

PF5200 シリーズ 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



■対象製品

このマニュアルは PF5200 シリーズを対象に記載しています。ソフトウェア機能は、ソフトウェア OS-F3PA によってサポートする機能について記載します。

■輸出時の注意

本製品は、外国為替及び外国貿易法に基づくリスト規制の該当貨物ですので、輸出（または非居住者への技術の提供あるいは外国において技術の提供をすることを目的とする取引）を行う場合には、経済産業大臣の輸出許可（または役務取引許可）が必要となります。

また、本製品には米国の輸出関連法令の規制を受ける技術が含まれており、輸出する場合輸出先によっては米国政府の許可が必要です。

■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、米国 Xerox Corp. の商品名称です。

Internet Explorer は、米国 Microsoft Corporation の、米国、日本およびその他の国における登録商標または商標です。

IPX は、Novell, Inc. の商標です。

Microsoft は、米国 Microsoft Corporation の、米国、日本およびその他の国における登録商標または商標です。

Octpower は、日本電気株式会社の登録商標です。

sFlow は、米国およびその他の国における米国 InMon Corp. の登録商標です。

UNIX は、X/Open Company Limited が独占的にライセンスしている米国ならびに他の国における登録商標です。

Windows は米国 Microsoft Corporation の米国およびその他の国における登録商標です。

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。

「プログラマブルフロー」および「ProgrammableFlow」は、日本電気株式会社の登録商標または商標です。

その他、各会社名、各製品名は、各社の商標または登録商標です。

■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。

■電波障害について

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

■高調波規制について

高調波電流規格 JIS C 61000-3-2 適合品

適合装置：

- PF5240F-48T4XW
- PF5240R-48T4XW

■発行

2011年10月(初版) NWD-126034-002

■著作権

Copyright (C) 2010-2011, NEC Corporation. All rights reserved.

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 PF5200 シリーズを対象に記載しています。ソフトウェア機能は、ソフトウェア OS-F3PA によってサポートする機能について記載します。

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

■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

■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について知りたい

PF5200 シリーズ
クイックスタートガイド
(NWD-126031-001)

- ハードウェアの設備条件、取り扱い方法について知りたい

PF5200 シリーズ
ハードウェア取扱説明書
(NWD-126033-001)

- ソフトウェアの機能、コンフィグレーションの設定、運用コマンドについて知りたい

PF5200 シリーズ 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.1
(NWD-126034-001)

PF5200 シリーズ 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
(NWD-126034-002)

PF5200 シリーズ ソフトウェアマニュアル
コンフィグレーションガイド Vol.3
(NWD-126034-003)

- コンフィグレーションコマンドの入力シンタックス、パラメータ詳細について知りたい

PF5200 シリーズ ソフトウェアマニュアル
コンフィグレーションコマンドレファレンス Vol.1
(NWD-126037-001)

PF5200 シリーズ ソフトウェアマニュアル
コンフィグレーションコマンドレファレンス Vol.2
(NWD-126037-002)

- 運用コマンドの入力シンタックス、パラメータ詳細について知りたい

PF5200 シリーズ ソフトウェアマニュアル
運用コマンドレファレンス Vol.1
(NWD-126039-001)

PF5200 シリーズ ソフトウェアマニュアル
運用コマンドレファレンス Vol.2
(NWD-126039-002)

- メッセージとログについて知りたい

PF5200 シリーズ ソフトウェアマニュアル
メッセージ・ログレファレンス
(NWD-126041-001)

- MIB について知りたい

PF5200 シリーズ ソフトウェアマニュアル
MIB レファレンス
(NWD-126042-001)

- ソフトウェアアップデートを行う手順について知りたい

PF5200 シリーズ
ソフトウェアアップデートガイド
(NWD-126047-001)

- ネットワーク接続のセキュアな運用管理について知りたい

PF5200 シリーズ
Secure Shell (SSH) ソフトウェアマニュアル
(NWD-126044-001)

- トラブル発生時の対処方法について知りたい

PF5200 シリーズ
トラブルシューティングガイド
(NWD-126043-001)

- Secure Channel の TLS 接続について知りたい

PF5200 シリーズ
【別冊】OpenFlow 機能 TLS 対応編
(NWD-126045-001)

■このマニュアルでの表記

AC	Alternating Current
ACK	ACKnowledge
ADSL	Asymmetric Digital Subscriber Line
ALG	Application Level Gateway
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AS	Autonomous System
AUX	Auxiliary
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol - version 4
BGP4+	Multiprotocol Extensions for Border Gateway Protocol - version 4
bit/s	bits per second * Described as bps in some cases.
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
CC	Continuity Check
CDP	Cisco Discovery Protocol
CFM	Connectivity Fault Management
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network System
CONS	Connection Oriented Network System
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNP	Complete Sequence Numbers PDU
CST	Common Spanning Tree
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DHCP	Dynamic Host Configuration Protocol
DIS	Draft International Standard/Designated Intermediate System
DNS	Domain Name System
DR	Designated Router
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
EAP	Extensible Authentication Protocol
EAPO	EAP Over LAN
EFM	Ethernet in the First Mile
E-Mail	Electronic Mail
ES	End System
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FQDN	Fully Qualified Domain Name
FTTH	Fiber To the Home
GBIC	GigaBit Interface Converter
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCP	IP Control Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IP Version 6 Control Protocol
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Internal Spanning Tree
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light Emitting Diode

LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLQ+3WFQ	Low Latency Queueing + 3 Weighted Fair Queueing
LSP	Label Switched Path
LSP	Link State PDU
LSR	Label Switched Router
MA	Maintenance Association
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MEP	Maintenance association End Point
MIB	Management Information Base
MIP	Maintenance domain Intermediate Point
MRU	Maximum Receive Unit
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transfer Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NAT	Network Address Translation
NCP	Network Control Protocol
NDP	Neighbor Discovery Protocol
NET	Network Entity Title
NLA ID	Next-Level Aggregation Identifier
NPDU	Network Protocol Data Unit
NSAP	Network Service Access Point
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OADP	Octpower Auto Discovery Protocol
OAM	Operations, Administration, and Maintenance
OFC	OpenFlow Controller
OFS	OpenFlow Switch
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
PAD	PADding
PAE	Port Access Entity
PC	Personal Computer
PCI	Protocol Control Information
PDU	Protocol Data Unit
PFS	Programmable Flow Switch
PICS	Protocol Implementation Conformance Statement
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PIM-SSM	Protocol Independent Multicast-Source Specific Multicast
PRI	Primary Rate Interface
PS	Power Supply
PSNP	Partial Sequence Numbers PDU
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
REJ	REject
RFC	Request For Comments
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RQ	ReQuest
RSI	Real Switch Instance
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
SD	Secure Digital
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SEL	NSAP SELector
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol

SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SPF	Shortest Path First
SSAP	Source Service Access Point
STP	Spanning Tree Protocol
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
TLV	Type, Length, and Value
TOS	Type Of Service
TPID	Tag Protocol Identifier
TTL	Time To Live
UDLD	Uni-Directional Link Detection
UDP	User Datagram Protocol
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
VLAN	Virtual LAN
VRRP	Virtual Router Redundancy Protocol
VSI	Virtual Switch Instance
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queueing
WoL	Wake on LAN
WRED	Weighted Random Early Detection
WS	Work Station
WWW	World-Wide Web
XFP	10 gigabit small Form factor Pluggable

■常用漢字以外の漢字の使用について

このマニュアルでは、常用漢字を使用することを基本としていますが、次に示す用語については、常用漢字以外を使用しています。

- 溢れ（あふれ）
- 迂回（うかい）
- 筐体（きょうたい）
- 每（ごと）
- 閾值（しきいち）
- 溜まる（たまる）
- 輻輳（ふくそう）
- 漏洩（ろうえい）

■ kB(バイト)などの単位表記について

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

目次

第1編 フィルタ

1	フィルタ	1
1.1	解説	2
1.1.1	フィルタの概要	2
1.1.2	フロー検出	3
1.1.3	受信側フロー検出モード	3
1.1.4	送信側フロー検出モード	4
1.1.5	フロー検出条件	5
1.1.6	アクセリスト	11
1.1.7	暗黙の廃棄	12
1.1.8	フィルタ使用時の注意事項	12
1.2	コンフィグレーション	14
1.2.1	コンフィグレーションコマンド一覧	14
1.2.2	受信側フロー検出モードの設定	14
1.2.3	送信側フロー検出モードの設定	15
1.2.4	MAC ヘッダで中継・廃棄をする設定	15
1.2.5	IP ヘッダ・TCP/UDP ヘッダで中継・廃棄をする設定	16
1.2.6	複数インターフェースフィルタの設定	18
1.3	オペレーション	19
1.3.1	運用コマンド一覧	19
1.3.2	フィルタの確認	19

第2編 QoS

2	QoS 制御の概要	21
2.1	QoS 制御構造	22
2.2	共通処理解説	24
2.2.1	ユーザ優先度マッピング	24
2.2.2	ユーザ優先度マッピングの注意事項	25
2.3	QoS 制御共通のコンフィグレーション	26
2.3.1	コンフィグレーションコマンド一覧	26
2.4	QoS 制御共通のオペレーション	27
2.4.1	運用コマンド一覧	27

3

フロー制御	29
3.1 フロー検出解説	30
3.1.1 受信側フロー検出モード	30
3.1.2 フロー検出条件	31
3.1.3 QoS フローリスト	34
3.1.4 フロー検出使用時の注意事項	35
3.2 フロー検出コンフィグレーション	36
3.2.1 受信側フロー検出モードの設定	36
3.2.2 複数インタフェースの QoS 制御の指定	36
3.2.3 TCP/UDP ポート番号の範囲で QoS 制御する設定	37
3.3 フロー検出のオペレーション	38
3.3.1 IPv4 パケットをフロー検出条件とした QoS 制御の動作確認	38
3.4 帯域監視解説	39
3.4.1 帯域監視	39
3.4.2 帯域監視使用時に採取可能な統計情報	40
3.4.3 帯域監視使用時の注意事項	41
3.5 帯域監視のコンフィグレーション	42
3.5.1 最大帯域制御の設定	42
3.5.2 最低帯域監視違反時のキューリング優先度の設定	42
3.5.3 最低帯域監視違反時の DSCP 書き換えの設定	43
3.5.4 最大帯域制御と最低帯域監視の組み合わせの設定	43
3.6 帯域監視のオペレーション	45
3.6.1 最大帯域制御の確認	45
3.6.2 最低帯域監視違反時のキューリング優先度の確認	45
3.6.3 最低監視帯域違反時の DSCP 書き換えの確認	46
3.6.4 最大帯域制御と最低帯域監視の組み合わせの確認	46
3.7 マーカー解説	47
3.7.1 ユーザ優先度書き換え	47
3.7.2 ユーザ優先度引き継ぎ	48
3.7.3 DSCP 書き換え	49
3.8 マーカーのコンフィグレーション	51
3.8.1 ユーザ優先度書き換えの設定	51
3.8.2 ユーザ優先度引き継ぎの設定	51
3.8.3 DSCP 書き換えの設定	52
3.9 マーカーのオペレーション	53
3.9.1 ユーザ優先度書き換えの確認	53
3.9.2 ユーザ優先度引き継ぎの確認	53
3.9.3 DSCP 書き換えの確認	53
3.10 優先度決定の解説	54
3.10.1 CoS 値・キューリング優先度	54
3.10.2 CoS マッピング機能	55

3.10.3 優先度決定使用時の注意事項	56
3.11 優先度決定コンフィグレーション	57
3.11.1 CoS 値の設定	57
3.12 優先度のオペレーション	58
3.12.1 優先度の確認	58
3.13 複数の QoS エントリに一致した場合の動作	59
4 送信制御	61
4.1 シェーパ解説	62
4.1.1 レガシーシェーパの概要	62
4.1.2 送信キュー長指定	62
4.1.3 スケジューリング	63
4.1.4 ポート帯域制御	65
4.1.5 シェーパ使用時の注意事項	66
4.2 シェーパのコンフィグレーション	67
4.2.1 スケジューリングの設定	67
4.2.2 ポート帯域制御の設定	67
4.3 シェーパのオペレーション	68
4.3.1 スケジューリングの確認	68
4.3.2 ポート帯域制御の確認	68
4.4 廃棄制御解説	69
4.4.1 廃棄制御	69
4.5 廃棄制御のコンフィグレーション	71
4.5.1 キューイング優先度の設定	71
4.6 廃棄制御のオペレーション	72
4.6.1 キューイング優先度の確認	72

第 3 編 OpenFlow 機能

5 OpenFlow 機能の解説	73
5.1 OpenFlow 機能の概要	74
5.1.1 OpenFlow 技術の基本概念	74
5.1.2 OpenFlow 機能の概要	74
5.1.3 OpenFlow 機能の動作概要	75
5.1.4 Programmable Flow Switch の概要	77
5.1.5 PFS の OpenFlow 機能	78
5.2 OpenFlow 機能の解説	81
5.2.1 OpenFlow スイッチインスタンスの解説	81
5.2.2 フローテーブルの解説	82

5.2.3 マッチ条件の解説	87
5.2.4 アクションの解説	88
5.2.5 Secure Channel の解説	92
5.2.6 フローテーブル制御の解説	98
5.2.7 Emergency モードの解説	99
5.2.8 Emergency リンクダウン制御機能	100
5.2.9 Packet In・Packet Out の解説	102
5.2.10 Packet In メッセージのスケジューリング / 帯域制限機能	104
5.2.11 OpenFlow プロトコル制御ポートの解説	105
5.2.12 OpenFlow プロトコル Features 通知機能の解説	109
5.2.13 OpenFlow プロトコルコンフィグレーション機能の解説	110
5.2.14 統計情報の解説	111
5.2.15 マルチヒット機能の解説	113
5.2.16 ポートグループ機能の解説	114
5.2.17 VLAN 設定機能の解説	115
5.2.18 指定パケットの周期送信機能の解説	118
5.3 サポート仕様	119
5.3.1 OpenFlow サポート機能	119
5.3.2 OpenFlow プロトコルサポートメッセージ	120
5.3.3 OpenFlow と L2/L3 スイッチング機能の共存	122

6

OpenFlow 機能の設定と運用	131
6.1 運用手順	132
6.1.1 概要	132
6.1.2 運用の流れ	132
6.2 OpenFlow 機能のコンフィグレーション	133
6.2.1 コンフィグレーションコマンド一覧	133
6.2.2 OpenFlow 機能のコンフィグレーションを設定する前に	134
6.2.3 RSI モードの設定例	135
6.2.4 RSI モードのパラメータ設定	136
6.2.5 VSI モードの設定例	141
6.2.6 VSI モードのパラメータ設定	142
6.3 OpenFlow 機能のオペレーション	148
6.3.1 オペレーションコマンド一覧	148
6.3.2 OpenFlow 情報の確認	149
6.3.3 フローテーブル情報の確認	153
6.3.4 OpenFlow プロトコルメッセージ統計情報の確認	154
6.3.5 PFS-OFC 間の送受信 OpenFlow プロトコルメッセージのリアルタイム表示	156

第4編 冗長化構成による高信頼化機能

7

VRRP

157

7.1 解説	158
7.1.1 仮想ルータの MAC アドレスと IP アドレス	158
7.1.2 VRRP における障害検出の仕組み	159
7.1.3 マスタの選出方法	160
7.1.4 ADVERTISEMENT パケットの認証	161
7.1.5 アクセプトモード	162
7.1.6 障害監視インターフェースと VRRP ポーリング	162
7.1.7 IPv6 VRRP ドラフト対応	166
7.1.8 VRRP 使用時の注意事項	167
7.2 コンフィグレーション	169
7.2.1 コンフィグレーションコマンド一覧	169
7.2.2 VRRP のコンフィグレーションの流れ	170
7.2.3 仮想ルータへの IPv4 アドレス設定	170
7.2.4 仮想ルータへの IPv6 アドレス設定	171
7.2.5 優先度の設定	171
7.2.6 ADVERTISEMENT パケット送出間隔の設定	172
7.2.7 自動切り戻し抑止の設定	172
7.2.8 自動切り戻し抑止時間の設定	173
7.2.9 障害監視インターフェースと VRRP ポーリングの設定	173
7.3 オペレーション	176
7.3.1 運用コマンド一覧	176
7.3.2 仮想ルータの設定確認	176
7.3.3 track の設定確認	177
7.3.4 切り戻し処理の実行	177

第5編 ネットワークの障害検出による高信頼化機能

8

IEEE802.3ah/UDLD

179

8.1 解説	180
8.1.1 概要	180
8.1.2 サポート仕様	180
8.1.3 IEEE802.3ah/UDLD 使用時の注意事項	181
8.2 コンフィグレーション	182
8.2.1 コンフィグレーションコマンド一覧	182
8.2.2 IEEE802.3ah/UDLD の設定	182
8.3 オペレーション	184

8.3.1 運用コマンド一覧	184
8.3.2 IEEE802.3ah/OAM 情報の表示	184

9**ストームコントロール** 187

9.1 解説	188
9.1.1 ストームコントロールの概要	188
9.1.2 ストームコントロール使用時の注意事項	188
9.2 コンフィグレーション	189
9.2.1 コンフィグレーションコマンド一覧	189
9.2.2 ストームコントロールの設定	189

10**L2 ループ検知** 191

10.1 解説	192
10.1.1 概要	192
10.1.2 動作仕様	193
10.1.3 適用例	194
10.1.4 L2 ループ検知使用時の注意事項	195
10.2 コンフィグレーション	196
10.2.1 コンフィグレーションコマンド一覧	196
10.2.2 L2 ループ検知の設定	196
10.3 オペレーション	199
10.3.1 運用コマンド一覧	199
10.3.2 L2 ループ状態の確認	199

11**CFM** 201

11.1 解説	202
11.1.1 概要	202
11.1.2 CFM の構成要素	203
11.1.3 ドメインの設計	208
11.1.4 Continuity Check	212
11.1.5 Loopback	214
11.1.6 Linktrace	215
11.1.7 共通動作仕様	218
11.1.8 CFM で使用するデータベース	220
11.1.9 CFM 使用時の注意事項	222
11.2 コンフィグレーション	224
11.2.1 コンフィグレーションコマンド一覧	224
11.2.2 CFM の設定（複数ドメイン）	224
11.2.3 CFM の設定（同一ドメイン、複数 MA）	226
11.3 オペレーション	228

11.3.1 運用コマンド一覧	228
11.3.2 MP 間の接続確認	228
11.3.3 MP 間のルート確認	228
11.3.4 ルート上の MP の状態確認	229
11.3.5 CFM の状態の確認	229
11.3.6 障害の詳細情報の確認	230

第 6 編 リモートネットワーク管理

12 SNMP を使用したネットワーク管理

12.1 解説	232
12.1.1 SNMP 概説	232
12.1.2 MIB 概説	235
12.1.3 SNMPv1, SNMPv2C オペレーション	237
12.1.4 SNMPv3 オペレーション	243
12.1.5 トラップ	247
12.1.6 RMON MIB	248
12.1.7 SNMP マネージャとの接続時の注意事項	249
12.2 コンフィグレーション	250
12.2.1 コンフィグレーションコマンド一覧	250
12.2.2 SNMPv1, SNMPv2C による MIB アクセス許可の設定	250
12.2.3 SNMPv3 による MIB アクセス許可の設定	251
12.2.4 SNMPv1, SNMPv2C による トラップ送信の設定	252
12.2.5 SNMPv3 による トラップ送信の設定	252
12.2.6 リンクトラップの抑止	253
12.2.7 RMON イーサネットヒストリグループの制御情報の設定	253
12.2.8 RMON による特定 MIB 値の閾値チェック	254
12.3 オペレーション	255
12.3.1 運用コマンド一覧	255
12.3.2 SNMP マネージャとの通信の確認	255

13 ログ出力機能

13.1 解説	258
13.2 コンフィグレーション	259
13.2.1 コンフィグレーションコマンド一覧	259
13.2.2 ログの syslog 出力の設定	259
13.2.3 ログの E-Mail 出力の設定	259

14 sFlow 統計（フロー統計）機能

14.1 解説	262
14.1.1 sFlow 統計の概要	262
14.1.2 sFlow 統計エージェント機能	263
14.1.3 sFlow パケットフォーマット	263
14.1.4 本装置での sFlow 統計の動作について	269
14.2 コンフィグレーション	271
14.2.1 コンフィグレーションコマンド一覧	271
14.2.2 sFlow 統計の基本的な設定	271
14.2.3 sFlow 統計コンフィグレーションパラメータの設定例	274
14.3 オペレーション	277
14.3.1 運用コマンド一覧	277
14.3.2 コレクタとの通信の確認	277
14.3.3 sFlow 統計機能の運用中の確認	277
14.3.4 sFlow 統計のサンプリング間隔の調整方法	278

第 7 編 隣接装置情報の管理

15 LLDP

15.1 解説	282
15.1.1 概要	282
15.1.2 サポート仕様	282
15.1.3 LLDP 使用時の注意事項	285
15.2 コンフィグレーション	286
15.2.1 コンフィグレーションコマンド一覧	286
15.2.2 LLDP の設定	286
15.3 オペレーション	287
15.3.1 運用コマンド一覧	287
15.3.2 LLDP 情報の表示	287

16 OADP

16.1 解説	290
16.1.1 概要	290
16.1.2 サポート仕様	291
16.1.3 OADP 使用時の注意事項	292
16.2 コンフィグレーション	294
16.2.1 コンフィグレーションコマンド一覧	294
16.2.2 OADP の設定	294

16.3 オペレーション	296
16.3.1 運用コマンド一覧	296
16.3.2 OADP 情報の表示	296

第 8 編 ポートミラーリング

17 ポートミラーリング	299
17.1 解説	300
17.1.1 ポートミラーリングの概要	300
17.1.2 ポートミラーリングの注意事項	301
17.2 コンフィグレーション	302
17.2.1 コンフィグレーションコマンド一覧	302
17.2.2 ポートミラーリングの設定	302

付録

付録 A 準拠規格	305
付録 A.1 Diff-serv	306
付録 A.2 VRRP	306
付録 A.3 IEEE802.3ah/UDLD	306
付録 A.4 CFM	306
付録 A.5 SNMP	307
付録 A.6 SYSLOG	308
付録 A.7 sFlow	308
付録 A.8 LLDP	308

索引

309

1 フィルタ

フィルタは、ある特定の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。

1.1 解説

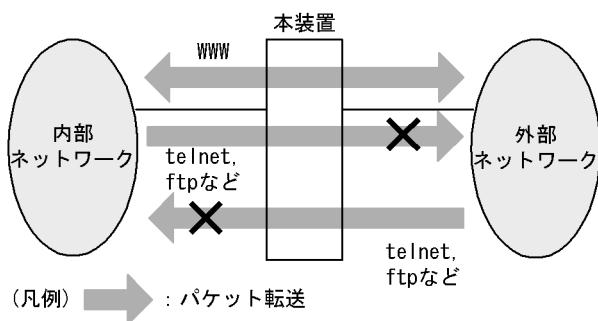
1.2 コンフィグレーション

1.3 オペレーション

1.1 解説

フィルタは、ある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。フィルタを使用すれば、ユーザ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。

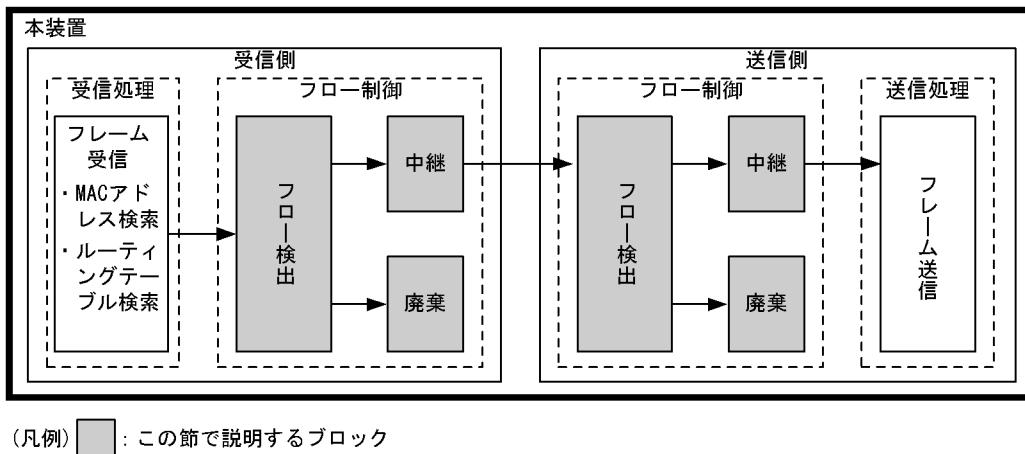
図 1-1 フィルタを使用したネットワーク構成例



1.1.1 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 1-2 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 1-1 フィルタの各機能ブロックの概要

機能部位	機能概要	
フロー制御部	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、ICMP ヘッダ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、ICMP ヘッダ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、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. 各インター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、そのフレームを廃棄します。廃棄動作の詳細は、「1.1.7 暗黙の廃棄」を参照してください。

! 注意事項

受信側インターフェースでフレームが廃棄された場合、送信側インターフェースではフロー検出しません。

1.1.2 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、ICMP ヘッダなどの条件に基づいて検出する機能です。アクセリストで設定します。アクセリストの詳細は、「1.1.6 アクセリスト」を参照してください。

本装置では、受信側イーサネットインターフェース・VLAN インタフェースで、イーサネット V2 形式および IEEE802.3 の SNAP/RFC1042 形式フレームのフロー検出ができます。設定可能なインターフェースは、受信側フロー検出モードによって変わります。なお、本装置宛ての受信フレームもフロー検出対象です。

本装置では、送信側イーサネットインターフェース・VLAN インタフェースで、イーサネット V2 形式および IEEE802.3 の SNAP/RFC1042 形式フレームのフロー検出ができます。設定可能なインターフェースは、送信側フロー検出モードによって変わります。なお、送信側では本装置が自発的に送信するフレームもフロー検出対象です。

1.1.3 受信側フロー検出モード

本装置では、ネットワーク構成や運用形態を想定して受信側フロー検出モードを用意しています。受信側フロー検出モードは、受信側インターフェースに対するフィルタ・QoS エントリの配分パターンを決めるモードです。使い方に合わせて選択してください。また、受信側フロー検出モードを選択する際の目安について次に示します。検出条件の詳細は「1.1.5 フロー検出条件」を参照してください。

- 検出対象インターフェースにイーサネットを指定したい場合は、openflow-2 を使用してください。
- 検出対象インターフェースに VLAN を指定したい場合は、openflow-3 を使用してください。

受信側フロー検出モードは flow detection mode コマンドで指定します。なお、選択した受信側フロー検出モードはフィルタ・QoS で共通です。受信側フロー検出モードを変更する場合、受信側および送信側インターフェースに設定された次のコマンドをすべて削除する必要があります。

- mac access-group
- ip access-group
- mac qos-flow-group
- ip qos-flow-group

受信側フロー検出モードを指定しない場合、openflow-1 がデフォルトのモードとして設定されます。

1. フィルタ

受信側フロー検出モードとフロー動作の関係を次の表に示します。

表 1-2 受信側フロー検出モードとフロー動作の関係

受信側 フロー検出 モード名称	運用目的	フロー動作	検出対象 インターフェース
openflow-1	フロー制御を使用しないモードです。	—	—
openflow-2	IP パケットやそれ以外のフレームのフロー制御を行いたい場合に使用します。また、IPv4 パケットに特化したフロー制御を行いたい場合にも使用できます。	MAC アドレス、イーサネットタイプなどの MAC ヘッダでフレームを検出します。 IPv4 パケットは、IP ヘッダ、TCP/UDP ヘッダ、ICMP ヘッダでフレームを検出します。	イーサネット
openflow-3	IP パケットやそれ以外のフレームのフロー制御を行いたい場合に使用します。また、IPv4 パケットに特化したフロー制御を行いたい場合にも使用できます。	MAC アドレス、イーサネットタイプなどの MAC ヘッダでフレームを検出します。 IPv4 パケットは、IP ヘッダ、TCP/UDP ヘッダ、ICMP ヘッダでフレームを検出します。	VLAN

1.1.4 送信側フロー検出モード

本装置では、ネットワーク構成や運用形態を想定して送信側フロー検出モードを用意しています。送信側フロー検出モードは、送信側インターフェースに対するフィルタエンタリの配分パターンを決めるモードです。使い方に合わせて選択してください。また、送信側フロー検出モードを選択する際の目安について次に示します。MAC 条件および IPv4 条件の詳細は「1.1.5 フロー検出条件」を参照してください。

- MAC 条件および IPv4 条件でフレームを検出したい場合は、openflow-1-out を使用してください。
- IPv4 条件に特化してフレームを検出したい場合は、openflow-2-out を使用してください。

送信側フロー検出モードは flow detection out mode コマンドで指定します。なお、選択した送信側フロー検出モードはフィルタで有効です。送信側フロー検出モードを変更する場合、受信側および送信側インターフェースに設定された次のコマンドをすべて削除する必要があります。

- mac access-group
- ip access-group

送信側フロー検出モードを指定しない場合、openflow-1-out がデフォルトのモードとして設定されます。

送信側フロー検出モードとフロー動作の関係を次の表に示します。

表 1-3 送信側フロー検出モードとフロー動作の関係

送信側フロー 検出モード名称	運用目的	フロー動作	検出対象 インターフェース
openflow-1-out	IP パケットやそれ以外のフレームのフロー制御を行いたい場合に使用します。また、IPv4 パケットに特化したフロー制御を行いたい場合にも使用できます。	MAC アドレス、イーサネットタイプなどの MAC ヘッダでフレームを検出します。 IPv4 パケットは、IP ヘッダ、TCP/UDP ヘッダ、ICMP ヘッダでフレームを検出します。	イーサネット

送信側フロー検出モード名称	運用目的	フロー動作	検出対象インターフェース
openflow-2-out	IPv4 パケットに特化したフロー制御を行いたい場合に使用します。	IPv4 パケットについて、IP ヘッダ、TCP/UDP ヘッダ、ICMP ヘッダでフレームを検出します	イーサネット

1.1.5 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。受信側および送信側インターフェースでのフロー検出条件を次に示します。

(1) 受信側インターフェースのフロー検出条件

受信側インターフェースのフロー検出条件は、受信側フロー検出モードによって異なります。受信側フロー検出モードごとの指定可能なフロー検出条件を次の表に示します。

表 1-4 受信側インターフェースで指定可能なフロー検出条件

種別	設定項目	openflow-2	openflow-3
		イーサネット	VLAN
MAC 条件	コンフィグレーション	VLAN ID ※ 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	○ ○	
	ユーザ優先度※ ²	○ ○	

1. フィルタ

種別	設定項目	openflow-2	openflow-3
		イーサネット	VLAN
IPv4 条件	コンフィグレーション	VLAN ID ^{※1}	○
	MAC ヘッダ	ユーザ優先度 ^{※2}	○
	IPv4 ヘッダ ^{※3}	上位プロトコル	○
		送信元 IP アドレス	○
		宛先 IP アドレス	○
		ToS	○
		DSCP	○
		Precedence	○
	IPv4-TCP ヘッダ	送信元ポート番号	单一指定 (eq)
			範囲指定 (range)
		宛先ポート番号	单一指定 (eq)
			範囲指定 (range)
	TCP 制御フラグ ^{※4}		○
	IPv4-UDP ヘッダ	送信元ポート番号	单一指定 (eq)
			範囲指定 (range)
		宛先ポート番号	单一指定 (eq)
			範囲指定 (range)
	IPv4-ICMP ヘッダ	ICMP タイプ値	○
		ICMP コード値	○

種別	設定項目	openflow-2	openflow-3
		イーサネット	VLAN
IPv6 条件	コンフィグレーション	VLAN ID ^{※1}	—
	MAC ヘッダ	ユーザ優先度 ^{※2}	—
	IPv6 ヘッダ ^{※6}	上位プロトコル	—
		送信元 IP アドレス	—
		宛先 IP アドレス	—
		トライフィッククラス	—
		DSCP	—
	IPv6-TCP ヘッダ	送信元ポート番号	单一指定 (eq) 範囲指定 (range)
		宛先ポート番号	单一指定 (eq) 範囲指定 (range)
		TCP 制御フラグ ^{※4}	—
	IPv6-UDP ヘッダ	送信元ポート番号	单一指定 (eq) 範囲指定 (range)
		宛先ポート番号	单一指定 (eq) 範囲指定 (range)
	IPv6-ICMP ヘッダ	ICMP タイプ値	—
		ICMP コード値	—

(凡例) ○ : 指定できる — : 指定できない

注※ 1

本装置のフロー検出で検出できる VLAN ID は、VLAN コンフィグレーションで入力した VLAN に対して付与する値です。受信フレームの属する VLAN ID を検出します。

注※ 2

次に示すフレームについてはユーザ優先度を検出できません。常に、ユーザ優先度 3 として検出します。

- ・ VLAN tag なしのフレーム
- ・ VLAN トンネリングを設定したポートで受信したフレーム

VLAN tag が複数あるフレームに対してユーザ優先度を検出する場合、MAC アドレス側から 1 段目の VLAN tag にあるユーザ優先度が対象となります。次の図に VLAN tag が複数あるフレームの例を示します。

1. フィルタ

(i) VLAN Tag 1段のフォーマット

MAC-DA	MAC-SA	1段目の VLAN Tag	Ether Type	Data	FCS
--------	--------	------------------	---------------	------	-----

(ii) VLAN Tag 2段のフォーマット

MAC-DA	MAC-SA	1段目の VLAN Tag	2段目の VLAN Tag	Ether Type	Data	FCS
--------	--------	------------------	------------------	---------------	------	-----

注※3

ToS フィールドの指定についての補足

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。

Bit0 Bit1 Bit2 Bit3 Bit4 Bit5 Bit6 Bit7
Precedence ToS -

DSCP : ToS フィールドの上位 6 ビットの値です。

Bit0 Bit1 Bit2 Bit3 Bit4 Bit5 Bit6 Bit7
DSCP -

注※4

ack/fin/psh/rst/syn/urg フラグが 1 のパケットを検出します。

注※5

TCP/UDP ポート番号検出パターンを最大 16 パターンまで使用できます。TCP/UDP ポート番号検出パターンの使用例については、マニュアル「コンフィグレーションガイド Vol.1 3.2 収容条件 (7) フィルタ・QoS」を参照してください。

(2) 送信側インターフェースのフロー検出条件

送信側インターフェースのフロー検出条件は、送信側フロー検出モードによって異なります。送信側フロー検出モードごとの指定可能なフロー検出条件を次の表に示します。

表 1-5 送信側インターフェースで指定可能なフロー検出条件

種別	設定項目	openflow-1-out	openflow-2-out
		イーサネット	イーサネット
MAC 条件	コンフィグレーション	VLAN ID ※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	○	—
	ユーザ優先度※2	○	—

種別	設定項目	openflow-1-out	openflow-2-out
		イーサネット	イーサネット
IPv4 条件	コンフィグレーション	VLAN ID ※1	○ ○
	MAC ヘッダ	ユーザ優先度※2	○ ○
	IPv4 ヘッダ※3	上位プロトコル	○ ○
		送信元 IP アドレス	○ ○
		宛先 IP アドレス	○ ○
		ToS	○ ○
		DSCP	○ ○
		Precedence	○ ○
	IPv4-TCP ヘッダ	送信元ポート番号	单一指定 (eq) ○ ○
			範囲指定 (range) — —
		宛先ポート番号	单一指定 (eq) ○ ○
			範囲指定 (range) — —
	IPv4-UDP ヘッダ	送信元ポート番号	单一指定 (eq) ○ ○
			範囲指定 (range) — —
		宛先ポート番号	单一指定 (eq) ○ ○
			範囲指定 (range) — —
	IPv4-ICMP ヘッダ	ICMP タイプ値	○ ○
		ICMP コード値	○ ○
IPv6 条件	コンフィグレーション	VLAN ID	— —
	MAC ヘッダ	ユーザ優先度	— —
	IPv6 ヘッダ	上位プロトコル	— —
		送信元 IP アドレス	— —
		宛先 IP アドレス	— —
		トラフィッククラス	— —
		DSCP	— —
	IPv6-TCP ヘッダ	送信元ポート番号	单一指定 (eq) — —
			範囲指定 (range) — —
		宛先ポート番号	单一指定 (eq) — —
			範囲指定 (range) — —
		TCP 制御フラグ※4	— —
	IPv6-UDP ヘッダ	送信元ポート番号	单一指定 (eq) — —
			範囲指定 (range) — —
		宛先ポート番号	单一指定 (eq) — —
			範囲指定 (range) — —
	IPv6-ICMP ヘッダ	ICMP タイプ値	— —
		ICMP コード値	— —

1. フィルタ

(凡例) ○ : 指定できる - : 指定できない

注※ 1

本装置のフロー検出で検出できる VLAN ID は、VLAN コンフィグレーションで入力した VLAN に対して付与する値です。送信フレームの属する VLAN ID を検出します。

次に示す場合、VLAN ID を指定できません。

- tag 変換を設定したイーサネットインターフェースに指定する場合
- VLAN トンネリングを設定したイーサネットインターフェースに指定する場合

注※ 2

送信フレームの VLAN tag にあるユーザ優先度を検出します。VLAN tag が複数あるフレームに対してユーザ優先度を検出する場合、MAC アドレス側から 1 段目の VLAN tag にあるユーザ優先度が対象となります。次の図に VLAN tag が複数あるフレームの例を示します。

(i) VLAN Tag 1段のフォーマット

MAC-DA	MAC-SA	1段目の VLAN Tag	Ether Type	Data	FCS
--------	--------	------------------	---------------	------	-----

(ii) VLAN Tag 2段のフォーマット

MAC-DA	MAC-SA	1段目の VLAN Tag	2段目の VLAN Tag	Ether Type	Data	FCS
--------	--------	------------------	------------------	---------------	------	-----

送信側インターフェースでは、VLAN tag なしのフレームについてもユーザ優先度を検出します。ユーザ優先度検出の詳細を次の表に示します。

表 1-6 送信側インターフェースでのユーザ優先度検出

フレーム送信ポート	送信フレーム	ユーザ優先度のフロー検出動作
VLAN トンネリング設定なし	-	受信側でマーカー機能を使用した場合は、マーカー後のユーザ優先度を検出します。 受信側でマーカー機能を使用していない場合で、かつ受信フレームが VLAN tag なしのときは、ユーザ優先度 3 として検出します。 受信側でマーカー機能を使用していない場合で、かつ受信フレームが VLAN tag ありのときは、受信時のユーザ優先度を検出します。ただし、次に示すフレームは優先度 3 として検出します。 • VLAN トンネリングを設定したポートで受信したフレーム
VLAN トンネリング設定あり	VLAN tag なし	同上
	VLAN tag あり	送信フレームのユーザ優先度を検出します。ただし、フロー検出条件に MAC を指定した場合、以下の通りとなります • VLAN トンネリングを設定したポートで受信した場合、優先度 3 として検出します • VLAN トンネリングを設定していないポートで受信した場合、受信フレームのユーザ優先度で検出します

(凡例) - : VLAN tag の有無に影響しない

注※ 3

ToS フィールドの指定についての補足

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。

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
Precedence		ToS	-				

DSCP : ToS フィールドの上位 6 ビットの値です。

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
DSCP	-						

受信側インターフェースでマーカー機能の DSCP 書き換えを使用した場合、送信側インターフェースでの ToS, DSCP および Precedence の検出は、DSCP 書き換え後のフレームに対して実施します。

注※4

ack/fin/psh/rst/syn/urg フラグが 1 のパケットを検出します。

1.1.6 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可能なフレーム種別が異なります。フロー検出条件と対応するアクセスリスト、および検出可能なフレーム種別の関係を次の表に示します。

表 1-7 フロー検出条件と対応するアクセスリスト、検出可能なフレーム種別の関係

設定可能な フロー検出 条件	アクセスリスト	対応する受信側 フロー検出モード	対応する送信側 フロー検出モード	検出可能なフレーム種別		
				非 IP	IPv4	IPv6
MAC 条件	mac access-list	openflow-2, openflow-3	openflow-1-out	○	○	○
IPv4 条件	access-list ip access-list	openflow-2, openflow-3	openflow-1-out, openflow-2-out	—	○	—
IPv6 条件	ipv6 access-list	なし	なし	—	—	○

(凡例) ○：検出できる —：検出できない

フィルタエントリの適用順序は、アクセスリストのパラメータであるシーケンス番号によって決定します。また、アクセスリストごとに、フィルタエントリの検索は独立して実施します。そのため、フレームが複数のフィルタエントリに一致することがあります。複数のフィルタエントリに一致した場合、実際に動作するのは単一のフィルタエントリです。

(1) イーサネットインターフェースと VLAN インタフェース同時に一致した場合の動作

(a) 受信側フロー検出モードの場合

この条件に該当する受信側フロー検出モードはありません。

(b) 送信側フロー検出モードの場合

この条件に該当する送信側フロー検出モードはありません。

(2) mac access-list と access-list/ip access-list に同時に一致した場合の動作

(a) 受信側フロー検出モードの場合

同一インターフェースに対して mac access-list と access-list/ip access-list をフロー検出条件としたフィルタエントリを設定して、該当するインターフェースからの受信フレームに対してフィルタを実施すると、複数のフィルタエントリに一致する場合があります。この場合、廃棄動作を指定したフィルタエントリ（暗黙の廃棄のエントリを含む）が優先となります。mac access-list、および access-list/ip access-list 共に中継動作を指定したフィルタエントリに一致する場合は mac access-list のフィルタエントリを優先します。複数のフィルタエントリに一致した場合の動作を次の表に示します。

1. フィルタ

表 1-8 複数のフィルタエントリに一致した場合の動作

複数フィルタエントリー一致となる組み合わせ		有効になるフィルタエントリ	
mac access-list	access-list ip access-list	インターフェース	動作
中継	中継	mac access-list	中継
中継	廃棄	access-list ip access-list	廃棄
廃棄	中継	mac access-list	廃棄
廃棄	廃棄	mac access-list	廃棄

この条件に該当する受信側フロー検出モードは、openflow-2,openflow-3 です。

(b) 送信側フロー検出モードの場合

同一インターフェースに対して mac access-list と access-list/ip access-list をフロー検出条件としたフィルタエントリを設定しても、送信フレームが複数のフィルタエントリに一致することはありません。この場合、常に mac access-list のフィルタエントリ（暗黙の廃棄のエントリを含む）に一致し、一致したフィルタエントリの指定動作が実施されます。

この条件に該当する送信側フロー検出モードは openflow-1-out です。

(3) 廃棄できないフレーム

受信側インターフェースで次に示すフレームは、フィルタの有無に関わらず、フレームを廃棄できません。

本装置が受信するフレームのうち次のフレーム

- MAC アドレス学習の移動検出とみなしたフレーム

本装置がレイヤ 3 中継し、本装置が受信するフレームのうち次のパケット / フレーム

- MTU を超える IPv4, IPv6 パケット
- TTL が 1 のフレーム
- ホップリミットが 1 のフレーム
- IP オプション付きのフレーム
- IPv6 拡張ヘッダ付きのフレーム
- 宛先不明の IPv4, IPv6 パケット

1.1.7 暗黙の廃棄

フィルタを設定したインターフェースでは、フロー検出条件に一致しないフレームは廃棄します。

暗黙の廃棄のフィルタエントリは、アクセリストを生成すると自動生成されます。アクセリストを一つも設定しない場合、すべてのフレームを中継します。

1.1.8 フィルタ使用時の注意事項

(1) 複数フィルタエントリー一致時の動作

フレームが複数のフィルタエントリに一致した場合、一致したフィルタエントリの統計情報が採られます。

(2) VLAN tag 付きフレームに対するフィルタ

2段のVLAN tag があるフレームに対して、イーサネットタイプ・IPヘッダ・TCP/UDPヘッダ・ICMPヘッダをフロー検出条件としたフィルタを受信側で実施するためには、次の条件のいずれかを満たす必要があります。

- 本装置でVLAN トンネリング機能が動作していない
- 本装置でVLAN トンネリング機能が動作していて、フレームを受信したポートがトランクポートである

VLAN トンネリングポートから VLAN-Tag が2段で送信されるフレームに対して、MAC 条件のイーサネットタイプまたはIPv4 条件をフロー検出条件としたフィルタを送信側で実施できません。

(3) IPv4 フラグメントパケットに対するフィルタ

IPv4 フラグメントパケットに対して TCP/UDP ヘッダ・ICMP ヘッダをフロー検出条件としたフィルタを行った場合、2番目以降のフラグメントパケットは TCP/UDP ヘッダ・ICMP ヘッダがパケット内にないため、検出できません。フラグメントパケットを含めたフィルタを実施する場合は、フロー検出条件に MAC ヘッダ、IP ヘッダを指定してください。

(4) フィルタエントリ適用時の動作

本装置では、インターフェースに対してフィルタを適用する※と、暗黙の廃棄エントリから適用します。そのため、ユーザが設定したフィルタエントリが適用されるまでの間、暗黙の廃棄に一致するフレームが一時的に廃棄されます。また、暗黙の廃棄エントリの統計情報が採られます。

注※

- 1エントリ以上を設定したアクセリストをアクセスグループコマンドによりインターフェースに適用する場合
- アクセリストをアクセスグループコマンドにより適用し、ひとつ目のエントリを追加する場合

(5) フィルタエントリ変更時の動作

本装置では、インター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が検出されなくなります。そのため、一時的には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されます。

(6) ほかの機能との同時動作

以下の場合フレームは廃棄しますが、受信側のインターフェースに対してフィルタエントリを設定し一致した場合、一致したフィルタエントリの統計情報が採られます。

- VLAN のポートのデータ転送状態が Blocking (データ転送停止中) の状態で、該当ポートからフレームを受信した場合
- ポート間中継遮断機能で指定したポートからフレームを受信した場合
- ネイティブ VLAN をトランクポートで送受信する VLAN に設定しないで、VLAN tag なしフレームを受信した場合
- トランクポートで送受信する VLAN に設定していない VLAN tag 付きフレームを受信した場合

1.2 コンフィグレーション

1.2.1 コンフィグレーションコマンド一覧

フィルタ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 1-9 コンフィグレーションコマンド一覧

コマンド名	説明
access-list	IPv4 フィルタとして動作するアクセリストを設定します。
deny	IPv4 フィルタでのアクセスを破棄する条件を指定します。
flow detection mode	フィルタ・QoS 制御の受信側フロー検出モードを設定します。
flow detection out mode	フィルタの送信側フロー検出モードを設定します。
ip access-group	イーサネットインターフェースまたは VLAN インタフェースに対して IPv4 フィルタを適用し、IPv4 フィルタ機能を有効にします。
ip access-list extended	IPv4 パケットフィルタとして動作するアクセ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	イーサネットインターフェースに対して IPv6 フィルタを適用し、IPv6 フィルタ機能を有効にします。
mac access-group	イーサネットインターフェースまたは VLAN インタフェースに対して MAC フィルタを適用し、MAC フィルタ機能を有効にします。
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。
mac access-list extended	MAC フィルタとして動作するアクセリストを設定します。
permit	IPv4 フィルタでのアクセスを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。

1.2.2 受信側フロー検出モードの設定

フィルタの受信側フロー検出モードを指定する例を次に示します。

[設定のポイント]

受信側フロー検出モードは、ハードウェアの基本的な動作条件を決定するため、最初に設定します。

[コマンドによる設定]

1. (config)# flow detection mode openflow-2

受信側フロー検出モード openflow-2 を有効にします。

1.2.3 送信側フロー検出モードの設定

フィルタの送信側フロー検出モードを指定する例を次に示します。

[設定のポイント]

送信側フロー検出モードは、ハードウェアの基本的な動作条件を決定するため、最初に設定します。

[コマンドによる設定]

1. **(config)# flow detection out mode openflow-1-out**

送信側フロー検出モード openflow-1-out を有効にします。

1.2.4 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、フレームを中継・廃棄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行い、フィルタエントリに一致したフレームを廃棄・中継します。

[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ことによって、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モードに戻ります。

5. **(config)# interface gigabitethernet 0/1**

ポート 0/1 のインターフェースモードに移行します。

6. **(config-if)# mac access-group IPX_DENY in**

受信側に MAC フィルタを有効にします。

1.2.5 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 アドレスをフロー検出条件とし、フレームを中継・廃棄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 アドレスによってフロー検出を行い、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ことによって、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 192.168.0.0 0.0.0.255**
送信元 IP アドレス 192.168.0.0/24 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-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モードに戻ります。
4. **(config)# interface vlan 10**
VLAN10 のインターフェースモードに移行します。
5. **(config-if)# ip access-group FLOOR_A_PERMIT in**
受信側に IPv4 フィルタを有効にします。

(2) IPv4 パケットをフロー検出条件とする設定

IPv4 telnet パケットをフロー検出条件とし、フレームを中継・廃棄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・TCP/UDP ヘッダによってフロー検出を行い、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 TELNET_DENY**
ip access-list (TELNET_DENY) を作成します。本リストを作成することによって、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 telnet**
telnet 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。
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モードに戻ります。

5. (config)# interface vlan 10

VLAN10 のインターフェースモードに移行します。

6. (config-if)# ip access-group TELNET_DENY in

受信側に IPv4 フィルタを有効にします。

(3) TCP/UDP ポート番号の範囲をフロー検出条件とする設定

UDP ポート番号の範囲をフロー検出条件とし、フレームを中継・廃棄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 UDP ヘッダの宛先ポート番号の範囲によってフロー検出を行い、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 PORT_RANGE_DENY**

ip access-list (PORT_RANGE_DENY) を作成します。本リストを作成することによって、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 udp any any range 10 20

UDP ヘッダの宛先ポート番号が 10 ~ 20 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。

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モードに戻ります。

5. (config)# interface vlan 10

VLAN10 のインターフェースモードに移行します。

6. (config-if)# ip access-group PORT_RANGE_DENY in

受信側に IPv4 フィルタを有効にします。

1.2.6 複数インターフェースフィルタの設定

複数のイーサネットインターフェースにフィルタを指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ー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)# access-list 10 permit host 192.168.0.1**

ホスト 192.168.0.1 からだけフレームを中継する IPv4 アドレスフィルタを設定します。

2. **(config)# interface range gigabitethernet 0/1-4**

ポート 0/1-4 のインターフェースモードに移行します。

3. **(config-if-range)# ip access-group 10 in**

受信側に IPv4 フィルタを有効にします。

1.3 オペレーション

show access-filter コマンドによって、設定した内容が反映されているかどうかを確認します。

1.3.1 運用コマンド一覧

フィルタで使用する運用コマンド一覧を次の表に示します。

表 1-10 運用コマンド一覧

コマンド名	説明
show access-filter	アクセスグループコマンド(mac access-group, ip access-group, ipv6 traffic-filter)で設定したアクセリスト(mac access-list, access-list, ip access-list, ipv6 access-list)の統計情報を表示します。
clear access-filter	アクセスグループコマンド(mac access-group, ip access-group, ipv6 traffic-filter)で設定したアクセリスト(mac access-list, access-list, ip access-list, ipv6 access-list)の統計情報をクリアします。

1.3.2 フィルタの確認

(1) イーサネットインター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ーフェースにフィルタを設定した場合の動作確認の方法を次の図に示します。

図 1-3 イーサネットインターフェースにフィルタを設定した場合の動作確認

```
> show access-filter 0/1 IPX_DENY
Date 2010/12/01 15:30:00 UTC
Using Port:0/1 in
Extended MAC access-list: IPX_DENY
    remark "deny only ipx"
    deny any any ipx
        matched packets      : 74699826
    permit any any
        matched packets      : 264176
    implicitly denied packets: 0
```

指定したポートのフィルタに「Extended MAC access-list」が表示されることを確認します。

(2) 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の方法を次の図に示します。

図 1-4 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 FLOOR_A_PERMIT
Date 2010/12/01 15:30:00 UTC
Using Interface:vlan 10 in
Standard IP access-list: FLOOR_A_PERMIT
    remark "permit only Floor-A"
    permit 192.168.0.0 0.0.0.255 any
        matched packets      : 74699826
    implicitly denied packets: 2698
```

指定した VLAN のフィルタに「Standard IP access-list」が表示されることを確認します。

2 QoS 制御の概要

QoS 制御は、帯域監視・マーカー・優先度決定・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。

-
- 2.1 QoS 制御構造
 - 2.2 共通処理解説
 - 2.3 QoS 制御共通のコンフィグレーション
 - 2.4 QoS 制御共通のオペレーション
-

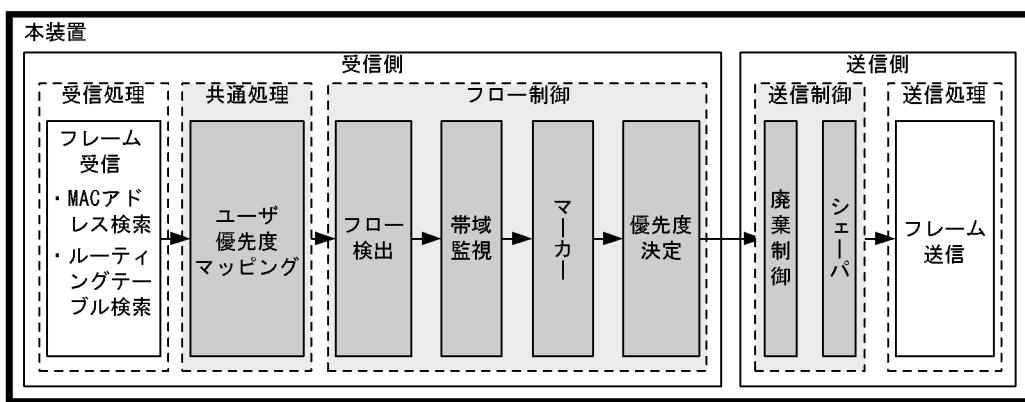
2.1 QoS 制御構造

ネットワークを利用したサービスの多様化に伴い、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 2-1 本装置の QoS 制御の機能ブロック



(凡例) : この節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 2-1 QoS 制御の各機能ブロックの概要

機能部位		機能概要
受信処理部	フレーム受信	フレームを受信し、MAC アドレステーブル検索やルーティングテーブル検索を実施します。
共通処理部	ユーザ優先度マッピング	受信フレームの VLAN tag のユーザ優先度に従い、優先度を決定します。
フロー制御部	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、ICMP ヘッダなどの条件に一致するフローを検出します。
	帯域監視	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	IP ヘッダ内の DSCP や VLAN tag のユーザ優先度を書き換える機能です。
	優先度決定	フローに対する優先度や、廃棄されやすさを示すキューイング優先度を決定します。
送信制御部	廃棄制御	パケット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。
	シェーバ	各キューからのフレームの出力順序および出力帯域を制御します。
送信処理部	フレーム送信	シェーバによって制御されたフレームを送信します。

本装置の QoS 制御は、受信フレームの優先度をユーザ優先度マッピング、またはフロー制御によって決定します。ユーザ優先度マッピングは、受信フレームの VLAN tag 内にあるユーザ優先度に基づいて優先度を決定します。ユーザ優先度ではなく、MAC アドレスや IP アドレスなどの特定の条件に一致するフレームに対して優先度を決定したい場合は、フロー制御を使用します。

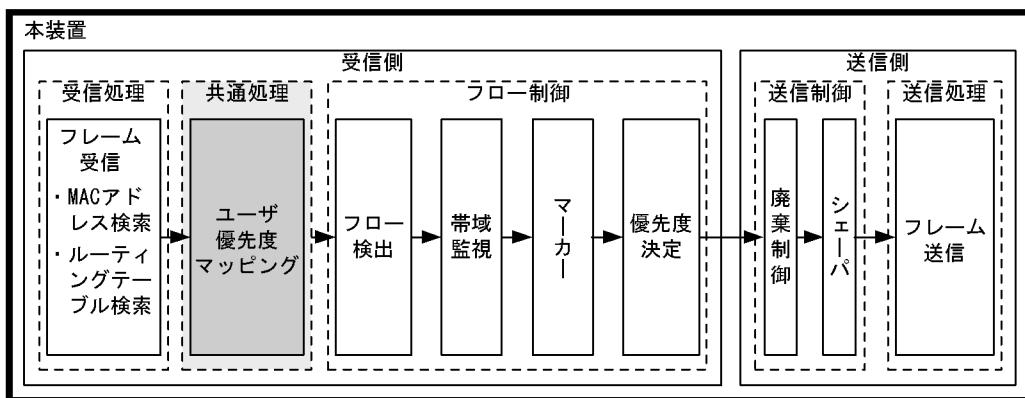
フロー制御による優先度の決定は、ユーザ優先度マッピングよりも優先されます。また、フロー制御は、優先度決定のほかに帯域監視やマーカーも実施することができます。フロー検出で検出したフローに対して、帯域監視、マーカー、優先度決定の各機能は同時に動作することができます。

送信制御は、ユーザ優先度マッピングやフロー制御によって決定した優先度に基づいて、廃棄制御やシェーパを実施します。

2.2 共通処理解説

この節で説明するユーザ優先度マッピングの位置づけを次の図に示します。

図 2-2 ユーザ優先度マッピングの位置づけ



(凡例) : この節で説明するブロック

2.2.1 ユーザ優先度マッピング

ユーザ優先度マッピングは、受信フレームの VLAN tag 内にあるユーザ優先度に基づいて優先度を決定する機能です。本装置では、常にユーザ優先度マッピングが動作し、すべての受信フレームに対して優先度を決定します。

優先度の値には、装置内の優先度を表す CoS 値を用います。受信フレームのユーザ優先度の値から CoS 値にマッピングし、CoS 値によって送信キューを決定します。CoS 値と送信キューの対応については、「3.10.2 CoS マッピング機能」を参照してください。

ユーザ優先度は、VLAN tag ヘッダ内タグ情報 (Tag Control) の上位 3 ビットを示します。なお、VLAN tag がないフレームは、常に CoS 値 3 を使用します。

フロー制御による優先度決定が動作する場合、ユーザ優先度マッピングよりも優先して動作します。

表 2-2 ユーザ優先度と CoS 値のマッピング

フレームの種類		マッピングされる CoS 値
VLAN tag の有無	ユーザ優先度値	
VLAN tag なし	—	3
VLAN tag あり※	0	0
	1	1
	2	2
	3	3
	4	4
	5	5
	6	6
	7	7

(凡例) - : 該当なし

注※ VLAN トンネリングを設定したポートで受信したフレームは、受信時のユーザ優先度値に関係なく、常に CoS 値 3 にマッピングされます。

2.2.2 ユーザ優先度マッピングの注意事項

(1) ユーザ優先度マッピングの対象

本装置がレイヤ 3 中継をする場合、ユーザ優先度マッピングは、2 段までの VLAN tag に対して有効です。3 段以上の VLAN tag が付与されている場合は、受信したフレームを廃棄します。ユーザ優先度マッピングが有効となる VLAN tag を次の図に示します。

図 2-3 ユーザ優先度マッピング対象部位

(i) VLAN Tag 1段のフォーマット

MAC-DA	MAC-SA	1段目の VLAN Tag	Ether Type	Data	FCS
--------	--------	------------------	---------------	------	-----

(ii) VLAN Tag 2段のフォーマット

MAC-DA	MAC-SA	1段目の VLAN Tag	2段目の VLAN Tag	Ether Type	Data	FCS
--------	--------	------------------	------------------	---------------	------	-----

(凡例)  : ユーザ優先度マッピング処理対象部位

2.3 QoS 制御共通のコンフィグレーション

2.3.1 コンフィグレーションコマンド一覧

QoS 制御共通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
flow detection mode	フィルタ・QoS 制御の受信側フロー検出モードを設定します。
ip qos-flow-group	イーサネットインターフェースまたは VLAN に対して、IPv4 QoS フローリストを適用し、IPv4 QoS 制御を有効にします。
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	イーサネットインターフェースに対して、IPv6 QoS フローリストを適用し、IPv6 QoS 制御を有効にします。
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	イーサネットインターフェースまたは VLAN に対して、MAC QoS フローリストを適用し、MAC QoS 制御を有効にします。
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 フローリストでのフロー検出条件および動作指定を設定します。
qos-queue-group	イーサネットインターフェースに対して、QoS キューリスト情報を適用し、レガシーシェーバを有効にします。
qos-queue-list	QoS キューリスト情報にスケジューリングモードを設定します。
remark	QoS の補足説明を記述します。
traffic-shaper rate	イーサネットインターフェースにポート帯域制御を設定します。

2.4 QoS 制御共通のオペレーション

2.4.1 運用コマンド一覧

QoS 制御共通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 qos-flow	QoS フローグループコマンド (mac qos-flow-group, ip qos-flow-group, ipv6 qos-flow-group) で設定した QoS フローリスト (mac qos-flow-list, ip qos-flow-list, ipv6 qos-flow-list) の統計情報を表示します。
clear qos-flow	QoS フローグループコマンド (mac qos-flow-group, ip qos-flow-group, ipv6 qos-flow-group) で設定した QoS フローリスト (mac qos-flow-list, ip qos-flow-list, ipv6 qos-flow-list) の統計情報をクリアします。
show qos queueing	イーサネットインターフェースの送信キューの統計情報を表示します。
clear qos queueing	イーサネットインターフェースの送信キューの統計情報をクリアします。

3

フロー制御

この章では本装置のフロー制御（フロー検出、帯域監視、マーカー、優先度決定）について説明します。

-
- 3.1 フロー検出解説
 - 3.2 フロー検出コンフィグレーション
 - 3.3 フロー検出のオペレーション
 - 3.4 帯域監視解説
 - 3.5 帯域監視のコンフィグレーション
 - 3.6 帯域監視のオペレーション
 - 3.7 マーカー解説
 - 3.8 マーカーのコンフィグレーション
 - 3.9 マーカーのオペレーション
 - 3.10 優先度決定の解説
 - 3.11 優先度決定コンフィグレーション
 - 3.12 優先度のオペレーション
 - 3.13 複数の QoS エントリに一致した場合の動作
-

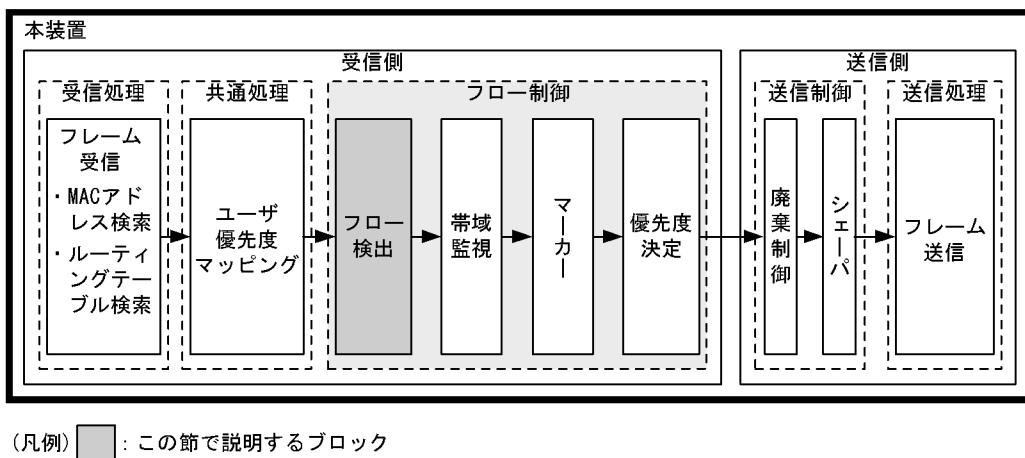
3.1 フロー検出解説

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、ICMP 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、「3.1.3 QoS フローリスト」を参照してください。

本装置では、受信側イーサネットインターフェース・VLAN インタフェースで、イーサネット V2 形式および IEEE802.3 の SNAP/RFC1042 形式フレームのフロー検出ができます。設定可能なインターフェースは、受信側フロー検出モードによって変わります。なお、本装置宛ての受信フレームもフロー検出対象です。

この節で説明するフロー検出の位置づけを次の図に示します。

図 3-1 フロー検出の位置づけ



3.1.1 受信側フロー検出モード

本装置では、ネットワーク構成や運用形態を想定して受信側フロー検出モードを用意しています。受信側フロー検出モードは、受信側インターフェースに対するフィルタ・QoS エントリの配分パターンを決めるモードです。使い方に合わせて選択してください。また、受信側フロー検出モードを選択する際の目安について次に示します。検出条件の詳細は「3.1.2 フロー検出条件」を参照してください。

- ・ 検出対象インターフェースにイーサネットを指定したい場合は、openflow-2 を使用してください。
- ・ 検出対象インターフェースに VLAN を指定したい場合は、openflow-3 を使用してください。

受信側フロー検出モードは `flow detection mode` コマンドで指定します。なお、選択した受信側フロー検出モードはフィルタ・QoS で共通です。受信側フロー検出モードを変更する場合、受信側および送信側インターフェースに設定された次のコマンドをすべて削除する必要があります。

- `mac access-group`
- `ip access-group`
- `mac qos-flow-group`
- `ip qos-flow-group`

受信側フロー検出モードを指定しない場合、`openflow-1` がデフォルトのモードとして設定されます。

受信側フロー検出モードとフロー動作の関係を次の表に示します。

表 3-1 受信側フロー検出モードとフロー動作の関係

受信側 フロー検出 モード	運用目的	フロー動作	検出対象 インターフェース
openflow-1	フロー制御を使用しないモードです。	—	—
openflow-2	IP パケットやそれ以外のフレームのフロー制御を行いたい場合に使用します。また、IPv4 パケットに特化したフロー制御を行いたい場合にも使用できます。	MAC アドレス、イーサネットタイプなどの MAC ヘッダでフレームを検出します。 IPv4 パケットは、IP ヘッダ、TCP/UDP ヘッダ、ICMP ヘッダでフレームを検出します。	イーサネット
openflow-3	IP パケットやそれ以外のフレームのフロー制御を行いたい場合に使用します。また、IPv4 パケットに特化したフロー制御を行いたい場合にも使用できます。	MAC アドレス、イーサネットタイプなどの MAC ヘッダでフレームを検出します。 IPv4 パケットは、IP ヘッダ、TCP/UDP ヘッダ、ICMP ヘッダでフレームを検出します。	VLAN

3.1.2 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。受信側インターフェースでのフロー検出条件を次に示します。

(1) 受信側インターフェースのフロー検出条件

受信側インターフェースのフロー検出条件は、受信側フロー検出モードによって異なります。受信側フロー検出モードごとの指定可能なフロー検出条件を次の表に示します。

表 3-2 受信側インターフェースで指定可能なフロー検出条件

種別	設定項目	openflow-2	openflow-3
		イーサネット	VLAN
MAC 条件	コンフィグレーション	VLAN ID ^{※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	○ ○	○ ○
	ユーザ優先度 ^{※2}	○ ○	○ ○

3. フロー制御

種別	設定項目	openflow-2	openflow-3
		イーサネット	VLAN
IPv4 条件	コンフィグレーション	VLAN ID ^{※1}	○
	MAC ヘッダ	ユーザ優先度 ^{※2}	○
	IPv4 ヘッダ ^{※3}	上位プロトコル	○
		送信元 IP アドレス	○
		宛先 IP アドレス	○
		ToS	○
		DSCP	○
		Precedence	○
	IPv4-TCP ヘッダ	送信元ポート番号	单一指定 (eq)
			範囲指定 (range)
		宛先ポート番号	单一指定 (eq)
			範囲指定 (range)
	TCP 制御フラグ ^{※4}		—
IPv4-UDP ヘッダ	送信元ポート番号	单一指定 (eq)	○
		範囲指定 (range)	○※5
	宛先ポート番号	单一指定 (eq)	○
		範囲指定 (range)	○※5
	IPv4-ICMP ヘッダ	ICMP タイプ値	○
		ICMP コード値	○

種別	設定項目	openflow-2	openflow-3
		イーサネット	VLAN
IPv6 条件	コンフィグレーション	VLAN ID ※1	—
	MAC ヘッダ	ユーザ優先度※2	—
	IPv6 ヘッダ※6	上位プロトコル	—
		送信元 IP アドレス	—
		宛先 IP アドレス	—
		トライフィッククラス	—
		DSCP	—
	IPv6-TCP ヘッダ	送信元ポート番号	单一指定(eq) 範囲指定(range)
		宛先ポート番号	单一指定(eq) 範囲指定(range)
		TCP 制御フラグ※4	—
	IPv6-UDP ヘッダ	送信元ポート番号	单一指定(eq) 範囲指定(range)
		宛先ポート番号	单一指定(eq) 範囲指定(range)
	IPv6-ICMP ヘッダ	ICMP タイプ値	—
		ICMP コード値	—

(凡例) ○ : 指定できる — : 指定できない

注※1

本装置のフロー検出で検出できる VLAN ID は、VLAN コンフィグレーションで入力した VLAN に対して付与する値です。受信フレームの属する VLAN ID を検出します。

注※2

次に示すフレームについてはユーザ優先度を検出できません。常に、ユーザ優先度 3 として検出します。

- ・ VLAN tag なしのフレーム
- ・ VLAN トンネリングを設定したポートで受信したフレーム

VLAN tag が複数あるフレームに対してユーザ優先度を検出する場合、MAC アドレス側から 1 段目の VLAN tag にあるユーザ優先度が対象となります。次の図に VLAN tag が複数あるフレームの例を示します。

3. フロー制御

(i) VLAN Tag 1段のフォーマット

MAC-DA	MAC-SA	1段目の VLAN Tag	Ether Type	Data	FCS
--------	--------	------------------	---------------	------	-----

(ii) VLAN Tag 2段のフォーマット

MAC-DA	MAC-SA	1段目の VLAN Tag	2段目の VLAN Tag	Ether Type	Data	FCS
--------	--------	------------------	------------------	---------------	------	-----

注※ 3

ToS フィールドの指定についての補足

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。

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
Precedence			ToS				-

DSCP : ToS フィールドの上位 6 ビットの値です。

Bit0	Bit1	Bit2	Bit3	Bit4	Bit5	Bit6	Bit7
DSCP							-

注※ 4

IPv4 条件では、 ack/fin/psh/rst/syn/urg フラグが 1 のパケットを検出します。

注※ 5

TCP/UDP ポート番号検出パターンを最大 16 パターンまで使用できます。TCP/UDP ポート番号検出パターンの使用例については、マニュアル「コンフィグレーションガイド Vol.1 3.2 収容条件（8）フィルタ・QoS」を参照してください。

3.1.3 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可能なフレーム種別が異なります。フロー検出条件と対応する QoS フローリスト、および検出可能なフレーム種別の関係を次の表に示します。

表 3-3 フロー検出条件と対応する QoS フローリスト、検出可能なフレーム種別の関係

フロー検出条件	対応する QoS フローリスト	対応する受信側 フロー検出モード	検出可能なフレーム種別		
			非 IP	IPv4	IPv6
MAC 条件	mac qos-flow-list	openflow-2, openflow-3	○	○	○
IPv4 条件	ip qos-flow-list	openflow-2, openflow-3	—	○	—
IPv6 条件	ipv6 qos-flow-list	なし	—	—	○

(凡例) ○ : 検出できる — : 検出できない

QoS フローリストのインター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。適用順序は、QoS フローリストのパラメータであるシーケンス番号によって決定します。また、QoS フローリストごとに、QoS エントリの検索は独立して実施します。そのため、フレームが複数の QoS エントリに一致することがあります。複数の QoS エントリに一致した場合の動作の詳細は、「3.13 複数の QoS エントリに一致した場合の動作」を参照してください。

3.1.4 フロー検出使用時の注意事項

(1) 複数 QoS エントリー一致時の動作

フレームが複数の QoS エントリに一致した場合、一致した QoS エントリの統計情報が採られます。

(2) VLAN tag 付きフレームに対する QoS フロー検出

2 段の VLAN tag があるフレームに対して、イーサネットタイプ・IP ヘッダ・TCP/UDP ヘッダ・ICMP ヘッダをフロー検出条件とした QoS フロー検出を受信側で実施するためには、次の条件のいずれかを満たす必要があります。

- 本装置で VLAN トンネリング機能が動作していない
- 本装置で VLAN トンネリング機能が動作していて、フレームを受信したポートがトランクポートである

該当するフレームを QoS フロー検出する場合、フロー検出条件に VLAN ID または MAC アドレスを指定してください。

(3) IPv4 フラグメントパケットに対する QoS フロー検出

IPv4 フラグメントパケットに対して TCP/UDP ヘッダ・ICMP ヘッダをフロー検出条件とした QoS フロー検出を行った場合、2 番目以降のフラグメントパケットは TCP/UDP ヘッダ・ICMP ヘッダがフレーム内にないため検出できません。フラグメントパケットを含めた QoS フロー検出を実施する場合は、フロー検出条件に MAC ヘッダ、IP ヘッダを指定してください。

(4) QoS エントリ変更時の動作

本装置では、インターフェースに適用済みの QoS 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が検出されなくなります。そのため、一時的にほかの QoS エントリで検出される場合があります。

(5) ほかの機能との同時動作

以下の場合フレームは廃棄しますが、受信側のインターフェースに対して QoS エントリを設定し一致した場合、一致した QoS エントリの統計情報が採られます。

- VLAN のポートのデータ転送状態が Blocking (データ転送停止中) の状態で、該当ポートからフレームを受信した場合
- ポート間中継遮断機能で指定したポートからフレームを受信した場合
- ネイティブ VLAN をトランクポートで送受信する VLAN に設定しないで、VLAN tag なしフレームを受信した場合
- トランクポートで送受信する VLAN に設定していない VLAN tag 付きフレームを受信した場合
- 廃棄動作を指定したフィルタエントリ (暗黙の廃棄のエントリを含む) に一致するフレームを受信した場合

3.2 フロー検出コンフィグレーション

3.2.1 受信側フロー検出モードの設定

QoS 制御の受信側フロー検出モードを指定する例を示します。

[設定のポイント]

受信側フロー検出モードは、ハードウェアの基本的な動作条件を決定するため、最初に設定します。

[コマンドによる設定]

1. **(config)# flow detection mode openflow-2**

受信側フロー検出モード openflow-2 を有効にします。

3.2.2 複数インタフェースの QoS 制御の指定

複数のイーサネットインターフェースに QoS 制御を指定する例を示します。

[設定のポイント]

config-if-range モードで QoS 制御を有効に設定することで、複数のイーサネットインターフェースに QoS 制御を設定できます。

[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ことによって、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 192.168.100.10 action cos 6**

192.168.100.10 の IP アドレスを宛先とし、CoS 値 = 6 の 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モードに戻ります。

4. **(config)# interface range gigabitethernet 0/1-4**

ポート 0/1-4 のインターフェースモードに移行します。

5. **(config-if-range)# ip qos-flow-group QOS-LIST1 in**

受信側に IPv4 QoS フローリストを有効にします。

3.2.3 TCP/UDP ポート番号の範囲で QoS 制御する設定

UDP ポート番号の範囲をフロー検出条件とし、QoS 制御を設定する例を示します。

[設定のポイント]

フレーム受信時に UDP ヘッダの宛先ポート番号の範囲によってフロー検出を行い、QoS 制御を実施します。

[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ことによって、IPv4 QoS フローリストモードに移行します。

2. **(config-ip-qos)# qos udp any any range 10 20 action cos 6**

UDP ヘッダの宛先ポート番号の範囲 10 ~ 20 をフロー検出条件とし、CoS 値 = 6 の 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モードに戻ります。

4. **(config)# interface gigabitethernet 0/1**

ポート 0/1 のインターフェース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 フローリストを有効にします。

3.3 フロー検出のオペレーション

show qos-flow コマンドによって、設定した内容が反映されているかどうかを確認します。

3.3.1 IPv4 パケットをフロー検出条件とした QoS 制御の動作確認

IPv4 パケットをフロー検出条件とした QoS 制御の動作確認の方法を次の図に示します。

図 3-2 IPv4 パケットをフロー検出条件とした QoS 制御の動作確認

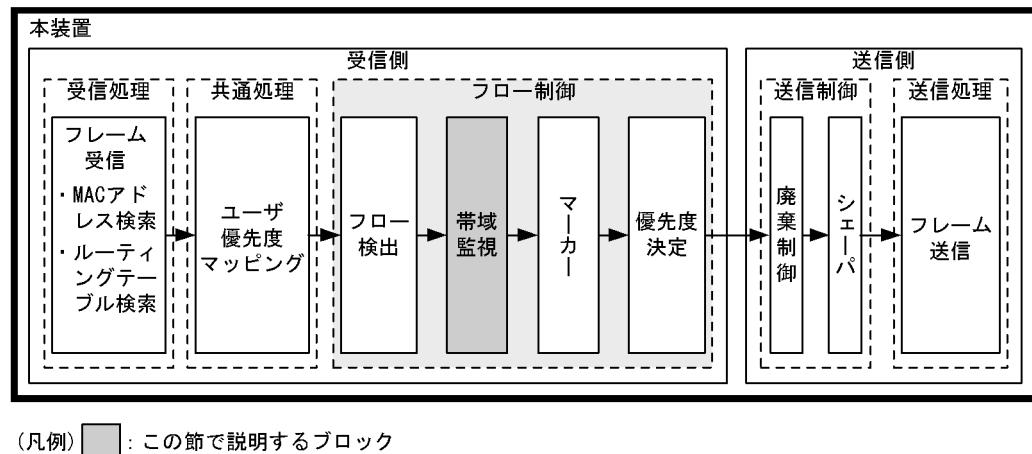
```
> show qos-flow 0/1
Date 2010/12/01 15:30:00 UTC
Using Port:0/1 in
IP qos-flow-list:QOS-LIST1
    ip any host 192.168.100.10 action replace-user-priority 6
        matched packets      : 74699826
```

指定したポートの QoS 制御に「IP qos-flow-list」が表示されることを確認します。

3.4 帯域監視解説

帯域監視は、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。この節で説明する帯域監視の位置づけを次の図に示します。

図 3-3 帯域監視の位置づけ



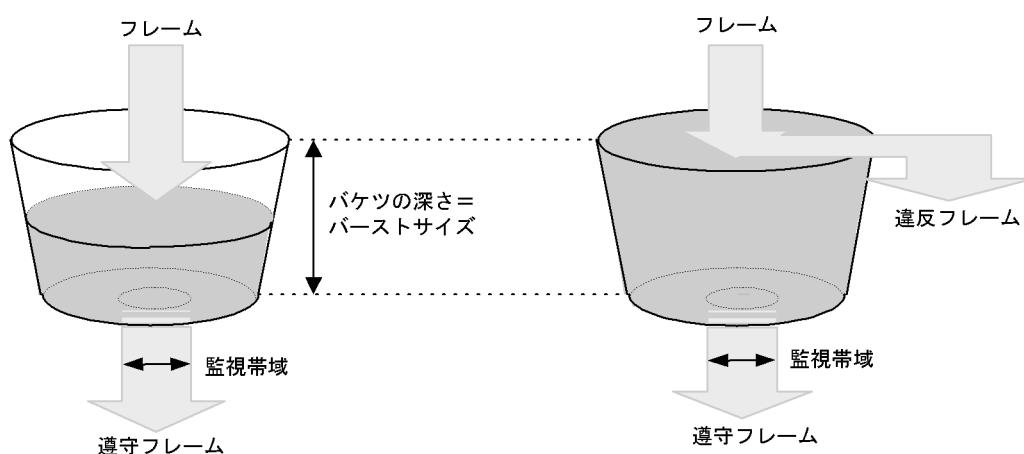
3.4.1 帯域監視

フロー検出で検出したフレームのフレーム長（MAC アドレスから FCS まで）を基に帯域を監視する機能です。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。

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 アルゴリズムを用いています。

Leaky Bucket アルゴリズムのモデルを次の図に示します。

図 3-4 Leaky Bucket アルゴリズムのモデル



3. フロー制御

バケツからは監視帯域分の水が流れ、フレーム受信時には MAC アドレスから 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。

バーストサイズのデフォルトは 16kbyte ですが、より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際には、バッファサイズを大きく設定してください。

本機能は、最低帯域監視と最大帯域制御から成り、最低帯域監視と最大帯域制御で使用できるペナルティの種類を次の表に示します。

表 3-4 最低帯域監視と最大帯域制御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	最大帯域制御
廃棄	—	○
キューイング優先度変更	○	—
DSCP 書き換え	○	—

(凡例) ○ : 使用可能なペナルティ – : 使用不可能なペナルティ

次のフレームについては、キューイング優先度変更および DSCP 書き換えのペナルティが動作しません。

- MTU を超える IPv4, IPv6 パケット
- TTL が 1 のフレーム
- ホップリミットが 1 のフレーム
- IP オプション付きのフレーム
- IPv6 拡張ヘッダ付きのフレーム
- 宛先不明の IPv4, IPv6 パケット

3.4.2 帯域監視使用時に採取可能な統計情報

帯域監視ごとに採取可能な統計情報が異なります。帯域監視使用時に採取可能な統計情報を次の表に示します。

表 3-5 帯域監視使用時に採取可能な統計情報

帯域監視種別	採取可能な統計情報			
	最大帯域違反	最大帯域遵守	最低帯域違反	最低帯域遵守
最低帯域監視	—	—	○	○
最大帯域制御	○	○	—	—
最低帯域監視と最大帯域制御の組み合わせ	○	○	—	—

(凡例) ○ : 採取可能 – : 採取不可能

3.4.3 帯域監視使用時の注意事項

(1) フローで指定した監視帯域と出力回線・出力キューの関係

複数のフローで帯域監視機能を使用している場合、各 QoS フローエントリで指定した監視帯域値の合計が、出力イーサネットインターフェース、または送信キューの帯域値以内となるように、各監視帯域値を調整してください。

(2) 帯域監視機能を使用しないフローとの混在

帯域監視機能を使用しないフローと使用するフローが同じ回線またはキューに出力されないようにしてください。

(3) プロトコル制御フレームの帯域監視

本装置では、プロトコル制御フレームも帯域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も最大帯域制御違反として廃棄される場合があります。そのため、本装置宛てのプロトコル制御フレームを考慮した最大帯域を確保する必要があります。

(4) TCP フレームに対する最大帯域制御の使用

最大帯域制御を使用した場合には、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場合があります。

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キューイング優先度を下げる」の動作を実施するようしてください。本設定によって、契約帯域を超えてすぐに廃棄されないで、出力回線が混んできたときだけに廃棄されるようになります。

(5) VLAN インタフェースに対する帯域監視機能の使用

次に示すモデルでは、イーサネットインターフェース 0/1 ~ 0/24, 0/49, 0/50 と、イーサネットインターフェース 0/25 ~ 0/48, 0/51, 0/52 をまたがった VLAN インタフェースに対して帯域監視を使用しないでください。

- PF5240F-48T4XW
- PF5240R-48T4XW

(6) ほかの機能との同時動作

次に示す場合、フレームは廃棄しますが帯域監視対象になります。

- 廃棄動作を指定したフィルタエントリ（暗黙の廃棄のエントリを含む）に一致するフレームを受信した場合

(7) 複数の QoS エントリに一致した場合の帯域監視

帯域監視機能を指定した QoS フローで、複数エントリに一致した場合、帯域監視機能が正しく動作しません。

(例) 同一インターフェースに対して mac qos-flow-list ,ip qos-flow-list をフロー検出条件とした帯域監視機能を指定した QoS エントリを設定し ,mac qos-flow-list,ip qos-flow-list の両方に一致するフレームを中継する場合。

3.5 帯域監視のコンフィグレーション

3.5.1 最大帯域制御の設定

[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行い、最大帯域制御を行う帯域監視を設定します。

[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ことによって、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 192.168.100.10 action max-rate 5M max-rate-burst 512**

宛先 IP アドレスが 192.168.100.10 のフローに対し、最大帯域制御の監視帯域 =5Mbit/s、最大帯域制御のバーストサイズ =512kbyte 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モードに戻ります。

4. **(config)#interface gigabitethernet 0/1**

ポート 0/1 のインターフェース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) を有効にします。

3.5.2 最低帯域監視違反時のキューリング優先度の設定

[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行い、最低帯域監視を行うことを設定します。最低帯域監視を違反したフレームに対しては、キューリング優先度の変更を行う設定をします。

[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ことによって、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 192.168.110.10 action min-rate 1M min-rate-burst 64 penalty-discard-class 1**

宛先 IP アドレスが 192.168.110.10 のフローに対し、最低監視帯域 =1Mbit/s、最低監視帯域のバーストサイズ =64kbyte、最低帯域監視での違反フレームのキューリング優先度 =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モードに戻ります。

4. (config)#interface gigabitethernet 0/3

ポート 0/3 のインターフェースモードに移行します。

5. (config-if)#ip qos-flow-group QOS-LIST2 in

受信側に IPv4 QoS フローリスト (QOS-LIST2) を有効にします。

3.5.3 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（違反フレームは DSCP の書き換え）を実施する場合に設定します。

[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行い、最低帯域監視 (min-rate) を行う帯域監視を設定します。最低監視帯域を違反したフレームに対しては、DSCP 値の変更を行う設定をします。

[コマンドによる設定]

1. (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ことによって、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 192.168.120.10 action min-rate 1M
min-rate-burst 64 penalty-dscp 8

宛先 IP アドレスが 192.168.120.10 のフローに対し、最低監視帯域 =1Mbit/s、最低監視帯域のバーストサイズ =64kbyte、最低帯域監視での違反フレームの DSCP 値 =8 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モードに戻ります。

4. (config)#interface gigabitethernet 0/5

ポート 0/5 のインターフェースモードに移行します。

5. (config-if)#ip qos-flow-group QOS-LIST3 in

受信側に IPv4 QoS フローリスト (QOS-LIST3) を有効にします。

3.5.4 最大帯域制御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制御と最低帯域監視（違反フレームは DSCP の書き換え）を実施したい場合に設定します。

[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行い、最大帯域制御と最低帯域監視を行う帯域監視を設定します。最低帯域監視を違反したフレームに対しては、DSCP 値の変更を行う設定をします。

3. フロー制御

[コマンドによる設定]

1. **(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ことによって、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 192.168.130.10 action max-rate 5M**

max-rate-burst 512 min-rate 1M min-rate-burst 64 penalty-dscp 8

宛先 IP アドレスが 192.168.130.10 のフローに対し、最大帯域制御の監視帯域 =5Mbit/s、最大帯域制御のバーストサイズ =512kbyte、最低監視帯域 =1Mbit/s、最低監視帯域のバーストサイズ =64kbyte、最低帯域監視での違反フレームの DSCP 値 =8 の IPv4 QoS フローリストを設定します。

3. **(config-ip-qos)#exit**

IPv4 フローリストモードからグローバルコンフィグモードに戻ります。

4. **(config)#interface gigabitethernet 0/7**

ポート 0/7 のインターフェースモードに移行します。

5. **(config-if)#ip qos-flow-group QOS-LIST4 in**

受信側に IPv4 QoS フローリスト (QOS-LIST4) を有効にします。

3.6 帯域監視のオペレーション

show qos-flow コマンドによって、設定した内容が反映されているかどうかを確認します。

3.6.1 最大帯域制御の確認

最大帯域制御の確認方法を次の図に示します。

図 3-5 最大帯域制御の確認

