の取得
- システムメッセージや SNMP 通知による，監視状態の変化の取得
- トラッキング連携をサポートする各機能による，監視状態と連携した装置の制御

また，トラッキング機能では，複数の監視を組み合わせられます。複数の監視を組み合わせ，トラッキング連携を結びつけることによって，組み合わせた条件に応じて通信経路やインタフェースを切り替えられます。

トラッキング連携とは，本装置の一部の制御機能がサポートする付加機能です。トラッキング連携をサポートする制御機能では，監視対象の状態に応じて制御を切り替えられます。トラッキング機能とトラッキング連携を結びつけることによって，装置への到達性に応じて通信経路やインタフェースを切り替えられます。

トラッキング機能での監視インスタンスをトラックと呼びます。監視状態はトラックで管理します。

23.1.2　BFD とトラッキング機能の関係について

BFD は，ユニキャストルーティングの隣接ルータを監視する機能です。ユニキャストルーティングに BFD 連携動作を指定すると，ユニキャストルーティングが隣接ルータを決定した時点で BFD による監視を要求します。この結果，BFD セッションが作成されます。

本装置では，BFD 連携動作の指定方法として，BFD を指定したトラックのコンフィグレーションを使用します。また，BFD セッションはトラックとしても管理されます。このため，トラックには，トラッキング機能のトラックと BFD のトラックの 2 種類があります。この 2 種類のトラックを見分ける必要がある場合，トラッキング機能によるトラックを静的監視トラック，BFD による監視インスタンスを動的監視トラックと呼びます。

表 23–1　監視対象の決定方法によるトラックの種別

種別	説明
静的監視トラック	トラッキング機能のコンフィグレーションで監視対象を指定するトラックです。
動的監視トラック	BFD 連携サポート各機能が監視対象を要求するトラックです。

以降，本章でトラックという場合，基本的に静的監視トラック，つまりトラッキング機能のトラックのことを指します。BFD については，「コンフィグレーションガイド Vol.3」「30　BFD」を参照してください。

23.1.3　トラックの解説

トラックは，コンフィグレーションで指定した方法で，指定した対象を監視します。

トラックが監視した結果を示す状態をトラック状態と呼び，トラックが監視する対象をトラック対象と呼びます。トラック状態は，次のどちらかの状態です。

- Up
  トラック対象が使用できることを示します。
- Down
  トラック対象が使用できないことを示します。

23.1.4　サポート仕様

トラック種別に関するサポート仕様を次の表に示します。

表 23-2　トラック種別

トラック種別		説明
ポーリング監視	ICMP 監視	ネットワーク上の装置を監視します。 ICMP Echo パケットを使用してポーリングをして，ICMP Echo Reply パケットの受信で Up とする監視方法です。IPv4 および IPv6 による監視をサポートします。
インタフェース監視	イーサネットインタフェース監視	イーサネットインタフェースを監視します。 イーサネットインタフェースの状態をトラック状態とする監視方法です。
	ポートチャネルインタフェース監視	ポートチャネルインタフェースを監視します。 ポートチャネルインタフェースの状態をトラック状態とする監視方法です。
リスト監視	AND リスト監視	複数のトラックを監視します。 トラック状態の論理積をトラック状態とする監視方法です。
	OR リスト監視	複数のトラックを監視します。 トラック状態の論理和をトラック状態とする監視方法です。

トラック動作に関するサポート仕様を次の表に示します。

表 23-3　トラック動作

トラック動作（状態）	説明
デフォルトトラック状態	トラック動作（監視）の開始前や停止中のトラック状態です。コンフィグレーションで指定できます。
トラック停止	トラック動作（監視）をコンフィグレーションで停止できます。
BCU 起動時の監視開始動作	BCU 起動時にトラック動作（監視）を開始するまでの時間を，コンフィグレーションで指定できます。
系切替時の監視開始動作	系切替時にトラック動作（監視）を開始するまでの時間を，コンフィグレーションで指定できます。
トラック状態の BCU 間同期	系切替直後のトラック状態を，旧運用系 BCU から引き継ぎます。

23.1.5　ポーリング監視

ポーリング監視は，ネットワーク上の装置をトラック対象とし，定期的にポーリングパケットを送信して，通信できればトラック状態を Up とするトラック種別です。

ポーリング監視では，トラック対象の装置へ定期的にポーリングパケットを送信し，その応答パケットを受信するかどうかを監視します。応答パケットを受信したらポーリング成功と見なし，連続して成功するとトラック状態が Up になります。応答パケットを受信しないとポーリング失敗と見なし，連続して失敗するとトラック状態が Down になります。

本装置のトラッキング機能では，ポーリング監視の方法として ICMP 監視をサポートしています。

(1)　ICMP 監視

ICMP 監視では，トラック対象としてネットワーク上の装置を IP アドレスで指定します。本装置は，ポーリングパケットとして，ICMP Echo パケットをトラック対象の IP アドレスへ定期的に送信します。ポーリングの応答パケットとして ICMP Echo Reply パケットを受信するかどうかを監視します。

(2)　ポーリングの成否と検証シーケンス

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，実質的に通信できないネットワークでも，一時的に通信できてしまうことがあります。このようなネットワークにポーリング監視を適用し，ポーリングの成否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ことがあります。このような状況に対応するため，本装置のポーリング監視では，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を指定できます。

また，ポーリング監視には，トラック状態のほかに，トラックの動作状況を示すトラック動作状態という状態があります。以降，各トラック動作状態とポーリング動作について説明します。

(a)　動作中

ポーリングの応答が安定している間，トラック動作状態は動作中になります。動作中の場合，ポーリングパケットの送信間隔にはコンフィグレーションコマンド interval の設定値が適用されます。

(b)　検証中（障害回復検証）

トラック状態が Down のときにポーリング応答を受信すると，トラック動作状態を検証中に更新します。

トラック状態を Down から Up に変更するかどうかの検証を，障害回復検証と呼びます。障害回復検証中は，コンフィグレーションコマンド recovery detection で設定するパラメータに従って，ポーリング動作をします。設定するパラメータと障害回復検証中のポーリング動作について次の表に示します。

表 23-4　障害回復検証中のポーリング動作

パラメータ	項目	説明
interval <seconds>	ポーリング間隔	障害回復検証中のポーリングパケット送信間隔
<success count>	ポーリング成功回数	トラック状態を Up に変更するために必要なポーリング成功回数 （障害回復検証を始めるきっかけとなったポーリングの成功も回数に含みます）
trial <count>	ポーリング試行回数	障害回復検証中のポーリング最大試行回数

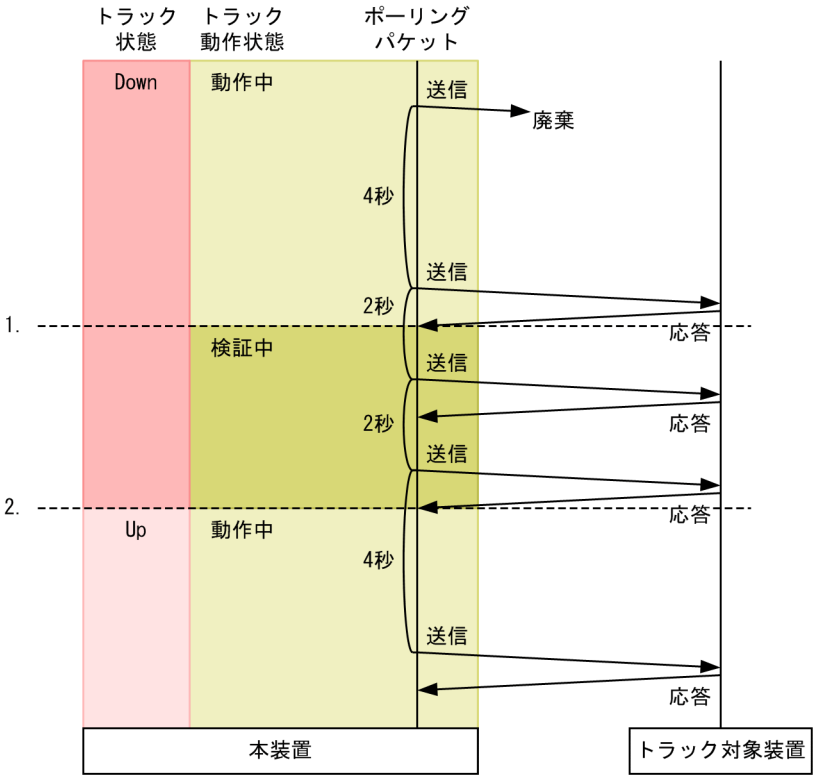
障害回復検証は，次のどちらかの条件を満たすまで実施します。

- ポーリングの成功回数が<success count>の設定値に達し，トラック状態を Up に変更する
- ポーリングの失敗回数が trial <count>－<success count>＋ 1 に達し，トラック状態が Down に確定する

障害回復検証が終了すると，トラック動作状態は前述した動作中に戻ります。

障害回復検証によって，トラック状態が Down から Up に遷移する場合のシーケンスを次の図に示します。この例では，トラック動作状態が動作中の場合のポーリング間隔を 4 秒，障害回復検証中のポーリング間隔を 2 秒，ポーリング成功回数を 3 回としています。

図 23-1　障害回復検証シーケンス例



1. トラック状態が Down，トラック動作状態が動作中のときに，トラック対象装置からポーリングの応答パケットを受信します。これを契機に，トラック動作状態は検証中に遷移し，ポーリング間隔が 2 秒に変更されます。
2. ポーリング成功回数を 3 回に設定しているため，3 回目の応答パケットの受信を契機として，トラック状態を Up に更新します。あわせて，トラック動作状態は検証中から動作中に遷移し，ポーリング間隔も 4 秒に戻ります。

(c)　検証中（障害発生検証）

トラック状態が Up のときにポーリングに失敗すると，トラック動作状態を検証中に更新します。

トラック状態を Up から Down に変更するかどうかの検証を，障害発生検証と呼びます。障害発生検証中は，コンフィグレーションコマンド failure detection で設定するパラメータに従って，ポーリング動作をします。設定するパラメータと障害発生検証中のポーリング動作について次の表に示します。

表 23-5　障害発生検証中のポーリング動作

パラメータ	項目	説明
interval <seconds>	ポーリング間隔	障害発生検証中のポーリングパケット送信間隔

パラメータ	項目	説明
<failure count>	ポーリング失敗回数	トラック状態を Down に変更するために必要なポーリング失敗回数 （障害発生検証を始めるきっかけとなったポーリングの失敗も回数に含みます）
trial <count>	ポーリング試行回数	障害発生検証中のポーリング最大試行回数

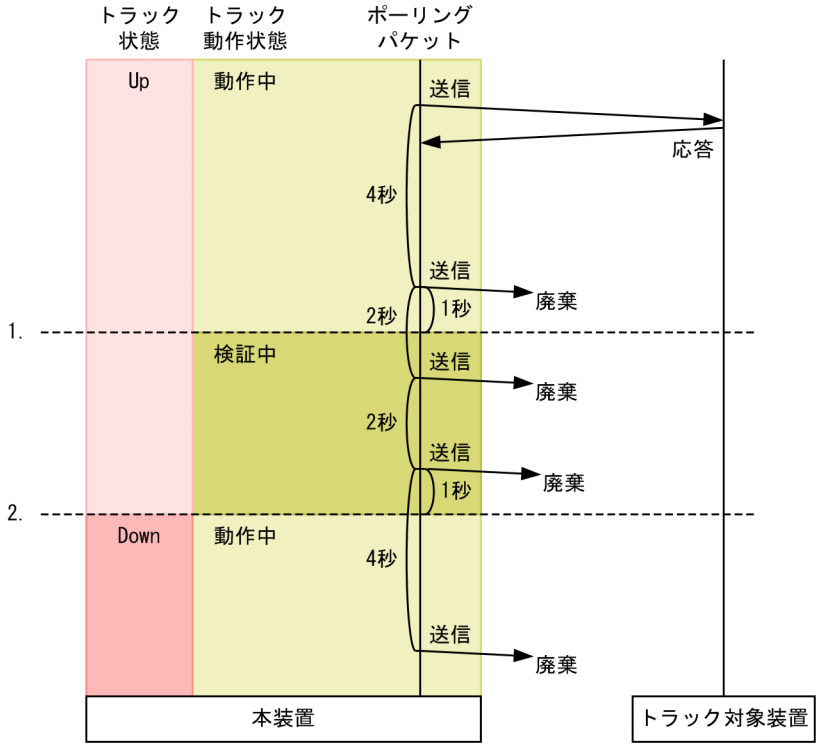
障害発生検証は，次のどちらかの条件を満たすまで実施します。

- ポーリングの失敗回数が<failure count>の設定値に達し，トラック状態を Down に変更する
- ポーリングの成功回数が trial <count>－<failure count>＋ 1 に達し，トラック状態が Up に確定する

障害発生検証が終了すると，トラック動作状態は前述した動作中に戻ります。

障害発生検証によって，トラック状態が Up から Down に遷移する場合のシーケンスを次の図に示します。この例では，トラック動作状態が動作中の場合のポーリング間隔を 4 秒，障害発生検証中のポーリング間隔を 2 秒，ポーリング失敗回数を 3 回，ポーリングの応答待ち時間を 1 秒としています。

図 23-2　障害発生検証シーケンス例



1. トラック状態が Up，トラック動作状態が動作中のときに，トラック対象装置からポーリングの応答パケットを応答待ち時間（1 秒）内に受信できませんでした。これを契機に，トラック動作状態は検証中に遷移し，ポーリング間隔が 2 秒に変更されます。
2. ポーリング失敗回数を 3 回に設定しているため，3 回目のポーリング失敗を契機として，トラック状態を Down に更新します。あわせて，トラック動作状態は検証中から動作中に遷移し，ポーリング間隔も 4 秒に戻ります。

(3)　ポーリングパケットのネクストホップ指定

トラッキング機能では，ICMP 監視トラックにネクストホップを指定できます。ポーリングパケットの宛先はトラック対象装置のアドレスですが，ネクストホップを指定すると，宛先アドレスや本装置の経路に関係なくネクストホップで指定した隣接装置へ転送されます。こうすると，ネクストホップで指定した装置を経由するトラック対象装置への通信を確認できます。

この機能を利用すると，本装置に接続したルータを経由するトラック対象装置への通信可能性を監視できます。例えば，本装置が 2 台のルータと接続していて，どちらのルータも同じサーバと接続している場合，トラック対象がサーバでネクストホップが各ルータとなる二つのトラックを設定することで，ルータ個別にサーバとの通信を確認できます。

(4)　ポーリング応答パケットの受信インタフェース指定

ICMP 監視トラックでネクストホップを指定している場合でも，障害に対して冗長経路を用意してあると，次の図に示すように，本装置自体やほかのルータを経由する冗長経路によってポーリングに成功し，意図した監視ができないことがあります。

図 23-3　冗長経路による意図しないポーリング成功例（自装置を経由する例）

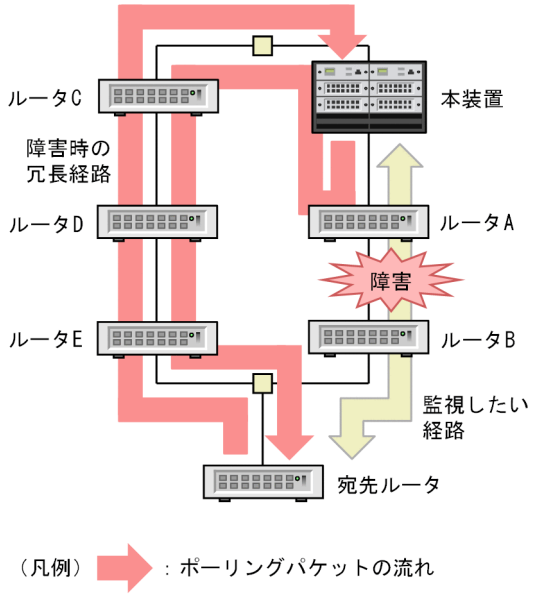
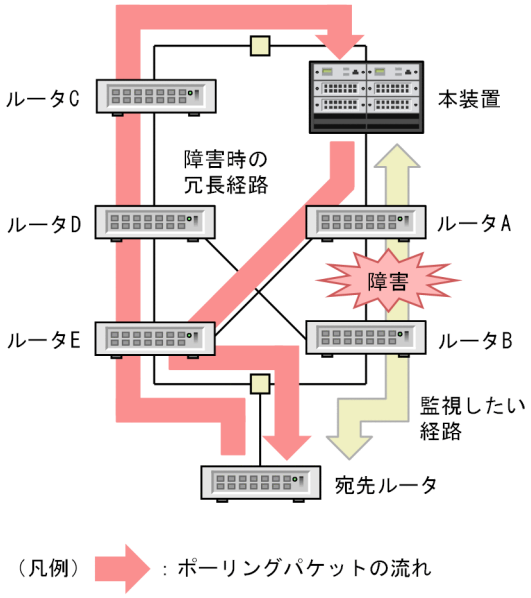


図 23-4　冗長経路による意図しないポーリング成功例（ほかのルータを経由する例）



意図しないポーリング成功を回避するために，本装置のトラッキング機能のポーリング監視では，コンフィグレーションコマンド icmp check-reply-interface で応答パケットの受信インタフェースを指定できます。受信インタフェースを指定した場合，指定したインタフェース以外で受信した応答パケットが廃棄されて，ポーリング失敗となります。

上図の例の場合，ポーリングパケットのネクストホップにルータ A を指定した上で，応答パケットの受信インタフェースとしてルータ A への接続インタフェースを指定することで，冗長経路による通信をポーリング失敗とします。

(5)　ポーリング監視の注意事項

すべての ICMP 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 1000pps です。

1000pps 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。1000pps を超える構成にした場合，結果として，1000pps に納まるようにすべてのトラックのポーリング間隔が長くなります。検証時にポーリング間隔が変わることを考慮した上で，1000pps に収まるようにしてください。

23.1.6　インタフェース監視

インタフェース監視は，インタフェースの Up/Down 状態をトラック状態に反映するトラック種別です。インタフェース状態が Up のときにトラック状態は Up になり，インタフェース状態が Down のときにトラック状態は Down になります。インタフェース監視では，イーサネットインタフェースおよびポートチャネルインタフェースの状態を監視できます。

なお，インタフェース監視トラックには，ポーリング監視のような状態遷移時の検証動作はありません。インタフェース状態が変化すると，その瞬間にトラック状態も変化します。

23.1.7　リスト監視

リスト監視は，複数のトラックをトラック対象として，それらのトラック状態を組み合わせてトラック状態とするトラック種別です。リスト監視は通常，トラッキング連携で複数のトラック状態と連携するときに使用します。例えば，次のような場合にリスト監視を使用します。

- 複数のサーバがあるデータセンターが二つあり，すべてのサーバが使用できるデータセンターを選択して通信したい場合
- ネットワーク上にルータが並列に 2 台あり，どちらか 1 台のルータが使用できれば通信に使用したい場合

リスト監視には，AND リスト監視と OR リスト監視があり，どちらを使用するかをコンフィグレーションコマンド boolean で設定します。AND リスト監視と OR リスト監視について，次の表に示します。

表 23-6　AND リスト監視と OR リスト監視

リスト監視の種類	トラック状態の判定
AND リスト監視	トラック対象の全トラックのトラック状態が Up の場合に，リスト監視トラックのトラック状態を Up とします。
	トラック対象のうちどれか一つのトラックでもトラック状態が Down の場合に，リスト監視トラックのトラック状態を Down とします。
OR リスト監視	トラック対象のうちどれか一つのトラックでもトラック状態が Up の場合に，リスト監視トラックのトラック状態を Up とします。
	トラック対象の全トラックのトラック状態が Down の場合に，リスト監視トラックのトラック状態を Down とします。

また，リスト監視では，トラック対象のトラックごとに，逆の状態（否定）で認識することをコンフィグレーションコマンド target object の not パラメータで指定できます。トラック対象に not パラメータを指定すると，該当するトラック対象のトラック状態が Down のときに，リスト監視トラックのトラック状態が Up になります。not パラメータを指定した AND リスト監視と OR リスト監視について，次の表に示します。