```
> show qos-flow 0/1

Date 2010/12/01 15:30:00 UTC
Using Port:0/1 in
IP qos-flow-list:QOS-LIST1
    ip any host 192.168.100.10 action max-rate 5M max-rate-burst 512
        matched packets(max-rate over) :      7
        matched packets(max-rate under): 28
>
```

QOS-LIST1 のリスト情報に「最大帯域制御の監視帯域 (max-rate 5M)」、「最大帯域制御のバーストサイズ (max-rate-burst 512)」が表示されることを確認します。

3.6.2 最低帯域監視違反時のキューリング優先度の確認

最低帯域監視違反時のキューリング優先度の確認方法を次の図に示します。

図 3-6 最低帯域監視違反時のキューリング優先度の確認

```
> show qos-flow 0/3

Date 2010/12/01 15:30:00 UTC
Using Port:0/3 in
IP qos-flow-list:QOS-LIST2
    ip any host 192.168.110.10 action min-rate 1M min-rate-burst 64
    penalty-discard-class 1
        matched packets(min-rate over) :      9826
        matched packets(min-rate under): 74699826
>
```

QOS-LIST2 のリスト情報に「最低監視帯域 (min-rate 1M)」、「最低監視帯域のバーストサイズ (min-rate-burst 64)」、「違反フレームのキューリング優先度 (penalty-discard-class 1)」が表示されることを確認します。

3. フロー制御

3.6.3 最低監視帯域違反時の DSCP 書き換えの確認

最低監視帯域違反時の DSCP 書き換えの確認方法を次の図に示します。

図 3-7 最低監視帯域違反時の DSCP 書き換えの確認

```
> show qos-flow 0/5

Date 2010/12/01 15:30:00 UTC
Using Port:0/5 in
IP qos-flow-list:QOS-LIST3
    ip any host 192.168.110.10 action min-rate 1M min-rate-burst 64 penalty-dscp
CS1
        matched packets(min-rate over) :          28
        matched packets(min-rate under):         7
>
```

QOS-LIST3 のリスト情報に「最低監視帯域 (min-rate 1M)」, 「最低監視帯域のバーストサイズ (min-rate-burst 64)」, 「違反フレームの DSCP 値 (penalty-dscp 8)」が表示されることを確認します。

3.6.4 最大帯域制御と最低帯域監視の組み合わせの確認

最大帯域制御と最低帯域監視の組み合わせの確認方法を次の図に示します。

図 3-8 最大帯域制御と最低帯域監視の組み合わせの確認

```
> show qos-flow 0/7

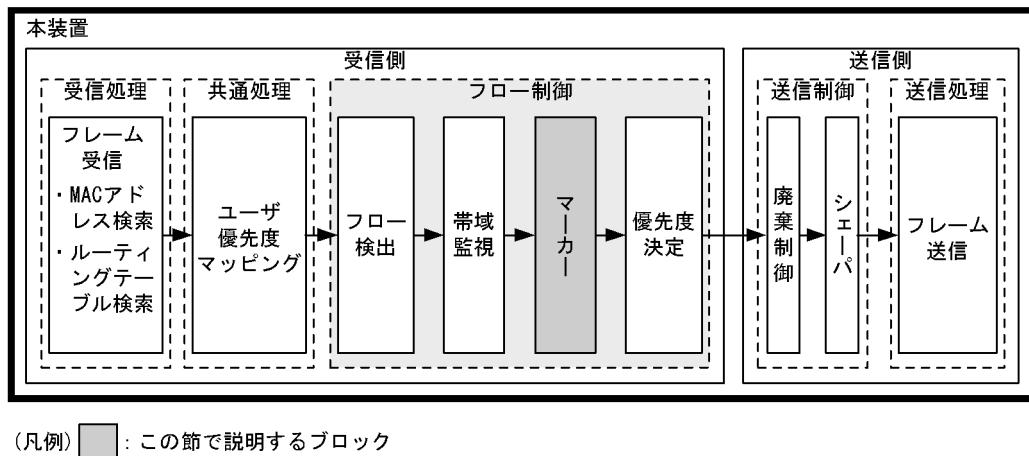
Date 2010/12/01 15:30:00 UTC
Using Port:0/7 in
IP qos-flow-list:QOS-LIST4
    ip any host 192.168.130.10 action max-rate 5M max-rate-burst 512 min-rate
1M min-rate-burst 64 penalty-dscp CS1
        matched packets(max-rate over) : 74699826
        matched packets(max-rate under):   28
>
```

QOS-LIST4 のリスト情報に「最大帯域制御の監視帯域 (max-rate 5M)」, 「最大帯域制御のバーストサイズ (max-rate-burst 512)」, 「最低監視帯域 (min-rate 1M)」, 「最低監視帯域のバーストサイズ (min-rate-burst 64)」, 「違反フレームの DSCP 値 (penalty-dscp 8)」が表示されることを確認します。

3.7 マーカー解説

マーカーは、フロー検出で検出したフレームの VLAN tag 内のユーザ優先度および IP ヘッダ内の DSCP を書き換える機能です。この節で説明するマーカーの位置づけを次の図に示します。

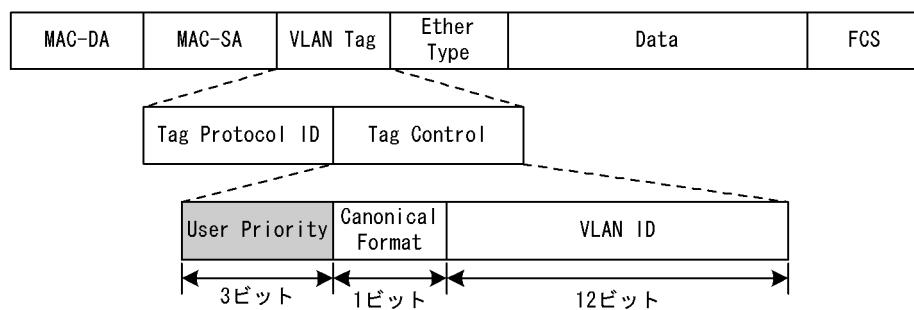
図 3-9 マーカーの位置づけ



3.7.1 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 内にあるユーザ優先度 (User Priority) を書き換える機能です。ユーザ優先度は、次の図に示すタグ情報 (Tag Control) フィールドの先頭 3 ビットを指します。

図 3-10 VLAN tag のヘッダフォーマット



VLAN tag が複数あるフレームに対してユーザ優先度書き換えを行う場合、MAC アドレス側から 1 段目の VLAN tag にあるユーザ優先度を書き換えます。次の図に VLAN tag が複数あるフレームフォーマットを示します。

図 3-11 VLAN tag が複数あるフレームフォーマットの概略図

(i) VLAN Tag 1段のフォーマット

MAC-DA	MAC-SA	1段目の VLAN Tag	Ether Type	Data	FCS
--------	--------	------------------	---------------	------	-----

(ii) VLAN Tag 2段のフォーマット

MAC-DA	MAC-SA	1段目の VLAN Tag	2段目の VLAN Tag	Ether Type	Data	FCS
--------	--------	------------------	------------------	---------------	------	-----

3. フロー制御

次のフレームについてはユーザ優先度を書き換えることができません。

- VLAN トンネリングを設定したポートで送信するフレーム
- MTU を超える IPv4, IPv6 パケット
- TTL が 1 のフレーム
- ホップリミットが 1 のフレーム
- IP オプション付きのフレーム
- IPv6 拡張ヘッダ付きのフレーム
- 宛先不明の IPv4, IPv6 パケット

ユーザ優先度書き換えは、ユーザ優先度引き継ぎと同時に設定することはできません。

ユーザ優先度書き換えおよびユーザ優先度引き継ぎをどちらも実施しない場合は、次の表に示すユーザ優先度となります。

表 3-6 フレーム送信時のユーザ優先度

フレーム送信時のユーザ優先度	対象となるフレーム
3	<ul style="list-style-type: none">• VLAN tag なしで受信し、VLAN tag ありで送信するフレーム• VLAN トンネリング機能で、アクセス回線からバックボーン回線に中継するフレーム
受信フレームのユーザ優先度	<ul style="list-style-type: none">• VLAN トンネリング機能で、アクセス回線からアクセス回線に中継する VLAN tag ありフレーム• tag 変換を設定していない、かつ VLAN トンネリングを設定していないポートで VLAN tag ありフレームを受信し、VLAN tag ありで送信するフレーム

ユーザ優先度書き換えを優先度決定機能と同時に設定した場合、優先度決定機能で決定した CoS 値に応じて固定的にユーザ優先度を決定します。

優先度決定機能とユーザ優先度書き換え機能を同時に設定した場合のユーザ優先度を次の表に示します。

表 3-7 優先度決定機能とユーザ優先度書き換え機能を同時に設定した場合のユーザ優先度

優先度決定機能で決定した CoS 値	ユーザ優先度
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

3.7.2 ユーザ優先度引き継ぎ

VLAN トンネリング機能で、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するときに、フロー検出で検出したフレームのユーザ優先度を、バックボーン回線のユーザ優先度（追加する VLAN tag のユーザ優先度）および優先度決定機能の CoS 値に引き継ぐ機能です。

ユーザ優先度引き継ぎは、VLAN トンネリングを設定した受信側イーサネットインターフェースに設定できます。

ユーザ優先度引き継ぎを設定した場合の動作について、次の表に示します。

表 3-8 ユーザ優先度引き継ぎ機能を設定した場合の動作

フロー検出で検出したフレームのユーザ優先度	送信フレーム	
	ユーザ優先度	CoS 値
VLAN tag なし	0	0
0	0	0
1	1	1
2	2	2
3	3	3
4	4	4
5	5	5
6	6	6
7	7	7

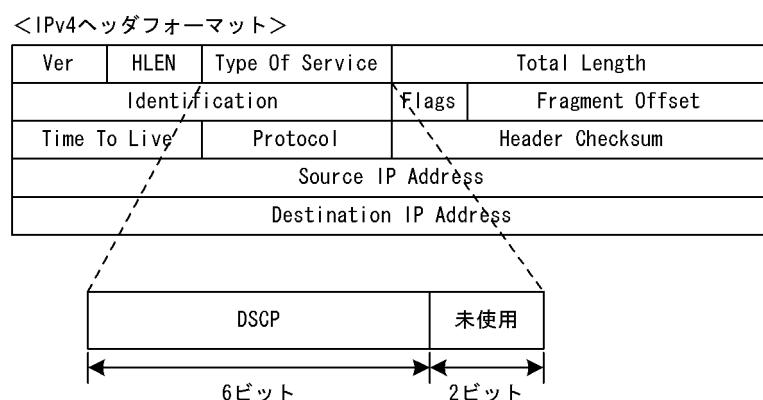
ユーザ優先度引き継ぎは、ユーザ優先度書き換え機能および優先度決定機能（CoS 値の指定）と同時に設定することはできません。

ユーザ優先度引き継ぎを設定しない場合の CoS 値については「3.10.1 CoS 値・キューイング優先度」を、ユーザ優先度については「3.7.1 ユーザ優先度書き換え」を参照してください。

3.7.3 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。

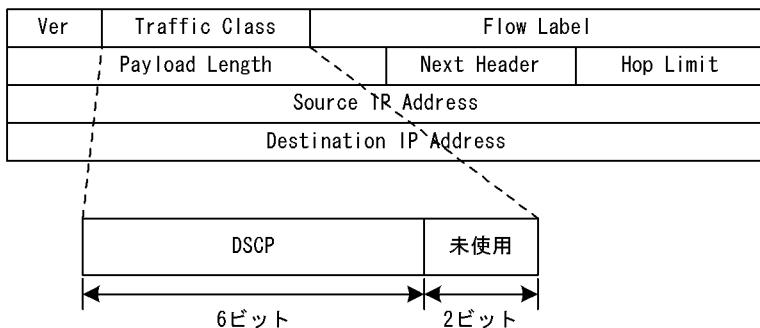
図 3-12 TOS フィールドのフォーマット



3. フロー制御

図 3-13 トラフィッククラスフィールドのフォーマット

<IPv6ヘッダフォーマット>



検出したフローの 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 ビットを書き換えます。

また、帯域監視からの指示によって、最低監視帯域を超えたフローの DSCP を書き換えることができます。例えば、最低監視帯域を超えたフローに対して、DSCP 値を 0 に設定できます。

最低帯域監視と同時に設定した場合の違反フレームの動作については、違反時のペナルティ指定動作が優先されます。

次のフレームについては DSCP を書き換えることができません。

- MTU を超える IPv4, IPv6 パケット
- TTL が 1 のフレーム
- ホップリミットが 1 のフレーム
- IP オプション付きのフレーム
- IPv6 拡張ヘッダ付きのフレーム
- 宛先不明の IPv4, IPv6 パケット

3.8 マーカーのコンフィグレーション

3.8.1 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に設定します。

[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行い、ユーザ優先度の書き換えを設定します。

[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ことによって、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 192.168.100.10 action replace-user-priority 6**

192.168.100.10 の IP アドレスを宛先とし、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モードに戻ります。

4. **(config)#interface gigabitethernet 0/1**

ポート 0/1 のインターフェースモードに移行します。

5. **(config-if)#ip qos-flow-group QOS-LIST1 in**

受信側の IPv4 QoS フローリスト (QOS-LIST1) を有効にします。

3.8.2 ユーザ優先度引き継ぎの設定

特定のフローに対してユーザ優先度引き継ぎを行う場合に設定します。

[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行い、ユーザ優先度引き継ぎを行います。

[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ことによって、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 192.168.100.10 action copy-user-priority**

192.168.100.10 の IP アドレスを宛先とし、ユーザ優先度引き継ぎを行う 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モードに戻ります。

3. フロー制御

4. **(config)#interface gigabitethernet 0/1**
ポート 0/1 のインターフェースモードに移行します。
5. **(config-if)#ip qos-flow-group QOS-LIST2 in**
受信側の IPv4 QoS フローリスト (QOS-LIST2) を有効にします。

3.8.3 DSCP 書き換えの設定

特定のフローに対して DSCP を書き換える場合に設定します。

[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行い、DSCP 値の書き換えを設定します。

[コマンドによる設定]

1. **(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ことによって、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 192.168.100.10 action replace-dscp 63**
192.168.100.10 の IP アドレスを宛先とし、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モードに戻ります。
4. **(config)#interface gigabitethernet 0/3**
ポート 0/3 のインターフェースモードに移行します。
5. **(config-if)#ip qos-flow-group QOS-LIST3 in**
受信側の IPv4 QoS フローリスト (QOS-LIST3) を有効にします。

3.9 マーカーのオペレーション

show qos-flow コマンドによって、設定した内容が反映されているかどうかを確認します。

3.9.1 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方法を次の図に示します。

図 3-14 ユーザ優先度書き換えの確認

```
> show qos-flow 0/1

Date 2010/12/01 15:30:00 UTC
Using Port:0/1 in
IP qos-flow-list:QOS-LIST1
    ip any host 192.168.100.10 action replace-user-priority 6
        matched packets : 0
>
```

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。

3.9.2 ユーザ優先度引き継ぎの確認

ユーザ優先度引き継ぎの確認方法を次の図に示します。

図 3-15 ユーザ優先度引き継ぎの確認

```
> show qos-flow 0/1

Date 2010/12/01 15:30:00 UTC
Using Port:0/1 in
IP qos-flow-list:QOS-LIST2
    ip any host 192.168.100.10 action copy-user-priority
        matched packets : 0
>
```

QOS-LIST2 のリスト情報に「copy-user-priority」が表示されることを確認します。

3.9.3 DSCP 書き換えの確認

DSCP 書き換えの確認方法を次の図に示します。

図 3-16 DSCP 書き換えの確認

```
> show qos-flow 0/3

Date 2010/12/01 15:30:00 UTC
Using Port:0/3 in
IP qos-flow-list:QOS-LIST3
    ip any host 192.168.100.10 action replace-dscp 63
        matched packets : 0
>
```

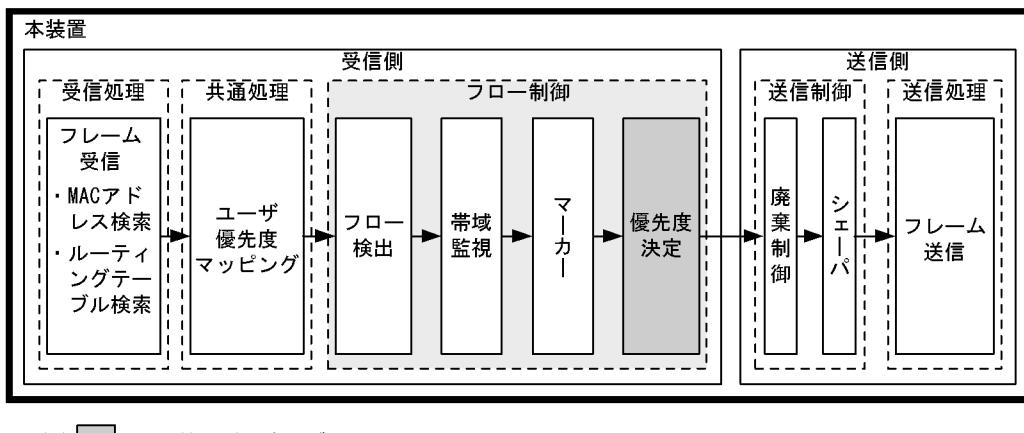
QOS-LIST3 のリスト情報に「replace-dscp 63」が表示されることを確認します。

3.10 優先度決定の解説

優先度決定は、フロー検出で検出したフレームの優先度を CoS 値で指定して、送信キューを決定する機能です。

この節で説明する優先度決定の位置づけを次の図に示します。

図 3-17 優先度決定の位置づけ



3.10.1 CoS 値・キューイング優先度

CoS 値は、フレームの装置内における優先度を表すインデックスを示します。キューイング優先度は、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します。

CoS 値とキューイング優先度の指定範囲を次の表に示します。

表 3-9 CoS 値とキューイング優先度の指定範囲

項目	指定範囲
CoS 値	0 ~ 7
キューイング優先度	1 ~ 3

CoS 値の指定は、ユーザ優先度引き継ぎと同時に設定することはできません。

また、フロー制御の優先度決定およびユーザ優先度引き継ぎが設定されていない場合は、次の表に示すデフォルトの CoS 値とキューイング優先度を使用します。

表 3-10 デフォルトの CoS 値とキューイング優先度

項目	デフォルト値	対象となるフレーム
CoS 値	ユーザ優先度マッピングに従います	<ul style="list-style-type: none"> フロー検出で検出しないフレーム フロー検出で検出し、優先度決定 (CoS 値の指定) およびマーカー (優先度引き継ぎ) を実施しないフレーム
キューイング優先度	3	<ul style="list-style-type: none"> フロー検出で検出しないフレーム フロー検出で検出し、優先度決定 (キューイング優先度値の指定) を実施しないフレーム

なお、次に示すフレームは、フロー制御の優先度決定およびユーザ優先度引き継ぎの有無に関わらず、固定的に CoS 値とキューイング優先度を決定します。

優先度決定およびユーザ優先度引き継ぎで変更できないフレームを次の表に示します。

表 3-11 優先度決定で変更できないフレーム一覧

フレーム種別	CoS 値	キューイング優先度
本装置が自発的に送信するフレーム	7	3
本装置が受信するフレームのうち次のフレーム ・ ARP フレーム ・ 回線テストに使用するフレーム	5	3
本装置が受信するフレームのうち次のフレーム ・ MAC アドレス学習の移動検出とみなしたフレーム	2	3
本装置がレイヤ 3 中継し、本装置が受信するフレームのうち次のパケット/フレーム ・ MTU を超える IPv4, IPv6 パケット ・ TTL が 1 のフレーム ・ ホップリミットが 1 のフレーム ・ IP オプション付きのフレーム ・ IPv6 拡張ヘッダ付きのフレーム	2	3
本装置がレイヤ 3 中継し、本装置が受信するフレームのうち次のパケット ・ 宛先不明の IPv4, IPv6 パケット	2	3
本装置でレイヤ 3 中継するフレームのうち次のフレーム ・ 本装置でフラグメントしたフレーム ・ IP オプション付きのフレーム ・ IPv6 拡張ヘッダ付きのフレーム ・ ARP/NDP の未解決により本装置に一時的に滞留する中継フレーム	3	3

3.10.2 CoS マッピング機能

CoS マッピング機能は、ユーザ優先度マッピングで決定した CoS 値、またはフロー制御の優先度決定で指定した CoS 値に基づいて、送信キューを決定する機能です。

CoS 値と送信キューのマッピングを次の表に示します。

表 3-12 CoS 値と送信キューのマッピング

CoS 値	送信時のキュー番号	
	送信キュー長 64	送信キュー長 1976
0	1	1
1	2	1
2	3	1
3	4	1
4	5	1
5	6	1
6	7	1
7	8	2

3.10.3 優先度決定使用時の注意事項

(1) フレームの優先度決定

「フレームの優先度を上げる」動作を指定すると、次に示すフレームが受信または送信できなくなることによって、通信が切断される場合があります。

- 本装置宛てのプロトコル制御フレーム
- 本装置が自発的に送信するフレーム

このような現象が発生した場合は、「フレームの優先度を下げる」動作を実施してください。

3.11 優先度決定コンフィグレーション

3.11.1 CoS 値の設定

特定のフローに対して CoS 値を設定します。

[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行い、CoS 値を設定します。

[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ことによって、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 192.168.100.10 action cos 6**

192.168.100.10 の IP アドレスを宛先とし、CoS 値 = 6 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モードに戻ります。

4. **(config) #interface 0/1**

ポート 0/1 のインターフェースモードに移行します。

5. **(config-if) #ip qos-flow-group QOS-LIST1 in**

IPv4 QoS フローリスト (QOS-LIST1) を有効にします。

3.12 優先度のオペレーション

3.12.1 優先度の確認

回線にトライフィック（宛先 IP アドレスが 192.168.100.10 のフレーム）を注入している状態で、`show qos queueing` コマンドによってキューイングされているキュー番号を確認します。対象のイーサネットインターフェースは、ポート 0/2 です。

図 3-18 優先度の確認

```
> show qos queueing 0/2
Date 2010/12/01 15:30:00 UTC
NIF0/Port2 (outbound)
Max_Queue=8, Rate_limit=100Mbit/s, Burst_size=32kbyte, Qmode=pq/tail_drop
Queue1: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue2: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue3: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue4: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue5: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue6: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue7: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue8: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Tail_drop= 0
```

3.13 複数の QoS エントリに一致した場合の動作

複数の QoS エントリに一致した場合、高優先エントリ、低優先エントリに振り分けられ、動作を決定します。

高優先エントリ、低優先エントリは、QoS フローリストの種類によって決定されます。

- (a) 同一インターフェースに対して mac qos-flow-list, ip qos-flow-list をフロー検出条件とした QoS エントリを設定した場合。

高優先エントリ mac qos-flow-list で設定した QoS エントリ

低優先エントリ ip qos-flow-list で設定した QoS エントリ

高優先エントリと低優先エントリによる動作を、次の表に示します。

表 3-13 複数の QoS エントリに一致した場合の動作

モデル	動作
PF5200 シリーズ	<ul style="list-style-type: none"> ・両方に指定された動作を実施する。 ・指定された動作が同じ場合、高優先エントリの動作を実施する。

4

送信制御

この章では本装置の送信制御（シェーパおよび廃棄制御）について説明します。

4.1 シェーパ解説

4.2 シェーパのコンフィグレーション

4.3 シェーパのオペレーション

4.4 廃棄制御解説

4.5 廃棄制御のコンフィグレーション

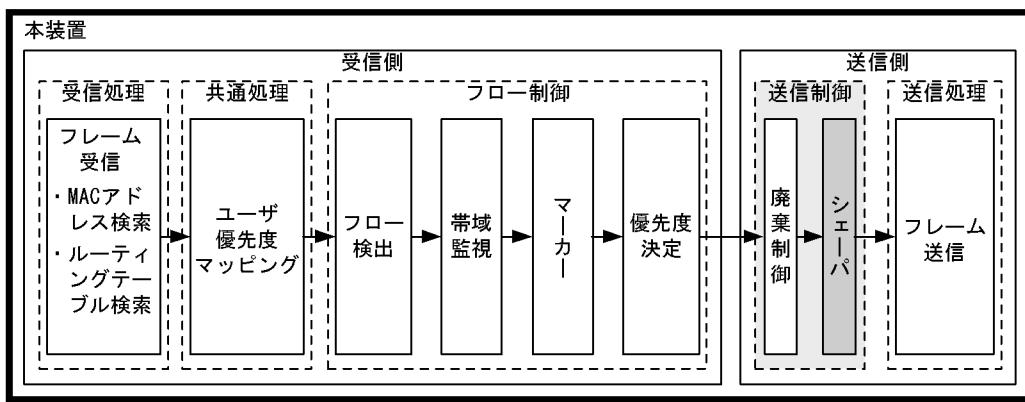
4.6 廃棄制御のオペレーション

4.1 シェーパ解説

4.1.1 レガシーシェーパの概要

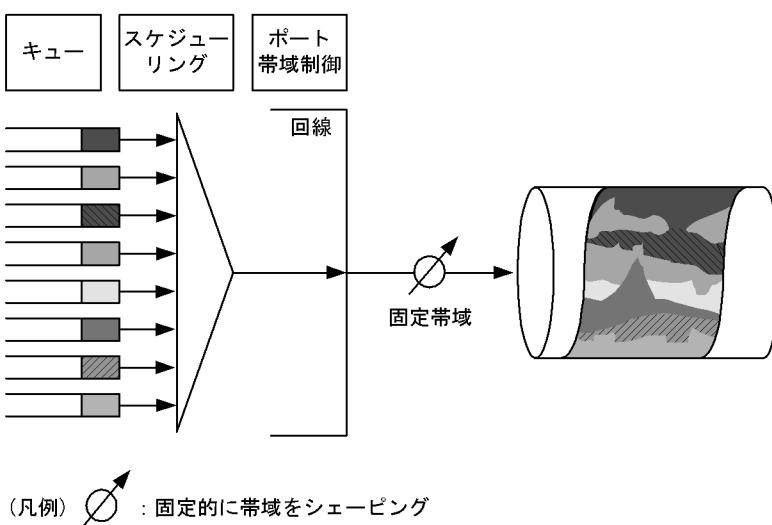
シェーパは、各キューからのフレームの出力順序、および各ポートの出力順序や出力帯域を制御する機能です。この節で説明するシェーパの位置づけを次の図に示します。

図 4-1 シェーパの位置づけ



レガシーシェーパは、次の図に示すように、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と、イーサネットインター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ています。レガシーシェーパの概念を次の図に示します。

図 4-2 レガシーシェーパの概念



4.1.2 送信キュー長指定

本装置では、ネットワーク構成や運用形態に合わせて送信キュー長を変更できます。送信キュー長の変更是コンフィグレーションコマンド `limit-queue-length` で指定します。送信キュー長を拡大することによって、バーストトラフィックによるキューあふれを低減させることができます。なお、指定した送信キュー

長は本装置のすべてのイーサネットインターフェースに対して有効になります。

送信キュー長を指定しない場合、キュー長 64 で動作します。なお、他のキュー長を指定する場合は、コンフィグレーションコマンド flowcontrol を使用して「ポーズパケットを送信する」設定をしてください。

表 4-1 送信キュー長と運用目的の関係

送信キュー長	運用目的
64	各キューに均等に負荷があり、送信制御を有効にしたい場合に指定します。
3200※	バーストトラフィックによるキューあふれを低減させたい場合に指定します。

注※

64 以外の送信キュー長を指定した場合、キュー 1、キュー 2 に対してだけキュー長を割り当て動作するため、各スケジューリングの動作は次のようになります。

PQ, RR, WRR : キュー 1、キュー 2 が PQ, RR, WRR で動作します。

2PQ+6DRR : キュー 1、キュー 2 が DRR で動作します。

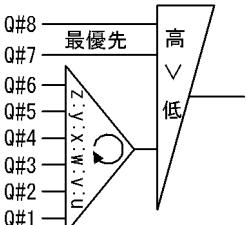
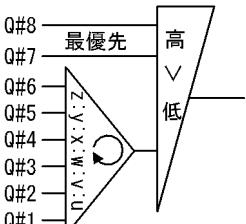
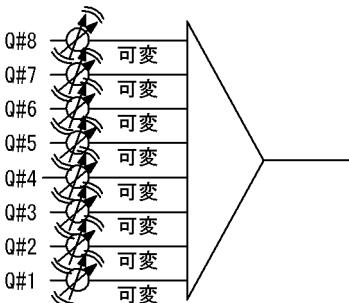
2PQ+6WRR : キュー 1、キュー 2 が WRR で動作します。

4.1.3 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、次に示す六つのスケジューリング機能があります。スケジューリングの動作説明を次の表に示します。

表 4-2 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出します。	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 フレームずつ送出します。フレーム長によらず、フレーム数が均等になる制御を行います。	データ系トラフィックだけの場合
WRR		重み（フレーム数）付きラウンドロビン。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設定した z:y:x:w:v:u:t:s の重み（フレーム数）に応じて、キュー 8 ~ 1（左図 Q#8 ~ Q#1）からフレームを送出します。	すべてのトラフィックの送信が要求されかつ、優先すべきトラフィックと優先しないトラフィックが混在している場合

スケジューリング種別	概念図	動作説明	適用例
2PQ+6DRR		最優先キュー + 重み（バイト数）付きラウンドロビン。最優先のキュー 8 (左図 Q#8) は、常に最優先でフレームを送出します。キュー 7 (左図 Q#7) は、キュー 8 (左図 Q#8) の次に優先的にフレームを送出します。キュー 8,7 の送出がないときに、キュー 6 ~ 1 (左図 Q#6 ~ Q#1) は各キュー設定したバイト数 (z : y : x : w : v : u) に応じてフレームを送出します。	最優先キューに映像、音声、DRR キューにデータ系トライフィック
2PQ+6WRR		最優先キューと重み（フレーム数）付きラウンドロビン。最優先のキュー 8 (左図 Q#8) は、常に最優先でフレームを送出します。キュー 7 (左図 Q#7) は、キュー 8 (左図 Q#8) の次に優先的にフレームを送出します。キュー 8,7 の送出がないときに、キュー 6 ~ 1 (左図 Q#6 ~ Q#1) は各キュー設定したフレームの重み (z : y : x : w : v : u) に応じてフレームを送出します。	最優先キューに映像、音声、WRR キューにデータ系トライフィック
WFQ		重み付き均等保証。すべてのキューに対して重み（最低保証帯域）を設定し、はじめにキューごとに最低保証帯域分を送出します。	すべてのトライフィックに対し最低帯域保証が要求される場合

スケジューリングの仕様について次の表に示します。

表 4-3 スケジューリング仕様

項目	仕様	
キュー数	8 キュー	
2PQ+6DRR	キュー 1 ~ 6 の重みの設定範囲	<ul style="list-style-type: none"> PF5200 シリーズの場合 【kbyte 単位】 2 ~ 254 (刻み値:2) 4 ~ 508 (刻み値:4) 8 ~ 1016 (刻み値:8) 16 ~ 2032 (刻み値:16)
2PQ+6WRR	キュー 1 ~ 6 の重みの設定範囲	1 ~ 15
WFQ	キュー 1 ~ 8 の重みの設定範囲	「表 4-4 WFQ の設定範囲」を参照してください。最低保証帯域の合計が回線帯域以下になるように設定してください。回線状態が半二重モードの場合は設定できません。設定できない場合は、運用ログが表示され WFQ の設定は無効となり、PQ で動作します。

項目	仕様
最低保証帯域の対象となるフレームの範囲	MAC ヘッダから FCS まで

表 4-4 WFQ の設定範囲

設定単位※1	設定範囲	刻み値
Gbit/s	1G ~ 10G	1Gbit/s
Mbit/s	1M ~ 10000M	1Mbit/s
kbit/s	1000 ~ 10000000	100kbit/s ※2
	64 ~ 960	64kbit/s ※3

注※1 1G, 1M, 1k はそれぞれ 1000000000, 1000000, 1000 として扱います。

注※2 設定値が 1000k 以上の場合 100k 刻みで指定します (1000, 1100, 1200, …, 10000000)。

注※3 設定値が 1000k 未満の場合 64k 刻みで指定します (64, 128, 192, …, 960)。

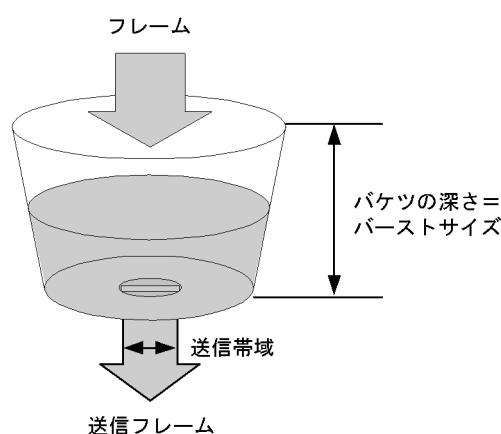
4.1.4 ポート帯域制御

ポート帯域制御は、スケジューリングを実施した後に、該当する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へ接続できます。

例えば、回線帯域が 1Gbit/s で ISP との契約帯域が 400Mbit/s の場合、ポート帯域制御機能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することができます。

ポート帯域制御は穴の開いたバケツをモデルとする、Leaky Bucket アルゴリズムを用いています。Leaky Bucket アルゴリズムのモデルを次の図に示します。

図 4-3 Leaky Bucket アルゴリズムのモデル



バケツには受信したフレームサイズ分の水が注ぎ込まれ、ポート帯域制御の送信帯域分の水が送信フレームとして流れます。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。バケツが空の状態でトラフィックを送信した際、送信帯域の揺らぎはバーストサイズに比例します。バーストサイズまで水が溜まった場合、フレームは送信キューに溜まります。

ポート帯域制御の設定範囲を次の表に示します。設定帯域は回線速度以下になるように設定してください。

4. 送信制御

回線状態が半二重モードの場合は設定できません。設定できない場合、運用ログが表示されポート帯域制御の設定は無効となります。

表 4-5 ポート帯域制御の設定範囲

設定単位※1	設定範囲	刻み値
Gbit/s	1G ~ 10G	1Gbit/s
Mbit/s	1M ~ 10000M	1Mbit/s
kbit/s	1000 ~ 10000000	100kbit/s ※2
	64 ~ 960	64kbit/s ※3

注※1 1G, 1M, 1k はそれぞれ 1000000000, 1000000, 1000 として扱います。

注※2 設定値が 1000k 以上の場合 100k 刻みで指定します (1000, 1100, 1200, …, 10000000)。

注※3 設定値が 1000k 未満の場合 64k 刻みで指定します (64, 128, 192, …, 960)。

バーストサイズの設定範囲を次に示します。

● バーストサイズの設定範囲

4, 8, 16, 32kbyte (設定省略時のデフォルトは 32kbyte)

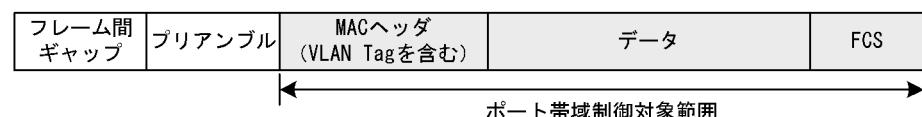
Leaky Bucket アルゴリズムの特性によるバーストサイズの特徴を次の表に示します。

表 4-6 バーストサイズの特徴

バーストサイズ	特徴
小さくする	バーストトラフィックが比較的廃棄されやすい。通信をしていない状態でトラフィックを送信した際、送信帯域の揺らぎが比較的小さい。
大きくする	バーストトラフィックが比較的廃棄されにくい。通信をしていない状態でトラフィックを送信した際、送信帯域の揺らぎが比較的大きい。

ポート帯域制御の対象となるフレームの範囲は MAC ヘッダから 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 4-4 ポート帯域制御の対象範囲



4.1.5 シェーパ使用時の注意事項

(1) パケットバッファ枯渇時のスケジューリングの注意事項

出力回線の帯域を上回るトラフィックを受信したとき、本装置のパケットバッファの枯渇が発生する場合があります。そのため、受信したフレームがキューにキューイングされず廃棄されるため、指定したスケジューリングどおりにフレームが送信されない場合があります。

パケットバッファの枯渇については、show qos queueing コマンドの HOL1 または HOL2 カウンタがインクリメントされていることで確認できます。

パケットバッファの枯渇が定常に発生する場合、ネットワーク設計の見直しが必要です。

4.2 シェーパのコンフィグレーション

4.2.1 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 キューリスト情報を作成し、該当するポートに設定します。

[コマンドによる設定]

1. **(config)#qos-queue-list QLIST-PQ pq**

QoS キューリスト情報 (QLIST-PQ) にスケジューリング (PQ) を設定します。

2. **(config)#interface gigabitethernet 0/1**

ポート 0/1 のインターフェースモードに移行します。

3. **(config-if)#qos-queue-group QLIST-PQ**

QoS キューインターフェース情報に QoS キューリスト名称を指定し、QoS キューリスト情報を有効にします。

4.2.2 ポート帯域制御の設定

該当するポート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]

該当するポート (100Mbit/s) に対し、ポート帯域制御による帯域の設定 (20Mbit/s) およびバーストサイズの設定 (4kbyte) を行います。

[コマンドによる設定]

1. **(config)#interface gigabitethernet 0/13**

ポート 0/13 のインターフェースモードに移行します。

2. **(config-if)#speed 100**

(config-if)#duplex full

該当するポートの回線速度を 100Mbit/s に設定します。

3. **(config-if)#traffic-shape rate 20M 4**

ポート帯域を 20Mbit/s、バーストサイズを 4kbyte に設定します。

4.3 シェーパのオペレーション

show qos queueing コマンドによって、イーサネットインターフェースに設定したレガシーシェーパの内容を確認します。

4.3.1 スケジューリングの確認

スケジューリングの確認方法を次の図に示します。

図 4-5 スケジューリングの確認

```
> show qos queueing 0/1

Date 2010/12/01 15:30:00 UTC
NIF0/Port1 (outbound)
Max_Queue=8, Rate_limit=64kbit/s, Burst_size=4kbyte, Qmode=pq/tail_drop ...1
Queue1: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue2: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue3: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue4: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue5: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue6: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue7: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue8: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Tail_drop= 0
```

1. Qmode パラメータの内容が、設定したスケジューリング（この例では、pq/tail_drop）になっていることを確認します。

4.3.2 ポート帯域制御の確認

ポート帯域制御の確認方法を次の図に示します。

図 4-6 ポート帯域制御の確認

```
> show qos queueing 0/13

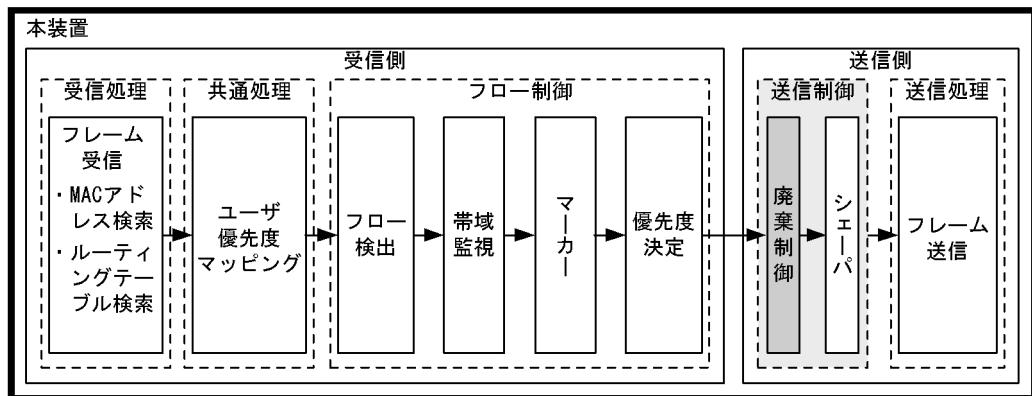
Date 2010/12/01 15:30:00 UTC
NIF0/Port13 (outbound)
Max_Queue=8, Rate_limit=20Mbit/s, Burst_size=4kbyte, Qmode=pq/tail_drop ... 1,2
Queue1: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue2: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue3: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue4: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue5: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue6: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue7: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue8: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Tail_drop= 0
```

1. Rate_limit パラメータの内容が、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。
2. Burst_size パラメータの内容が、指定したバーストサイズ（この例では、4kbyte）になっていることを確認します。

4.4 廃棄制御解説

この節で説明する廃棄制御の位置づけを次の図に示します。

図 4-7 廃棄制御の位置づけ



(凡例) : この節で説明するブロック

4.4.1 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キューイング優先度と、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。

キューにフレームが滞留している場合、キューイング優先度を変えることによって、さらに木目細かい QoS を実現できます。

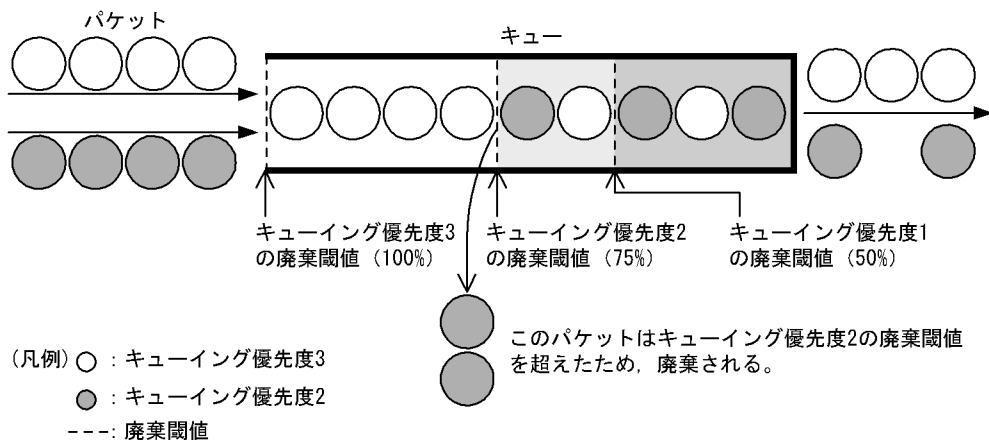
一つのキューにキューイングできるフレーム数を「キュー長」と呼びます。

本装置は、テールドロップ方式で廃棄制御を行います。

(1) 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、キューイング優先度ごとに異なり、キューイング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。キューイング優先度 2 の廃棄閾値を超えると、キューイング優先度 2 のフレームをすべて廃棄します。

図 4-8 テールドロップの概念



次に、テールドロップ機能におけるキューライング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溜まり具合を百分率で表します。

表 4-7 テールドロップでの廃棄閾値

キューライング優先度	廃棄閾値 [%]
1	50
2	75
3	100

4.5 廃棄制御のコンフィグレーション

4.5.1 キューイング優先度の設定

特定のフローに対してキューイング優先度を設定します。

[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行い、キューイング優先度を設定します。

[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ことによって、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 192.168.100.10 action discard-class 2**

192.168.100.10 の IP アドレスを宛先とし、キューイング優先度 = 2 の 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モードに戻ります。

4. **(config)#interface gigabitethernet 0/1**

ポート 0/1 のインターフェースモードに移行します。

5. **(config-if)#ip qos-flow-group QOS-LIST2 in**

受信側に QoS フローリスト (QOS-LIST2) を有効にします。

4.6 廃棄制御のオペレーション

回線にトライフィック (Queue6 の Qlen が 64 程度の滞留が発生するトライフィック) を注入している状態で、show qos queueing コマンドによってキューイングされているキュー番号および廃棄パケット数を確認します。

4.6.1 キューイング優先度の確認

キューイング優先度の確認方法を次の図に示します。

図 4-9 キューイング優先度の確認

```
> show qos queueing 0/2

Date 2010/12/01 15:30:00 UTC
NIF0/Port2 (outbound)
Max_Queue=8, Rate_limit=64kbit/s, Burst_size=4kbyte, Qmode=pq/tail_drop
Queue1: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue2: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue3: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue4: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue5: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue6: Qlen= 48, Limit_Qlen= 64, HOL1= 1514      ... 1,2
Queue7: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Queue8: Qlen= 0, Limit_Qlen= 64, HOL1= 0
Tail_drop= 18                                     ... 2
```

1. Queue6 の Qlen の値がカウントされていることを確認します。
2. Qlen の値が Limit_Qlen の値の 75% であり、discard packets の Tail_drop のカウンタがインクリメントされていることを確認します。

5 OpenFlow機能の解説

この章では、OpenFlow機能について解説します。

5.1 OpenFlow機能の概要

5.2 OpenFlow機能の解説

5.3 サポート仕様

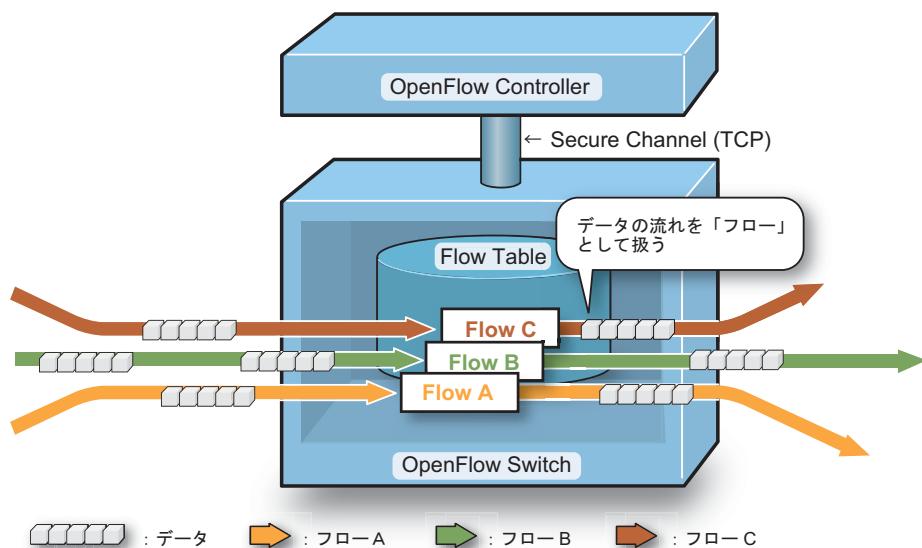
5.1 OpenFlow 機能の概要

5.1.1 OpenFlow 技術の基本概念

次世代ネットワーク技術である「OpenFlow」は、従来のネットワークの通信経路制御機能とパケット転送制御機能を OpenFlow プロトコルにより分離しています。ネットワークを構成する要素は、通信経路制御を行う OpenFlow Controller (OFC) とパケット転送制御を行う OpenFlow Switch (OFS) です。OFC で複数の OFS を集中管理することにより、ネットワーク全体が 1 台の仮想的なスイッチのように管理することができます。

OpenFlow アーキテクチャでは、データの流れを「フロー」単位で制御します。OFS は、パケット転送処理を決定するためのデータベースであるフローテーブルを持ち、フローテーブル内のフローエントリに従ってパケットを処理・出力します。OFS と OFC の間は Secure Channel という経路で接続され、OFS は OFC からの指示に従ってフローテーブル内のフローエントリを設定・変更・削除します。

図 5-1 OpenFlow 概念図



5.1.2 OpenFlow 機能の概要

OpenFlow 機能では、IP パケットやイーサネットフレーム等で用いられる 12 のフィールドの組み合わせで、パケットをフローとして識別することができます。フロー識別条件とフローに対するアクションのセットをフローエントリと呼び、これを格納したデータベースをフローテーブルと呼びます。検索できるフィールドの詳細は「表 5-2 フローの検索キー」を参照してください。各フローエントリの統計情報（ヒットしたパケット数やオクテット数）は保持され、OpenFlow プロトコルの統計情報取得メッセージで確認することができます。OFS では、フローの識別を IP やイーサネットなどで行いますが、ルーティングテーブルや FDB に従って転送するのではなく、フローエントリ毎にアクションを決めることができます。

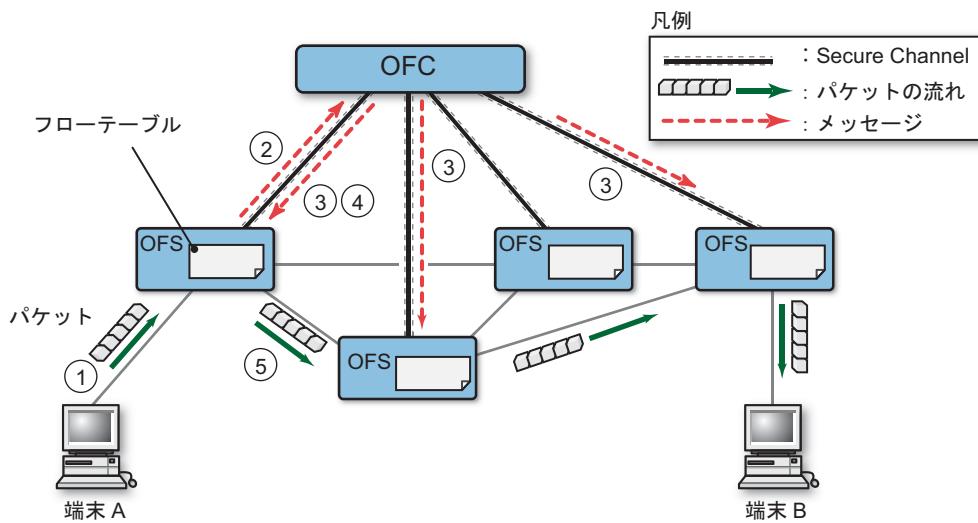
アクションには、以下のような処理があります。

- 出力インターフェースを指定して送信
- 出力インターフェースを複数指定
- MAC アドレス、VLAN タグ、IP アドレスの書き換え
- VLAN タグ内の IEEE802.1p 優先度の書き換え、DSCP 値の書き換え

また、本装置から OFC にパケットを送信し、OFC 側で状況に応じてアクションを決め、フローエントリを OFS のフローテーブルに登録することも可能です。

OpenFlow 機能を用いたネットワーク構成図の一例を以下に示します。

図 5-2 OpenFlow によるパケット転送の流れ



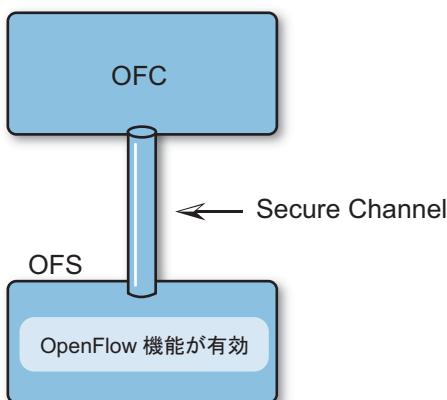
- ① 端末 A から端末 B 宛にパケットを送信
- ② 未知のパケットのため、OFC へパケット情報を転送
- ③ 新規フローエントリを登録
- ④ パケット出力を要求
- ⑤ 新規で登録されたフローエントリに従い、端末 B までパケットが転送される

5.1.3 OpenFlow 機能の動作概要

OFC と OFS の間では、OpenFlow プロトコルメッセージを使用し制御を行います。次に、Secure Channel 確立からパケット転送までの仕組みを示します。やり取りされるメッセージの詳細や両装置間のシーケンスは、「5.3.2 OpenFlow プロトコルサポートメッセージ」を参照してください。

(1) Secure Channel の確立

図 5-3 Secure Channel 確立動作



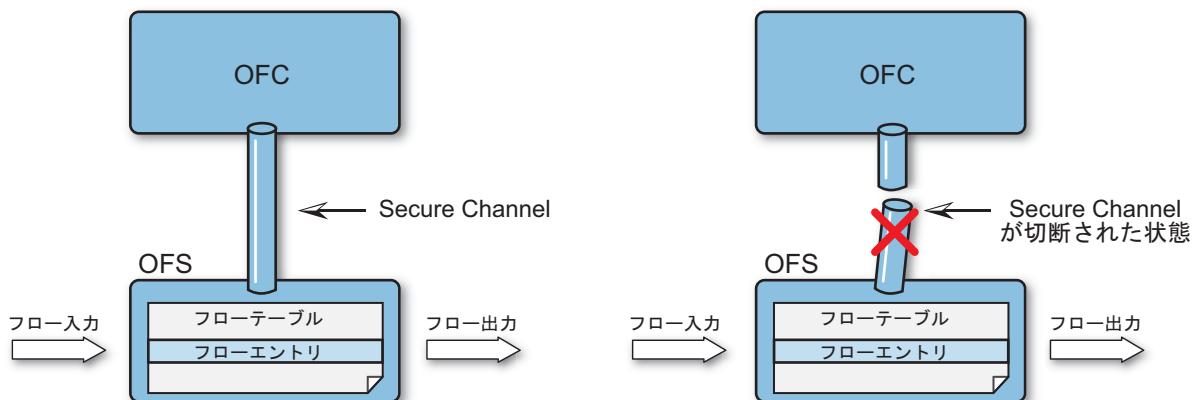
OpenFlow 機能が有効化されると、OFS と OFC の間で Secure Channel の接続が行われます。

(2) フロー転送処理と OFC からの制御

Secure Channel 確立後、下記に示す(2-1), (2-2)の動作を行います。

(2-1) フロー転送処理

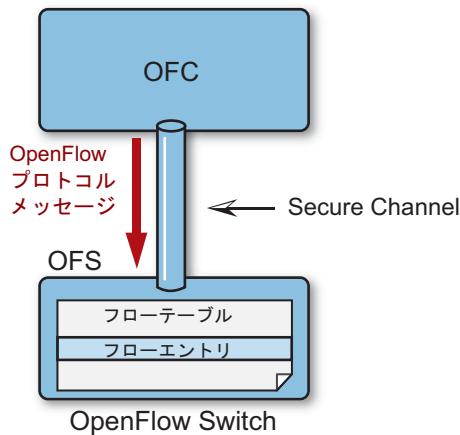
図 5-4 フロー転送処理



OFS にパケットが入力されると、OFS のフローテーブルを検索し、パケットに適合するフローエントリがある場合、設定されたアクションに従って処理を行います。なお、Secure Channel が切断されている状態でも、フローエントリが存在する場合、同様の動作を行います（「図 5-4 フロー転送処理」の右図を参照）。

(2-2) OFC からの制御

図 5-5 OFC からの制御



OFC は Secure Channel を経由して、OpenFlow プロトコルメッセージを利用し、フローエントリの登録、変更、削除を行うことができます。その他、ポートの管理、コンフィグレーション管理、統計情報取得などが可能です。詳細は、「5.3.2 OpenFlow プロトコルサポートメッセージ」を参照してください。

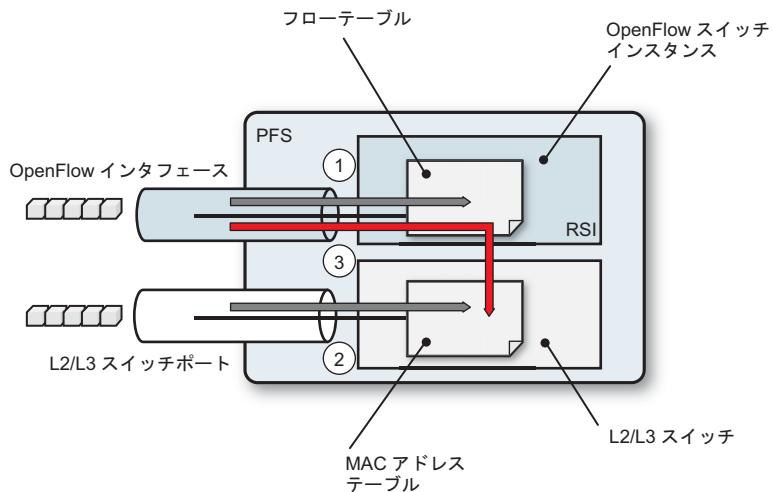
5.1.4 Programmable Flow Switch の概要

Programmable Flow Switch (PFS) は、OpenFlow 機能を搭載した PF5200 シリーズの名称です。

本装置では、OFS として動作する仮想スイッチである、OpenFlow スイッチインスタンスを生成することができます。OpenFlow スイッチインスタンスに所属する物理ポートおよびリンクアグリゲーションインターフェースを、OpenFlow インタフェースと呼びます。OpenFlow インタフェースからパケットが入力されると、対応する OpenFlow スイッチインスタンス（「5.2.1 OpenFlow スイッチインスタンスの解説」を参照）のフローテーブル内を検索します。検索にヒットするフローエントリが存在した場合は、フローの統計情報が更新されると共に、指定されたアクションに従ってパケットが処理されます。PF5200 シリーズは従来の L2/L3 スイッチング機能をサポートしており、OpenFlow インタフェース以外から入力されたパケットは、L2/L3 スイッチング機能により、処理されます。OpenFlow 機能と共に存在できる L2/L3 スイッチング機能については、「5.3.3 OpenFlow と L2/L3 スイッチング機能の共存」を参照してください。

5. OpenFlow 機能の解説

図 5-6 PFS の構造



- ① OpenFlow インタフェースから入力
② OpenFlow インタフェース以外から入力
③ OpenFlow インタフェースから入力され、フロー テーブルで L2/L3 スイッチでの処理を指定

(注) [3] の様に L2/L3 スイッチでの処理を指定するアクションもあります。詳細は、「5.2.4 アクションの解説」を参照してください。

5.1.5 PFS の OpenFlow 機能

本装置のサポートする OpenFlow 機能について、以下に示します。

本機能は OpenFlow の仕様に基づいていますが、OFC を含めたシステムとして実際に使用できる機能は、OFC との組み合わせで決まります。また、本装置の接続動作の保証対象となる OFC は、NEC 製品の PFC(ProgrammableFlow Controller) になります。

(1) OpenFlow スイッチインスタンス

本装置は、RSI (Real Switch Instance) モードと VSI (Virtual Switch Instance) モードで動作できます。RSI モードでは 1 個、VSI モードでは 16 個の OpenFlow スイッチインスタンスを作成できます。RSI と VSI は混在できません。詳細は、「5.2.1 OpenFlow スイッチインスタンスの解説」を参照してください。

(2) OpenFlow インタフェース

RSI では、OpenFlow インタフェースとして、ポートまたはリンクアグリゲーションインターフェースを指定することができます。リンクアグリゲーションインターフェースに所属するポートを、直接指定することも可能です。RSI では、l2-inband-secure-channel コマンドで指定したポートとリンクアグリゲーションインターフェースにおいて、特定の VLAN のパケットを OpenFlow フローエントリによる制御対象から除外することができます。除外したポート・リンクアグリゲーションインターフェースは L2/L3 スイッチング機能で動作します。

VSI では、openflow-vlan コマンドで指定した VLAN に含まれるポート・リンクアグリゲーションインターフェースすべてが、OpenFlow インタフェースとして動作します。ただし、リンクアグリゲーションインターフェースに所属するポートは含まれません。

(3) OFC 接続機能

本装置には、OpenFlow スイッチインスタンスあたり最大 4 個の接続先 OFC を設定することができます。OFC とスイッチインスタンスとの間の接続は、Secure Channel と呼びます。OpenFlow プロトコルメッセージは、Secure Channel を通して送受信を行います。また、Secure Channel 接続性確認機能をサポートしています。OFC との接続が切断されると再接続を試み、それでも再接続できない場合は別の OFC との接続を試みます。詳細は、「5.2.5 Secure Channel の解説」を参照してください。

(4) フロー統計モード

本装置は、フロー毎の受信パケット数と受信オクテット数の統計を収集できます。装置単位で、パケットとオクテットの両方か、あるいはどちらか一方のみの統計収集を指定できます。詳細は、「5.2.14 統計情報の解説」を参照してください。

(5) フローテーブル

本装置のフローテーブルは主に 3 つのグループに分類されます。1 つは基本グループで normal1 フローテーブル、expanded フローテーブル、normal2 フローテーブル、software フローテーブルの合計 4 個のフローテーブルが基本グループに属します。もう 1 つは可視化グループで vnormal1 フローテーブル、vexpanded フローテーブル、vnormal2 フローテーブルの合計 3 個のフローテーブルが可視化グループに属します。もう 1 つは QoS グループで qnormal1 のフローテーブルが QoS グループに属します。また、どのグループにも属しない emergency フローテーブルが存在し、装置全体で合計 8 個のフローテーブルを持ちます。

基本グループに属する normal1 フローテーブル、expanded フローテーブル、normal2 フローテーブル上のフローエントリにおいて、ハードウェアがサポートしているアクションのみを指定した場合には、そのフローエントリにヒットしたパケットはハードウェアにて高速に処理されます。基本グループに属する software フローテーブル上のフローエントリにヒットしたパケットは、すべてソフトウェアで処理されます。可視化グループに属するフローテーブルは、フローの統計情報を取得する為のフローエントリを登録するので経路の制御には使用されません。emergency フローテーブルは、Emergency モード時に用いるフローエントリを管理するフローテーブルです。詳細は、「5.2.2 フローテーブルの解説」を参照してください。

(6) ポート状態制御機能

OpenFlow プロトコルメッセージを用いて、OpenFlow インタフェースに対し、リンクアップ・ダウン等の OpenFlow インタフェース設定を変更することができます。更に、VSI モードでは、各 VSI に対して、OpenFlow インタフェース設定をすることができます。ただし、リンクアグリゲーションインターフェースに対しリンクダウン設定を行った場合、リンクアグリゲーションインターフェースに登録されている全ての物理ポートは、アップ状態のまま通信停止状態となります。詳細は、「5.2.9 (1) 対象インターフェース」を参照してください。

(7) Emergency モード対応

本装置は、OpenFlow Switch Specification で規定された Emergency モードをサポートします。いずれの OFC にも接続が不可能と判断した場合、emergency フローテーブルに登録されたフローエントリを normal1 フローテーブルに上書きします。本機能は、emergency-mode disable コマンドによって無効化することも可能です。詳細は、「5.2.7 Emergency モードの解説」を参照してください。

(8) フローテーブル検索にヒットしなかった時のパケット制御機能

OpenFlow インタフェースから入力されたパケットが、対応する OpenFlow スイッチインスタンスの持ついずれのフローエントリにもヒットしなかった場合の処理は、本装置では下記の 2 通りの動作のうち 1 つを選択することができます。

- OpenFlow プロトコルの Packet In メッセージを使用して、OFC にそのパケットを送信します。
miss-action コマンドで controller を設定した場合に、この動作を行います。
OpenFlow Switch Specification で規定されている動作で、本装置のデフォルト設定となります。
- 従来の L2/L3 スイッチング機能によりパケットを処理します。
miss-action コマンドで normal を設定した場合に、この動作を行います。

(9) MAC アドレス学習制御機能

OpenFlow スイッチインスタンス毎に、mac-learning コマンドを用いて、MAC アドレス学習を行うか行わないかを指定することができます。

(10) 出力インターフェースの VSI ポリシング機能

VSI モードの場合、outbound コマンドを用いて、トランクポートにおいて VSI 每の送信帯域を制限するポリシングを行うことができます。

(11) L2/L3 スイッチング機能

OpenFlow インタフェース以外から入力されたパケットは、従来の L2/L3 スイッチング機能により処理を行います。

(12) マルチヒット機能

フローエントリを 3 つの論理グループ（基本グループと可視化グループと QoS グループ）に分類して保持し、1 つの検索対象パケットに対して論理グループ毎に並行して検索とアクション実行を行うことができます。

5.2 OpenFlow 機能の解説

5.2.1 OpenFlow スイッチインスタンスの解説

本装置で生成可能な OpenFlow スイッチインスタンスには、RSI (Real Switch Instance) と VSI (Virtual Switch Instance) の 2 種類があります。それぞれの概要図を図 5-7、図 5-8 に示します。

図 5-7 RSI 概要図

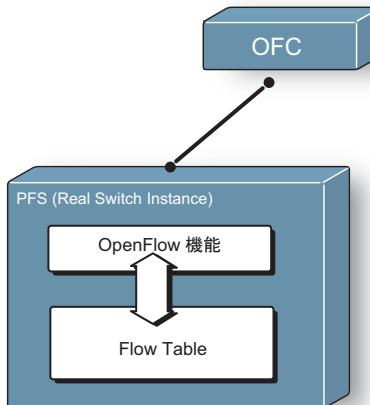
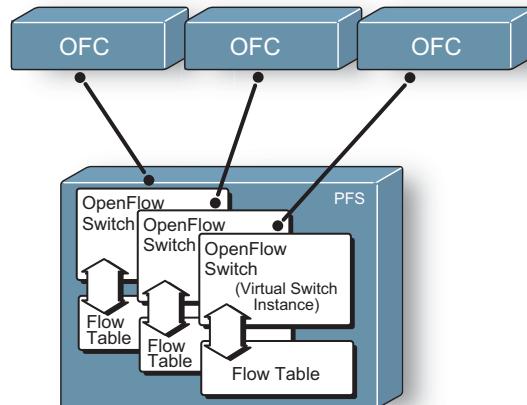


図 5-8 VSI 概要図



(1) Real Switch Instance (RSI)

RSI モードは、L2/L3 スイッチング機能が基本として動作しており、そこに OpenFlow 機能を付加機能として配置し、ネットワークのフロー制御を行うネットワークモデルです。L2/L3 スイッチング機能が動作するネットワークと同じネットワーク上に OpenFlow 機能が動作し、OpenFlow ネットワークと既存ネットワークはオーバーレイされて動作します。RSI では、OpenFlow インタフェースとして、ポート・リンクアグリゲーションインターフェースを指定することができます。リンクアグリゲーションインターフェースに所属するポートを直接指定することも可能です。パケットが OpenFlow インタフェースから入力された場合には RSI で処理され、それ以外から入力された場合には L2/L3 スイッチング機能により処理されます。RSI モード使用時は、トネリング VLAN 機能は使用できません。

(2) Virtual Switch Instance (VSI)

VSI モードは、物理的にはネットワークを共有していますが、L2/L3 スイッチング機能を OpenFlow 機能とは異なる VLAN で使用するため、論理的には L2/L3 スイッチング機能と OpenFlow 機能が分離しているネットワークモデルです。

独立した OpenFlow ネットワークごとに 1 グループ（1 台、もしくはクラスタリングされた OFC グループ）で、OpenFlow ネットワークのフロー制御を行います。PFS 上には、16 個までの VSI を動作させることができます。VSI を 1 個のみ動作させた場合でも、RSI とは異なるモデルとなります。VSI では、openflow-vlan コマンドで指定した VLAN に含まれるポート・リンクアグリゲーションインターフェースすべてが OpenFlow インタフェースとして動作します。ただし、リンクアグリゲーションインターフェースに所属するポートは含まれません。OpenFlow インタフェースとして識別される組み合わせを以下に示します。

- VLAN と入力ポートの組み合わせ

5. OpenFlow 機能の解説

- VLAN とリンクアグリゲーションインターフェースの組み合わせ

VSI の OpenFlow インタフェースは、ある VLAN に閉じており、基本的に別の VLAN との通信は行うことはできません。L2/L3 スイッチング機能で L3 転送を使用する場合に限り、異なる VLAN 間で通信することが可能です。VSI は、指定した VLAN で受信したパケットのみを扱います。いずれの VSI にも設定されていない VLAN で受信したパケットは、L2/L3 スイッチング機能により処理されます。

5.2.2 フローテーブルの解説

フローテーブルは、「表 5-1 フローエントリの構成要素」を持つフローエントリで構成されます。

表 5-1 フローエントリの構成要素

#	要素	意味
1	検索キー	フローを検索する際のキー情報
2	アクション	フローに対する動作（複数指定可能）
3	統計	フロー毎の統計情報（パケット数、オクテット数）
4	フロークッキー	フローエントリ毎に保持している 64bit の識別子

フローエントリは、指定された検索キーフィールドに従って、下記の 2 種類に分類されます。また、検索キーフィールドの詳細を「表 5-2 フローの検索キー」に示します。

- Wildcard 指定フローエントリ

「表 5-2 フローの検索キー」に示した検索キーフィールドの一部またはすべてに any 指定があるもの。※一部指定可能な検索キーは、IP アドレスと MAC アドレス、ICMP-Type と ICMP-Code、L4 ポート番号です。

- Exact 指定フローエントリ

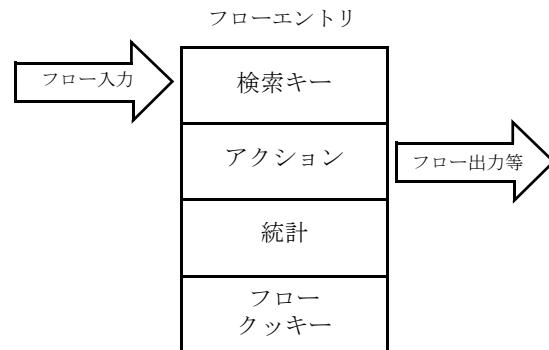
「表 5-2 フローの検索キー」に示した検索キーフィールドに any 指定が無いもの。

表 5-2 フローの検索キー

分類	フィールド
物理インターフェース	入力ポート番号
イーサネット	宛先 MAC アドレス、送信元 MAC アドレス、VLAN ID、IEEE802.1D の User Priority、Ethernet-type
ARP	宛先 IP アドレス、送信元 IP アドレス、ARP opcode
IPv4	宛先 IP アドレス、送信元 IP アドレス、プロトコル、ToS(DSCP) 値
IPv6	宛先 IP アドレス、送信元 IP アドレス
ICMP	ICMP Type、ICMP Code
TCP/UDP	宛先ポート番号、送信元ポート番号

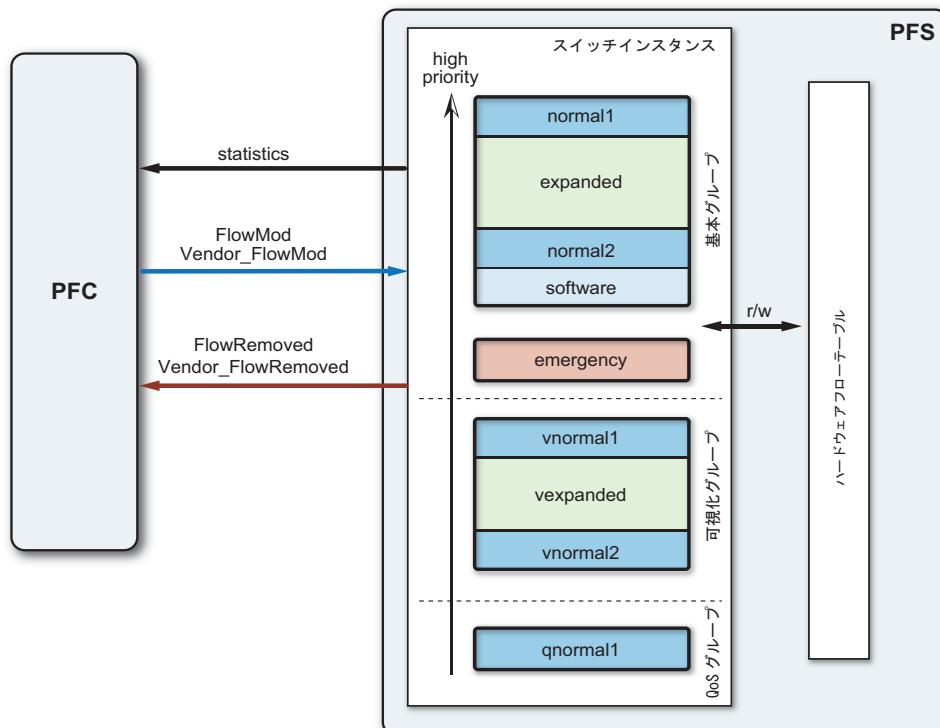
本装置は、パケットを受信するとフローテーブルを検索します。受信パケットと一致するフローエントリが検出された場合には、フローエントリに指定されたアクションに従ってパケット処理を行います（「図 5-9 OpenFlow のパケット処理」を参照）。受信パケットと一致するフローエントリが見つからなかった場合の動作は、「5.1.5 (8) フローテーブル検索にヒットしなかった時のパケット制御機能」を参照してください。

図 5-9 OpenFlow のパケット処理



本装置のフローテーブル構成を次に解説します。スイッチインスタンスごとに、ハードウェアに登録されたフロー エントリを管理する基本グループの normal1, expanded, normal2 フローテーブル、ソフトウェア上で検索を行う基本グループの software フローテーブル、Emergency モード時に用いるフロー エントリを管理する emergency フローテーブル、フローの統計情報を取得することができる可視化グループの vnormal1, vexpanded, vnormal2、検索結果のフローに対して QoS に関するアクションをサポートする QoS グループの qnormal1 フローテーブルで構成されています。miss-action コマンドで normal を設定した場合、software フローテーブルは使用できません。emergency フローテーブルは、Emergency モード時のためのフローテーブルで、通常の転送には使用されません。また、emergency-mode disable コマンドで、Emergency モードを無効に設定した場合、emergency フローテーブルは使用できません。Emergency モードについては、5.2.7 Emergency モードの解説を参照してください。フローテーブル構成とフロー エントリの操作を「図 5-10 フローテーブル構成図」に示します。

図 5-10 フローテーブル構成図



次に、本装置のフローテーブルの検索順序について解説します。

基本グループの `normal1` フローテーブル、`expanded` フローテーブル、`normal2` フローテーブル、`software` フローテーブルでは、`normal1` フローテーブルの方が常に検索優先度が高くなります。本装置は、OFC が Flow Mod メッセージによってフローエントリを登録する際に、指定された検索優先度に従って、フローエントリを `normal1` フローテーブル、`expanded` フローテーブル、`normal2` フローテーブル、`software` フローテーブルに振り分けます。

可視化グループの `vnormal1` フローテーブル、`vexpanded` フローテーブル、`vnormal2` フローテーブルでは、`vnormal1` フローテーブルの方が常に検索優先度が高くなります。本装置は、OFC が Flow Mod メッセージによってフローエントリを登録する際に、指定されたテーブル ID に従って、フローエントリを `vnormal1` フローテーブル、`vexpanded` フローテーブル、`vnormal2` フローテーブルに振り分けます。

基本グループのフローテーブルの振り分け基準となる検索優先度の境界値は、OpenFlow スイッチインスタンス毎に `table` コマンドで設定できます。また、Vendor 拡張 Flow Mod メッセージでは、テーブル ID を指定する事が出来る為、フローテーブルを選択してフローエントリを登録することが可能です。

Vendor 拡張 Flow Mod メッセージを使用してフローエントリを登録する際は、`table` コマンドで設定された各フローテーブルの検索優先度の境界値に関わらず、全ての検索優先度のフローが登録可能となります。

基本、可視化、QoS 各グループの機能比較を「表 5-3 基本グループと可視化グループと QoS グループのフローテーブルの機能」に示します。

基本グループおよび、可視化グループ内のフローエントリの検索順序を「図 5-11 基本グループにおける各フローテーブルの検索順序」、「図 5-12 可視化グループにおける各フローテーブルの検索順序」に示します。

また、各フローテーブル内に登録されているフローエントリの検索順序を「図 5-13 フローテーブル内のフロー検索順序」に示します。フローテーブルの検索をするとき、Exact 指定フローエントリを検索した後、Wildcard 指定フローエントリを検索します。さらに、Wildcard 指定フローエントリは、検索優先度の大きいエントリから順に検索します。検索優先度値は、0（最小値）から 65535（最大値）の範囲となります。但し `expanded` フローテーブルで利用可能な検索優先度の値は最大で 64 種類となります。

検索優先度値が同一の Wildcard 指定フローエントリが複数存在する場合、検索順は保証しません。

`qnormal1` フローテーブルのアクションが基本グループのフローテーブルのアクションと競合した場合、基本グループのフローテーブルのアクションが優先されます。

表 5-3 基本グループと可視化グループと QoS グループのフローテーブルの機能

グループ	名称	テーブル ID	検索順	検索速度	H/W フロー エントリ	転送方法
基本グループ	normal1	#0	1	高速	消費する	ハードウェア (*1) またはソフトウェア
	expanded	#1	2			
	normal2	#20	3			
	software	#99	4		消費しない	ソフトウェア
可視化グループ	vnormal1	#100	1	高速	消費する	対象外
	vexpanded	#101	2			
	vnormal2	#120	3			
QoS グループ	qnormal1	#140	1	高速	消費する	ハードウェア

(*1) : ハードウェア転送可能なアクションが設定されている場合のみハードウェア転送を行ないます。

図 5-11 基本グループにおける各フローテーブルの検索順序

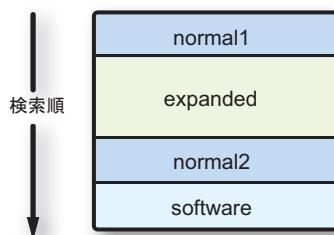


図 5-12 可視化グループにおける各フローテーブルの検索順序

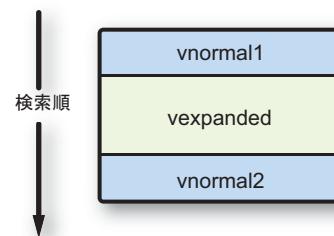
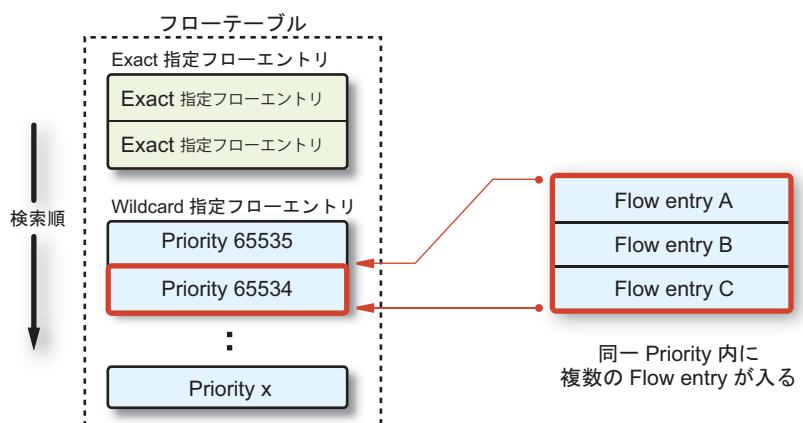


図 5-13 フローテーブル内のフロー検索順序



5.2.3 マッチ条件の解説

本装置でフローエントリを登録する際の、フローエントリの例について、「表 5-4 フロー識別条件の VLAN ID による登録判定 (RSI)」、「表 5-5 フロー識別条件の VLAN ID による登録判定 (VSI)」に示します。

表 5-4 フロー識別条件の VLAN ID による登録判定 (RSI)

検索キーフィールド (入力ポート)	検索キーフィールド (VLAN ID)	判定	受信可能パケット
ポート VLAN	アクセスポート	Any	○ untagged パケット
		0xffff(untagged)	○ untagged パケット
		上記以外	○ —
	トランクポート	Any	○ 全パケット
		VLAN ID	○ tagged パケット
		0xffff(untagged)	○ untagged パケット
		上記以外	○ —

表 5-5 フロー識別条件の VLAN ID による登録判定 (VSI)

検索キーフィールド (入力ポート)	検索キーフィールド (VLAN ID)	判定	受信可能パケット
ポート VLAN	アクセスポート	Any	○ untagged パケット
		0xffff(untagged)	○ untagged パケット
		上記以外	× (*1) —
	トランクポート	Any	○ 全パケット
		VLAN ID	○ tagged パケット
		0xffff(untagged)	○ untagged パケット
		上記以外	× (*1) —
トンネル VLAN	トンネリングポート	Any	○ 全パケット
		0xffff(untagged)	○ untagged パケット
		上記以外	○ tagged パケット
	トランクポート	Any	○ tagged, 2 段 tagged パケット
		0xffff(untagged)	○ tagged パケット
		上記以外	○ 2 段 tagged パケット

(*1) : フローエントリとして登録することは出来ますが、登録しないでください。

5.2.4 アクションの解説

アクションとは、フローが「表 5-2 フローの検索キー」に示した検索キーにマッチした場合に行う、フローに対する動作です。1 つのフローに対して、複数のアクションを指定することができます。転送アクション（OUTPUT および ENQUEUE）を 1 つも含まない場合は、廃棄動作とみなします。

表 5-6 フローエントリに設定可能なアクション

アクション名	アクションの内容	動作可能パケット
OUTPUT	指定したポートに出力します。	すべて
ENQUEUE	出力先ポート番号とキュー番号を指定し、指定された優先度で指定されたポートに出力します。	すべて
SET_VLAN_VID	VLAN ID を変更または追加します。（*1）	すべて
SET_VLAN_PCP	VLAN タグ内のユーザプライオリティ（*2）を変更します。	tagged パケット
STRIP_VLAN	VLAN タグを削除します。	すべて
SET_DL_SRC	送信元 MAC アドレスを変更します。	すべて
SET_DL_DST	宛先 MAC アドレスを変更します。	すべて
SET_NW_SRC	送信元 IP アドレスを変更します。	IPv4 パケット
SET_NW_DST	宛先 IP アドレスを変更します。	IPv4 パケット
SET_NW_TOS	IP ToS (DSCP) を変更します。	IPv4 パケット
SET_TP_SRC	送信元 L4 ポートを変更します。	TCP または UDP のパケット
SET_TP_DST	宛先 L4 ポートを変更します。	TCP または UDP のパケット

（*1）：（3）VLAN タグ変換（SET_VLAN_VID / STRIP_VLAN）参照

（*2）：IEEE802.1D の Priority を示します。

「表 5-6 フローエントリに設定可能なアクション」に示した各アクションの動作を次に説明します。

（1）出力ポート指定（OUTPUT）

OUTPUT アクションでは、出力ポートの指定として、「表 5-7 出力ポートとして利用可能なポート」に示すポートを指定することができます。

（2）出力ポートと優先度指定（ENQUEUE）

ENQUEUE アクションでは、出力ポートの指定として、「表 5-7 出力ポートとして利用可能なポート」に示すポートを指定することができます。さらに、キュー番号を指定し、優先度制御を行うことができます。

表 5-7 出力ポートとして利用可能なポート

ポート名	意味	H/W（*3）	S/W（*4）
ポート番号（*1）	指定した番号のポートへ出力します。	○	○
IN_PORT	パケットを受信したポートへ出力します。	○	○
NORMAL	PF5200 シリーズの L2/L3 スイッチング機能を使用して、パケットを転送します。	○	×

ポート名	意味	H/W(*3)	S/W(*4)
FLOOD	パケットを受信したポートと OpenFlow 上で NO_FLOOD 設定にしているポートを除く、すべてのポートへ出力します。	×	○
ALL	パケットを受信したポート以外のすべてのポートへ出力します。	○	○
CONTROLLER	Secure Channel を経由して、OFC 宛てにパケットを転送します。	○	○
LOCAL	スイッチ内部のプロトコルスタックで終端処理を行います。	△ (*2)	△ (*2)
TABLE	フローテーブル検索にかけます。	×	△ (*5)

(*1) : 「5.2.11 (1) 対象インターフェース」参照

(*2) : IPv4・IPv6・ARP パケットのみを受信します。

(*3) : ハードウェア転送

(*4) : ソフトウェア転送

(*5) : Packet Out メッセージ専用で、フローエントリとしての使用不可

(3) VLAN タグ変換 (SET_VLAN_VID / STRIP_VLAN)

SET_VLAN_VID アクションでは、VLAN タグの変更または追加を行います。untagged パケットに対しては、VLAN プライオリティ = 3 として、指定された VLAN ID の VLAN タグを追加します。

STRIP_VLAN アクションでは、VLAN タグの削除を行います。STRIP_VLAN アクションで削除できる VLAN タグは 1 個のみで、STRIP_VLAN アクションを複数指定して複数の VLAN タグを削除することはできません。

VLAN タグ変換アクションを指定したフローエントリ登録には装置側のコンフィグレーションにより、RSI モード、VSI モードそれぞれ、表 5-8、表 5-9 のような条件があります。

表 5-8 VLAN タグ変換アクションとフローエントリ登録の対応 (RSI)

VLAN モード	VLAN ポート種別 (出力インターフェース)	送信パケット種別	RSI による 対象 VLAN	指定可能 VLAN アクション
ポート VLAN	アクセスポート	untagged パケット	native VLAN	STRIP_VLAN
	トランクポート	untagged パケット	native VLAN	STRIP_VLAN
		tagged パケット	tag VLAN	SET_VLAN_VID
トンネル VLAN	非対応			

表 5-9 VLAN タグ変換アクションとフローエントリ登録の対応 (VSI)

VLAN モード	VLAN ポート種別 (出力インターフェース)	送信パケット種別	VSI による 操作対象 VLAN	指定可能 VLAN アクション
ポート VLAN	アクセスポート	untagged パケット	制御対象なし	なし(指定不可)(*1)
	トランクポート	untagged パケット	制御対象なし	なし(指定不可)(*1)
		tagged パケット	制御対象なし	なし(指定不可)(*1)

5. OpenFlow 機能の解説

VLAN モード	VLAN ポート種別 (出カインタフェース)	送信パケット種別	VSIによる 操作対象 VLAN	指定可能 VLAN アクション
トンネル VLAN	トンネリングポート	untagged パケット	native VLAN	STRIP_VLAN
		tagged パケット	tag VLAN	SET_VLAN_VID
	トランクポート	untagged パケット	不定	不使用推奨 (*1)
		tagged パケット	native VLAN	STRIP_VLAN
		2段 tagged パケット	inner VLAN	SET_VLAN_VID

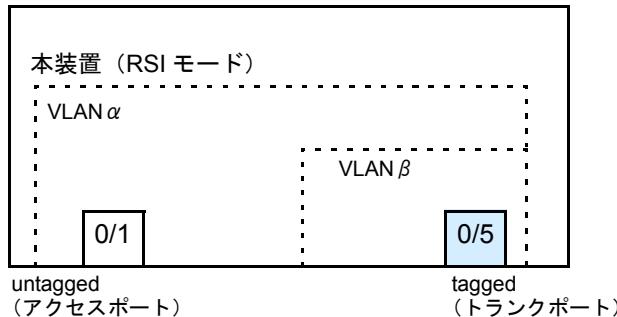
(*1) : VSIにおける VLAN トンネリングモードでの untagged パケットは送信可能ですが、受信する際に tag が付いていないと別の OpenFlow スイッチインスタンスに受信されてしまう可能性があります。そのため、native VLAN は停止状態にしておくことを推奨します。

なお、受信パケットと同じ VLAN タグの tagged パケットを送信する場合、および untagged パケットを受信して untagged パケットを送信する場合には、VLAN タグ変換アクションを指定しなくても送信可能です。

また、受信時の VLAN ID と異なる VLAN ID に対する転送でも、PF5200 シリーズの L2/L3 スイッチング機能で設定しているコンフィグレーション情報と一致していれば転送が可能です。

例として図 5-14 のようなインターフェース設定状態における RSI モードでの VLAN タグ変換アクションを持つフローエントリ登録方法について示します。

図 5-14 VLAN タグ書き換えアクション説明図



RSI モードにおいて、「図 5-14 VLAN タグ書き換えアクション説明図」のように、PF5200 シリーズの L2/L3 スイッチでのポート 0/1 を VLAN α のアクセスポート、ポート 0/5 を VLAN α と VLAN β のトランクポートに設定した場合、「表 5-10 VLAN タグ変換アクションによるフローエントリ登録判定(図 5-13 構成)」のように判定を行います。

表 5-10 VLAN タグ変換アクションによるフローエントリ登録判定(図 5-13 構成)

検索キーフィールド (入力ポート番号)	OUTPUTアクション	VLAN タグ変換アクション	判定	送信パケット
0/1 (アクセスポート)	0/5 (トランクポート)	なし	○	untagged パケット
		STRIP_VLAN	○	untagged パケット
		SET_VLAN_VID α または β	○	tagged パケット
			×	—
		上記以外	—	—

検索キーフィールド (入力ポート番号)	OUTPUTアクション	VLAN タグ変換アクション	判定	送信パケット
0/5 (トランクポート)	0/1 (アクセスポート)	なし	○	untagged パケット
		STRIP_VLAN	○	untagged パケット
		SET_VLAN_VID	×	—

「表 5-10 VLAN タグ変換アクションによるフローエントリ登録判定(図 5-13 構成)」は、それぞれ以下に示すような動作をします。

1. 検索キーフィールドの入力ポート番号が 0/1, OUTPUT アクションの物理ポートが 0/5 の場合

- VLAN タグ変換アクションが指定されていない場合および VLAN タグ変換アクションが STRIP_VLAN の場合は、出力ポートである物理ポート 0/5 に native VLAN が設定されていれば、OFC から登録されるフローエントリと PF5200 シリーズの L2/L3 スイッチング機能で設定しているコンフィグレーション情報との間で不一致が発生しないため、フローテーブルにフローエントリを登録します。
- VLAN タグ変換アクションが SET_VLAN_VID で値が α または β の場合は、OFC から登録されるフローエントリと PF5200 シリーズの L2/L3 スイッチング機能で設定しているコンフィグレーション情報との間で不一致が発生しないため、フローテーブルにフローエントリを登録します。
- VLAN タグ変換アクションが SET_VLAN_VID で値が α または β 以外の場合は、OFC から登録されるフローエントリと PF5200 シリーズの L2/L3 スイッチング機能で設定しているコンフィグレーション情報との間で不一致が発生するため、登録判定結果はエラーとなります。フローエントリ登録は行わず、Error メッセージを返します。

2. 検索キーフィールドの入力ポート番号が 0/5, OUTPUT アクションの物理ポートが 0/1 の場合

- VLAN タグ変換アクションが指定されていない場合は、入力ポート 0/5 に native VLAN が設定されていれば、OFC から登録されるフローエントリと PF5200 シリーズの L2/L3 スイッチング機能で設定しているコンフィグレーション情報との間で不一致が発生しないため、フローテーブルにフローエントリを登録します。
- VLAN タグ変換アクションが STRIP_VLAN の場合は、OFC から登録されるフローエントリと PF5200 シリーズの L2/L3 スイッチング機能で設定しているコンフィグレーション情報との間で不一致が発生しないため、フローテーブルにフローエントリを登録します。
- VLAN タグ変換アクションが SET_VLAN_VID の場合は、OFC から登録されるフローエントリと PF5200 シリーズの L2/L3 スイッチング機能で設定しているコンフィグレーション情報との間で不一致が発生するため、登録判定結果はエラーとなります。フローエントリ登録は行わず、Error メッセージを返します。

(4) VLAN プライオリティ変換 (SET_VLAN_PCP)

SET_VLAN_PCP アクションでは、VLAN タグ内のプライオリティ値を変更します。転送アクションで指定されたポートがアクセスポートであった場合、出力されるパケットには VLAN タグが付かないため、VLAN プライオリティを追加しません。

(5) 送信元 MAC アドレス変更 (SET_DL_SRC)

SET_DL_SRC アクションでは、送信元 MAC アドレスを変更します。

5. OpenFlow 機能の解説

(6) 宛先 MAC アドレス変更 (SET_DL_DST)

SET_DL_DST アクションでは、宛先 MAC アドレスを変更します。

(7) 送信元 IP アドレス変更 (SET_NW_SRC)

SET_NW_SRC アクションでは、IPv4 パケットの送信元 IP アドレスを変更します。

(8) 宛先 IP アドレス変更 (SET_NW_DST)

SET_NW_DST アクションでは、IPv4 パケットの宛先 IP アドレスを変更します。

(9) IP ToS (DSCP) 変更 (SET_NW_TOS)

SET_NW_TOS アクションでは、IPv4 パケットの ToS(DCSP) を書き換えます。

(10) 送信元 L4 ポート変更 (SET_TP_SRC)

SET_TP_SRC アクションでは、TCP または UDP パケットの送信元 L4 ポートを変更します。

(11) 宛先 L4 ポート変更 (SET_TP_DST)

SET_TP_DST アクションでは、TCP または UDP パケットの宛先 L4 ポートを変更します。

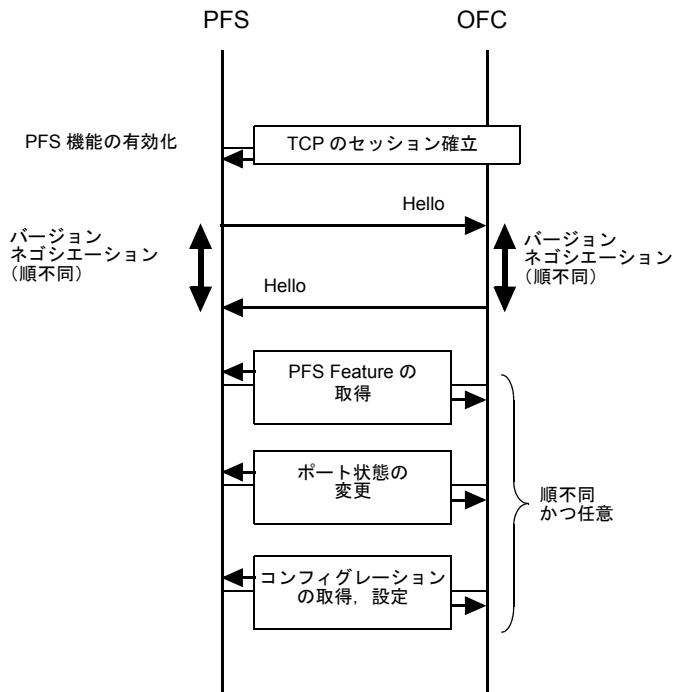
5.2.5 Secure Channel の解説

Secure Channel は、OFC と PFS の間で接続される制御用経路であり、OpenFlow プロトコルメッセージのやり取りに使用されます。OpenFlow スイッチインスタンスごとに、同時接続数 1 本の Secure Channel 接続能力を持ちます。OpenFlow スイッチインスタンス 1 つあたり 4 台までの OFC の IP アドレス・ポート番号を設定でき、OFC への接続が不可能と判断した場合は、異なる OFC への接続を試みます。Secure Channel の動作について、次に説明します。

(1) Secure Channel の確立

PFS は、OpenFlow 機能を有効にしたときに OFC に対し、Secure Channel の接続を開始します。Secure Channel は TCP セッション上に構築されます。「図 5-15 Secure Channel 確立シーケンス」に、Secure Channel 確立時のシーケンス図を示します。(2) 以降の処理は、Secure Channel 確立後の標準的な処理ですが、確立条件とはなりません。

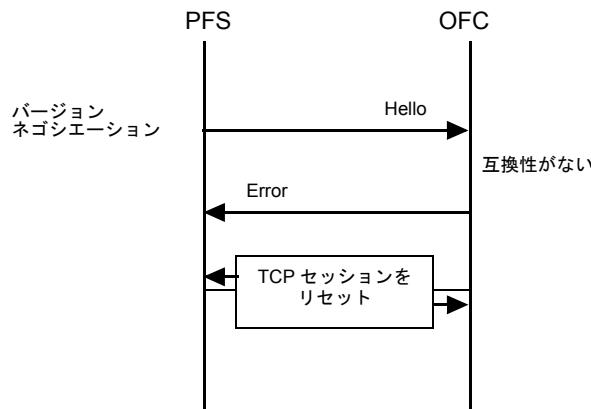
図 5-15 Secure Channel 確立シーケンス



(a) OpenFlow プロトコルバージョンネゴシエーション

TCP セッション確立後、直ちに OFC へ Hello メッセージを送信します。バージョンネゴシエーションが完了した後に、Secure Channel の接続が確立します。バージョンネゴシエーションの結果、サポートしているバージョンではなかった場合、Error メッセージを送信します。バージョンネゴシエーション時に OFC から Error メッセージを受信した場合は、TCP セッションをリセットします。バージョンネゴシエーション失敗時のシーケンスを「図 5-16 バージョンネゴシエーション失敗時のシーケンス」に示します。

図 5-16 バージョンネゴシエーション失敗時のシーケンス



(b) PFS Features 確認

OFC からの Features Request メッセージに対し、Features Reply メッセージを送信します。詳細は「5.2.12 OpenFlow プロトコル Features 通知機能の解説」を参照してください。

(c) ポート状態変更

OFC からの Port Mod メッセージを受信した場合、その情報を PFS に反映させます。その結果ポート状態が変化した場合は、Port Status メッセージを送信します。詳細は「5.2.12 (2) ポート状態管理」を参照してください。

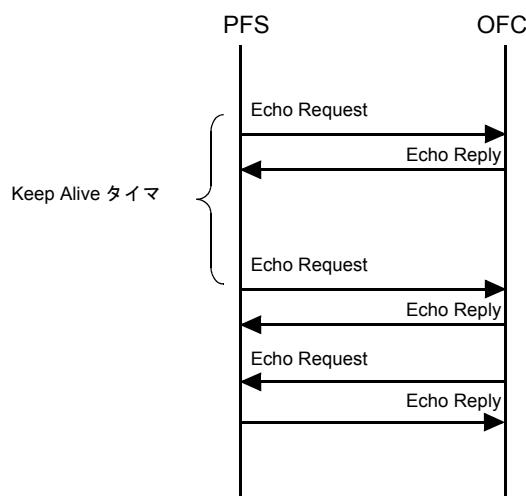
(d) コンフィグレーション確認

OFC からの Get Configuration Request メッセージに対し、Get Configuration Reply メッセージを送信します。OFC からの Set Configuration メッセージを受信した場合、そのコンフィグレーションを PFS に反映させます。詳細は「5.2.12 OpenFlow プロトコル Features 通知機能の解説」を参照してください。

(2) Secure Channel の接続性確認

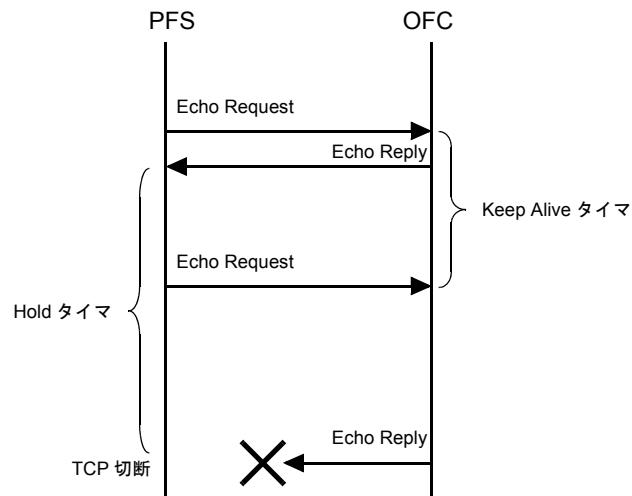
Secure Channel 確立後、PFS は OFC に対し、Keep Alive タイマに従い周期的に Echo Request メッセージを送信します。また、OFC から送信された Echo Request メッセージに対し、Echo Reply メッセージを送信します。本装置では、Keep Alive タイマの設定を echo-request interval コマンドで行うことができます。

図 5-17 Secure Channel の接続性確認シーケンス



PFS は、Echo Request メッセージ送信後、Hold タイマに設定した秒数だけ、OpenFlow プロトコルメッセージを待ちます。Hold 時間に内に OpenFlow プロトコルメッセージを受信した場合、PFS は Hold タイマのカウントダウンをリセットし、引き続き OpenFlow プロトコルメッセージを待ちます。Hold 時間に内に OpenFlow プロトコルメッセージを受信しなかった場合、PFS はセッションを切断します。装置では Hold タイマの設定を echo-reply timeout コマンドで行うことができます。

図 5-18 Secure Channel 障害時シーケンス

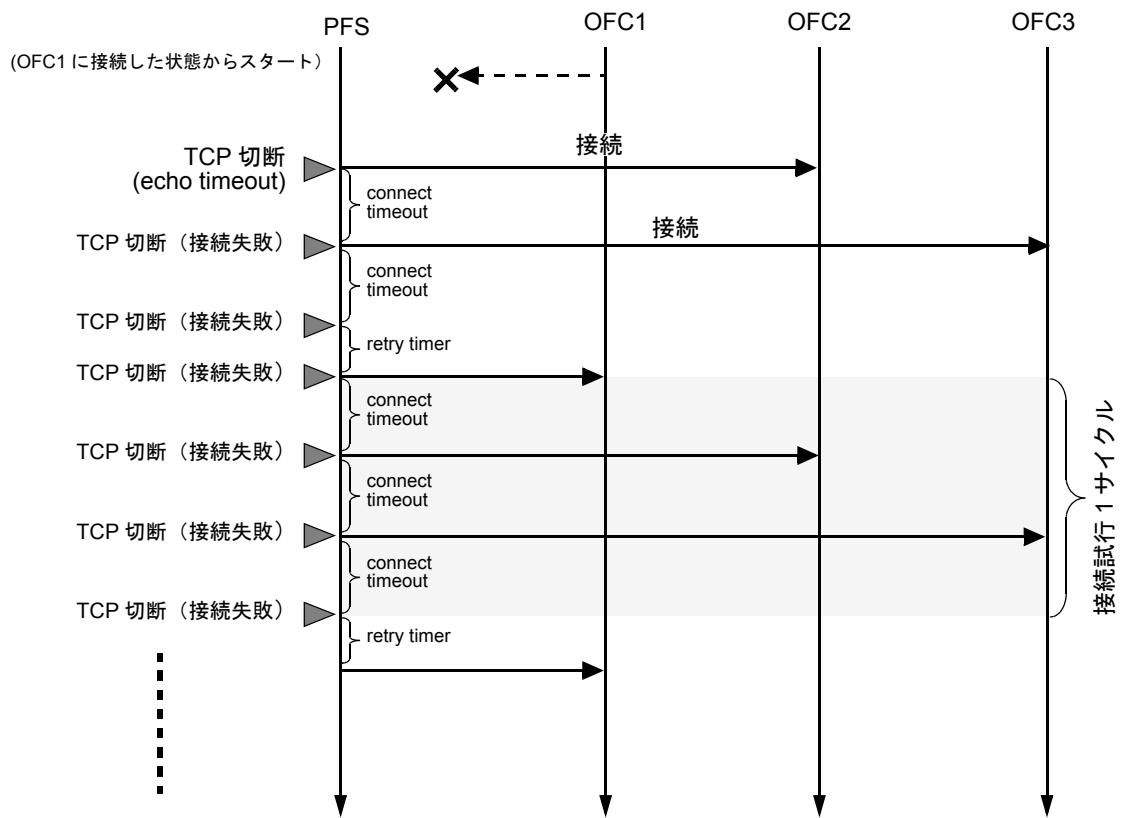


(3) Secure Channel 接続・再接続試行時の動作

Secure Channel が接続開始から Connect タイマで設定した秒数以内に接続を確立できなかった場合、その OFC への接続を切断します。TCP の 3way ハンドシェークが完了しない場合や、Hello が返ってこない場合などに、接続できないと判断します。Secure Channel が切断された場合は、Retry タイマ秒待ち、再接続を試みます。

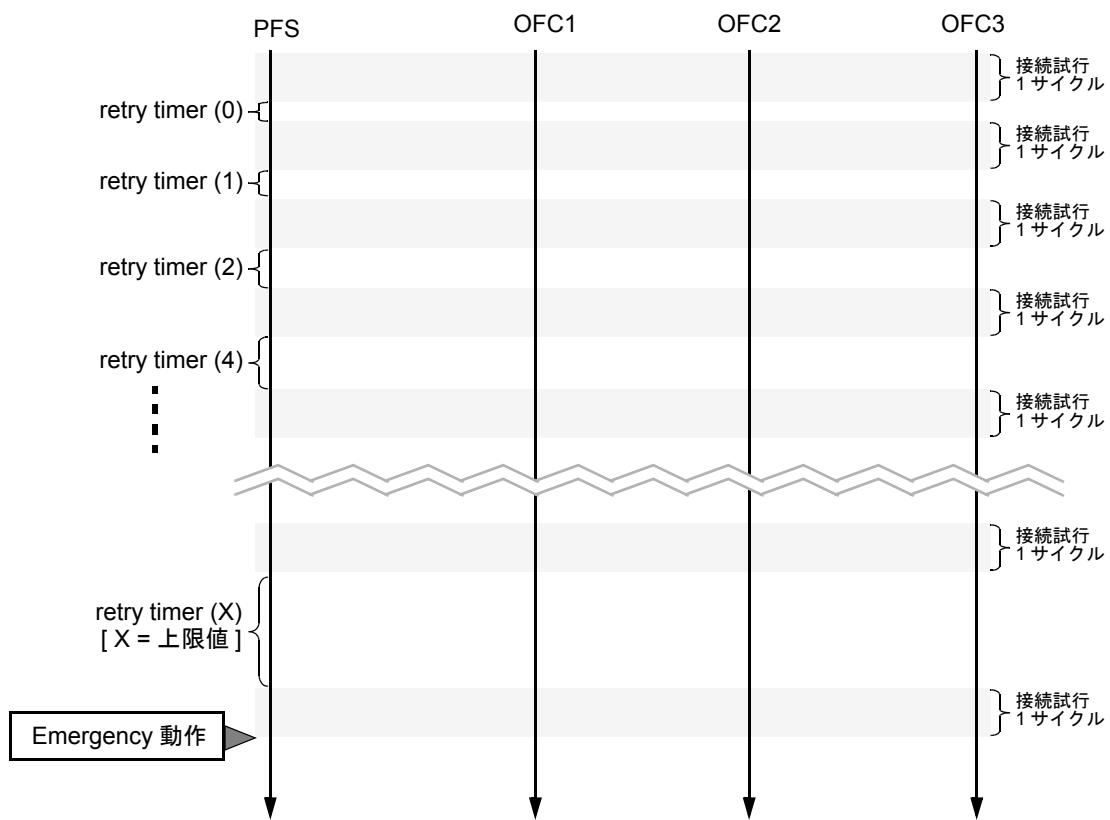
- Retry タイマは、接続に失敗する度に 0, 1, 2, 4... と、指定した最大値まで指数的に増加していきます。最大値を超えた場合は、その最大値を使用します。例えば、Retry タイマの最大値が 100 と設定された場合、64 秒の次が 100 秒となり、その後 100 秒を使用し続けます。
- Retry タイマは、正常に接続が行われると 0 にリセットされます。

図 5-19 Secure Channel 接続試行シーケンス



- Emergency モードへの移行を行うかどうかを、スイッチインスタンス毎にコンフィグレーションコマンドで設定できます。
- 設定されているすべての OFC への接続が不可能と判断した場合、Emergency モードが有効な設定であれば、Emergency モードへ移行します。Emergency モードへ移行するタイミングは、Retry タイマが最大値を超えたときです（「図 5-20 Emergency モードへの移行タイミング」を参照してください）。

図 5-20 Emergency モードへの移行タイミング



スイッチインスタンスの Data path ID が、異なる値に変更された場合には、Secure Channel を切断します。

(4) Secure Channel 切断時の動作

Secure Channel が切断された場合、下記の動作を行います。

- 「(3) Secure Channel 接続・再接続試行時の動作」と同様の手順で、OFC への再接続を試みます。
- Secure Channel 切断時には、OpenFlow のメッセージ送信は行いません。

詳細は「(5) Secure Channel 切断時のメッセージ処理」を参照してください。

(5) Secure Channel 切断時のメッセージ処理

Secure Channel が切断された状態では、OpenFlow プロトコルメッセージの送信は行いませんが、フローテーブルに設定されたフローエントリに従って、パケットは転送され続けます。ただし、ソフトウェア転送となるパケットは転送されません。

5.2.6 フローテーブル制御の解説

フローテーブルの制御方法について説明します。

(1) Flow Mod メッセージによるフローテーブル制御

OpenFlow プロトコルの Flow Mod メッセージを用いて、PFC より PFS にフローエントリの登録・変更・削除を要求します。

Flow Mod メッセージで制御できる動作一覧およびその動作内容について次に示します。

表 5-11 Flow Mod メッセージによるフローテーブル制御項目一覧

コマンド	意味
ADD	フローエントリを追加します
MODIFY	一致したフローエントリすべてを変更します
MODIFY_STRICT	完全一致したフローエントリ 1 個を変更します (*1)
DELETE	一致したフローエントリすべてを削除します
DELETE_STRICT	完全一致したフローエントリ 1 個を削除します

(*1) : インタフェースあたりのフローエントリ数が最大登録されている場合、MODIFY_STRICT は実行できません。エントリを削除して再登録してください。

(a) Flow Mod メッセージによるフローエントリの追加

- Flow Mod(ADD) にてフローエントリの追加を行います。
 - FlowMod(ADD) メッセージ受信時に、マッチ条件のフローエントリが既に存在する場合には、既存エントリを上書きします。この際、統計はリセットされ,flow_cookie,idle_timeout および hard_timeout は更新されます。なお、Exact match フローエントリは、すべて同じ検索優先度とみなされます。
- FlowMod(Modify/Modify Strict) メッセージの場合上記の動作は発生しません。

(b) Flow Mod メッセージによるフローエントリの変更

- Flow Mod (MODIFY・MODIFY_STRICT) メッセージにより、指定されたフローエントリのアクションを、メッセージ内で指定したものへと変更を行います。
- メッセージで指定されたフローエントリが存在しない場合には、メッセージ内で指定された情報を用いて、Flow Mod(ADD) の動作を行います。

(c) Flow Mod メッセージによるフローエントリの削除

- Flow Mod (DELETE・DELETE_STRICT) メッセージにより、フローエントリを削除します。指定されたフローエントリが存在せず削除ができない場合は、Error メッセージを出さず装置内に記録します。

(d) Flow Mod メッセージにおけるエラー処理

- フローテーブルにフローエントリを登録できない場合には、Error メッセージを OFC に送信します。Error メッセージのタイプおよびコード番号により、フローエントリ登録に失敗した原因を知ることができます。

(2) タイムアウトによるフローテーブル制御

PFS はフローテーブルの各フローエントリを周期的にチェックし、必要に応じてタイムアウト処理を行います。タイムアウトの種類とその処理について次に示します。

表 5-12 タイムアウトによるフローテーブル制御項目一覧

項目	意味
idle_timeout	無通信時間
hard_timeout	最大生存時間

(a) idle_timeout

- 最後にパケットがヒットしてから、idle_timeout(秒)が経過したフローエントリを削除します。
- idle_timeout に 0 が設定されているフローエントリは、削除を行いません。

(b) hard_timeout

- フローテーブルに登録されてから、hard_timeout(秒)が経過したフローエントリを削除します。
- hard_timeout に 0 が設定されているフローエントリは、削除を行いません。

(3) Vendor 拡張 FlowMod メッセージによるフローテーブル制御

本装置では、OpenFlow スペック Ver. 1.0.0 に準拠したフローエントリ検索条件をさらに拡張させ、検索条件の、MAC DA, MAC SA, IP DA, IP SA, L4 Dst Port, L4 Src Port(ICMP Code, ICMP Type) それぞれに対して、マスクビット(Wildcard Bit)を任意に指定することができます。これにより、さらに柔軟なフローテーブルの制御を実現できます。

拡張フローエントリの登録・変更・削除は、OpenFlow プロトコルメッセージである Vendor メッセージを用いて PFC より PFS に通知されます。「表 5-13 Vendor メッセージを用いた拡張フローエントリ」では、拡張フローエントリに関する Vendor メッセージについて解説します。また、フローエントリの登録時には、テーブル ID を指定することにより、エントリを登録するフローテーブルを選択することが可能です。

表 5-13 Vendor メッセージを用いた拡張フローエントリ

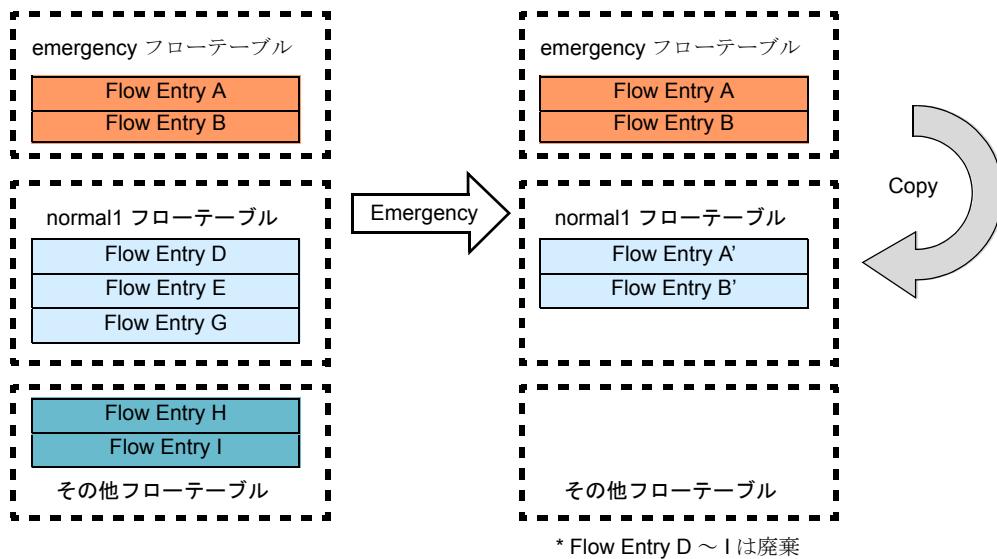
メッセージ	解説
Vendor FlowMod (Add/Mod/ModStrict/Del/DelStrict)	PFC より PFS に拡張フローエントリの追加・変更・削除が通知されます。検索条件それぞれに対して、wildcard を任意に指定可能です。フロー設定の操作は標準の Flow Mod メッセージと同様です。
Vendor FlowRemoved	Vendor FlowMod にて登録された拡張フローエントリが、PFS で削除された場合、PFS より PFC に通知されるメッセージです。

拡張フローエントリによるフローの統計情報は Statistics Request/Reply メッセージにより PFC に通知することができます。

5.2.7 Emergency モードの解説

Secure Channel が切断されたのち、再接続を試みたにも関わらず、設定されているすべての OFC への接続が不可能であると判断した場合、Emergency モードが有効な設定(no emergency-mode disable)であれば、Emergency モードへ移行します(「図 5-20 Emergency モードへの移行タイミング」を参照)。Emergency モードへ移行すると「図 5-21 Emergency モードが有効であるときの動作」のように、使用中のフローエントリを削除し、emergency フローエントリを転送用のフローテーブルにコピーして、パケット転送に用います。

図 5-21 Emergency モードが有効であるときの動作



Emergency モードへ移行すると、emergency フローテーブル内のフローエントリを normal1 フローテーブルにコピーします。Secure Channel が再び接続された際に、Emergency モードへ移行する前に有効であったフローエントリの再有効化等は行いません。

5.2.8 Emergency リンクダウン制御機能

PFS が PFC との接続が切れた状態では、OpenFlow インタフェースで受信するパケットを正しく処理できなくなります。このようなケースにおいて、本装置では対向ネットワークに異常状態を通知する手段として、障害発生時にスイッチ自律にて OpenFlow インスタンスのインターフェースをダウンさせることができます。

この機能は、PFC 側からあらかじめ設定をおこないます。Emergency リンクダウン制御機能は、Emergency モードとは独立し、個別に動作の設定が可能です。

(1) リンクダウン対象ポート

OpenFlow インスタンスに含まれる、全てのポートが設定の対象となり、PFC から設定を行います。

RSI では l2-inband-secure-channel 設定されていない物理 / リンクアグリゲーションインターフェース、VSI では該当インスタンスで PFC 側からの port-mod 操作が許可されている物理 / リンクアグリゲーションインターフェースが対象となります。Emergency リンクダウン制御機能で指定できないインターフェースを「表 5-14 Emergency LinkDown 指定不可能ポート対象一覧」に示します。

リンクアグリゲーションインターフェースがリンクダウンの対象となった場合は、配下の物理インターフェースも全てリンクダウンとなります。このとき、OpenFlow インスタンスに含まれていない物理インターフェースもリンクダウンされます。リンクダウンの対象外のインターフェースを指定した場合、設定を行わず、PFC に対してエラーメッセージを送信します。

ただし、リンクアグリゲーションインターフェース配下の物理インターフェースに、「表 5-14 Emergency LinkDown 指定不可能ポート対象一覧」に示すリンクダウンに指定できないインターフェースが含まれている場合は、リンクダウンしません。

また、リンクアグリゲーションインターフェースが Emergency 状態から復帰後に、リンクアップの対象となつた場合は、配下の物理インターフェースも全てリンクアップの対象となります。

表 5-14 Emergency LinkDown 指定不可能ポート対象一覧

インスタンス種別	Emergency LinkDown 指定できないポート 物理ポート / リンクアグリゲーションインターフェース
共通	OpenFlow インスタンスに所属しないポート (*1)
RSI	l2-inband-secure-channel コマンド指定されているポート
VSI	port-modify-access permit されていないアクセスポート port-modify-trunk permit されていないトランクポート (*2)

(*1) : リンクアグリゲーションインターフェース配下の物理インターフェースは OpenFlow インスタンスに所属していない場合でも、リンクアグリゲーションインターフェースが OpenFlow インスタンスに所属しリンクアップ/ダウンの対象になっている場合は、配下物理インターフェースもリンクアップ/ダウンの対象となる。

(*2) : 複数のインスタンスに関連するトランクポートにおいて、port-modify-trunk permit が投入されているインスタンスが存在する場合、該当トランクポートはリンクアップ/ダウンの対象となる。

(2) フローエントリの削除

Emergency リンクダウンを指定する場合、指定したインターフェースがリンクダウンした際に、関連するフローエントリを削除します。ただし、設定にて削除しないことも可能です。フローエントリの削除設定は、PFC による Vendor EmergencyLinkDown(Set/Del) メッセージにて、Emergency リンクダウン指定と同時にいます。削除設定の対象となるフローエントリの条件を、「表 5-15 Emergency リンクダウン指定インターフェースに関連するフローエントリの削除条件」に示します。

表 5-15 Emergency リンクダウン指定インターフェースに関連するフローエントリの削除条件

フローエントリ フィールド	Emergency リンクダウン指定インターフェースの関連フィールド		
検索条件	Import	ポート指定	Any 指定
		○	×
アクション	Output Enqueue	ポート指定	All
		○	×
			Flood
			×

(3) Emergency 状態からの復帰

全 Secure Channel の切断状態から、Secure Channel の接続状態に復帰した場合、Emergency リンクダウンにてリンクがダウンしていたインターフェースを、自動でリンクアップすることができます。この機能は、Emergency リンクダウン指定時に、VendorEmergencyLinkDown(Set/Del) メッセージで同時に設定が可能です。

リンクアップの設定がない場合、Emergency 状態から復帰しても、リンクダウン状態を維持します。

(4) OpenFlow 制御メッセージ

Emergency リンクダウン制御機能の動作指定のメッセージは、OpenFlow メッセージ Vendor EmergencyLinkDown(Set/Del) メッセージを使用します。本機能の設定内容は、show openflow コマンド及び、PFC より Vendor EmergencyLinkDown(Get/Reply) を使用して確認することができます。「表 5-16 Emergency リンクダウン動作用 Vendor メッセージ一覧」に、Emergency リンクダウン制御機能で使用するメッセージ一覧を示します。

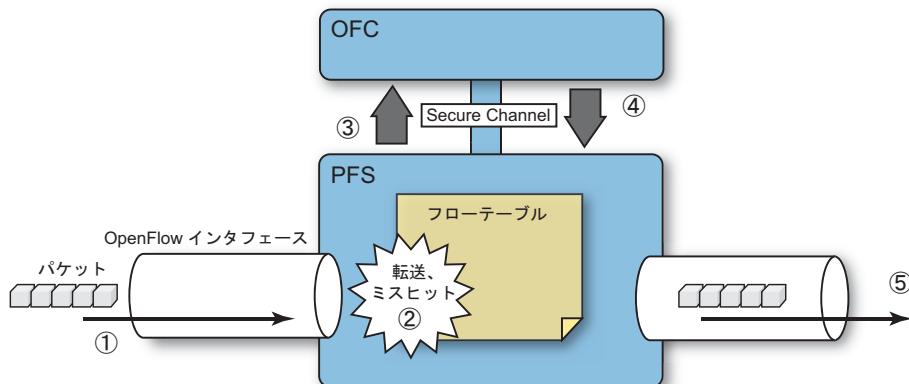
表 5-16 Emergency リンクダウン動作用 Vendor メッセージ一覧

メッセージ種別	方向	説明
Vendor EmergencyLinkDown (Set/Del)	PFC ⇒ PFS	Emergency トリガ発動時にリンクダウンするインターフェースの設定・削除 Set による上書きで更新とみなす。
Vendor EmergencyLinkDown (Status)	PFS ⇒ PFC	Emergency トリガ発動時にリンクダウン指定インターフェース情報変更通知 Vendor EmergencyLinkDown メッセージによる新規設定および変更が行われた場合に PFC に通知される。
Vendor EmergencyLinkDown (Get/Reply)	PFS ⇄ PFC	Get:Emergency トリガ発動時にリンクダウンするインターフェースの情報を PFC から PFS へ要求 Reply:PFC からの Get に対して、リンクダウン指定されているインターフェース情報を返送。
Error (type : PFET_EMERGENCY_MOD_FAILED)	PFS ⇒ PFC	Vendor EmergencyLinkDown(Set/Del) に対し、一つでも指定不可能なポートが含まれていた場合、設定を行わず、Controller に理由とともに通知するメッセージ。

5.2.9 Packet In・Packet Out の解説

次の図は、Packet In・Packet Out の流れを示しています。

図 5-22 Packet In・Packet Out の流れ



- ① OpenFlow インタフェースでパケットを受信
- ② OFC 宛の転送アクション、またはフローテーブル検索でパケットがフローエントリにヒットしない
- ③ Secure Channel を経由し、Packet In メッセージでパケットデータを OFC へ転送
- ④ OFC から Packet Out メッセージを送信
- ⑤ Packet Out メッセージのアクションに従い、パケットを出力する

(1) Packet In

OpenFlow プロトコルの Packet In メッセージは、図 5-22 のように、OFC に対して、Secure Channel を経由してパケットを送信するために使われます。OFC は、パケットを受けて処理方法を決定します。

表 5-17 Packet In メッセージの構成

フィールド名	意味
buffer_id	バッファ番号
total_len	トータルフレーム長
in_port	入力ポート
reason	Packet In メッセージ発生理由
data	フレーム本体

表 5-18 Packet In メッセージの reason

フィールド名	意味
OFPR_NO_MATCH	フローテーブル検索でヒットせず
OFPR_ACTION	OUTPUT アクションによる OFC 宛てのパケット転送
PFPR_ACTION_VISUAL	可視化グループのフローテーブルにヒット
PFPR_ACTION_MIRROR	アクションに Normal + Controller 指定されているフローエントリにヒット

本装置では、入力パケットがフローエントリにヒットしなかった場合の処理を、Packet In メッセージでパケットを OFC に送る (miss-action controller 設定時) か、L2/L3 スイッチング機能で処理する (miss-action normal 設定時) かの 2 種類から選択することができます。

設定で miss-action controller が有効、かつポートの NO_PACKET_IN フラグが無効であれば、パケットがフローエントリにヒットしなかった時に Packet In メッセージを OFC に送信します。また、フローエントリの OUTPUT アクションで CONTROLLERへの出力が指定された場合にも、Packet In メッセージを OFC に送信します。本装置では、OpenFlow プロトコルメッセージで指定されたサイズの入力パケットを Packet In メッセージに付加し、OFC へ送信します。VSI モードの場合は、VSI を認識するために用いる VLAN タグを外した上で送信します。

(2) Packet Out

OpenFlow プロトコルの Packet Out メッセージは、図 5-22 のように、OFC が PFS に対してパケット出力指示を行うためのメッセージです。Packet Out メッセージに付加されたパケットデータを、そのメッセージで指示されたアクションに従って処理します。Packet Out メッセージの構成は「表 5-19 Packet Out メッセージの構成」を参照してください。

表 5-19 Packet Out メッセージの構成

フィールド名	意味
buffer_id	バッファ ID
in_port	入力ポート
actions_len	action 配列のサイズ
Actions	action 構造体の配列
Data	パケットデータ

TABLE への OUTPUT アクションが指定された Packet Out メッセージを受信した場合には、そのパケットをフローテーブルによる検索にかけます。

本装置では、VSI が Packet Out メッセージを受信した場合、出力する際には、必要に応じて VSI を識別するための VLAN タグを付加して出力します（アクセスポートでは付与されません）。

5.2.10 Packet In メッセージのスケジューリング / 帯域制限機能

本機能は Packet In のトラフィックにおいて、スケジューリングと帯域制限を行います。

PFC にて、出力先が Controller となるフローエントリに優先度を指定することでスケジューリングを実現します。

また、PFC に対する Packet In のトラフィックを PFC から制限することができます。

(1) Packet In メッセージのスケジューリング設定

PFC より、出力先が Controller のフローエントリについて、Enqueue アクションに queue_id を指定することでフローエントリに優先度を設定し、スケジューリングを行います。

(2) Packet In メッセージの帯域制限

PFC のメッセージ処理能力に応じて、PFS に対し Packet In メッセージの帯域を制限させることができます。Packet In メッセージの帯域制限値の設定は、Secure Channel 単位で PFC から動的に変更が可能です。

本機能は Vendor Set Configuration メッセージを用いて設定します。Vendor Set Configuration メッセージで設定できるのは、Secure Channel 単位での Packet In の総和帯域であり、フロー単位など個別に制限の設定はできません。「表 5-20 Packet In 帯域制限 OpenFlow プロトコルメッセージ」にて、本機能で使用するメッセージの説明をします。

表 5-20 Packet In 帯域制限 OpenFlow プロトコルメッセージ

メッセージ種別	方向	説明
Vendor Set Configuration	PFC ⇒ PFS	Secure Channel 単位で Packet In 出力帯域の制限設定時に使用。 ※ Packet In 帯域制限以外の設定にも使用される
Error (PFET_SET_CONFIG_FAILED)	PFS ⇒ PFC	PFC からの Vendor Set Configuration 内容に誤りがあった場合にエラーを返す。 ※ Packet In 帯域制限以外の設定にも使用される

5.2.11 OpenFlow プロトコル制御ポートの解説

OpenFlow プロトコルで制御されるポートについて、解説します。

(1) 対象インターフェース

OpenFlow インタフェースはポート番号(16ビット)で管理されます。

ポート番号の値は以下のように指定します。

- 物理ポートとリンクアグリゲーションの場合

ポート番号は、物理ポートと、リンクアグリゲーションと、リンクアグリゲーションを構成する物理ポートであることが分かるように定義されます。

ポート番号の上位 1 ビットは 0 となります。

上位 2 番目からの 7 ビットは、リンクアグリゲーションのリンクアグリゲーションインターフェース番号を示します。ただし、物理ポート(リンクアグリゲーションなし)の場合は、0 固定です。

下位 8 ビットは、1 オリジンの物理ポート番号を表します。ただし、リンクアグリゲーションインターフェースの場合は、0 固定です。

- ポートグループ・ポート(PG ポート)の場合

ポート番号の上位 1 ビットは 1 となります。下位 10 ビットは、PG ポート番号を表します。

表 5-21 ポート番号のマッピング(物理ポートとリンクアグリゲーションの場合)

#	インターフェース	上位 bits Port[15]	リンクアグリゲーション インターフェース番号 Port[14-8]	物理 ポート番号 Port[7-0]
1	物理ポート (リンクアグリゲーションなし)	0	0	1-52
2	物理ポート (リンクアグリゲーション配下)(*1)(*2)	0	1-32	1-52
3	リンクアグリゲーション(*2)	0	1-32	0

(*1)：物理ポートが属するリンクアグリゲーションが OpenFlow インタフェースであるか否かによらず、表中のポート番号形式で指定します。

(*2)：リンクアグリゲーションと当該リンクアグリゲーション配下の物理ポートについては、どちらも独立して OpenFlow インタフェースとして指定することができ、両方を混在させることも可能です。

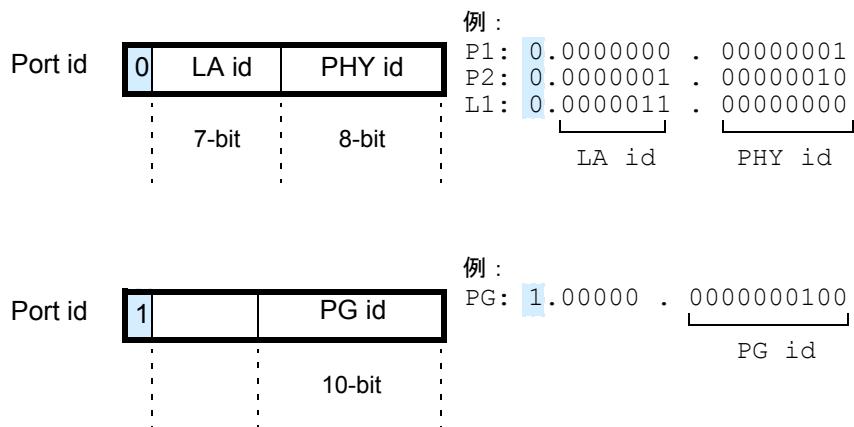
表 5-22 ポート番号のマッピング(ポートグループ・ポート(PG ポート)の場合)

#	インターフェース	上位 bits Port[15]	Port[14-10]	PG ポート番号 Port[9-0]
4	PG ポート	1	0	0-1023

5. OpenFlow 機能の解説

ポート番号の表示例を次に示します。

図 5-23 ポート番号の表示例



P1 : 物理ポート GbE 0/1 #1

P2 : 物理ポート GbE 0/2 #2 (リンクアグリゲーションインターフェース 1 に所属)

L1 : リンクアグリゲーション #3

PG : PG ポート #4

PFS が制御するポート情報一覧を次に示します。

表 5-23 ポート情報一覧

#	項目	値		OFC から の書き換 え可 / 不可
1	ポート番号	「5.2.11 (1) 対象インターフェース」を参照		不可
2	インターフェース MAC アドレス	物理ポート	ポートの MAC アドレス	不可
		リンクアグリゲーション	設定されているインターフェースの最若番の MAC 情報を使用（該当 IF の up/down によりません。）	
3	インターフェース名 (*1)	物理ポート	1G	文字列 "GBE" + NIF 番号 + / + ポート番号
			10G	文字列 "10GBE" + NIF 番号 + / + ポート番号
			リンクアグリゲーション	文字列 "LAG" + リンクアグリゲーションインターフェース番号
4	ポート 設定フラグ	admin ポートダウン	ポートダウン(1) またはポートアップ(0) (*2)	可
5		STP 無効	無効(1) 固定	不可
6		STP 以外を Drop	Drop しない(0) 固定	不可
7		STP を Drop	Drop しない(0) 固定	不可
8		Flood 対象外	無効(0) または有効(1)	可
9		Forward しない	Forward する(0) 固定	不可
10		Packet In メッセージ送信の 対象外	無効(0) または有効(1)	可
11	ポート 運用状態	リンクダウン	リンクダウン(1) またはリンクアップ(0)	不可
12		STP 状態	Forward(2) 固定	不可
13	回線速度 / モード / 機能	物理ポートの状態	物理ポート	装置(PF5200 シリーズ)の情報を 使用
14			リンクアグリゲーション	固定値(0x00000000) (値を持たない)
15		広告している内容	固定値(0x00000000)	
16		サポート内容	固定値(0x00000000)	
17		対向ポートの情報	固定値(0x00000000)	

(*1) : インターフェース名の表示例 : GBE0/1, 10GBE0/25, LAG10

(*2) : VSI の場合, port-modify-access コマンドおよび port-modify-trunk コマンドにより許可した場合のみ, OFC から設定可能です。

「表 5-23 ポート情報一覧」の #2 の MAC アドレスについて、物理ポートの場合はポートの MAC アドレスを保持します。リンクアグリゲーションの場合は、"設定されている" インタフェースの最若番の MAC 情報を使用します(該当インターフェースの up/down によらない)。「表 5-23 ポート情報一覧」の #13 から #17 までのフィールドは、次に示す情報を表現するビット列で構成されます。

表 5-24 ポートの速度 / モード / 機能フィールド詳細

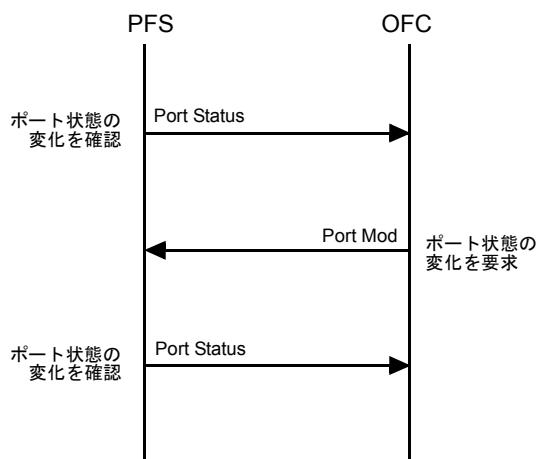
ビット	内容
0	10Mb half-duplex
1	10Mb full-duplex
2	100Mb half-duplex
3	100Mb full-duplex
4	1Gb half-duplex
5	1Gb full-duplex
6	10Gb full-duplex
7	Copper medium
8	Fiber medium
9	Autonegotiation
10	Pause
11	Asymmetric Pause

(2) ポート状態管理

PFS は、管理しているポートの追加、削除、および状態変更時に、Port Status メッセージを用いて OFC に通知します。状態変更には、リンクのアップダウン等が含まれます。OFC から Port Mod メッセージを受信した場合は、指示された通りに PFS のポート状態を変更します。その結果ポート状態が変化した場合は、Port Status メッセージを OFC に送信します。ポート状態制御のシーケンスを次に示します。

Port Mod は Port Status と必ず対になるものではありません。Port Status メッセージはポート状態変更に起因し送信するものです。Port Mod メッセージを受信したにも関わらず設定変更が発生しなかった場合は、Port Status メッセージの送信は行われません。

図 5-24 ポート状態制御シーケンス



5.2.12 OpenFlow プロトコル Features 通知機能の解説

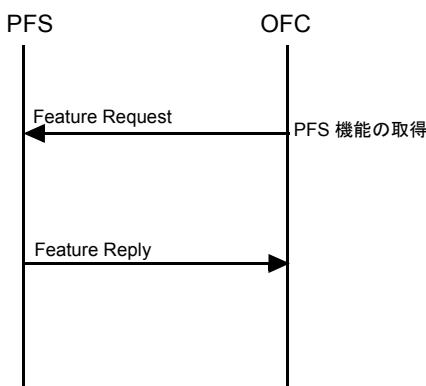
OpenFlow プロトコルの Features メッセージは OFC からの機能・特徴の問い合わせ要求 (Request)・応答 (Reply) に用いられます。Features Reply メッセージには、PFS の装置情報・OpenFlow 機能の capability・スイッチインスタンスに属するすべてのポート情報等が含まれます。Features Reply メッセージにて通知する Features 一覧を次に示します。

表 5-25 PFS Features 一覧

#	項目	意味
1	ヘッダ	OpenFlow ヘッダ
2	DPID	スイッチインスタンスの Data path ID (装置の識別 ID)
3	バッファ数	スイッチインスタンスでバッファできるパケット最大数
4	テーブル数	サポートするテーブルの数
5	Capabilities	フロー毎の統計情報 フローテーブルの統計情報 ポート毎の統計情報 STP 複数物理ポートからの送信 IP フラグメントのリアセンブル
6	アクション	サポートするアクション一覧 「表 5-6 フローエントリに設定可能なアクション」 参照
7	ポート	所属する全ポートの情報配列 「表 5-23 ポート情報一覧」 参照

「図 5-25 PFS Features 通知シーケンス」に OpenFlow プロトコルの Features メッセージの OFC, PFS 間シーケンスを示します。PFS は、Features Request メッセージを受信すると、PFS のサポートする機能およびポート情報を Features Reply メッセージで返信します。

図 5-25 PFS Features 通知シーケンス



5.2.13 OpenFlow プロトコルコンフィグレーション機能の解説

OpenFlow プロトコルでは、Set Configuration メッセージを用いて、OFC から PFS にコンフィグレーションを設定することができます。また、Get Configuration (Request および Reply) メッセージを用いて、OFC は PFS のコンフィグレーション取得を行えます。PFS が Set Configuration メッセージを受信すると、そのコンフィグレーションを反映させます。Set Configuration メッセージには対となる Reply や Ack は存在しないため、コンフィグレーションが正しく反映されたかどうかの確認は、OFC からの Get Configuration Request メッセージに対する Get Configuration Reply メッセージで行います。

コンフィグレーション機能のシーケンスを「図 5-26 コンフィグレーション機能のシーケンス」に、各メッセージ構成を「表 5-26 Set Configuration メッセージの構成」、「表 5-27 Get Configuration Reply メッセージの構成」に示します。

図 5-26 コンフィグレーション機能のシーケンス

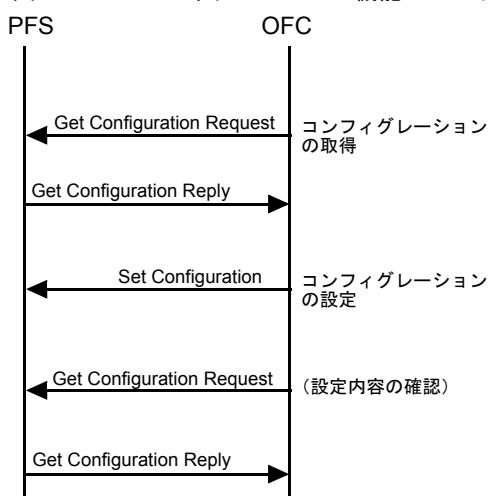


表 5-26 Set Configuration メッセージの構成

フィールド名	意味	補足
header	OpenFlow ヘッダ	—
flags	IP フラグメントパケットの処理方法フラグ	選択不可
miss_send_len	Packet In メッセージに付加するパケットサイズ	—

表 5-27 Get Configuration Reply メッセージの構成

フィールド名	意味	補足
header	OpenFlow ヘッダ	—
flags	IP フラグメントパケットの処理方法フラグ	0 固定 (処理しない)
miss_send_len	Packet In メッセージに付加するパケットサイズ	Set Configuration メッセージで設定されていない場合は 65535(初期値)

5.2.14 統計情報の解説

PFS の持つ統計情報を OFC へ通知する方法は、以下の 2 通りです。

(1) Statistics Request/Reply メッセージによる統計情報通知

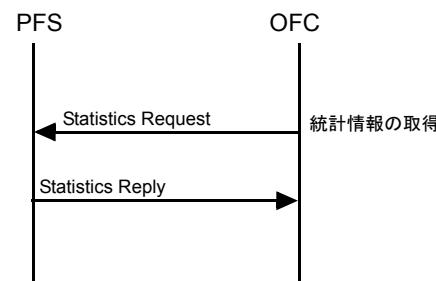
OFC から、必要な情報種別を指定し、統計情報を取得します。統計情報の種別を次に示します。

表 5-28 統計情報一覧

#	項目	Request 付加条件	Reply 内容
1	FLOW (個別のフロー)	フロー検索条件、テーブル番号、出力ポート	指定した検索条件に一致したフローエントリが持つ統計情報を個別に返す
2	AGGREGATE (集約したフロー)	フロー検索条件、テーブル番号、出力ポート	指定した検索条件に一致したフローエントリが持つ統計情報の合計値
3	PORT (全ポート)	なし	ポートが持つ統計情報を、全ポート分返す
4	VENDOR_FLOW_STRICT (ベンダ拡張完全一致フロー情報)	フロー検索条件、優先度、出力ポート	指定した Request 付加条件に完全一致したフローエントリが持つ統計情報
5	DESC (装置情報)	なし	装置情報(ベンダ、HW/SW 情報、シリアル番号)を返す
6	TABLE (フローテーブル情報)	フロー検索条件、テーブル番号、出力ポート	フローテーブル情報(フローテーブルが持つ統計情報)を返す
7	VENDOR_PF_FLOW	フロー検索条件、テーブル番号、出力ポート	指定した検索条件に一致したフローエントリが持つ統計情報を個別に返す
8	VENDOR_PF_FLOW_STRICT	フロー検索条件、テーブル番号、出力ポート	指定した Request 付加条件に完全一致したフローエントリが持つ統計情報
9	VENDOR_PF_FLOW_PORTGROUP	ポートグループ番号	ポートグループ情報

PFS は、Statistics Request メッセージを受信すると、要求された統計情報を Statistics Reply メッセージで返信します。シーケンスを「図 5-27 Statistics Request/Reply メッセージによる統計情報通知シーケンス」に示します。

図 5-27 Statistics Request/Reply メッセージによる統計情報通知シーケンス

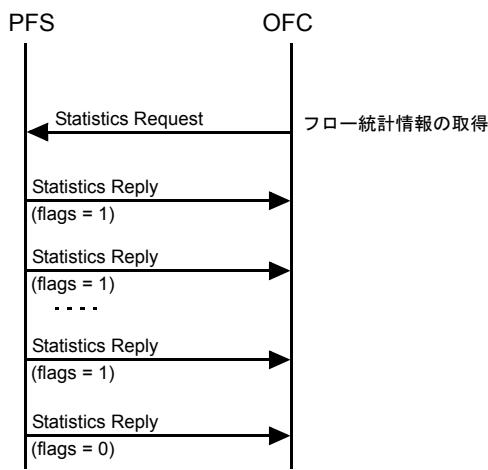


「表 5-28 統計情報一覧」の #1 の個別フロー統計情報が要求された場合、一致したフローエントリの数だけフローエントリごとに Statistics Reply メッセージを返します。#3 ではすべてのポート情報を、続けて送信します。Statistics Reply メッセージに後続メッセージが存在する場合は、Statistics Reply メッセージの flags に 1 が、それ以外は 0 が設定されます。

5. OpenFlow 機能の解説

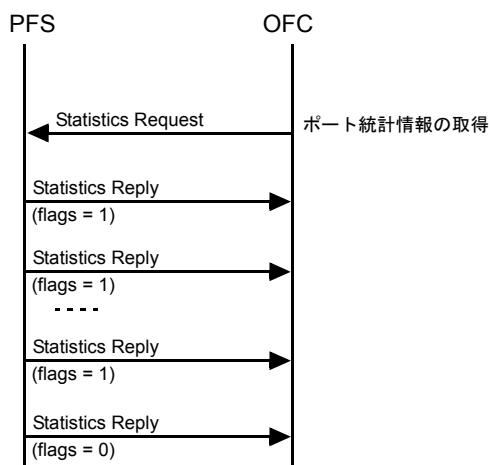
OFC が個別フロー統計情報を要求した場合のシーケンスを次に示します。

図 5-28 個別フロー統計情報通知シーケンス



OFC が物理ポート統計情報を要求した場合のシーケンスを次に示します。

図 5-29 物理ポート統計情報通知シーケンス



(2) Flow Removed メッセージによる統計情報通知

「5.2.6 フローテーブル制御の解説」の「(2) タイムアウトによるフローテーブル制御」に記載したタイムアウト処理、Flow Mod メッセージによる削除処理 (DELETE, DELETE_STRICT), または運用コマンド clear openflow table によってフローエントリの削除が行われた場合に、そのフローエントリの統計情報を含む Flow Removed メッセージを送信できます。Flow Removed の送信が必要な場合は、Flow Mod メッセージによるフローエントリ新規追加の際に、OFPFF_SEND_FLOW_Rem フラグを設定してください。

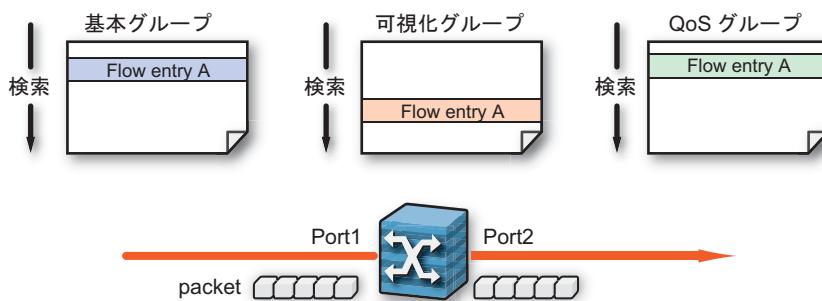
PFS の運用コマンドでは、フローエントリ・テーブルの統計情報を show openflow table コマンドにて確認できます。また、各 OpenFlow プロトコルメッセージ送受信に関する統計情報を show openflow statistics コマンドにて確認できます。コマンドの詳細は「運用コマンドレファレンス Vol.1」を参照してください。

5.2.15 マルチヒット機能の解説

一般的な OpenFlow の動作では、1つのパケットは最大1つのフローエントリにヒットし、アクションが決定されます。それに対してマルチヒット機能では、フローエントリを複数の論理グループに分類して保持し、1つの検索対象パケットに対して論理グループごとに並行して検索とアクション実行を行うことが可能です。

本装置は OpenFlow 標準の動作を行う「基本グループ」と、フローの可視化を目的とした「可視化グループ」、フローへの QoS 制御を実現する「QoS グループ」の合計3つの論理グループを持ちます。これにより、経路の制御とは別の基準でフローの統計情報を取得し、フローの可視化が可能となります（例：経路は MAC アドレスにより決定し、統計はポート番号別に行う等）。

図 5-30 マルチヒット機能のイメージ



(1) マルチヒットアクション

1つの検索対象パケットに対して、それぞれ基本グループ、可視化グループと QoS グループに登録したフローエントリを検索し、それぞれのグループに設定されたアクションを行うことができます。

(2) 基本グループ

基本グループに登録するフローエントリには、どのアクションでも登録する事が可能です。Default エントリ (miss-action 実行用のエントリ) は、基本グループに属するフローテーブルにのみ設定することができます。可視化グループの全エントリにヒットしなかった場合は何も処理を行わない為、可視化グループについては miss-action 実行用のエントリは不要となります。

(3) 可視化グループ

可視化グループに登録するフローエントリは、OUTPUT Controller アクション、Enqueue Controller アクション、及び no action(何もアクションを登録しない)である必要があります。可視化グループでは、フローテーブルに設定されたフローエントリに対して、フローの統計情報を収集したり、フローテーブルに対して、テーブルの統計情報を収集したりする事ができます。可視化グループのフローテーブルにおいて、入力されたパケットが OUTPUT Controller アクションが設定されている有効なフローエントリにヒットした場合、Vendor 拡張の Packet In メッセージを送信します。

(4) QoS グループ

QoS グループには QoS 用フローの登録が可能です。登録できるアクションは、Set TOS, Set VLAN PCP, 装置内優先度指定 (enqueue アクションの queue_id のみ参照し、出力ポート情報は無視する: none(0xffff) のみ許容) を設定する事ができます。ただし、基本グループのアクションと QoS グループのアクションが競合した場合、基本グループのアクションが優先されます。

5.2.16 ポートグループ機能の解説

本装置は、複数の物理インターフェース及びリンクアグリゲーションインターフェースをグループ化して管理する機能をサポートしています。これを、ポートグループ機能と呼びます。ポートグループ機能では、フローエントリ毎に複数の実ポートを指定することができます、さらにその中から自動的にリンクアップしているポートを選択します。これによって、スイッチの自律的な障害時切り替え機能として使用することができます。ポートグループはインスタンス毎に独立しています。相互に影響することはありません。ポートグループの機能の概要図を、「図 5-31 ポートグループ概要図」に示します。

図 5-31 ポートグループ概要図



(1) PG ポート番号

ポートグループ・ポート (PG ポート) 番号は、フローエントリの中でポートグループをインターフェースとして指定する為に使用されます。PG ポート番号は OpenFlow プロトコル制御ポート番号の 0x8000 ~ 0x83ff が割り当てられます。(OpenFlow プロトコル制御ポート番号については、「5.2.11 OpenFlow プロトコル制御ポートの解説」を参照。) PG ポートはフローエントリの output または enqueue のアクションとして指定することができます。また、OpenFlow の仮想ポートである ALL/FLOOD ポートには PG ポートを含むことはできません。

(2) ポートグループの設定

ポートグループの登録・削除は、PFC より Vendor PortGroupMod(Add/Del) メッセージを使用して行います。また、設定したポートグループの状態を確認する為に、Vendor PortGroupStatus メッセージを PFC へ通知することができます。「表 5-29 ポートグループ設定時の OpenFlow プロトコルメッセージ」では、これらのポートグループに関する OpenFlow プロトコルメッセージについて説明します。

表 5-29 ポートグループ設定時の OpenFlow プロトコルメッセージ

メッセージ	説明
Vendor PortGroupMod(ADD/DEL)	ポートグループの追加・削除を PFC より PFS へ要求。 設定内容を更新の際は、ADD を使用し上書き。
Vendor PortGroupStatus	ポートグループの状態を PFS より PFC へ通知。

また、ポートグループの設定に関する統計情報は、PFC にて Statistics Request/Reply(Vendor) メッセージを用いて収集することができます。

! 注意事項

PFC にてポートグループが削除された場合、該当する PG ポートが指定されているフローエントリは削除されます。

5.2.17 VLAN 設定機能の解説

従来 L2/L3 スイッチング機能部分からのみ設定可能としていた VLAN 設定を、OpenFlow インタフェースに対して PFC から設定することができます。OpenFlow で設定可能な VLAN 数は 4094 となります。OpenFlow により設定される VLAN を OF-VLAN、PFS の L2/L3 スイッチング機能部分（CLI）にて設定される VLAN を CLI-VLAN と呼びます。

(1) OpenFlow による VLAN 設定 (OF-VLAN)

OF-VLAN は、PFC より Vlan_Mod メッセージを用いて設定します。

OF-VLAN の設定における動作を以下に記載します。

1. OF-VLAN は、1 ~ 4094 の範囲で指定できます。また、最大で 4094 個の VLAN を設定できます。
2. OpenFlow 機能が RSI モードで動作している場合のみ使用可能です。
3. OpenFlow に所属するインターフェースに登録 / 変更 / 削除を行うことができます。
4. 物理インターフェース、リンクアグリゲーションインターフェースで設定可能です。ただしリンクアグリゲーション配下の物理インターフェース、配下に物理インターフェースを持たないリンクアグリゲーションインターフェースには設定できません。
5. トランクポートに対してのみ設定できます。
6. VLAN tag あり /VLAN tag なし (native VLAN) の両方の VLAN ID が設定できます。
7. 1 つの VLAN tag なし (native VLAN)、複数の VLAN tag ありの VLAN ID が同時に設定できます。
8. OpenFlow インタフェース単位で設定を行います。複数の OpenFlow インタフェースの同時設定はできません。
9. OF-VLAN は、L2/L3 スイッチング機能のコンフィグレーションには保存されません。

設定可能であるインターフェースを以下の「表 5-30 OpenFlow にて設定可能なインターフェース」に示します。

表 5-30 OpenFlow にて設定可能なインターフェース

OpenFlow インタフェース状態	Vlan_Mod メッセージによる設定可否
リンクアグリゲーションインターフェース	○
リンクアグリゲーション配下の物理インターフェース	×
物理インターフェース	○
OpenFlow インタフェース以外のインターフェース	×

○ : Vlan Mod メッセージによる設定可能

× : Vlan Mod メッセージによる設定不可

その他、以下の条件では OpenFlow による VLAN の設定 (Vlan Mod) は行えません。

- VLAN が L2/L3 スイッチング機能にてインターフェースがアクセスモード (access)，およびトンネリングモード (dot1q-tunnel) の設定がされている場合
- VLAN が L2/L3 スイッチング機能にてタグ変換機能が設定されているインターフェースである場合
- CLI-VLAN として設定されている VLAN に対して、OpenFlow で CLI と異なる設定を行う場合

5. OpenFlow 機能の解説

OpenFlow にて OF-VLAN に設定できない条件が含まれる場合、OF-VLAN 設定を受け付けず、コントローラに対して OpenFlow メッセージによる Error メッセージ (type : PFET_VLAN_MOD_FAILED) を返します。

また、設定変更、もしくは本装置の状態変化によって OpenFlow インタフェースに指定された VLAN の設定に変更が発生した場合は、PFC に対して Vendor Vlan Status メッセージを用いて通知を行います。ただし、装置に設定されている VLAN が OpenFlow による設定か、CLI による設定かについては区別しません。両方の VLAN において、情報が変化した場合に通知されます。

以下の「表 5-31 OpenFlow による VLAN 設定時の OpenFlow プロトコルメッセージ」に、OpenFlow による VLAN 設定に用いる OpenFlow プロトコルメッセージについて説明します。

表 5-31 OpenFlow による VLAN 設定時の OpenFlow プロトコルメッセージ

メッセージ種別	方向	説明
VendorVlan Mod (Add/Mod/Del)	PFC ⇒ PFS	OpenFlow による VLAN の設定（追加・変更・削除）。 VLAN は複数指定が可能です。
Vendor Vlan Status	PFS ⇒ PFC	OpenFlow インタフェースに指定した VLAN の状態通知メッセージ。
Error (PFET_VLAN_MOD_FAILED)	PFS ⇒ PFC	OpenFlow による VLAN 設定失敗時のエラーメッセージ。
Statistics Request/Reply (PFST_VLAN)	PFS ⇄ PFC	VLAN の統計情報を要求 / 返答。 全 port の VLAN か、1 port の VLAN のいずれかの情報を返答。

(2) OpenFlow により設定した VLAN の使用

OpenFlow により設定した VLAN は、フローエントリの Match 条件の dl_vlan フィールド、またアクションフィールドの SET_VLAN_VID にて使用できます。

ただし、OpenFlow により設定した VLAN は、L2/L3 スイッチング機能では動作しません。「表 5-32 VLAN 情報の動作可否」に、L2/L3 スイッチング機能と OpenFlow により設定した VLAN について、各機能からの動作可否を示します。

表 5-32 VLAN 情報の動作可否

	本装置機能部による動作可否	
	L2/L3 スイッチング 機能部分	OpenFlow
CLI-VLAN	○	○
OF-VLAN	×	○
CLI-VLAN/OF-VLAN 両方で同じ VLAN が設定されている場合	○	○

○：該当機能にて動作可能

×：該当機能にて動作不可

(3) L2/L3 スイッチング機能 (CLI) による設定との併用

L2/L3 スイッチング機能による設定 (CLI-VLAN 設定含む) は、OpenFlow による VLAN 設定 (OF-VLAN) よりも優先されます。運用中に L2/L3 スイッチング機能による設定 (CLI-VLAN 設定含む) を受け付けた場合、CLI-VLAN と OF-VLAN の設定に矛盾があれば OF-VLAN の設定が削除されます。

また、PFC に対して OF-VLAN が削除されたことを OpenFlow メッセージ (VLAN_STATUS) にて通知します。

(4) 未定義の VLAN ID を持つパケット受信時の処理

OpenFlow インタフェースに L2/L3 スイッチング機能 /OpenFlow の両方で設定されていない VLAN を持つパケットを受け取った場合でも、これを廃棄せずに OpenFlow 機能により処理されます。パケットを廃棄せずにフローエントリ検索を行い、これにヒットすればエントリに従って処理し、ヒットしなければ miss-action 時の処理を行います。

(5) VLAN 登録情報

装置に設定されている OF-VLAN/CLI-VLAN 情報は、OpenFlow の統計取得メッセージ (type : PFST_VLAN) により PFC から確認することができます。

また、OF-VLAN/CLI-VLAN は、リモートの管理端末から MIB 情報を取得することができます。

CLI-VLAN は show vlan コマンド、OF-VLAN は show openflow detail コマンドにて設定内容を確認することができます。

5.2.18 指定パケットの周期送信機能の解説

本装置は、OFC より OpenFlow メッセージで指定されたフォーマットのパケットを周期的に送信する機能をサポートしています。これを、指定パケットの周期送信機能と呼びます。本機能では、指定されたパケットを一定周期で本装置より自動的に送信し続けることができます。

OFC から OpenFlow メッセージ（Vendor 拡張）を使用して、指定パケットの送信周期、出力ポート、指定パケットに対する書き換えアクションなどを設定することができます。出力ポートには、OpenFlow インタフェースとして設定された物理ポート、リンクアグリゲーションインターフェースを指定でき、複数ポートの指定も可能です。

「表 5-33 指定パケット周期送信機能・動作用メッセージ一覧」に、指定パケット周期送信機能で使用する各メッセージについて示します。

表 5-33 指定パケット周期送信機能・動作用メッセージ一覧

メッセージ種別	方向	説明
Vendor Cyclic Packet Out Mod	PFC ⇒ PFS	周期的に送付を行うパケットに関する設定を行うことができます。
Vendor Cyclic Packet Out Status	PFS ⇒ PFC	OpenFlow メッセージによる設定変更、または本装置の状態変化によってパケットの周期送付設定の状態変化が発生した場合は、PFC に対して状態変化通知を行います。
Vendor Pfst Cyclic Packet Out (Get/Reply)	PFS ⇄ PFC	パケット周期送信について、PFC からの OpenFlow 統計取得メッセージにより統計情報の取得ができ、また、CLI コマンドにより統計情報の取得ができます。 統計情報は、Packet-ID 単位で取得が可能ですが（統計情報は Packet-ID 単位で合算される）。
Vendor Cyclic Packet Out Mod Failed	PFS ⇒ PFC	本装置で受付不可な情報が含まれていた場合は、PFC に対してエラーメッセージを送信します。

5.3 サポート仕様

5.3.1 OpenFlow サポート機能

「表 5-34 OpenFlow サポート機能一覧」に、本装置でサポートする OpenFlow 機能一覧を示します。

表 5-34 OpenFlow サポート機能一覧

#	分類	機能		RSI (*1)	VSI (*2)	備考
1	OpenFlow 機能	バージョン	OpenFlow Version 1.0.0	○	○	
2		スイッチインスタンス	Real Switch Instance	○	×	
3			Virtual Switch Instance	×	○	最大スイッチインスタンス数は 16
4		Secure Channel	TCP	○	○	スイッチインスタンスあたり 1 本
5			TLS	○	○	
6		プロトコル	「表 5-35 サポートメッセージ一覧」、および「表 5-36 Vendor 拡張メッセージ一覧」参照	○	○	
7		フレークレート条件	入力ポート、送信元 MAC アドレス、宛先 MAC アドレス、VLAN ID、VLAN priority、Ethernet type、IP プロトコル番号 /ARP opcode、IPv4 ToS ビット、送信元 IPv4/IPv6 アドレス、宛先 IPv4/IPv6 アドレス、送信元トランスポート・ポート番号 /ICMP Type、宛先トランスポート・ポート番号 /ICMP Code	○	○	
8		パケット転送	单一ポート出力 (Unicast)、複数ポート出力 (Multicast)、ポートグループ出力、全ポート出力、コントローラ転送、自装置 TCP/IP 終端、入力ポート折り返し、L2/L3 転送機能、フラッディング、QoS クラスキー指定、廃棄	○	○	
9		フィールド書換	送信元 MAC アドレス、宛先 MAC アドレス、VLAN ID、VLAN priority、VLAN タグヘッダ除去、IPv4 ToS ビット、送信元 IPv4 アドレス、宛先 IPv4 アドレス、送信元トランスポート・ポート番号、宛先トランスポート・ポート番号	○	○	

(*1) : RSI 欄は該当パケットが RSI の OpenFlow インタフェースを通る場合のサポート可否です。

(*2) : VSI 欄は該当パケットが VSI の OpenFlow インタフェースを通る場合のサポート可否です。

ここでは、該当パケットとは、通信パケットに何かの処理（ミラーリング、転送等）をする機能の場合は通信パケットそのものを表し、プロトコル（LLDP 等）の場合はプロトコルパケットを表します。

【RSI, VSI 欄の記号】

○ : 使用できる。

× : 使用できない。

5.3.2 OpenFlow プロトコルサポートメッセージ

「表 5-35 サポートメッセージ一覧」に、本装置でサポートする OpenFlow プロトコルのメッセージ一覧を示します。動作の詳細に関しては、「5.2 OpenFlow 機能の解説」を参照してください。

表 5-35 サポートメッセージ一覧

#	メッセージ名	方向	用途	サポート状況
1	Hello	OFC ⇄ PFS	バージョンネゴシエーションに使用	○
2	Error	OFC ⇄ PFS	メッセージにエラーがあった事を通知	○
3	Echo Request	OFC ⇄ PFS	Echo 要求	○
4	Echo Reply	OFC ⇄ PFS	Echo 応答	○
5	Vendor	OFC ⇄ PFS	ベンダ定義メッセージ	○
6	Features Request	OFC ⇒ PFS	PFS の機能・特徴の問い合わせを要求	○
7	Features Reply	PFS ⇒ OFC	PFS の機能・特徴の問い合わせに応答	○
8	Get Configuration Request	OFC ⇒ PFS	PFS の OpenFlow コンフィグレーションの取得要求 (*1)	○
9	Get Configuration Reply	PFS ⇒ OFC	PFS の OpenFlow コンフィグレーションを返答 (*1)	○
10	Set Configuration	OFC ⇒ PFS	PFS の OpenFlow コンフィグレーションを設定 (*1)	○
11	Packet In	PFS ⇒ OFC	パケットを OFC に送信 (*2)	○
12	Port Status	PFS ⇒ OFC	インターフェースの状態・設定変化を OFC に通知	○
13	Packet Out	OFC ⇒ PFS	OFC から PFS にパケットの出力を指示	○
14	Flow Mod	OFC ⇒ PFS	OFC が PFS にフローの登録・変更・削除を要求	○
15	Flow Removed	PFS ⇒ OFC	フローエントリ削除およびタイムアウト時に、統計情報を OFC に通知 (*3)	○
16	Port Mod	OFC ⇒ PFS	インターフェースの設定変更を要求	○
17	Statistics Request	OFC ⇒ PFS	統計情報取得を要求	○
18	Statistics Reply	PFS ⇒ OFC	統計情報取得に応答	○
19	Barrier Request	OFC ⇒ PFS	PFS へメッセージの処理順序の同期要求	○
20	Barrier Reply	PFS ⇒ OFC	OFC にメッセージの処理順序の同期が完了したことを通知	○
21	Queue Get Config Request	OFC ⇒ PFS	キューの情報を要求	○
22	Queue Get Config Reply	PFS ⇒ OFC	キューの情報を返答	○

(*1) : OpenFlow コンフィグレーションとは、本装置に「コンフィグレーションコマンドレファレンス Vol.1」に示すコマンドを用いて設定したコンフィグレーションではなく、OpenFlow プロトコルで規定されているコンフィグレーションを示します。

(*2) : miss-action controller が設定されており、かつポートに NO_PACKET_IN 設定がされていない場合のみ送信されます。

(*3) : フローエントリ登録時に、OFPFF_SEND_FLOWREM フラグを設定した場合のみ、送信されます。

- : サポート
- : 未サポート
- ↔ : 双方向のメッセージの送信
- ⇒ : 片方向のメッセージ送信

「表 5-36 Vendor 拡張メッセージ一覧」に、本装置でサポートする OpenFlow プロトコルの Vendor メッセージを示します。

表 5-36 Vendor 拡張メッセージ一覧

#	メッセージ名	方向	用途	サポート状況
1	Vendor (PF_Flow_Mod)	PFC ⇒ PFS	ベンダ定義メッセージ PFC が PFS にフローの登録・変更・削除を要求	○
2	Vendor (PF_Flow_Removed)	PFS ⇒ PFC	ベンダ定義メッセージ フロー登録時に、統計情報を PFC に通知 (*1)	○
3	Vendor (Port_Group_Mod)	PFC ⇒ PFS	ベンダ定義メッセージ PortGroup の状態・設定変更を要求	○
4	Vendor (Port_Group_Status)	PFS ⇒ PFC	ベンダ定義メッセージ PortGroup の状態・設定変更を通知	○
5	Vendor (Vlan_Mod)	PFC ⇒ PFS	ベンダ定義メッセージ OF-VLAN の追加 / 変更 / 削除を要求	○
6	Vendor (Vlan_Status)	PFS ⇒ PFC	ベンダ定義メッセージ OF-VLAN の追加 / 変更 / 削除を通知	○
7	Vendor (Cyclic_PacketOut)	PFC ⇒ PFS	ベンダ定義メッセージ 指定パケットの周期送付を設定	○
8	Vendor (Cyclic_PacketOut_Status)	PFS ⇒ PFC	ベンダ定義メッセージ 指定パケットの周期送付状態を通知	○
9	Vendor (Set Configuration)	PFC ⇒ PFS	ベンダ定義メッセージ PFC が PFS に各種状態変更を要求	○
10	Vendor (Get Configuration Request)	PFC ⇒ PFS	ベンダ定義メッセージ PFC が PFS の各種状態を要求	○
11	Vendor (Get Configuration Reply)	PFS ⇒ PFC	ベンダ定義メッセージ PFS が PFC に各種状態を通知	○
12	Vendor (Emergency Linkdown Mod)	PFC ⇒ PFS	ベンダ定義メッセージ Emergency-linkdown 設定を要求	○
13	Vendor (Emergency Linkdown Status)	PFS ⇒ PFC	ベンダ定義メッセージ Emergency-linkdown 状態を通知	○

- : サポート
- : 未サポート
- ↔ : 双方向のメッセージの送信
- ⇒ : 片方向のメッセージ送信

(*1): フロー登録時に、OFPFF_SEND_VENDOR_FLOW_Rem フラグを設定した場合のみ、送信されます

5.3.3 OpenFlow と L2/L3 スイッチング機能の共存

PF5200 シリーズでは、OpenFlow と L2/L3 スイッチ機能を共存させることができます。

(1) OpenFlow スイッチインスタンスと L2/L3 スイッチング機能の振り分け

本装置に入力されたパケットは下記のように OpenFlow スイッチインスタンスと L2/L3 スイッチング機能に振り分けられます。

- OpenFlow 機能を有効にすると、OpenFlow インタフェースから入力されたパケットは OpenFlow スイッチインスタンスで OpenFlow によって処理されます。
- L2/L3 スイッチング機能の Filter による廃棄は、フローエントリより優先されます。
- このため、Filter にヒットして廃棄となる場合は OpenFlow インタフェースから入力されたパケットであっても、廃棄されます。
- OpenFlow インタフェース以外から入力されたパケットは L2/L3 スイッチング機能により処理されます。
- OpenFlow インタフェースから入力されたパケットのうち、フローエントリにおいて NORMAL に指定されたパケットは、L2/L3 スイッチング機能で処理されます。
- RSIにおいて l2-inband に指定された OpenFlow インタフェースから入力されたパケットも L2/L3 スイッチング機能で処理されます。
- miss-action normal の場合に、OpenFlow インタフェースから入力されたパケットのうち、フローエントリにヒットしないパケットは、L2/L3 スイッチング機能により処理されます。

(2) L2/L3 スイッチング機能の共存時の注意事項

ルーティングプロトコル (OSPF など) や L2 制御プロトコル (UDLD など) などのプロトコルパケットや、L2/L3 スイッチング機能で中継される通信パケットなどが OpenFlow インタフェースを経由する接続構成の場合は、これらのパケットが L2/L3 スイッチング機能に渡されるようにする必要があります。

(例) 2つの PFS 間がケーブルで接続され、そのポートがアクセスポートかつ OpenFlow インタフェースになっている場合、UDLD のパケットを L2/L3 スイッチング機能で処理するためにはフローテーブルに UDLD の制御フレームを NORMAL ～ OUTPUT するエントリを登録する必要があります。(miss-action が controller に設定されているとき)※注 UDLD パケットには VLAN タグが付与されません。

対向する 2 つの装置の L2/L3 スイッチング機能間は、ユーザが構成定義した VLAN 設定とは別に、制御フレームの中に、untagged で通信されるプロトコル (LLDP, UDLD など) があることを考慮する必要があります。L2/L3 スイッチング機能間が OpenFlow インタフェースを経由しない構成の場合は、フローエントリにプロトコルパケットを NORMAL ～ OUTPUT するエントリの登録は不要です。また、miss-action normal の場合は、同様にフローエントリの設定は不要です。なお、制御フレームを廃棄または転送するようなフローを登録すると、L2/L3 スイッチング機能は正常に動作しなくなりますので、登録しないでください。

(3) 共存機能のサポート仕様

「表 5-37 OpenFlow 機能と L2/L3 スイッチング機能の共存可能判定一覧」に OpenFlow 機能と PF5200 シリーズの機能の共存可能判定を示します。

表 5-37 OpenFlow 機能と L2/L3 スイッチング機能の共存可能判定一覧

#	分類	機能	L2/L3(※1)	RSI(※2)	VSI(※3)	備考
1	LAN	イーサネット	1000BASE-T	○	○	○
2			100BASE-TX	○	○	○
3			10BASE-T	○	○	○
4			1000BASE-SX	○	○	○
5			1000BASE-LX	○	○	○
6			1000BASE-ZX	○	○	○
7			10GBASE-LR	○	○	○
8			10GBASE-SR	○	○	○
9			スタティックリンクアグリゲーション	○	○	○
10			スタンバイリンク機能	○	○	○
11			異速度混在モード	○	○	○
12	レイヤ2機能	トランスペアレントブリッジ	○	○	○	
13		VLAN	ポート VLAN	○	○	○
14			IEEE802.1Q	○	○	○
15			tag 変換	○	×	×
16		スパニングツリー	IEEE802.1D (装置単位の STP)	○ (*S1)	×	×
17			IEEE802.1w (RSTP)	○ (*S1)	×	×
18			PVST+ (VLAN 単位の STP)	○ (*S6)(*S8)	○ (*S7)	×

5. OpenFlow 機能の解説

#	分類	機能		L2/L3(※1)	RSI(※2)	VSI(※3)	備考
19	レイヤ2機能	スパニングツリー	IEEE802.1s (MSTP)	○ (*S1)	×	×	
20		Autonomous Extensible Ring Protocol		○	×	×	RSI, VSIに含まれないポートのみでサポート
21		VLAN トンネリング		○	×	○ (*B)	VSI 時のみサポート
22		IGMP / MLD snooping		○	○ (*C)	○	VLAN トンネリングと排他
23		ポート間中継遮断機能		○	○ (*B)	○ (*B)	
24		ストームコントロール		○	○	○	
25		ジャンボフレーム		○	○	○	
26		IEEE802.3ah/UDLD		○	○ (*C)	○ (*C)	
27		L2 ループ検知		○	○ (*C)	○ (*C)	
28		CFM(Connectivity Fault Management)		○	○ (*C)	○ (*C)	
29	L3スイッチ機能	ユニキャスト	IPv4 スタティックルーティング (ホスト通信)	○	○	○	
30			IPv6 スタティックルーティング (ホスト通信)	○	○	○	
31			RIP, RIP2	○	○ (*C)	○ (*C)	
32			RIPng	○	○ (*C)	○ (*C)	
33			OSPF	○	○ (*C)	○ (*C)	アドバンストセットのみサポート
34			OSPFv3	○	○ (*C)	○ (*C)	
35			BGP4 / BGP4+	○	○ (*C)	○ (*C)	
36		IPv4マルチキャスト	IGMPv2	○	○ (*C)	○ (*C)	
37			IGMPv3	○	○ (*C)	○ (*C)	

#	分類	機能		L2/L3(※1)	RSI(※2)	VSI(※3)	備考
38	L3 スイッチ機能	IPv4 マルチキャスト	PIM-SM/-SSM	○	○ (*C)	○ (*C)	
39		IPv6 マルチキャスト	MLD ver1	○	○ (*C)	○ (*C)	
40			MLD ver2	○	○ (*C)	○ (*C)	
41			PIM-SM/-SSM	○	○ (*C)	○ (*C)	
42	付加機能	フロー検出	MAC 条件	○	○ (*A)	○ (*A)	out 側のみサポート
43			IPv4 条件 (IPv4 ヘッダ, TCP ヘッダ, UDP ヘッダ)	○	○ (*A)	○ (*A)	
44			IPv6 条件 (IPv6 ヘッダ)	×	×	×	
45		フィルタ		○	○ (*A)	○ (*A)	VSI 時は、out 側フィルタは VLANID を条件に使えない。
46		QoS / Diff-serv		○	○	○	
47		帯域監視	帯域監視	○	○	○	
48			マーカー (ユーザ優先度)	○	○	○	
49			マーカー (DSCP)	○	○	○	
50			PQ	○	○	○	
51			RR	○	○	○	
52			WRR	○	○	○	
53			2 PQ+ 6 DRR	○	○	○	
54			2 PQ+ 6 WRR	○	○	○	
55			WFQ	○	○	○	
56			テーブルドロップ	○	○	○	
57		DHCPv4 リレーエージェント		○	○ (*C)	○ (*C)	
58		DHCPv4 サーバ		○	○ (*C)	○ (*C)	

5. OpenFlow 機能の解説

#	分類	機能		L2/L3(※1)	RSI(※2)	VSI(※3)	備考
59	付加機能	DHCPv6 サーバ (Prefix delegation)		○	○ (*C)	○ (*C)	
60		マルチバス(ロードバランス)	IPv4	○	○ (*B)	○ (*B)	
61			IPv6	○	○ (*B)	○ (*B)	
62		ポートミラーリング	ローカル	○	○	○	
63	信頼性	環境モニタ		○	○	○	
64		自己診断 (MD)		○	○	○	
65		ホットスタンバイ (VRRP)	IPv4	○	○ (*C)	○ (*C)	
66			IPv6	○	○ (*C)	○ (*C)	
67		アップリンク・リダンダント受信機能		○	○ (*C)	○ (*C)	
68	ネットワーク管理	SNMP ver1, ver2, ver3		○	○ (*C)	○ (*C)	
69		MIB-II, RMON, IP Forwarding MIB, Interface MIB, IPv6 MIB		○	○ (*C)	○ (*C)	
70		プライベート MIB		○	○ (*C)	○ (*C)	
71		LLDP		○	○ (*C)	○ (*C)	
72		OADP		○	○ (*C)	○ (*C)	
73		CDP		○	○ (*C)	○ (*C)	受信のみサポート
74		フロー統計	sFlow	○	○	○	
75	運用保守	運用端末接続	シリアル (コンソール)	○	○	○	
76			通信用ポート (NIF)	○	○	○	
77			マネージメントポート	○	○	○	
78		コンフィグレーション情報	CLI	○	○	○	
79		セキュリティ	ログイン認証 (パスワード / ホストアドレス /RADIUS/TACACS+)	○	○ (*C)	○ (*C)	

#	分類	機能	L2/L3(※1)	RSI(※2)	VSI(※3)	備考
80		SSH	○	○(*C)	○(*C)	
81	運用保守	管理情報収集	装置・インターフェース状態表示	○	○	○
82			運用メッセージ・ログ	○	○	○
83			回線毎統計情報	○	○	○
84		NTP	○	○(*C)	○(*C)	
85		コマンドレス保守	○	○	○	
86	省電力機能	リモート電源制御機能	○	○	○	
87		ポート LED 輝度制御機能	○	○	○	
88		消費電力モニタ機能	○	○	○	

(※1) : L2/L3 欄は該当パケットが RSI/VSI の OpenFlow インタフェースを通らない場合のサポート可否です。

(※2) : RSI 欄は該当パケットが RSI/VSI の OpenFlow インタフェース (RSI) を通る場合のサポート可否です。

(※3) : VSI 欄は該当パケットが RSI/VSI の OpenFlow インタフェース (VSI) を通る場合のサポート可否です。

ここでは、該当パケットとは、通信パケットに何かの処理（ミラーリング、転送等）をする機能の場合は通信パケットそのものを表し、プロトコル（LLDP 等）の場合はプロトコルパケットを表します。

5. OpenFlow 機能の解説

【L2/L3 欄の記号】

○：使用できる。

×：使用できない。

(*S1)～(*S8)：条件を満たしている場合、使用できる。

「(4) STP, RSTP, MSTP, PVST+ を OpenFlow と共存させる場合の注意事項」参照

【RSI, VSI 欄の記号】

○：使用できる。OpenFlow 動作と独立して動作し、OpenFlow 動作も処理される。

×：使用できない。

(*A)：入力インターフェースでの動作は、flow detection mode コマンドで指定したフロー検出モードによって動作が異なる。OpenFlow 動作との間に、以下のような優先度の差がある。

1. Filter による廃棄は常に優先される。
2. フロー検出モードに openflow-1 を指定した時、Filter, QoS は使用できない。
3. フロー検出モードに openflow-2 を指定した時、QoS と OpenFlow の両方で優先度制御をした場合は、OpenFlow の内容が優先される。
4. フロー検出モードに openflow-3 を指定した時、QoS と OpenFlow の両方で優先度制御をした場合は、QoS の内容が優先される。

(*B)：以下の条件を満たしている場合、使用できる。

1. miss-action コマンドで controller を指定した時、通信パケットを NORMAL に OUTPUT するフローエントリが登録されていれば、L2/L3 スイッチング機能で処理される。
2. miss-action コマンドで normal を指定した時、L2/L3 スイッチング機能で処理される。

(*C)：以下の条件を満たしている場合、使用できる。

1. miss-action コマンドで controller を指定した時、プロトコルパケットを NORMAL に OUTPUT するフローエントリが登録されていれば使用できる。
2. miss-action コマンドで normal を指定した時、L2/L3 スイッチング機能で処理される。

(*S1)～(*S8)：条件を満たしている場合、使用できる。

「(4) STP, RSTP, MSTP, PVST+ を OpenFlow と共存させる場合の注意事項」参照

※備考欄に注がある場合は、その条件下でサポートする。

ただし、制御フレームを廃棄または転送するようなフローエントリを登録すると、L2/L3 スイッチング機能は正常に動作しなくなりますので、登録しないでください。miss-action normal 時でも、制御フレームがヒットするフローエントリの登録が必要な場合は、制御フレームを NORMAL に転送するフローエントリを合わせて登録してください。

(4) STP, RSTP, MSTP, PVST+ を OpenFlow と共存させる場合の注意事項

STP, RSTP, MSTP, PVST+ は下記の *S1～*S8 のいずれかの条件下でのみ動作させることができます。

*S1～*S8 はそれぞれ排他で、同時にいずれか 1 つの使用方法のみで使用することができます。

「表 5-37 OpenFlow 機能と L2/L3 スイッチング機能の共存可能判定一覧」の (*S1)～(*S8) の注に対する注意事項を示します。

(1) STP, RSTP, MSTP 使用時の注意事項

(*S1): L2/L3 スイッチング機能で使用する場合

OpenFlow 機能と一緒に動作させることはできません。STP, RSTP, MSTP を有効にする際は OpenFlow 機能を無効にしてください。また、OpenFlow 機能を有効にする際は STP, RSTP, MSTP を無効にしてください。

(2) PVST+ 使用時の注意事項

(*S6):[RSI モード時] L2/L3 スイッチング機能で使用する場合

RSI モードで使用する際には、OpenFlow インタフェース以外のポートで PVST+ を使用することができます。この際、下記の条件を満たす必要があります。

- 条件 1 : RSI に含まれないポートだけからなる VLAN に対してのみ PVST+ を適用すること。
- 条件 2 : 条件 1 を満たす VLAN 以外の VLAN の PVST+ を無効にする設定をすること。

(*S7):[RSI モード時] OpenFlow インタフェースのポートで使用する場合

RSI モードで使用する際には、OpenFlow インタフェースのポートで PVST+ を使用することができます。この際、下記の条件を満たす必要があります。

- 条件 1 : VLAN を構成するすべてのポートが l2-inband コマンドで OpenFlow の制御対象外となつているような VLAN のみに PVST+ を適用すること。
- 条件 2 : 条件 1 を満たす VLAN 以外の VLAN の PVST+ を無効にする設定をすること。

本操作は、PVST+ 対象の vlan を OpenFlow の制御対象外として、OpenFlow インタフェースで PVST+ を動作させるという操作です。PVST+ が RSI モードと連携して動作するわけではありません。

(*S8):[VSI モード時] L2/L3 スイッチング機能で使用する場合

VSI モードで使用する際には、VSI の VLAN 以外の VLAN を構成するポートで PVST+ を使用することができます。ただし、下記の条件を満たす必要があります。

- 条件 1 : VSI の VLAN を構成するポートが VSI 以外の VLAN を構成するポートに含まれていないこと。
- 条件 2 : VSI に指定されている VLAN の PVST+ を無効にする設定をすること。

(5) VLAN トンネリングに関する注意事項

VLAN トンネリングと他機能との関係について、仕様一覧を次に示します。

表 5-38 VLAN トンネリング仕様一覧

#	機能	対象機種	解説
1	ポート VLAN	設定可	VLAN トンネリング機能はポート VLAN で設定する
2	デフォルト VLAN	自動加入なし	デフォルト VLAN への自動加入を一切行わない。デフォルト VLAN 自体は存在する。構成定義で明示的にアクセスポート、トランクポート指定した場合はその指定で動作する。
3	VLAN TPID	可	0x8100 以外の TPID を指定可能。PF5200 シリーズでは 0x8100 以外の TPID 指定時、指定値以外は TPID と扱われない。
4	ハイブリッドリンク	不可	アクセスポートとトランクポートの同一ポート共存は不可
5	VLAN トンネリング	—	
6	未定義フレーム廃棄機能	—	設定は可能。 アクセスポート（アクセス回線）の動作： 本機能は動作しない。すべてのフレームを受け入れる。 トランクポート（バックボーン回線）の動作： 常にこの起動が動作しているのと同様となる。ハイブリッドリンク不可で未定義フレームを扱う VLAN が存在しないため。
7	VLAN 每 MAC アドレス	—	VLAN トンネリング時は L3 中継しない。
8	MAC 学習	—	MAC ヘッダと先頭 tag の組み合わせで MAC アドレス学習する。

5. OpenFlow 機能の解説

#	機能	対象機種	解説
9	BPDU フォワーディング	可	アクセス回線から BPDU を受信した場合に VLAN トネリング網を通過させることができる BPDU フォワーディングを設定するとバックボーン回線でスパニングツリーが使用できない。
10	リンクアグリゲーション	可	通常通り動作
11	スパニングツリー (single)	制限有り	VLAN トネリング使用時は trunk ポートのみ動作可能とする。
12	スパニングツリー (PVST+)	制限有り	VLAN トネリング使用時は trunk ポートのみ動作可能とする。
13	スパニングツリー (MSTP)	制限有り	VLAN トネリング使用時は trunk ポートのみ動作可能とする。
14	LLDP/OADP	可	通常通り動作
15	IGMP snooping MLD snooping	不可	tag 2段以上の IGMP パケットおよび MLD パケットを snooping することはできない。
16	ジャンボフレーム	—	バックボーン回線は、ジャンボフレーム機能で 1522 バイト以上(FCS 除く)を設定する。
17	filter / QoS, Shaper	可	VLAN タグは先頭 tag が条件評価の対象となる。 VLAN タグ 0 - 2段までのフレームは L3 条件も動作する。
18	VLAN に ip(L3 機能)	可	VLAN トネリングと VLAN への ip 設定が共存可
19	タグ変換	可	通常通り動作
20	ポート間遮断機能	可	通常通り動作
21	ポートミラーリング	可	モニターポートのみ可。ミラーポートは vlan 動作しない。

6

OpenFlow 機能の設定と運用

この章では、OpenFlow 機能の設定例について説明します。

6.1 運用手順

6.2 OpenFlow 機能のコンフィグレーション

6.3 OpenFlow 機能のオペレーション

6.1 運用手順

6.1.1 概要

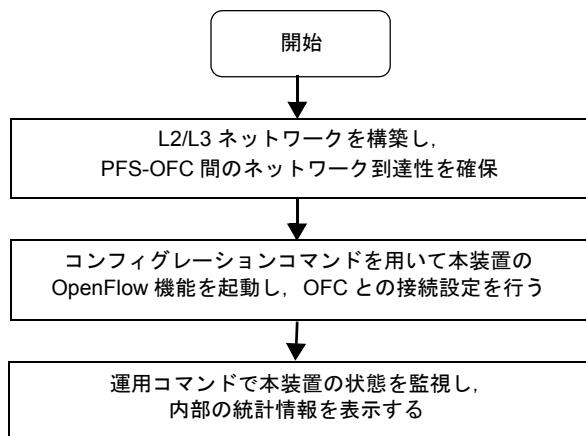
OpenFlow 機能を利用するためには、OFC からの制御が必要になります。そのため、本装置の L2/L3 スイッチング機能で PFS-OFC 間のネットワーク構築・設定を行い、ネットワークの到達性を確保します。

PFS-OFC 間のネットワークの構築・設定を完了後、OpenFlow 機能を起動し、OpenFlow 機能のコンフィグレーションを設定し運用を開始します。OFC と Secure Channel を確立するために使用するポートでは、OpenFlow 機能を無効にしてください。

6.1.2 運用の流れ

本装置の OpenFlow 機能の運用フローを示します。

図 6-1 OpenFlow 機能運用の流れ



6.2 OpenFlow 機能のコンフィグレーション

6.2.1 コンフィグレーションコマンド一覧

OpenFlow 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 6-1 コンフィグレーションコマンド一覧

コマンド名	説明
controller	接続先 OFC を指定します
connect timeout	OFC との接続試行を中止するまでのタイムアウト時間を指定します
connect timeout retry	OFC との接続が失敗した場合に、再度接続試行処理を開始するまでの待ち時間の最大値を指定します
dpid	OpenFlow インスタンスの Data Path ID を指定します
echo-reply timeout	Echo Request メッセージに対する Echo Reply メッセージ受信までの保護時間を設定します
echo-request interval	Echo Request メッセージの送信間隔を設定します
emergency-mode disable	Emergency モードを無効にします
enable	OpenFlow 機能を有効にします
openflow-interface	RSI の所属ポート、所属リンクアグリゲーションインターフェースを設定します
openflow-vlan	VSI の所属 VLAN を設定します
l2-inband-secure-channel	OpenFlow の制御から除外する VLAN ID とポートを指定します
mac-learning disable	ダイナミックな MAC アドレス学習を抑止します
miss-action	パケットがエントリにヒットしなかった時、OFC へパケットを送信するか、従来の L2/L3 スイッチング機能による転送を行うかを設定します
openflow	OpenFlow インスタンスを作成します
openflow-table-resource	OpenFlow で扱うフローテーブルでの最大エントリ数の配分パターンを設定します
outbound	出力インターフェースから送信されるトラフィックのうち、VSI を構成する VLAN から送信されるトラフィックの最大出力レートを制限します
port-modify-access	Port Mod メッセージによるアクセスポートへの設定変更の可否を設定します
port-modify-trunk	Port Mod メッセージによるトランクポートへの設定変更の可否を設定します
table	テーブル毎にフローの上限数、および検索優先度の境界値を設定します

6.2.2 OpenFlow 機能のコンフィグレーションを設定する前に

OpenFlow 機能のコンフィグレーションを設定する前に、受信側および送信側インターフェースに対するフロー検出モードを設定してください。設定例を以下に示します。

[設定のポイント]

フィルタ・QoS 機能・OpenFlow 機能の最大ハードウェアエントリ数の配分パターンを変更します。運用形態に応じた配分パターンに変更することで、ハードウェアリソースを必要なテーブルに集中させて使用できるようになります。

[コマンドによる設定]

1. **(config)# flow detection mode openflow-3**

受信側フロー検出モード openflow-3 を有効にします。

2. **(config)# no flow detection mode**

既に設定されている受信側フロー検出モードを無効にします。

3. **(config)# flow detection out mode openflow-2-out**

送信側フロー検出モード openflow-2-out を有効にします。

4. **(config)# no flow detection out mode**

既に設定されている送信側フロー検出モードを無効にします。

[注意事項]

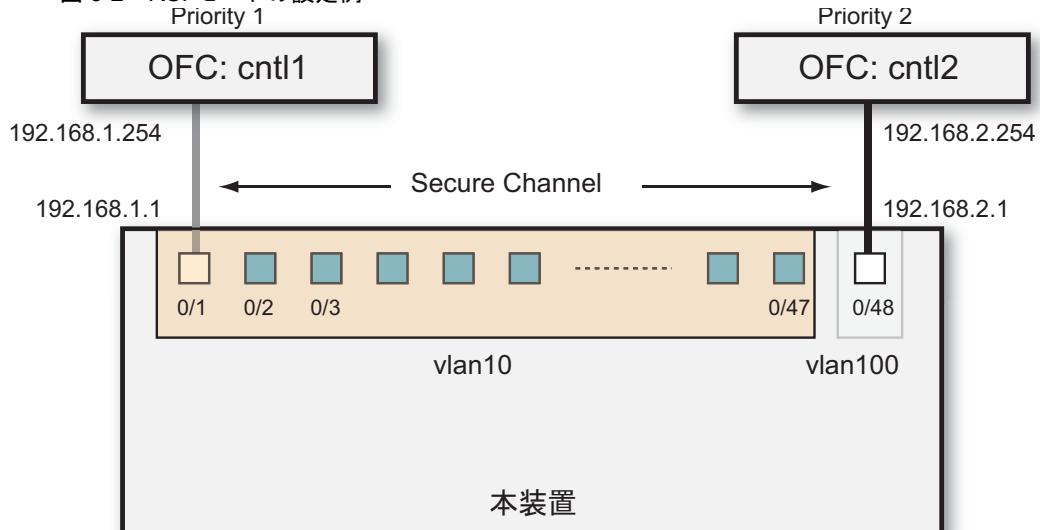
- **flow detection mode** コマンド設定後、一時的にデータ送受信不可となります。

6.2.3 RSI モードの設定例

[設定のポイント]

RSI に OFC を 2 台接続した場合の設定例を示します。

図 6-2 RSI モードの設定例
Priority 1



<OpenFlow パラメータ設定 >