表 23-7　AND リスト監視と OR リスト監視（not パラメータ指定）

リスト監視の種類	トラック状態の判定
AND リスト監視	not パラメータを指定していないトラック対象のトラック状態がすべて Up で，not パラメータを指定したトラック対象のトラック状態がすべて Down の場合だけ，リスト監視トラックのトラック状態を Up とします。
OR リスト監視	どちらかの条件を満たす場合に，リスト監視トラックのトラック状態を Up とします。 • not パラメータを指定していないトラック対象のトラック状態がどれか一つでも Up の場合 • not パラメータを指定したトラック対象のトラック状態がどれか一つでも Down の場合

AND リスト監視と OR リスト監視のどちらでも，トラック対象を一つも設定していないリスト監視トラックのトラック状態は Down です。

リスト監視トラックは，ほかのリスト監視トラックをトラック対象に指定できます。リスト監視トラックによるリスト監視トラックの監視は，8 段まで重ねられます。

なお，リスト監視トラックには，ポーリング監視のような状態遷移時の検証動作はありません。トラック対象のトラック状態が変化すると，その瞬間にリスト監視トラックのトラック状態も変化します。

23.1.8　トラック動作

トラッキング機能では，トラックのコンフィグレーションを追加したり変更したりする間，またはBCU起動時や系切替時に，トラッキング連携で動作する制御対象にとって影響が少ないトラック状態に固定し，影響が少ないタイミングでトラックの動作を開始させられます。

(1)　デフォルトトラック状態

デフォルトトラック状態は，系切替時を除くトラック停止時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，トラックごとに設定できます。コンフィグレーションを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。

コンフィグレーションでトラック種別を指定していないトラックや，コンフィグレーションで停止しているトラックでも，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。つまり，リスト監視トラックやトラッキング連携をしている機能が参照しているトラックにトラック種別が指定されていない場合，そのトラックはデフォルトトラック状態として動作します。これによって，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しておくと，コンフィグレーションで設定済みのトラッキング連携を削除しないで，影響を与えないように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停止

トラックにコンフィグレーションコマンドshutdownを設定すると，トラックごとに動作を停止できます。動作を停止しているトラックの状態は，デフォルトトラック状態です。

(3)　装置起動時のトラック動作

ポーリング監視トラックおよびインタフェース監視トラックは，本装置が起動または再起動してからしばらくの間，動作を停止します。これは，装置が起動した直後は，次に示す理由などによって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

本装置が起動してからこれらのトラックが動作を開始するまでのトラック動作状態を，起動中と呼びます。起動中のトラック状態は，デフォルトトラック状態です。

本装置が起動してからポーリング監視トラックおよびインタフェース監視トラックが動作を開始するまでの時間は，装置全体についてコンフィグレーションで変更できます。本装置が起動してから，ポーリング監視トラックが使用する通信，または監視するインタフェース状態が安定するまでの時間を指定してください。デフォルトでは600秒です。

なお，リスト監視トラックは，本装置が起動または再起動すると，すぐに動作を開始します。

(4)　系切替時のトラック動作

BCUを二重化構成で運用している場合，ポーリング監視トラックおよびインタフェース監視トラックは，系切替後，現在の装置の状態や経路情報を収集する時間を待つために，動作を停止します。

系切替してからこれらのトラックが動作を開始するまでのトラック動作状態を，切替中と呼びます。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。こうすることで，トラッキング連携をサポートしている機能が系切替前と同じトラック状態に基づいて制御できるため，トラッキング連携を使用しても系切替時に通信を継続できます。

系切替してからポーリング監視トラックおよびインタフェース監視トラックが動作を開始するまでの時間は，装置全体についてコンフィグレーションで変更できます。系切替してからパケットの送受信が安定するまでの時間を指定してください。デフォルトでは 180 秒です。

なお，リスト監視トラックは，系切替後すぐに動作を開始します。しかし，リスト監視トラックが監視している各トラックが系切替前のトラック状態を引き継いでいるため，リスト監視トラックも実質的には系切替前のトラック状態を引き継ぐことになります。

23.2　トラッキング連携の解説

トラッキング連携をサポートした制御機能では，一つの制御対象につき通常は一つのトラックを指定して，制御対象の状態がトラック状態と同じになるように制御します。具体的には，トラック状態が Up のときだけ制御対象を使用できるようにして，トラック状態が Down の間は制御対象を使用できないようにします。トラッキング連携を使用することで，トラックで通信できることを確認できた場合だけ動作するように制御できます。

また，一部の制御機能では，トラッキング連携の代替連携をサポートしています。代替連携は，通常のトラッキング連携とは逆に，制御対象の状態をトラック状態と逆になるように制御します。具体的には，トラック状態が Up の間は制御対象を使用できないようにして，トラック状態が Down のときだけ制御対象を使用できるようにします。代替連携を使用して，主な通信経路をトラック対象とし，代替通信方法を制御対象とすることで，主な通信経路で障害を検出した場合に代替通信方法に切り替えられます。

23.2.1　サポート仕様

トラッキング連携をサポートする制御機能を次の表に示します。

表 23-8　トラッキング連携のサポート仕様一覧

機能名	代替連携	連携内容の説明
イーサネットインタフェース※1	○	トラック状態が Up の間だけ，イーサネットインタフェースを使用できるようにします。
IP インタフェース※2	○	トラック状態が Up の間だけ，IP インタフェースを使用できるようにします。
VRRP	×	トラック状態に応じて仮想ルータの優先度を変更します。
スタティックルーティング	○	トラック状態が Up の間だけ，IPv4 スタティック経路および IPv6 スタティック経路を有効にします。
ポリシーベースルーティング	○	トラック状態が Up の間だけ，ポリシーベースルーティングのネクストホップを有効にします。

（凡例）　○：サポート　×：未サポート

注※1　マネージメントポートを除きます。

注※2　マネージメントポート，AUX ポートを除きます。

23.2.2　イーサネットインタフェースのトラッキング連携

本装置のイーサネットインタフェースは，トラッキング連携をサポートしています。イーサネットインタフェースにトラックを指定すると，トラック状態が Down の間はインタフェースをシャットダウン状態にします。トラック状態が Up の間はシャットダウン状態を解除し，回線の状態に応じてリンクアップまたはリンクダウンします。

本装置のイーサネットインタフェースでは，トラッキング連携の代替連携もサポートしています。イーサネットインタフェースにトラックと代替連携を指定すると，トラック状態が Up の間はインタフェースをシャットダウン状態にします。

23.2.3　IP インタフェースのトラッキング連携

本装置の IP インタフェースは，トラッキング連携をサポートしています。IP インタフェースにトラックを指定すると，トラック状態が Down の間は IP インタフェースをシャットダウン状態にします。トラック状態が Up の間はシャットダウン状態を解除し，IP インタフェースの実体であるインタフェースの状態に応じて UP 状態または DOWN 状態にします。

本装置の IP インタフェースでは，トラッキング連携の代替連携もサポートしています。IP インタフェースにトラックと代替連携を指定すると，トラック状態が Up の間は IP インタフェースをシャットダウン状態にします。

23.2.4　VRRP のトラッキング連携

本装置の VRRP はトラッキング連携をサポートしていて，トラック状態に応じて仮想ルータの優先度を変更できます。詳細は「コンフィグレーションガイド Vol.3」「12.1.6　トラッキング連携による優先度変更」を参照してください。

23.2.5　スタティックルーティングのトラッキング連携

本装置のスタティックルーティング機能は，トラッキング連携をサポートしています。スタティック経路にトラックを指定すると，トラック状態が Down の間はスタティック経路が無効になります。トラック状態が Up の間は，ゲートウェイへの経路の有無や IP インタフェースの状態に応じてスタティック経路が有効になり，同じ宛先プレフィックスへの経路の中でスタティック経路が最優先である場合には，そのスタティック経路がアクティブ経路になります。

本装置のスタティックルーティング機能では，トラッキング連携の代替連携もサポートしています。スタティック経路にトラックと代替連携を指定すると，トラック状態が Up の間はスタティック経路を無効にします。

23.2.6　ポリシーベースルーティングのトラッキング連携

本装置のポリシーベースルーティングは，トラッキング連携をサポートしています。ポリシーベースルーティングのネクストホップとトラッキング連携することで，トラック状態に応じてネクストホップの切り替えができます。詳細は，「コンフィグレーションガイド Vol.3」「8.1.6　ネクストホップのトラッキング連携」を参照してください。

23.3　コンフィグレーション

23.3.1　コンフィグレーションコマンド一覧

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 23-9　コンフィグレーションコマンド一覧（トラッキング機能）

コマンド名	説明
boolean	リスト監視の論理演算方法を指定します。
default-state	デフォルトトラック状態を指定します。
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指定します。
icmp	ICMP 監視での IP パケットを設定します。
icmp check-replay-interface	ICMP 監視の受信インタフェースを指定します。
interval	ポーリング間隔を指定します。
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指定します。
shutdown	トラックの動作を停止します。
target interface	インタフェース監視の対象インタフェースを指定します。
target ip	ICMP 監視の対象 IPv4 アドレスを指定します。
target ipv6	ICMP 監視の対象 IPv6 アドレスを指定します。
target object	リスト監視のトラック対象を指定します。
timeout	ポーリング応答待ち時間を指定します。
track-target aging-interval	系切替時の一時的なトラック監視停止時間を指定します。
track-target init-interval	BCU 起動時の一時的なトラック監視停止時間を指定します。
track-target name	静的監視のトラックを設定します。
type	トラック種別を指定します。
track name※	動的監視のトラックを設定します。

注※

「コンフィグレーションコマンドレファレンス Vol.3」「25　BFD」を参照してください。

トラッキング連携をサポートする機能の, トラッキング連携について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 23-10　コンフィグレーションコマンド一覧（トラッキング連携をサポートする機能）

コマンド名	説明
track-target-control-shutdown※1	イーサネットインタフェースに連携するトラックを指定します。
track-target-control-ip-down※2	IP インタフェースに連携するトラックを指定します。

コマンド名	説明
policy-interface※3	ポリシーベースルーティングリストにネクストホップを設定します。パラメータで連携するトラックを指定できます。
vrrp track-target※4	仮想ルータに，連携するトラックと連携方法を指定します。
ip route※5	IPv4 スタティック経路を設定します。パラメータで連携するトラックを指定できます。
ipv6 route※6	IPv6 スタティック経路を設定します。パラメータで連携するトラックを指定できます。

注※1
「コンフィグレーションコマンドレファレンス Vol.1」「16　イーサネット」を参照してください。

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

注※3
「コンフィグレーションコマンドレファレンス Vol.3」「8　ポリシーベースルーティング」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」「12　VRRP」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」「15　スタティックルーティング (IPv4)」を参照してください。

注※6
「コンフィグレーションコマンドレファレンス Vol.3」「16　スタティックルーティング (IPv6)」を参照してください。

23.3.2　ICMP 監視トラックの設定

ICMP 監視トラックの設定例を次に示します。

[設定のポイント]

ICMP 監視には，応答待ち時間，ポーリング間隔，ポーリング回数など，複数の設定パラメータがあります。すべてのパラメータを指定してからポーリングを開始したい場合は，次の順に設定してください。

1. track-target name コマンドでトラック名を指定する
2. shutdown コマンドを設定してトラックの動作を停止する
3. すべてのパラメータを指定する
4. shutdown コマンドを削除する

なお，ICMP 監視では，送信元 IP アドレスを設定しておくことを推奨します。応答パケットの宛先アドレスが固定されて，応答パケットの経路が設計しやすくなるためです。

ここでは，IPv4 の ICMP 監視の設定例を示します。

[コマンドによる設定]

1. **(config)# track-target name TRACK1000**
   設定するトラック名（TRACK1000）を指定します。
2. **(config-track-target)# shutdown**

トラック（TRACK1000）の動作を停止します。

3. **(config-track-target)# default-state up**

   トラック（TRACK1000）のデフォルトトラック状態を Up と設定します。これ以降，トラックが動作を始めてポーリングに失敗し，検証して Down であると確定するまで，トラック状態は Up です。

4. **(config-track-target)# type icmp**

   (config-track-target)# target ip 192.0.2.2 source 198.51.100.1

   (config-track-target)# timeout 5

   (config-track-target)# interval 10

   (config-track-target)# failure detection 4 trial 5 interval 10

   (config-track-target)# recovery detection 4 trial 5 interval 10

   トラック（TRACK1000）を，192.0.2.2 を監視する ICMP 監視トラックとして設定します。ポーリングパケットの送信元アドレスには 198.51.100.1 を指定します。ほかに，次の項目を指定します。

   - 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およびポーリング間隔
   - 障害回復検証中のポーリング回数およびポーリング間隔

5. **(config-track-target)# no shutdown**

   トラック（TRACK1000）の動作を停止するコンフィグレーションを削除します。削除するとすぐに，トラックが動作を始めます。

23.3.3　インタフェース監視トラックの設定

インタフェース監視トラックの設定例を次に示します。

[設定のポイント]

ここでは，イーサネットインタフェースを監視する設定例を示します。

[コマンドによる設定]

1. **(config)# track-target name TRACK1000**

   設定するトラック名（TRACK1000）を指定します。

2. **(config-track-target)# type interface**

   (config-track-target)# target interface gigabitethernet 1/5

   トラック（TRACK1000）を，イーサネットインタフェース 1/5 を監視するインタフェース監視トラックとして設定します。

23.3.4　リスト監視トラックの設定

リスト監視トラックの設定を次に示します。

[設定のポイント]

すべてのトラック対象のトラックを指定してからリスト監視を開始したい場合は，次の順に設定してください。

1. track-target name コマンドでトラック名を指定する
2. shutdown コマンドを設定してトラックの動作を停止する

3. すべてのトラック対象のトラックを指定する
4. shutdown コマンドを削除する

ここでは，トラック（TRACK_A）のトラック状態が Up，かつトラック（TRACK_B）のトラック状態が Down の場合に限って，トラック状態が Up となるリスト監視トラックの設定例を示します。

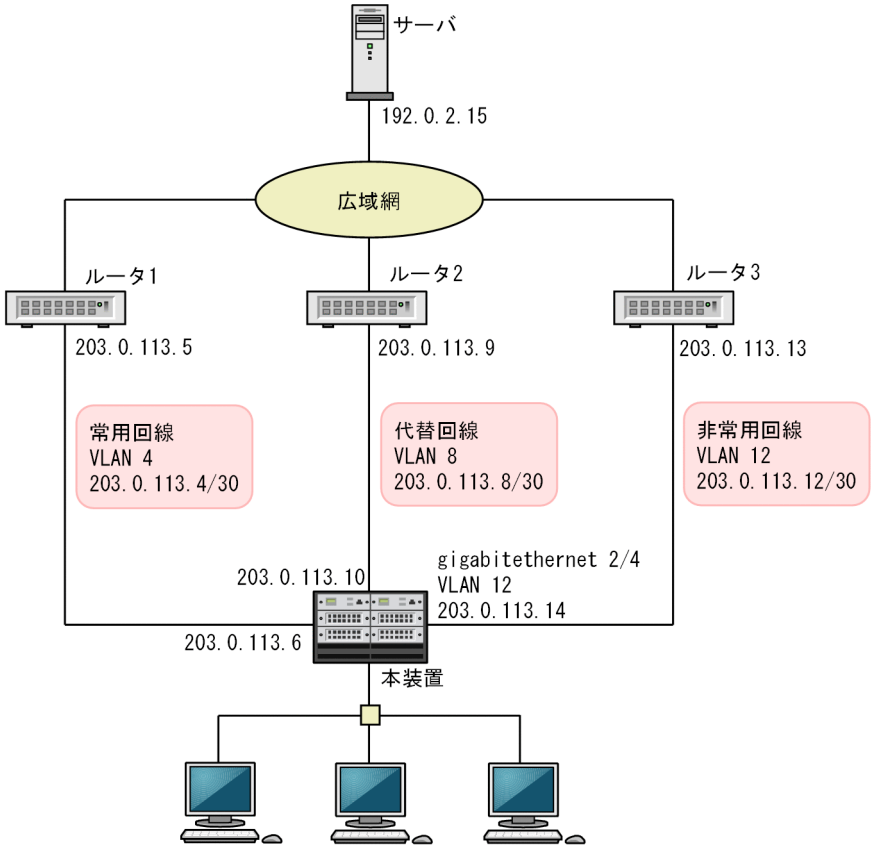
[コマンドによる設定]

1. **(config)# track-target name TRACK1000**
   リスト監視を設定するトラック名（TRACK1000）を指定します。
2. **(config-track-target)# shutdown**
   設定対象のトラック（TRACK1000）の動作を停止します。
3. **(config-track-target)# default-state up**
   トラック（TRACK1000）のデフォルトトラック状態を Up と設定します。これ以降，shutdown を削除するまで，トラック状態は Up です。
4. **(config-track-target)# type list**
   (config-track-target)# boolean and
   トラック（TRACK1000）を，AND リスト監視トラックとして設定します。
5. **(config-track-target)# target object TRACK_A**
   トラック対象のトラックに，TRACK_A を指定します。
6. **(config-track-target)# target object TRACK_B not**
   トラック対象のトラックに，TRACK_B のトラック状態とは逆の状態（否定）を指定します。
7. **(config-track-target)# no shutdown**
   トラック（TRACK1000）の動作を停止するコンフィグレーションを削除します。削除するとすぐに，指定したリスト監視を開始します。

23.3.5　トラッキング連携の設定

次の図に示す構成例に基づいて，VRRP およびポリシーベースルーティングを除くトラッキング連携の設定を説明します。VRRP のトラッキング連携の設定については，「コンフィグレーションガイド Vol.3」「12.1.6　トラッキング連携による優先度変更」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連携の設定については，「コンフィグレーションガイド Vol.3」「8.2.5　ネクストホップのトラッキング連携の設定」を参照してください。

図 23-5　トラッキング連携の構成例



この構成例では，広域網へつながるルータが 3 台あり，接続する回線が 1 本ずつ合計 3 本あります。

ルータ 1 に接続している 1 本目の回線は，常用回線です。普段のデフォルト経路はルータ 1 経由です。

ルータ 2 に接続している 2 本目の回線は，代替回線です。常用回線が使用できる間，代替回線のポートはリンクアップしておきますが，IP インタフェースは DOWN 状態にしておきます。常用回線が使用できなくなったときに IP インタフェースを UP 状態にし，デフォルト経路を切り替えて通信できるようにします。

ルータ 3 に接続している 3 本目の回線は，非常用回線です。普段はポートをシャットダウン状態にしておきます。常用回線も代替回線も使用できなくなったときにポートのシャットダウン状態を解除し，経路を切り替えて通信に使用します。

常用回線および代替回線が使用できるかどうかを監視するトラックとして，各回線に接続しているルータ経由でサーバへポーリングする ICMP ポーリング監視トラックを用意します。

ここで，常用回線を監視するトラックとして，次に示すトラックをそれぞれ用意します。

- 代替回線の VLAN インタフェースおよびデフォルト経路に連携させるトラック
- 非常用回線のポートに連携させるトラック

このとき，非常用回線のポートに連携するトラックの方が，常用回線に障害が発生してからトラック状態が Down になるまでの時間が長くなるように設定します。こうすることで，常用回線に障害が発生したあと，代替回線で通信できるようになるまでの間，非常用回線のシャットダウン状態が解除されなくなります。

[設定のポイント]

- 監視対象が Down になったときに制御対象を使用できるようにしたいときには，代替連携を使用します。二つ以上のトラックの組み合わせと連携して制御するときには，リスト監視トラックを設定し，このリスト監視トラックと制御対象を連携させます。
- 隣接する装置経由でトラック対象への通信を確認したい場合は，隣接する装置をポーリング監視のネクストホップとして指定します。

  冗長経路によって本来の意図から外れてポーリングが成功するおそれがある場合は，隣接装置との接続に使用している IP インタフェースを，応答パケットの受信インタフェースに指定します。
- 複数の制御対象が同じトラックと連携している場合や，リスト監視トラックを通じて複数の制御対象が間接的に同じトラックと連携している場合，複数の制御対象が同時に使用できるようになったり，使用できなくなったりすることがあります。複数の制御対象を排他利用したい場合は，このような動作が発生する可能性があるかどうか，検討が必要です。