```

DPID          : 0000000000000001
miss-action   : controller
echo-request interval : 10
echo-reply timeout    : 5
connect timeout      : 30
connect timeout retry: 60
table normal priority: 30000
table expanded priority: 24000
  
```

■ : OpenFlow インタフェース

* 本装置は 2 台の OFC と接続しており、うち priority 値の高い cntl2 と SecureChannel の接続を確立しています。

[コマンドによる設定]

(config) # interface vlan 10	→VLAN 10の設定
(config-if) # ip address 192.168.1.1 255.255.255.0	→VLAN 10のIPアドレスを設定
(config-if) # interface vlan 100	→VLAN 100の設定
(config-if) # ip address 192.168.2.1 255.255.255.0	→VLAN 100のIPアドレスを設定
(config-if) # interface range gigabitethernet 0/1-47	→インターフェース0/1-47の設定
(config-if-range)# switchport mode access	→インターフェースをアクセスモードに設定
(config-if-range)# switchport access vlan 10	→インターフェースをVLAN 10に設定
(config-if-range)# interface gigabitethernet 0/48	→インターフェース0/48の設定
(config-if) # switchport mode access	→インターフェースをアクセスモードに設定
(config-if) # switchport access vlan 100	→インターフェースをVLAN 100に設定
(config-if) # exit	

6. OpenFlow 機能の設定と運用

```
(config)# openflow openflow-id 1 real-switch          →OpenFlow RSIコンフィグレーションモードに遷移
(config-of)# controller controller-name cntl1 1 192.168.1.254 port 6633   →接続先OFC:cntl1の指定
(config-of)# controller controller-name cntl2 2 192.168.2.254 port 6633   →接続先OFC:cntl2の指定
(config-of)# dpid 0000000000000001                  →Data Path IDを指定
(config-of)# openflow-interface gigabitethernet 0/2-47   →RSI所属ポートの指定
(config-of)# echo-request interval 10                 →Echo Request 送信間隔値設定
(config-of)# echo-reply timeout 5                   →Echo Replyタイムアウト値設定
(config-of)# connect timeout 30                  →接続試行タイムアウト値設定
(config-of)# connect timeout retry 60            →接続試行Retry時間最大値設定
(config-of)# table normal1 priority 30000        →normal1とexpandedのフロー テーブル検索優先度の境界値設定
(config-of)# table expanded priority 24000       →expandedとnormal2のフロー テーブル検索優先度の境界値設定
(config-of)# enable                                →OpenFlow機能を有効化
(config-of)# exit
```

[注意事項]

- enable コマンド投入後の設定変更は、コマンドによって反映しない場合があります。
（「6.3 OpenFlow 機能のオペレーション」参照） no enable コマンドにより Secure Channel 切断後、設定変更を行い、再度 enable コマンドを投入してください。

6.2.4 RSI モードのパラメータ設定

(1) OpenFlow スイッチインスタンスの作成

[設定のポイント]

RSI を作成します。

[コマンドによる設定]

1. **(config)# openflow openflow-id 1 real-switch**
RSI としてスイッチを動作させるためインスタンスを作成します。

[注意事項]

- 設定削除の場合、接続中の Secure Channel が切断されます。

(2) OpenFlow インタフェース (ポート、リンクアグリゲーション) の設定

[設定のポイント]

RSI の所属ポートの指定および追加・削除を行います。本設定は、RSI インスタンス作成において必須となります。

[コマンドによる設定]

1. **(config-of)# openflow-interface gigabitethernet 0/2-47**
RSI 所属ポートとして、gigabitethernet 0/2-47 を設定します。
2. **(config-of)# openflow-interface port-channel 10**
RSI 所属ポートチャンネルとして、チャンネルグループ 10 を設定します。

[注意事項]

- add/remove パラメータ省略時、設定の上書きを行います。
- l2-inband-secure-channel コマンド中に関連している <interface id list> の設定が残っている場合、削除を行わないでください。
- l2-inband-secure-channel コマンド中の <vlan id> に関連している設定が残っている場合、削除を行わないでください。

(3) DPID 設定

[設定のポイント]

RSI に Data Path ID を設定します。

Data Path ID は、64 ビットの Data Path ID を 16 進数表示形式で指定します。

設定を省略した場合、Data Path ID は上位 16bit が <Open flow ID>、下位 48bit が MAC アドレスとなります。

[コマンドによる設定]

1. (config-of)# **dpid 0000000000000001**

OpenFlow スイッチの Data Path ID として 0000000000000001 を指定します。

[注意事項]

- OpenFlow が運用中に設定を変更し、使用中の Data Path ID と異なる値を設定した場合、Secure Channel を一旦切断します。

(4) OFC の設定

[設定のポイント]

RSI と接続する OFC を指定します。OFC は最大 4 つまで設定可能です。

本設定は、RSI 作成において必須となります。

[コマンドによる設定]

1. (config-of)# **controller controller-name cntl1 1 192.168.1.254 port 6633**

(config-of)# **controller controller-name cntl2 2 192.168.2.254 port 6633**

接続先 OFC <cntl1> として、プライオリティ <1>、IPv4 アドレス <192.168.1.254>、TCP ポート <6633> を指定します。

接続先 OFC <cntl2> として、プライオリティ <2>、IPv4 アドレス <192.168.2.254>、TCP ポート <6633> を指定します。

[注意事項]

- 接続中の OFC と異なる IP アドレスまたは TCP ポート番号に変更した場合は、Secure Channel を一旦切断します。
- 削除設定の場合は、Secure Channel の切断を行います。
- RSI 内に有効な OFC の設定が複数存在する場合は、最も高いプライオリティの OFC へ接続を行います。

(5) L2-inband インタフェース

[設定のポイント]

OpenFlow の制御対象から VLAN およびポートを除外して、Secure Channel のトラフィックを保護します。最大 4 つまで設定可能です。

[コマンドによる設定]

1. **(config-of)# l2-inband-secure-channel vlan 100 gigabitethernet 0/48**

OpenFlow の制御から除外する VLAN として 100、インターフェース gigabitethernet 0/48 を指定します。

[注意事項]

- 同一 VLAN を指定した場合、上書きとなります。
- no l2-inband-secure-channel vlan <vlan id> 指定時に指定されたポートは、すべて削除されます。
- <vlan id> に関連していない <interface id list> を指定しないでください。
- 該当インスタンスの enable 中に、<vlan id list> に関連しているポートの設定変更・削除・追加を行わないでください。

(6) Secure Channel (echo request, echo reply タイマ設定)

[設定のポイント]

echo-request コマンドでは、メッセージの送信間隔を秒単位で指定します。0 を設定した場合、メッセージの送信は行いません。

echo-reply コマンドでは、メッセージ受信までの保護時間を秒単位で指定します。

[コマンドによる設定]

1. **(config-of)# echo-request interval 10**

echo-request メッセージの送信間隔を 10 秒に設定します。

2. **(config-of)# echo-reply timeout 15**

echo-reply メッセージを受信できない場合 Secure Channel を切断と判断するまでの保護時間を 15 秒に設定します。

[注意事項]

- echo-request interval コマンドで設定する値は、echo-reply timeout コマンドで設定した値（コマンドで設定していない場合はコマンド省略時の値である 9 秒）よりも小さい値を設定してください。echo-request interval コマンドで設定可能な値は 1 ~ 60 秒です。
- echo-reply timeout コマンドで設定する値は、echo-request interval コマンドで設定した値（コマンドで設定していない場合はコマンド省略時の値である 3 秒）よりも大きい値を設定してください。echo-reply timeout コマンドで設定可能な値は 2 ~ 120 秒です。

(7) Secure Channel (connect timeout, connect timeout retry タイマ設定)

[設定のポイント]

connect timeout コマンドでは、OFC との接続を開始してから、応答なしと判断するまでの応答待ち時間を秒単位で指定します。
connect timeout retry コマンドでは、OFC との接続試行間隔の最大値を秒単位で指定します。

[コマンドによる設定]

1. (config-of)# connect timeout 30

OFC との接続試行を中止するまでのタイムアウト時間を 30 秒に設定します。

2. (config-of)# connect timeout retry 60

OFC との Secure Channel 再接続試行処理を開始するまでの最大時間を 60 秒に設定します。

[注意事項]

- Secure Channel 接続動作中の場合は、connect timeout コマンド設定時点での再設定を行います。
- リトライタイマにより待ち合わせしている最中にタイマ値が変更された場合、（待ち合わせ時間 > 新リトライタイマ値となるような変更の場合）次回のリトライタイマからの設定値が有効となります。

(8) Emergency モードの設定

[設定のポイント]

Emergency モードを無効にします。デフォルトでは有効になります。

[コマンドによる設定]

1. (config-of)# emergency-mode disable

Emergency モードを無効にする場合に設定します。

2. (config-of)# no emergency-mode disable

無効に設定した Emergency モードを有効に戻す場合に設定します。

(9) フローテーブル検索優先度の境界値・上限数の設定

[設定のポイント]

各フローテーブルの検索優先度の境界値、フローエントリ数の上限値を登録します。(ただし、`{software, vnormal1, vexpanded, vnormal2, qnormal1}` テーブルには境界値を設定しても無効です。) 境界値を設定する際は、各フローテーブルの検索優先度の境界値が、`normal1>expanded>normal2` となるように指定してください。例えば、`normal1` フローテーブルの境界値を 30000、`expanded` フローテーブルの境界値を 24000 とすると、Flow Mod で指定された検索優先度に従って、以下のように基本グループの各フローテーブルに登録されます。

- `normal1` : 検索優先度が 30000 ~ 65535 のフローエントリ
- `expanded` : 検索優先度が 24000 ~ 29999 のフローエントリ
- `normal2` : 検索優先度が 0 ~ 23999 のフローエントリ
- `software` : 登録されない

[コマンドによる設定]

1. **(config-of)# table normal1 priority 30000**
`normal1` と `expanded` フローテーブルの検索優先度の境界値を 30000 として設定します。
2. **(config-of)# table normal1 maxflow 512**
基本グループの `normal1` テーブルに設定するフローの上限数を 512 に設定します。
3. **(config-of)# table software maxflow 2048**
基本グループの `software` テーブルに設定するフローの上限数を 2048 に設定します。

[注意事項]

- 本コンフィグレーションで設定した値が、現在登録されているフローエントリ数を下回っている限り、新規フローの登録ができません。
- 装置使用状況により最大フロー数登録できない場合があります。
- `table` コマンドでは、設定条件により 上限値に設定できる範囲が変わります。詳しくは「コンフィグレーションコマンドレファレンス Vol.1」を参照してください。

(10) MAC アドレス学習制御

[設定のポイント]

ダイナミックな MAC アドレス学習を抑止します。MAC アドレス学習を抑止すると、自装置宛てのフレームおよびスタティックエントリが設定されたフレーム以外はフラッディングします。デフォルトでは、MAC アドレス学習機能は有効です。

[コマンドによる設定]

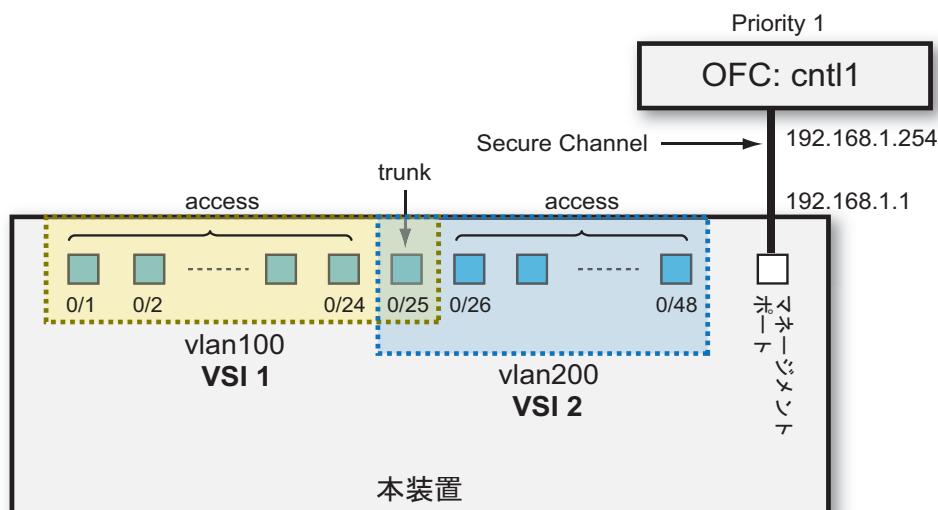
1. **(config-of)# mac-learning disable**
MAC アドレス学習機能を抑止する場合に設定します。
2. **(config-of)# no mac-learning disable**
抑止した MAC アドレス学習機能を再度起動する場合に設定します。

6.2.5 VSI モードの設定例

[設定のポイント]

VSI に OFC を 1 台接続した場合の設定例を示します。本設定例では ,Secure Channel にマネージメントポートを用いています。

図 6-3 VSI モードの設定例



<OpenFlow パラメータ設定 >

: OpenFlow インタフェース

DPID	:	[VSI 1] 0000000000000001	echo-reply timeout	:	5
		[VSI 2] 0000000000000002	connect timeout	:	30
miss-action	:	controller	connect timeout retry	:	60
echo-request interval	:	10	table normal priority	:	30000
			table expanded priority	:	24000

[コマンドによる設定]

```
(config) # interface mgmt 0                                     →マネージメントポートの設定
(config-if) # ip address 192.168.1.1 255.255.255.0          →マネージメントポートのIPアドレスを設定
(config-if) # interface vlan 100                                →VLAN 100の設定
(config-if) # ip address 192.168.100.1 255.255.255.0         →VLAN 100のIPアドレスを設定
(config-if) # interface vlan 200                                →VLAN 200の設定
(config-if) # ip address 192.168.200.1 255.255.255.0         →VLAN 200のIPアドレスを設定
(config-if) # interface range gigabitethernet 0/1-24           →インターフェース0/1-24の設定
(config-if-range)# switchport mode access                      →インターフェースをアクセスモードに設定
(config-if-range)# switchport access vlan 100                  →インターフェースをVLAN 100に設定
(config-if-range)# interface range gigabitethernet 0/26-48      →インターフェース0/26-48の設定
(config-if-range)# switchport mode access                      →インターフェースをアクセスモードに設定
(config-if-range)# switchport access vlan 200                  →インターフェースをVLAN 200に設定
(config-if-range)# interface gigabitethernet 0/25              →インターフェース0/25の設定
(config-if) # switchport mode trunk                           →インターフェースをトランクモードに設定
(config-if) # switchport trunk allowed vlan 100,200           →インターフェースをVLAN 100, 200に設定
(config-if) # exit
```

6. OpenFlow 機能の設定と運用

```
(config)# openflow openflow-id 1 virtual-switch      →OpenFlow VSI ID 1 の作成
(config-of)# controller controller-name cntl1 1 192.168.1.254
(config-of)# dpid 00000000000000000001      →接続先OFC:cntl1の指定
(config-of)# openflow-vlan 100      →DataPath IDを指定
(config-of)# echo-request interval 10      →VLANマッピングの設定
(config-of)# echo-reply timeout 5      →Echo Request 送信間隔値設定
(config-of)# connect timeout 30      →Echo Reply タイムアウト値設定
(config-of)# connect timeout retry 60      →接続試行タイムアウト値設定
(config-of)# table normal1 priority 30000      →接続試行Retry時間最大値設定
(config-of)# table expanded priority 24000      →normal1とexpandedのフロー
(config-of)# port-modify-access permit      →テーブル検索優先度の境界値設定
(config-of)# port-modify-trunk permit      →expandedとnormal2のフロー
(config-of)# enable      →テーブル検索優先度の境界値設定
(config-of)# exit      →OFCによるアクセスポート
                           設定変更許可設定
(config)# openflow openflow-id 2 virtual-switch      →OpenFlow VSI ID 2 の作成
(config-of)# controller controller-name cntl1 1 192.168.1.254
(config-of)# dpid 00000000000000000002      →接続先OFC:cntl1の指定
(config-of)# openflow-vlan 200      →DataPath IDを指定
(config-of)# echo-request interval 10      →VLANマッピングの設定
(config-of)# echo-reply timeout 5      →Echo Request 送信間隔値設定
(config-of)# connect timeout 30      →Echo Reply タイムアウト値設定
(config-of)# connect timeout retry 60      →接続試行タイムアウト値設定
(config-of)# table normal1 priority 30000      →接続試行Retry時間最大値設定
(config-of)# table expanded priority 24000      →normal1とexpandedのフロー
(config-of)# port-modify-access permit      →テーブル検索優先度の境界値設定
(config-of)# port-modify-trunk permit      →expandedとnormal2のフロー
(config-of)# enable      →テーブル検索優先度の境界値設定
(config-of)# exit      →OFCによるアクセSpoort
                           設定変更許可設定
                           設定変更許可設定
                           →OpenFlow 機能を有効化
```

[注意事項]

- enable コマンド投入後の設定変更は、コマンドによって反映しない場合があります。
（「6.3 OpenFlow 機能のオペレーション」参照）no enable コマンドにより Secure Channel 切断後、設定変更を行い、再度 enable コマンドを投入してください。

6.2.6 VSI モードのパラメータ設定

(1) OpenFlow スイッチインスタンスの作成

[設定のポイント]

VSI を作成します。VSI は 16 個まで作成可能です。

[コマンドによる設定]

1. (config)# openflow openflow-id 1 virtual-switch
VSI としてスイッチを動作させるためインスタンスを作成します。

[注意事項]

- 設定削除の場合、接続中の Secure Channel が切断されます。

(2) VLAN の指定

[設定のポイント]

VSI の所属 VLAN を設定します。
本設定は、VSI 作成において必須となります。

[コマンドによる設定]

1. **(config-of)# openflow-vlan 10**

VSI の所属 VLAN として、vlan id 10 を指定します。

[注意事項]

- 他の Virtual Switch Instance にて同一 VLAN の指定はできません。
- outbound コマンドに設定が残っている場合、設定削除・変更を行わないでください。

(3) DPID 設定

[設定のポイント]

VSI に Data Path ID を設定します。

Data Path ID は、64 ビットの Data Path ID を 16 進数表示形式で指定します。

設定を省略した場合、Data Path ID は上位 16bit が <Open flow ID>、下位 48bit が MAC アドレスとなります。

[コマンドによる設定]

1. **(config-of)# dpid 0000000000000001**

OpenFlow スイッチの Data Path ID として 0000000000000001 を指定します。

[注意事項]

- OpenFlow が運用中に設定を変更し、使用中の Data Path ID と異なる値を設定した場合、Secure Channel を一旦切断します。

(4) OFC の設定

[設定のポイント]

VSI と接続する OFC を指定します。OFC は VSI 毎に最大 4 つまで設定可能です。

[コマンドによる設定]

1. **(config-of)# controller controller-name cntl1 1 192.168.1.254 port 6633**

(config-of)# controller controller-name cntl2 2 192.168.2.254 port 6633

接続先 OFC <cntl1> として、プライオリティ <1>、IPv4 アドレス <192.168.1.254>、TCP ポート <6633> を指定します。

接続先 OFC <cntl2> として、プライオリティ <2>、IPv4 アドレス <192.168.2.254>、TCP ポート <6633> を指定します。

[注意事項]

- 接続中の OFC と異なる IP アドレスまたは TCP ポート番号に変更した場合は、Secure Channel を一旦切断します。
- 削除設定の場合は、Secure Channel の切断を行います。
- VSI 内に有効な OFC の設定が複数存在する場合は、最も高いプライオリティの OFC へ接続を行います

(5) Secure Channel (echo request, echo reply タイマ設定)

[設定のポイント]

echo-request コマンドでは、メッセージの送信間隔を秒単位で指定します。0 を設定した場合、メッセージの送信は行いません。
echo-reply コマンドでは、メッセージ受信までの保護時間を秒単位で指定します。

[コマンドによる設定]

1. (config-of)# echo-request interval 10

echo-request メッセージの送信間隔を 10 秒に設定します。

2. (config-of)# echo-reply timeout 15

echo-reply メッセージを受信できない場合 Secure Channel を切断と判断するまでの保護時間を 15 秒に設定します。

[注意事項]

- echo-request interval コマンドで設定する値は、echo-reply timeout コマンドで設定した値（コマンドで設定していない場合はコマンド省略時の値である 9 秒）よりも小さい値を設定してください。
echo-request interval コマンドで設定可能な値は 1 ~ 60 秒です。
- echo-reply timeout コマンドで設定する値は、echo-request interval コマンドで設定した値（コマンドで設定していない場合はコマンド省略時の値である 3 秒）よりも大きい値を設定してください。
echo-reply timeout コマンドで設定可能な値は 2 ~ 120 秒です。

(6) Secure Channel (connect timeout, connect timeout retry タイマ設定)

[設定のポイント]

connect timeout コマンドでは、OFC との接続を開始してから、応答なしと判断するまでの応答待ち時間を秒単位で指定します。connect timeout retry コマンドでは、OFC との接続試行間隔の最大値を秒単位で指定します。

[コマンドによる設定]

1. (config-of)# connect timeout 30

OFCとの接続試行を中止するまでのタイムアウト時間を30秒に設定します。

2. (config-of)# connect timeout retry 60

OFCとのSecure Channel再接続試行処理を開始するまでの最大時間を60秒に設定します。

[注意事項]

- Secure Channel接続動作中の場合は、connect timeoutコマンド設定時点でのタイマの再設定を行います。
- リトライタイマにより待ち合わせしている最中にタイマ値が変更された場合、(待ち合わせ時間>新リトライタイマ値となるような変更の場合)次回のリトライタイマからの設定値が有効となります。

(7) Emergencyモードの設定

[設定のポイント]

Emergencyモードを無効にします。デフォルトでは有効になります。

[コマンドによる設定]

1. (config-of)# emergency-mode disable

Emergencyモードを無効にする場合に設定します。

2. (config-of)# no emergency-mode disable

無効に設定したEmergencyモードを有効に戻す場合に設定します。

(8) フローテーブル検索優先度の境界値・上限数の設定

各フローテーブルの検索優先度の境界値、フローエントリ数の上限値を登録します。(ただし、{software, vnormal1, vexpanded, vnormal2, qnormal1}テーブルには境界値を設定しても無効です。)境界値を設定する際は、各フローテーブルの検索優先度の境界値が、normal1>expanded>normal2となるように指定してください。例えば、normal1フローテーブルの境界値を30000、expandedフローテーブルの境界値を24000とすると、Flow Modで指定された検索優先度に従って、以下のように基本グループの各フローテーブルに登録されます。

- normal1：検索優先度が30000～65535のフローエントリ
- expanded：検索優先度が24000～29999のフローエントリ
- normal2：検索優先度が0～23999のフローエントリ
- software：登録されない

[コマンドによる設定]

1. (config-of)# table normal1 priority 30000

normal1とexpandedフローテーブルの検索優先度の境界値を30000として設定します。

2. (config-of)# table normal1 maxflow 512

基本グループのnormal1テーブルに設定するフローの上限数を512に設定します。

3. (config-of)# table software maxflow 2048

基本グループのsoftwareテーブルに設定するフローの上限数を2048に設定します。

[注意事項]

- 本コンフィグレーションで設定した値が、現在登録されているフローエントリ数を下回っている限り、新規フローの登録ができません。
- 装置使用状況により最大フロー数登録できない場合があります。

(9) MAC アドレス学習制御

[設定のポイント]

ダイナミックな MAC アドレス学習を抑止します。MAC アドレス学習を抑止すると、自装置宛てのフレームおよびスタティックエントリが設定されたフレーム以外はフラッディングします。デフォルトでは、MAC アドレス学習機能は有効です。

[コマンドによる設定]

1. **(config-of)# mac-learning disable**

MAC アドレス学習機能を抑止する場合に設定します。

2. **(config-of)# no mac-learning disable**

抑止した MAC アドレス学習機能を再度起動する場合に設定します。

(10) 出力インターフェースにおける VSI 帯域制限

[設定のポイント]

出力インターフェースから送信されるトラフィックのうち、VSI を構成する VLAN から送信されるトラフィックの最大出力レートを制限します。

[コマンドによる設定]

1. **(config-of)# outbound gigabitethernet 0/25 max-rate 2M**

出力インターフェース gigabitethernet 0/25 から送信される、当該 VSI を構成する VLAN のトラフィックの最大出力レートを 2Mbps に設定します。

[注意事項]

- max-rate と max-rate-burst は、同時省略不可となります。
- 設定可能なコマンド数は、装置あたり 128 となります。
- openflow-vlan にて設定を行った VLAN インタフェースに所属しないポートの指定を行わないでください。

(11) PortMod によるポート状態変更の可否設定

[設定のポイント]

PortMod メッセージによるアクセス / トランクポートへの設定変更の可否を設定します。
デフォルトでは、拒否 (deny) となります。

[コマンドによる設定]

1. (config-of)# **port-modify-access permit**

OFC からアクセスポートへの設定変更を許可する場合、設定します。

2. (config-of)# **port-modify-access deny**

OFC からアクセスポートへの設定変更を拒否する場合、設定します。

3. (config-of)# **port-modify-trunk permit**

OFC からトランクポートへの設定変更を許可する場合、設定します。

4. (config-of)# **port-modify-trunk deny**

OFC からトランクポートへの設定変更を拒否する場合、設定します。

6.3 OpenFlow 機能のオペレーション

6.3.1 オペレーションコマンド一覧

表 6-2 オペレーションコマンド一覧

コマンド名	説明
show openflow	OpenFlow 情報を表示します
show openflow table	OpenFlow のフローテーブル情報を表示します
show openflow statistics	OFC との通信に関する統計情報を表示します
show openflow resource	OpenFlow リソース情報を表示します
show openflow controller-session	PFS - OFC 間で送受信する OpenFlow プロトコルメッセージをリアルタイムに表示します
clear openflow table	OpenFlow のフローテーブル情報をクリアします
clear openflow statistics	OFC との通信に関する統計情報をクリアします
restart openflow	OpenFlow プログラムを再起動します
dump protocols openflow	OpenFlow 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情報をファイルへ出力します

6.3.2 OpenFlow 情報の確認

show openflow detail コマンドで、OpenFlow 情報を確認できます。

(1) RSI モードの場合

図 6-4 OpenFlow 詳細情報の表示例 (RSI モードの場合)

```
> show openflow detail [Enter]キー押下
Date 2011/09/01 13:30:00 JST

Switch Protocol Version : 0x01 .....(a)
Flow Detection Mode      : openflow-1

[OpenFlow 1 Real]
  OpenFlow Software State   : enable .....(b)
  VLAN ID                  : -
  Data Path ID              : 0x0101010101010101 .....(c)
  Data Path Name :
    PFS_01
  Controller Connection Mode : single
  Number of Controllers     : 1
  Controllers :
    #1 : Cnt11 192.168.0.254 (port 6633, pri 1, ver 0x01) is connected .....(d)
        connection method          : TCP
        session connect time 0day 0:06:33
        session reset time ----/--- --:--- ---:---
        connect retry count       : 0
        connect retry timer(max/current) : 1 sec/ 0 sec
        deterrence level         : 0
        band limit for paket-in   : unlimited
        asynchronous message      : NONE

  Miss Action                : controller .....(e)
  Miss Send Length           : 65535
  Handling IP Fragments      : normal
  Connect Timeout             : 3 sec .....(f)
  Connect Retry Timer         : 1 sec .....(g)
  Echo Request Interval       : 3 sec .....(h)
  Echo Reply Timeout          : 9 sec .....(i)
  Emergency Mode             : disable
  MAC Learning               : disable
  Controller Mode             : 1

  Port                      : 0/1-2,25-26 .....(j)
  ChGr(LAG)                 : .....(k)
  Number of ports : 4
  Port State : _: undefined, U: Up, D: Down
    Line : 1 10 11 20 21 30 31 40 41 50 51
    Port : UU _____ UU _____
    ChGr(LAG) :
  Controller Administered Port State : _: undefined, U: Up, D: Down
    Line : 1 10 11 20 21 30 31 40 41 50 51
    Port : UU _____ UU _____
    ChGr(LAG) :
  Port Group : NONE .....(l)
  Allowed VLAN :
    GBE0/1 : 100*
    GBE0/2 : 100*
    GBE0/25 : 100*
    GBE0/26 : 100*

  Switch Support Buffer Size   : 544 Packets
  Switch Support Number of Tables : 9
  Switch Support Capabilities :
    FLOW_STATS : enable TABLE_STATS : enable
    PORT_STATS : enable STP : disable
    IP_REASM : disable QUEUE_STATS : disable
    ARP_MATCH_IP : enable
  Switch Support Action :
    OUTPUT : enable STRIP_VLAN : enable
    SET_VLAN_VID : enable SET_VLAN_PCP : enable
    SET_DL_SRC : enable SET_DL_DST : enable
    SET_NW_SRC : enable SET_NW_DST : enable
    SET_NW_TOS : enable SET_TP_SRC : enable
    SET_TP_DST : enable ENQUEUE : enable
    VENDOR : disable
```

6. OpenFlow 機能の設定と運用

```

Switch Port Feature :
  if-name      port-no    config     state   current  advertise  support   peer
  GBE0/1       : 0x00000001 0x0002    0x0200  0x02a0   0x0000    0x0000  0x0000
  GBE0/2       : 0x00000002 0x0002    0x0200  0x02a0   0x0000    0x0000  0x0000
  GBE0/25      : 0x00000019 0x0002    0x0200  0x02a0   0x0000    0x0000  0x0000
  GBE0/26      : 0x0000001a 0x0002    0x0200  0x02a0   0x0000    0x0000  0x0000

Inband Secure Channel :

Emergency-LinkDown ports : _: undefined, D: Down ..... (m)
  Line : 1      10 11      20 21      30 31      40 41      50 51
  Port : _____
  ChGr(LAG) : _____
Emergency-FlowDeletion ports : _: undefined, D: Delete
  Line : 1      10 11      20 21      30 31      40 41      50 51
  Port : _____
  ChGr(LAG) : _____
ControllerRecover-LinkUp ports : _: undefined, U: Up
  Line : 1      10 11      20 21      30 31      40 41      50 51
  Port : _____
  ChGr(LAG) : _____
>

```

[確認のポイント]

- (a) Switch Protocol Version : OpenFlow バージョン情報です。
- (b) OpenFlow Software State : OpenFlow インスタンスのステータス遷移状態です。
- (c) Data Path ID : OpenFlow ID です。
- (d) Configure Controller : 接続先 Controller の構成情報です。
- (e) Miss Action : パケットがフローエントリにヒットしなかった時の動作です。
- (f) Connect Timeout : Controller との接続試行タイムアウト値です。
- (g) Connect Retry Timer : 接続試行 Retry 時間(最大値 / 現在のタイマ値)です。
- (h) Echo Request Interval : Echo Request 送信間隔です。
- (i) Echo Reply Timeout : Echo Reply 待ちタイムアウト値です。
- (j) Port : OpenFlow インスタンスの有効ポートです。
- (k) ChGr(LAG) : OpenFlow インスタンスの有効リンクアグリゲーションインターフェース (LAG) です。
- (l) Port Group : OpenFlow で使用しているポートグループの状態を表示します。
- (m) Emergency-LinkDown ports : Emergency-LinkDown の対象ポートです。

(2) VSI モードの場合

図 6-5 OpenFlow 詳細情報の表示例 (VSI モードの場合)

```

> show openflow detail [Enter]キー押下
Date 2011/09/01 13:30:00 JST

Switch Protocol Version : 0x01 ..... (a)
Flow Detection Mode     : openflow-1

[OpenFlow 1 Virtual]
  OpenFlow Software State   : enable ..... (b)
  VLAN ID                  : 100
  Data Path ID             : 0x0101010101010101 ..... (c)
  Data Path Name :
    PFS_01-01
  Controller Connection Mode : single
  Number of Controllers     : 1
  Controllers :
    #1 : Cnt11 192.168.0.254 (port 6633, pri 1, ver 0x01) is connected ..... (d)
      connection method        : TCP
      session connect time    : 0day 0:01:15
      session reset time      : 2011/09/01 13:28:45 JST
      connect retry count     : 1
      connect retry timer(max/current) : 1 sec/ 0 sec
      deterrence level        : 0
      band limit for paket-in : unlimited

```

```

asynchronous message :
NONE

Miss Action : controller ..... (e)
Miss Send Length : 65535
Handling IP Fragments : normal
Connect Timeout : 3 sec ..... (f)
Connect Retry Timer : 1 sec ..... (g)
Echo Request Interval : 3 sec ..... (h)
Echo Reply Timeout : 9 sec ..... (i)
Emergency Mode : disable
MAC Learning : disable
Controller Mode : 1

Port Modify :
Access : deny
Trunk : deny

Port : 0/1-2,25-26 ..... (j)
ChGr(LAG) : ..... (k)
Number of ports : 4
Port State : _ undefined, U: Up, D: Down
Line : 1 10 11 20 21 30 31 40 41 50 51
Port : UU _____ UU _____
ChGr(LAG) :
Controller Administered Port State : _ undefined, U: Up, D: Down
Line : 1 10 11 20 21 30 31 40 41 50 51
Port : UU _____ UU _____
ChGr(LAG) :
Port Group : NONE ..... (l)

Switch Support Buffer Size : 544 Packets
Switch Support Number of Tables : 9
Switch Support Capabilities :
FLOW_STATS : enable TABLE_STATS : enable
PORT_STATS : enable STP : disable
IP_REASM : disable QUEUE_STATS : disable
ARP_MATCH_IP : enable
Switch Support Action :
OUTPUT : enable STRIP_VLAN : enable
SET_VLAN_VID : enable SET_VLAN_PCP : enable
SET_DL_SRC : enable SET_DL_DST : enable
SET_NW_SRC : enable SET_NW_DST : enable
SET_NW_TOS : enable SET_TP_SRC : enable
SET_TP_DST : enable ENQUEUE : enable
VENDOR : disable
Switch Port Feature :
if-name port-no config state current advertise support peer
GBE0/1 : 0x00000001 0x0002 0x0200 0x02a0 0x0000 0x0000 0x0000
GBE0/2 : 0x00000002 0x0002 0x0200 0x02a0 0x0000 0x0000 0x0000
GBE0/25 : 0x00000019 0x0002 0x0200 0x02a0 0x0000 0x0000 0x0000
GBE0/26 : 0x0000001a 0x0002 0x0200 0x02a0 0x0000 0x0000 0x0000

Outbound Rate :
port-id max-rate max-rate-burst
lag-id max-rate max-rate-burst

Emergency-LinkDown ports : _ undefined, D: Down ..... (m)
Line : 1 10 11 20 21 30 31 40 41 50 51
Port :
ChGr(LAG) :
Emergency-FlowDeletion ports : _ undefined, D: Delete
Line : 1 10 11 20 21 30 31 40 41 50 51
Port :
ChGr(LAG) :
ControllerRecover-LinkUp ports : _ undefined, U: Up
Line : 1 10 11 20 21 30 31 40 41 50 51
Port :
ChGr(LAG) :
>

```

[確認のポイント]

- (a) Switch Protocol Version : OpenFlow バージョン情報です。
- (b) OpenFlow Software State : OpenFlow インスタンスのステータス遷移状態です。
- (c) Data Path ID : OpenFlow ID です。
- (d) Configure Controller : 接続先 Controller の構成情報です。
- (e) Miss Action : パケットがフローエントリにヒットしなかった時の動作です。
- (f) Connect Timeout : Controller との接続試行タイムアウト値です。
- (g) Connect Retry Timer : 接続試行 Retry 時間(最大値 / 現在のタイマ値)です。
- (h) Echo Request Interval : Echo Request 送信間隔です。
- (i) Echo Reply Timeout : Echo Reply 待ちタイムアウト値です。
- (j) Port : OpenFlow インスタンスの有効ポートです。
- (k) ChGr(LAG) : OpenFlow インスタンスの有効リンクアグリゲーションインターフェース (LAG) です。
- (l) Port Group : OpenFlow で使用しているポートグループの状態を表示します。
- (m) Emergency-LinkDown ports : Emergency-LinkDown の対象ポートです。

6.3.3 フローテーブル情報の確認

show openflow table detail コマンドで、フローテーブル情報を確認できます。

図 6-6 フローテーブルの詳細情報の表示例 (VSI モードの場合)

```
> show openflow table openflow-id 1 detail [Enter]キー押下
Date 2011/09/01 13:30:00 JST

FLOW entries information

[OpenFlow 1]

<entry 1>
  table type           : expanded
  forwarding state    : hardware-based
  matched octets      :          0 octet .....(a)
  matched packets      :          0 packet .....(b)
  idle timer(max/current) : 0 sec / 0 sec .....(c)
  hard timer(max/current) : 0 sec / 0 sec .....(d)
  priority             : 65535 .....(e)
  added command        : vendorflowmod*
  added time           : 2011/09/01 13:25:30 JST
  last modified time   : -
  flow cookie          : 0xabcdef9012345678

  match .....(f)
    input port       : 0/ 1[0x00000001]
    src mac address : 0000.1100.0000
    dst mac address : 0000.2200.0000
    input vlan       : any
    input vlan pcp   : any
    ethernet type   : 0x86dd
    tos / dscp       : 0(0x00) / 0(0x00)
    ip protocol     : TCP
    src ip address  : 2000::2
    dst ip address  : 2000::1
    src 14 port     : 1024(0x400)
    dst 14 port     : 1025(0x401)

  action 1
    type            : OUTPUT .....(g)
    out port         : 0/ 2[0x00000002]
>
```

[確認のポイント]

- (a) matched bytes : マッチしたパケットのオクテット数の統計情報です。
- (b) matched packets : マッチしたパケット数の統計情報です。
- (c) idle timer(max/current) : 無通信時間 (最大値 / 現在の残り時間) です。
- (d) hard timer(max/current) : 最大保持時間 (最大値 / 現在の残り時間) です。
- (e) priority : エントリの優先度の値です。
- (f) match : 検索キーのフィールドです。
- (g) action : アクションの情報です。

6.3.4 OpenFlow プロトコルメッセージ統計情報の確認

show openflow statistics コマンドで、PFS と OFC 間の通信に関する統計情報を確認できます。

図 6-7 統計情報の表示例

```
> show openflow statistics [Enter]キー押下
Date 2011/09/12 16:26:57 UTC

[OpenFlow 1]
<Discard counter>
Packet In          0
#1 : ofunit1 192.168.66.254 (port 6633, pri 1, ver 0x01) is connected

<Sent messages counter>           <Received messages counter>
Hello                  1 Hello                  1
Echo Request          115 Echo Request          0
Echo Reply             0 Echo Reply             115
Features Reply         1 Features Request       1
Get Configuration Reply 0 Get Configuration Request 0
Set Configuration      0
Barrier Reply          0 Barrier Request        0
Packet Out             0
Port Status :
  ADD                 0
  DELETE              0
  MODIFY              0
Vendor :
  PF Flow Removed :
    IDLE TIMEOUT      0 ADD                   0
    HARD TIMEOUT       0 MODIFY                0
    DELETE              0 MODIFY STRICT        0
                           0 DELETE                0
                           0 DELETE STRICT         0
                           0 Port Mod             0
PF Port Group Status :
  ADD                 0
  MODIFY              0
  DELETE              0
PF Vlan Status :
  SET VLAN            0 SET VLAN              0
  CLEAR VLAN           0 CLEAR VLAN             0
  CLEAR ALL VLAN       0 CLEAR ALL VLAN         0
PF Get Config Reply   0 PF Get Config Request 0
PF Set Config          0 PF Emergency Mod :
  UPDATED             0 ADD                   0
  DELETED             0 DELETE                0
                           0 DELETE ALL             0
                           0 PF Cyclic Packet Out Mod :
                           0 ADD                   0
                           0 DELETE                0
                           0 Unknown Vendor Type 0
Statistics Reply :
  DESC                0 DESC                  0
  FLOW                0 FLOW                 0
  AGGREGATE           0 AGGREGATE             0
  TABLE               0 TABLE                 0
  PORT                0 PORT                  0
  QUEUE               0 QUEUE                 0
  VENDOR :
    FLOW STRICT        0 FLOW STRICT           0
    PF FLOW             0 PF FLOW               0
    PF FLOW STRICT      0 PF FLOW STRICT        0
    PORT GROUP          0 PORT GROUP            0
    VLAN                0 VLAN                 0
    EMERGENCY            0 EMERGENCY             0
    CYCLIC PACKET OUT    0 CYCLIC PACKET OUT      0
                           0 Unknown Vendor Type 0
```

Queue Get Config Reply	0	Unknown Type Message	0
	0	Queue Get Config Request	0
	0	Unknown Type Message	0
<Sent Error counter>		<Received Error counter>	
Error	0	Error	0
HELLO FAILED :		HELLO FAILED :	
INCOMPATIBLE	0	INCOMPATIBLE	0
EPERM	0	EPERM	0
BAD REQUEST :		BAD VERSION	0
BAD VERSION	0	BAD TYPE	0
BAD TYPE	0		
BAD STAT	0		
BAD VENDOR	0		
BAD SUBTYPE	0		
EPERM	0		
BAD LEN	0		
BUFFER EMPTY	0		
BUFFER UNKNOWN	0		
BAD ACTION :			
BAD TYPE	0		
BAD LEN	0		
BAD VENDOR	0		
BAD VENDOR TYPE	0		
BAD OUT PORT	0		
BAD ARGUMENT	0		
EPERM	0		
TOO MANY	0		
BAD QUEUE	0		
FLOW MOD FAILED :			
ALL TABLES FULL	0		
OVERLAP	0		
EPERM	0		
BAD EMERG TIMEOUT	0		
BAD COMMAND	0		
UNSUPPORTED	0		
POR T MOD FAILED :			
BAD PORT	0		
BAD HW ADDR	0		
QUEUE OP FAILED :			
BAD PORT	0		
BAD QUEUE	0		
EPERM	0		
VENDOR SET CONFIG FAILED :			
BAD ITEM FLAGS	0		
BAD PACKET IN RATE	0		
BAD LED STATUS	0		
BAD CONNECTION MODE	0		
BAD ASYNC MESSAGE	0		
BAD CONFIG TYPE	0		
EPERM	0		
VENDOR GET CONFIG REQUEST FAILED :			
BAD CONFIG TYPE	0		
EPERM	0		
VENDOR EMERGENCY MOD FAILED :			
BAD COMMAND	0		
BAD PORT	0		
BAD FLAGS	0		
CONFLICT	0		
EPERM	0		
VENDOR VLAN MOD FAILED :			
BAD COMMAND	0		
UNMATCHED INSTANCE	0		
BAD PORT	0		
BAD VALUE	0		
CONFLICT	0		
EPERM	0		
VENDOR CYCLIC PACKET OUT MOD FAILED :			
BAD COMMAND	0		
BAD PACKET ID	0		
BAD ACTION	0		
BAD PACKET DATA	0		
RESOURCE FULL	0		
EPERM	0		
Other Error Type	0	Other Error Type	0
<Secure Channel Disconnected counter>			
Secure Channel	0		
TCP Session	0		
<Cyclic Packet-out counter>			
No entry.			

>

6.3.5 PFS-OFC 間の送受信 OpenFlow プロトコルメッセージのリアルタイム表示

show openflow controller-session コマンドで、PFS-OFC 間で送受信されている OpenFlow プロトコルメッセージをリアルタイムで確認できます。

図 6-8 送受信 OpenFlow プロトコルメッセージの表示例

```
> show openflow controller-session [Enter]キー押下
Date 2011/09/12 16:32:53 UTC

16:32:56.390081 OFS( 1) SENT 192.168.66.254(6633) : ECHO_REQUEST
16:32:56.392504 OFS( 1) RECV 192.168.66.254(6633) : ECHO_REPLY
16:32:58.848847 OFS( 1) RECV 192.168.66.254(6633) : VENDOR(PF_FLOW_MOD)
16:32:58.849257 OFS( 1) SENT 192.168.66.254(6633) : ERROR(BAD_ACTION, BAD_OUT_PORT)
16:32:59.390103 OFS( 1) SENT 192.168.66.254(6633) : ECHO_REQUEST
16:32:59.392597 OFS( 1) RECV 192.168.66.254(6633) : ECHO_REPLY
16:33:02.360084 OFS( 1) SENT 192.168.66.254(6633) : ECHO_REQUEST
16:33:02.361855 OFS( 1) RECV 192.168.66.254(6633) : ECHO_REPLY
16:33:05.380089 OFS( 1) SENT 192.168.66.254(6633) : ECHO_REQUEST
16:33:05.382792 OFS( 1) RECV 192.168.66.254(6633) : ECHO_REPLY
16:33:08.390178 OFS( 1) SENT 192.168.66.254(6633) : ECHO_REQUEST
16:33:08.391946 OFS( 1) RECV 192.168.66.254(6633) : ECHO_REPLY
16:33:10.704383 OFS( 1) RECV 192.168.66.254(6633) : VENDOR(PF_FLOW_MOD)
16:33:11.360091 OFS( 1) SENT 192.168.66.254(6633) : ECHO_REQUEST
16:33:11.361866 OFS( 1) RECV 192.168.66.254(6633) : ECHO_REPLY
16:33:14.400120 OFS( 1) SENT 192.168.66.254(6633) : ECHO_REQUEST
16:33:14.401888 OFS( 1) RECV 192.168.66.254(6633) : ECHO_REPLY
16:33:17.420088 OFS( 1) SENT 192.168.66.254(6633) : ECHO_REQUEST
16:33:17.422754 OFS( 1) RECV 192.168.66.254(6633) : ECHO_REPLY
16:33:20.410092 OFS( 1) SENT 192.168.66.254(6633) : ECHO_REQUEST
16:33:20.412081 OFS( 1) RECV 192.168.66.254(6633) : ECHO_REPLY
16:33:23.420085 OFS( 1) SENT 192.168.66.254(6633) : ECHO_REQUEST
16:33:23.4223033 OFS( 1) RECV 192.168.66.254(6633) : ECHO_REPLY
16:33:26.400092 OFS( 1) SENT 192.168.66.254(6633) : ECHO_REQUEST
16:33:26.404661 OFS( 1) RECV 192.168.66.254(6633) : ECHO_REPLY
16:33:29.420076 OFS( 1) SENT 192.168.66.254(6633) : ECHO_REQUEST
16:33:29.422346 OFS( 1) RECV 192.168.66.254(6633) : ECHO_REPLY
^C
>
```

[注意事項]

- OpenFlow プログラムに対する負荷が増加するため、OFC との接続を多量に取り扱っている場合、OFC との通信に支障をきたすおそれがあります。通常運用での本コマンドの使用は避けてください。

7

VRRP

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

7.1 解説

7.2 コンフィグレーション

7.3 オペレーション

7.1 解説

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

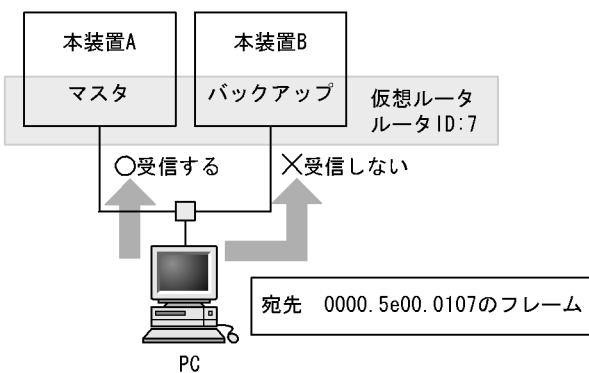
VRRP を使用すると、同一イーサネット上の複数のルータから構成される仮想ルータを設定できます。端末がデフォルトゲートウェイとしてこの仮想ルータを設定しておくことによって、ルータに障害が発生したときの別ルータへの切り替えを意識することなく、通信を継続できます。

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

7.1.1 仮想ルータの MAC アドレスと IP アドレス

仮想ルータは自身の物理的な MAC アドレスとは別に、仮想ルータ用の MAC アドレスとして仮想 MAC アドレスを持ちます。仮想 MAC アドレスは、 $0000.5e00.01\{\text{仮想ルータ ID}\}$ に決められており、仮想ルータ ID から自動的に生成されます。マスタの仮想ルータは仮想 MAC アドレス宛てのイーサネットフレームを受信してパケットをフォワーディングする能力を持ちますが、バックアップの仮想ルータは仮想 MAC アドレス宛てのフレームを受信しません。VRRP は仮想ルータの状態に応じて仮想 MAC アドレス宛てイーサネットフレームを受信するかどうかを制御します。マスタの仮想ルータは仮想 MAC 宛てフレームを受信すると、ルーティングテーブルに従って IP パケットのフォワーディング処理を行います。そのため、端末は仮想 MAC アドレスを宛先としてフレームの送出を行うことで、マスタとバックアップが切り替わった後でも通信を継続できます。仮想 MAC アドレス宛てフレームの受信を次の図に示します。

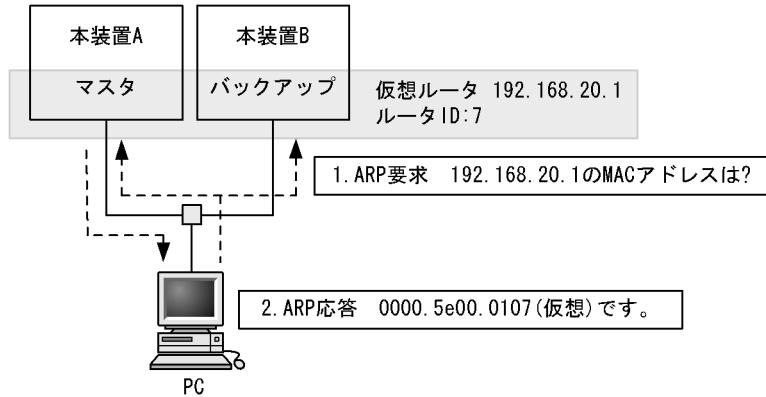
図 7-1 仮想 MAC 宛てフレームの受信



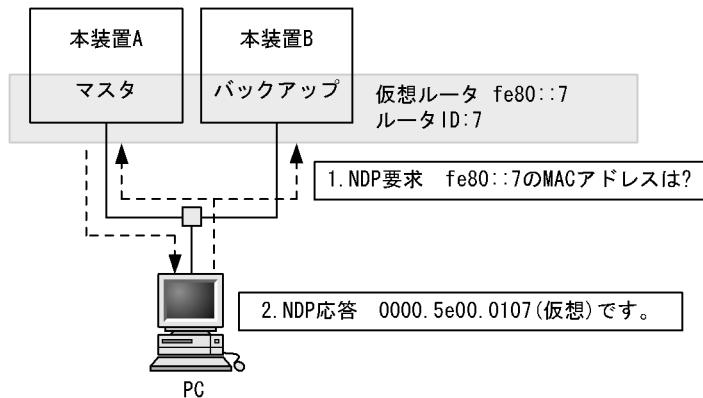
仮想ルータは仮想ルータ用の IP アドレスである仮想 IP アドレスを持ちます。マスタの仮想ルータは、仮想 IP アドレスに対する ARP 要求パケットまたは NDP 要求パケットを受信すると、常に仮想 MAC アドレスを使用して ARP 応答または NDP 応答します。仮想 MAC アドレスによる ARP 応答および NDP 応答を次の図に示します。

図 7-2 仮想 MAC アドレスによる ARP 応答および NDP 応答

●ARP応答



●NDP応答

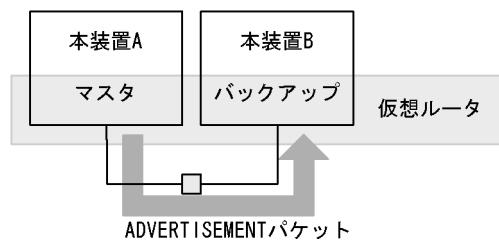


仮想ルータをデフォルトルータとして使用する PC などのホストは、自 ARP キャッシュテーブル内に仮想 IP アドレス宛てのフレームは仮想 MAC アドレス宛てに送出するように学習します。このように学習されたホストは常に仮想ルータへフレームを送出するときに仮想 MAC アドレスを宛先に指定するようになるため、VRRP のマスタ／バックアップの切り替えが発生した場合でも、通信を継続できます。

7.1.2 VRRP における障害検出の仕組み

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

図 7-3 ADVERTISEMENT パケットの送出



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

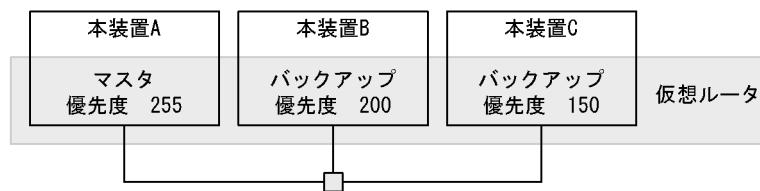
バックアップの仮想ルータは一定の間 ADVERTISEMENT パケットをマスターの仮想ルータから受信しなかった場合に、マスターの仮想ルータに障害が発生したと判断し、バックアップからマスターへと状態を変化させます。

7.1.3 マスターの選出方法

(1) 優先度

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

図 7-4 マスターの選出



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

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

(2) 自動切り戻しおよび自動切り戻しの抑止

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

「図 7-4 マスターの選出」の構成を例にしてみると、仮想ルータ A と仮想ルータ B がダウンし仮想ルータ C がマスターになっている状態から、仮想ルータ B が復旧すると、仮想ルータ C よりも優先度の高い仮想ルータ B がマスターに変化し、仮想ルータ C がマスターからバックアップへ状態を変化することになります。

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

● PREEMPT モードによる抑止

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

● 抑止タイマによる抑止

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

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

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

● 手動による切り戻し

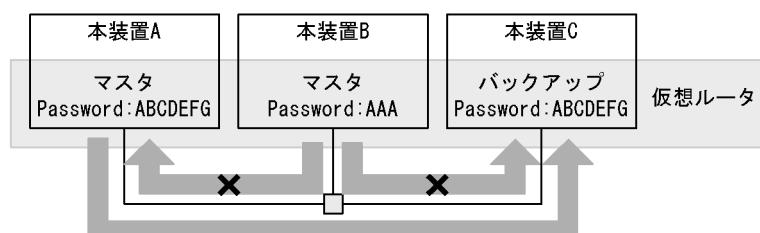
自動切り戻し抑止中状態でも、運用コマンド `swap vrrp` によって仮想ルータの切り戻し処理を起動できます。

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

7.1.4 ADVERTISEMENT パケットの認証

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

図 7-5 パスワードの不一致



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

7.1.5 アクセプトモード

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

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

7.1.6 障害監視インターフェースと VRRP ポーリング

本装置では、仮想ルータの優先度を動的に操作するための機能として、障害監視インターフェースと VRRP ポーリングをサポートしています。

仮想ルータを設定したインターフェースに障害が発生した場合、マスタの切り替えが行われます。しかし、パケットルーティング先の IP インタフェースなど、仮想ルータが設定されていないほかのインターフェースで障害が発生した場合は、通信が不可能な状態であってもマスタの切り替えが行われません。本装置では独自の付加機能として、本装置内のほかのインターフェースを監視して、そのインターフェースがダウンした場合に、仮想ルータの優先度を下げて運用する機能を使用できます。このインターフェースを障害監視インターフェースと呼びます。

障害監視インターフェースでは、インターフェースのダウンで検出できるレベルの障害しか監視できないため、ルータをまたいだ先の障害を検出できません。本装置では独自の付加機能として、指定した宛先へ ping で疎通確認を行い、応答がない場合に仮想ルータの優先度を下げて運用する機能を使用できます。この機能を VRRP ポーリングと呼びます。

障害監視インターフェースは本装置と隣接する機器間の障害監視に、VRRP ポーリングはルータをまたいだ先にある機器との間の障害監視に利用できます。

また、仮想ルータの優先度を操作する方式は 2 とおりあります。

一つは、障害監視インターフェースがダウンしたときに仮想ルータの優先度をコンフィグレーションコマンド vrrp track priority であらかじめ設定しておいた切替優先度に変更して運用する優先度切替方式です。

もう一つは、障害監視インターフェースがダウンしたときに、コンフィグレーションコマンド vrrp track decrement であらかじめ障害監視インターフェースに設定した優先度減算値を仮想ルータの優先度から引いて運用する優先度減算方式です。

優先度切替方式の場合、障害監視インターフェースまたは VRRP ポーリングのどちらかを一つだけ設定できます。優先度減算方式の場合、障害監視インターフェースと VRRP ポーリングを複数設定できます。

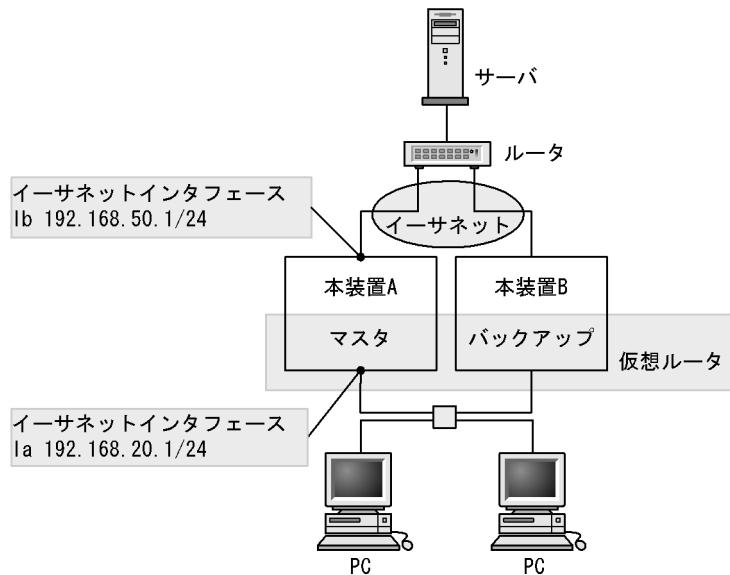
表 7-1 優先度操作方式と監視方法組み合わせ

優先度操作方式	インターフェースダウン監視	VRRP ポーリング
優先度切替方式	一つだけ設定可	一つだけ設定可
優先度減算方式	複数設定可	複数設定可

(1) 障害監視インターフェース

仮想ルータの障害監視インターフェースを次の図に示します。

図 7-6 障害監視インターフェース



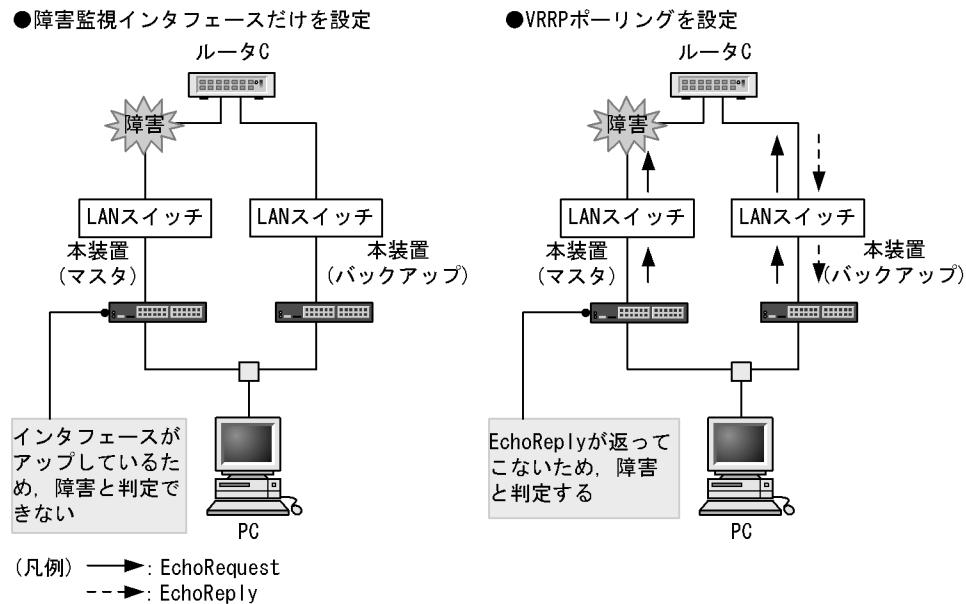
この図を例にして説明します。本装置 A には Ia という IP インタフェースと Ib という IP インタフェースの二つが設定されています。仮想ルータはインターフェース Ia に設定されています。通常の VRRP の動作では VLAN の障害によってインターフェース Ib がダウンしても、仮想ルータの動作には影響を与えません。しかし、本装置では障害監視インターフェースと障害監視インターフェースダウン時の切替優先度、または優先度減算値を指定することによって、仮想ルータの動作状態を変更させることができます。

本装置 A の仮想ルータの障害監視インターフェースを Ib、そして障害監視インターフェースダウン時の優先度を 0 に設定した場合、インターフェース Ib のダウン時には自動的にマスタが本装置 A の仮想ルータから本装置 B の仮想ルータへ切り替わります。

(2) VRRP ポーリング

VRRP ポーリングを設定した場合と設定していない場合の比較を次の図に示します。

図 7-7 VRRP ポーリングを設定した場合と設定していない場合の比較

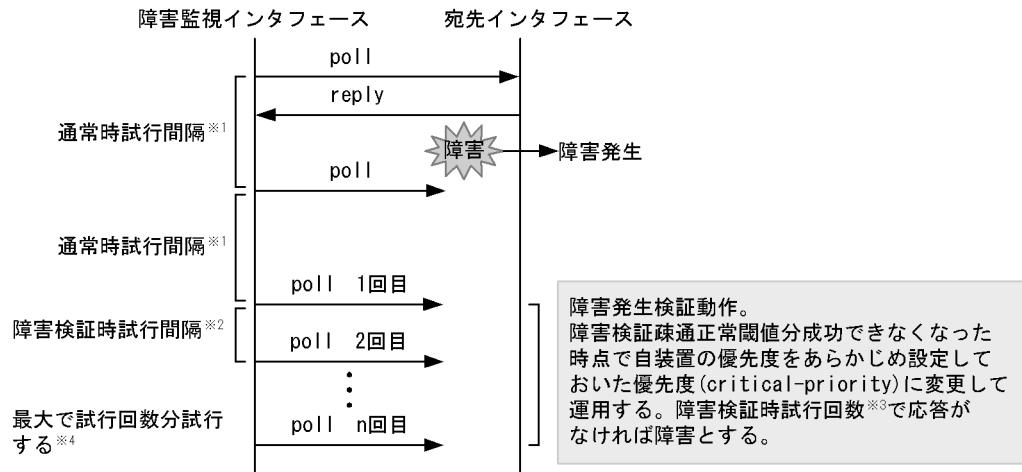


VRRP ポーリングの宛先の機器で障害が発生したり、ネットワーク上で障害が発生して応答が返らなくなると、仮想ルータの優先度を障害監視インターフェースにあらかじめ設定しておいた切替優先度に変更します。

通常時は、一定の試行間隔でポーリングを継続しています。通常時に応答が返らないままタイムアウトすると、障害検証を行います。

障害検証では、障害検証のための試行間隔でポーリングを行います。障害検証中に、正常と判定するための閾値を上まわる回数の応答が返ってこない場合は、障害中と判定します。障害検出動作シーケンスを次の図に示します。

図 7-8 障害検出動作シーケンス



注※ 1 コンフィギュレーションコマンド track check-status-interval で指定できます。

注※ 2 コンフィギュレーションコマンド track failure-detection-interval で指定できます。

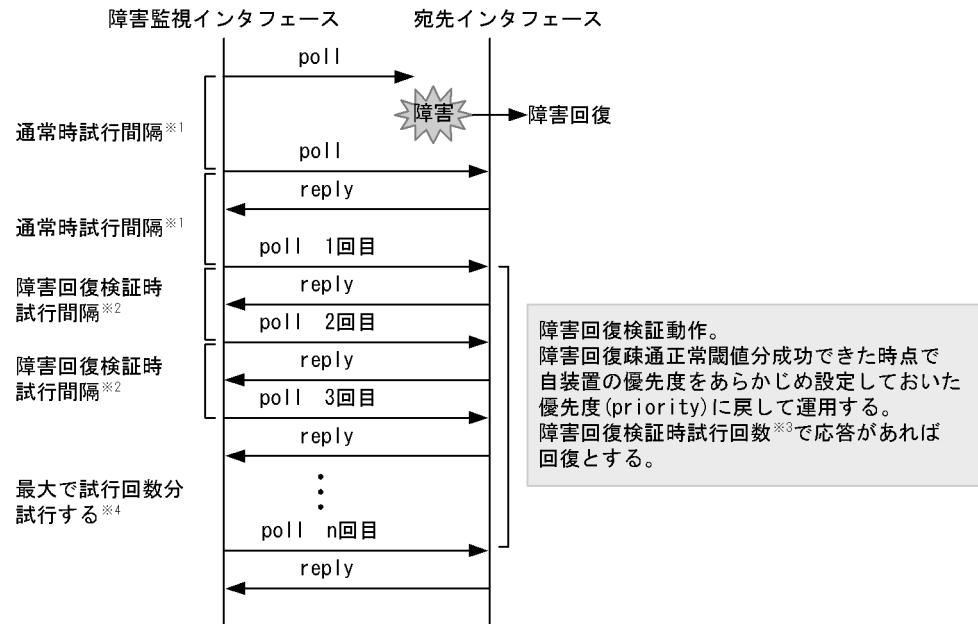
注※ 3 コンフィギュレーションコマンド track failure-detection-times で指定できます。

注※4 コンフィギュレーションコマンド track check-trial-times で指定できます。

障害中も一定の試行間隔でポーリングを継続しています。障害中に応答が返ってくると回復検証を行います。

回復検証では、回復検証のための試行間隔でポーリングを行います。回復検証中に、正常と判定するための閾値を上まわる回数の応答が返ってきた場合は、障害が回復し正常時と判定します。障害回復動作シーケンスを次の図に示します。

図 7-9 障害回復動作シーケンス



注※1 コンフィギュレーションコマンド track check-status-interval で指定できます。

注※2 コンフィギュレーションコマンド track recovery-detection-interval で指定できます。

注※3 コンフィギュレーションコマンド track recovery-detection-times で指定できます。

注※4 コンフィギュレーションコマンド track check-trial-times で指定できます。

インターフェースがダウンした場合、VRRP ポーリングは障害中と判断し、インターフェースがアップするまで待機します。インターフェースがアップしたとき、再度ポーリングを始め、復旧検証によって正常時と判定した場合、切り戻しを行います。

VRRP ポーリングの宛先 IP アドレスが、ルータをまたいだ先のネットワーク上にある場合は、各ルータのルーティングテーブルに依存します。このため、「図 7-10 送受信インターフェースが一致しない場合」のように VRRP ポーリングの応答を受信するインターフェースが VRRP ポーリングを送信したインターフェースと一致しない場合があります。この場合、受信インターフェースチェック（コンフィギュレーションコマンド track check-reply-interface）を指定することで、送信インターフェースと受信インターフェースをチェックできます。送信インターフェースと受信インターフェースが不一致の場合に該当するパケットを廃棄します。なお、「図 7-11 自装置配下ではないネットワーク上のインターフェース不一致」のような自装置配下でないネットワーク上のインターフェースが不一致の場合は、保証しません。

図 7-10 送受信インターフェースが一致しない場合

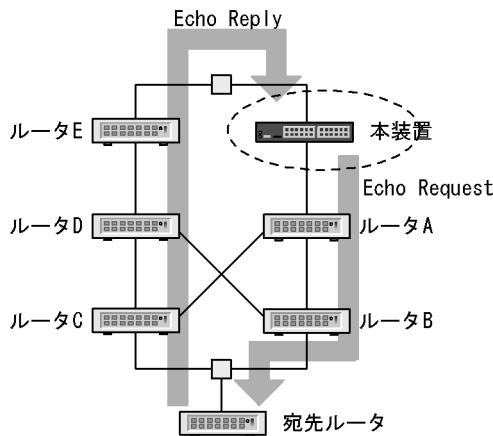
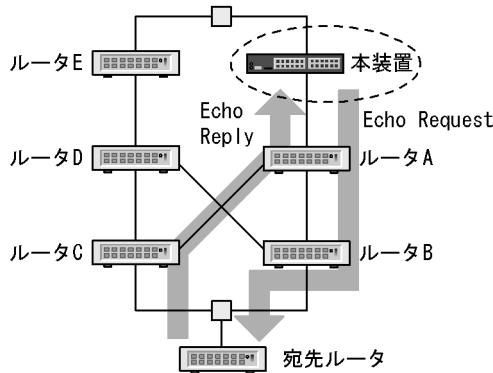


図 7-11 自装置配下ではないネットワーク上のインターフェース不一致



7.1.7 IPv6 VRRP ドラフト対応

本装置は、IPv6 VRRP ドラフト spec-01 と spec-07 をサポートしているので、既存システムに採用されている規格へ合わせて柔軟に導入できます。

デフォルトでは spec-01 で動作します。spec-07 に設定する場合は、コンフィグレーションコマンド `vrrp ietf-ipv6-spec-07-mode` で設定してください。

spec-01 と spec-07 では ADVERTISEMENT パケットのフォーマットが異なるため、仮想ルータを構成するお互いの装置で異なった設定をすると ADVERTISEMENT パケットを不正パケットと判断して破棄しちゃいお互いがマスタ状態になります。このため、仮想ルータを設定する装置間では、ADVERTISEMENT パケットのフォーマットが一致するようにコンフィグレーションを設定してください。

spec-01 で動作していた仮想ルータを spec-07 で動作させるには、MASTER 側の装置と BACKUP 側の装置の両方にコンフィグレーションコマンド `vrrp ietf-ipv6-spec-07-mode` を設定してください。

7.1.8 VRRP 使用時の注意事項

(1) CPU 過負荷時

CPU が過負荷状態となった場合、本装置が送受信する VRRP ADVERTISEMENT パケットの破棄または処理遅延が発生し、状態遷移が発生するおそれがあります。過負荷状態による状態遷移が頻発する場合は、VRRP ADVERTISEMENT パケットの送出間隔を大きい値に設定して運用してください。

(2) VRRP ポーリングによるマルチパス経路の監視について

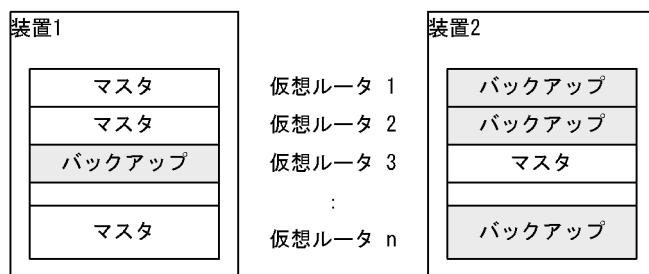
VRRP ポーリング機能はマルチパス経路に対する監視ができません。

(3) track コマンドの入力について

二つ以上の track コマンドを連続入力してコンフィグレーションの変更を行うと、バックアップ状態の仮想ルータがバックアップからマスタへ切り替わる場合があります。track コマンドを連続入力する場合は、コマンドの応答を待ってから次のコマンドを入力してください。

バックアップからマスタへ切り替わる例を次の図に示します。

図 7-12 track コマンド入力時に切り替わる例



上記図の VRRP 変更を行なうと、装置 1 と装置 2 のバックアップの仮想ルータがバックアップからマスタへ切り替わる場合があります。

(4) IPv6 VRRP と RA の連携について

IPv6 VRRP を設定したインターフェースで RA (Router Advertisement) が有効になっている場合、RA は VRRP と連携して次のように動作します。

- RA は IPv6 VRRP のマスタルータとなっている場合だけ情報を配布します。
- RA パケットの MAC ヘッダの送信元 MAC アドレスは、仮想ルータに設定した仮想 MAC アドレスになります。
- RA パケットの IPv6 ヘッダの送信元 IPv6 アドレスは、仮想ルータに設定した仮想 IPv6 アドレスになります。

これによって、端末は IPv6 自動構成機能で、仮想ルータをデフォルトルータとすることができます。

ただし、次のような場合、端末の動作によっては RA を使用したネットワーク運用に支障があるので注意してください。

- 一つのインターフェースに複数の仮想ルータを設定した場合、最初の仮想ルータとだけ連携します。したがって、負荷分散のために VRRP を使用する場合、各端末でデフォルトルータを手動で設定してください。

- 仮想 IPv6 アドレスにリンクローカルアドレスではなくグローバルアドレスを設定した場合、RA の送信元 IPv6 アドレスにはリンクローカルアドレスが必要なため、RA の送信元 IPv6 アドレスには仮想 IPv6 アドレスではなくインターフェースに固有のリンクローカルアドレスを使用します。このため、VRRP と RA の連携動作はできません。VRRP と RA を連携させる運用をする場合は、仮想 IPv6 アドレスにグローバルアドレスを設定しないでください。

7.2 コンフィグレーション

VRRP の設定を行う VLAN には、IP アドレスが設定されている必要があります。VLAN に IP アドレスが設定されていない場合、VRRP のコンフィグレーションコマンドを入力しても仮想ルータは動作しません。

仮想ルータを実際に運用する場合には、同様の仮想ルータの設定を本装置だけでなく、仮想ルータを構成するほかの装置にも行う必要があります。また、仮想ルータの設定のほかにルーティングの設定も必要です。

7.2.1 コンフィグレーションコマンド一覧

VRRP のコンフィグレーションコマンド一覧を次の表に示します。

表 7-2 VRRP 設定用コンフィグレーションコマンド一覧

コマンド名	説明
vrrp accept	アクセプトモードを設定します。
vrrp authentication	ADVERTISEMENT パケット認証のパスワードを設定します。
vrrp ietf-ipv6-spec-07-mode	IPv6 の仮想ルータへ draft-ietf-vrrp-ipv6-spec-07.txt に準拠した動作となるよう設定します。
vrrp ip vrrp ipv6	仮想ルータへ IP アドレスを設定します。
vrrp timers non-preempt-swap	自動切り戻し抑止中に切り戻し処理を行う場合の切り戻し抑止時間を設定します。
vrrp preempt	自動切り戻しを設定します。
vrrp preempt delay	自動切り戻し抑止時間を設定します。
vrrp priority	仮想ルータの優先度を設定します。
vrrp timers advertise	仮想ルータの ADVERTISEMENT パケット送出間隔を設定します。

表 7-3 障害監視インターフェース設定用コマンド一覧

コマンド名	説明
track check-reply-interface	VRRP ポーリングで送受信インターフェースの一一致を確認するか設定します。
track check-status-interval	VRRP ポーリング間隔を設定します。
track check-trial-times	VRRP ポーリングの判定回数を設定します。
track failure-detection-interval	障害発生検証中の VRRP ポーリング間隔を設定します。
track failure-detection-times	障害発生検証中の VRRP ポーリング判定回数を設定します。
track interface	障害監視を行うインターフェースと障害監視方法を設定します。
track ip route	track で VRRP ポーリングを行う宛先を指定します。
track recovery-detection-interval	障害回復検証中の VRRP ポーリング間隔を設定します。
track recovery-detection-times	障害回復検証中の VRRP ポーリング判定回数を設定します。
vrrp track decrement	track を仮想ルータへ優先度減算方式で割り当てます。
vrrp track priority	track を仮想ルータへ優先度切替方式で割り当てます。

7.2.2 VRRP のコンフィグレーションの流れ

IPv4/IPv6 混在モードで動作させる場合は、事前に swrt_table_resource l3switch-2 コマンドを実行してコンフィグレーションを保存したあと、装置を再起動してリソース配分を変更する必要があります。

(1) あらかじめ、IP インタフェースを設定します。

VLAN に対して、仮想ルータに設定しようとしている IP アドレスと同一アドレスファミリの IP アドレスを設定します。

VLAN に初めて IPv6 アドレスを設定する場合は、続けて ipv6 enable コマンドを実行して IPv6 アドレスを有効にする必要があります。

(2) 仮想ルータへ IP アドレスを設定します。

IP インタフェースに設定した IP アドレスと同一の IP アドレスを仮想ルータへ設定すると、仮想ルータはアドレス所有者となり、優先度が 255 固定となります。

仮想ルータへ IPv6 アドレスを設定する場合、規格上はリンクローカルユニキャストアドレスだけ指定でできますが、本装置ではグローバルアドレス（サイトローカルアドレスも含む）も指定できます。

(3) 仮想ルータの優先度を設定します。

IP アドレス所有者でない同一仮想ルータ ID の仮想ルータの優先度を、それぞれ異なる値に設定します。

(4) ADVERTISEMENT パケット送出間隔を設定します。

ネットワークの負荷が高く、バックアップの仮想ルータが ADVERTISEMENT パケットを頻繁に取りこぼす場合は、ADVERTISEMENT パケットの送出間隔をマスタとバックアップの仮想ルータに設定します。

(5) 障害監視インターフェースと VRRP ポーリングを設定します。

必要に応じて、仮想ルータが設定されているインターフェース以外の障害で仮想ルータの切り替えが行われるように、仮想ルータへ障害監視インターフェースや VRRP ポーリングを設定します。

7.2.3 仮想ルータへの IPv4 アドレス設定

[設定のポイント]

仮想ルータへ仮想 IPv4 アドレスを設定します。仮想ルータへ仮想 IP アドレスを設定することで、仮想ルータは動作を開始します。仮想ルータへ設定できる IP アドレスは一つだけです。

仮想ルータに設定する IP アドレスと仮想ルータを設定する VLAN の IP アドレスが同一の場合、仮想ルータは IP アドレス所有者となり、優先度が 255（固定）となります。

仮想 IP アドレスを設定する仮想ルータ ID は、同一 IP サブネットワーク内でユニークとなるように設定してください。

[コマンドによる設定]

```
1. (config)#interface vlan 10
(config-if)#ip address 192.168.10.10 255.255.255.0
例えば、VLAN 10 に仮想ルータを設定する場合、まず vlan 10 の VLAN コンフィグモードに入ります。VLAN へ IP アドレスを設定していない場合は、ここで IP アドレスを設定します。
```

2. (config-if)#vrrp 1 ip 192.168.10.1

仮想ルータ ID1 の仮想ルータへ仮想 IP アドレスとして 192.168.10.1 を設定します。

[注意事項]

- 仮想ルータに IP アドレスを設定後、運用端末に”The VRRP virtual MAC address entry can't be registered at hardware tables.” というログが表示された場合、仮想ルータは正常に動作しません。一度仮想ルータの設定を削除したあと、仮想ルータ ID を変更するか、または仮想ルータを設定する VLAN の VLAN ID を変更してから、再度仮想ルータへ IP アドレスを設定し直してください。
- 仮想ルータへ IP アドレスを設定すると、仮想ルータは動作を始めます。ほかの仮想ルータの優先度設定によっては、仮想ルータがマスタとして追加される場合もあります。
- 装置に仮想ルータを 64 個以上設定する場合は、「表 7-4 ADVERTISEMENT パケット送出間隔の設定目安値」を参照して ADVERTISEMENT パケットの送出間隔を調整してください。

7.2.4 仮想ルータへの IPv6 アドレス設定

[設定のポイント]

仮想ルータへ仮想 IPv6 アドレスを設定します。仮想ルータへ仮想 IPv6 アドレスを設定することで、仮想ルータは動作を開始します。仮想ルータへ設定できる IPv6 アドレスは一つだけです。仮想ルータに設定する IP アドレスと仮想ルータを設定する VLAN の IP アドレスが同一の場合、仮想ルータは IP アドレス所有者となり、優先度が 255 (固定) となります。仮想 IP アドレスを設定する仮想ルータ ID は、同一 IP サブネットワーク内でユニークとなるように設定してください。

[コマンドによる設定]

**1. (config)#interface vlan 50
(config-if)#ipv6 enable
(config-if)#ipv6 address 2001:100::1/64**

例えば、VLAN 50 に仮想ルータを設定する場合、まず vlan 50 の VLAN コンフィグモードに入ります。VLAN へ IPv6 アドレスを設定していない場合は、ここで IPv6 アドレスを設定します。

2. (config-if)#vrrp 3 ipv6 fe80::10

仮想ルータ ID3 の仮想ルータへ仮想 IPv6 アドレス fe80::10 を設定します。

[注意事項]

- 「7.2.3 仮想ルータへの IPv4 アドレス設定」の注意事項と同じです。

7.2.5 優先度の設定

仮想ルータの優先度を 1 から 254 の間で設定します。優先度のデフォルト値は、IP アドレス所有者でない場合は 100 です。仮想ルータが IP アドレス所有者の場合は優先度が 255 (固定) となって変更できません。

仮想ルータを構成する装置のうちで最も優先度の大きい装置がマスタになります。また、マスタの仮想ルータがダウンした場合、バックアップの仮想ルータのうちで最も優先度の高い仮想ルータがマスタになります。

[設定のポイント]

マスタになる装置を明確にするために、同じ仮想ルータ ID の仮想ルータには異なる優先度を設定してください。

[コマンドによる設定]

1. **(config-if)#vrrp 1 priority 150**

仮想ルータ ID1 の仮想ルータの優先度を 150 に設定します。

7.2.6 ADVERTISEMENT パケット送出間隔の設定

ネットワークの負荷が高く、ADVERTISEMENT パケットの損失が多いために、仮想ルータのマスタとバックアップがたびたび切り替わる場合は、ADVERTISEMENT パケットの送出間隔を長くすることで、現象を軽減することができます。ただし、バックアップの仮想ルータは、ADVERTISEMENT パケットを 3 回続けて受信できないときにマスタに変わるために、ADVERTISEMENT パケットの送出間隔を長くすると、マスタの仮想ルータで障害が発生した場合に、バックアップの仮想ルータがマスタに変わるまでの時間も長くなります。

また、装置に多くの仮想ルータを設定した場合、上記と同様にマスタとバックアップが切り替わることがあります。その場合は、次の表を基にADVERTISEMENT パケット送出間隔を調整してください。

表 7-4 ADVERTISEMENT パケット送出間隔の設定目安値

装置当たりの仮想ルータ数	ADVERTISEMENT パケット送出間隔
1 ~ 64	1 秒以上
65 ~ 128	2 秒以上
129 ~ 192	3 秒以上
193 ~ 255	4 秒以上

[設定のポイント]

ADVERTISEMENT パケット送出間隔は、マスタおよびバックアップの仮想ルータへ同一の値を設定してください。

[コマンドによる設定]

1. **(config-if)#vrrp 1 timers advertise 3**

仮想ルータ ID1 の仮想ルータのADVERTISEMENT パケット送出間隔を 3 (秒) に設定します。

7.2.7 自動切り戻し抑止の設定

自動切り戻しはデフォルトで動作し、マスタの仮想ルータに障害が発生してバックアップに切り替わったあと、障害が復旧すると、はじめにマスタであった優先度の高いバックアップの仮想ルータが自動的にマスタに切り替わります。自動切り戻しを抑止すると、優先度の高いバックアップの仮想ルータが自動的にマスタに切り替わらなくなります。

[設定のポイント]

自動切り戻し抑止の設定を行う場合は、IP アドレス所有者でないマスタの仮想ルータに対して行ってください。

[コマンドによる設定]

1. **(config-if)#no vrrp 1 preempt**

仮想ルータ ID1 の仮想ルータの自動切り戻しを抑止します。

7.2.8 自動切り戻し抑止時間の設定

マスタの仮想ルータに障害が発生してバックアップに切り替わったあと、障害が復旧した場合、優先度の高いバックアップの仮想ルータが自動的にマスタに切り替え処理を開始するまでの時間を設定します。自動切り戻し抑止時間のデフォルト値は 0 (秒) で、自動切り戻しを抑止しません。

[設定のポイント]

自動切り戻し抑止時間の設定を行う場合は、IP アドレス所有者でないマスタの仮想ルータに対して行ってください。

[コマンドによる設定]

1. **(config-if)#vrrp 1 preempt delay 60**

仮想ルータ ID1 の仮想ルータの自動切り戻し抑止時間を 60 秒に設定します。

7.2.9 障害監視インターフェースと VRRP ポーリングの設定

本装置では、障害監視インターフェースと VRRP ポーリングの設定を、番号付けした track で管理します。track の設定は、コンフィグレーションコマンド **track** で track 番号を指定します。track を仮想ルータに割り当てることで、仮想ルータは指定された track 番号の track に保存された障害監視インターフェースの設定に従い、障害監視インターフェースを利用します。仮想ルータに track を割り当てるには、コンフィグレーションコマンド **vrrp track** を利用します。

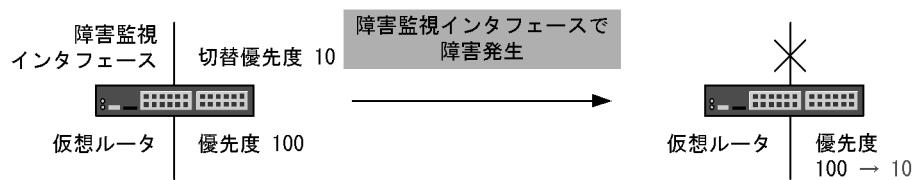
一つの仮想ルータには、優先度切替方式の track と優先度減算方式の track のどちらか一方だけを設定できます。

一つの仮想ルータに対して track を複数割り当てる場合は、優先度操作方式として優先度減算方式だけ設定できます。

優先度切替方式の場合、障害発生時に仮想ルータの優先度を指定した切替優先度に変更します。切替優先度の指定を省略または仮想ルータの優先度より大きい値を指定した場合は、デフォルト値の 0 が使用されます。優先度切替方式を指定した場合は、一つの仮想ルータに track を一つだけ割り当てるることができます。

優先度切替方式で「図 7-13 優先度切替方式」のように、仮想ルータの優先度を 100、障害監視インターフェースの切替優先度として 10 を指定した場合、障害監視インターフェースで障害が発生すると、仮想ルータの優先度は切替優先度の 10 に設定されます。

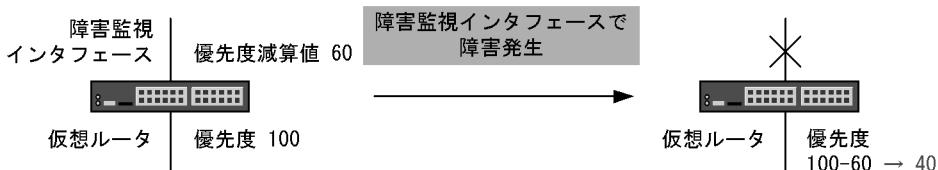
図 7-13 優先度切替方式



優先度減算方式の場合、障害発生時に仮想ルータの優先度を指定した優先度減算値だけ減算した値に変更します。優先度の指定を省略した場合は、デフォルト値の 255 が使用されます。decrement を指定した場合は、一つの仮想ルータに最大 16 の track を割り当てることができます。

優先度減算方式で「図 7-14 優先度減算方式」のように、仮想ルータの優先度を 100、障害監視インターフェースの優先度減算値として 60 を指定した場合、障害監視インターフェースで障害が発生すると、仮想ルータの優先度は元々の優先度 100 から優先度減算値 60 を引いた 40 に設定されます。

図 7-14 優先度減算方式



(1) インタフェースの障害を監視する track の設定

[設定のポイント]

コンフィギュレーションコマンド `track interface` で `line-protocol` を指定すると、指定した VLAN インタフェースの状態を監視します。

`track` に監視する VLAN インタフェースを設定します。

仮想ルータにコンフィギュレーションコマンド `vrrp track` で障害監視を行う track を設定します。

障害監視を行う VLAN インタフェースには、IP アドレスが設定されている必要があります。

[コマンドによる設定]

1.

```
(config)#track 20 interface vlan 30 line-protocol
(config)#track 30 interface vlan 31 line-protocol
(config)#track 40 interface vlan 32 line-protocol
```

 - `track` 番号 20 の `track` に、障害監視インターフェースとして `vlan 30` の状態を監視するよう、設定します。
 - `track` 番号 30 の `track` に、障害監視インターフェースとして `vlan 31` の状態を監視するよう、設定します。
 - `track` 番号 40 の `track` に、障害監視インターフェースとして `vlan 32` の状態を監視するよう、設定します。

2.

```
(config-if)#vrrp 1 track 20 decrement 60
(config-if)#vrrp 1 track 30 decrement 10
(config-if)#vrrp 1 track 40 decrement 40
```

あらかじめ仮想ルータが設定してある VLAN の VLAN コンフィグモードにしておきます。この場合、仮想ルータ ID1 の仮想ルータに、`track` 番号 20, 30, 40 の `track` を割り当てます。

- `track` 番号 20 の `track` に設定された障害監視インターフェースで障害が発生した場合、仮想ルータ 1 の優先度が 60 下がります。
- `track` 番号 30 の `track` に設定された障害監視インターフェースで障害が発生した場合、仮想ルータ 1 の優先度が 10 下がります。
- `track` 番号 40 の `track` に設定された障害監視インターフェースで障害が発生した場合、仮想ルータ 1 の優先度が 40 下がります。

(2) VRRP ポーリングを行う track の設定

[設定のポイント]

コンフィグレーションコマンド `track interface` で `ip routing` を指定すると、指定した VLAN からコンフィグレーションコマンド `track ip route` で指定した宛先への ping による疎通を監視します。VRRP ポーリングとして利用する VLAN インタフェースを `track` に設定します。仮想ルータにコンフィグレーションコマンド `vrrp track` で VRRP ポーリングを行う `track` を設定します。VRRP ポーリングによる障害監視を行う場合は、VRRP ポーリングを行う VLAN インタフェースに IP アドレスを設定し、`track ip route` コマンドで指定した宛先への経路情報が設定されている必要があります。

[コマンドによる設定]

1.

```
(config)#track 50 interface vlan 34 ip routing
(config)#track 51 interface vlan 35 ip routing
(config)#track 52 interface vlan 36 ip routing
```

 - track 番号 50 の track に、VRRP ポーリングの送信インターフェースとして `vlan34` の状態を監視するよう、設定します。
 - track 番号 51 の track に、VRRP ポーリングの送信インターフェースとして `vlan35` の状態を監視するよう、設定します。
 - track 番号 52 の track に、VRRP ポーリングの送信インターフェースとして `vlan36` の状態を監視するよう、設定します。

2.

```
(config)#track 50 ip route 192.168.20.1 reachability
(config)#track 51 ip route 192.168.21.1 reachability
(config)#track 52 ip route 192.168.22.1 reachability
```

 - track 番号 50 の track に、VRRP ポーリングの宛先として `192.168.20.1` を設定します。
 - track 番号 51 の track に、VRRP ポーリングの宛先として `192.168.21.1` を設定します。
 - track 番号 52 の track に、VRRP ポーリングの宛先として `192.168.22.1` を設定します。

3.