  このような動作を回避するためには，制御対象ごとにトラックを用意します。各トラックの状態変更に必要なポーリング回数や時間を指定することで，障害発生から制御対象の状態が変わるまでの時間を調整します。

[コマンドによる設定]

1. **(config)# track-target name ServerByR1**
   (config-track-target)# type icmp
   (config-track-target)# target ip 192.0.2.15 source 203.0.113.6 nexthop 203.0.113.5
   (config-track-target)# icmp check-reply-interface vlan 4
   ルータ 1 経由でサーバを監視するトラック ServerByR1 を設定します。
2. **(config)# ip route 0.0.0.0 0.0.0.0 203.0.113.5 track-target ServerByR1 noresolve**
   ルータ 1 をゲートウェイとするデフォルト経路のスタティック経路を設定します。この経路は，トラック ServerByR1 と連携することで，ルータ 1 を経由するサーバと通信できる場合にだけ有効になります。
3. **(config)# interface vlan 8**
   (config-interface)# track-target-control-ip-down ServerByR1 not
   IP インタフェース VLAN 8 を，トラック ServerByR1 と代替連携させます。これによって，ルータ 1 を経由する通信ができている間は，VLAN 8 を通信に使用しないようにします。
4. **(config)# track-target name ServerByR2**
   (config-track-target)# type icmp
   (config-track-target)# target ip 192.0.2.15 source 203.0.113.10 nexthop 203.0.113.9
   (config-track-target)# icmp check-reply-interface vlan 8
   ルータ 2 経由でサーバを監視するトラック ServerByR2 を設定します。
5. **(config)# track-target name R2Only**
   (config-track-target)# type list
   (config-track-target)# boolean and
   (config-track-target)# target object ServerByR1 not
   (config-track-target)# target object ServerByR2
   トラック ServerByR1 が Down，かつトラック ServerByR2 が Up である場合にだけ Up になるリスト監視トラック R2Only を設定します。
6. **(config)# ip route 0.0.0.0 0.0.0.0 203.0.113.9 track-target R2Only noresolve**

ルータ 2 をゲートウェイとするデフォルト経路を，トラック R2Only と連携させます。

7. **(config)# track-target name ServerByR1Slow**
   (config-track-target)# type icmp
   (config-track-target)# target ip 192.0.2.15 source 203.0.113.6 nexthop 203.0.113.5
   (config-track-target)# icmp check-reply-interface vlan 4
   (config-track-target)# failure detection 4 trial 5 interval 6
   ルータ 1 経由でサーバを監視するトラック ServerByR1Slow を設定します。トラック ServerByR1 とほぼ同じですが，トラック ServerByR1 よりも障害検出に時間が掛かるように，障害発生検証中のポーリング試行間隔をデフォルトの 2 秒から 6 秒に変更しています。
8. **(config)# track-target name R1orR2**
   (config-track-target)# type list
   (config-track-target)# boolean or
   (config-track-target)# target object ServerByR1Slow
   (config-track-target)# target object ServerByR2
   トラック ServerByR1Slow と ServerByR2 のどちらかが Up の場合に Up になるリスト監視トラック R1orR2 を設定します。
9. **(config)# interface gigabitethernet 2/4**
   (config-interface)# track-target-control-shutdown R1orR2 not
   イーサネットインタフェース 2/4 をトラック R1orR2 と代替連携させます。これによって，R1 と R2 の両方が使用できない場合にだけ，イーサネットインタフェース 2/4 が Up になります。
10. **(config)# ip route 0.0.0.0 0.0.0.0 203.0.113.13 noresolve**
    ルータ 3 経由のデフォルト経路を設定します。

23.4　オペレーション

23.4.1　運用コマンド一覧

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 23-11　運用コマンド一覧（トラッキング機能）

コマンド名	説明
show track	トラック情報を表示します。
show track-icmp	ICMP 監視の情報を表示します。

トラッキング連携をサポートする機能の，トラッキング連携についての運用コマンド一覧を次の表に示します。

表 23-12　運用コマンド一覧（トラッキング連携をサポートする機能）

コマンド名	説明
show interfaces※1	イーサネットインタフェースがトラッキング連携している場合，連携しているトラック名とトラック状態を表示します。
show port※1	track-target パラメータを指定すると，イーサネットインタフェースが連携しているトラック名を表示できます。
show ip-dual interface※2	IPv4 および IPv6 インタフェースがトラッキング連携している場合，連携しているトラック名とトラック状態を表示します。
show ip interface※2	IPv4 インタフェースがトラッキング連携している場合，連携しているトラック名とトラック状態を表示します。
show ipv6 interface※3	IPv6 インタフェースがトラッキング連携している場合，連携しているトラック名とトラック状態を表示します。
show ip cache policy※4	IPv4 ポリシーベースルーティングリストが連携しているトラック名と，ネクストホップの情報を表示します。
show ipv6 cache policy※4	IPv6 ポリシーベースルーティングリストが連携しているトラック名と，ネクストホップの情報を表示します。
show vrrpstatus※5	仮想ルータがトラッキング連携している場合，連携しているトラック名とトラック状態を表示します。
show ip static※6	route パラメータと track-target パラメータを指定すると，IPv4 スタティック経路が連携しているトラック名とトラック状態を表示できます。
show ipv6 static※7	route パラメータと track-target パラメータを指定すると，IPv6 スタティック経路が連携しているトラック名とトラック状態を表示できます。

注※1

「運用コマンドレファレンス Vol.1」「22　イーサネット」を参照してください。

注※2

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

注※3

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

注※4

「運用コマンドレファレンス Vol.3」「5　ポリシーベースルーティング」を参照してください。

注※5

「運用コマンドレファレンス Vol.3」「9　VRRP」を参照してください。

注※6

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

注※7

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

23.4.2　トラックの状態確認

(1)　各トラックのトラック状態の確認

show track コマンドで，トラッキング機能のトラック情報を表示します。State で，各トラックのトラック状態を確認できます。

図 23-6　show track コマンドの実行結果

```
> show track
Date 20XX/01/18 13:53:16 UTC
Total: 9
ID    Name                          State Type       Target
30001 ALL_ICMPv4_TRACK              Up    ICMP       172.16.178.2
30002 ALL_ICMPv6_GLOBAL_TRACK       Up    ICMP       2001:db8:1::2
30003 ICMPv4_TRACK                  Up    ICMP       172.16.178.2
30004 ICMPv6_GLOBAL_TRACK           Up    ICMP       2001:db8:1::2
30005 ICMPv6_LINKLOCAL_TRACK        Up    ICMP       fe80::2%Eth1/5.101
30006 List_track                    Up    LIST       -
30007 TRACK_IF1_1                   Up    INTERFACE  geth1/1
30008 noType_TRACK                  Up    -          -
30009 TRACK_LA3                     Up    INTERFACE  ChGr3
>
```

トラック ID と detail パラメータを指定すると，特定のトラック情報の詳細を表示します。

図 23-7　show track コマンド（detail パラメータ指定）の実行結果

```
> show track id 30001 detail
Date 20XX/01/18 13:53:16 UTC
Track ID: 30001, Name: ALL_ICMPv4_TRACK
   State: Up(Active), Last Change: 20XX/01/17 20:41:32 UTC
   Type: ICMP, Target Type: Static
      Destination: 172.16.178.2
   Follower: -
>
```

(2)　ICMP 監視の監視状態の確認

show track-icmp コマンドで，ICMP 監視情報を表示します。State で，各監視対象の監視状態を確認できます。

図 23-8　show track-icmp コマンドの実行結果

```
> show track-icmp
Date 20XX/01/18 13:53:16 UTC
Total: 5
Index Target                        VRF   State   Track
1     172.16.178.2                  -     Reach   ALL_ICMPv4_TRACK
2     2001:db8:1::2                 -     Reach   ALL_ICMPv6_GLOBAL_TRACK
3     172.16.178.2                  -     Reach   ICMPv4_TRACK
4     2001:db8:1::2                 -     Reach   ICMPv6_GLOBAL_TRACK
5     fe80::2%Eth1/5.101            -     Reach   ICMPv6_LINKLOCAL_TRACK
>
```

トラック名と detail パラメータを指定すると，特定の ICMP 監視情報の詳細を表示します。

図 23-9　show track-icmp コマンド（detail パラメータ指定）の実行結果

```
> show track-icmp name ALL_ICMPv4_TRACK detail
Date 20XX/01/19 20:42:31 UTC
Index: 1
   State: Reach, Last Change: 20XX/01/19 20:41:32 UTC
   Target Type: Static
     Destination: 172.16.178.2
     Source: 172.16.17.1
     Nexthop: 172.16.1.2
     DSCP: 0
     TTL: 255, Packet Size: 56
     Interval: 6sec, Timeout: 2sec
     Operation State: Active
   Track Name: ALL_ICMPv4_TRACK
>
```

23.4.3　トラッキング連携で制御されている制御対象の状態確認

(1)　イーサネットインタフェースのトラッキング連携状態確認

show port コマンドに track-target パラメータを指定することで，イーサネットインタフェースの状態と，連携するトラックを一覧形式で確認できます。

図 23-10　show port コマンド（track-target パラメータ指定）の実行結果

```
> show port track-target
Date 20XX/01/18 13:53:16 UTC
Port Counts: 12
Port  Status   Track ID  Track Target
 2/1  up       -         -
 2/2  up       -         -
 2/3  dis      -         -
 2/4  distrack 30049     R1orR2(not)
 2/5  dis      -         -
 2/6  dis      -         -
 2/7  dis      -         -
 2/8  dis      -         -
 2/9  dis      -         -
 2/10 dis      -         -
 2/11 dis      -         -
 2/12 dis      -         -
>
```

(2)　IP インタフェースのトラッキング連携状態確認

次のコマンドで，IP インタフェースが連携するトラック名とトラック状態を確認できます。

- show ip-dual interface
- show ip interface
- show ipv6 interface

図 23-11　show ip interface コマンドの実行結果

```
> show ip interface vlan 8
Date 20XX/01/18 13:53:16 UTC
VLAN0008
   Status: DOWN,MULTICAST,BROADCAST
   mtu: 1500   MAC address: 0012.e206.8700
   IPv4: 203.0.113.6/30    broadcast 203.0.113.7    PRIMARY
   IPv4 uRPF: Disable      VRRP: Disable  Multicast Routing: Disable
   Time-since-last-status-change: 02:03:56
   Last down at: 20XX/01/18 11:49:20 JP
   VLAN ID: 8
   Description: VLAN0008
```

```
   Detail status: Up
   Track-Target: ServerByR1(not)  ID: 30045  State: Up
>
```

(3)　スタティックルーティングのトラッキング連携状態確認

次のコマンドに route パラメータおよび track-target パラメータを指定することで，スタティック経路が連携しているトラック名とトラック状態を確認できます。

- show ip static
- show ipv6 static

図 23-12　show ip static コマンド（route パラメータと track-target パラメータ指定）の実行結果

```
> show ip static route track-target
Date 20XX/01/18 13:53:16 UTC
Status Codes: * valid, > active, r RIB failure
   Destination        Next Hop                                                Distance
Weight Status           Flag                Track Target
*> 0.0.0.0/0          203.0.113.5                                              2
0      Act TrackUp      NoResolve           ServerByR1(30007)
                      203.0.113.9                                              2
0      IFdown TrackDown NoResolve           R2Only(30047)
                      203.0.113.13                                             2
0      IFdown           NoResolve
>
```

(4)　仮想ルータのトラッキング連携状態確認

「コンフィグレーションガイド Vol.3」「12.3.2　仮想ルータの確認」を参照してください。

(5)　ポリシーベースルーティングのトラッキング連携状態確認

「コンフィグレーションガイド Vol.3」「8.3.2　ポリシーベースルーティングの確認」を参照してください。

24 ポートミラーリング

ポートミラーリングは, 送受信するフレームのコピーを指定したポートへ送信する機能です。この章では, ポートミラーリングの解説と操作方法について説明します。

24.1　解説

24.1.1　ポートミラーリングの概要

ポートミラーリングは，送受信するフレームのコピーを指定したポートへ送信する機能です。フレームをコピーすることを**ミラーリング**と呼びます。この機能を利用して，ミラーリングしたフレームをアナライザなどで受信することによって，トラフィックの監視や解析ができます。

受信フレームおよび送信フレームに対するミラーリングのそれぞれの動作を次の図に示します。

図 24-1　受信フレームのミラーリング

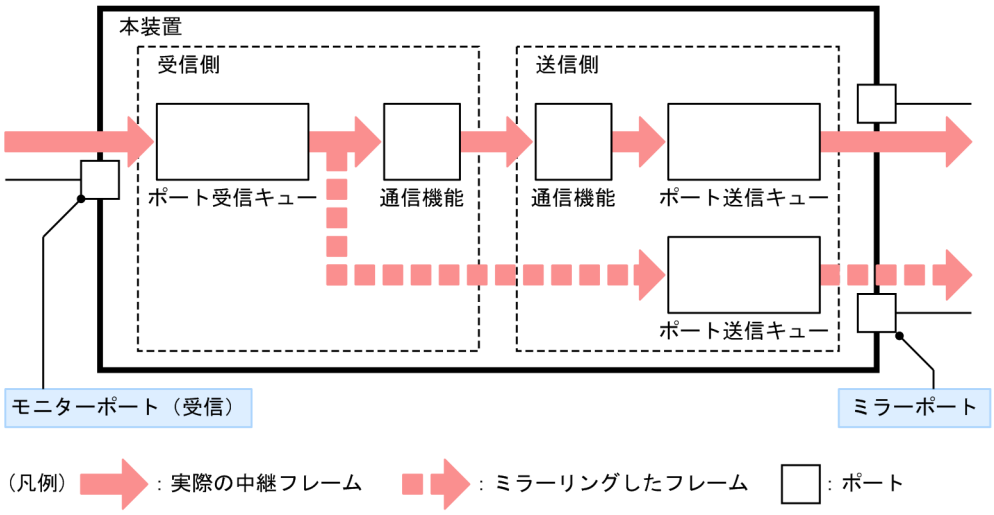
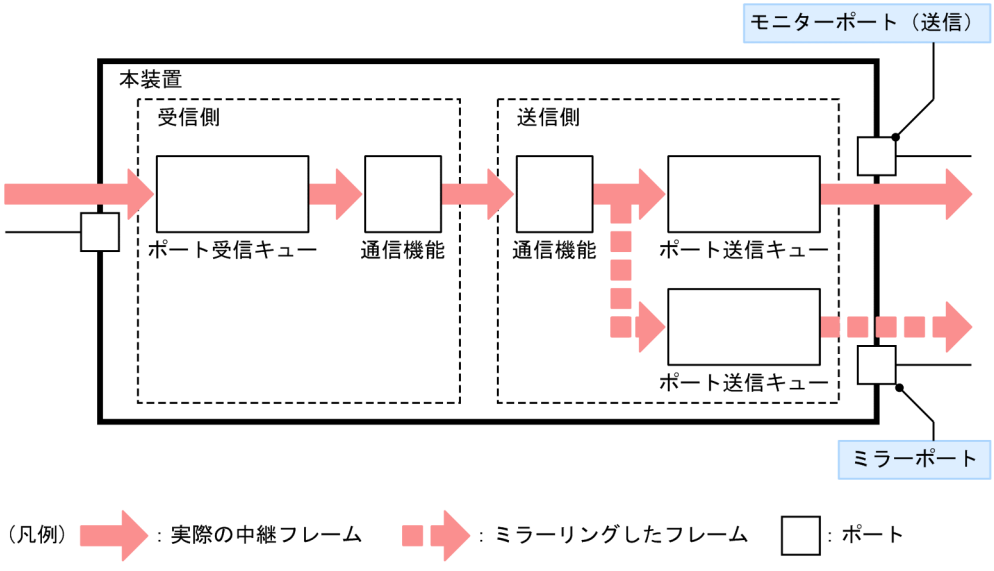


図 24-2　送信フレームのミラーリング



これらの図で示すとおり，トラフィックを監視するポートを**モニターポート**と呼び，ミラーリングしたフレームの送信先となるポートを**ミラーポート**と呼びます。

本装置の受信フレームに対するポートミラーリングでは，ポート受信キューから出力された直後のフレームをコピーします。また，送信フレームに対するポートミラーリングでは，ポート送信キューにキューイングされる前のフレームをコピーします。

24.1.2　ポートミラーリングの動作仕様

(1)　基本仕様

ミラーポートとして設定したポートを除いて，すべてのポートをモニターポートに設定できます。モニターポートとして設定しても，ポートやインタフェースの各機能に対する制限はありません。

トラフィックの監視や解析などのために，アナライザなどを接続するポートをミラーポートに設定します。ミラーポートは，ミラーリング専用のポートになります。

モニターポートとミラーポートの組み合わせを**モニターセッション**と呼びます。本装置では，複数のモニターセッションを設定できます。

モニターセッションでは，モニターポートの受信フレーム，送信フレーム，および送受信フレームに対してミラーリングを設定します。モニターポートの受信フレームと送信フレームは，それぞれ異なるミラーポートへ送信する設定ができます。しかし，モニターポートの受信フレームおよび送信フレームを，複数のミラーポートへ送信する設定はできません。

また，モニターポートとミラーポートは「多対一」で設定できます。こうすると，複数のモニターポートから送受信したフレームのコピーを一つのミラーポートへ送信します。なお，モニターポートおよびミラーポートにはそれぞれ異なる速度のポートを設定できます。

本装置では，ミラーリングしたフレームを，ミラーポートの回線帯域内で送信します。なお，ミラーリングしたフレームの量がミラーポートの回線帯域を超えると，そのフレームを廃棄します。

(2)　ミラーポートの仕様

ミラーポートでは，オートネゴシエーションやフローコントロールなど，イーサネットの機能を使用できます。しかし，レイヤ 2 の機能を使用できないため，スパニングツリーなどをミラーポートで使用できません。

また，次に示すポートはミラーポートとして使用できません。

- チャネルグループに所属しているイーサネットインタフェース
- VLAN に所属している，またはポート種別をトランクポートにしている
- IP アドレス，またはサブインタフェースを設定している

なお，ミラーポートでフィルタおよび QoS 制御を動作させた場合，フィルタおよび QoS フローによるポリサー，マーカー，優先度変更ではミラーリングしたフレームを対象としません。しかし，ポートシェーパによる廃棄制御，スケジューリング，およびポート帯域制御ではミラーリングしたフレームを対象とします。

(3)　受信フレームのミラーリング

モニターポートで受信するすべてのフレームが，ミラーリングの対象となります。ただし，受信したフレームに異常があるときはミラーリングしません。

(4)　送信フレームのミラーリング

モニターポートから送信するすべてのフレームが，ミラーリングの対象となります。なお，モニターポートの輻輳などで廃棄されるフレームをミラーリングしたり，モニターポートから送信するフレームがミラーポートの輻輳などでミラーリングされなかったりすることがあります。

モニターポートにポートシェーパによる廃棄制御，スケジューリング，およびポート帯域制御を設定した場合，送信フレームに対するポートミラーリングでは，ポートシェーパによって制御される前のフレームをミラーリングします。そのため，モニターポートで廃棄するフレームをミラーリングしたり，モニターポートとミラーポートで送信するフレームの順序が異なったりすることがあります。

(5)　ポートミラーリングの使用帯域

ポートミラーリングが動作すると，PSU 内の FE の帯域を使用します。使用する帯域は，ポートミラーリングの設定内容によって異なります。

ミラーリングによる PSU 内の FE の使用帯域を次の表に示します。なお，ここで示す使用帯域はモニターポートを収容する FE がポートミラーリングで使用する帯域であり，ミラーリングの対象となるフレームの使用帯域を含みます。

表 24-1　ミラーリングによる PSU 内の FE の使用帯域

ミラーリングの設定	モニターポートとミラーポートの位置関係	受信側の帯域	送信側の帯域
受信フレームのミラーリング	同一 FE	モニターポートの受信帯域×2	－
	異なる FE		
送信フレームのミラーリング	同一 FE	－	モニターポートの送信帯域×2
	異なる FE	モニターポートの送信帯域	
送受信フレームのミラーリング	同一 FE	モニターポートの受信帯域×2	モニターポートの送信帯域×2
	異なる FE	次の帯域の合計値 • モニターポートの送信帯域 • モニターポートの受信帯域×2	

（凡例）　－：ミラーリングによる使用帯域なし

PSU の種別によって，実装される FE の数や，FE と NIF のつながりが異なるため，設定する際は注意してください。PSU 内の FE と NIF のつながりについては，「20.1.1　概要」を参照してください。

24.1.3　ポートミラーリング使用時の注意事項

(1)　送信フレームのミラーリングに関する注意事項

モニターポートとミラーポートが異なる FE の場合，モニターポート側の FE では，ミラーリングできるパケットのミラーリング処理性能が約 19Mpacket/s に制限されます。また，モニターポート側の FE で，送信フレームのポリシーベースミラーリングのモニターポートを併用する場合，ポートミラーリングとポリシーベースミラーリングの合計で FE ごとに約 19Mpackets/s に制限されます。

なお，PSU の種別によって，実装される FE の数や，FE と NIF のつながりが異なるため，設定する際は注意してください。PSU 内の FE と NIF のつながりについては，「20.1.1　概要」を参照してください。

(2)　スパニングツリー併用時の注意事項

シングルスパニングツリーまたはマルチプルスパニングツリー併用時，ミラーポートにコンフィグレーションコマンド switchport mode の access パラメータを設定した場合，該当するミラーポートから BPDU を送信します。

(3)　IEEE802.3ah OAM 併用時の注意事項

IEEE802.3ah OAM 有効時，次に示す条件のどちらかを満たすと，ミラーポートから OAMPDU を送信します。

- ミラーポートにコンフィグレーションコマンド efmoam active を設定
- ミラーポートで OAMPDU を受信

24.2　コンフィグレーション

24.2.1　コンフィグレーションコマンド一覧

ポートミラー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 24-2　コンフィグレーションコマンド一覧

コマンド名	説明
monitor session	ポートミラーリングを設定します。

24.2.2　ポートミラーリングの設定

ポートミラーリングのコンフィグレーションでは, モニターポートとミラーポートの組み合わせをモニターセッションとして設定します。

(1)　受信フレームのミラーリング

[設定のポイント]

設定できるインタフェースはイーサネットインタフェースです。リンクアグリゲーションで使用している場合も，単独のイーサネットインタフェースを指定します。

[コマンドによる設定]

1. **(config)# monitor session 2 source interface gigabitethernet 1/1 rx destination interface gigabitethernet 1/5**

   アナライザをポート 1/5 に接続し, ポート 1/1 で受信するフレームをミラーリングすることを設定します。セッション番号は 2 を使用します。

(2)　送信フレームのミラーリング

[設定のポイント]

設定できるインタフェースはイーサネットインタフェースです。リンクアグリゲーションで使用している場合も，単独のイーサネットインタフェースを指定します。

[コマンドによる設定]

1. **(config)# monitor session 1 source interface gigabitethernet 1/2 tx destination interface gigabitethernet 1/6**

   アナライザをポート 1/6 に接続し, ポート 1/2 で送信するフレームをミラーリングすることを設定します。セッション番号は 1 を使用します。

(3)　送受信フレームのミラーリング

[設定のポイント]

設定できるインタフェースはイーサネットインタフェースです。リンクアグリゲーションで使用している場合も，単独のイーサネットインタフェースを指定します。

[コマンドによる設定]

1. **(config)# monitor session 1 source interface gigabitethernet 1/3 both destination interface gigabitethernet 1/11**

   アナライザをポート 1/11 に接続し，ポート 1/3 で送受信するフレームをミラーリングすることを設定します。セッション番号は 1 を使用します。

(4)　送受信フレームの別ポートへのミラーリング

[設定のポイント]

モニターポートの送信フレームのミラーリングと受信フレームのミラーリングを別のミラーポートに設定します。

[コマンドによる設定]

1. **(config)# monitor session 1 source interface gigabitethernet 1/3 rx destination interface gigabitethernet 1/11**

   (config)# monitor session 2 source interface gigabitethernet 1/3 tx destination interface gigabitethernet 1/12

   ポート 1/3 で受信するフレームをポート 1/11 にミラーリングして，ポート 1/3 で送信するフレームをポート 1/12 にミラーリングすることを設定します。セッション番号は 1 と 2 を使用します。

25 ポリシーベースミラーリング

ポリシーベースミラーリングは，送受信するフレームから特定のフローをコピーして，指定したインタフェースへ送信する機能です。この章では，ポリシーベースミラーリングの解説と操作方法について説明します。

25.1　解説

25.1.1　概要

ポリシーベースミラーリングは，送受信するフレームから特定のフローをコピーして，指定したインタフェースへ送信する機能です。フレームをコピーすることを**ミラーリング**と呼びます。この機能を利用して，フロー単位でミラーリングしたフレームをアナライザなどで受信することによって，トラフィックの監視や解析ができます。

受信フレームおよび送信フレームに対するミラーリングのそれぞれの動作を次の図に示します。

図 25-1　受信フレームのミラーリング

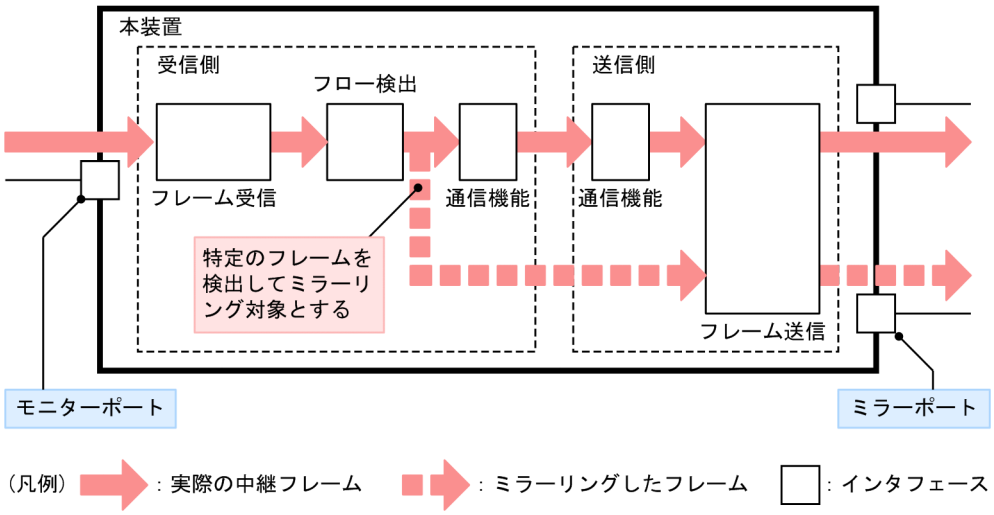
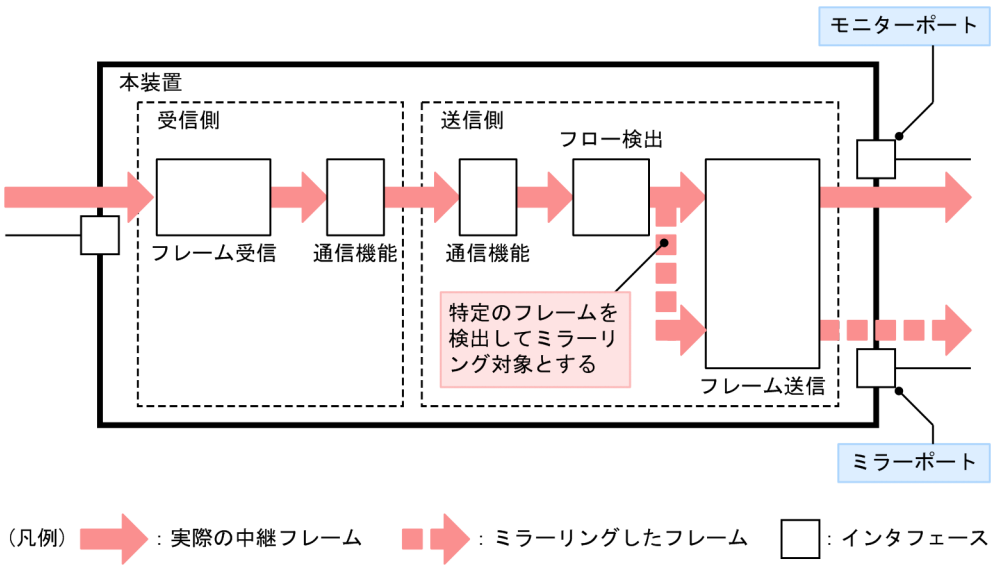


図 25-2　送信フレームのミラーリング



これらの図で示すとおり，トラフィックを監視するインタフェースを**モニターポート**と呼び，ミラーリングしたフレームの送信先となるインタフェースを**ミラーポート**と呼びます。

本装置のポリシーベースミラーリングは，フロー検出によって細かくフレームを特定できます。また，複数のミラーポートに同時にミラーリングできます。

25.1.2　動作仕様

(1)　基本仕様

トラフィックの監視や解析などのために，アナライザなどを接続するインタフェースをミラーポートに設定します。ミラーポートは，ミラーリング専用のポートになります。

モニターポートとミラーポートの組み合わせを**モニターセッション**と呼びます。本装置では，複数のモニターセッションを設定できます。

モニターポートとミラーポートは，次に示す組み合わせで使用できます。

- 1 モニターポート対 1 ミラーポート
- 1 モニターポート対複数ミラーポート
- 複数モニターポート対 1 ミラーポート
- 複数モニターポート対複数ミラーポート

モニターポートおよびミラーポートには，それぞれ異なる速度のインタフェースを設定できます。なお，ミラーリングしたフレームは，ミラーポートの回線帯域内で送信するため，回線帯域を超えるフレームは廃棄します。

(2)　モニターポートの仕様

ポリシーベースミラーリングのモニターポートは，対象とするフローを特定するアクセスリストを使用して設定します。モニターポートを設定する場合は，フロー配分パターンに mirror を設定してください。

ポリシーベースミラーリングの送信先インタフェースリストを動作に指定したアクセスリストをインタフェースに適用することで，該当するインタフェースをモニターポートとして使用します。アクセスリストをインタフェースに適用するときに指定する，コンフィグレーションコマンドのパラメータを次の表に示します。

表 25-1　アクセスリスト適用時に指定するパラメータ

ミラーリング方向	パラメータ
受信側	in-mirror
送信側	out-mirror

なお，対象インタフェース，フロー検出条件，注意事項などについては，「10　フィルタ」を参照してください。

(3)　ミラーポートの仕様

ポリシーベースミラーリングのミラーポートは，送信先インタフェースリストで設定します。

送信先インタフェースリストには，複数のミラーポートが設定できます。複数のミラーポートを設定した場合は，設定したすべてのミラーポートに同時にミラーリングします。ミラーポートとして設定できるインタフェースを次に示します。

- イーサネットインタフェース

- ポートチャネルインタフェース

送信先インタフェースにポートチャネルインタフェースを設定することで，リンクアグリゲーションの機能であるロードバランスやポートの冗長化などが可能となります。

ミラーポートでは，オートネゴシエーションやフローコントロールなどのイーサネットの機能や，フィルタおよびQoSの機能を使用できます。また，ミラーポートにミラーリングするフレームは，本装置内ではレイヤ2中継フレームとして扱います。したがって，フィルタおよびQoSの機能を使用する場合は，レイヤ2中継としてフロー検出してください。また，送信先インタフェースとしてポートチャネルインタフェースを使用する場合は，レイヤ2中継としてポート振り分けをします。ただし，ミラーポートでは，スパニングツリーなどのレイヤ2機能は使用できません。

また，次に示すインタフェースはミラーポートとして使用できません。

- チャネルグループに所属しているイーサネットインタフェース
- VLANに所属している，またはポート種別をトランクポートにしている
- IPアドレス，またはサブインタフェースを設定している

(4)　受信フレームのミラーリング

モニターポートで受信するフレームのうち，アクセスリストでフロー検出したフレームがミラーリングの対象となります。

(5)　送信フレームのミラーリング

モニターポートから送信するフレームのうち，アクセスリストでフロー検出したフレームがミラーリングの対象となります。なお，モニターポートの輻輳などで廃棄されるフレームをミラーリングしたり，モニターポートから送信するフレームがミラーポートの輻輳などでミラーリングされなかったりすることがあります。

モニターポートにポートシェーパによる廃棄制御，スケジューリング，およびポート帯域制御を設定した場合，送信フレームに対するポリシーベースミラーリングでは，ポートシェーパによって制御される前のフレームをミラーリングします。そのため，モニターポートで廃棄するフレームをミラーリングしたり，モニターポートとミラーポートで送信するフレームの順序が異なったりすることがあります。

送信フレームのポリシーベースミラーリングでは，モニターポート側のミラーリング処理性能がFEごとに約19Mpacket/sに制限されます。また，同一FEで送信フレームのポートミラーリングのモニターポートを併用し，かつポートミラーリングのモニターポートとミラーポートが異なるFEの場合，モニターポート側のミラーリング性能は，ポートミラーリングとポリシーベースミラーリングの合計でFEごとに約19Mpackets/sに制限されます。

なお，PSUの種別によって，実装されるFEの数や，FEとNIFのつながりが異なるため，設定する際は注意してください。PSU内のFEとNIFのつながりについては，「20.1.1　概要」を参照してください。

(6)　ポリシーベースミラーリングの使用帯域

ポリシーベースミラーリングが動作すると，PSU内のFEの帯域を使用します。

ミラーリングによるPSU内のFEの使用帯域を次の表に示します。なお，ここで示す使用帯域はモニターポートを収容するFEがポリシーベースミラーリングで使用する帯域であり，ミラーリングの対象となるフレームの使用帯域を含みます。

表 25-2　ミラーリングによる PSU 内の FE の使用帯域

ミラーリングの設定	受信側の帯域	送信側の帯域
受信フレームのミラーリング	モニターポートの受信帯域＋ポリシーベースミラーリング対象フローの帯域	送信フロー＋（ポリシーベースミラーリング対象フローの帯域×モニターポート数分※1）
送信フレームのミラーリング	モニターポートの送信帯域＋ポリシーベースミラーリング対象フローの帯域※2	送信フロー＋（ポリシーベースミラーリング対象フローの帯域※2×モニターポート数分※1）

注※1

各モニターポートが属する FE が異なる場合は，FE ごとに算出してください。

注※2

ポリシーベースミラーリング対象フローの帯域は最大で約 19Mpacket/s です。

PSU の種別によって，実装される FE の数や，FE と NIF のつながりが異なるため，設定する際は注意してください。PSU 内の FE と NIF のつながりについては，「20.1.1　概要」を参照してください。

25.1.3　ポリシーベースミラーリング使用時の注意事項

(1)　スパニングツリー併用時の注意事項

シングルスパニングツリーまたはマルチプルスパニングツリー併用時，ミラーポートにコンフィグレーションコマンド switchport mode の access パラメータを設定した場合，該当するミラーポートから BPDU を送信します。

(2)　IEEE802.3ah OAM 併用時の注意事項

IEEE802.3ah OAM 有効時，次に示す条件のどちらかを満たすと，ミラーポートから OAMPDU を送信します。

- ミラーポートにコンフィグレーションコマンド efmoam active を設定
- ミラーポートで OAMPDU を受信

(3)　モニターポート設定時の注意事項

アクセスリストをポリシーベースミラーリングとしてインタフェースに適用すると，フィルタで自動生成される暗黙の廃棄エントリがポリシーベースミラーリングでも生成されます。このエントリは，フロー検出をしてもミラーリングはしない，無効エントリとなります。なお，暗黙の廃棄エントリの自動生成を抑止すると，無効エントリは生成されません。

(4)　ポリシーベースミラーリングで検出しないフレーム

本装置の受信側に設定したポリシーベースミラーリングでは，次に示すフレームをフロー検出しません。

- uRPF によって廃棄したフレーム

また，送信側に設定したポリシーベースミラーリングでは，次に示すフレームをフロー検出しません。

- フィルタで廃棄したフレーム
- QoS フロー廃棄で廃棄したフレーム
- ポリサーで廃棄したフレーム

- ポートミラーリングでミラーリングしたフレーム
- 送信フレームのポリシーベースミラーリングでミラーリングしたフレーム

(5)　オプションヘッダのある IPv4 パケットに対するポリシーベースミラーリング

オプションヘッダのある IPv4 パケットをフロー検出する場合は，フロー検出に次の条件を指定してください。

- コンフィグレーション
- MAC ヘッダ
- VLAN Tag ヘッダ
- IPv4 ヘッダ
- 中継種別

TCP/UDP/ICMP/IGMP ヘッダをフロー検出条件に指定しても，フロー検出しません。

(6)　拡張ヘッダのある IPv6 パケットに対するポリシーベースミラーリング

拡張ヘッダのある IPv6 パケットをフロー検出する場合は，フロー検出条件に次の条件を指定してください。

- コンフィグレーション
- MAC ヘッダ
- VLAN Tag ヘッダ
- IPv4 ヘッダ
- 中継種別

上位プロトコルおよび TCP/UDP/ICMP ヘッダをフロー検出条件に指定した場合のフロー検出可否については，「10　フィルタ」の「表 10-7　受信側インタフェースでのフロー検出可否」および「表 10-8　送信側インタフェースでのフロー検出可否」を参照してください。

(7)　送信フレームのミラーリング時の注意事項

送信フレームのポリシーベースミラーリングでは，次の点に注意してください。

- ミラーリングしたフレームをフィルタや QoS フローでフロー検出する場合，2 段目の VLAN Tag ヘッダの検出条件は検出対象外となり，該当フローエントリには一致しません。
- ミラーリングしたフレームをアクセスリストロギングの対象とした場合，アクセスリストログの表示項目である受信インタフェースは表示対象外となります。

  また，0x8100 以外の TPID を設定したインタフェースへ送信するパケットをミラーリングの対象とすると，非 IP パケットでの表示および VLAN ID が表示対象外となります。

(8)　ミラーポートにポートチャネルインタフェース指定時の注意事項

フレーム送信時のポート振り分けに VLAN Tag ごとのポート振り分けを選択しても，チャネルグループを構成するどれか一つのポートから送信するため，ポート振り分けをしたい場合は VLAN Tag ごとのポート振り分け以外の方法を選択してください。

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

ポリシーベースミラー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 25-3　コンフィグレーションコマンド一覧

コマンド名	説明
destination	ポリシーベースミラーリングのミラーポートを設定します。
destination-interface-list	ポリシーベースミラーリングの送信先インタフェースリストを設定します。
flow detection mode※1	フロー検出モードを設定します。
flow-table allocation※1	フロー配分パターンを設定します。
advance access-group※2	インタフェースに対して，ポリシーベースミラーリングの対象フレームを検出する Advance フィルタを適用します。
advance access-list※2	ポリシーベースミラーリングの対象フレームを Advance フィルタで検出するアクセスリストを設定します。
ip access-group※2	インタフェースに対して，ポリシーベースミラーリングの対象フレームを検出する IPv4 パケットフィルタを適用します。
ip access-list extended※2	ポリシーベースミラーリングの対象フレームを IPv4 パケットフィルタで検出するアクセスリストを設定します。
ipv6 access-list※2	ポリシーベースミラーリングの対象フレームを IPv6 フィルタで検出するアクセスリストを設定します。
ipv6 traffic-filter※2	インタフェースに対して，ポリシーベースミラーリングの対象フレームを検出する IPv6 フィルタを適用します。
mac access-group※2	インタフェースに対して，ポリシーベースミラーリングの対象フレームを検出する MAC フィルタを適用します。
mac access-list extended※2	ポリシーベースミラーリングの対象フレームを MAC フィルタで検出するアクセスリストを設定します。
permit※2	対象パケットを検出するフロー検出条件と，対象フレームのミラーリング先となる送信先インタフェースリストを，アクセスリストに指定します。

注※1

「コンフィグレーションコマンドレファレンス Vol.1」「10　装置とソフトウェアの管理」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」「7　アクセスリスト」を参照してください。

25.2.2　フロー配分パターンの設定

フロー配分パターンをポリシーベースミラーリング使用に設定すると，送信先インタフェースリストを動作に指定したアクセスリストを設定できます。

[設定のポイント]

設定したフロー配分パターンを反映させるために，すべての PSU を再起動してください。

[コマンドによる設定]