```
(config-if)#vrrp 3 track 50 priority 10
(config-if)#vrrp 4 track 51 decrement 20
(config-if)#vrrp 4 track 52 decrement 50
```

 - あらかじめ仮想ルータが設定してある VLAN の VLAN コンフィグモードにしておきます。
 - 仮想ルータ ID3 の仮想ルータに、track 番号 50 の track を割り当て、優先度操作方式に優先度切替方式、切替優先度に 10 を指定します。track 番号 50 の track に設定された VRRP ポーリングで障害が発生した場合、仮想ルータ 3 の優先度を 10 に切り替えます。
 - 仮想ルータ ID4 の仮想ルータに、track 番号 51 と 52 の track を割り当てます。優先度操作方式に優先度減算方式を設定します。track 番号 51 の優先度減算値に 20 を設定します。track 番号 52 の優先度減算値に 50 を設定します。track 番号 51 の track に設定された VRRP ポーリングで障害が発生した場合、仮想ルータ 4 の優先度が 20 下がります。track 番号 52 の track に設定された VRRP ポーリングで障害が発生した場合、仮想ルータ 4 の優先度が 50 下がります。track 番号 51 と 52 の両方の障害監視インターフェースで障害が発生した場合は仮想ルータ 4 の優先度が 70 下がります。

7.3 オペレーション

7.3.1 運用コマンド一覧

VRRP の運用コマンド一覧を次の表に示します。

表 7-5 運用コマンド一覧

コマンド名	説明
show vrrpstatus	仮想ルータの動作状態を表示します。
show vrrpstatus statistics	仮想ルータの統計情報を表示します。
clear vrrpstatus	仮想ルータの統計情報を初期化します。
swap vrrp	自動切り戻しが抑止されているときに切り戻し処理を起動します。
show track	track に保存されている障害監視方法の設定を表示します。

7.3.2 仮想ルータの設定確認

仮想ルータの設定確認は、運用コマンド show vrrpstatus で行います。detail パラメータを指定すると、仮想ルータの設定の詳細情報を取得できます。

図 7-15 show vrrpstatus コマンドの実行結果

```
> show vrrpstatus detail interface vlan 10 vrid 1
Date 2010/12/01 15:30:00 UTC
VLAN0010: VRID 1
  Virtual Router IP Address : 192.168.10.1
  Virtual MAC Address : 0000.5e00.0101
  Current State : MASTER
  Admin State : enable
  Priority : 100/100
  IP Address Count : 1
  Master Router's IP Address : 192.168.10.10
  Primary IP Address : 192.168.10.10
  Authentication Type : SIMPLE TEXT PASSWORD
  Authentication Key : ABCDEFG
  Advertisement Interval : 1
  Preempt Mode : ON
  Preempt Delay : 60(Now Waiting, 30sec. left)
  Non Preempt swap timer : 0
  Accept Mode : OFF
  Virtual Router Up Time : Fri Feb 18 13:05:53 2011
  track 20 VLAN0030 Status : (IF_UP) Down Priority : 60
    Target Address : 192.168.20.1 Vrrp Polling Status : (reachable)
  track 30 VLAN0031 Status : (IF_UP) Down Priority : 10
  track 40 VLAN0032 Status : (IF_UP) Down Priority : 40
    Target Address : 192.168.40.1 Vrrp Polling Status : (reachable)
>
```

7.3.3 track の設定確認

track の設定確認は、運用コマンド show track で行います。

図 7-16 show track コマンドの実行結果

```
> show track detail
Date 2010/12/01 15:30:00 UTC
track : 20 interface : VLAN0030 Mode : (polling)
    Target Address : 192.168.20.1
    Assigned to :
        VLAN0010: VRID 1
track : 30 interface : VLAN0031 Mode : (interface)
    Assigned to :
        VLAN0010: VRID 1
track : 40 interface : VLAN0032 Mode : (polling)
    Target Address : 192.168.40.1
    Assigned to :
        VLAN0010: VRID 1
track : 50 interface : VLAN0034 Mode : (polling)
    Target Address : 192.168.20.1
>
```

7.3.4 切り戻し処理の実行

自動切り戻しが抑止されている、マスタより優先度が高いにも関わらずバックアップに留まっている仮想ルータへ swap vrrp コマンドを実行すると、切り戻し処理を起動できます。ただし、swap vrrp コマンドを実行しても、優先度の低い仮想ルータをマスタにすることはできません。

8 IEEE802.3ah/UDLD

IEEE802.3ah/UDLD 機能は、片方向リンク障害を検出し、それに伴うネットワーク障害の発生を事前に防止する機能です。

この章では、IEEE802.3ah/UDLD 機能の解説と操作方法について説明します。

8.1 解説

8.2 コンフィグレーション

8.3 オペレーション

8.1 解説

8.1.1 概要

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ず、もう一方の装置では受信はできるが送信ができない状態になり、上位プロトコルで誤動作が発生し、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発生や、リンクアグリゲーションでのフレーム紛失が挙げられます。これらの障害は、片方向リンク障害を検出した場合に該当するポートを `inactivate` することによって未然に防ぐことができます。

IEEE802.3ah (Ethernet in the First Mile) で slow プロトコルの一部として位置づけられた OAM (Operations, Administration, and Maintenance) プロトコル（以下、IEEE802.3ah/OAM と示す）では、双方向リンク状態の監視を行うために、制御フレームを用いて定常的に対向装置と自装置の OAM 状態情報の交換を行い、相手装置とのフレームの到達性を確認する方式が述べられています。本装置では IEEE802.3ah/OAM 機能を用いて双方向リンク状態の監視を行い、その確認がとれない場合に片方向リンク障害を検出する方式で UDLD 機能を実現しています。

また、IEEE802.3ah/OAM プロトコルでは、Active モードと Passive モードの概念があり、Active モード側から制御フレームの送信が開始され、Passive モード側では、制御フレームを受信するまで制御フレームの送信は行いません。本装置では工場出荷時の設定で IEEE802.3ah/OAM 機能が有効になっていて、全ポートが Passive モードで動作します。

Ethernet ケーブルで接続された片方の装置側のポートにコンフィグレーションコマンド `efmoam active udld` を設定することで、片方向リンク障害の検出動作を行います。正しく片方向リンク障害を検出させるためには、もう一方の装置側のポートで IEEE802.3ah/OAM 機能が有効である必要があります。`efmoam active udld` コマンドを設定したポートで片方向リンク障害を検出した場合、該当するポートを `inactivate` することで対向装置側のポートでもリンクダウンが検出され、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。

8.1.2 サポート仕様

IEEE802.3ah/UDLD 機能では、次の表に示すとおり IEEE802.3ah/OAM 機能をサポートしています。

表 8-1 IEEE802.3ah/UDLD でサポートする IEEE802.3ah OAMPDU

名称	説明	サポート
Information	相手装置に OAM 状態情報を送信する。	○
Event Notification	相手装置に Link Event の警告を送信する。	×
Variable Request	相手装置に 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	相手装置の 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

8.1.3 IEEE802.3ah/UDLD 使用時の注意事項

(1) IEEE802.3ah/UDLD 機能を設定した装置間に IEEE802.3ah/OAM 機能をサポートしない装置を接続した場合

一般的なスイッチでは、IEEE802.3ah/OAM 機能で使用する制御フレームは中継しません。このため、装置間で情報の交換ができず、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片方向リンク障害を検出してしまいます。IEEE802.3ah/UDLD 機能の運用はできません。

(2) IEEE802.3ah/UDLD 機能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、efmoam active udld コマンドを設定したポートで相手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てしまいます。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的に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) 他社の UDLD 機能との接続について

UDLD 機能はそれぞれ各社の独自仕様で機能を実装しているため、本装置の IEEE802.3ah/UDLD 機能と他社装置の UDLD 機能の相互接続はできません。

8.2 コンフィグレーション

8.2.1 コンフィグレーションコマンド一覧

IEEE802.3ah/UDLD のコンフィグレーションコマンド一覧を次の表に示します。

表 8-2 コンフィグレーションコマンド一覧

コマンド名	説明
efmoam active	物理ポートで IEEE802.3ah/OAM 機能の active モードにします。
efmoam disable	IEEE802.3ah/OAM 機能を無効にします。
efmoam udld-detection-count	片方向リンク障害とするためのカウンタ値を指定します。

8.2.2 IEEE802.3ah/UDLD の設定

(1) IEEE802.3ah/UDLD 機能の設定

[設定のポイント]

IEEE802.3ah/UDLD 機能を運用するには、先ず装置全体で IEEE802.3ah/OAM 機能を有効にしておくことが必要です。本装置では工場出荷時の設定で IEEE802.3ah/OAM 機能が有効となっている状態（全ポート Passive モード）です。次に、実際に片方向リンク障害検出機能を動作させたいポートに対し、UDLD パラメータを附加した Active モードの設定をします。

ここでは、gigabitethernet 0/1 で IEEE802.3ah/UDLD 機能を運用させます。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/1**

ポート 0/1 のイーサネットインターフェースコンフィグレーションモードに移行します。

2. **(config-if)# efmoam active udld**

ポート 0/1 で IEEE802.3ah/OAM 機能の Active モード動作を行い、片方向リンク障害検出動作を開始します。

(2) 片方向リンク障害検出カウントの設定

[設定のポイント]

片方向リンク障害は、相手からの情報がタイムアウトして双方向リンク状態の確認ができない状態が、決められた数だけ連続して発生した場合に検出します。この数が片方向リンク障害検出カウントです。双方向リンク状態は、1 秒に 1 回確認しています。

片方向リンク障害検出カウントを変更すると、実際に片方向リンク障害が発生してから検出するまでの時間を調整できます。片方向リンク障害検出カウントを少なくすると障害を早く検出する一方で、誤検出のおそれがあります。通常、本設定は変更する必要はありません。

片方向リンク障害発生から検出までのおよその時間を次に示します。なお、最大 10% の誤差が生じます。

5+ (片方向リンク障害検出カウント) [秒]

[コマンドによる設定]

1. **(config) # efmoam udld-detection-count 60**

片方向リンク障害検出とするための相手からの情報タイムアウト発生連続回数を 60 回に設定します。

8.3 オペレーション

8.3.1 運用コマンド一覧

IEEE802.3ah/OAM 機能の運用コマンド一覧を次の表に示します。

表 8-3 運用コマンド一覧

コマンド名	説明
show efmoam	IEEE802.3ah/OAM の設定情報およびポートの設定情報を表示します。
show efmoam statistics	IEEE802.3ah/OAM に関する統計情報を表示します。
clear efmoam statistics	IEEE802.3ah/OAM に関する統計情報をクリアします。
restart efmoam	IEEE802.3ah/OAM プログラムを再起動します。
dump protocols efmoam	IEEE802.3ah/OAM 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。

8.3.2 IEEE802.3ah/OAM 情報の表示

IEEE802.3ah/OAM 情報の表示は、運用コマンド show efmoam で行います。show efmoam コマンドは、IEEE802.3ah/OAM 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 detail コマンドは、active モードに設定されたポートに加え、相手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。また、show efmoam statistics コマンドでは、IEEE802.3ah/OAM プロトコルの統計情報を加え、IEEE802.3ah/UDLD 機能で検出した障害状況を表示します。

図 8-1 show efmoam コマンドの実行結果

```
> show efmoam
Date 2010/12/01 15:30:00 UTC
Status: Enabled
udld-detection-count: 30
Port Link status UDLD status Dest MAC
0/1 Up detection * 0012.e298.dc20
0/2 Down active unknown
0/4 Down (uni-link) detection unknown
>
```

図 8-2 show efmoam detail コマンドの実行結果

```
> show efmoam detail
Date 2010/12/01 15:30:00 UTC
Status: Enabled
udld-detection-count: 30
Port Link status UDLD status Dest MAC
0/1 Up detection * 0012.e298.dc20
0/2 Down active unknown
0/3 Up passive 0012.e298.7478
0/4 Down (uni-link) detection unknown
>
```

図 8-3 show efmoam statistics コマンドの実行結果

```
> show efmoam statistics
Date 2010/12/01 15:30:00 UTC
Port 0/1 [detection]
  OAMPDUs :Tx      =    295 Rx      =    295
            Invalid   =      0 Unrecogn.=      0
  TLVs    :Invalid =      0 Unrecogn.=      0
  Info TLV :Tx_Local=    190 Tx_Remote=    105 Rx_Remote=    187
            Timeout   =      3 Invalid   =      0 Unstable =      0
  Inactivate:TLV =      0 Timeout   =      0
Port 0/2 [active]
  OAMPDUs :Tx      =    100 Rx      =    100
            Invalid   =      0 Unrecogn.=      0
  TLVs    :Invalid =      0 Unrecogn.=      0
  Info TLV :Tx_Local=    100 Tx_Remote=    100 Rx_Remote=    100
            Timeout   =      0 Invalid   =      0 Unstable =      0
  Inactivate:TLV =      0 Timeout   =      0
Port 0/3 [passive]
  OAMPDUs :Tx      =    100 Rx      =    100
            Invalid   =      0 Unrecogn.=      0
  TLVs    :Invalid =      0 Unrecogn.=      0
  Info TLV :Tx_Local=      0 Tx_Remote=    100 Rx_Remote=    100
            Timeout   =      0 Invalid   =      0 Unstable =      0
  Inactivate:TLV =      0 Timeout   =      0
>
```


9

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中継の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。

9.1 解説

9.2 コンフィグレーション

9.1 解説

9.1.1 ストームコントロールの概要

レイヤ2ネットワークでは、ネットワーク内にループが存在すると、ブロードキャストフレームなどがスイッチ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異常な負荷を掛けることになります。このような現象はブロードキャストストームと呼ばれ、レイヤ2ネットワークでは避けなければならぬ問題です。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、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も防止する必要があります。

ネットワークおよび接続された機器への影響を抑えるために、スイッチでフラッディング対象フレーム中継の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、イーサネットインターフェースごとに、閾値として1秒間で受信する最大フレーム数を設定でき、その値を超えたフレームを廃棄します。閾値の設定は、ブロードキャストフレーム、マルチキャストフレーム、ユニキャストフレームの3種類のフレームで個別に設定します。

さらに、受信したフレーム数が閾値を超えた場合、そのポートを閉塞したり、プライベートトラップやログメッセージを出力できます。

ストームコントロールの運用コマンドはありません。

9.1.2 ストームコントロール使用時の注意事項

(1) ユニキャストフレームの扱い

本装置では、ユニキャストストームの検出と、フレームの廃棄で対象フレームが異なります。ユニキャストストームの検出は、受信するすべてのユニキャストフレームの数で行います。フレームの廃棄は、MACアドレステーブルに宛先MACアドレスが登録されていないためにフラッディングされるユニキャストフレームだけが対象です。

(2) ストームの検出と回復の検出

本装置は、1秒間に受信したフレーム数が、コンフィグレーションで設定された閾値を超えたときに、ストームが発生したと判定します。ストームが発生したあと、1秒間に受信したフレーム数が閾値以下の状態が30秒続いたときに、ストームが回復したと判定します。

ストーム発生時にポートを閉塞する場合は、そのポートではフレームを受信しなくなるため、ストームの回復も検出できなくなります。ストーム発生時にポートの閉塞を設定した場合は、ネットワーク監視装置などの本装置とは別の手段でストームが回復したことを見つけてください。

9.2 コンフィグレーション

9.2.1 コンフィグレーションコマンド一覧

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 9-1 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	ストームコントロールの閾値を設定します。また、ストームを検出した場合の動作を設定できます。

9.2.2 ストームコントロールの設定

● ブロードキャストフレームの抑制

ブロードキャストストームを防止するためには、イーサネットインターフェースで受信するブロードキャストフレーム数を閾値として設定します。ブロードキャストフレームには、ARPパケットなど通信に必要なフレームも含まれるので、閾値には通常使用するフレーム数を考慮して余裕のある値を設定します。

● マルチキャストフレームの抑制

マルチキャストストームを防止するためには、イーサネットインターフェースで受信するマルチキャストフレーム数を閾値として設定します。マルチキャストフレームには、IPv4マルチキャストパケット、IPv6マルチキャストパケット、OSPFパケットなどの制御パケットなど通信に必要なフレームも含まれるので、閾値には通常使用するフレーム数を考慮して余裕のある値を設定します。

● ユニキャストストームの抑制

ユニキャストストームを防止するためには、イーサネットインターフェースで受信するユニキャストフレーム数を閾値として設定します。閾値には通常使用するフレーム数を考慮して余裕のある値を設定します。

なお、本装置では、ユニキャストフレームの検出には、受信する全ユニキャストフレーム数を使用しますが、中継せずに廃棄するフレームは、MACアドレステーブルに宛先MACアドレスが登録されていないためにフラッディングされるユニキャストフレームだけが対象です。特にストーム検出時の動作にポートの閉塞を指定する場合は、通常使用するフレームでストーム検出とならないよう、閾値の設定には十分余裕のある値としてください。

● ストーム検出時の動作

ストームを検出したときの本装置の動作を設定します。ポートの閉塞、プライベートトラップの送信、ログメッセージの出力を、ポートごとに組み合わせて選択できます。

• ポートの閉塞

ストームを検出したとき、そのポートを `inactive` 状態にします。ストームが回復したあと、再びそのポートを `active` 状態に戻すには、`activate` コマンドを使用します。

• プライベートトラップの送信

ストームを検出したときおよびストームの回復を検出したとき、プライベートトラップを送信して通知します。

• ログメッセージの出力

ストームを検出したときおよびストームの回復を検出したとき、ログメッセージを出力して通知します。ただし、ポートの閉塞時のメッセージは必ず出力します。

9. ストームコントロール

[設定のポイント]

設定できるインターフェースはイーサネットインターフェースです。
ストームが発生したとき、ポートを閉塞します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/10**
(config-if)# storm-control broadcast level pps 50
ブロードキャストフレームの閾値を 50 に設定します。

2. **(config-if)# storm-control multicast level pps 500**
マルチキャストフレームの閾値を 500 に設定します。

3. **(config-if)# storm-control unicast level pps 1000**
ユニキャストフレームの閾値を 1000 に設定します。

4. **(config-if)# storm-control action inactivate**
ストームを検出したときに、ポートを inactive 状態にします。

10 L2 ループ検知

L2 ループ検知機能は、レイヤ 2 ネットワークでループ障害を検知し、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 ループ検知機能の解説と操作方法について説明します。

10.1 解説

10.2 コンフィグレーション

10.3 オペレーション

10.1 解説

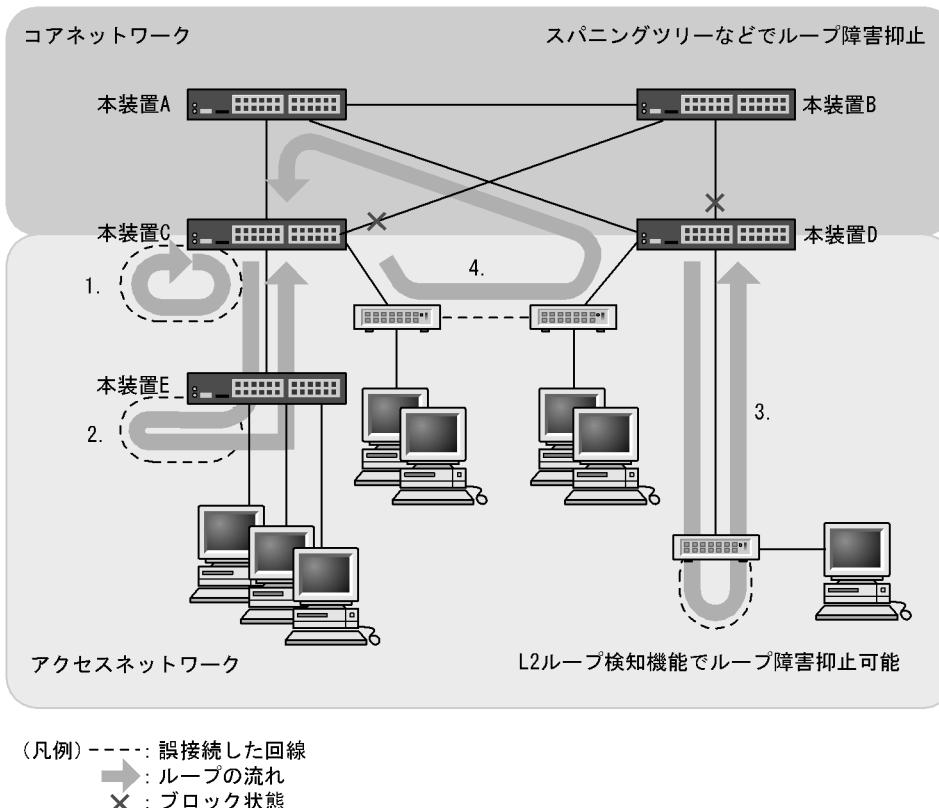
10.1.1 概要

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 ループ検知機能は、一般的にそれら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 ループ検知機能は、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、ネットワーク全体にループ障害が波及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 10-1 ループ障害の基本パターン



ループ障害のパターン例

1. 自装置で回線を誤接続し、ループ障害が発生している。
- 2, 3. 自装置から下位の本装置または L2 スイッチで回線を誤接続し、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、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 ループ検知機能は、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。

10.1.2 動作仕様

L2 ループ検知機能では、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 ループ検知機能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、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後に運用コマンドで **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) L2 ループ検知機能のポート種別

L2 ループ検知機能で使用するポートの種別を次の表に示します。

表 10-1 ポート種別

種別	機能
検知送信閉塞ポート	<ul style="list-style-type: none"> 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、運用ログを表示し、当該ポートを inactive 状態にします。
検知送信ポート	<ul style="list-style-type: none"> 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、運用ログを表示します。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)	<ul style="list-style-type: none"> ループを検知するための L2 ループ検知フレームは送信しません。 ループ障害検知時は、運用ログを表示します。inactive 状態にはしません。
検知対象外ポート	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> ループを検知するための L2 ループ検知フレームは送信しません。 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であれば、運用ログを表示し、送信元ポートを 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。詳細については、マニュアル「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。

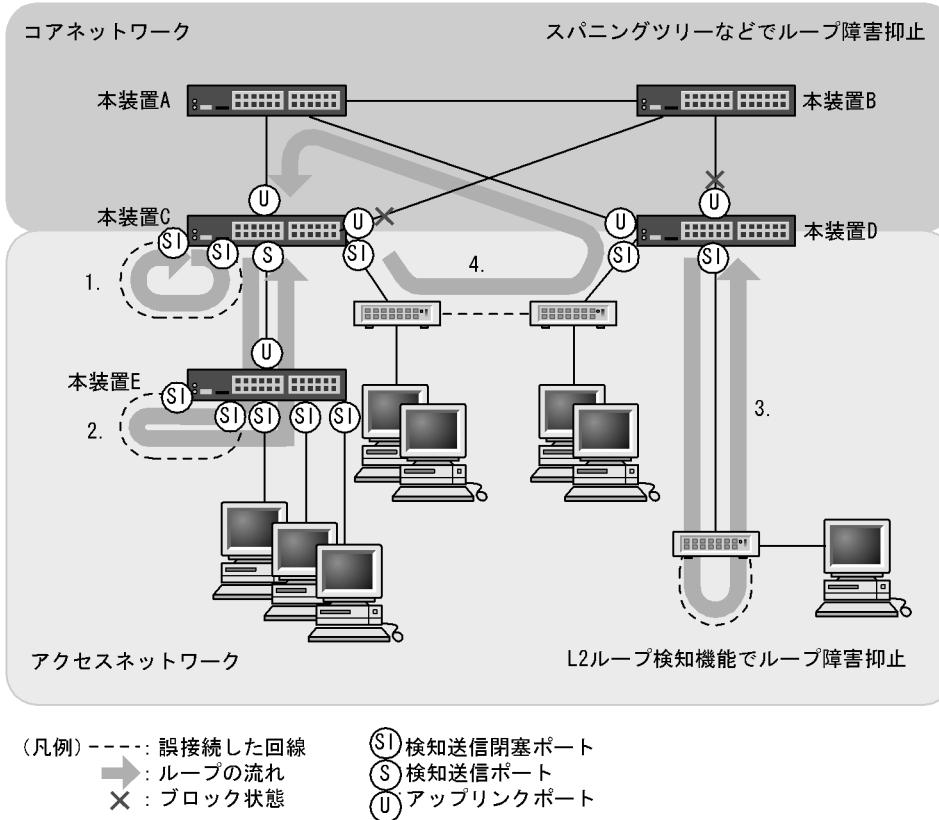
(3) ループ障害の検知方法とポートを **inactive** 状態にする条件

自装置から送信した L2 ループ検知フレームを受信した場合、ポートごとに受信数を計上し、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、該当するポートを **inactive** 状態（検知送信閉塞ポートだけ）にします。

10.1.3 適用例

L2 ループ検知機能を適用したネットワーク構成を示します。

図 10-2 L2 ループ検知機能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 ループ検知機能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

ループ障害の波及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 ループ検知機能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 ループ検知機能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繋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、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。

10.1.4 L2 ループ検知使用時の注意事項

(1) tag 変換機能使用時の動作について

本装置の tag 変換ポートから送信した L2 ループ検知フレームを tag 変換後の VLAN で受信した場合、ループ障害と判断します。また、他装置で tag 変換されて本装置の別の VLAN として L2 ループ検知フレームを受信した場合もループ障害と判断します。

(2) L2 ループ検知機能の動作環境について

本機能を使用する場合に、同一ネットワーク内に L2 ループ検知未サポートの装置を配置したとき、その装置でループ検知フレームを受信するとフレームを廃棄する場合があります。その場合、その装置を含む経路でループ障害が発生しても検知できません。

(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。

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

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 10-2 コンフィグレーションコマンド一覧

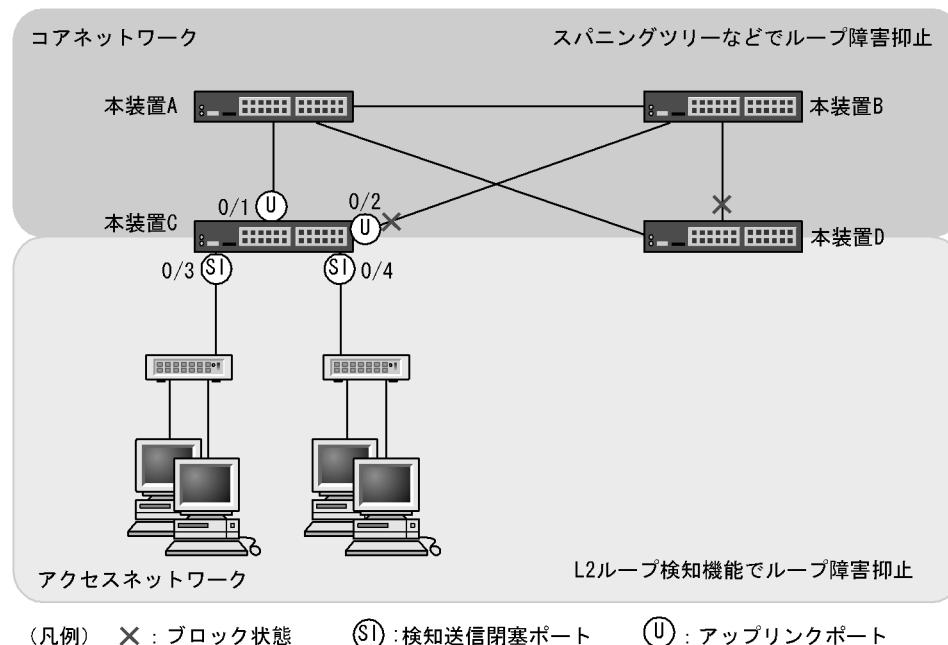
コマンド名	説明
loop-detection	L2 ループ検知機能でのポート種別を設定します。
loop-detection auto-restore-time	inactive 状態にしたポートを自動的に active 状態にするまでの時間を秒単位で指定します。
loop-detection enable	L2 ループ検知機能を有効にします。
loop-detection hold-time	inactive 状態にするまでの L2 ループ検知フレーム受信数の保持時間を秒単位で指定します。
loop-detection interval-time	L2 ループ検知フレームの送信間隔を設定します。
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。

10.2.2 L2 ループ検知の設定

L2 ループ検知機能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 0/1 および 0/2 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を設定します。ポート 0/3 および 0/4 は下位装置と接続しているため、検知送信閉塞ポートを設定します。

図 10-3 L2 ループ検知の設定例



(1) L2 ループ検知機能の設定

[設定のポイント]

L2 ループ検知機能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 ループ障害を検知したい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**

本装置で L2 ループ検知機能を有効にします。

2. **(config)# interface range gigabitethernet 0/1-2**

(config-if-range)# loop-detection uplink-port

(config-if-range)# exit

ポート 0/1 および 0/2 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 0/1 および 0/2 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 0/3-4**

(config-if-range)# loop-detection send-inact-port

(config-if-range)# exit

ポート 0/3 および 0/4 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 0/3 および 0/4 で L2 ループ検知フレームを送信し、また、本ポートでループ障害検知時は、本ポートを 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つたポートや 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 回受信することで 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 状態にしたい場合に設定します。

[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。

10.3 オペレーション

10.3.1 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 10-3 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 ループ検知のダンプ情報をファイルへ出力します。

10.3.2 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できます。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 10-4 L2 ループ検知の情報

```
> show loop-detection
Date 2010/12/01 15:30:00 UTC
Interval Time      :10
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
    0/1   Up       send-inact  0            -          -
    0/2   Down     send-inact  0            -          -
    0/3   Up       send       0            -          -
    0/4   Up       exception  0            -          -
    0/5   Down (loop) send-inact  1            -          CH:32 (U)  100
    CH:1  Up       trap      0            -          -
    CH:32 Up       uplink    -            -          0/5          100
>
```


11 CFM

CFM (Connectivity Fault Management) は、レイヤ 2 レベルでのブリッジ間の接続性の検証とルート確認を行う、広域イーサネット網の保守管理機能です。

この章では、CFM の解説と操作方法について説明します。

11.1 解説

11.2 コンフィグレーション

11.3 オペレーション

11.1 解説

11.1.1 概要

イーサネットは企業内 LAN だけでなく広域網でも使われるようになってきました。これに伴い、イーサネットに SONET や ATM と同等の保守管理機能が求められています。

CFM では、次の三つの機能を使って、レイヤ 2 ネットワークの保守管理を行います。

1. Continuity Check

管理ポイント間で、情報が正しく相手に届くか（到達性・接続性）を常時監視します。

2. Loopback

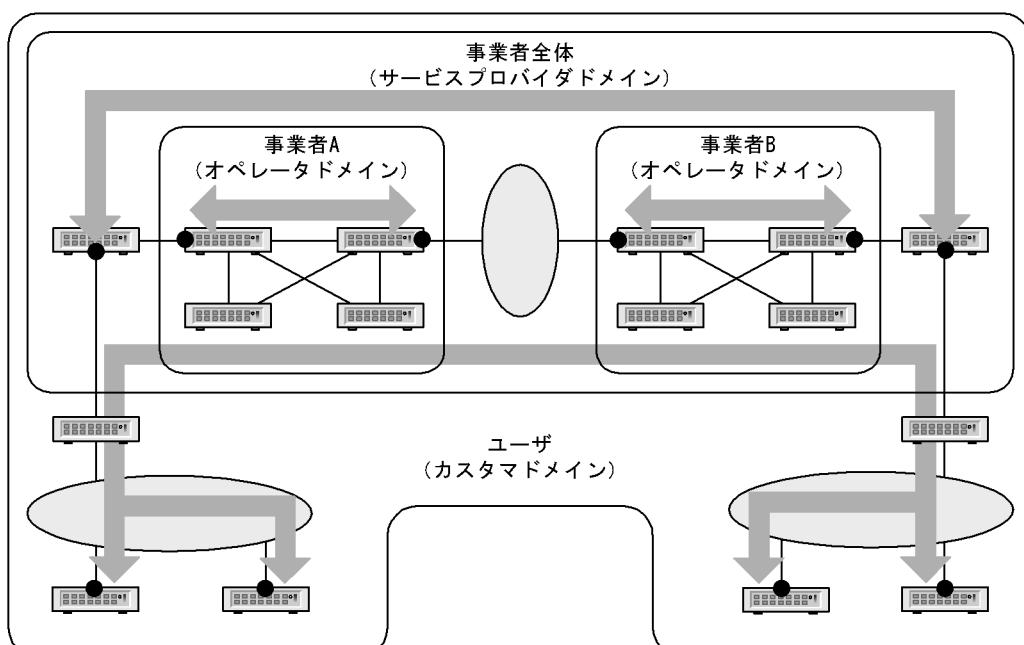
障害を検出したあと、Loopback でルート上のどこまで到達するのかを特定します（ループバック試験）。

3. Linktrace

障害を検出したあと、Linktrace で管理ポイントまでのルートを確認します（レイヤ 2 ネットワーク内のルート探索）。

CFM の構成例を次の図に示します。

図 11-1 CFM の構成例



(凡例) ● : 管理ポイント

← : 接続性の確認

(1) CFM の機能

CFM は IEEE802.1ag で規定されていて、次の表に示す機能があります。本装置は、これらの機能をサポートしています。

表 11-1 CFM の機能

名称	説明
Continuity Check (CC)	管理ポイント間の到達性の常時監視
Loopback	ループバック試験 ping相当の機能をレイヤ 2 で実行します。
Linktrace	ルート探索 traceroute相当の機能をレイヤ 2 で実行します。

(2) CFM の構成

CFM を構成する要素を次の表に示します。CFM はドメイン、MA、MEP および MIP から構成された保守管理範囲内で動作します。

表 11-2 CFM を構成する要素

名称	説明
ドメイン (Maintenance Domain)	CFM を適用するネットワーク上の管理用のグループのこと。
MA (Maintenance Association)	ドメインを細分化して管理する VLAN のグループのこと。
MEP (Maintenance association End Point)	管理終端ポイントのこと。 ドメインの境界上のポートで、MA 単位に設定します。 また、CFM の各機能を実行するポートです。
MIP (Maintenance domain Intermediate Point)	管理中間ポイントのこと。 ドメインの内部に位置する管理ポイントです。
MP (Maintenance Point)	管理ポイントのことで、MEP と MIP の総称です。

11.1.2 CFM の構成要素

(1) ドメイン

CFM ではドメインという単位でネットワークを階層的に管理し、ドメイン内で CFM PDU を送受信することで保守管理を行います。ドメインには 0 ~ 7 のレベル（ドメインレベル）があり、レベルの値が大きいほどが高いレベルとなります。

高いドメインレベルでは、低いドメインレベルの CFM PDU を廃棄します。低いドメインレベルでは、高いドメインレベルの CFM PDU を処理しないで転送します。したがって、低いドメインレベルの CFM PDU が高いドメインレベルのドメインに渡ることはなく、ドメインで独立した保守管理ができます。

ドメインレベルは区分に応じて使用するように、規格で規定されています。区分に割り当てられたドメインレベルを次の表に示します。

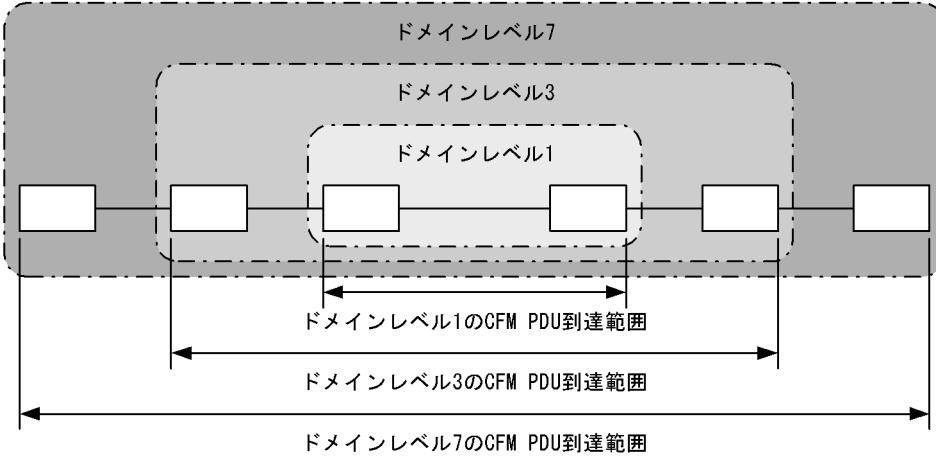
表 11-3 区分に割り当てられたドメインレベル

ドメインレベル	区分
7	カスタマ（ユーザ）
6	
5	
4	サービスプロバイダ（事業者全体）

ドメインレベル	区分
3	
2	オペレータ（事業者）
1	
0	

ドメインは階層的に設定できます。ドメインを階層構造にする場合は低いドメインレベルを内側に、高いドメインレベルを外側に設定します。階層的なドメインの構成例を次の図に示します。

図 11-2 階層的なドメインの構成例



(2) MA

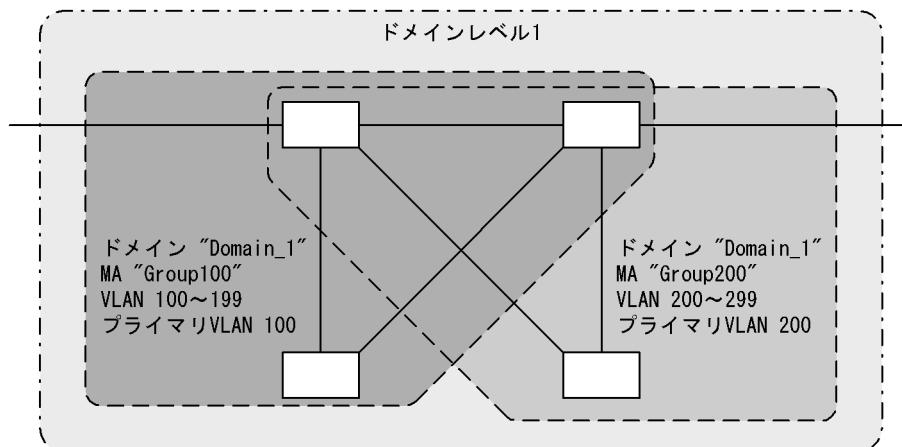
MA はドメイン内を VLAN グループで分割して管理する場合に使います。ドメインには最低一つの MA が必要です。

CFM は MA 内で動作するため、MA を設定することで管理範囲を細かく制御できます。

MA はドメイン名称および MA 名称で識別されます。そのため、同じ MA 内で運用する各装置では、設定時にドメインと MA の名称を合わせておく必要があります。

MA の管理範囲の例を次の図に示します。

図 11-3 MA の管理範囲の例



また、CFM PDU を送受信する VLAN（プライマリ VLAN）を同一 MA 内で合わせておく必要があります。

初期状態では、MA 内で VLAN ID の値がいちばん小さい VLAN がプライマリ VLAN になります。コンフィグレーションコマンド `ma vlan-group` を使えば、任意の VLAN を明示的にプライマリ VLAN に設定できます。

プライマリ VLAN をデータ転送用の VLAN と同じ VLAN に設定することで、実際の到達性を監視できます。

(3) MEP

MEP はドメインの境界上の管理ポイントで、MA に対して設定します。MEP には MEP ID という MA 内でユニークな ID を設定して各 MEP を識別します。

CFM の機能は MEP で実行されます。CFM は MEP 間（ドメインの境界から境界までの間）で CFM PDU を送受信することで、該当ネットワークの接続性を確認します。

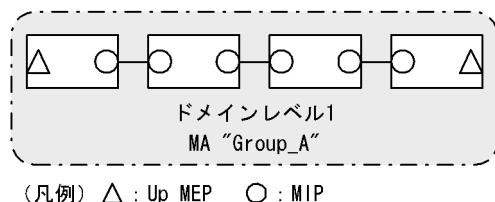
MEP には次の二つの種類があります。

● Up MEP

リレー側に設定する MEP です。Up MEP 自身は CFM PDU を送受信しないで、同一 MA 内の MIP またはポートを介して送受信します。

Up MEP の設定例を次の図に示します。

図 11-4 Up MEP の設定例

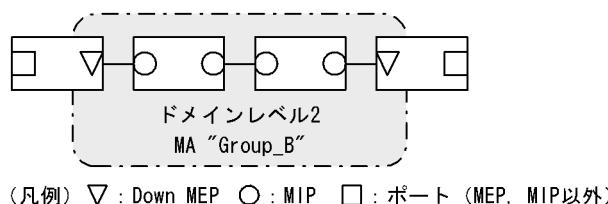


● Down MEP

回線側に設定する MEP です。Down MEP 自身が CFM PDU を送受信します。

Down MEP の設定例を次の図に示します。

図 11-5 Down MEP の設定例



Down MEP, Up MEP からの送信例、および Down MEP, Up MEP での受信例を次の図に示します。

図 11-6 Down MEP, Up MEP からの送信

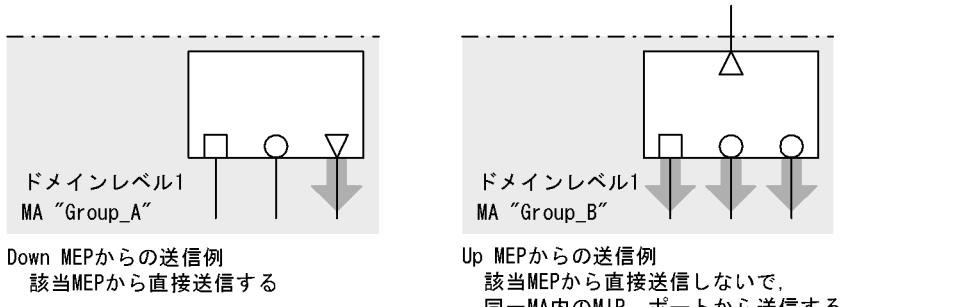
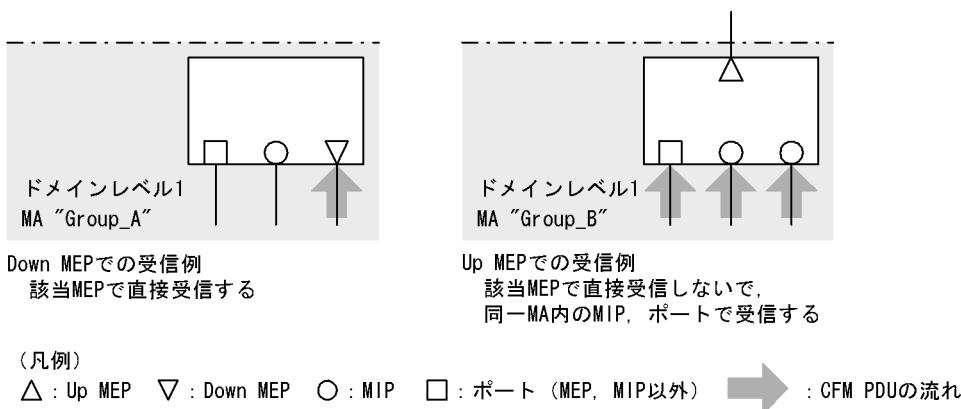
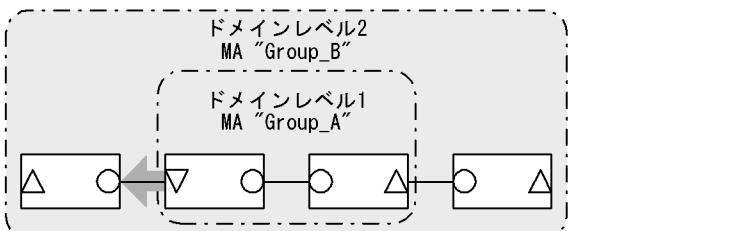


図 11-7 Down MEP, Up MEP での受信



Down MEP および Up MEP は正しい位置に設定してください。例えば、Down MEP は回線側 (MA の内側) に設定する必要があります。リレー側 (MA の外側) に対して設定した場合、CFM PDU が MA の外側に送信されるため、CFM の機能が正しく動作しません。誤って Down MEP を設定した例を次の図に示します。

図 11-8 誤って Down MEP を設定した例



誤ってMA "Group_A"の外側にDown MEPを設定すると、
MA "Group_A"の外側 (ドメインレベル1より外) にCFM PDUが送信されるため、
CFMの機能が正しく動作しない。

(凡例) \triangle : Up MEP ∇ : Down MEP \circ : MIP \rightarrow : CFM PDUの流れ

(4) MIP

MIPはドメインの内部に設定する管理ポイントで、ドメインに対して設定します（同一ドメイン内の全MAで共通）。階層構造の場合、MIPは高いドメインレベルのドメインが低いドメインレベルのドメインと重なる個所に設定します。また、MIPはLoopbackおよびLinktraceに応答するので、ドメイン内の保守管理したい個所に設定します。

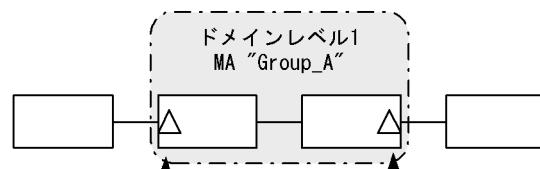
(a) ドメインが重なる個所に設定する場合

ドメインが重なる個所にMIPを設定すると、上位ドメインでは、低いドメインを認識しながらも、低いドメインの構成を意識しない状態で管理できます。

ドメインレベル1とドメインレベル2を使った階層構造の例を次の図に示します。

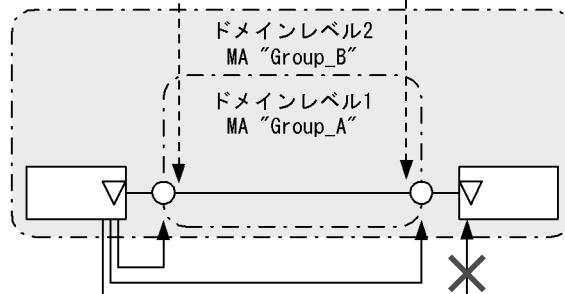
図 11-9 ドメインレベル1とドメインレベル2の階層構造の例

ドメインレベル1の視点



ドメインレベル1でMEPだった個所を
ドメインレベル2ではMIPとして設定する。

ドメインレベル2の視点



Loopbackによる確認

ここで応答が返ってこない場合、
ドメインレベル1を出たところまでは
接続性が有り、ドメインレベル2に
問題があることが確認できる。

(凡例)

△ : Up MEP ▽ : Down MEP ○ : MIP

ドメインレベル2を設計する際、ドメインレベル1のMAでMEPに設定しているポートをドメインレベル2のMIPとして設定します。これによって、ドメインレベル2ではドメインレベル1の範囲を認識しながらも、運用上は意識しない状態で管理できます。

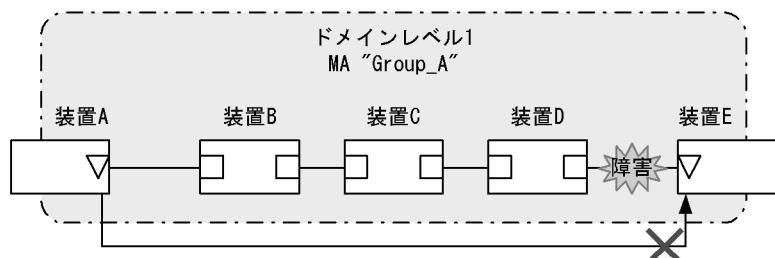
障害発生時は、ドメインレベル2の問題か、ドメインレベル1のどこかの問題かを切り分けられるため、調査範囲を特定できます。

(b) 保守管理したい個所に設定する場合

ドメイン内で細かく MIP を設定すれば、より細かな保守管理ができるようになります。

ドメイン内に MIP が設定されていない構成の例を次の図に示します。この例では、ネットワークに障害が発生した場合、装置 A、装置 E の MEP 間で通信できないことは確認できますが、どこで障害が発生したのか特定できません。

図 11-10 ドメイン内に MIP が設定されていない構成の例

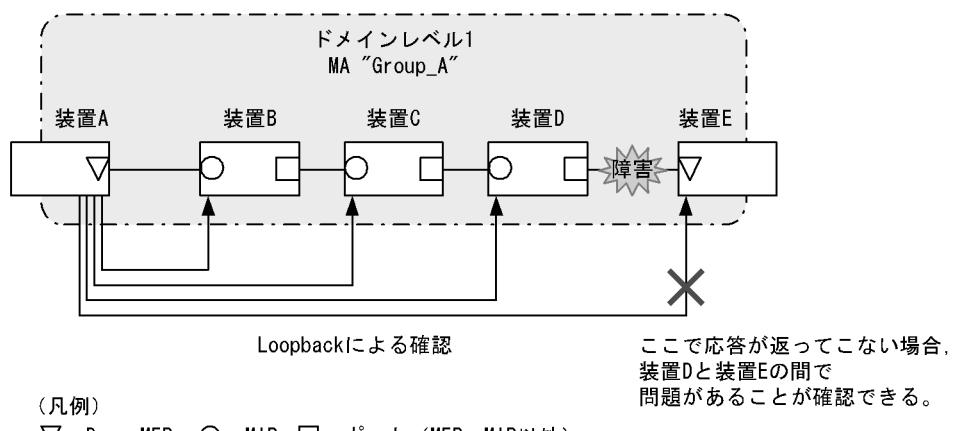


(凡例)

▽ : Down MEP □ : ポート (MEP, MIP以外)

ドメイン内に MIP を設定した構成の例を次の図に示します。この例では、ドメイン内に MIP を設定することで、Loopback や Linktrace の応答が各装置から返ってくるため、障害発生個所を特定できるようになります。

図 11-11 ドメイン内に MIP を設定した構成の例



11.1.3 ドメインの設計

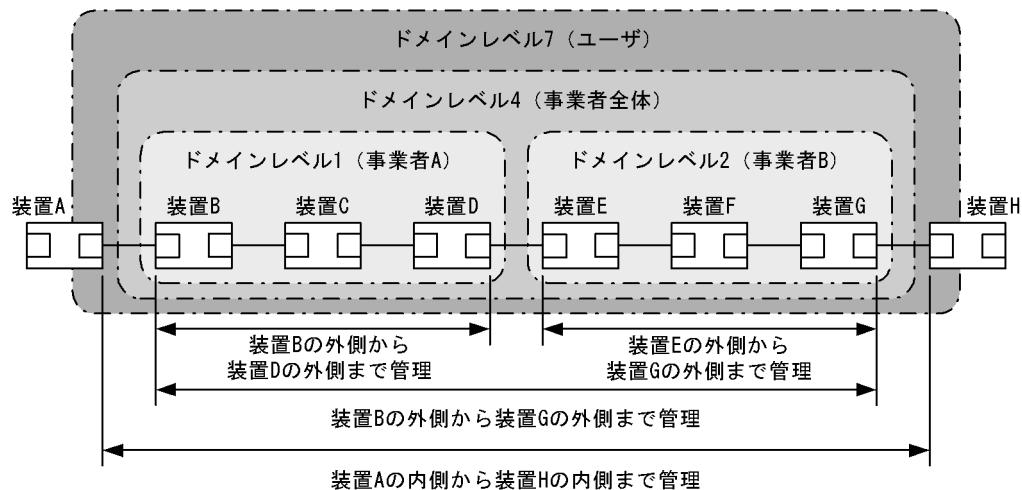
CFM を使用する際には、まずドメインを設計します。ドメインの構成と階層構造を設計し、次に個々のドメインの詳細設計をします。

ドメインの設計には、ドメインレベル、MA、MEP および MIP の設定が必要です。

(1) ドメインの構成と階層構造の設計

ドメインの境界となる MA のポートを MEP に設定し、低いドメインと重なるポートを MIP に設定します。次に示す図の構成例を基に、ドメインの構成および階層構造の設計手順を示します。

図 11-12 構成例



事業者 A, 事業者 B, 事業者全体, ユーザという単位でドメインを設計し, 区分に応じたドメインレベルを設定します。また, 次の項目を想定しています。

- 事業者 A, 事業者 B, 事業者全体は, ユーザに提供する回線が利用できることを保障するために, ユーザに提供するポートを含めた接続性を管理
- ユーザは, 事業者の提供する回線が使用できるかどうかを監視するために, 事業者から提供される回線の接続性を管理

ドメインの設計は, 次に示すように低いレベルから順に設定します。

• ドメインレベル 1, 2 の設定

- ドメインレベル 1 で MA “Group_A” を設定します。

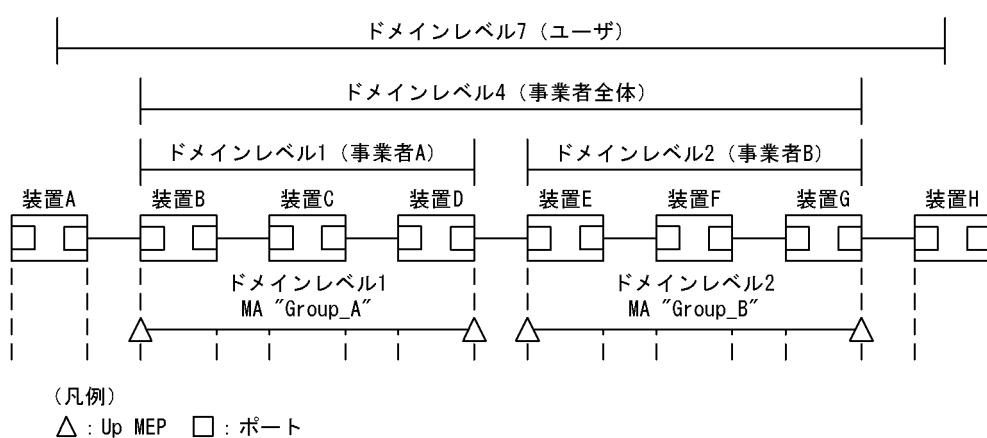
この例では, 一つのドメインを一つの MA で管理していますが, ドメイン内を VLAN グループ単位に分けて詳細に管理したい場合は, 管理する単位で MA を設定します。

- ドメインの境界に当たる装置 B, D で, MA のポートに MEP を設定します。

事業者はユーザに提供するポートを含めた接続性を管理するため, Up MEP を設定します。

- ドメインレベル 2 も同様に, MA を設定し, 装置 E, G に Up MEP を設定します。

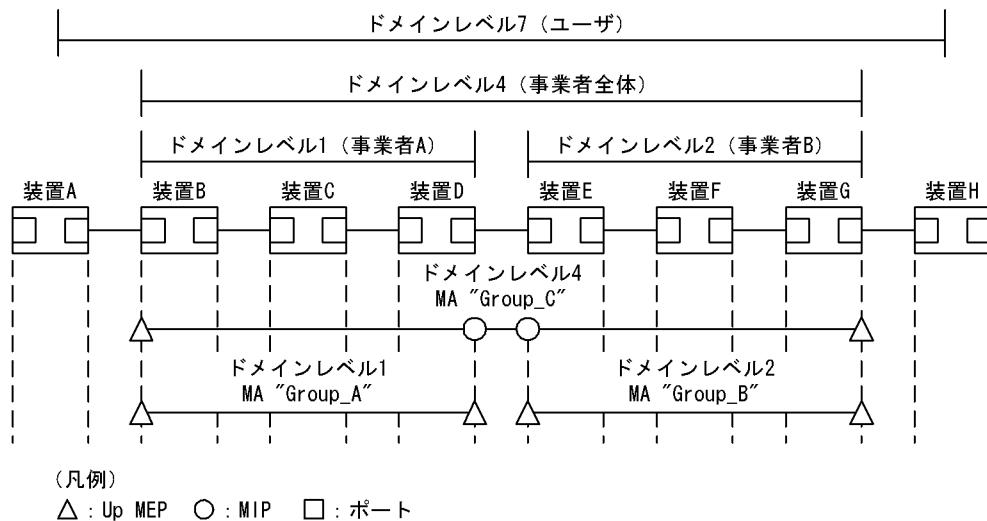
図 11-13 ドメインレベル 1, 2 の設定



- ドメインレベル4の設定

- ドメインレベル4でMA “Group_C”を設定します。
- ドメインレベル4の境界に当たる装置B, Gで、MAのポートにMEPを設定します。
事業者はユーザに提供するポートを含めた接続性を管理するため、Up MEPを設定します。
- ドメインレベル4はドメインレベル1と2を包含しているため、それぞれの中継点である装置D, EにMIPを設定します。
低いドメインのMEPを高いドメインでMIPに設定すると、LoopbackやLinktraceを使って自分で管理するドメインでの問題か、低いレベルで管理するドメインでの問題かを切り分けられるため、調査範囲を特定しやすくなります。

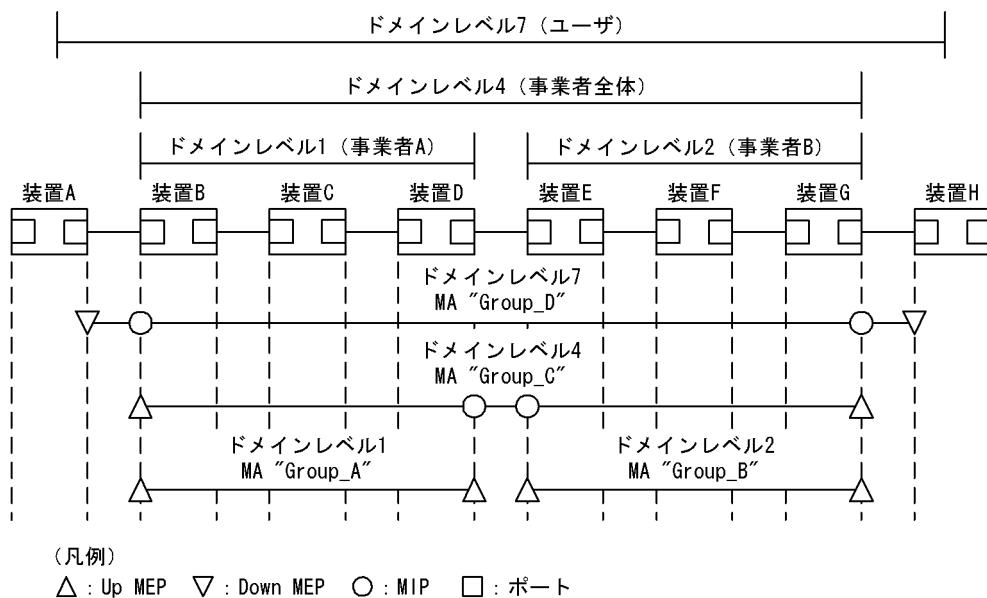
図 11-14 ドメインレベル4の設定



- ドメインレベル7の設定

- ドメインレベル7でMA “Group_D”を設定します。
- ドメインレベル7の境界に当たるA, Hで、MAのポートにMEPを設定します。
ユーザは事業者から提供される回線の接続性を管理するため、Down MEPを設定します。
- ドメインレベル7はドメインレベル4を包含しているため、中継点である装置B, GにMIPを設定します。
ドメインレベル1と2は、ドメインレベル4の中継点として設定しているため、ドメインレベル7では設定する必要はありません。

図 11-15 ドメインレベル 7 の設定



(2) 個々のドメインの詳細設計

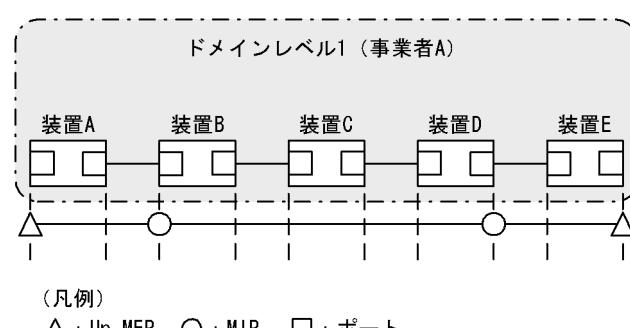
個々の詳細設計では、Loopback、Linktrace を適用したい個所に MIP を設定します。

MIP 設定前の構成および MIP 設定後の構成の例を次の図に示します。

図 11-16 MIP 設定前の構成例



図 11-17 MIP 設定後の構成例



ドメインの内側で Loopback, Linktrace の宛先にしたいポートを MIP に設定します。この例では、装置 B, D に MIP を設定しています。この設定によって装置 B, D の MIP に対し、Loopback, Linktrace を実行できます。また、Linktrace のルート情報として応答を返すようになります。

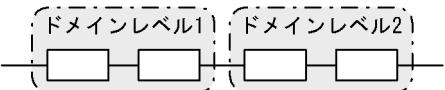
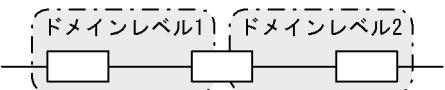
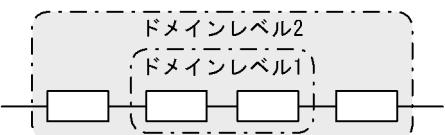
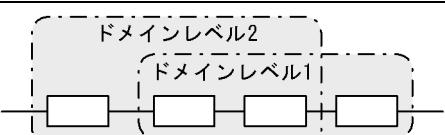
MIP を設定していない装置 C は Loopback, Linktrace の宛先として指定できません。また、Linktrace に応答しないためルート情報に装置 C の情報は含まれません。

(3) ドメインの構成例

ドメインは階層的に設定できますが、階層構造の内側が低いレベル、外側が高いレベルとなるように設定する必要があります。

ドメインの構成例と構成の可否を次の表に示します。

表 11-4 ドメインの構成例と構成の可否

構成状態	構成例	構成の可否
ドメインの隣接		可
ドメインの接触		可
ドメインのネスト		可
ドメインの隣接とネストの組み合わせ		可
ドメインの交差		不可

11.1.4 Continuity Check

Continuity Check (CC) は MEP 間の接続性を常時監視する機能です。MA 内の全 MEP が CCM (Continuity Check Message。CFM PDU の一種) を送受信し合い、MA 内の MEP を学習します。MEP の学習内容は Loopback, Linktrace でも使用します。

CC を動作させている装置で CCM を受信しなくなったり、該当装置の MA 内のポートが通信できない状態になったりした場合に、障害が発生したと見なします。この際、障害検出フラグを立てた CCM を送信し、MA 内の MEP に通知します。

CC で検出する障害を次の表に示します。検出する障害には障害レベルがあります。本装置では検出する障害レベルは初期値固定で、障害レベル 2 以上を検出します。

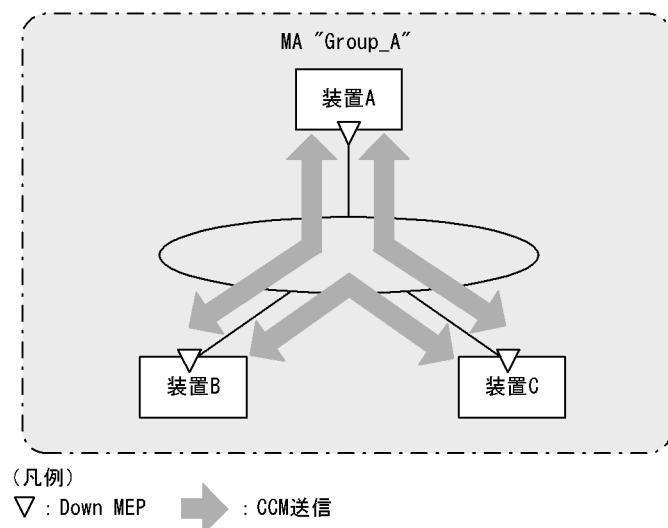
表 11-5 CC で検出する障害

障害レベル	障害内容	初期状態
5	ドメイン、MA が異なる CCM を受信した。	検出する
4	MEP ID または送信間隔が誤っている CCM を受信した。	
3	CCM を受信しなくなった。	
2	該当装置のポートが通信できない状態になった。	
1	障害検出通知の CCM を受信した。 Remote Defect Indication	検出しない

次の図の装置 B に着目して CC の動作例を示します。

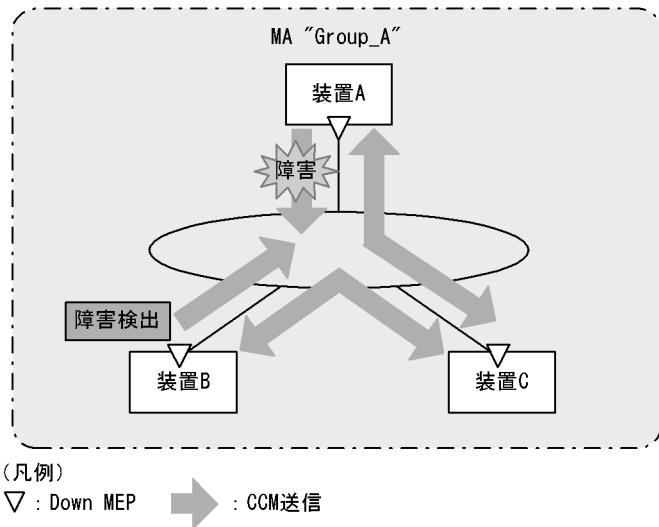
各 MEP はマルチキャストで MA 内に CCM を 1 分間隔で定期的に送信します。各 MEP の CCM を定期的に受信することで常時接続性を監視します。

図 11-18 CC での常時接続性の監視



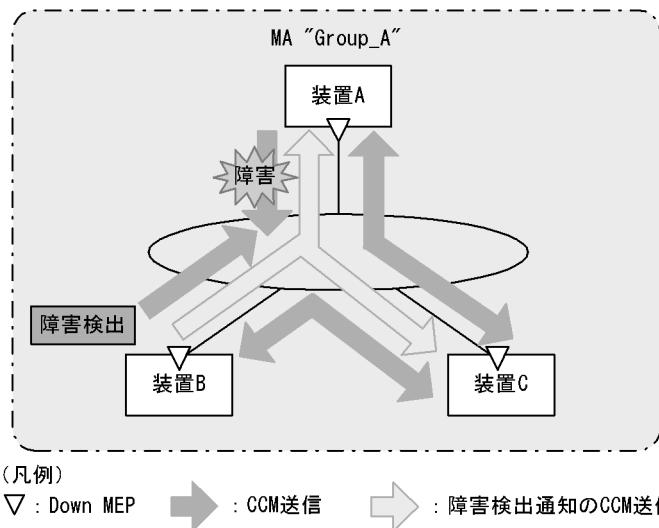
装置 A の CCM が装置の故障またはネットワーク上の障害によって、装置 B に届かなくなると、装置 B は装置 A とのネットワーク上の障害として検出します。

図 11-19 CC で障害を検出



障害を検出した装置 B は、MA 内の全 MEP に対して、障害を検出したことを通知します。

図 11-20 障害を全 MEP に通知



障害検出通知の CCM を受信した各 MEP は、MA 内のどこかで障害が発生したことを認識します。各装置で Loopback, Linktrace を実行することによって、MA 内のどのルートで障害が発生したのかを確認できます。

11.1.5 Loopback

Loopback はレイヤ 2 レベルで動作する、ping 相当の機能です。同一 MA 内の MEP-MEP 間または MEP-MIP 間の接続性を確認します。

CC が MEP-MEP 間の接続性の確認であるのに対し、Loopback では MEP-MIP 間の確認もできるため、MA 内の接続性を詳細に確認できます。

MEP から宛先ヘループバックメッセージ (CFM PDU の一種) を送信し、宛先から応答が返ってくることを確認することで接続性を確認します。

Loopback には MIP または MEP が直接応答するため、例えば、装置内に複数の MIP を設定した場合、MIP ごとに接続性を確認できます。

MIP および MEP に対する Loopback の実行例を次の図に示します。

図 11-21 MIP に対して Loopback を実行

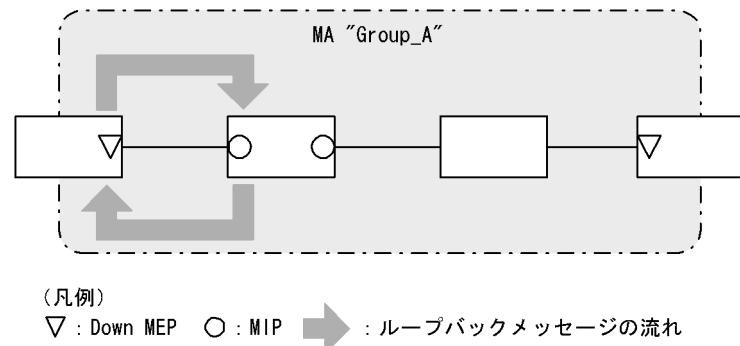
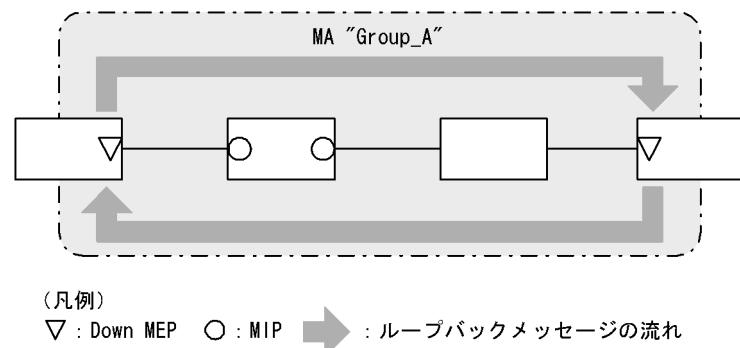


図 11-22 MEP に対して Loopback を実行



Loopback は CC の学習内容を使用するため、事前に CC を動作させておく必要があります。また、宛先に MIP を指定する場合は、事前に MIP のポートの MAC アドレスを調べておく必要があります。

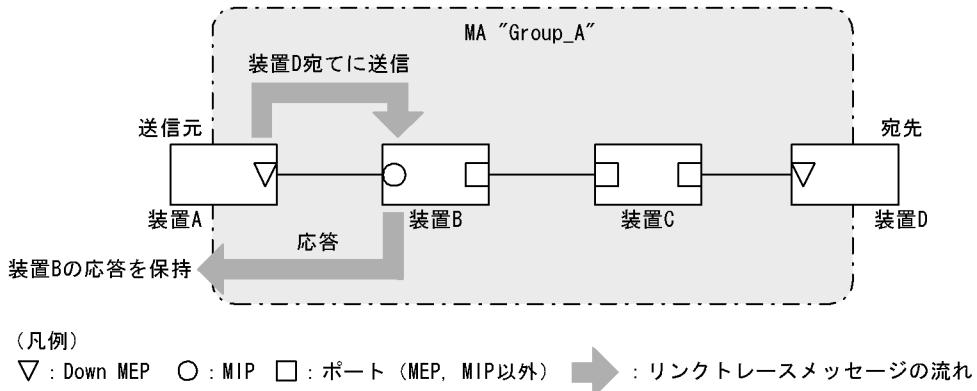
11.1.6 Linktrace

Linktrace はレイヤ 2 レベルで動作する traceroute 相当の機能です。同一 MA 内の MEP-MEP 間または MEP-MIP 間を経由する装置の情報を収集し、ルート情報を出力します。

リンクトレースメッセージ (CFM PDU の一種) を送信し、返ってきた応答をルート情報として収集します。

宛先にリンクトレースメッセージを送信した例を次の図に示します。

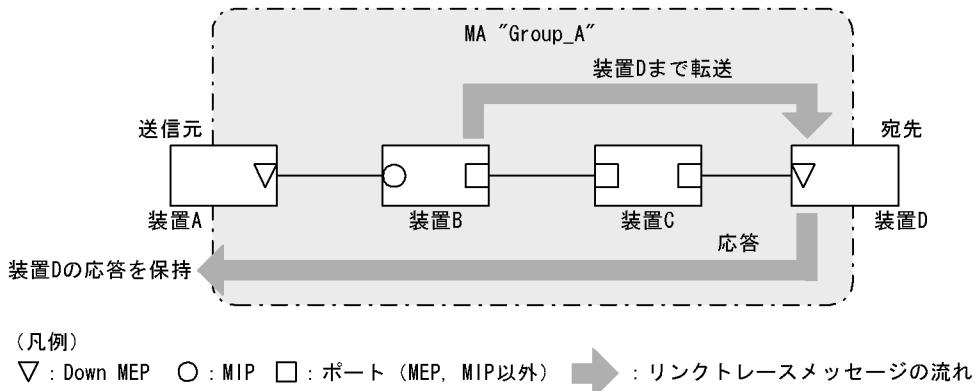
図 11-23 宛先にリンクトレースメッセージを送信



リンクトレースメッセージは宛先まで MIP を介して転送されます。MIP は転送する際に、自装置のどのポートで受信し、どのポートで転送したのかを応答します。送信元装置はルート情報として応答メッセージを保持します。

宛先にリンクトレースメッセージを転送した例を次の図に示します。

図 11-24 宛先にリンクトレースメッセージを転送



応答を返した MIP は宛先までリンクトレースメッセージを転送します。装置 C のように、MEP または MIP が設定されていない装置は応答を返しません（応答を返すには一つ以上の MIP が設定されている必要があります）。

宛先の MEP または MIP までリンクトレースメッセージが到達すると、宛先の MEP または MIP は到達したことと、どのポートで受信したのかを送信元に応答します。

送信元では、保持した応答をルート情報として出力し、宛先までのルートを確認します。

Linktrace は装置単位に応答します。例えば、装置内に設定された MIP が一つでも複数でも、どちらの場合も同じように、受信ポートと転送ポートの情報を応答します。

Linktrace は CC の学習内容を使用するため、事前に CC を動作させておく必要があります。また、宛先に MIP を指定する場合は、事前に MIP のポートの MAC アドレスを調べておく必要があります。

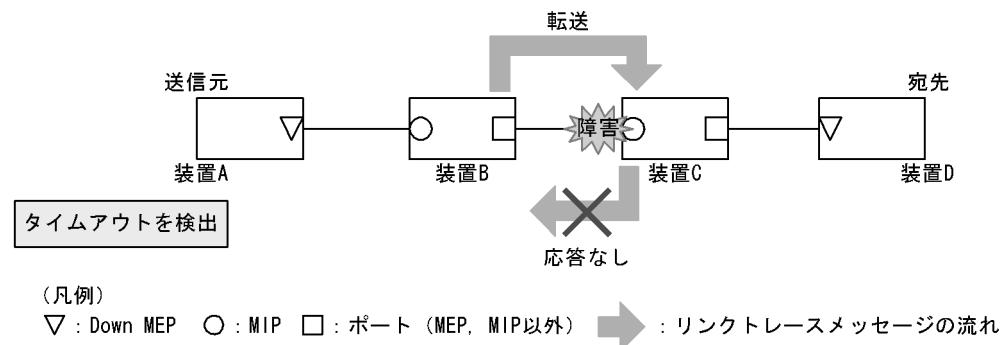
(a) Linktrace による障害の切り分け

Linktrace の実行結果によって、障害が発生した装置やポートなどを絞り込みます。

• タイムアウトを検出した場合

Linktrace でタイムアウトを検出した例を次の図に示します。

図 11-25 Linktrace でタイムアウトを検出した例

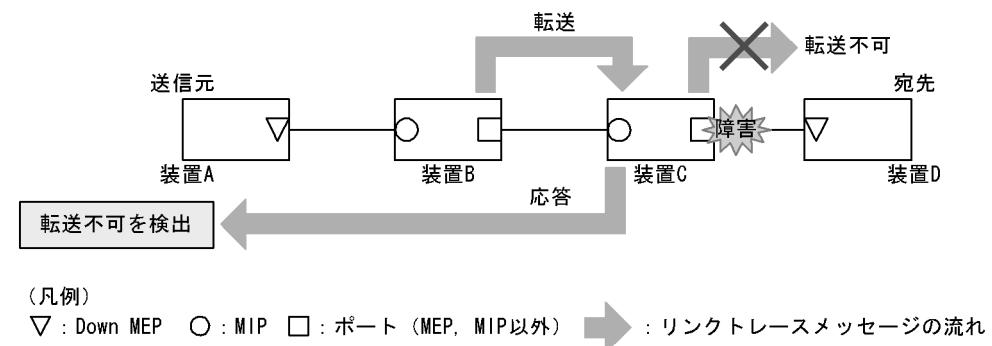


この例では、装置 A が Linktrace でタイムアウトを検出した場合、ネットワーク上の受信側のポートが通信できない状態が考えられます。リンクトレースメッセージが装置 B から装置 C に転送されていますが、装置 C が通信できない状態になっていて、応答を返さないため、タイムアウトになります。

• 転送不可を検出した場合

Linktrace で通信不可を検出した例を次の図に示します。

図 11-26 Linktrace で通信不可を検出した例



装置 A が Linktrace での転送不可を検出した場合、ネットワーク上の送信側のポートが通信できない状態が考えられます。これは、装置 C が装置 D (宛先) にリンクトレースメッセージを転送できなかった場合、装置 A に送信側ポートが通信できない旨の応答を返すためです。

(b) Linktrace の応答について

リンクトレースメッセージはマルチキャストフレームです。

CFM が動作している装置でリンクトレースメッセージを転送する際には、MIP CCM データベースと MAC アドレステーブルを参照して、どのポートで転送するか決定します。

CFM が動作していない装置ではリンクトレースメッセージをフラッディングします。このため、CFM が動作していない装置がネットワーク上にある場合、宛先のルート以外の装置からも応答が返ります。

11.1.7 共通動作仕様

(1) ブロック状態のポートでの動作

CFM の各機能について、ブロック状態のポートでの動作を次の表に示します。

表 11-6 Up MEP がブロック状態の場合

機能	動作
CC	<ul style="list-style-type: none"> CCM を送受信する。送信する CCM のポート状態には Blocked を設定する
Loopback	<ul style="list-style-type: none"> 運用コマンド l2ping は実行できない 自宛のループバックメッセージに応答する
Linktrace	<ul style="list-style-type: none"> 運用コマンド l2traceroute は実行できない リンクトレースメッセージに応答する。応答するリンクトレースメッセージの Egress Port の状態には Blocked を設定する

表 11-7 Down MEP がブロック状態の場合

機能	動作
CC	<ul style="list-style-type: none"> CCM を送受信しない
Loopback	<ul style="list-style-type: none"> 運用コマンド l2ping は実行できない 自宛のループバックメッセージに応答しない
Linktrace	<ul style="list-style-type: none"> 運用コマンド l2traceroute は実行できない リンクトレースメッセージに応答しない

表 11-8 MIP がブロック状態の場合

機能	動作
CC	<ul style="list-style-type: none"> CCM を透過しない
Loopback	<ul style="list-style-type: none"> 回線側から受信した自宛のループバックメッセージに応答しない リレー側から受信した自宛のループバックメッセージに応答する ループバックメッセージを透過しない
Linktrace	<ul style="list-style-type: none"> 回線側から受信したリンクトレースメッセージに応答しない リレー側から受信したリンクトレースメッセージに応答する。応答するリンクトレースメッセージの Egress Port の状態には Blocked を設定する リンクトレースメッセージを透過しない

表 11-9 MEP, MIP 以外のポートがブロック状態の場合

機能	動作
CC	<ul style="list-style-type: none"> CCM を透過しない
Loopback	<ul style="list-style-type: none"> ループバックメッセージを透過しない
Linktrace	<ul style="list-style-type: none"> リンクトレースメッセージを透過しない

(2) VLAN トンネル構成での設定について

VLAN トンネリング網で CFM を使用する場合、VLAN トンネリング網内と VLAN トンネリング網外で ドメインを分け、それぞれで管理します。なお、ドメインの設定個所によっては、CFM の機能の使用に一部制限があります。ドメインの設定個所別の機能の使用制限について次の表に示します。

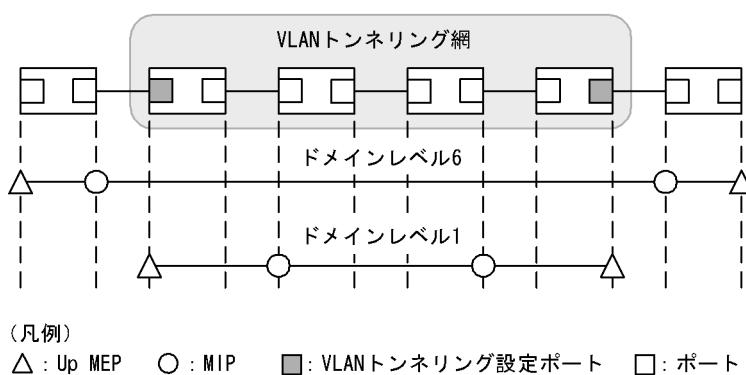
表 11-10 ドメインの設定個所別の機能の使用制限

ドメインの設定個所	機能		
	CC	Loopback	Linktrace
VLAN トンネリング網内と VLAN トンネリング網外	使用可	使用可	<ul style="list-style-type: none"> • VLAN トンネリング網内では使用可 • VLAN トンネリング網外では VLAN トンネルを越えては使用不可
VLAN トンネリング網内だけ	使用可	使用可	使用可
VLAN トンネリング網外だけ	使用可	使用可	使用可

(a) VLAN トンネリング網内と VLAN トンネリング網外で CFM を使用する場合

VLAN トンネリング網内と VLAN トンネリング網外で CFM を使用する例を次の図に示します。

図 11-27 VLAN トンネリング網内と VLAN トンネリング網外で CFM を使用する例



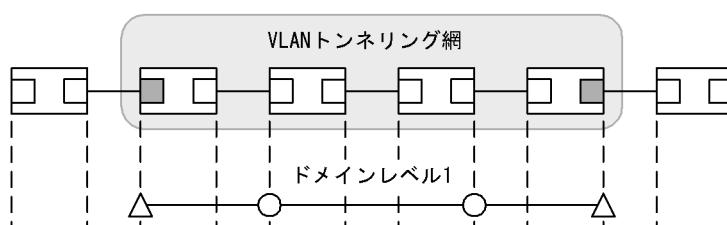
VLAN トンネリング網内のドメインレベル 1 は、VLAN トンネリング網内で任意の個所に管理ポイントを設定できます。VLAN トンネリング網外のドメインレベル 6 は、VLAN トンネリング網外の装置だけに管理ポイントを設定できます。VLAN トンネリング網内にはドメインレベル 6 の管理ポイントは設定できません。VLAN トンネリング網内の管理はドメインレベル 1 です。

また、VLAN トンネリング網外のドメインレベル 6 では VLAN トンネルを越えては Linktrace を使用できません。

(b) VLAN トンネリング網内だけで CFM を使用する場合

VLAN トンネリング網内だけで CFM を使用する例を次の図に示します。

図 11-28 VLAN トンネリング網内だけで CFM を使用する例

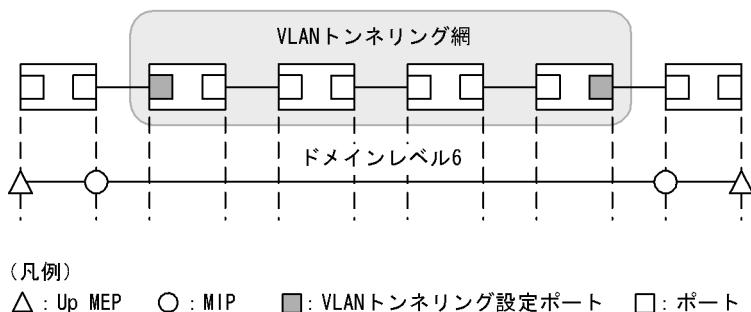


VLAN トンネリング網内のドメインレベル 1 は、VLAN トンネリング網内で任意の個所に管理ポイントを設定できます。該当ドメインでは CFM の各機能が使用できます。

(c) VLAN トンネリング網外だけで CFM を使用する場合

VLAN トンネリング網外だけで CFM を使用する例を次の図に示します。

図 11-29 VLAN トンネリング網外だけで CFM を使用する例



VLAN トンネリング網外のドメインレベル 6 は、VLAN トンネリング網外の装置だけに管理ポイントを設定できます。VLAN トンネリング網内にはドメインレベル 6 の管理ポイントは設定できません。該当ドメインでは CFM の各機能が使用できます。

11.1.8 CFM で使用するデータベース

CFM で使用するデータベースを次の表に示します。

表 11-11 CFM で使用するデータベース

データベース	内容	内容確認コマンド
MEP CCM データベース	各 MEP が保持しているデータベース。 同一 MA 内の MEP の情報。 CC で常時接続性の監視をする際に使用。 保持する内容は次のとおりです。 <ul style="list-style-type: none">• MEP ID• MEP ID に対応する MAC アドレス• 該当 MEP で発生した障害情報	show cfm remote-mep
MIP CCM データベース	装置で保持しているデータベース。 同一ドメイン内の MEP の情報。 リンクトレースメッセージを転送する際、どのポートで転送するかを決定する際に使用。 保持する内容は次のとおりです。 <ul style="list-style-type: none">• MEP の MAC アドレス• 該当 MEP の CCM を受信した VLAN とポート	なし
リンクトレースデータベース	Linktrace の実行結果を保持しているデータベース。 保持する内容は次のとおりです。 <ul style="list-style-type: none">• Linktrace を実行した MEP と宛先• TTL• 応答を返した装置の情報• リンクトレースメッセージを受信したポートの情報• リンクトレースメッセージを転送したポートの情報	show cfm l2traceroute-db

(1) MEP CCM データベース

MEP CCM データベースは、同一 MA 内にどのような MEP があるかを保持しています。また、該当する MEP で発生した障害情報も保持しています。

Loopback, Linktrace では宛先を MEP ID で指定できますが、MEP CCM データベースに登録されていない MEP ID は指定できません。MEP ID がデータベース内に登録されているかどうかは運用コマンド `show cfm remote-mep` で確認できます。

本データベースのエントリは CC 実行時に MEP が CCM を受信したときに作成します。

(2) MIP CCM データベース

MIP CCM データベースは、リンクトレースメッセージを転送する際にどのポートから転送すればよいかを決定する際に使用します。

転送時、MIP CCM データベースに宛先 MEP の MAC アドレスが登録されていない場合は、MAC アдресテーブルを参照して転送するポートを決定します。

MAC アドレステーブルにもない場合はリンクトレースメッセージは転送しないで、転送できなかつた旨の応答を転送元に返します。

本データベースのエントリは CC 実行時に MIP が CCM を転送したときに作成します。

(3) リンクトレースデータベース

リンクトレースデータベースは、Linktrace の実行結果を保持しています。

運用コマンド `show cfm l2traceroute-db` で、過去に実行した Linktrace の結果を参照できます。

(a) 保持できるルート数について

1 ルート当たり最大で 256 装置分の応答を保持します。装置全体では 1024 装置分の応答を保持します。

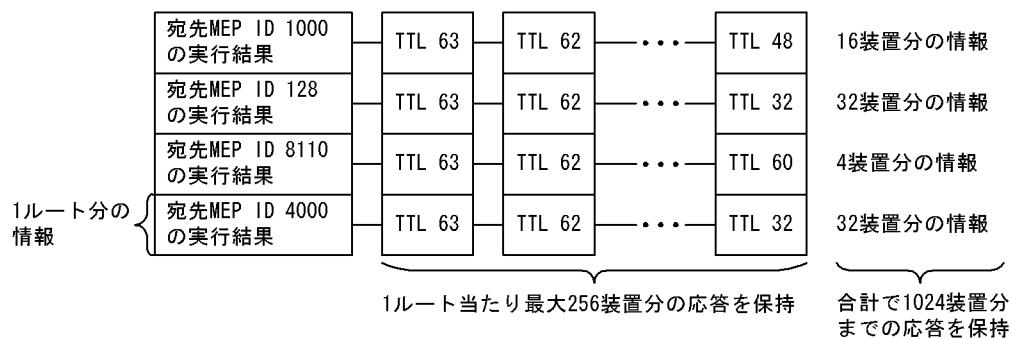
1 ルート当たり何装置分の応答を保持するかで何ルート分保持できるかが決ります。1 ルート当たり 256 装置分の応答を保持した場合は 4 ルート、1 ルート当たり 16 装置分の応答を保持している場合は 64 ルート保持できます。

応答が 1024 装置分を超えた場合、古いルートの情報が消去され、新しいルートの情報を保持します。

リンクトレースデータベースに登録されている宛先に対して Linktrace を実行した場合、リンクトレースデータベース上から該当宛先までのルート情報を削除したあとに新しい Linktrace の応答を保持します。

リンクトレースデータベースを次の図に示します。

図 11-30 リンクトレースデータベース



本データベースのエントリは Linktrace 実行時に MEP が応答を受信したときに作成します。

11.1.9 CFM 使用時の注意事項

(1) CFM を動作させない装置について

CFM を適用する際、ドメイン内の全装置で CFM を動作させる必要はありませんが、CFM を動作させない装置では CFM PDU を透過させる必要があります。

本装置を除き、CFM を動作させない装置は、次の表に示すフレームを透過するように設定してください。

表 11-12 透過させるフレーム

フレーム種別	宛先 MAC アドレス
マルチキャスト	0180.c200.0030 ~ 0180.c200.003f

本装置は、CFM が動作していない場合はすべての CFM PDU を透過します。

(2) 他機能との共存について

次に示すポートでは同時に使用できません。

- レイヤ 2 認証設定ポート

(3) CFM PDU のバースト受信について

CC で常時監視するリモート MEP 数が 96 以上あると、リモート MEP からの CFM PDU 送信タイミングが偶然一致した場合に、本装置で CFM PDU をバースト受信することがあります。その場合、本装置で CFM PDU を廃棄することがあり、障害を誤検出するおそれがあります。

本現象が頻発する場合は、各装置での CFM PDU の送信タイミングが重ならないように調整してください。

(4) 同一ドメインで同一プライマリ VLAN を設定している MA での MEP 設定について

同一ドメインで同一プライマリ VLAN を設定している MA (同一 MA も含む) で、2 個以上の MEP を設定できません。設定した場合は、該当する MEP で CFM が正常に動作しません。

(5) Linktrace でのルート情報の収集について

Linktrace ではリンクトレースメッセージの転送先ポートは、MIP CCM データベースまたは MAC アドレステーブルを参照して決定します。そのため、リンクアップ時（リンクダウン後の再アップ含む）やスパニングツリーなどによる経路変更後は、CC で CCM を送受信するまで転送先ポートが決定できないため、正しいルート情報の収集ができません。

(6) Up MEP および MIP で CFM が動作しないタイミング

次のイベント発生後に、一度もリンクアップしていない Up MEP および MIP のポートでは CFM の各機能が動作しません。一度リンクアップさせることで動作します。

- 装置起動（装置再起動も含む）
- コンフィグレーションファイルのランニングコンフィグレーションへの反映
- 運用コマンド `restart vlan` の実行
- 運用コマンド `restart cfm` の実行

(7) ブロック状態のポートで MIP が Loopback, Linktrace に応答しない場合について

ブロック状態のポートに MIP を設定し、該当ポートで次に示す運用をした場合、MIP は Loopback, Linktrace に応答しないことがあります。

- スパニングツリー（PVST+, シングル）でループガード機能を運用
- スパニングツリー（MSTP）の運用時に、アクセス VLAN またはネイティブ VLAN をプライマリ VLAN として設定
- LLDP を運用
- OADP を運用

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

CFM 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。

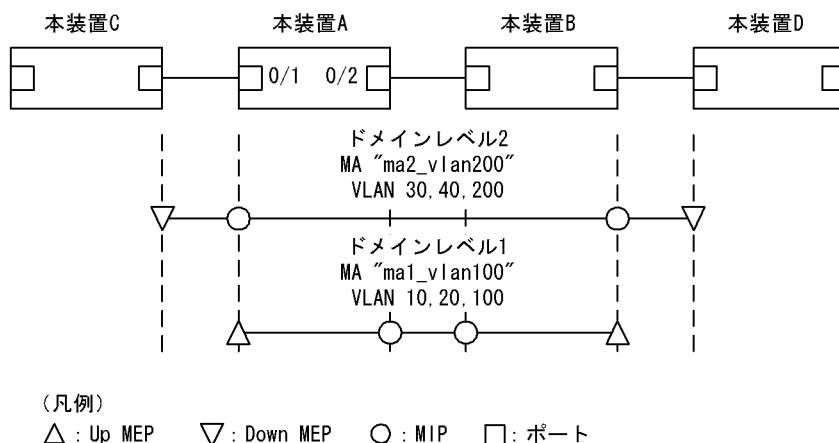
表 11-13 コンフィグレーションコマンド一覧

コマンド名	説明
domain name	該当ドメインで使用する名称を設定します。
ethernet cfm cc enable	ドメインで CC を使用する MA を設定します。
ethernet cfm domain	ドメインを設定します。
ethernet cfm enable (global)	CFM を開始します。
ethernet cfm enable (interface)	no ethernet cfm enable 設定時に CFM を停止します。
ethernet cfm mep	CFM で使用する MEP を設定します。
ethernet cfm mip	CFM で使用する MIP を設定します。
ma name	該当ドメインで使用する MA の名称を設定します。
ma vlan-group	該当ドメインで使用する MA に所属する VLAN を設定します。

11.2.2 CFM の設定（複数ドメイン）

複数ドメインを設定する手順を説明します。ここでは、次の図に示す本装置 A の設定例を示します。

図 11-31 CFM の設定例（複数ドメイン）



(1) 複数ドメインおよびドメインごとの MA の設定

[設定のポイント]

複数のドメインがある場合、低いドメインレベルのドメインから設定します。MA の設定はドメインレベルと MA 識別番号、ドメイン名称、および MA 名称を対向装置と一致させる必要があります。設定が異なる場合、本装置と対向装置は同一 MA と判断されません。

MA のプライマリ VLAN には、本装置の MEP から CFM PDU を送信する VLAN を設定します。

primary-vlan パラメータが設定されていない場合は、vlan-group パラメータで設定された VLAN の中から、最も小さな VLAN ID を持つ VLAN がプライマリ VLAN になります。

[コマンドによる設定]

1. (config)# **ethernet cfm domain level 1 direction-up**
(config-ether-cfm) # domain name str operator_1
ドメインレベル1とMEPの初期状態をUp MEPにすることを設定します。コンフィグレーションイーサネットCFMモードに移行し、ドメイン名称を設定します。

2. (config-ether-cfm) # **ma 1 name str ma1_vlan100**
(config-ether-cfm) # ma 1 vlan-group 10,20,100 primary-vlan 100
(config-ether-cfm) # exit
MA1でMA名称、MAに所属するVLAN、プライマリVLANを設定します。

3. (config)# **ethernet cfm domain level 2**
(config-ether-cfm) # domain name str operator_2
(config-ether-cfm) # ma 2 name str ma2_vlan200
(config-ether-cfm) # ma 2 vlan-group 30,40,200 primary-vlan 200
(config-ether-cfm) # exit
ドメインレベル2とMEPの初期状態をDown MEPにすることを設定します。
MA2でMA名称、MAに所属するVLAN、プライマリVLANを設定します。

(2) MEPおよびMIPの設定

[設定のポイント]

MEPおよびMIPの設定数は、収容条件数以内に収まるように設定してください。

設定したMEPおよびMIPの運用を開始するには、装置のCFMを有効にする設定が必要になります。

[コマンドによる設定]

1. (config)# **interface gigabitethernet 0/1**
(config-if) # ethernet cfm mep level 1 ma 1 mep-id 101
(config-if) # ethernet cfm mip level 2
(config-if) # exit
(config)# interface gigabitethernet 0/2
(config-if) # ethernet cfm mip level 1
(config-if) # exit
ポート0/1に、ドメインレベル1、MA1に所属するMEPを設定します。また、ドメインレベル2のMIPを設定します。ポート0/2にドメインレベル1のMIPを設定します。

2. (config)# **ethernet cfm enable**
本装置のCFMの運用を開始します。

(3) ポートのCFMの停止

[設定のポイント]

一時的にポートのCFMを停止したい場合に設定します。

[コマンドによる設定]