1. **(config)# flow-table allocation mirror**
   グローバルコンフィグレーションモードでフロー配分パターンをポリシーベースミラーリング使用に設定します。

25.2.3　ポリシーベースミラーリングの設定

ポリシーベースミラーリングの対象フレーム，および対象フレームのミラーリング先となる送信先インタフェースリストは，アクセスリストで指定します。送信先のインタフェースは，送信先インタフェースリストで設定します。

(1)　1 モニターポート対 1 ミラーポートの設定

1 モニターポート対 1 ミラーポートで動作させる場合の例を次に示します。この例では，アナライザをイーサネットインタフェース 1/2 に接続します。

[設定のポイント]

ミラーポートには，送信先インタフェースリストを設定します。モニターポートには，送信先インタフェースリストを動作に指定したアクセスリストをポリシーベースミラーリングとして設定します。

[コマンドによる設定]

1. **(config)# destination-interface-list MIRROR-LIST-A mode mirror**
   (config-dest-mirror)# destination interface gigabitethernet 1/2
   (config-dest-mirror)# exit
   送信先インタフェースリスト（MIRROR-LIST-A）に，イーサネットインタフェース 1/2 をミラーポートとして設定します。
2. **(config)# ip access-list extended IPv4-MIRROR-A**
   (config-ext-nacl)# permit tcp any any action policy-mirror-list MIRROR-LIST-A
   (config-ext-nacl)# exit
   IPv4 アクセスリスト（IPv4-MIRROR-A）を作成して，IPv4 パケットに対して送信先インタフェースリスト（MIRROR-LIST-A）を設定します。
3. **(config)# interface gigabitethernet 1/1**
   (config-if)# ip access-group IPv4-MIRROR-A in-mirror
   イーサネットインタフェース 1/1 の受信側に，IPv4 アクセスリスト（IPv4-MIRROR-A）をポリシーベースミラーリングとして適用します。

(2)　1 モニターポート対複数ミラーポートの設定

1 モニターポート対複数ミラーポートで動作させる場合の例を次に示します。この例では，アナライザをイーサネットインタフェース 1/2，2/2，および 3/2 に接続します。

[設定のポイント]

ミラーポートとして，送信先インタフェースリストに複数のインタフェースを設定します。

[コマンドによる設定]

1. **(config)# destination-interface-list MIRROR-LIST-B mode mirror**
   (config-dest-mirror)# destination interface gigabitethernet 1/2

```
(config-dest-mirror)# destination interface gigabitethernet 2/2
(config-dest-mirror)# destination interface gigabitethernet 3/2
(config-dest-mirror)# exit
```

送信先インタフェースリスト（MIRROR-LIST-B）に，イーサネットインタフェース 1/2，2/2，および 3/2 をミラーポートとして設定します。

2.
```
(config)# ip access-list extended IPv4-MIRROR-B
(config-ext-nacl)# permit udp any any action policy-mirror-list MIRROR-LIST-B
(config-ext-nacl)# exit
```

IPv4 アクセスリスト（IPv4-MIRROR-B）を作成して，IPv4 パケットに対して送信先インタフェースリスト（MIRROR-LIST-B）を設定します。

3.
```
(config)# interface gigabitethernet 1/1
(config-if)# ip access-group IPv4-MIRROR-B out-mirror
```

イーサネットインタフェース 1/1 の送信側に，IPv4 アクセスリスト（IPv4-MIRROR-B）をポリシーベースミラーリングとして適用します。

(3)　複数モニターポート対 1 ミラーポートの設定

複数モニターポート対 1 ミラーポートで動作させる場合の例を次に示します。この例では，アナライザをイーサネットインタフェース 1/2 に接続します。

[設定のポイント]

複数のモニターポートに，同一の送信先インタフェースリストを指定したアクセスリストを設定します。

[コマンドによる設定]

1.
```
(config)# destination-interface-list MIRROR-LIST-C mode mirror
(config-dest-mirror)# destination interface gigabitethernet 1/2
(config-dest-mirror)# exit
```

送信先インタフェースリスト（MIRROR-LIST-C）に，イーサネットインタフェース 1/2 をミラーポートとして設定します。

2.
```
(config)# ip access-list extended IPv4-MIRROR-C1
(config-ext-nacl)# permit tcp any any action policy-mirror-list MIRROR-LIST-C
(config-ext-nacl)# exit
```

IPv4 アクセスリスト（IPv4-MIRROR-C1）を作成して，IPv4 パケットに対して送信先インタフェースリスト（MIRROR-LIST-C）を設定します。

3.
```
(config)# interface gigabitethernet 1/1
(config-if)# ip access-group IPv4-MIRROR-C1 out-mirror
(config-if)# exit
```

イーサネットインタフェース 1/1 の送信側に，IPv4 アクセスリスト（IPv4-MIRROR-C1）をポリシーベースミラーリングとして適用します。

4.
```
(config)# ip access-list extended IPv4-MIRROR-C2
(config-ext-nacl)# permit udp any any action policy-mirror-list MIRROR-LIST-C
(config-ext-nacl)# exit
```

IPv4 アクセスリスト（IPv4-MIRROR-C2）を作成して，IPv4 パケットに対して送信先インタフェースリスト（MIRROR-LIST-C）を設定します。

5. (config)# interface gigabitethernet 2/1
   (config-if)# ip access-group IPv4-MIRROR-C2 in-mirror
   イーサネットインタフェース 2/1 の受信側に，IPv4 アクセスリスト（IPv4-MIRROR-C2）をポリシーベースミラーリングとして適用します。

25.2.4　ミラーポートでのロードバランス

ミラーポートでロードバランスをする場合の例を次に示します。この例では，アナライザをチャネルグループ 10 に接続します。

[設定のポイント]

ポートチャネルインタフェースをミラーポートとして設定することで，リンクアグリゲーションによってミラーポートでロードバランスをします。リンクアグリゲーションについては，「コンフィグレーションガイド Vol.1」「19　リンクアグリゲーション」を参照してください。

[コマンドによる設定]

1. (config)# destination-interface-list MIRROR-LIST-LB mode mirror
   (config-dest-mirror)# destination interface port-channel 10
   (config-dest-mirror)# exit
   送信先インタフェースリスト（MIRROR-LIST-LB）に，チャネルグループ 10 をミラーポートとして設定します。
2. (config)# ipv6 access-list IPv6-MIRROR-LB
   (config-ext-nacl)# permit tcp any any action policy-mirror-list MIRROR-LIST-LB
   (config-ext-nacl)# exit
   IPv6 アクセスリスト（IPv6-MIRROR-LB）を作成して，IPv6 パケットに対して送信先インタフェースリスト（MIRROR-LIST-LB）を設定します。
3. (config)# interface gigabitethernet 1/1
   (config-if)# ipv6 traffic-filter IPv6-MIRROR-LB in-mirror
   イーサネットインタフェース 1/1 の受信側に，IPv6 アクセスリスト（IPv6-MIRROR-LB）をポリシーベースミラーリングとして適用します。

25.2.5　ミラーポートの冗長化

ミラーポートを冗長化する場合の例を次に示します。この例では，アナライザをチャネルグループ 20 に接続します。

[設定のポイント]

ポートチャネルインタフェースをミラーポートとして設定して，リンクアグリゲーションのスタンバイリンク機能によってミラーポートを冗長化します。リンクアグリゲーションについては，「コンフィグレーションガイド Vol.1」「19　リンクアグリゲーション」を参照してください。

[コマンドによる設定]

1. (config)# interface port-channel 20
   (config-if)# channel-group max-active-port 1
   (config-if)# exit
   (config)# interface gigabitethernet 1/2

```
(config-if)# channel-group 20 mode on
(config-if)# lacp port-priority 100
(config-if)# exit
(config)# interface gigabitethernet 2/2
(config-if)# channel-group 20 mode on
(config-if)# lacp port-priority 200
(config-if)# exit
```

チャネルグループ 20 にイーサネットインタフェース 1/2 および 2/2 を集約します。また，イーサネットインタフェース 2/2 をスタンバイリンクとして設定します。

2.
```
(config)# destination-interface-list MIRROR-LIST-SL mode mirror
(config-dest-mirror)# destination interface port-channel 20
(config-dest-mirror)# exit
```

送信先インタフェースリスト（MIRROR-LIST-SL）に，チャネルグループ 20 をミラーポートとして設定します。

3.
```
(config)# ipv6 access-list IPv6-MIRROR-SL
(config-ext-nacl)# permit udp any any action policy-mirror-list MIRROR-LIST-SL
(config-ext-nacl)# exit
```

IPv6 アクセスリスト（IPv6-MIRROR-SL）を作成して，IPv6 パケットに対して送信先インタフェースリスト（MIRROR-LIST-SL）を設定します。

4.
```
(config)# interface gigabitethernet 1/1
(config-if)# ipv6 traffic-filter IPv6-MIRROR-SL out-mirror
```

イーサネットインタフェース 1/1 の送信側に，IPv6 アクセスリスト（IPv6-MIRROR-SL）をポリシーベースミラーリングとして適用します。

25.3　オペレーション

25.3.1　運用コマンド一覧

ポリシーベースミラーリングの運用コマンド一覧を次の表に示します。

表 25-4　運用コマンド一覧

コマンド名	説明
show access-filter※	ポリシーベースミラーリングの送信先インタフェースリストを動作に指定したアクセスリストの設定内容と統計情報を表示します。
clear access-filter※	ポリシーベースミラーリングの送信先インタフェースリストを動作に指定したアクセスリストの統計情報を 0 クリアします。

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

25.3.2　ポリシーベースミラーリングの確認

show access-filter コマンドで, ポリシーベースミラーリングの送信先インタフェースリストを動作に指定したアクセスリストを確認できます。

図 25-3　show access-filter コマンドの実行結果

```
> show access-filter interface gigabitethernet 1/1 in-mirror
Date 20XX/01/01 12:00:00 UTC
Using interface : gigabitethernet 1/1 in-mirror
Extended IP access-list : IPv4-MIRROR-A
      10 tcp(6) any any action policy-mirror-list MIRROR-LIST-A
                        Matched packets        Matched bytes
         Total  :          25800211584       38700317376000
         PSU 1  :          25800211584       38700317376000
      Implicit-entry
                        Matched packets        Matched bytes
         Total  :                  4178             3342432
         PSU 1  :                  4178             3342432
```

指定したインタフェースのフィルタに「Extended IP access-list」とアクセスリスト名（IPv4-MIRROR-A）が表示されることを確認します。また，アクセスリストに「action policy-mirror-list」と送信先インタフェースリスト名（MIRROR-LIST-A）が表示されて，Matched packets および Matched bytes がカウントされていることを確認します。

26 sFlow 統計（フロー統計）機能

この章では, 本装置を中継するパケットのトラフィック特性を分析する機能である sFlow 統計の解説と操作方法について説明します。

26.1　解説

26.1.1　sFlow 統計の概要

sFlow 統計はエンドーエンドのトラフィック（フロー）特性や隣接するネットワーク単位のトラフィック特性を分析するため，ネットワークの上を流れるトラフィックを中継装置（ルータやスイッチ）でモニタする機能です。sFlow 統計は国際的に公開されているフロー統計プロトコル（RFC3176）で，レイヤ 2 からレイヤ 7 までの統計情報をサポートしています。sFlow 統計情報（以降，sFlow パケット）を受け取って表示する装置を sFlow コレクタ（以降，コレクタ）と呼び，コレクタに sFlow パケットを送付する装置を sFlow エージェント（以降，エージェント）と呼びます。sFlow 統計を使ったネットワーク構成例を次の図に示します。

図 26–1　sFlow 統計のネットワーク構成例

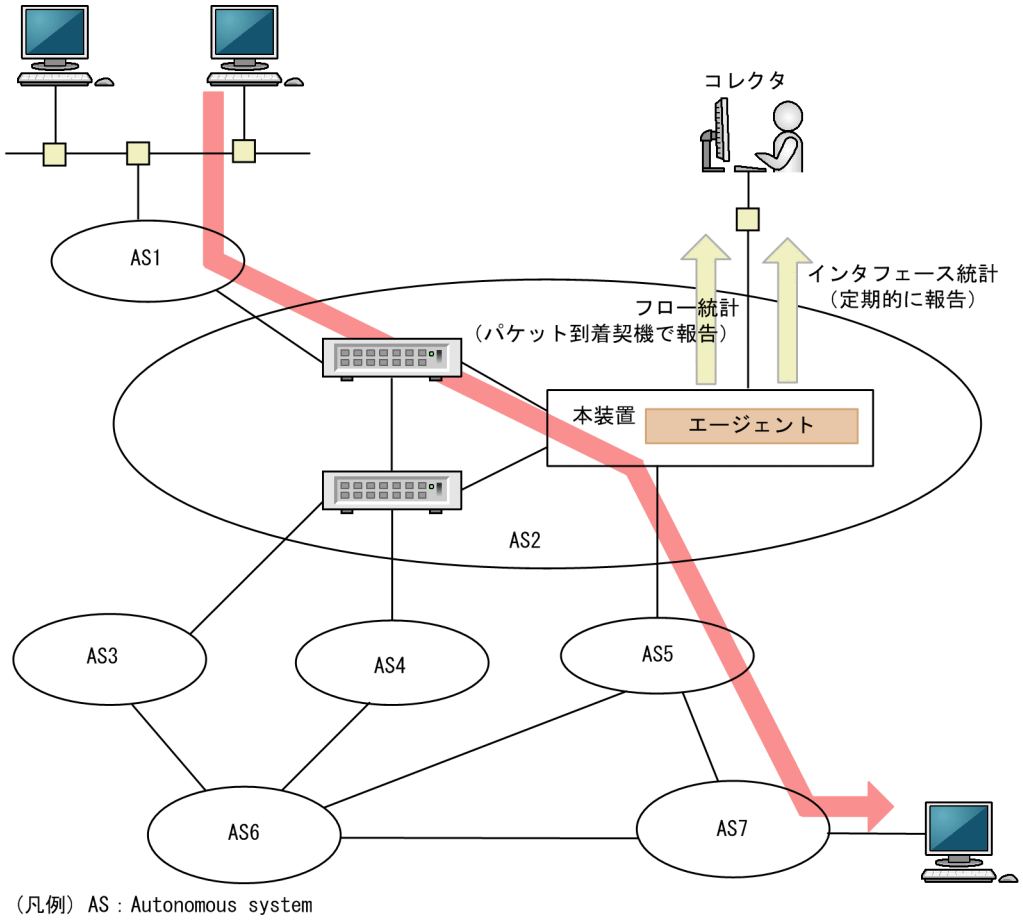
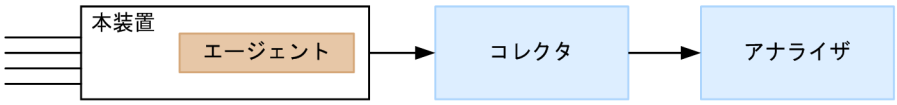


図 26–2　システム構成



本装置のエージェントでモニタされた情報はコレクタに集められ，統計結果をアナライザによってグラフィカルに表示できます。したがって，sFlow 統計機能を利用するにはコレクタとアナライザが必要です。

表 26-1　システム構成要素

構成要素	役割
エージェント（本装置）	統計情報を収集してコレクタに送付します。
コレクタ※	エージェントから送付される統計情報を集計・編集・表示します。さらに，編集データをアナライザに送付します。
アナライザ	コレクタから送付されるデータをグラフィカルに表示します。

注※　アナライザと一緒になっている場合もあります。

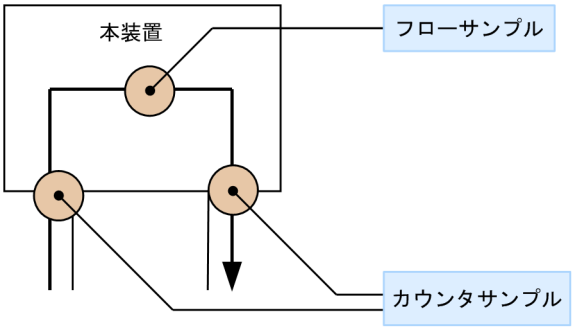
26.1.2　sFlow 統計エージェント機能

本装置のエージェントには，次の二つの機能があります。

- フロー統計（sFlow 統計ではフローサンプルと呼びます。以降，この名称で表記します。）作成機能
- インタフェース統計（sFlow 統計ではカウンタサンプルと呼びます。以降，この名称で表記します。）作成機能

フローサンプル作成機能は送受信パケット（フレーム）をユーザ指定の割合でサンプリングして，パケット情報を加工してフローサンプル形式でコレクタに送信する機能です。カウンタサンプル作成機能はインタフェース統計をカウンタサンプル形式でコレクタに送信する機能です。それぞれの収集個所と収集内容を次に示します。

図 26-3　フローサンプルとカウンタサンプル



フローサンプル（フロー統計）

　トラフィック特性の分析（どこからどこへ，どのようなトラフィックが流れているか）

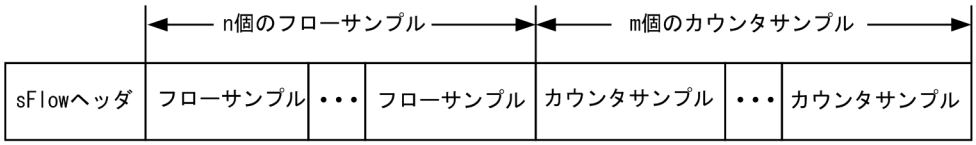
カウンタサンプル（インタフェース統計）

　インタフェースで発生するイベントの分析（送受信カウンタやエラーの発生数＝ MIB 情報相当）

26.1.3　sFlow パケットフォーマット

本装置がコレクタに送信する sFlow パケット（フローサンプルパケットとカウンタサンプルパケット）について説明します。コレクタに送信するフォーマットは RFC3176 で規定されています。sFlow パケットのフォーマットを次の図に示します。

図 26-4　sFlow パケットフォーマット



なお，本装置では一つの sFlow パケットにフローサンプルとカウンタサンプルが同時に入ることはありません。

(1)　sFlow ヘッダ

sFlow ヘッダへ設定される内容を次の表に示します。

表 26-2　sFlow ヘッダのフォーマット

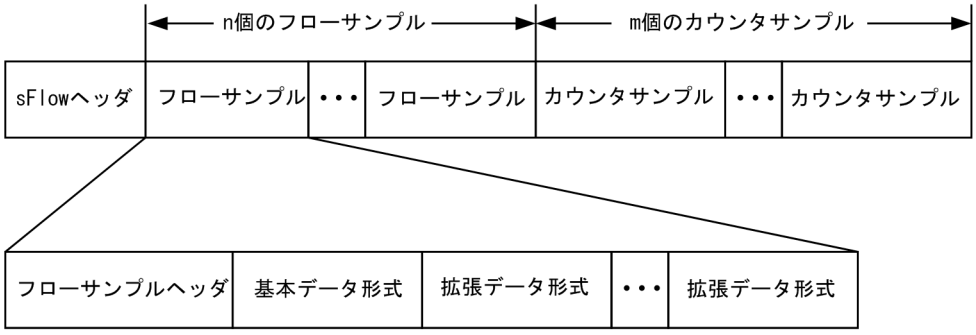
設定項目	説明	サポート
バージョン番号	sFlow パケットのバージョン（バージョン 4 をサポート）	○
アドレスタイプ	エージェントの IP タイプ（IPv4=1，IPv6=2）	○
エージェント IP アドレス	エージェントの IP アドレス	○
シーケンス番号	sFlow パケットの生成ごとに増加する番号	○
生成時刻	現在の時間（装置の起動時からのミリセカンド）	○
サンプル数	この信号に含まれるサンプリング（フロー・カウンタ）したパケット数（「図 26-4　sFlow パケットフォーマット」の例では n ＋ m が設定されます）	○

（凡例）○：サポートする

(2)　フローサンプル

フローサンプルとは，受信パケットのうち，他装置へ転送または本装置宛てと判定されるパケットの中から一定のサンプリング間隔でパケットを抽出して，コレクタに送信するためのフォーマットです。フローサンプルにはモニタしたパケットに加えて，パケットには含まれていない情報（受信インタフェース，送信インタフェース，AS 番号など）も収集するため，詳細なネットワーク監視ができます。フローサンプルのフォーマットを次の図に示します。

図 26-5　フローサンプルのフォーマット



(a)　フローサンプルヘッダ

フローサンプルヘッダへ設定する内容を次の表に示します。

表 26-3　フローサンプルヘッダのフォーマット

設定項目	説明	サポート
sequence_number	フローサンプルの生成ごとに増加する番号	○
source_id	フローサンプルの装置内の発生源（受信インタフェース）を表す SNMP Interface Index。 インタフェースが不明な場合は 0 を設定。	○
sampling_rate	フローサンプルのサンプリング間隔	○
sample_pool	インタフェースに到着したパケットの総数	○
drops	資源不足のため失ったフローサンプルの総数。 本装置では 0 固定。	○
input	受信インタフェースの SNMP Interface Index。 インタフェースが不明な場合 0 を設定。 （source_id と同じ）	○
output	送信インタフェースの SNMP Interface Index※1。 送信インタフェースが不明な場合は 0 を設定。 送信インタフェースが複数の場合（マルチキャストなど）は最上位ビットを立て，下位ビットが送信インタフェースの数を示します※2。	○

（凡例）○：サポートする

注※1　ソフトウェア中継の場合は 0 になることがあります。

注※2　未サポートのため，下位ビットは 0 固定です。

(b)　基本データ形式

基本データ形式はヘッダ型，IPv4 型および IPv6 型の 3 種類があり，このうち一つだけ設定できます。基本データ形式のデフォルト設定はヘッダ型です。IPv4 型, IPv6 型を使用する場合はコンフィグレーションコマンドで設定してください。各形式のフォーマットを次に示します。

表 26-4　ヘッダ型のフォーマット

設定項目	説明	サポート
packet_information_type	基本データ形式のタイプ（ヘッダ型=1）※	○
header_protocol	ヘッダプロトコル番号（ETHERNET=1）	○
frame_length	オリジナルのパケット長	○
header_length	オリジナルからサンプリングした分のパケット長（デフォルト 128）	○
header<>	サンプリングしたパケットの内容	○

（凡例）○：サポートする

注※　IP パケットとして解析ができない場合は，このフォーマットになります。

表 26-5　IPv4 型のフォーマット

設定項目	説明	サポート
packet_information_type	基本データ形式のタイプ（IPv4 型=2）	○
length	IPv4 パケットの長さ	○
protocol	IP プロトコルタイプ（例：TCP=6，UDP=17）	○
src_ip	送信元 IP アドレス	○
dst_ip	宛先 IP アドレス	○
src_port	送信元ポート番号	○
dst_port	宛先ポート番号	○
tcp_flags	TCP フラグ	○
TOS	IP のタイプオブサービス	○

（凡例）○：サポートする

表 26-6　IPv6 型のフォーマット

設定項目	説明	サポート
packet_information_type	基本データ形式のタイプ（IPv6 型=3）	○
length	低レイヤを除いた IPv6 パケットの長さ	○
protocol	IP プロトコルタイプ（例：TCP=6，UDP=17）	○
src_ip	送信元 IP アドレス	○
dst_ip	宛先 IP アドレス	○
src_port	送信元ポート番号	○
dst_port	宛先ポート番号	○
tcp_flags	TCP フラグ	○
priority	優先度（トラフィッククラス）	○

（凡例）○：サポートする

(c)　拡張データ形式

拡張データ形式はスイッチ型・ルータ型・ゲートウェイ型・ユーザ型・URL 型の 5 種類があります。拡張データ形式のデフォルト設定ではスイッチ型以外のすべての拡張形式を収集して，コレクタに送信します。本形式はコンフィグレーションで変更できます。各形式のフォーマットを次に示します。

表 26-7　拡張データ形式の一覧

拡張データ形式	説明	サポート
スイッチ型	スイッチ情報（VLAN 情報など）を収集する。	×
ルータ型	ルータ情報（NextHop など）を収集する。	○
ゲートウェイ型	ゲートウェイ情報（AS 番号など）を収集する。	○

拡張データ形式	説明	サポート
ユーザ型	ユーザ情報（TACACS/RADIUS 情報など）を収集する。	○
URL 型	URL 情報（URL 情報など）を収集する。	○

（凡例）○：サポートする　×：サポートしない

表 26-8　ルータ型のフォーマット

設定項目	説明	サポート
extended_information_type	拡張データ形式のタイプ（ルータ型=2）	○
nexthop_address_type	次の転送先ルータの IP アドレスタイプ	○※
nexthop	次の転送先ルータの IP アドレス	○※
src_mask	送信元アドレスのプレフィックスマスクビット	○
dst_mask	宛先アドレスのプレフィックスマスクビット	○

（凡例）○：サポートする

注※　宛先アドレスがグループアドレスの場合は 0 で収集されます。

表 26-9　ゲートウェイ型のフォーマット

設定項目	説明	サポート
extended_information_type	拡張データ形式のタイプ（ゲートウェイ型=3）	○
as	本装置の AS 番号	○
src_as	送信元の AS 番号	○※1
src_peer_as	送信元への隣接 AS 番号	○※1※2
dst_as_path_len	AS 情報数（1 固定）	○
dst_as_type	AS 経路種別（2：AS_SEQUENCE）	○
dst_as_len	AS 数（2 固定）	○
dst_peer_as	宛先への隣接 AS 番号	○※1
dst_as	宛先の AS 番号	○※1
communities<>	本経路に関するコミュニティ※3	×
localpref	本経路に関するローカル優先※3	×

（凡例）○：サポートする　×：サポートしない

注※1　送受信先がダイレクト経路の場合は AS 番号が 0 で収集されます。

注※2　本装置から送信元へパケットを送信する場合に隣接 AS 番号として扱っている値が本フィールドに入ります。本装置へ到着前に実際に通過した隣接 AS 番号と異なる場合があります。

注※3　未サポートのため 0 固定です。

表 26-10　ユーザ型のフォーマット

設定項目	説明	サポート
extended_information_type	拡張データ形式のタイプ（ユーザ型=4）※1	○
src_user_len	送信元のユーザ名の長さ	○
src_user<>	送信元のユーザ名	○
dst_user_len	宛先のユーザ名の長さ※2	×
dst_user<>	宛先のユーザ名※2	×

（凡例）○：サポートする　×：サポートしない

注※1　RADIUS は宛先 UDP ポート番号 1812，TACACS は宛先 UDP ポート番号 49 が対象となります。

注※2　未サポートのため 0 固定です

表 26-11　URL 型のフォーマット

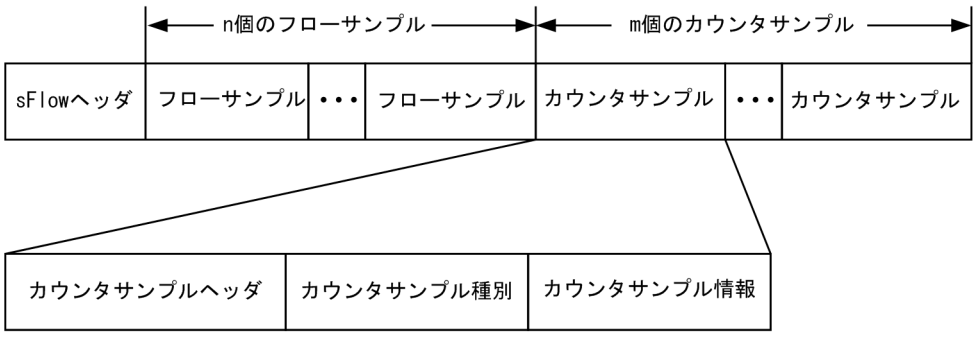
設定項目	説明	サポート
extended_information_type	拡張データ形式のタイプ（URL 型=5）	○
url_direction	URL 情報源 （source address=1，destination address=2）	○
url_len	URL 長	○
url<>	URL 内容	○

（凡例）○：サポートする

(3)　カウンタサンプル

カウンタサンプルは，インタフェース統計情報（到着したパケット数や，エラーの数など）を送信します。インタフェース種別によってコレクタに送信するフォーマットが決まります。カウンタサンプルのフォーマットを次の図に示します。

図 26-6　カウンタサンプルのフォーマット



(a)　カウンタサンプルヘッダ

カウンタサンプルヘッダへ設定される内容を次の表に示します。

表 26-12　カウンタサンプルヘッダのフォーマット

設定項目	説明	サポート
sequence_number	カウンタサンプルの生成ごとに増加する番号	○
source_id	カウンタサンプルの装置内の発生源（特定のポート）を表す SNMP Interface Index	○
sampling_interval	コレクタへのカウンタサンプルの送信間隔	○

（凡例）○：サポートする

(b)　カウンタサンプル種別

カウンタサンプル種別はインタフェース種別ごとに分類されて収集されます。カウンタサンプル種別として設定される内容を次の表に示します。

表 26-13　カウンタサンプル種別一覧

設定項目	説明	サポート
GENERIC	一般的な統計（counters_type=1）	×※1
ETHERNET	イーサネット統計（counters_type=2）	○
TOKENRING	トークンリング統計（counters_type=3）	×※2
FDDI	FDDI 統計（counters_type=4）	×※2
100BaseVG	VG 統計（counters_type=5）	×※2
WAN	WAN 統計（counters_type=6）	×※2
VLAN	VLAN 統計（counters_type=7）	×※2

（凡例）○：サポートする　×：サポートしない

注※1　GENERIC 情報は ETHERNET 種別のフォーマットに含まれています。

注※2　本装置で未サポートのインタフェース種別です。

(c)　カウンタサンプル情報

カウンタサンプル情報はカウンタサンプル種別によって収集される内容が変わります。VLAN 統計以外は MIB で使われている統計情報（RFC）に従って送信されます。カウンタサンプル情報として設定される内容を次の表に示します。

表 26-14　カウンタサンプル情報

設定項目	説明	サポート
GENERIC	一般的な統計［RFC2233 参照］	×
ETHERNET	イーサネット統計［RFC2358 参照］	○※
TOKENRING	トークンリング統計［RFC1748 参照］	×
FDDI	FDDI 統計［RFC1512 参照］	×
100BaseVG	VG 統計［RFC2020 参照］	×

設定項目	説明	サポート
WAN	WAN 統計［RFC2233 参照］	×
VLAN	VLAN 統計	×

（凡例）○：サポートする　×：サポートしない

注※　イーサネット統計のうち ifDirection は収集できません。

26.1.4　本装置での sFlow 統計の動作について

(1)　フローサンプル収集の対象パケットに関する注意点

- 本装置でのフローサンプルは，受信パケットを対象パケットとします。
- 受信時に廃棄と判定されるパケット（フィルタ機能で廃棄判定されるパケットなど）は，フローサンプル収集の対象外パケットとします。ただし，送信側の QoS 機能の廃棄制御に従ってキューイング時に廃棄されるパケットは，フローサンプル収集の対象パケットとします。

(2)　フローサンプルのデータ収集位置による注意点

- フローサンプルパケットの内容には，本装置に入ってきた時点のパケット内容が収集されます（本装置内でパケット内容の変換などが行われても，sFlow パケットには反映されません）。
- 本装置でのフローサンプルは，受信パケットをサンプリングしてコレクタに送信します。この性質上，送信側にフィルタ機能や QoS 機能を設定してパケットを廃棄する条件でも，コレクタには中継しているように送信する場合があります。フィルタ機能や QoS 機能と併用するときは，パケットが廃棄される条件を確認して運用してください。他機能と併用時のフローサンプル収集条件を次の表と図に示します。

表 26-15　他機能と併用時のフローサンプル収集条件

機能	受信パケットがフローサンプル対象
フィルタ機能（受信側）	廃棄対象は収集されない
QoS 機能（ポリサーおよび QoS フロー廃棄）（受信側）	廃棄対象は収集されない
フィルタ機能（送信側）※1	廃棄対象でも収集される
QoS 機能（ポリサー，QoS フロー廃棄，およびシェーパ）（送信側）※1	廃棄対象でも収集される
uRPF 機能	廃棄対象は収集されない
ストームコントロール	廃棄対象は収集されない
自宛	収集される
自発（本装置からの ping など）	－
ポリシーベースルーティング	収集される※2※3

（凡例）－：該当なし

注※1

フローサンプルパケットの内容には本装置に入ってきた時点のパケット内容が収集されます。

注※2

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。

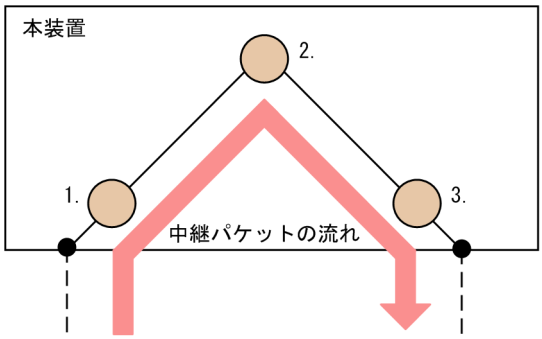
・ルータ型のフォーマットのうち，nexthop および dst_mask

・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

注※3

デフォルト動作の deny 指定によって廃棄したパケットも収集されます。

図 26-7　他機能と併用時のフローサンプル対象判定位置



1. 受信側フィルタ機能チェック，受信側 QoS 機能チェック
2. 受信パケットのフローサンプル対象判定
3. 送信側フィルタ機能チェック，送信側 QoS 機能チェック

(3)　カウンタサンプル収集の対象パケット

- 本装置でのカウンタサンプルは，受信パケットおよび送信パケットを対象パケットとします。

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

sFlow 統計で使用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 26-16　コンフィグレーションコマンド一覧

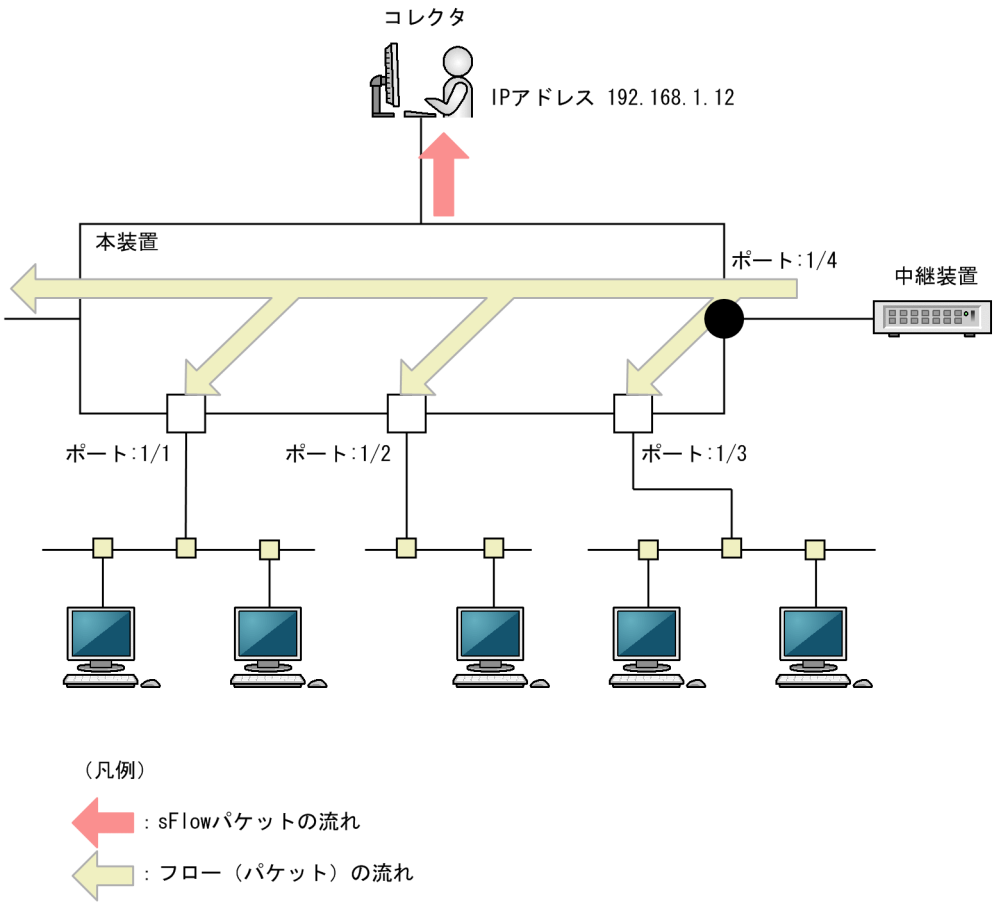
コマンド名	説明
sflow additional-http-port	拡張データ形式で URL 情報を使用する場合に，HTTP パケットと判断するポート番号を 80 以外に追加指定します。
sflow destination	sFlow パケットの宛先であるコレクタの IP アドレスを指定します。
sflow extended-information-type	フローサンプルの各拡張データ形式の送信有無を指定します。
sflow forward ingress	指定したポートの受信トラフィックをフローサンプルの監視対象にします。また，指定したポートの送受信トラフィックをカウンタサンプルの監視対象にします。
sflow max-header-size	基本データ形式にヘッダ型を使用している場合，サンプルパケットの先頭からコピーされるヘッダの最大サイズを指定します。
sflow max-packet-size	sFlow パケットのサイズを指定します。
sflow packet-information-type	フローサンプルの基本データ形式を指定します。
sflow polling-interval	カウンタサンプルをコレクタへ送信する間隔を指定します。
sflow sample	装置全体に適用するサンプリング間隔を指定します。
sflow source	sFlow パケットの送信元（エージェント）に設定される IP アドレスを指定します。

26.2.2　sFlow 統計の基本的な設定

(1)　受信パケットをモニタする設定

ポート 1/4 で受信するパケットをモニタする場合の設定例を次に示します。

図 26-8　ポート 1/4 の受信パケットをモニタする設定例



[設定のポイント]

sFlow 統計のコンフィグレーションでは装置全体で有効な設定と，実際に運用するポートを指定する設定の二つが必要です。

[コマンドによる設定]

1. **(config)# sflow destination 192.168.1.12**

   コレクタとして IP アドレス 192.168.1.12 を設定します。

2. **(config)# sflow sample 512**

   512 パケットごとにトラフィックをモニタします。

3. **(config)# interface gigabitethernet 1/4**

   ポート 1/4 のコンフィグレーションモードに移行します。

4. **(config-if)# sflow forward ingress**

   ポート 1/4 の受信パケットに対してフローサンプル作成機能を，送受信パケットに対してカウンタサンプル作成機能を有効にします。

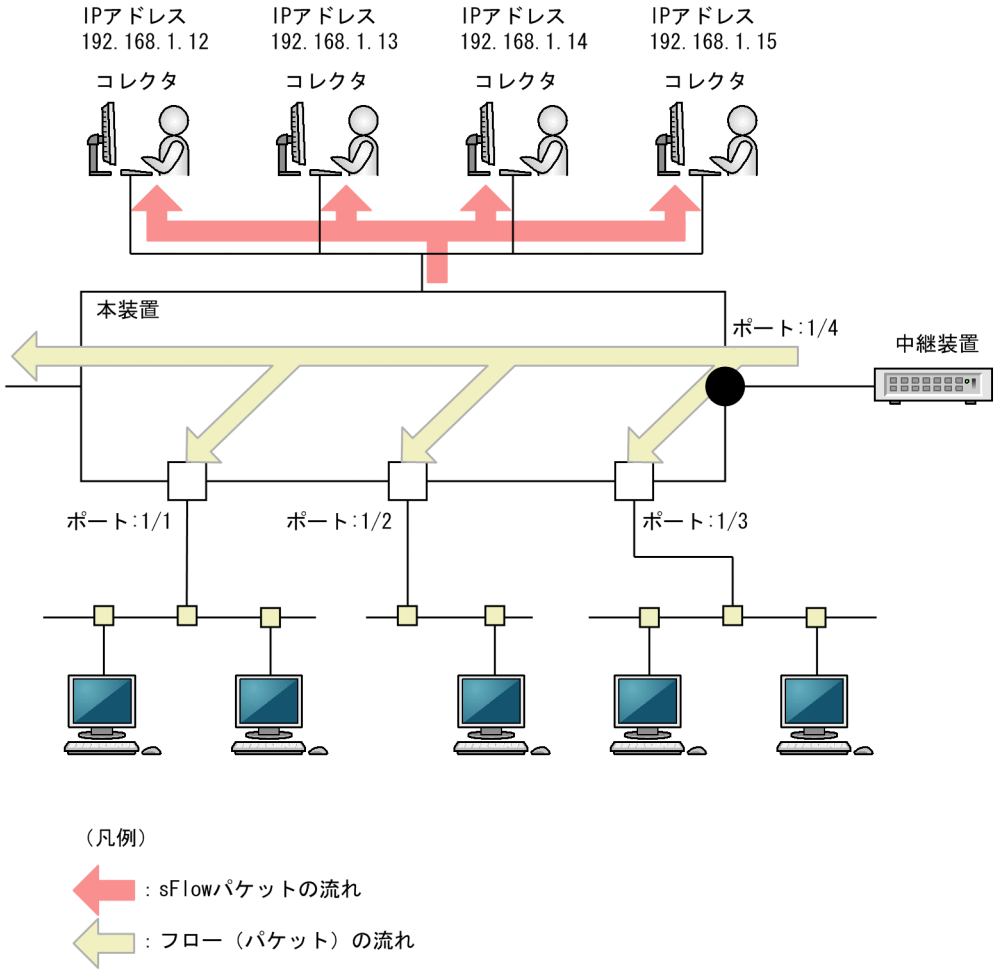
[注意事項]

sflow sample コマンドで設定するサンプリング間隔については，パケット流量（packet/s）を考慮して決める必要があります。詳細は，「コンフィグレーションコマンドレファレンス Vol.2」「sflow sample」を参照してください。