```
1. (config)# interface gigabitethernet 0/1
(config-if)# no ethernet cfm enable
(config-if)# exit
```

ポート 0/1 の CFM を停止します。

(4) CC の設定

[設定のポイント]

ethernet cfm cc enable コマンドの設定直後から、CC が動作します。

[コマンドによる設定]

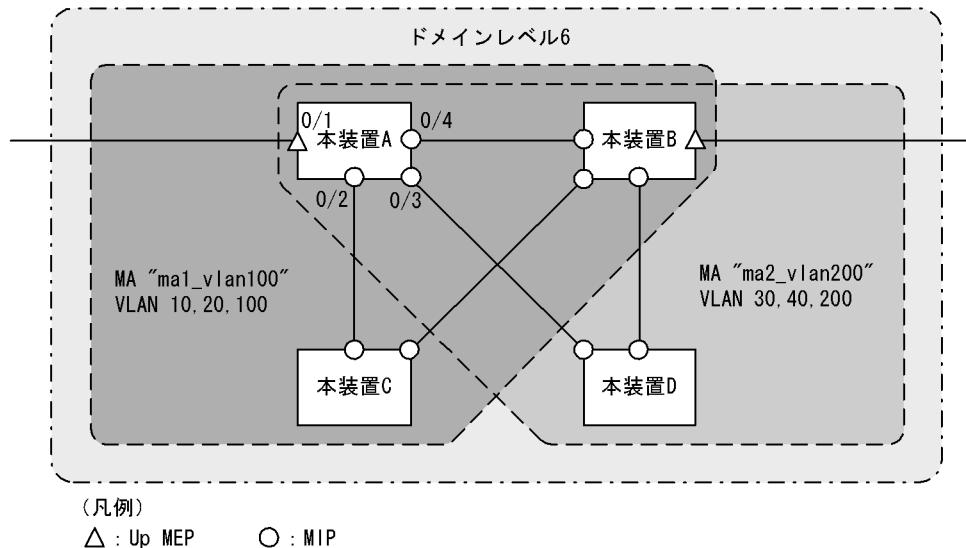
```
1. (config)# ethernet cfm cc level 1 ma 1 enable
```

ドメインレベル 1、MA1 で、CC の動作を開始します。

11.2.3 CFM の設定（同一ドメイン、複数 MA）

同一ドメインで複数の MA を設定する手順を説明します。ここでは、次の図に示す本装置 A の設定例を示します。

図 11-32 CFM の設定例（同一ドメイン、複数 MA）



(1) 同一ドメインでの複数 MA の設定

[設定のポイント]

同一ドメインで複数の MA を設定する場合は、MA 識別番号および MA 名称が重複しないように設定します。ドメインおよび MA の基本的な設定のポイントは、「11.2.2 CFM の設定（複数ドメイン）」を参照してください。

[コマンドによる設定]

```
1. (config)# ethernet cfm domain level 6 direction-up
(config-ether-cfm)# domain name str customer_6
```

ドメインレベルと MEP の初期状態を Up MEP にすることを設定します。コンフィグレーションインターネット CFM モードに移行し、ドメイン名称を設定します。

```
2. (config-ether-cfm)# ma 1 name str ma1_vlan100
(config-ether-cfm)# ma 1 vlan-group 10,20,100 primary-vlan 100
(config-ether-cfm)# ma 2 name str ma2_vlan200
(config-ether-cfm)# ma 2 vlan-group 30,40,200 primary-vlan 200
(config-ether-cfm)# exit
```

MA 識別番号と MA 名称、MA に所属する VLAN、プライマリ VLAN を設定します。

(2) MEP および MIP の設定

[設定のポイント]

MEP は MA ごとに設定する必要があります。MIP は複数の MA で共通で、ポート単位に一つ設定します。MEP および MIP の基本的な設定のポイントは、「11.2.2 CFM の設定（複数ドメイン）」を参照してください。

[コマンドによる設定]

```
1. (config)# interface gigabitethernet 0/1
(config-if)# ethernet cfm mep level 6 ma 1 mep-id 101
(config-if)# ethernet cfm mep level 6 ma 2 mep-id 201
(config-if)# exit
(config)# interface range gigabitethernet 0/2-4
(config-if-range)# ethernet cfm mip level 6
(config-if-range)# exit
```

ポート 0/1 に、ドメインレベル 6、MA1 に所属する MEP を設定します。また、MA2 に所属する MEP を設定します。ポート 0/2 ~ 0/4 にドメインレベル 6 の MIP を設定します。

2. (config)# ethernet cfm enable

本装置の CFM の運用を開始します。

11.3 オペレーション

11.3.1 運用コマンド一覧

CFM の運用コマンド一覧を次の表に示します。

表 11-14 運用コマンド一覧

コマンド名	説明
l2ping	CFM の Loopback 機能を実行します。指定 MP 間の接続を確認します。
l2traceroute	CFM の Linktrace 機能を実行します。指定 MP 間のルートを確認します。
show cfm	CFM のドメイン情報を表示します。
show cfm remote-mep	CFM のリモート MEP の情報を表示します。
show cfm fault	CFM の障害情報を表示します。
show cfm l2traceroute-db	l2traceroute コマンドで取得したルート情報を表示します。
show cfm statistics	CFM の統計情報を表示します。
clear cfm remote-mep	CFM のリモート MEP 情報をクリアします。
clear cfm fault	CFM の障害情報をクリアします。
clear cfm l2traceroute-db	l2traceroute コマンドで取得したルート情報をクリアします。
clear cfm statistics	CFM の統計情報をクリアします。
restart cfm	CFM プログラムを再起動します。
dump protocols cfm	CFM のダンプ情報をファイルへ出力します。

11.3.2 MP 間の接続確認

l2ping コマンドで、指定した MP 間の疎通を確認して、結果を表示します。コマンドには確認回数および応答待ち時間を指定できます。指定しない場合、確認回数は 5 回、応答待ち時間は 5 秒です。疎通確認の応答受信または応答待ち時間経過を契機に、次の確認を繰り返します。

図 11-33 l2ping コマンドの実行結果

```
>l2ping remote-mep 1010 level 7 ma 1000 mep 1020 count 3 timeout 1
L2ping to MP:1010(0012.e220.00a3) on Level:7 MA:1000 MEP:1020 VLAN:20
Time:2009/03/14 19:10:24
1: L2ping Reply from 0012.e220.00a3 64bytes Time= 751 ms
2: L2ping Reply from 0012.e220.00a3 64bytes Time= 752 ms
3: L2ping Reply from 0012.e220.00a3 64bytes Time= 744 ms

--- L2ping Statistics ---
Tx L2ping Request : 3 Rx L2ping Reply : 3 Lost Frame : 0%
Round-trip Min/Avg/Max : 744/749/752 ms

>
```

11.3.3 MP 間のルート確認

l2traceroute コマンドで、指定した MP 間のルート情報を収集し、結果を表示します。コマンドには応答待ち時間と TTL 値を指定できます。指定しない場合、応答待ち時間は 5 秒、TTL 値は 64 です。

宛先に指定した MP から応答を受信したことを「Hit」で確認できます。

図 11-34 l2traceroute コマンドの実行結果

```
> l2traceroute remote-mep 2010 level 7 ma 1000 mep 2020 timeout 10 ttl 64
Date 2010/12/01 15:30:00 UTC
L2traceroute to MP:0012.e220.00a3 on Level:7 MA:1000 MEP:1020 VLAN:1000
Time:2010/12/01 15:30:00
63 0012.e220.00c0 Forwarded
62 0012.e210.000d Forwarded
61 0012.e242.00a3 NotForwarded Hit
```

11.3.4 ルート上の MP の状態確認

show cfm l2traceroute-db detail コマンドで、宛先の MP までのルートとルート上の MP の詳細情報を確認できます。「NotForwarded」が表示された場合、Ingress Port および Egress Port の「Action」で、リンクトレースメッセージが中継されなかった理由を確認できます。

図 11-35 show cfm l2traceroute-db detail コマンドの実行結果

```
> show cfm l2traceroute-db remote-mac 0012.e220.1040 detail
Date 2010/12/01 15:30:00 UTC
L2traceroute to MP:2010(0012.e220.1040) on Level:7 MA:2000 MEP:2020 VLAN:20
Time:2010/12/01 15:30:00
63 0012.e220.10a9 Forwarded
    Last Egress : 0012.f110.2400 Next Egress : 0012.e220.10a0
    Relay Action: MacAdrTbl
    Chassis ID Type: MAC Info: 0012.e228.10a0
    Ingress Port MP Address: 0012.e220.10a9 Action: OK
    Egress Port MP Address: 0012.e220.10aa Action: OK
62 0012.e228.aa3b NotForwarded
    Last Egress : 0012.e220.10a0 Next Egress : 0012.e228.aa30
    Relay Action: MacAdrTbl
    Chassis ID Type: MAC Info: 0012.e228.aa30
    Ingress Port MP Address: 0012.e228.aa2c Action: -
    Egress Port MP Address: 0012.e228.aa3b Action: Down
>
```

11.3.5 CFM の状態の確認

show cfm コマンドで、CFM の設定状態と障害検知状態を表示します。CC で障害を検知した場合、検知した障害の中で、最も障害レベルの高い障害種別を「Fault」で確認できます。

図 11-36 show cfm コマンドの実行結果

```
>show cfm
Date 2010/12/01 15:30:00 UTC
Domain Level 3 Name(str): ProviderDomain_3
  MA 300 Name(str) : Tokyo_to_Osaka
    Primary VLAN:300 VLAN:10-20,300
    CC:Enable Interval:1min
    Alarm Priority:3 Start Time:2500ms Reset Time:10000ms
    MEP Information
      ID:8012 UpMEP CH12(Up) Enable MAC:0012.e200.00b2 Fault:Timeout
    MA 400 Name(str) : Tokyo_to_Nagoya
      Primary VLAN:400 VLAN:30-40,400
      CC:Enable Interval:1min
      Alarm Priority:3 Start Time:2500ms Reset Time:10000ms
      MEP Information
        ID:8014 DownMEP 0/21(Up) Disable MAC:0012.e220.0040 Fault:-
        MIP Information
          0/12(Up) Enable MAC:0012.e200.0012
          0/22(Down) Disable MAC:-
Domain Level 4 Name(str): ProviderDomain_4
  MIP Information
    CH12(Up) Enable MAC:0012.e220.00b2
>
```

11.3.6 障害の詳細情報の確認

show cfm fault detail コマンドで、障害種別ごとに、障害検知状態と障害検知のきっかけとなった CCM 情報を表示します。CCM を送信したリモート MEP は「RMEP」、「MAC」および「VLAN」で確認できます。

図 11-37 show cfm fault detail コマンドの実行結果

```
>show cfm fault detail
Date 2010/12/01 15:30:00 UTC
MD:7 MA:1000 MEP:1000 Fault
OtherCCM : - RMEP:1020 MAC:0012.e220.1e22 VLAN:1000 Time:10/11/30 11:22:17
ErrorCCM : -
Timeout : -
PortState: -
RDI      : On RMEP:1011 MAC:0012.e220.11a2 VLAN:1000 Time:2010/12/01 11:42:10
>
```

12 SNMP を使用したネットワーク管理

この章では本装置の SNMP エージェント機能についてサポート仕様を中心に説明します。

12.1 解説

12.2 コンフィグレーション

12.3 オペレーション

12.1 解説

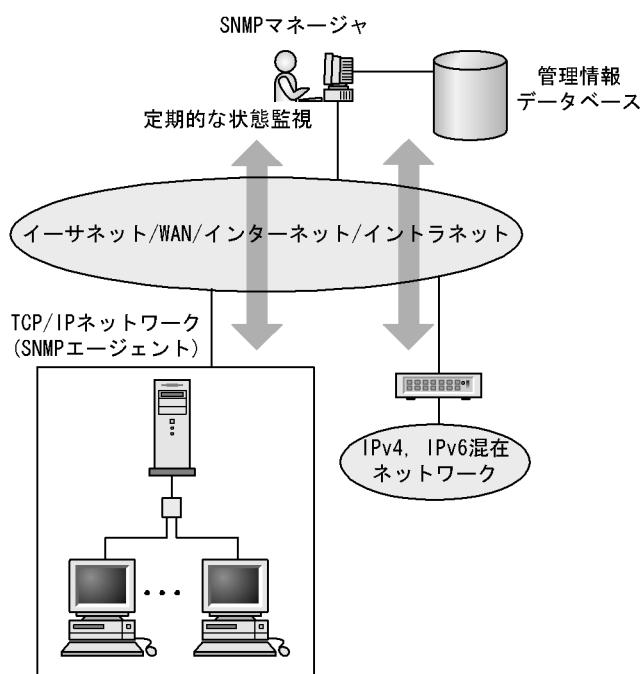
12.1.1 SNMP 概説

(1) ネットワーク管理

ネットワークシステムの稼働環境や性能を維持するためには、高度なネットワーク管理が必要です。

SNMP (simple network management protocol) は業界標準のネットワーク管理プロトコルです。SNMP をサポートしているネットワーク機器で構成されたマルチベンダーネットワークを管理できます。管理情報を収集して管理するサーバを **SNMP マネージャ**、管理される側のネットワーク機器を **SNMP エージェント**といいます。ネットワーク管理の概要を次の図に示します。

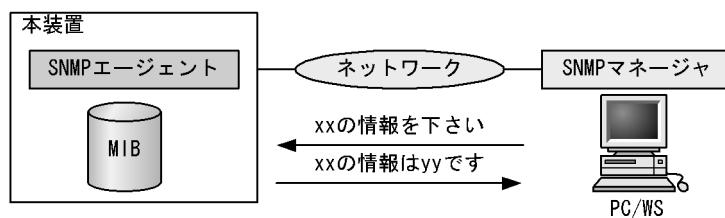
図 12-1 ネットワーク管理の概要



(2) SNMP エージェント機能

本装置の SNMP エージェントは、ネットワーク上の装置内部に組み込まれたプログラムです。装置内の情報を SNMP マネージャに提供する機能があります。装置内にある各種情報を MIB (Management Information Base) と呼びます。SNMP マネージャは、装置の情報を取り出して編集・加工し、ネットワーク管理を行うための各種情報をネットワーク管理者に提供するソフトウェアです。MIB 取得の例を次の図に示します。

図 12-2 MIB 取得の例

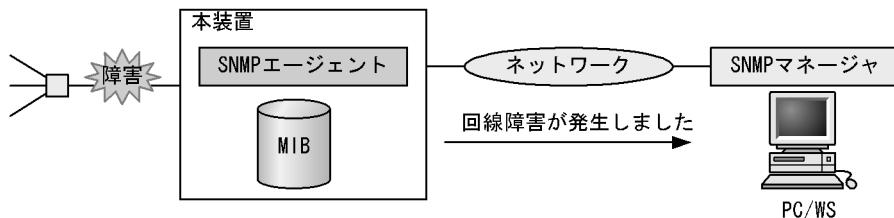


本装置の運用コマンドには MIB 情報を表示するための SNMP コマンドがあります。このコマンドは、自装置およびリモート装置の SNMP エージェントの MIB を表示します。

本装置では、SNMPv1 (RFC1157), SNMPv2C (RFC1901)，および SNMPv3 (RFC3410) をサポートしています。SNMP マネージャを使用してネットワーク管理を行う場合は、SNMPv1, SNMPv2C, または SNMPv3 プロトコルで使用してください。なお、SNMPv1, SNMPv2C, SNMPv3 をそれぞれ同時に使用することもできます。

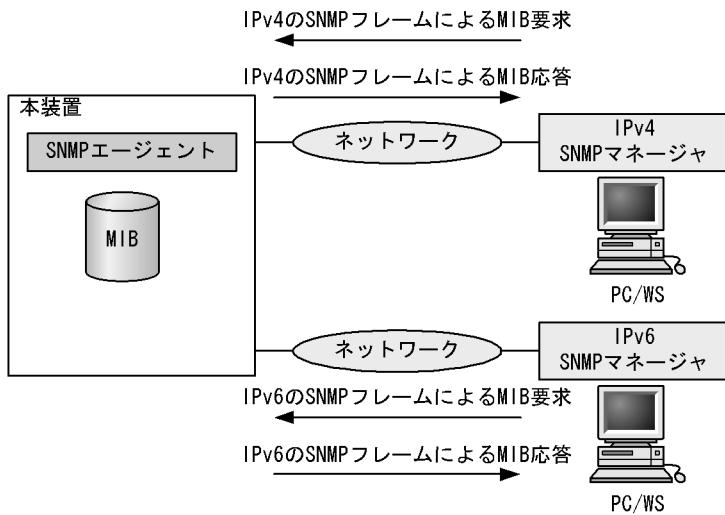
また、SNMP エージェントは **トラップ (Trap)** と呼ばれるイベント通知（主に障害発生の情報など）機能があります。SNMP マネージャは、トラップを受信することで定期的に装置の状態変化を監視しなくても変化を知ることができます。ただし、トラップは UDP を使用しているため、装置から SNMP マネージャに対するトラップの到達確認ができません。そのため、ネットワークの輻輳などによって、トラップがマネージャに到達しない場合があります。トラップの例を次の図に示します。

図 12-3 トラップの例



本装置の SNMP プロトコルは IPv6 に対応しています。コンフィグレーションに設定した SNMP マネージャの IP アドレスによって、IPv4 または IPv6 アドレスが設定されている SNMP マネージャからの MIB 要求や、SNMP マネージャへのトラップ送信ができます。IPv4/IPv6 SNMP マネージャからの MIB 要求と応答の例を次の図に示します。

図 12-4 IPv4/IPv6 SNMP マネージャからの MIB 要求と応答の例



(3) SNMPv3

SNMPv3 は SNMPv2C までの全機能に加えて、管理セキュリティ機能が大幅に強化されています。ネットワーク上を流れる SNMP パケットを認証・暗号化することによって、SNMPv2C でのコミュニティ名と SNMP マネージャの IP アドレスの組み合わせによるセキュリティ機能では実現できなかった、盗聴、なりすまし、改ざん、再送などのネットワーク上の危険から SNMP パケットを守ることができます。

(a) SNMP エンティティ

SNMPv3 では、SNMP マネージャおよび SNMP エージェントを「SNMP エンティティ」と総称します。本装置の SNMPv3 は、SNMP エージェントに相当する SNMP エンティティをサポートしています。

(b) SNMP エンジン

SNMP エンジンは認証、および暗号化したメッセージ送受信と管理オブジェクトへのアクセス制御のためのサービスを提供します。SNMP エンティティとは 1 対 1 の関係です。SNMP エンジンは、同一管理ドメイン内でユニークな SNMP エンジン ID により識別されます。

(c) ユーザ認証とプライバシー機能

SNMPv1、SNMPv2C でのコミュニティ名による認証に対して、SNMPv3 ではユーザ認証を行います。また、SNMPv1、SNMPv2C にはなかったプライバシー機能（暗号化、復号化）も SNMPv3 でサポートされています。ユーザ認証とプライバシー機能は、ユーザ単位に設定できます。

本装置では、ユーザ認証プロトコルとして次の二つプロトコルをサポートしています。

- HMAC-MD5-96 (メッセージダイジェストアルゴリズムを使用した認証プロトコル。128 ビットのダイジェストのうち、最初の 96 ビットを使用する。秘密鍵は 16 オクテット)
- HMAC-SHA-96 (SHA メッセージダイジェストアルゴリズムを使用した認証プロトコル。160 ビットの SHA ダイジェストのうち、最初の 96 ビットを使用する。秘密鍵は 20 オクテット)

プライバシープロトコルとして次のプロトコルをサポートしています。

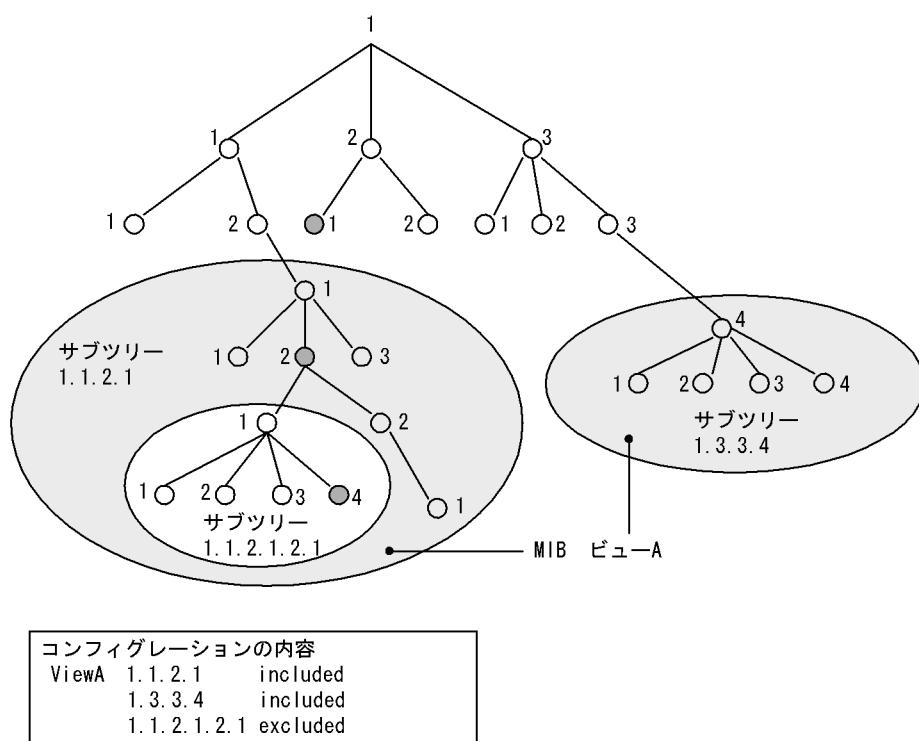
- CBC-DES (Cipher Block Chaining - Data Encryption Standard。共通鍵暗号アルゴリズムである DES (56 ビット鍵) を、CBC モードで強力にした暗号化プロトコル)

(d) MIB ビューによるアクセス制御

SNMPv3 では、ユーザ単位に、アクセスできる MIB オブジェクトの集合を設定できます。この MIB オブジェクトの集合を MIB ビューと呼びます。MIB ビューは、MIB のオブジェクト ID のツリーを表すビューサブツリーを集約することによって表現されます。集約する際には、ビューサブツリーごとに included (MIB ビューに含む)、または excluded (MIB ビューから除外する) を選択できます。MIB ビューは、ユーザ単位に、Read ビュー、Write ビュー、Notify ビューとして設定できます。

次に、MIB ビューの例を示します。MIB ビューは、「図 12-5 MIB ビューの例」に示すような MIB ツリーの一部である MIB サブツリーをまとめて設定します。オブジェクト ID 1.1.2.1.2 は、サブツリー 1.1.2.1 に含まれるので、MIB ビュー A でアクセスできます。しかし、オブジェクト ID 1.2.1 は、どちらのサブツリーにも含まれないので、アクセスできません。また、オブジェクト ID 1.1.2.1.2.1.4 は、サブツリー 1.1.2.1.2.1 がビュー A から除外されているためアクセスできません。

図 12-5 MIB ビューの例



12.1.2 MIB 概説

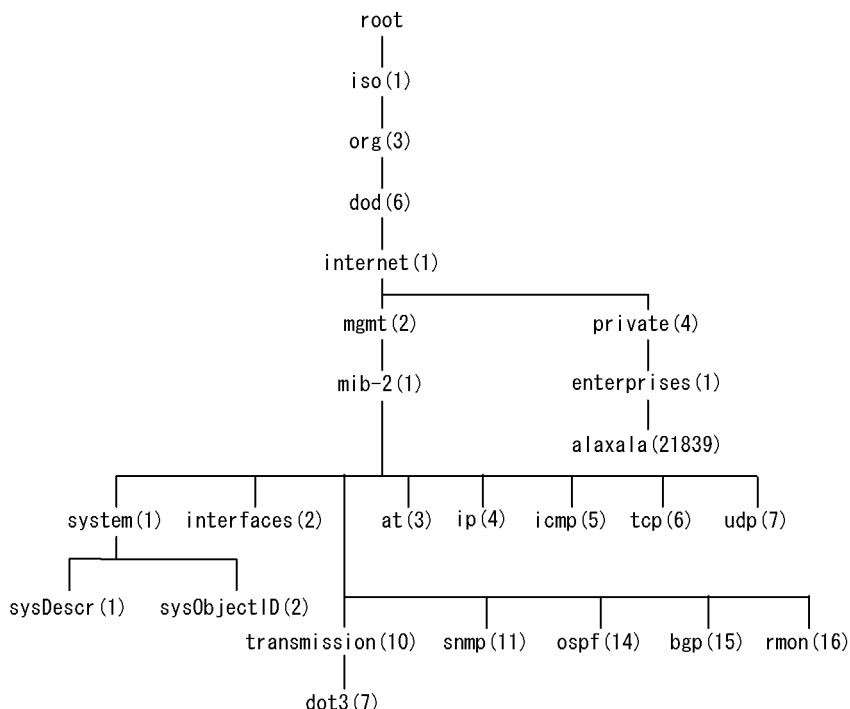
装置が管理し、SNMP マネージャに提供する MIB は、RFC で規定されたものと、装置の開発ベンダーが独自に用意する情報の 2 種類があります。

RFC で規定された MIB を**標準 MIB** と呼びます。標準 MIB は規格化されているため提供情報の内容の差はありません。装置の開発ベンダーが独自に用意する MIB を**プライベート MIB** と呼び、装置によって内容が異なります。ただし、MIB のオペレーション（情報の採取・設定など）は、標準 MIB、プライベート MIB で共通です。オペレーションは、装置と目的の MIB 情報を指定するだけです。装置は IP アドレスで、MIB 情報はオブジェクト ID で指定します。

(1) MIB 構造

MIB の構造はツリー構造になっています。MIB はツリー構造のため、各ノードを識別するために番号を付けて表す決まりになっています。root から各ノードの数字を順番にたどって番号を付けることで個々の MIB 情報を一意に識別できます。この番号列をオブジェクト ID と呼びます。オブジェクト ID は root から下位のオブジェクトグループ番号をドットで区切って表現します。例えば、sysDescr という MIB をオブジェクト ID で示すと 1.3.6.1.2.1.1.1 になります。MIB ツリーの構造例を次の図に示します。

図 12-6 MIB ツリーの構造例



(2) MIB オブジェクトの表し方

オブジェクト ID は数字と. (ドット) (例 : 1.3.6.1.2.1.1.1) で表現します。しかし、数字の羅列ではわかりにくいため、マネージャによっては、sysDescr というニーモニックで指定できるものもあります。ニーモニックで指定する場合、SNMP マネージャがどの MIB のニーモニックを使えるか確認してから使用してください。また、本装置の SNMP コマンドで使用できるニーモニックについては、snmp lookup コマンドを実行することで確認できます。

(3) インデックス

MIB を指定するときのオブジェクト ID を使用しますが、一つの MIB に一つの意味だけある場合と一つの MIB に複数の情報がある場合があります。MIB を特定するためにはインデックス (INDEX) を使用します。インデックスは、オブジェクト ID の後ろに数字を付加して表し、何番目の情報かなどを示すために使用します。

一つの MIB に一つの意味だけがある場合、MIB のオブジェクト ID に ".0" を付加して表します。一つの MIB に複数の情報がある場合、MIB のオブジェクト ID の後ろに数字を付加して何番目の情報であるか表します。例えば、インターフェースのタイプを示す MIB に ifType (1.3.6.1.2.1.2.2.1.2) があります。本装置には複数のインターフェースがあります。特定のインターフェースのタイプを調べるには、"2 番目のインターフェースのタイプ" というように具体的に指定する必要があります。MIB で指定するときは、2 番目を示すインデックス .2 を MIB の最後に付加して ifType.2 (1.3.6.1.2.1.2.2.1.2.2) と表します。

インデックスの表し方は、各 MIB によって異なります。RFC などの MIB の定義で、INDEX{xxxxx,yyyyy,zzzzz} となっている MIB のエントリは、xxxxx と yyyyy と zzzzz をインデックスに持ちます。それぞれの MIB について、どのようなインデックスを取るか確認して MIB のオペレーションを行ってください。

(4) 本装置のサポート MIB

本装置では、装置の状態、インターフェースの統計情報、装置の機器情報など、管理に必要な MIB を提供しています。なお、プライベート MIB の定義 (ASN.1) ファイルは、ソフトウェアと共に提供します。

各 MIB の詳細については、マニュアル「MIB レファレンス」を参照してください。

12.1.3 SNMPv1, SNMPv2C オペレーション

管理データ (MIB:management information base) の収集や設定を行うため、SNMP では次に示す 4 種類のオペレーションがあります。

- GetRequest : 指定した MIB の情報を取り出します。
- GetNextRequest : 指定した次の MIB の情報を取り出します。
- GetBulkRequest : GetNextRequest の拡張版です。
- SetRequest : 指定した MIB に値を設定します。

各オペレーションは SNMP マネージャから装置 (SNMP エージェント) に対して行われます。各オペレーションについて説明します。

(1) GetRequest オペレーション

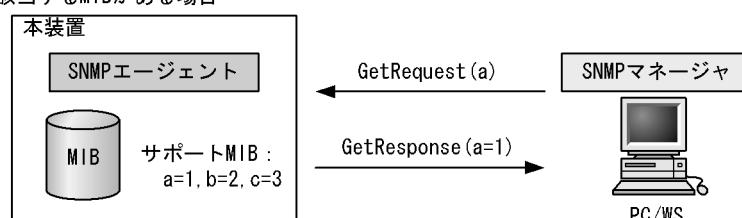
GetRequest オペレーションは、SNMP マネージャから装置 (エージェント機能) に対して MIB の情報を取り出すときに使用します。このオペレーションでは、一つまたは複数 MIB を指定できます。

装置が該当する MIB を保持している場合、GetResponse オペレーションで MIB 情報を応答します。該当する MIB を保持していない場合は、GetResponse オペレーションで noSuchName を応答します。

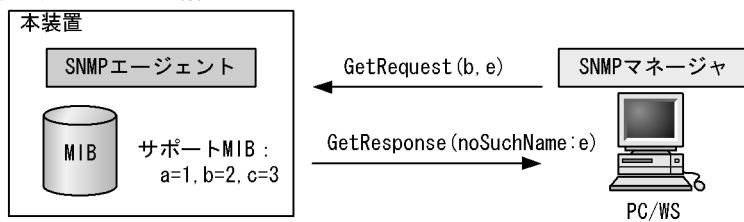
GetRequest オペレーションを次の図に示します。

図 12-7 GetRequest オペレーション

●該当するMIBがある場合

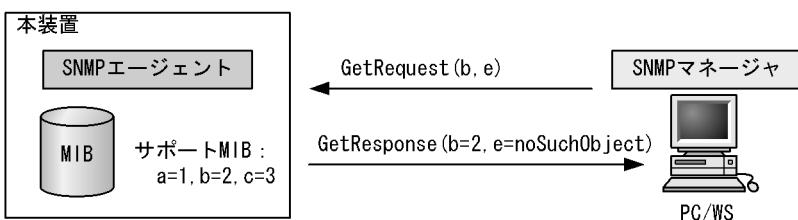


●該当するMIBがない場合



SNMPv2C では、装置が該当する MIB を保持していない場合は、GetResponse オペレーションで MIB 値に noSuchObject を応答します。SNMPv2C の場合の GetRequest オペレーションを次の図に示します。

図 12-8 GetRequest オペレーション (SNMPv2C)



(2) GetNextRequest オペレーション

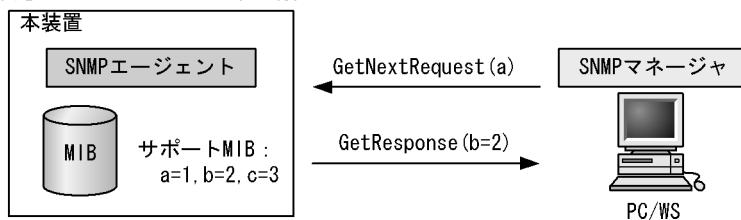
GetNextRequest オペレーションは、GetRequest オペレーションに似たオペレーションです。

GetRequest オペレーションは、指定した MIB の読み出しに使用しますが、GetNextRequest オペレーションは、指定した MIB の次の MIB を取り出すときに使用します。このオペレーションも一つまたは複数の MIB を指定できます。

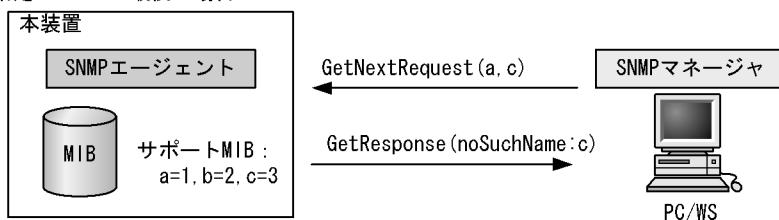
装置が指定した次の MIB を保持している場合は、GetResponse オペレーションで MIB を応答します。指定した MIB が最後の場合は、GetResponse で noSuchName を応答します。GetNextRequest オペレーションを次の図に示します。

図 12-9 GetNextRequest オペレーション

●指定したMIBの次のMIBがある場合

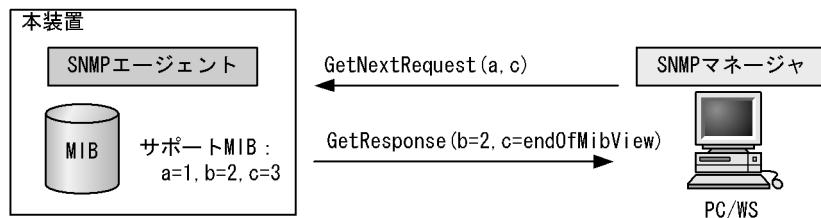


●指定したMIBが最後の場合



SNMPv2C の場合、指定した MIB が最後の場合は GetResponse で MIB 値に endOfMibView を応答します。SNMPv2C の場合の GetNextRequest オペレーションを次の図に示します。

図 12-10 GetNextRequest オペレーション (SNMPv2C)



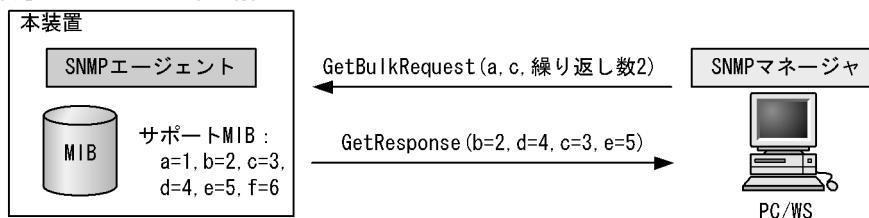
(3) GetBulkRequest オペレーション

GetBulkRequest オペレーションは、GetNextRequest オペレーションを拡張したオペレーションです。このオペレーションでは繰り返し回数を設定し、指定した MIB の次の項目から指定した繰り返し回数個分の MIB を取得できます。このオペレーションも、一つまたは複数の MIB を指定できます。

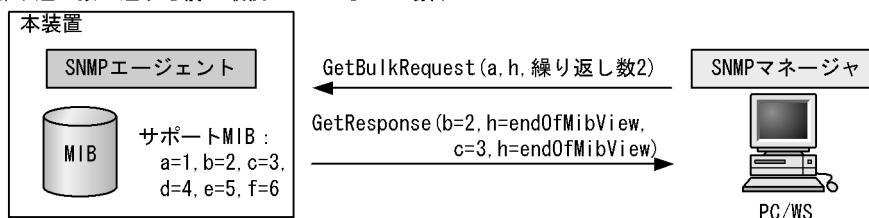
装置が、指定した MIB の次の項目から指定した繰り返し回数個分の MIB を保持している場合は、GetResponse オペレーションで MIB を応答します。指定した MIB が最後の場合、または繰り返し数に達する前に最後の MIB になった場合、GetResponse オペレーションで MIB 値に endOfMibView を応答します。GetBulkRequest オペレーションを次の図に示します。

図 12-11 GetBulkRequest オペレーション

●指定MIBの次のMIBがある場合



●繰り返し数に達する前に最後のMIBになった場合

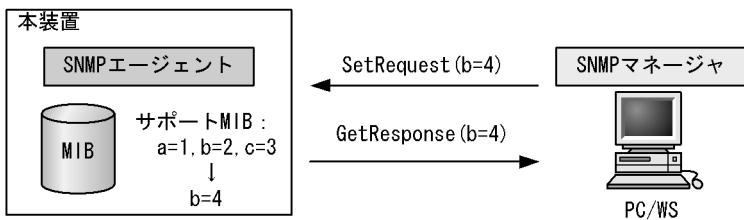


(4) SetRequest オペレーション

SetRequest オペレーションは、SNMP マネージャから装置（エージェント機能）に対して行うオペレーションという点で GetRequest, GetNextRequest, GetBulkRequest オペレーションと似ていますが、値の設定方法が異なります。

SetRequest オペレーションでは、設定する値と MIB を指定します。値を設定すると、GetResponse オペレーションで MIB と設定値を応答します。SetRequest オペレーションを次の図に示します。

図 12-12 SetRequest オペレーション



(a) MIB を設定できない場合の応答

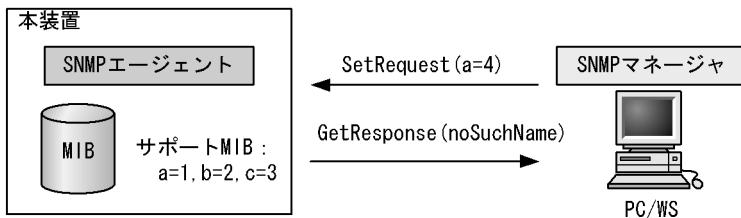
MIB を設定できないケースは、次に示す 3 とおりです。

- MIB が読み出し専用の場合（読み出し専用コミュニティに属するマネージャの場合も含む）
- 設定値が正しくない場合
- 装置の状態によって設定できない場合

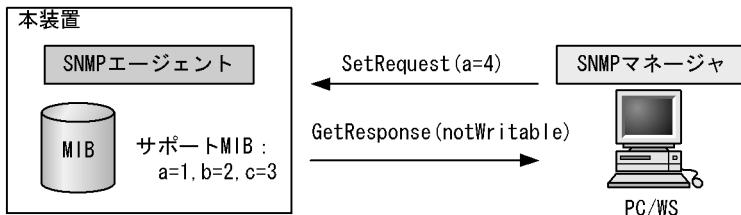
各ケースによって、応答が異なります。MIB が読み出し専用の場合、noSuchName の GetResponse 応答をします。SNMPv2C の場合、MIB が読み出し専用のときは notWritable の GetResponse 応答をします。MIB が読み出し専用の場合の SetRequest オペレーションを次の図に示します。

図 12-13 MIB 変数が読み出し専用の場合の SetRequest オペレーション

●SNMP

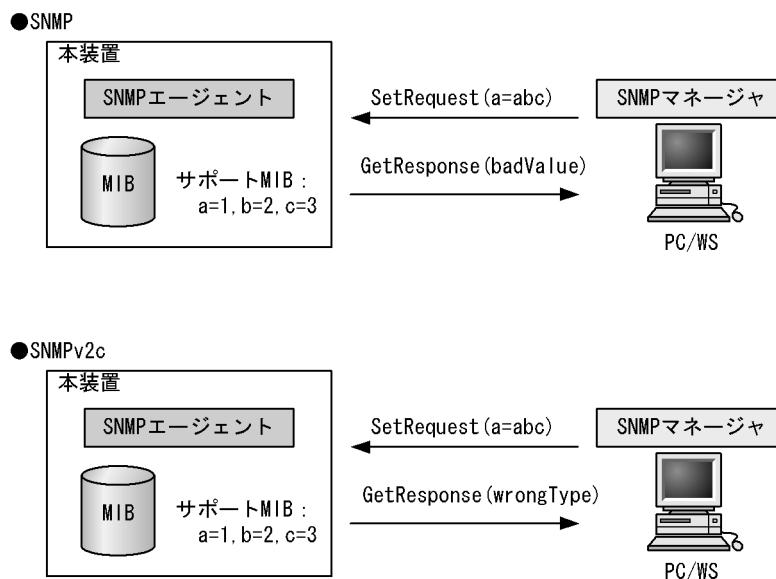


●SNMPv2c



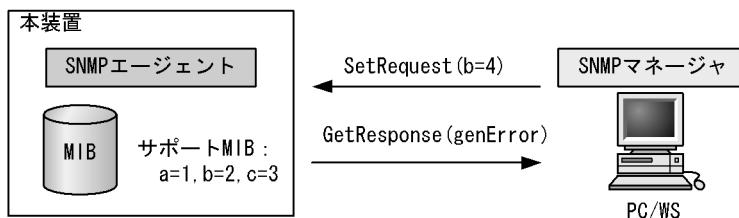
設定値のタイプが正しくない場合、badValue の GetResponse 応答をします。SNMPv2C の場合、設定値のタイプが正しくないときは wrongType の GetResponse 応答をします。設定値のタイプが正しくない場合の SetRequest オペレーションを次の図に示します。

図 12-14 設定値のタイプが正しくない場合の SetRequest オペレーション例



装置の状態によって設定できない場合、`genError`を応答します。例えば、装置内で値を設定しようとしたときに、装置内部で設定タイムアウトを検出した場合などがこれに当てはまります。装置の状態によって設定できない場合の SetRequest オペレーションを次の図に示します。

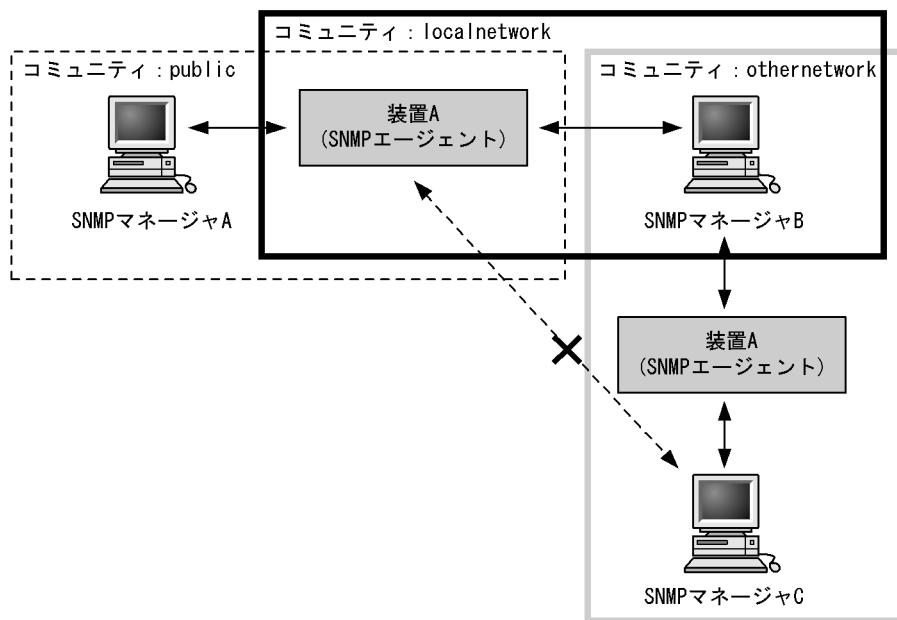
図 12-15 装置の状態によって設定できない場合の SetRequest オペレーション



(5) コミュニティによるオペレーション制限

SNMPv1 および SNMPv2C では、オペレーションを実行する SNMP マネージャを限定するため、コミュニティという概念があります。コミュニティはオペレーションを実行する SNMP マネージャと SNMP エージェントを一つのグループとして割り当てる名称です。MIB に対してオペレーションする場合は、SNMP マネージャと SNMP エージェントは、同一のグループ（コミュニティ）に属する必要があります。コミュニティによるオペレーションを次の図に示します。

図 12-16 コミュニティによるオペレーション



装置 A はコミュニティ (public) およびコミュニティ (localnetwork) に属しています。コミュニティ (othernetwork) には属していません。この場合、装置 A はコミュニティ (public) およびコミュニティ (localnetwork) の SNMP マネージャ A, B から MIB のオペレーションを受け付けますが、コミュニティ (othernetwork) の SNMP マネージャ C からのオペレーションは受け付けません。

(6) IP アドレスによるオペレーション制限

本装置では、セキュリティを考慮し、アクセスリストを使用することでコミュニティと SNMP マネージャの IP アドレスの組み合わせが合わないときは MIB のオペレーションを受け付けないようにできます。本装置で SNMPv1 および SNMPv2C を使用するときは、コミュニティをコンフィグレーションコマンドで登録する必要があります。なお、コミュニティは文字列で設定します。また、一般的にコミュニティ名称は、public を使用している場合が多いです。

(7) SNMP オペレーションのエラーステータスコード

オペレーションでエラーが発生した場合、SNMP エージェントはエラーステータスにエラーコードを設定し、何番目の MIB 情報でエラーが発生したかをエラー位置番号に設定した GetResponse オペレーションの応答を返します。オペレーションの結果が正常なら、エラーステータスにエラーなしのコードを設定し、MIB 情報内にオペレーションした MIB 情報を設定した GetResponse オペレーションの応答を返します。エラーステータスコードを次の表に示します。

表 12-1 エラーステータスコード

エラーステータス	コード	内容
noError	0	エラーはありません。
tooBig	1	データサイズが大きく PDU に値を設定できません。
noSuchName	2	指定 MIB がない、または書き込みできませんでした。
badValue	3	設定値が不正です。
readOnly	4	書き込みできませんでした（本装置では、応答することはできません）。

エラーステータス	コード	内容
genError	5	その他のエラーが発生しました。
noAccess	6	アクセスできない MIB に対して set を行おうとしました。
wrongType	7	MIB で必要なタイプと異なるタイプが指定されました。
wrongLength	8	MIB で必要なデータ長と異なる長さが指定されました。
wrongEncoding	9	ASN.1 符号が不正でした。
wrongValue	10	MIB 値が不正でした。
noCreation	11	該当する MIB が存在しません。
inconsistentValue	12	現在何か理由があつて値が設定できません。
resourceUnavailable	13	値の設定のためにリソースが必要ですが、リソースが利用できません。
commitFailed	14	値の更新に失敗しました。
undoFailed	15	値の更新に失敗したときに、更新された値を元に戻すのに失敗しました。
notWritable	17	セットできません。
inconsistentName	18	該当する MIB が存在しないため、現在は作成できません。

12.1.4 SNMPv3 オペレーション

管理データ（MIB:management information base）の収集や設定を行うため、SNMP では次に示す四種類のオペレーションがあります。

- GetRequest : 指定した MIB の情報を取り出します。
- GetNextRequest : 指定した次の MIB の情報を取り出します。
- GetBulkRequest : GetNextRequest の拡張版です。
- SetRequest : 指定した MIB に値を設定します。

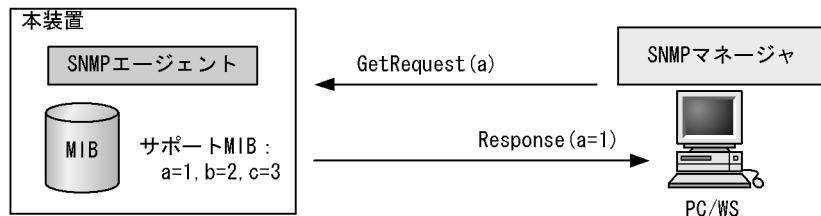
各オペレーションは SNMP マネージャから装置（SNMP エージェント）に対して行われます。各オペレーションについて説明します。

(1) GetRequest オペレーション

GetRequest オペレーションは、SNMP マネージャから装置（エージェント機能）に対して MIB の情報を取り出すときに使用します。このオペレーションでは、一つまたは複数の MIB を指定できます。装置が該当する MIB を保持している場合、Response オペレーションで MIB 情報を応答します。

GetRequest オペレーションを次の図に示します。

図 12-17 GetRequest オペレーション



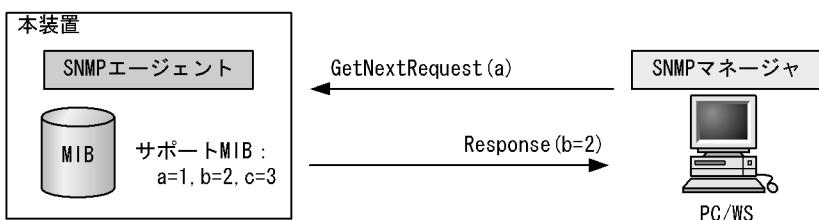
(2) GetNextRequest オペレーション

GetNextRequest オペレーションは、GetRequest オペレーションに似たオペレーションです。

GetRequest オペレーションが指定した MIB の読み出しに使用するのに対し、GetNextRequest オペレーションは指定した MIB の次の MIB を取り出すときに使用します。このオペレーションも一つまたは複数の MIB を指定できます。

GetNextRequest オペレーションを次の図に示します。

図 12-18 GetNextRequest オペレーション

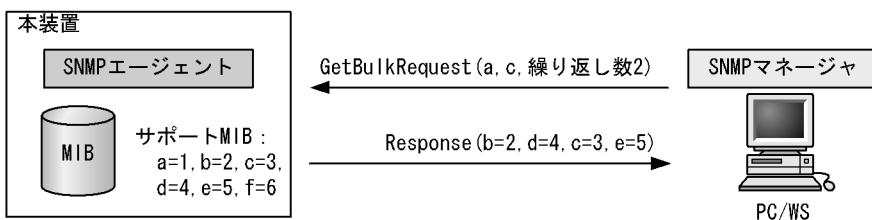


(3) GetBulkRequest オペレーション

GetBulkRequest オペレーションは、GetNextRequest オペレーションを拡張したオペレーションです。このオペレーションでは繰り返し回数を設定し、指定した MIB の次の項目から指定した繰り返し回数個分の MIB を取得できます。このオペレーションも、一つまたは複数の MIB を指定できます。

GetBulkRequest オペレーションを次の図に示します。

図 12-19 GetBulkRequest オペレーション



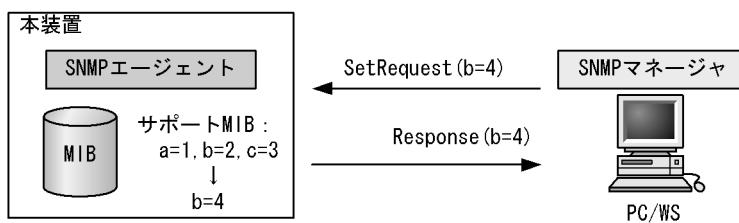
(4) SetRequest オペレーション

SetRequest オペレーションは、SNMP マネージャから装置（エージェント機能）に対して行うオペレーションという点で GetRequest, GetNextRequest, GetBulkRequest オペレーションと似ていますが、値の設定方法が異なります。

SetRequest オペレーションでは、設定する値と MIB を指定します。値を設定すると、Response オペレーションで MIB と設定値を応答します。

SetRequest オペレーションを次の図に示します。

図 12-20 SetRequest オペレーション



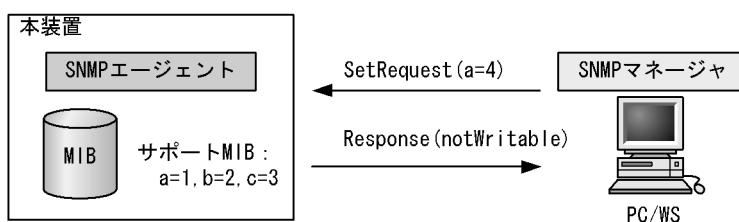
(a) MIB を設定できない場合の応答

MIB を設定できないケースは、次に示す 3 とおりです。

- MIB が読み出し専用の場合
- 設定値が正しくない場合
- 装置の状態によって設定できない場合

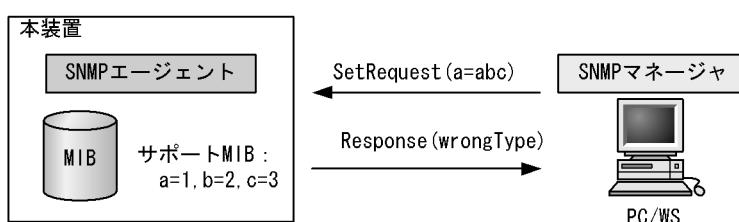
各ケースによって、応答が異なります。MIB が読み出し専用のときは notWritable の Response 応答をします。MIB が読み出し専用の場合の SetRequest オペレーションを次の図に示します。

図 12-21 MIB 変数が読み出し専用の場合の SetRequest オペレーション



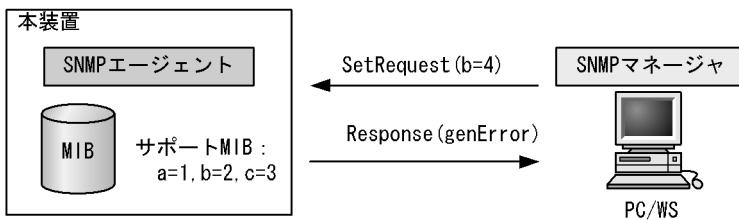
設定値のタイプが正しくないときは wrongType の Response 応答をします。設定値のタイプが正しくない場合の SetRequest オペレーションを次の図に示します。

図 12-22 設定値のタイプが正しくない場合の SetRequest オペレーション例



装置の状態によって設定できない場合、genError を応答します。例えば、装置内で値を設定しようとしたときに、装置内部で設定タイムアウトを検出した場合などがこれに当たります。装置の状態によって設定できない場合の SetRequest オペレーションを次の図に示します。

図 12-23 装置の状態によって設定できない場合の SetRequest オペレーション



(5) SNMPv3 でのオペレーション制限

SNMPv1 および SNMPv2C ではコミュニティと SNMP マネージャの IP アドレスの組み合わせによって確認が行われるのに対し、SNMPv3 ではユーザ認証と MIB ビューによって MIB のオペレーションを制限します。本装置で SNMPv3 を使用するときは、SNMP セキュリティユーザ、MIB ビューおよびセキュリティグループをコンフィグレーションコマンドで登録する必要があります。また、トラップを送信するには、SNMP セキュリティユーザ、MIB ビュー、セキュリティグループ、およびトラップ送信 SNMP マネージャをコンフィグレーションコマンドで登録する必要があります。

(6) SNMPv3 オペレーションのエラーステータスコード

オペレーションの結果エラーが発生した場合、SNMP エージェントはエラーステータスにエラーコードを設定し、何番目の MIB 情報でエラーが発生したかをエラー位置番号に設定した Response オペレーションの応答を返します。オペレーションの結果が正常であれば、エラーステータスにエラーなしのコードを設定し、MIB 情報内にオペレーションした MIB 情報を設定した Response オペレーションの応答を返します。エラーステータスコードを次の表に示します。

表 12-2 エラーステータスコード

エラーステータス	コード	内容
noError	0	エラーはありません。
tooBig	1	データサイズが大きく PDU に値を設定できません。
noSuchName	2	指定 MIB がない、または書き込みできませんでした。
badValue	3	設定値が不正です。
readOnly	4	書き込みできませんでした（本装置では、応答することはできません）。
genError	5	その他のエラーが発生しました。
noAccess	6	アクセスできない MIB に対して set を行おうとしました。
wrongType	7	MIB で必要なタイプと異なるタイプが指定されました。
wrongLength	8	MIB で必要なデータ長と異なる長さが指定されました。
wrongEncoding	9	ASN.1 符号が不正でした。
wrongValue	10	MIB 値が不正でした。
noCreation	11	該当する MIB が存在しません。
inconsistentValue	12	現在何か理由があつて値が設定できません。
resourceUnavailable	13	値の設定のためにリソースが必要ですが、リソースが利用できません。
commitFailed	14	値の更新に失敗しました。
undoFailed	15	値の更新に失敗したときに、更新された値を元に戻すのに失敗しました。
authorizationError	16	認証に失敗しました。
notWritable	17	セットできません。

エラーステータス	コード	内容
inconsistentName	18	該当する MIB が存在しないため、現在は作成できません。

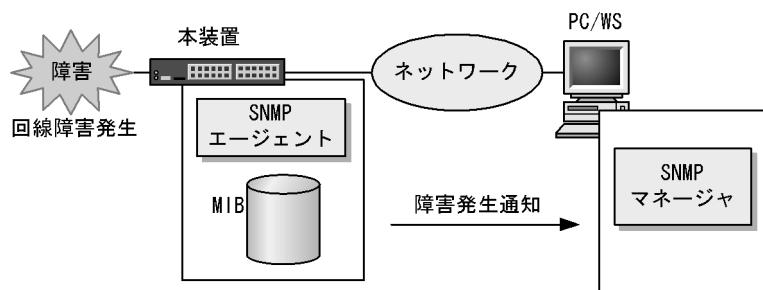
12.1.5 トラップ

(1) トラップ概説

SNMP エージェントはトラップ (Trap) と呼ばれるイベント通知（主に障害発生の情報やログ情報など）機能があります。トラップは重要なイベントを SNMP エージェントから SNMP マネージャに非同期に通知する機能です。SNMP マネージャは、トラップを受信することで定期的に装置の状態変化を検知できます。この通知を基に、装置内の MIB を取得して、さらに詳細な情報を得ることができます。

なお、トラップは UDP を使用しているため、装置から SNMP マネージャに対するトラップの到達が確認できません。そのため、ネットワークの輻輳などによってトラップがマネージャに到達しない場合があります。トラップの例を次の図に示します。

図 12-24 トラップの例



(2) トラップフォーマット

トラップフレームには、どの IP アドレスの装置で、いつ、何が発生したかを示す情報を含みます。トラップフォーマットを次の図に示します。

図 12-25 トラップフォーマット

SNMPバージョン	Community名	Trap PDU						
TRAP	装置ID	エージェントアドレス	トラップ番号	拡張トラップ番号	発生時刻	関連MIB情報		

装置ID : 装置の識別 ID（通常MIB-IIのsysObjectIDの値が設定される）

エージェントアドレス : トラップが発生した装置のIPアドレス

トラップ番号 : トラップの種別を示す識別番号

拡張トラップ番号 : トラップ番号の補足をするための番号

発生時刻 : トラップが発生した時間（装置が起動してからの経過時間）

関連MIB情報 : このトラップに関連するMIB情報

12.1.6 RMON MIB

RMON (Remote Network Monitoring) とは、イーサネット統計情報を提供する機能、収集した統計情報の閾値チェックを行ってイベントを発生させる機能、パケットをキャプチャする機能などを持ちます。この RMON は RFC1757 で規定されています。

RMON MIB のうち、statistics、history、alarm、event の各グループについて概要を説明します。

(1) statistics グループ

監視対象のサブネットワークについての、基本的な統計情報を収集します。例えば、サブネットワーク中の総パケット数、ブロードキャストパケットのような各種類ごとのパケット数、CRC エラー、コリジョンエラーなどのエラー数などです。statistics グループを使うと、サブネットワークのトラフィック状況や回線状態などの統計情報を取得できます。

(2) history グループ

statistics グループで収集する情報とほぼ同じ統計情報をサンプリングし、来歴情報として保持できます。

history グループには historyControlTable という制御テーブルと、etherHistoryTable というデータテーブルがあります。historyControlTable はサンプリング間隔や来歴記録数の設定を行うための MIB です。

etherHistoryTable は、サンプリングした統計情報の来歴記録の MIB です。history グループは、一定期間の統計情報を装置内で保持しています。このため、SNMP マネージャなどが定期的にポーリングして統計情報を収集するのと比較して、ネットワークに負荷をかけることが少なく、連続した一定期間の統計情報を取得できます。

(3) alarm グループ

監視対象とする MIB のチェック間隔、閾値などを設定して、その MIB が閾値に達したときにログを記録したり、SNMP マネージャにトラップを発行したりすることを指定する MIB です。

この alarm グループは、例えば、サンプルタイムとして設定した 5 分間のうちに、パケットを取りこぼすという状態が 10 回以上検出したときにログを収集したり、SNMP マネージャにトラップを発行したりできます。この alarm グループを使用するときは、event グループも設定する必要があります。

(4) event グループ

event グループには alarm グループで設定した MIB の閾値を超えたときの動作を指定する eventTable グループ MIB と閾値を超えたときにログを記録する logTable グループ MIB があります。

eventTable グループ MIB は、閾値に達したときにログを記録するのか、SNMP マネージャにトラップを発行するのか、またはその両方するか何もしないかを設定するための MIB です。

logTable グループ MIB は、eventTable グループ MIB でログの記録を指定したときに、装置内にログを記録します。装置内のログのエントリ数は決まっているので、エントリをオーバーした場合、新しいログ情報の追加によって、古いログ情報が消去されていきます。定期的に SNMP マネージャに記録を退避しないと、前のログが消されてしまう可能性がありますので注意してください。

12.1.7 SNMP マネージャとの接続時の注意事項

(1) MIB 情報収集周期のチューニング

SNMP マネージャは、ネットワーク上の新しい装置を検出したり、トライフィック状況を監視したりするため、SNMP エージェントサポート機器から定期的に MIB を取得します。この定期的な MIB 取得の間隔が短いと、ネットワーク機器やネットワークに負荷が掛かります。また、装置の状態や構成などによって、MIB 取得時にマネージャ側でタイムアウトが発生するおそれがあります。特に、次に示すケースでは応答タイムアウトの発生するおそれがあります。

- 接続 SNMP マネージャ数が多い場合

本装置に SNMP マネージャが多数接続され、MIB 情報の収集が集中した場合。

- SNMP イベントが同時に多数発生している場合

本装置から大量にトラップが発行されるような状態のときに、MIB を取得した場合や、本装置から発行されたトラップに基づいて、並行して MIB を取得した場合。

応答タイムアウトが頻発する場合は、SNMP マネージャのポーリング周期や応答監視タイマ値をチューニングしてください。代表的な SNMP マネージャのチューニングパラメータには、次の三つがあります。

- ポーリング周期

- 応答監視タイマ

- 応答監視タイムアウト時のリトライ回数

12.2 コンフィグレーション

12.2.1 コンフィグレーションコマンド一覧

SNMP/RMON に関するコンフィグレーションコマンド一覧を次の表に示します。

表 12-3 コンフィグレーションコマンド一覧

コマンド名	説明
hostname	本装置のホスト名称を設定します。本設定は RFC1213 の sysName に対応します。
rmon alarm	RMON (RFC1757) アラームグループの制御情報を設定します。
rmon collection history	RMON (RFC1757) イーサネットの統計来歴の制御情報を設定します。
rmon event	RMON (RFC1757) イベントグループの制御情報を設定します。
snmp-server community	SNMP コミュニティに対するアクセスリストを設定します。
snmp-server contact	本装置の連絡先などを設定します。本設定は RFC1213 の sysContact に対応します。
snmp-server engineID local	SNMP エンジン ID 情報を設定します。
snmp-server group	SNMP セキュリティグループ情報を設定します。
snmp-server host	トラップを送信するネットワーク管理装置 (SNMP マネージャ) を登録します。
snmp-server location	本装置を設置する場所の名称を設定します。本設定は RFC1213 の sysLocation に対応します。
snmp-server traps	トラップの発行契機を設定します。
snmp-server user	SNMP セキュリティユーザ情報を設定します。
snmp-server view	MIB ビュー情報を設定します。
snmp trap link-status	回線がリンクアップまたはダウンした場合に、トラップ (SNMP link down および up Trap) の送信を抑止します。

12.2.2 SNMPv1, SNMPv2C による MIB アクセス許可の設定

[設定のポイント]

SNMP マネージャから本装置の MIB へのアクセスを許可するための設定をします。

[コマンドによる設定]

1. **(config)# access-list 1 permit 128.1.1.2 0.0.0.0**

IP アドレス 128.1.1.2 からのアクセスを許可するアクセスリストの設定を行います。

2. **(config)# snmp-server community "NETWORK" ro 1**

SNMP マネージャのコミュニティに対する MIB アクセスマードおよび適用するアクセスリストを設定します。

- コミュニティ名 : NETWORK
- アクセスリスト : 1
- アクセスマード : read only

12.2.3 SNMPv3 による MIB アクセス許可の設定

[設定のポイント]

SNMPv3 で MIB にアクセスするために、アクセスを許可する MIB オブジェクトの集合を MIB ビューとして設定し、ユーザ認証とプライバシー機能の情報を SNMP セキュリティユーザとして設定します。また、MIB ビューと SNMP セキュリティユーザを関連づけるために、SNMP セキュリティグループを設定します。

[コマンドによる設定]

1.