(2)　複数のコレクタと接続する設定

４台のコレクタと接続する場合の設定例を次に示します。

図 26-9　４台のコレクタと接続する設定例



[設定のポイント]

バックアップのため，コレクタを複数台（最大４台）接続できます。

[コマンドによる設定]

1. **(config)# sflow destination 192.168.1.12**
   コレクタとして IP アドレス 192.168.1.12 を設定します。
2. **(config)# sflow destination 192.168.1.13**
   コレクタとして IP アドレス 192.168.1.13 を設定します。
3. **(config)# sflow destination 192.168.1.14**
   コレクタとして IP アドレス 192.168.1.14 を設定します。
4. **(config)# sflow destination 192.168.1.15**
   コレクタとして IP アドレス 192.168.1.15 を設定します。
5. **(config)# sflow sample 512**
   512 パケットごとにトラフィックをモニタします。

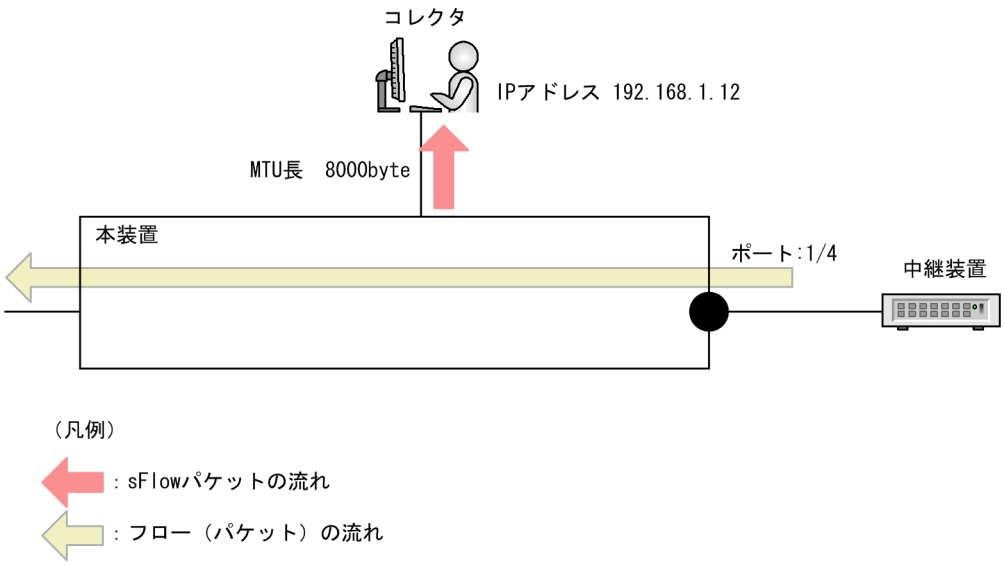
6. **(config)# interface gigabitethernet 1/4**
   ポート 1/4 のコンフィグレーションモードに移行します。
7. **(config-if)# sflow forward ingress**
   ポート 1/4 の受信パケットに対してフローサンプル作成機能を，送受信パケットに対してカウンタサンプル作成機能を有効にします。

26.2.3　sFlow 統計コンフィグレーションパラメータの設定例

(1)　MTU 長と sFlow パケットサイズの調整

コレクタと MTU 長が 8000byte の回線で接続している場合に，コレクタへ送信する sFlow パケットサイズを調整する場合の設定例を次に示します。

図 26-10　コレクタへの送信を MTU=8000byte に設定する例



[設定のポイント]
sFlow パケットはデフォルトでは 1400byte 以下のサイズでコレクタに送信されます。コレクタへの回線の MTU 値が大きい場合，同じ値に調整することでコレクタに対して効率よく送信できます。

[コマンドによる設定]

1. **(config)# sflow destination 192.168.1.12**
   コレクタとして IP アドレス 192.168.1.12 を設定します。
2. **(config)# sflow sample 32**
   32 パケットごとにトラフィックをモニタします。
3. **(config)# sflow max-packet-size 8000**
   sflow パケットサイズの最大値を 8000byte に設定します。
4. **(config)# interface gigabitethernet 1/4**
   ポート 1/4 のコンフィグレーションモードに移行します。
5. **(config-if)# sflow forward ingress**

ポート 1/4 の受信パケットに対してフローサンプル作成機能を，送受信パケットに対してカウンタサンプル作成機能を有効にします。

(2)　収集したい情報を絞る

IP アドレス情報だけが必要な場合の設定例を次に示します。

[設定のポイント]

sFlow パケットの情報はコンフィグレーションを指定しないとすべて収集する条件になっています。しかし，不要な情報がある場合，その情報を取らない設定をすると CPU 使用率を下げられます。

[コマンドによる設定]

1. **(config)# sflow destination 192.168.1.12**
   コレクタとして IP アドレス 192.168.1.12 を設定します。
2. **(config)# sflow sample 512**
   512 パケットごとにトラフィックをモニタします。
3. **(config)# sflow packet-information-type ip**
   フローサンプルの基本データ形式に IP 形式を設定します。
4. **(config)# sflow extended-information-type router**
   フローサンプルの拡張データ形式にルータ形式を設定します（ルータ情報だけが取得できます）。
5. **(config)# interface gigabitethernet 1/4**
   ポート 1/4 のコンフィグレーションモードに移行します。
6. **(config-if)# sflow forward ingress**
   ポート 1/4 の受信パケットに対してフローサンプル作成機能を，送受信パケットに対してカウンタサンプル作成機能を有効にします。

(3)　sFlow パケットのエージェント IP アドレスを固定する

ループバックインタフェースに割り当てられた IP アドレスをエージェント IP アドレスとして利用して，コレクタへ送信する場合の設定例を次に示します。

[設定のポイント]

一般的なコレクタは，sFlow パケットに含まれるエージェント IP アドレスの値を基にして同一の装置かどうかを判断しています。この理由から，sflow source コマンドや interface loopback コマンドでエージェント IP アドレスを設定していない場合，コレクタ側で複数装置から届いているように表示されるおそれがあります。長期的に情報を見る場合はエージェント IP アドレスを固定してください。

[コマンドによる設定]

1. **(config)# interface loopback 0**
   ループバックインタフェースのコンフィグレーションモードに移行します。
2. **(config-if)# ip address 192.168.1.1**
   ループバックインタフェースに IPv4 アドレスとして 192.168.1.1 を設定します。
3. **(config-if)# ipv6 address 2001:db8:811:ff00::1**
   (config-if)# exit
   ループバックインタフェースに IPv6 アドレスとして 2001:db8:811:ff00::1 を設定します。
4. **(config)# sflow destination 192.168.1.12**

コレクタとして IP アドレス 192.168.1.12 を設定します。

5. **(config)# sflow sample 512**

   512 パケットごとにトラフィックをモニタします。

6. **(config)# interface gigabitethernet 1/4**

   ポート 1/4 のコンフィグレーションモードに移行します。

7. **(config-if)# sflow forward ingress**

   ポート 1/4 の受信パケットに対してフローサンプル作成機能を，送受信パケットに対してカウンタサンプル作成機能を有効にします。

[注意事項]

ループバックインタフェースの IP アドレスを使用する場合は，sflow source コマンドで設定する必要はありません。もし，sflow source コマンドで IP アドレスが指定されている場合は，その IP アドレスが優先されます。

(4)　ローカルネットワーク環境での URL 情報収集

ローカルネットワーク環境で HTTP パケットのポート番号として 8080 番を利用している場合の設定例を次に示します。

[設定のポイント]

本装置では sFlow 統計で URL 情報（HTTP パケット）を収集する場合，宛先のポート番号として 80 番を利用している環境がデフォルトになっています。ローカルなネットワークなどでポート番号が異なる場合は，ポート番号を追加で設定します。

[コマンドによる設定]

1. **(config)# sflow destination 192.168.1.12**

   コレクタとして IP アドレス 192.168.1.12 を設定します。

2. **(config)# sflow sample 512**

   512 パケットごとにトラフィックをモニタします。

3. **(config)# sflow additional-http-port 8080**

   拡張データ形式で URL 情報を使用する場合に，HTTP パケットと判断する宛先ポート番号 8080 を追加で設定します。

4. **(config)# interface gigabitethernet 1/4**

   ポート 1/4 のコンフィグレーションモードに移行します。

5. **(config-if)# sflow forward ingress**

   ポート 1/4 の受信パケットに対してフローサンプル作成機能を，送受信パケットに対してカウンタサンプル作成機能を有効にします。

[注意事項]

本パラメータを設定したあとでも，HTTP パケットの対象として宛先ポート番号 80 番は有効です。

26.3　オペレーション

26.3.1　運用コマンド一覧

sFlow 統計で使用する運用コマンド一覧を次の表に示します。

表 26-17　運用コマンド一覧

コマンド名	説明
show sflow	sFlow 統計機能についての設定条件と動作状況を表示します。
clear sflow statistics	sFlow 統計で管理している統計情報をクリアします。
restart sflow	フロー統計プログラムを再起動します。
dump sflow	フロー統計プログラム内で収集しているデバック情報をファイル出力します。

26.3.2　コレクタとの通信の確認

本装置で sFlow 統計を設定してコレクタに送信する場合，次のことを確認してください。

(1)　コレクタとの疎通確認

ping コマンドをコレクタの IP アドレスを指定して実行して，本装置からコレクタに対して IP 通信ができることを確認してください。通信ができない場合は，「トラブルシューティングガイド」を参照してください。

(2)　sFlow パケット通信確認

コレクタ側で sFlow パケットを受信していることを確認してください。

受信していない場合の対応は，「トラブルシューティングガイド」を参照してください。

26.3.3　sFlow 統計の運用中の確認

本装置で sFlow 統計を使用した場合，運用中の確認内容には次のものがあります。

(1)　sFlow パケット廃棄数の確認

show sflow コマンドを実行して sFlow 統計情報を表示し，sFlow 統計で廃棄しているパケット数を確認してください。廃棄パケット数が増加する場合は，廃棄パケット数が増加しないサンプリング間隔を設定してください。

図 26-11　show sflow コマンドの実行結果

```
> show sflow
Date 20XX/07/19 12:00:00 UTC
sFlow service status : enable
Elapsed time from sFlow statistics clearance :  8:00:05
sFlow agent data :
 sFlow service version : 4
 CounterSample interval rate : 60 seconds
 Received sFlow samples :     37269  Dropped sFlow samples      :       2093   <-1
 Exported sFlow samples :     37269  Non-exported sFlow samples :          0
sFlow collector data :
 Collector IP address : 192.168.1.19  UDP :  6343  Source IP address : 192.168.1.1
  Send FlowSample UDP packets    :      12077  Send failed packets :          0
```

```
  Send CounterSample UDP packets :        621  Send failed packets :          0
 Collector IP address : 192.168.1.20  UDP : 65535  Source IP address : 192.168.1.1
  Send FlowSample UDP packets    :      12077  Send failed packets :          0
  Send CounterSample UDP packets :        621  Send failed packets :          0
sFlow sampling data :
 Configured rate(actual rate) : 1 per 2048 packets(1 per 2048 packets)
  Configured sFlow ingress ports : 1/2-4
```

1. Dropped sFlow samples の値を確認して廃棄パケット数が増加している場合，サンプリング間隔の設定を見直してください。

26.3.4　sFlow 統計のサンプリング間隔の調整方法

本装置で sFlow 統計を使用した場合，サンプリング間隔の調整方法として次のものがあります。

(1)　回線速度から調整する

sFlow 統計機能を有効にしている全ポートのパケット流量（packet/s）を show interfaces コマンドで確認して，「Input rate」の値を合計してください。その合計値を 1000 で割った値が，目安となるサンプリング間隔となります。この値でサンプリング間隔を設定後，show sflow コマンドで廃棄パケット数が増えないかどうかを確認してください。

ポート 1/4 とポート 3/1 に対して受信パケットをとる場合の目安となるサンプリング間隔の例を次に示します。

図 26-12　show interfaces コマンドの実行結果

```
> show interfaces gigabitethernet 1/4
Date 20XX/07/19 12:00:00 UTC
NIF1 : active  12-port 10BASE-T/100BASE-TX/1000BASE-T  retry:0
        Average:700Mbps/24Gbps  Peak:750Mbps at 08:10:30
Port4: active up  1000BASE-T full(auto) 0012.e240.0a04
        Time-since-last-status-change:10:30:30
        Bandwidth:1000000kbps  Average out:350Mbps  Average in:350Mbps
        Peak out:380Mbps at 08:10:30  Peak in:370Mbps at 08:10:30
        Output rate:290.0Mbps  70.8kpps
        Input  rate:290.0Mbps  70.8kpps
        Flow control send   :off
        Flow control receive:off
        TPID:8100
                            :

> show interfaces gigabitethernet 3/1
Date 20XX/07/19 12:01:00 UTC
NIF3 : active  12-port 10BASE-T/100BASE-TX/1000BASE-T  retry:0
        Average:700Mbps/24Gbps  Peak:750Mbps at 08:10:30
Port1: active up  1000BASE-T full(auto)    0012.e220.ec31
        Time-since-last-status-change:1:47:47
        Bandwidth:1000000kbps  Average out:5Mbps  Average in:605Mbps
        Peak out:5Mbps at 15:44:36  Peak in:705Mbps at 15:44:18
        Output rate:4893.5kbps  512pps
        Input  rate:634.0Mbps  310.0kpps
        Flow control send   :off
        Flow control receive:off
        TPID:8100
                            :
```

目安となるサンプリング間隔

＝　sFlow 統計機能を有効にしているポートの PPS 合計値/1000

＝　(70.8kpps+310.0kpps) /1000

＝　380.8※

注※　サンプリング間隔を 381 で設定すると実際は 512 で動作します。サンプリング間隔の詳細は，「コンフィグレーションコマンドレファレンス Vol.2」「sflow sample」を参照してください。

27 IEEE802.3ah OAM

IEEE802.3ah OAM は，物理層で隣接装置間の運用状態を確認するためのプロトコルです。

この章では，IEEE802.3ah OAM の解説と操作方法について説明します。

27.1　解説

27.1.1　概要

IEEE802.3ah OAM は，IEEE802.3ah（Ethernet in the First Mile）に規定された，物理層で隣接装置間の運用状態を確認するためのプロトコルです。ネットワークオペレータにネットワーク状態の監視機能と，リンク障害個所および障害状態の検査機能を提供します。

本装置がサポートする IEEE802.3ah OAM の機能一覧を次の表に示します。

表 27-1　本装置がサポートする IEEE802.3ah OAM の機能一覧

名称	説明
IEEE802.3ah OAM（Information）	隣接装置と OAM 情報を送受信する機能。
UDLD	片方向リンク障害を検出し，ポートを inactive 状態にする機能。
ループ検出機能	誤接続が想定されるループを検出し，ポートを inactive 状態にする機能。

27.1.2　IEEE802.3ah OAM

IEEE802.3ah OAM は，監視および検査に Slow Protocols として規定された OAM Protocols Data Unit（OAMPDU）を使用します。OAMPDU を使用して隣接装置と自装置の OAM 情報を交換し，常時一定間隔で，隣接装置とのフレームの到達性を確認します。

IEEE802.3ah OAM は，隣接装置間の正常運用を確認するためのプロトコルであり，基本的にブリッジ・スイッチは透過しません。隣接装置とは 1 対 1 で接続する必要があります。

(1)　サポート仕様

本装置がサポートする IEEE802.3ah OAM の仕様を「表 27-2　IEEE802.3ah OAM でサポートする OAMPDU」から「表 27-4　IEEE802.3ah OAM でサポートするモード」に示します。

表 27-2　IEEE802.3ah OAM でサポートする OAMPDU

名称	説明	サポート
Information	隣接装置に OAM 状態情報を送信する。	○
Event Notification	隣接装置に Link Event の警告を送信する。	×
Variable Request	隣接装置に MIB 変数を要求する。	×
Variable Response	要求された MIB 変数を送信する。	×
Loopback Control	隣接装置の Loopback 状態を制御する。	×
Organization Specific	機能拡張用。	×

（凡例）○：サポート　×：未サポート

表 27-3　Information OAMPDU でサポートする TLV

名称	説明	サポート
Local Information	送信元装置の OAM 情報。	○
Remote Information	隣接装置の OAM 情報。	○
Organization Specific Information	ベンダー・組織独自の OAM 情報。	○

（凡例）○：サポート

表 27-4　IEEE802.3ah OAM でサポートするモード

モード	説明	サポート
active	隣接装置に関係なく OAMPDU を送信する。	○
passive	隣接装置から Information OAMPDU を受信した場合に OAMPDU を送信する。	○

（凡例）○：サポート

(2)　装置 MAC アドレス

IEEE802.3ah OAM では，装置 MAC アドレスを装置識別子として使用します。

27.1.3　UDLD

UDLD（Uni-Directional Link Detection）とは，片方向リンク障害を検出する機能です。

片方向リンク障害が発生すると，一方の装置では送信はできるが受信ができない状態，もう一方の装置では受信はできるが送信はできない状態になります。上位プロトコルでは誤動作が発生し，ネットワーク上でさまざまな障害が発生します。よく知られている例として，スパニングツリーでのループの発生や，リンクアグリゲーションでのフレームの損失が挙げられます。これらの障害は，片方向リンク障害を検出した時に該当するポートを inactive 状態にすることで，未然に防げます。

本装置は，IEEE802.3ah OAM に規定された Information OAMPDU の Organization Specific Information TLV を使って UDLD を実現します。常時，隣接装置と自装置間で OAM 状態情報を交換して，フレームの到達性を確認することで双方向リンク状態を監視します。UDLD は双方向リンク状態を確認できなくなったときに，片方向リンク障害が発生したと判断します。

本装置では，双方向リンク状態を 1 秒に 1 回確認します。OAMPDU の応答タイムアウトが決められた回数だけ連続すると，片方向リンク障害と判断し，ポートを inactive 状態にします。ポートが inactive 状態になると隣接装置側のポートでもリンクダウンを検出し，接続された双方の装置で該当ポートでの運用を停止します。

inactive 状態になったポートは，片方向リンク障害要因を取り除いたあと，運用コマンド activate で active 状態に戻します。

(1)　サポート仕様

本装置での UDLD のサポート仕様を次の表に示します。

表 27-5　UDLD のサポート仕様

名称	サポート
片方向リンク障害検出	○
片方向リンク障害と判断する回数設定※	○
片方向リンク障害検出ポートの inactivate	○
片方向リンク障害検出システムメッセージ	○
片方向リンク障害検出 SNMP 通知	○

（凡例）○：サポート

注※　片方向リンク障害と判断する回数の設定によって，片方向リンク障害発生から検出までのおよその時間は次のようになります。

5（隣接装置からの情報タイムアウト時間）+片方向リンク障害と判断する回数（秒）

(2)　UDLD の設定

UDLD を使用する場合，接続した双方のポートで UDLD を有効にします。接続した双方のポートのどちらか一方でも UDLD を有効にしなかった場合は，障害を検出できないことがあります。

27.1.4　ループ検出機能

ループ検出機能は，誤接続が想定されるポート単位のループを検出する機能です。

本装置は，IEEE802.3ah OAM に規定された Information OAMPDU を使ってループを検出します。IEEE802.3ah OAM は，物理層で隣接装置間の正常運用を確認するプロトコルのため，OAMPDU は隣接装置が終端になります。この特徴を利用して，本装置が送出した OAMPDU が戻ってきた場合にループを検出したと判断し，ポートを inactive 状態にします。

レイヤ 2 ネットワーク上のループを検出したい場合は，L2 ループ検知を使用します。

(1)　サポート仕様

本装置でのループ検出機能のサポート仕様を次の表に示します。

表 27-6　ループ検出機能のサポート仕様

名称	サポート
ループ検出	○※
ループ検出ポートの inactivate	○
ループ検出システムメッセージ	○
ループ検出 SNMP 通知	○

（凡例）○：サポート

注※　UDLD を有効にすることで，ループ検出機能も有効になります。

27.1.5　IEEE802.3ah OAM の注意事項

(1)　他社の UDLD との接続について

UDLD は，各社独自仕様で機能を実装しています。本装置は，IEEE802.3ah OAM を使って，Information OAMPDU の Organization Specific Information TLV によって UDLD を実現しています。このため，本装置の UDLD と他社装置の UDLD は，相互接続できません。

(2)　UDLD を設定した装置間にメディアコンバータなどの中継装置を接続した場合

片方のリンク状態が切断された場合に，もう片方のリンク状態を自動的に切断しないメディアコンバータを装置間に設置した場合，装置間でリンク状態の認識にずれが生じます。このため，コンフィグレーションコマンド efmoam active udld を設定したポートで対向となる装置が動作していない状態でも片方向リンク障害を検出します。復旧する際にも，双方の装置で同期をとる必要があり，運用が困難になります。片方のリンク状態が切断された場合に，もう片方のリンク状態を自動で切断する機能のあるメディアコンバータを使用してください。

(3)　リンクアグリゲーションとの共存について

スタティックリンクアグリゲーションのポートで，チャネルグループを Disable 状態にすると，対向装置から受信する OAMPDU を廃棄します。

27.2　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

IEEE802.3ah OAM 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
efmoam active	IEEE802.3ah OAM の監視対象ポートを active モードに設定します。また，UDLD およびループ検出機能を有効にします。
efmoam disable	IEEE802.3ah OAM を無効にします。
efmoam udld-detection-count	OAMPDU の応答タイムアウトが発生した場合に，片方向リンク障害と判断する回数を設定します。

27.2.2　UDLD とループ検出機能の設定

(1)　IEEE802.3ah OAM の設定と UDLD およびループ検出機能の有効化

[設定のポイント]

UDLD を使用するには，まず装置全体で IEEE802.3ah OAM を有効にすることが必要です。本装置では初期導入時に IEEE802.3ah OAM が有効です（全ポート passive モード）。

次に，UDLD を使用するポートを，udld パラメータを指定した efmoam active コマンドで，active モードに設定します。UDLD を設定することで，ループ検出機能も同時に有効になります。

ここでは，gigabitethernet 1/1 で UDLD とループ検出機能を有効にします。

[コマンドによる設定]

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

   ポート 1/1 のコンフィグレーションモードに移行します。

2. **(config-if)# efmoam active udld**

   ポート 1/1 で IEEE802.3ah OAM を active モードに設定し，UDLD およびループ検出機能を有効にします。

27.3　オペレーション

27.3.1　運用コマンド一覧

IEEE802.3ah OAM の運用コマンド一覧を次の表に示します。

表 27-8　運用コマンド一覧

コマンド名	説明
show efmoam	IEEE802.3ah OAM，UDLD およびループ検出機能の設定情報ならびにポートの状態を表示します。
show efmoam statistics	IEEE802.3ah OAM，UDLD およびループ検出機能の統計情報を表示します。
clear efmoam statistics	IEEE802.3ah OAM，UDLD およびループ検出機能の統計情報をクリアします。

27.3.2　IEEE802.3ah OAM，UDLD，およびループ検出機能の情報の表示

IEEE802.3ah OAM，UDLD およびループ検出機能の情報は，show efmoam コマンドで表示します。show efmoam コマンドは，IEEE802.3ah OAM および UDLD の設定情報と active モードに設定されたポートの情報を表示します。show efmoam コマンドに detail パラメータを指定すると，active モードに設定されたポートに加え，隣接装置を認識している passive モードのポートの情報を表示します。

図 27-1　show efmoam コマンドの実行結果

```
> show efmoam
Date 20XX/10/02 23:59:59 UTC
Status: Enabled
udld-detection-count: 30
Port   Link status     UDLD status    Dest MAC
1/1    Up              detection    * 0012.e298.dc20
1/2    Down            active         unknown
1/4    Down(uni-link)  detection      unknown
>
```

図 27-2　show efmoam detail コマンドの実行結果

```
> show efmoam detail
Date 20XX/10/02 23:59:59 UTC
Status: Enabled
udld-detection-count: 30
Port   Link status     UDLD status    Dest MAC
1/1    Up              detection    * 0012.e298.dc20
1/2    Down            active         unknown
1/3    Up              passive        0012.e298.7478
1/4    Down(uni-link)  detection      unknown
>
```

28 LLDP

この章では，本装置に隣接する装置の情報を検出および管理する機能である LLDP の解説と操作方法について説明します。

28.1　解説

28.1.1　概要

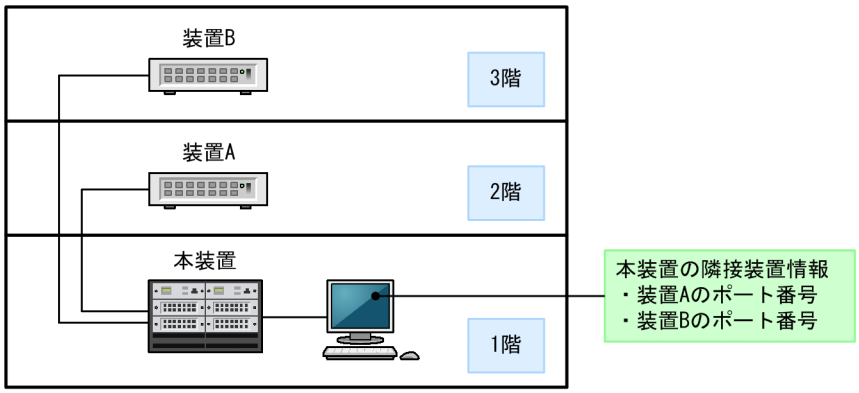
LLDP（Link Layer Discovery Protocol）はデータリンク層の接続を検出および管理するプロトコルです。LLDP フレーム（LLDPDU）の送受信によって，隣接装置の情報を自動で検出します。

(1)　LLDP の適用例

LLDP は，本装置が収容するすべてのイーサネットポートで使用できます。LLDP を使用したポートでは，接続装置から受信する情報を隣接装置情報として管理します。

LLDP の適用例を次の図に示します。この例では，同一ビル内の各階に設置された各装置との接続状態を，1 階に設置した本装置から把握できるようになります。

図 28–1　LLDP の適用例



28.1.2　サポート仕様

(1)　接続できる LLDP 規格

本装置では次に示す二つの規格をサポートします。

- IEEE Std 802.1AB-2009
- IEEE802.1AB/D6.0（Draft6.0 LLDP）

デフォルトでは IEEE Std 802.1AB-2009 で動作して，Draft6.0 の LLDPDU だけを受信したポートからは Draft6.0 の LLDPDU を送信します。なお，IEEE Std 802.1AB-2005 とも接続できます。規格別受信 LLDPDU と送信 LLDPDU の関係を次の表に示します。

表 28–1　規格別受信 LLDPDU と送信 LLDPDU の関係

受信 LLDPDU		送信 LLDPDU の規格
IEEE Std 802.1AB-2009, IEEE Std 802.1AB-2005	Draft6.0	
受信なし	受信なし	IEEE Std 802.1AB-2009
	受信あり	Draft6.0

受信 LLDPDU		送信 LLDPDU の規格
IEEE Std 802.1AB-2009, IEEE Std 802.1AB-2005	Draft6.0	
受信あり	受信なし	IEEE Std 802.1AB-2009
	受信あり	IEEE Std 802.1AB-2009

(2)　サポート TLV

本装置での TLV のサポート状況を次の表に示します。

表 28-2　TLV のサポート状況

TLV name	送信	受信	説明
Chassis ID	○	○	装置の MAC アドレスを送信します。
Port ID	○	○	ポートの MAC アドレスを送信します。
Time To Live	○	○	本装置が送信する情報の保持時間はコンフィグレーションで変更できます。
Port Description	○	○	interface グループ MIB の ifDescr と同じ値を送信します。
System Name	○	○	system グループ MIB の sysName と同じ値を送信します。
System Description	○	○	system グループ MIB の sysDescr と同じ値を送信します。
System Capabilities	×	○	なし。
Management Address	×	○	なし。
Organizationally Specific TLVs • VLAN 情報 • VLAN Address 情報	○※	○	Draft6.0 だけサポートします。 VLAN Tag 値の一覧情報，および IP アドレスと対応する VLAN Tag 値を一つ送受信します。

（凡例）　○：サポート　×：非サポート

注※

スイッチポートでは送信しません。

28.1.3　LLDP 隣接装置の検出および削除のシステムメッセージ出力機能

本装置は，LLDP が隣接装置を検出および削除したときに，ポートごとにシステムメッセージを出力します。本機能を有効にすると，LLDP での隣接装置の検出および削除をシステムメッセージでリアルタイムに確認できます。LLDP 隣接装置の検出および削除のシステムメッセージ出力契機を次の表に示します。

表 28-3　LLDP 隣接装置の検出および削除のシステムメッセージ出力契機

システムメッセージの種類	システムメッセージの出力契機
LLDP 隣接装置検出	• 本機能を有効にしたあと，最初の LLDP 隣接装置を受信したとき。

システムメッセージの種類	システムメッセージの出力契機
	• LLDP 隣接装置の保持時間経過などで LLDP 隣接装置を削除したあと，最初の LLDP 隣接装置を受信したとき。
LLDP 隣接装置削除	• LLDP 隣接装置の保持時間が経過して，LLDP 隣接装置を削除したとき。 • 二重化構成で系切替して新運用系になり，LLDP 隣接装置を削除したとき。 • 運用コマンド clear lldp を実行して，LLDP 隣接装置を削除したとき。 • shutdown LLDPDU を受信して，LLDP 隣接装置を削除したとき。 • ポートがリンクアップして，LLDP 隣接装置を削除したとき。※ • コンフィグレーションコマンド lldp enable または lldp run を削除して，LLDP 隣接装置を削除したとき。

注※

Draft6.0 では出力しません。

28.1.4 LLDP 使用時の注意事項

(1) 系切替時の動作について

BCU の系切替時は，新運用系で隣接装置情報を新たに取得します。

(2) VRF 機能との共存について（Draft6.0 動作時）

VRF を設定したインタフェースに設定された IP アドレス情報は送信しません。

(3) リンクアグリゲーションとの共存について

スタティックリンクアグリゲーションの使用時，チャネルグループを Disable 状態にすると，チャネルグループのポートで対向装置から受信する LLDPDU を廃棄します。

28.2　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

LLDP 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 28-4　コンフィグレーションコマンド一覧

コマンド名	説明
lldp enable	ポートで LLDP の運用を開始します。
lldp hold-count	本装置が送信する LLDP フレームに対して隣接装置が保持する時間を指定します。
lldp interval-time	本装置が送信する LLDP フレームの送信間隔を指定します。
lldp logging enable	ポートで LLDP 隣接装置の検出および削除のシステムメッセージ出力を開始します。
lldp run	装置全体で LLDP を有効にします。

28.2.2　LLDP の設定

(1)　LLDP の設定

[設定のポイント]

LLDP のコンフィグレーションでは装置全体で LLDP を有効にする設定と，実際に運用するポートで LLDP を有効にする設定が必要です。

ここでは，gigabitethernet 1/1 で LLDP を運用します。

[コマンドによる設定]

1. **(config)# lldp run**
   装置全体で LLDP を有効にします。
2. **(config)# interface gigabitethernet 1/1**
   ポート 1/1 のコンフィグレーションモードに移行します。
3. **(config-if)# lldp enable**
   ポート 1/1 で LLDP の動作を開始します。

(2)　LLDP フレームの送信間隔，保持時間の設定

[設定のポイント]

LLDP フレームの保持時間は，送信間隔の倍率で指定します。

[コマンドによる設定]

1. **(config)# lldp interval-time 60**
   LLDP フレームの送信間隔を 60 秒に設定します。
2. **(config)# lldp hold-count 3**
   本装置が送信した情報を隣接装置が保持する時間を，送信間隔の倍率で指定します。この場合，60 秒×3 で 180 秒になります。

28.3 オペレーション

28.3.1 運用コマンド一覧

LLDP の運用コマンド一覧を次の表に示します。

表 28-5 運用コマンド一覧

コマンド名	説明
show lldp	LLDP の設定情報および隣接装置情報を表示します。
show lldp statistics	LLDP の統計情報を表示します。
clear lldp	LLDP の隣接装置情報をクリアします。
clear lldp statistics	LLDP の統計情報をクリアします。
restart lldp	LLDP プログラムを再起動します。
dump protocols lldp	LLDP プログラムで採取している詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。

28.3.2 LLDP 情報の表示

show lldp コマンドで LLDP の設定情報とポートごとの隣接装置数を表示します。コマンドの実行結果を次の図に示します。

図 28-2 show lldp コマンドの実行結果

```
> show lldp
Date 20XX/04/01 12:00:00 UTC
Status: Enabled     Chassis ID: Type=MAC          Info=0012.e2c8.3c31
Interval Time: 30       Hold Count: 4     TTL: 121
Port Counts=3
  1/ 1(CH:  10) Link: Up      Neighbor Counts:    1
  1/ 2          Link: Down    Neighbor Counts:    0
  1/ 3          Link: Up      Neighbor Counts:    1
>
```

show lldp コマンドで detail パラメータを指定すると，隣接装置の詳細情報を表示します。コマンドの実行結果を次の図に示します。

図 28-3 show lldp コマンド（detail パラメータ指定時）の実行結果

```
> show lldp detail
Date 20XX/04/01 12:00:00 UTC
Status: Enabled     Chassis ID: Type=MAC          Info=0012.e2c8.3c31
Interval Time: 30       Hold Count: 4     TTL: 121      Draft TTL: 120
System Name: LLDP1
System Description: ALAXALA AX8600S AX-8600-S16 [AX8616S] Switching software
 (including encryption) Ver. 12.4 [OS-SE]
Neighbor Counts=1
Draft Neighbor Counts=1
Port Counts=3
Port 1/1  (CH:  10)
  Link: Up      PortEnabled: TRUE     AdminStatus: enabledRxTx
  Neighbor Counts:   1    Draft Neighbor Counts:   0
  Port ID: Type=MAC          Info=0012.e238.4cc0
  Port Description: GigabitEther 1/1
  Neighbor 1      TTL: 100
    Chassis ID: Type=MAC          Info=0012.e2c8.3c85
    System Name: LLDP2
    System Description: ALAXALA AX8600S AX-8600-S16 [AX8616S] Switching software
```

```
 (including encryption) Ver. 12.4 [OS-SE]
    Port ID: Type=MAC          Info=0012.e238.4cd1
    Port Description: GigabitEther 1/12
Port 1/2
  Link: Down    PortEnabled: FALSE    AdminStatus: enabledRxTx
  Neighbor Counts:   0    Draft Neighbor Counts:   0
Port 1/3
  Link: Up      PortEnabled: TRUE     AdminStatus: enabledRxTx
  Neighbor Counts:   0    Draft Neighbor Counts:   1
  Port ID: Type=MAC          Info=0012.e238.4cc2
  Port Description: GigabitEther 1/3
  Tag ID: Tagged=1,10-20,4094
  IPv4 Address: Tagged: 10      192.168.248.240
  IPv6 Address: Tagged: 20      2001:db8:811:ff01:200:8798:5cc0:e7f4
  Draft Neighbor 1      TTL: 100
    Chassis ID: Type=MAC          Info=0012.e268.2c21
    System Name: LLDP3
    System Description: ALAXALA AX6300S AX-6300-S08 [AX6308S] Switching software
 Ver. 11.9 [OS-SE]
    Port ID: Type=MAC          Info=0012.e298.5cc4
    Port Description: GigabitEther 1/5
    Tag ID: Tagged=1,10-20,4094
    IPv4 Address: Tagged: 10      192.168.248.244
    IPv6 Address: Tagged: 20      2001:db8:811:ff01:200:8798:5cc0:e7f8
>
```

付録

付録 A　準拠規格

付録 A.1　VLAN

表 A–1　VLAN の準拠規格および勧告

規格	規格名
IEEE802.1Q (IEEE Std 802.1Q-2003)	Virtual Bridged Local Area Networks※

注※　GVRP/GMRP はサポートしていません。

付録 A.2　スパニングツリー

表 A–2　スパニングツリーの準拠規格および勧告

規格	規格名
IEEE802.1D (ANSI/IEEE Std 802.1D-1998 Edition)	Media Access Control (MAC) Bridges (The Spanning Tree Algorithm and Protocol)
IEEE802.1t (IEEE Std 802.1t-2001)	Media Access Control (MAC) Bridges - Amendment 1
IEEE802.1w (IEEE Std 802.1w-2001)	Media Access Control (MAC) Bridges - Amendment 2: Rapid Reconfiguration
IEEE802.1s (IEEE Std 802.1s-2002)	Virtual Bridged Local Area Networks - Amendment 3: Multiple Spanning Trees

付録 A.3　IGMP/MLD snooping

表 A–3　IGMP/MLD snooping の準拠規格および勧告

規格番号(発行年月)	規格名
RFC4541(2006 年 5 月)	Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

付録 A.4　ポリサー

表 A–4　ポリサーの準拠規格および勧告

規格番号(発行年月)	規格名
RFC2697(1999 年 9 月)	A Single Rate Three Color Marker
RFC2698(1999 年 9 月)	A Two Rate Three Color Marker

付録 A.5　マーカー

表 A-5　マーカーの準拠規格および勧告

規格(発行年月)	規格名
IEEE802.1D(2004 年 6 月) (IEEE Std 802.1D-2004)	Media Access Control (MAC) Bridges

付録 A.6　Diff-serv

表 A-6　Diff-serv の準拠規格および勧告

規格番号(発行年月)	規格名
RFC2474(1998 年 12 月)	Definition of the Differentiated Services Field(DS Field) in the IPv4 and IPv6 Headers
RFC2475(1998 年 12 月)	An Architecture for Differentiated Services
RFC2597(1999 年 6 月)	Assured Forwarding PHB Group
RFC3246(2002 年 3 月)	An Expedited Forwarding PHB (Per-Hop Behavior)
RFC3260(2002 年 4 月)	New Terminology and Clarifications for Diffserv

付録 A.7　sFlow

表 A-7　sFlow の準拠規格および勧告

規格番号(発行年月)	規格名
RFC3176(2001 年 9 月)	InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks

付録 A.8　IEEE802.3ah OAM

表 A-8　IEEE802.3ah OAM の準拠規格および勧告

規格(発行年月)	規格名
IEEE802.3ah(2004 年 9 月)	Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment: Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks

付録 A.9　LLDP

表 A-9　LLDP の準拠規格および勧告

規格(発行年月)	規格名
IEEE802.1AB/D6.0(2003 年 10 月)	Draft Standard for Local and Metropolitan Networks: Station and Media Access Control - Connectivity Discovery
IEEE Std 802.1AB-2009(2009 年 9 月)	IEEE Standard for Local and metropolitan area networks: Station and Media Access Control Connectivity Discovery

索引

い

え

か

け

こ

さ

し

す

そ

と

ふ

ほ

ま

み

も

ゆ

れ