```
(config)# snmp-server view "READ_VIEW" 1.3.6.1 included
(config)# snmp-server view "READ_VIEW" 1.3.6.1.6.3 excluded
(config)# snmp-server view "WRITE_VIEW" 1.3.6.1.2.1.1 included
```

MIB ビューを設定します。

 - ビュー名 READ_VIEW に internet グループ MIB (サブツリー : 1.3.6.1) を登録します。
 - ビュー名 READ_VIEW から snmpModules グループ MIB (サブツリー : 1.3.6.1.6.3) を対象外にします。
 - ビュー名 WRITE_VIEW に system グループ MIB (サブツリー : 1.3.6.1.2.1.1) を登録します。

2.

```
(config)# snmp-server user "ADMIN" "ADMIN_GROUP" v3 auth md5 "ABC*_1234" priv des "XYZ/+6789"
```

SNMP セキュリティユーザを設定します。

 - SNMP セキュリティユーザ名 : ADMIN
 - SNMP セキュリティグループ名 : ADMIN_GROUP
 - 認証プロトコル : HMAC-MD5
 - 認証パスワード : ABC*_1234
 - 暗号化プロトコル : CBC-DES
 - 暗号化パスワード : XYZ/+6789

3.

```
(config)# snmp-server group "ADMIN_GROUP" v3 priv read "READ_VIEW" write "WRITE_VIEW"
```

SNMP セキュリティグループを設定します。

 - SNMP セキュリティグループ名 : ADMIN_GROUP
 - セキュリティレベル : 認証あり, 暗号化あり
 - Read ビュー名 : READ_VIEW
 - Write ビュー名 : WRITE_VIEW

12.2.4 SNMPv1, SNMPv2C によるトラップ送信の設定

[設定のポイント]

トラップを発行する SNMP マネージャを登録します。

[コマンドによる設定]

```
1. (config)# snmp-server host 128.1.1.2 traps "NETWORK" version 1 snmp
```

SNMP マネージャに標準トラップを発行する設定をします。

- コミュニティ名 : NETWORK
- SNMP マネージャの IP アドレス : 128.1.1.2
- 発行するトラップ : 標準トラップ

12.2.5 SNMPv3 によるトラップ送信の設定

[設定のポイント]

MIB ビューと SNMP セキュリティユーザを設定の上、SNMP セキュリティグループを設定し、さらに SNMP トラップモードを設定します。

[コマンドによる設定]

```
1. (config)# snmp-server view "ALL_TRAP_VIEW" * included
```

MIB ビューを設定します。

- ビュー名 ALL_TRAP_VIEW に全サブツリーを登録します。


```
2. (config)# snmp-server user "ADMIN" "ADMIN_GROUP" v3 auth md5 "ABC*_1234" priv des "XYZ/+6789"
```

SNMP セキュリティユーザを設定します。

- SNMP セキュリティユーザ名 : ADMIN
- SNMP セキュリティグループ名 : ADMIN_GROUP
- 認証プロトコル : HMAC-MD5
- 認証パスワード : ABC*_1234
- 暗号化プロトコル : DES
- 暗号化パスワード : XYZ/+6789


```
3. (config)# snmp-server group "ADMIN_GROUP" v3 priv notify "ALL_TRAP_VIEW"
```

SNMP セキュリティグループを設定します。

- SNMP セキュリティグループ名 : ADMIN_GROUP
- セキュリティレベル : 認証あり、暗号化あり
- Notify ビュー名 : ALL_TRAP_VIEW


```
4. (config)# snmp-server host 128.1.1.2 traps "ADMIN" version 3 priv snmp
```

SNMPv3 によって SNMP マネージャに標準トラップを発行する設定をします。

- SNMP マネージャの IP アドレス : 128.1.1.2
- SNMP セキュリティユーザ名 : ADMIN
- セキュリティレベル : 認証あり、暗号化あり
- 発行するトラップ : 標準トラップ

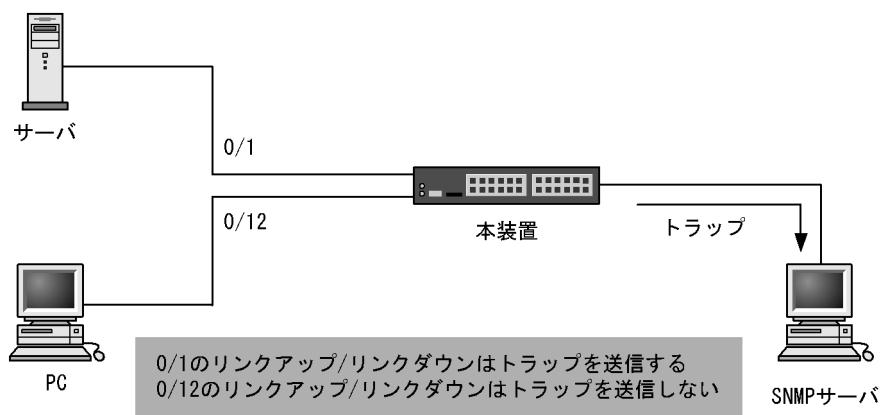
12.2.6 リンクトラップの抑止

本装置は、デフォルト動作としてイーサネットインターフェースがリンクアップまたはリンクダウンしたときに、SNMP トラップを発行します。また、コンフィグレーションによって、イーサネットインターフェースごとに、リンクトラップの送信抑止を設定できます。例えば、サーバと接続する回線のように重要度の高い回線だけトラップを送信し、そのほかの回線のリンクトラップの送信を抑止することで、本装置、ネットワーク、および SNMP マネージャの不要な処理を削減できます。

[設定のポイント]

リンクトラップの設定内容はネットワーク全体の運用方針に従って決定します。

図 12-26 リンクトラップの構成図



ここでは、ポート 0/1 については、トラップを送信するので、コンフィグレーションの設定は必要ありません。ポート 0/12 については、トラップを送信しないように設定します。

[コマンドによる設定]

1. `(config)# interface gigabitethernet 0/12`
`(config-if)# no snmp trap link-status`
 リンクアップ／リンクダウン時にトラップを送信しません。
2. `(config-if)# exit`

12.2.7 RMON イーサネットヒストリグループの制御情報の設定

[設定のポイント]

RMON (RFC1757) イーサネットの統計来歴の制御情報を設定します。本コマンドでは最大 32 エントリの設定ができます。あらかじめ SNMP マネージャを登録しておく必要があります。

[コマンドによる設定]

1. `(config)# interface gigabitethernet 0/5`
 ギガビット・イーサネットインターフェース 0/5 のインターフェースモードに遷移します。

```
2. (config-if)# rmon collection history controlEntry 33 owner "NET-MANAGER"
```

```
    buckets 10
```

統計来歴の制御情報の情報識別番号、設定者の識別情報、および統計情報を格納する来歴エントリ数を設定します。

- 情報識別番号 : 33
- 来歴情報の取得エントリ : 10 エントリ
- 設定者の識別情報 : " NET-MANAGER "

12.2.8 RMON による特定 MIB 値の閾値チェック

[設定のポイント]

特定の MIB の値に対して定期的に閾値チェックを行い、閾値を超えたなら SNMP マネージャにイベントを通知するように設定します。

イベント実行方法に trap を指定する場合は、あらかじめ SNMP トラップモードの設定が必要です。

[コマンドによる設定]

```
1. (config)# rmon event 3 log trap public
```

アラームが発生したときに実行するイベントを設定します。

- 情報識別番号 : 3
- イベント実行方法 : log, trap
- Trap 送信コミュニティ名 : public

```
2. (config)# rmon alarm 12 "ifOutDiscards.3" 256111 delta rising-threshold 400000
    rising-event-index 3 falling-threshold 100 falling-event-index 3 owner
    "NET-MANAGER"
```

RMON アラームグループの制御情報を次の条件で設定します。

- RMON アラームグループの制御情報識別番号 : 12
- 閾値チェックを行う MIB のオブジェクト識別子 : ifOutDiscards.3
- 閾値チェックを行う時間間隔 : 256111 秒
- 閾値チェック方式 : 差分値チェック (delta)
- 上方閾値の値 : 400000
- 上方閾値を超えたときのイベント方法の識別番号 : 3
- 下方閾値の値 : 100
- 下方閾値を超えたときのイベント方法の識別番号 : 3
- コンフィグレーション設定者の識別情報 : NET-MANAGER

12.3 オペレーション

12.3.1 運用コマンド一覧

SNMP/RMON に関する運用コマンド一覧を次の表に示します。

表 12-4 運用コマンド一覧

コマンド名	説明
snmp lookup	サポート MIB オブジェクト名称およびオブジェクト ID を表示します。
snmp get	指定した MIB の値を表示します。
snmp getnext	指定した次の MIB の値を表示します。
snmp walk	指定した MIB ツリーを表示します。
snmp getif	interface グループの MIB 情報を表示します。
snmp getroute	ipRouteTabler (IP ルーティングテーブル) を表示します。
snmp getarp	ipNetToMediaTable (IP アドレス変換テーブル) を表示します。
snmp getforward	ipForwardTable (IP フォワーディングテーブル) を表示します。
snmp rget	指定したリモート装置の MIB の値を表示します。
snmp rgetnext	指定したリモート装置の次の MIB の値を表示します。
snmp rwalk	指定したリモート装置の MIB ツリーを表示します。
snmp rgetroute	指定したリモート装置の ipRouteTabler (IP ルーティングテーブル) を表示します。
snmp rgetarp	指定したリモート装置の ipNetToMediaTable (IP アドレス変換テーブル) を表示します。

12.3.2 SNMP マネージャとの通信の確認

本装置に SNMP エージェント機能を設定して SNMP プロトコルによるネットワーク管理を行う場合、次のことを確認してください。

- ネットワーク上の SNMP マネージャから本装置に対して MIB を取得できること
- 本装置からネットワーク上の SNMP マネージャへ SNMP のトラップが送信されていること

確認手順を次に示します。なお、本装置から取得できる MIB についてはマニュアル「MIB レファレンス

1. サポート MIB の概要」を、本装置から送信されるトラップについてはマニュアル「MIB レファレンス 4.2 サポートトラップ -PDU 内パラメータ」を、それぞれ参照してください。

1. ping コマンドを SNMP マネージャの IP アドレスを指定して実行し、本装置から SNMP マネージャに対して IP 通信ができるかを確認してください。通信ができない場合はマニュアル「トラブルシューティングガイド」を参照してください。
2. SNMP マネージャから本装置に対して MIB の取得ができるかを確認してください。取得できない場合の対応はマニュアル「トラブルシューティングガイド」を参照してください。

13 ログ出力機能

この章では、本装置のログ出力機能について説明します。

13.1 解説

13.2 コンフィギュレーション

13.1 解説

本装置では動作情報や障害情報などを運用メッセージとして通知します。同メッセージは運用端末に出力するほか、運用ログとして装置内に保存します。この情報で装置の運用状態や障害の発生を管理できます。

運用ログは装置運用中に発生した事象（イベント）を発生順に記録したログ情報で、運用メッセージと同様の内容が格納されます。運用ログとして格納する情報には次に示すものがあります。

- オペレータの操作および応答メッセージ
- 運用メッセージ

種別ログは装置内で発生した障害や警告についての運用ログ情報をメッセージ ID ごとに分類した上で、同事象が最初に発生した日時および最後に発生した日時と累積回数をまとめた情報です。

これらのログは装置内にテキスト形式で格納されています。装置管理者は、表示コマンドでこれらの情報を参照できます。

採取した本装置のログ情報は、syslog インタフェースを使用して syslog 機能を持つネットワーク上の他装置（UNIX ワークステーションなど）に送ることができます^{※1}、^{※2}。また、同様に、ログ情報を E-Mail を使用してネットワーク上の他装置に送ることもできます。これらのログ出力機能を使用することで、多数の装置を管理する場合にログの一元管理ができるようになります。また、ログ情報を E-Mail で送信することもできます。

注※ 1

他装置からの syslog メッセージを受信する機能はサポートしていません。

注※ 2

本装置で生成した syslog メッセージでは、RFC3164 で定義されている HEADER 部の HOSTNAME 欄は未設定です。

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

ログ出力機能に関するコンフィグレーションコマンド一覧を次の表に示します。

表 13-1 コンフィグレーションコマンド一覧（syslog 出力に関する設定）

コマンド名	説明
logging event-kind	syslog サーバに送信対象とするログ情報のイベント種別を設定します。
logging facility	ログ情報を syslog インタフェースで出力するためのファシリティを設定します。
logging host	ログ情報の出力先を設定します。
logging trap	syslog サーバに送信対象とするログ情報の重要度を設定します。

表 13-2 コンフィグレーションコマンド一覧（E-Mail 出力に関する設定）

コマンド名	説明
logging email	ログ情報を E-Mail で出力するための E-Mail アドレスを設定します。
logging email-event-kind	E-Mail で出力対象とするログ情報のイベント種別を設定します。
logging email-from	ログ情報を E-Mail で出力する E-Mail の送信元を設定します。
logging email-interval	ログ情報を E-Mail で出力するための送信間隔を設定します。
logging email-server	ログ情報を E-Mail で出力するため SMTP サーバの情報を設定します。

13.2.2 ログの syslog 出力の設定

[設定のポイント]

syslog 出力機能を使用して、採取したログ情報を syslog サーバに送信するための設定をします。

[コマンドによる設定]

1. **(config) # logging host LOG_HOST**

ログをホスト名 LOG_HOST 宛てに出力するように設定します。

13.2.3 ログの E-Mail 出力の設定

[設定のポイント]

E-Mail 送信機能を使用して、採取したログ情報をリモートホスト、PC などに送信するための設定をします。

[コマンドによる設定]

1. **(config) # logging email system@loghost**

送信先のメールアドレスとして system@loghost を設定します。

14 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。

14.1 解説

14.2 コンフィグレーション

14.3 オペレーション

14.1 解説

14.1.1 sFlow 統計の概要

sFlow 統計はエンド-to-end 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（RFC 3176）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 14-1 sFlow 統計のネットワーク構成例

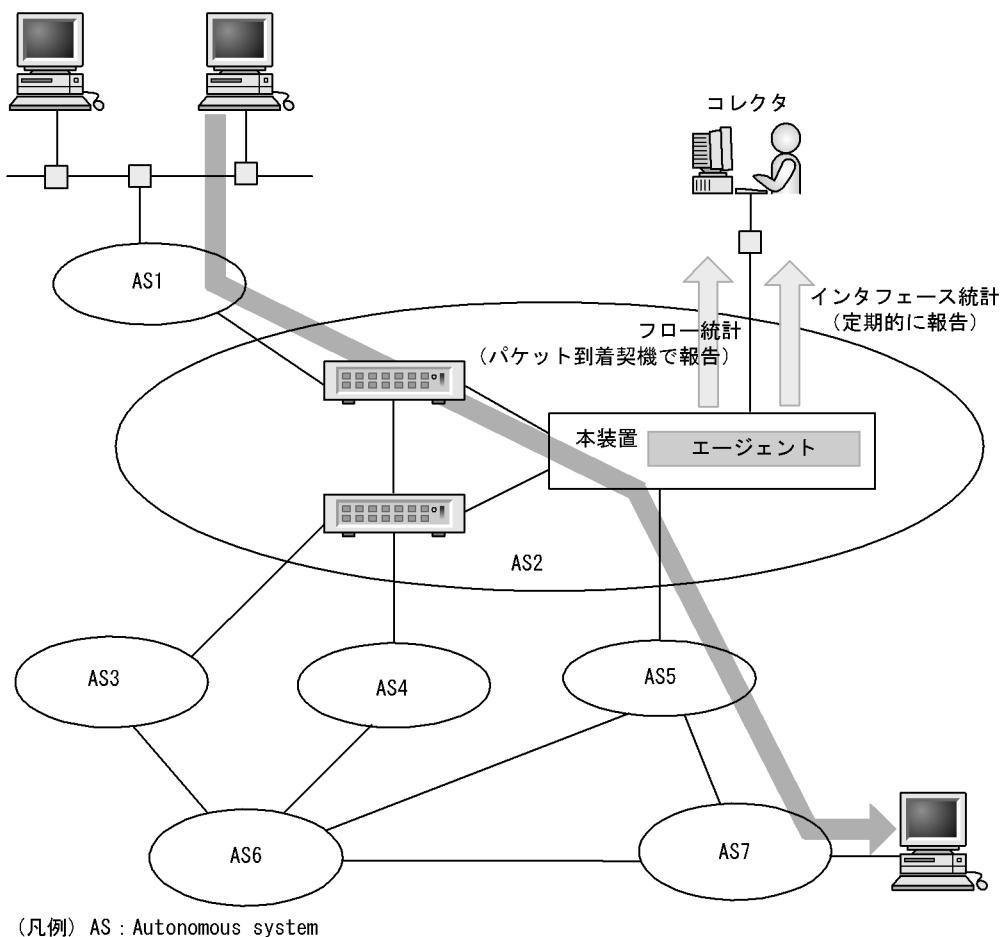


図 14-2 システム構成

本装置



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 14-1 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になっている場合もあります。

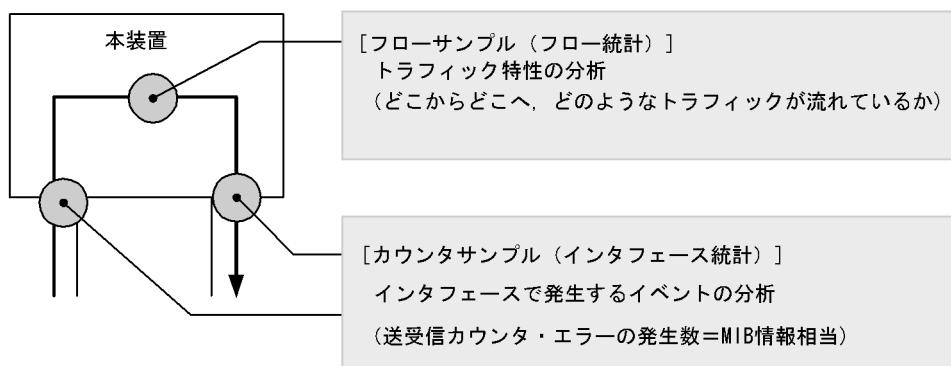
14.1.2 sFlow 統計エージェント機能

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、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ー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の図に示します。

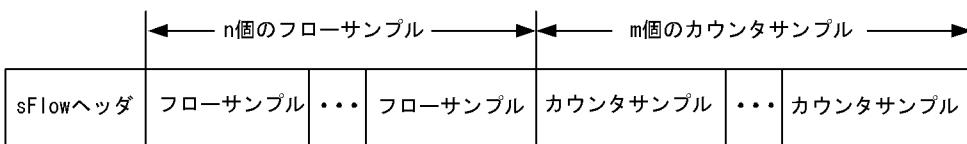
図 14-3 フローサンプルとカウンタサンプル



14.1.3 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（フローサンプルとカウンタサンプル）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 RFC 3176 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 14-4 sFlow パケットフォーマット



(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 14-2 sFlow ヘッダのフォーマット

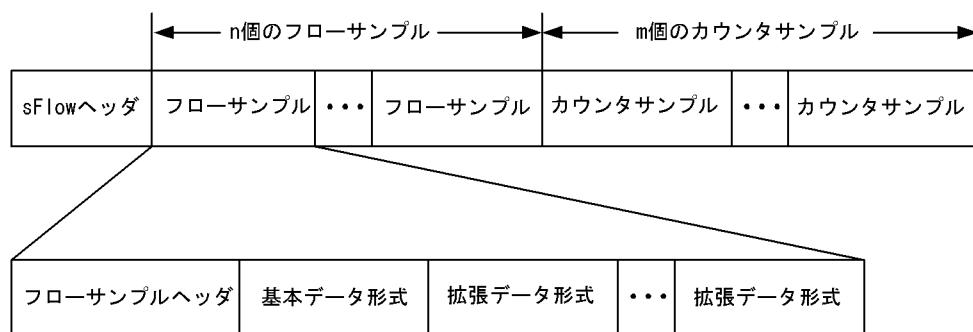
設定項目	説明	サポート
バージョン番号	sFlow パケットのバージョン（バージョン 2, 4 をサポート）	○
アドレスタイプ	エージェントの IP タイプ（IPv4=1, IPv6=2）	○
エージェント IP アドレス	エージェントの IP アドレス	○
シーケンス番号	sFlow パケットの生成ごとに増加する番号	○
生成時刻	現在の時間（装置の起動時からのミリセカンド）	○
サンプル数	この信号に含まれるサンプリング（フロー・カウンタ）したパケット数 (「図 14-4 sFlow パケットフォーマット」の例では $n + m$ が設定されます)	○

（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、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（受信インターフェース、送信インターフェース、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 14-5 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 14-3 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（受信インターフェース）を表す SNMP Interface Index	○
sampling_rate	フローサンプルのサンプリング間隔	○
sample_pool	インターフェースに到着したパケットの総数	○
drops	廃棄したフローサンプルの総数	○
input	受信インターフェースの SNMP Interface Index。 インターフェースが不明な場合 0 を設定	○
output	送信インターフェースの SNMP Interface Index [※] 。 送信インターフェースが不明な場合は 0 を設定。	×

(凡例) ○：サポートする ×：サポートしない

注※ 本装置では output をサポートしていないため 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 型を使用したい場合はコンフィギュ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以降の表に示します。

表 14-4 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できない場合には、本フォーマットになります。

表 14-5 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 のタイプオプサービス	○

(凡例) ○ : サポートする

表 14-6 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	○

(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すべての拡張形式を収集し、コレクタに送信します。本形式はコンフィグレーションにより変更可能です。各形式のフォーマットを以降の表に示します。

表 14-7 拡張データ形式の種別一覧

拡張データ種別	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。	○※1※2
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。	○※1※2
ユーザ型	ユーザ情報 (TACACS/RADIUS 情報など) を収集する。	○※2
URL型	URL 情報 (URL 情報など) を収集する。	○※2

(凡例) ○ : サポートする

注※1 L2 中継時は sFlow パケットに収集されません。

注※2 2 段以上の VLAN tag 付きフレームが対象になった場合は、sFlow パケットに収集されません。

表 14-8 スイッチ型のフォーマット

設定項目	説明	サポート
extended_information_type	拡張データ形式のタイプ (スイッチ型=1)	○
src_vlan	受信パケットの 802.1Q VLAN ID	○
src_priority	受信パケットの 802.1p 優先度	○
dst_vlan	送信パケットの 802.1Q VLAN ID	×※
dst_priority	送信パケットの 802.1p 優先度	×※

(凡例) ○ : サポートする × : サポートしない

注※ 未サポートのため 0 固定です。

表 14-9 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※ 宛先アドレスへの経路がマルチパス経路の場合は0で収集されます。

表 14-10 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 本装置から送信元を検索した場合の隣接AS番号です。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 14-11 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）	○
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※	×
dst_user<>	宛先のユーザ名※	×

(凡例) ○：サポートする ×：サポートしない

注※ 未サポートのため0固定です。

表 14-12 URL 型のフォーマット

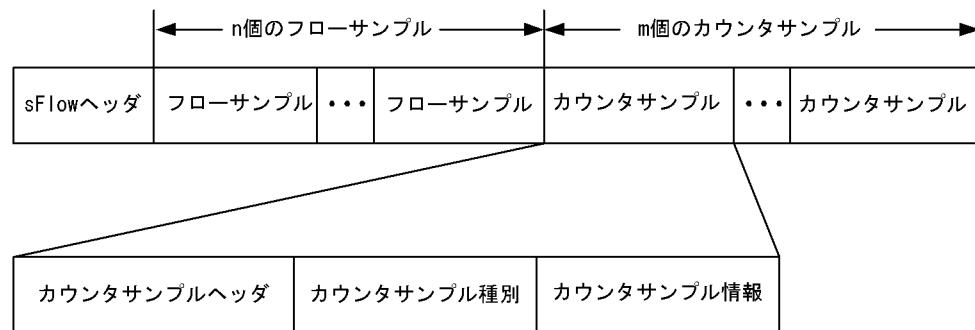
設定項目	説明	サポート
extended_information_type	拡張データ形式のタイプ (URL型=5)	○
url_direction	URL 情報源 (source address=1, destination address=2)	○
url_len	URL 長	○
url<>	URL 内容	○

(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、インターフェース統計情報（到着したパケット数や、エラーの数など）を送信します。また、インターフェースの種別よりコレクタに送信するフォーマットが決定されます。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 14-6 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 14-13 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ーフェースの種別ごとに分類され収集されます。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 14-14 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

設定項目	説明	サポート
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)	×※1
FDDI	FDDI 統計 (counters_type=4)	×※1
100BaseVG	VG 統計 (counters_type=5)	×※1
WAN	WAN 統計 (counters_type=6)	×※1
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 本装置で未サポートなインターフェースタイプのためです。

注※2 本装置では VLAN 統計はサポートしていません。

(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り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 14-15 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 [RFC 2233 参照]	×
ETHERNET	イーサネット統計 [RFC 2358 参照]	○※
TOKENRING	トークンリング統計 [RFC 1748 参照]	×
FDDI	FDDI 統計 [RFC 1512 参照]	×
100BaseVG	VG 統計 [RFC 2020 参照]	×
WAN	WAN 統計 [RFC 2233 参照]	×
VLAN	VLAN 統計 [RFC 3176 参照]	×

(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, dot3StatsSymbolErrors, ifOutUcastPkts は収集できません。

14.1.4 本装置での sFlow 統計の動作について

(1) sFlow 統計収集の対象パケットに関する注意点

- 本装置での sFlow 統計は、受信パケットと送信パケットを対象パケットとして扱います。
- 送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断されるパケットなど）は、sFlow 統計収集の対象外パケットとして扱います。
- ソフトウェア中継パケットや自発パケット、自宛パケットは sFlow 統計収集の対象外パケットとして扱います。
- ポートミラーリングのミラーポートからの送信パケットは、sFlow 統計収集の対象外パケットとして扱います。

(2) データ収集位置による注意点

- ingress 指定および egress 指定のどちらで検出されても、sFlow パケットの内容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 sFlow 統計は、受信パケットまたは送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、受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ご確認の上運用してください。他機能と併用時の sFlow 統計収集条件を次の表に示します。

表 14-16 他機能と併用時の sFlow 統計収集条件

機能	受信パケットが sFlow 統計対象	送信パケットが sFlow 統計対象
フィルタ機能	廃棄対象でも収集される	廃棄対象は収集されない※
QoS 機能（受信側）	廃棄対象でも収集される	廃棄対象は収集されない※
QoS 機能（送信側）	廃棄対象でも収集される	廃棄対象でも収集される※
自宛	収集されない	収集されない
自発	収集されない	収集されない

注※ sFlow パケットの内容は、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。

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

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 14-17 コンフィグレーションコマンド一覧

コマンド名	説明
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 egress	指定したポートの送信トラフィックを sFlow 統計の監視対象にします。
sflow forward ingress	指定したポートの受信トラフィックを sFlow 統計の監視対象にします。
sflow max-header-size	基本データ形式 (sflow packet-information-type コマンド参照) 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。
sflow url-port-add	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 version	送信する sFlow パケットのバージョンを設定します。

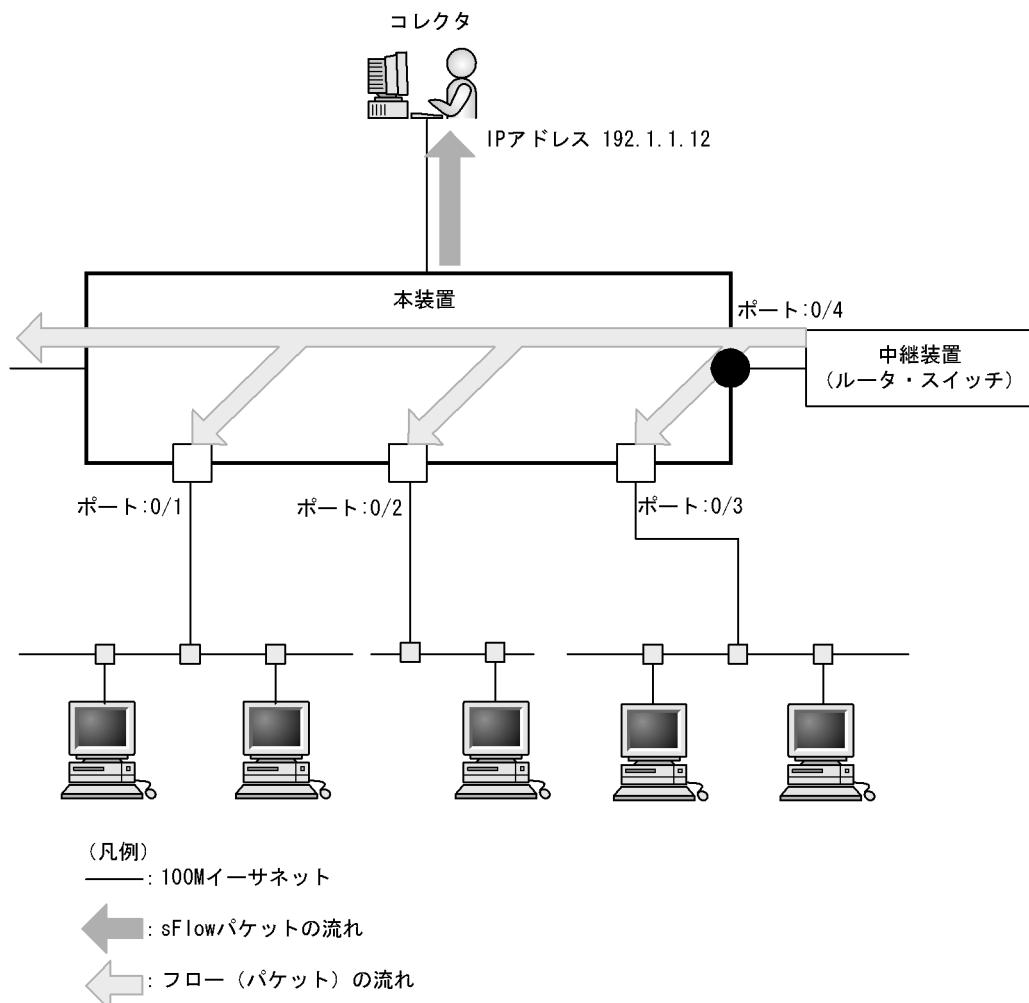
14.2.2 sFlow 統計の基本的な設定

(1) 受信パケットをモニタする設定

[設定のポイント]

sFlow 統計のコンフィグレーション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。ここではポート 0/4 に対して入ってくるパケットをモニタする設定を示します。

図 14-7 ポート 0/4 の受信パケットをモニタする設定例



[コマンドによる設定]

1. **(config)# sflow destination 192.1.1.12**

コレクタとして IP アドレス 192.1.1.12 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 0/4**

ポート 0/4 のイーサネットインターフェース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 0/4 の受信パケットに対して sFlow 統計機能を有効にします。

[注意事項]

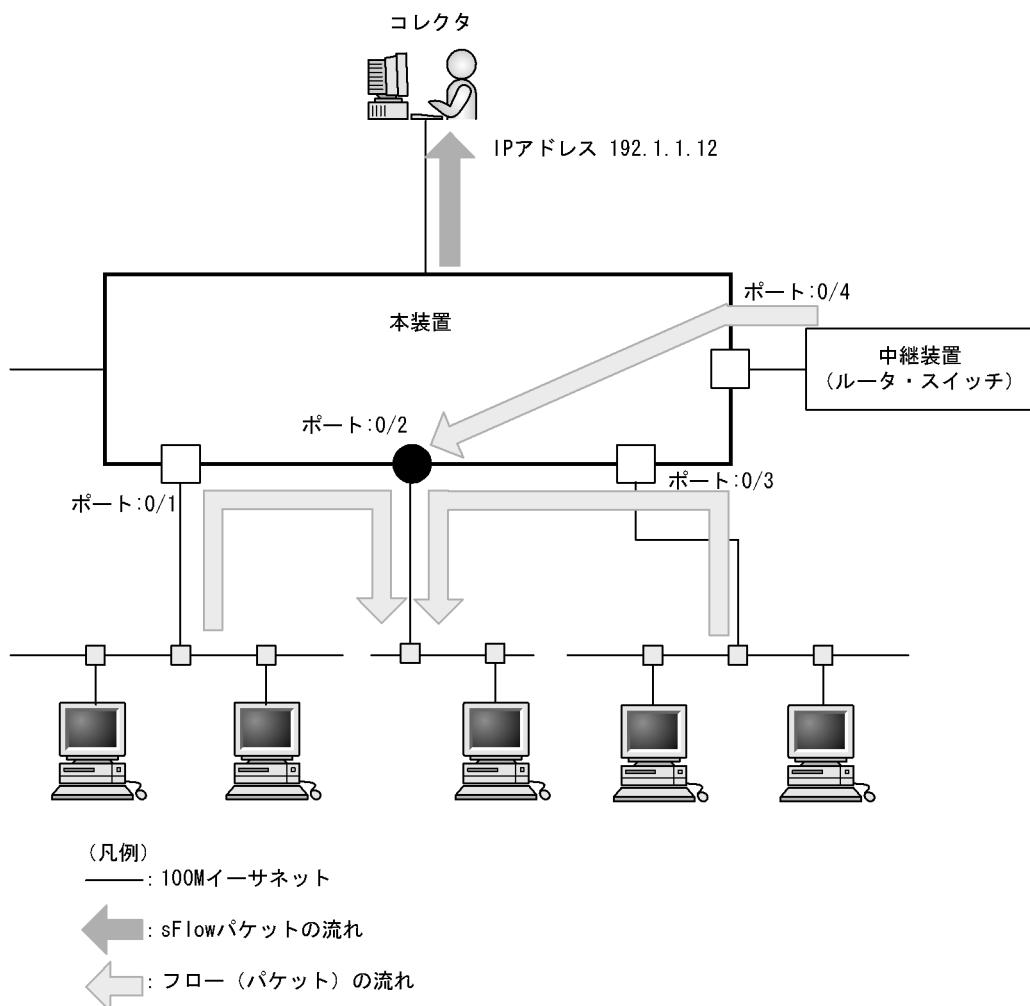
sflow sample コマンドで設定するサンプリング間隔については、インターフェースの回線速度を考慮して決める必要があります。詳細は、「コンフィグレーションコマンドレファレンス Vol.1」を参照してください。

(2) 送信パケットをモニタする設定

[設定のポイント]

sFlow 統計機能を、受信パケットまたは送信パケットのどちらに対して有効にするかは、インターフェースコンフィグレーションモードで設定するときに `sflow forward ingress` コマンドまたは `sflow forward egress` コマンドのどちらを指定するかによって決まります。ここではポート 0/2 から出て行くパケットをモニタする設定を示します。

図 14-8 ポート 0/2 の送信パケットをモニタする設定例



[コマンドによる設定]

1. `(config)# sflow destination 192.1.1.12`
コレクタとして IP アドレス 192.1.1.12 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 0/2`
ポート 0/2 のイーサネットインターフェースコンフィグレーションモードに移行します。

4. (config-if)# sflow forward egress

ポート 0/2 の送信パケットに対して sFlow 統計機能を有効にします。

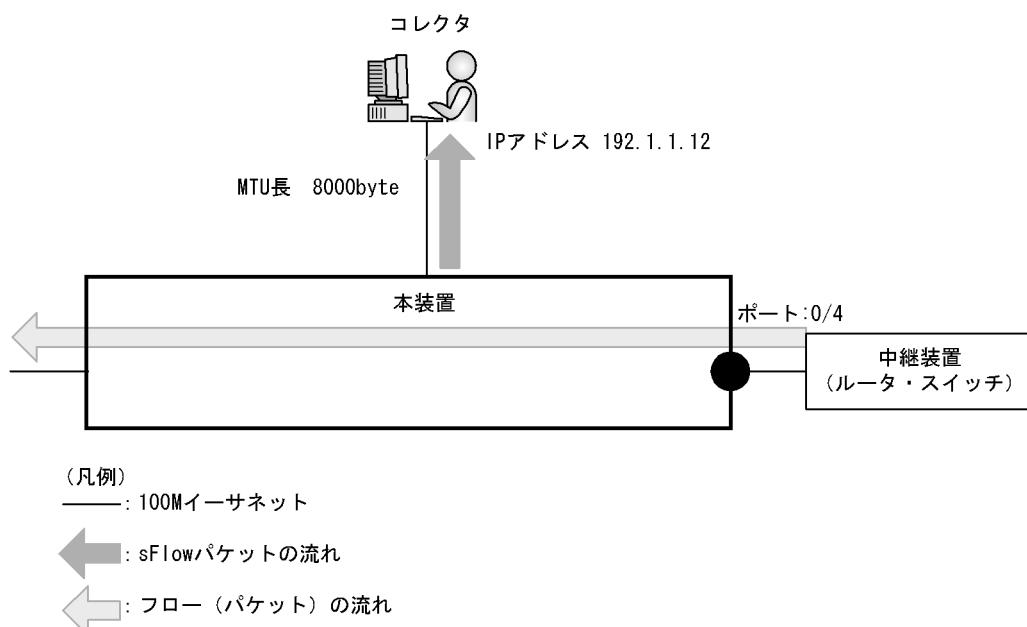
14.2.3 sFlow 統計コンフィグレーションパラメータの設定例

(1) MTU 長と sFlow パケットサイズの調整

[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。ここでは MTU 長が 8000byte の回線とコレクタが繋がっている設定を記述します。

図 14-9 コレクタへの送信を MTU=8000byte に設定する例



[コマンドによる設定]

1. (config)# sflow destination 192.1.1.12

コレクタとして IP アドレス 192.1.1.12 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 0/4

ポート 0/4 のイーサネットインターフェース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 0/4 の受信パケットに対して sFlow 統計機能を有効にします。

(2) 収集したい情報を絞る

[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に、その情報を取らない設定をすることで CPU 使用率を下げることができます。ここでは IP アドレス情報だけが必要な場合の設定を記述します。

[コマンドによる設定]

1. **(config)# sflow destination 192.1.1.12**

コレクタとして IP アドレス 192.1.1.12 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」を設定します（ルータ情報だけが取得できます）。

5. **(config)# interface gigabitethernet 0/4**

ポート 0/4 のイーサネットインターフェース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 0/4 の受信パケットに対して sFlow 統計機能を有効にします。

(3) sFlow パケットのエージェント IP アドレスを固定化する

[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 アドレスを固定化してください。ここでは loopback 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、コレクタに送る設定を示します。

[コマンドによる設定]

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

ループバックインターフェースコンフィグレーションモードに移行します。

2. **(config-if)# ip address 176.1.1.11**

ループバックインターフェースに IPv4 用として 176.1.1.11 を設定します。

3. **(config-if)# ipv6 address 3ffe:100::1**

(config-if)# exit

ループバックインターフェースに IPv6 用として 3ffe:100::1 を設定します。

4. (config)# sflow destination 192.1.1.12

コレクタとして IP アドレス 192.1.1.12 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 0/4

ポート 0/4 のイーサネットインターフェース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 0/4 の受信パケットに対して sFlow 統計機能を有効にします。

[注意事項]

loopback の IP アドレスを使う場合は、`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とその 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**[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。しかし、ローカルなネットワークではポート番号が異なる場合があります。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を示します。

[コマンドによる設定]**1. (config)# sflow destination 192.1.1.12**

コレクタとして IP アドレス 192.1.1.12 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 url-port-add 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 0/4

ポート 0/4 のイーサネットインターフェース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 0/4 の受信パケットに対して sFlow 統計機能を有効にします。

[注意事項]

本パラメータを設定した後でも、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。

14.3 オペレーション

14.3.1 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 14-18 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。
show sflow detail	sFlow 統計機能についての設定条件と動作状況と詳細情報を表示します。
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。

14.3.2 コレクタとの通信の確認

本装置で sFlow 統計機能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、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、マニュアル「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、マニュアル「トラブルシューティングガイド」を参照してください。

14.3.3 sFlow 統計機能の運用中の確認

本装置で sFlow 統計機能を使用した場合、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 統計機能で Dropped sFlow samples (廃棄しているパケット数) や Overflow Time of sFlow Queue (廃棄パケット時間) を確認してください。どちらかの値が増加する場合は、増加しないサンプリング間隔を設定してください。

図 14-10 show sflow コマンドの実行結果

```
> show sflow
Date 2010/12/01 15:30:00 UTC
sFlow service status: enable
Progress time from sFlow statistics cleared: 16:00:05
sFlow agent data :
  sFlow service version : 4
  CounterSample interval rate: 60 seconds
  Default configured rate: 1 per 2048 packets
  Default actual rate : 1 per 2048 packets
  Configured sFlow ingress ports : 0/2-4
  Configured sFlow egress ports : -----
  Received sFlow samples : 37269 Dropped sFlow samples : 2093
  Exported sFlow samples : 37269 Couldn't export sFlow samples : 0
  Overflow time of sFlow queue: 12 seconds ...1
sFlow collector data :
  Collector IP address: 192.168.4.199 UDP:6343 Source IP address: 130.130.130.1
  Send FlowSample UDP packets : 12077 Send failed packets: 0
  Send CounterSample UDP packets: 621 Send failed packets: 0
  Collector IP address: 192.168.4.203 UDP:65535 Source IP address: 130.130.130.1
  Send FlowSample UDP packets : 12077 Send failed packets: 0
  Send CounterSample UDP packets: 621 Send failed packets: 0
```

1. 廃棄パケット時間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。

(2) CPU 使用率の確認

show cpu コマンドを実行して CPU 使用率を表示し、負荷を確認してください。CPU 使用率が高い場合は、コンフィグレーションコマンド sflow sample でサンプリング間隔を再設定してください。

図 14-11 show cpu コマンドの実行結果

```
>show cpu minutes
Date 2010/12/01 15:30:00 UTC
*** minute ***
date      time          cpu average
Dec 01    14:42:00-14:42:59      6
Dec 01    14:43:00-14:43:59     20
:
:
Dec 01    15:21:00-15:21:59     10           ...1
```

1. CPU 使用率が高くなっている場合、サンプリング間隔の設定を見直してください。

14.3.4 sFlow 統計のサンプリング間隔の調整方法

本装置で sFlow 統計機能を使用した場合、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 pps を show interfaces コマンドで確認し、受信パケットを対象にしている場合は「Input rate」を合計してください。もし、送信パケットを対象にしている場合は、「Output rate」も合計してください。その合計値を 100 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 コマンドで廃棄数が増えないかどうかを確認してください。

ポート 0/4 とポート 0/5 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 14-12 show interfaces コマンドの実行結果

```
> show interfaces gigabitethernet 0/4
Date 2010/12/01 15:30:00 UTC
NIF0:
Port4: active up 100BASE-TX full(auto) 0012.e220.ec30
    Time-since-last-status-change:1:47:47
    Bandwidth:10000kbps Average out:0Mbps Average in:5Mbps
    Peak out:5Mbps at 15:44:36 Peak in:5Mbps at 13:44:18
    Output rate: 0.0bps 0.0pps
    Input rate: 4063.5kbps 10.3kpps
    Flow control send :off
    Flow control receive:off
    TPID:8100
    :

> show interfaces gigabitethernet 0/5
Date 2010/12/01 15:30:00 UTC
NIF0:
Port5: active up 100BASE-TX full(auto) 0012.e220.ec31
    Time-since-last-status-change:1:47:47
    Bandwidth:10000kbps Average out:5Mbps Average in:5Mbps
    Peak out:5Mbps at 15:14:36 Peak in:5Mbps at 15:14:18
    Output rate: 4893.5kbps 16.8kpps
    Input rate: 4893.5kbps 16.8kpps
    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 /100
- = (10.3kpps+16.8kpps) /100
- = 271※

注※ サンプリング間隔を 271 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 Vol.1」にて sflow sample コマンドを参照してください。

(2) 詳細情報から調整する

show sflow detail コマンドを実行して表示される Sampling rate to collector (廃棄が発生しない推奨するサンプリング間隔) の値をサンプリング間隔として設定します。設定後は clear sflow statistics コマンドを実行し、しばらく様子を見てまだ Sampling rate to collector の値が設定より大きい場合は同じ手順でサンプリング間隔を設定してください。

図 14-13 show sflow detail コマンドの実行結果

```
> show sflow detail
Date 2010/12/01 15:30:00 UTC
sFlow service status: enable
Progress time from sFlow statistics cleared: 8:00:05
:
    Collector IP address: 192.168.4.203 UDP:65535 Source IP address:
130.130.130.1
    Send FlowSample UDP packets : 12077 Send failed packets: 0
    Send CounterSample UDP packets: 621 Send failed packets: 0
Detail data :
    Max packet size: 1400 bytes
    Packet information type: header
    Max header size: 128 bytes
    Extended information type: switch,router,gateway,user,url
    Url port number: 80,8080
    Sampling mode: random-number
    Sampling rate to collector: 1 per 2163 packets
    Target ports for CounterSample: 0/2-4
```


15 LLDP

この章では、本装置に隣接する装置の情報を収集する機能である LLDP の解説と操作方法について説明します。

15.1 解説

15.2 コンフィグレーション

15.3 オペレーション

15.1 解説

15.1.1 概要

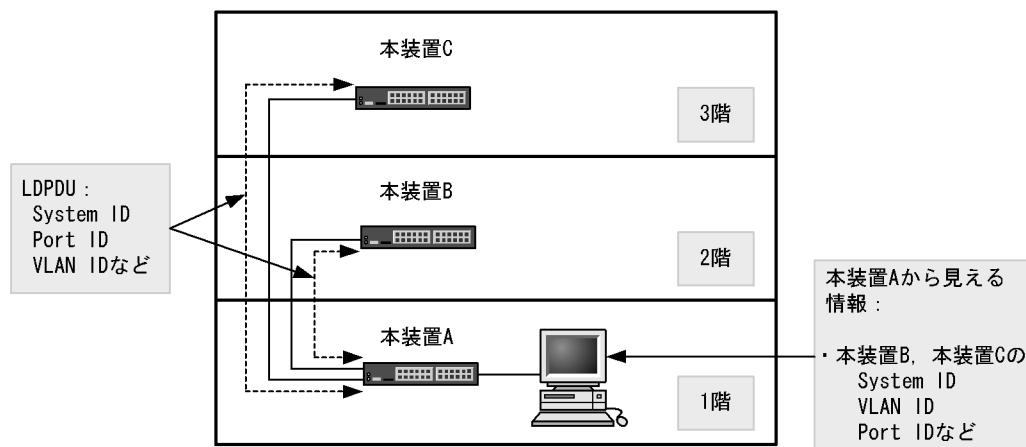
LLDP (Link Layer Discovery Protocol) は隣接する装置情報を収集するプロトコルです。運用・保守時に接続装置の情報を簡単に調査できることを目的とした機能です。

(1) LLDP の適用例

LLDP 機能を使用することで隣接装置と接続している各ポートに対して、自装置に関する情報および該当ポートに関する情報を送信します。該当ポートで受信した隣接装置の情報を管理することで自装置と隣接装置間の接続状態を把握できるようになります。

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本装置間の接続状態を、1 階に設置した本装置 A から把握できるようになります。

図 15-1 LLDP の適用例



15.1.2 サポート仕様

この機能を用いて隣接装置に配布する情報は、IEEE 802.1AB Draft 6 をベースに拡張機能として本装置独自の情報をサポートしています。サポートする情報を次の表に示します。

表 15-1 LLDP でサポートする情報

項目番	名称	説明
1	Time-to-Live	情報の保持時間
2	Chassis ID	装置の識別子
3	Port ID	ポート識別子
4	Port description	ポート種別
5	System name	装置名称
6	System description	装置種別
7	Organizationally-defined TLV extensions	ベンダー・組織が独自に定めた TLV
a	VLAN ID	設定されている VLAN ID
b	VLAN Address	VLAN に関連づけられた IP アドレス

(凡例) - : 該当なし

LLDP でサポートする情報の詳細を以下に示します。

なお、MIB についてはマニュアル「MIB レファレンス」を参照してください。

(1) Time-to-Live (情報の保持時間)

配布する情報を受信装置側で保持する時間を示します。

保持時間はコンフィグレーションで変更できますが、初期状態で使用することをお勧めします。

(2) Chassis ID (装置の識別子)

装置を識別する情報です。この情報には subtype が定義され、 subtype によって送信内容が異なります。 subtype と送信内容を次の表に示します。

表 15-2 Chassis ID の subtype 一覧

subtype	種別	送信内容
1	Chassis component	Entity MIB の entPhysicalAlias と同じ値
2	Chassis interface	interface MIB の ifAlias と同じ値
3	Port	Entity MIB の portEntPhysicalAlias と同じ値
4	Backplane component	Entity MIB の backplaneEntPhysicalAlias と同じ値
5	MAC address	LLDP MIB の macAddress と同じ値
6	Network address	LLDP MIB の networkAddress と同じ値
7	Locally assigned	LLDP MIB の local と同じ値

Chassis ID についての送受信条件は次のとおりです。

- 送信 : subtype = 5 だけ送信します。送信する MAC アドレスは装置 MAC アドレスを使用します。
- 受信 : 上記に示した全 subtype について受信できます。
- 受信データ最大長 : 255byte

(3) Port ID (ポート識別子)

ポートを識別する情報です。この情報には subtype が定義され、 subtype によって送信内容が異なります。 subtype と送信内容を次の表に示します。

表 15-3 Port ID の subtype 一覧

subtype	種別	送信内容
1	Port	Interface MIB の ifAlias と同じ値
2	Port component	Entity MIB の portEntPhysicalAlias と同じ値
3	Backplane component	Entity MIB の backplaneEntPhysicalAlias と同じ値
4	MAC address	LLDP MIB の macAddr と同じ値
5	Network address	LLDP MIB の networkAddr と同じ値
6	Locally assigned	LLDP MIB の local と同じ値

Port IDについての送受信条件は次のとおりです。

- 送信：subtype = 4だけ送信します。送信する MAC アドレスは該当 Port の MAC アドレスを使用します。
- 受信：上記に示した全 subtype について受信できます。
- 受信データ最大長：255Byte

(4) Port description (ポート種別)

ポートの種別を示す情報です。この情報には subtype はありません。

送信内容および受信条件は次のとおりです。

- 送信内容：「Interface MIB の ifDescr と同じ値」
- 受信データ最大長：255Byte

(5) System name (装置名称)

装置名称を示す情報です。この情報には subtype はありません。

送信内容および受信条件は次のとおりです。

- 送信内容：「systemMIB の sysName と同じ値」
- 受信データ最大長：255Byte

(6) System description (装置種別)

装置の種別を示す情報です。この情報には subtype はありません。

送信内容および受信条件は次のとおりです。

- 送信内容：「systemMIB の sysDescr と同じ値」
- 受信データ最大長：255Byte

(7) Organizationally-defined TLV extensions

本装置独自に以下の情報をサポートしています。

(a) VLAN ID

該当ポートが使用する VLAN tag の VLAN ID を示します。tag 変換機能を使用している場合は、変換後の VLAN ID を示します。この情報はトランクポートだけ有効な情報です。

(b) VLAN Address

この情報は、該当ポートにおいて IP アドレスが設定されている VLAN のうち、最も小さい VLAN ID とその IP アドレスを一つ示します。

15.1.3 LLDP 使用時の注意事項

(1) 本機能を設定した装置間に本機能をサポートしない別装置を接続した場合

次に示す構成とした場合、隣接装置との接続状態を正確に把握しにくい状態になります。

- スイッチを経由して接続した場合、スイッチは LLDP の配布情報を中継します。そのため、直接接続していない装置間で、隣接情報として配布情報を受信できるので、直接接続されている装置間の情報と区別が付かなくなります。
- ルータを経由して接続した場合、LLDP の配布情報はルータで廃棄されるため LLDP 機能を設定した装置間では受信できません。

(2) 他社接続について

他社が独自にサポートしている Link Layer Discovery Protocol[※]との相互接続はできません。

注※

Cisco Systems 社 : CDP (Cisco Discovery Protocol)

Extreme Networks 社 : EDP (Extreme Discovery Protocol)

Foundry Networks 社 : FDP (Foundry Discovery Protocol)

(3) IEEE 802.1AB 規格との接続について

本装置の LLDP は IEEE 802.1AB Draft 6 をベースにサポートした独自機能です。IEEE 802.1AB 規格との接続性はありません。

(4) 隣接装置の最大数について

装置当たり最大 50 の隣接装置情報を収容できます。最大数を超えた場合、受信した配布情報は廃棄します。受信済みの隣接装置情報がタイムアウトで削除される時間を確保するために、廃棄状態は一定時間継続されます。時間は、最大収容数の閾値以上になった隣接装置情報の保持時間と同一です。

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

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 15-4 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 run	装置全体で LLDP 機能を有効にします。

15.2.2 LLDP の設定

(1) LLDP 機能の設定

[設定のポイント]

LLDP 機能のコンフィグレーションは装置全体で機能を有効にする設定と、実際に運用するポートで有効にする設定が必要です。

ここでは、gigabitethernet 0/1において LLDP 機能を運用させます。

[コマンドによる設定]

1. **(config)# lldp run**

装置全体で LLDP 機能を有効にします。

2. **(config)# interface gigabitethernet 0/1**

ポート 0/1 のイーサネットインターフェース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 0/1 で LLDP 機能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 フレームの送信間隔を変更すると、装置の情報の変更が反映される時間を調整できます。送信間隔を短くすると変更が早く反映され、送信間隔を長くすると変更の反映が遅くなります。

[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 interval-time 時間の回数で設定します。この場合、60 秒 × 3 で 180 秒になります。

15.3 オペレーション

15.3.1 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 15-5 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。

15.3.2 LLDP 情報の表示

LLDP 情報の表示は、運用コマンド show lldp で行います。show lldp コマンドは、LLDP の設定情報とポートごとの隣接装置数を表示します。show lldp detail コマンドは、隣接装置の詳細な情報を表示します。

図 15-2 show lldp コマンドの実行結果

```
> show lldp
Date 2010/12/01 15:30:00 UTC
Status: Enabled Chassis ID: Type=MAC      Info=0012.e268.2c21
Interval Time: 30   Hold Count: 4   TTL:120
Port Counts=3
0/1 (CH:10) Link:Up    Neighbor Counts: 2
0/2          Link:Down   Neighbor Counts: 0
0/3          Link:Up    Neighbor Counts: 0
>
```

図 15-3 show lldp detail コマンドの実行結果

```
> show lldp detail
Date 2010/12/01 15:30:00 UTC
Status: Enabled Chassis ID: Type= MAC      Info=0012.e268.2c21
Interval Time: 30   Hold Count: 4   TTL:120
System Name: LLDP1
System Description: NEC PF5200 PF5240R-48T4XW-A [PF5240R-48T4XW] Switching
software Ver. S2.0.0.0 [OS-F3PA]
Total Neighbor Counts=2
Port Counts=3
Port 0/1 (CH:10) Link: Up    Neighbor Counts: 2
  Port ID: Type=MAC      Info=0012.e298.5cc0
  Port Description: GigabitEther 0/1
  Tag ID: Tagged=1,10-20,4094
  IPv4 Address: Tagged: 10    192.168.248.240
  IPv6 Address: Tagged: 20    3ffe:501:811:ff01:200:8798:5cc0:e7f4
  1   TTL:110   Chassis ID: Type=MAC      Info=0012.e268.2505
  System Name: LLDP2
  System Description: NEC PF5200 PF5240R-48T4XW-A [PF5240R-48T4XW] Switching
```

15. LLDP

```
software Ver. S2.0.0.0 [OS-F3PA]
  Port ID: Type=MAC      Info=0012.e298.dc20
  Port Description: GigabitEther 0/5
  Tag ID: Tagged=1,10-20,4094
  IPv4 Address: Tagged: 10    192.168.248.220
  2  TTL:100   Chassis ID: Type=MAC      Info=0012.e268.2c2d
  System Name: LLDP3
  System Description: NEC PF5200 PF5240R-48T4XW-A [PF5240R-48T4XW] Switching
software Ver. S2.0.0.0 [OS-F3PA]
  Port ID: Type=MAC      Info=0012.e298.7478
  Port Description: GigabitEther 0/24
  Tag ID: Tagged=1,10-20,4094
  IPv4 Address: Tagged: 10    192.168.248.200
  IPv6 Address: Tagged: 20    3ffe:501:811:ff01:200:8798:7478:e7f4
Port 0/2           Link: Down  Neighbor Counts: 0
Port 0/3           Link: Up    Neighbor Counts: 0
>
```

16 OADP

この章では、本装置に隣接する装置の情報を収集する機能である OADP の解説と操作方法について説明します。

16.1 解説

16.2 コンフィグレーション

16.3 オペレーション

16.1 解説

16.1.1 概要

(1) OADP 機能の概要

OADP (Octpower Auto Discovery Protocol) 機能とは、本装置のレイヤ 2 レベルで動作する機能で、 OADP PDU (Protocol Data Unit) のやりとりによって隣接装置の情報を収集し、隣接装置の接続状況を表示できます。

この機能では、隣接装置の装置情報やポート情報を表示することで隣接装置との接続状況を容易に把握できることから、隣接装置にログインしたりネットワーク構成図を参照したりしなくとも、装置間の接続の状況を確認できます。また、この機能によって表示される接続状況とネットワーク構成図を比較することで、装置間が正しく接続されているかどうかを確認できます。

隣接装置として認識できる装置には、本装置のほかに、CDP を実装した装置、 OADP を実装した装置があります。

(2) CDP 受信機能の概要

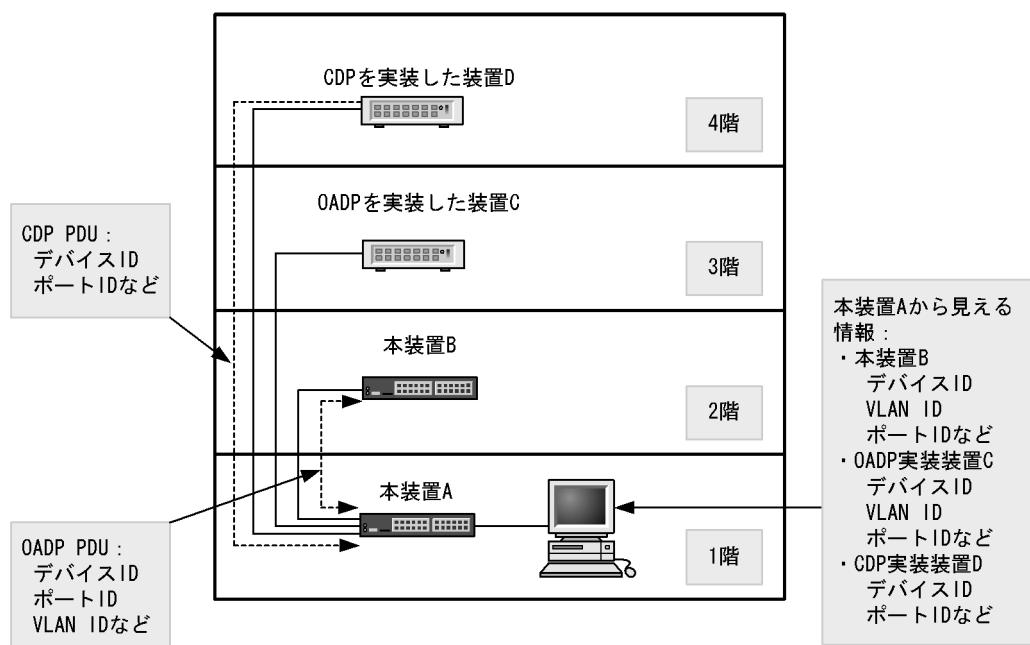
OADP 機能では、CDP (Cisco Discovery Protocol) を解釈できるため、CDP PDU を送信する隣接装置との接続構成も確認できます。ただし、本装置は CDP PDU を送信しません。CDP とは、 Cisco Systems 社製装置のレイヤ 2 レベルで動作する隣接装置検出プロトコルです。

(3) OADP の適用例

OADP 機能を使用することで、隣接装置と接続している各ポートに対して自装置に関する情報および該当ポートに関する情報を送信します。自装置やポートに関する情報としては、デバイス ID、ポート ID、IP アドレス、VLAN ID などがあります。隣接装置から送られてきた情報を該当ポートで受信することで、自装置と隣接装置間の接続状態を把握できるようになります。

OADP 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装置間の接続状態を、1 階に設置した本装置 A から把握することが可能となります。

図 16-1 OADP の適用例



16.1.2 サポート仕様

(1) OADP のサポート仕様

OADP でサポートする項目と仕様を次の表に示します。

表 16-1 OADP でサポートする項目・仕様

項目	内容	
適用レイヤ	レイヤ 2	○
	レイヤ 3	×
OADP PDU 送受信単位	物理ポートまたはリンクアグリゲーション	
リセット機能	○	
OADP PDU 送信間隔	5 ~ 254 秒の範囲で 1 秒単位	
OADP PDU 情報保有時間	10 ~ 255 秒の範囲で 1 秒単位	
CDP 受信機能	○	

(凡例) ○: サポート ×: 未サポート

(2) OADP で使用する情報

OADP PDU で使用する情報を次の表に示します。

表 16-2 OADP でサポートする情報

項番	名称	説明
1	Device ID	装置を一意に識別する識別子
2	Address	OADP PDU を送信するインターフェースに関連するアドレス、およびループバックインターフェースのアドレス

項番	名称	説明
3	Port ID	OADP PDU を送信するポートの識別子
4	Capabilities	装置の機能
5	Version	ソフトウェアバージョン
6	Platform	プラットフォーム
7	Duplex	OADP PDU を送信するポートの Duplex 情報
8	ifIndex	OADP PDU を送信するポートの ifIndex
9	ifSpeed	OADP PDU を送信するポートの ifSpeed
10	VLAN ID	OADP PDU を送信するポートの VLAN ID
11	ifHighSpeed	OADP PDU を送信するポートの ifHighSpeed

受信する CDP PDU で使用される可能性のある情報を次の表に示します。項番 1 ~ 7 は OADP PDU と共通です。

表 16-3 CDP でサポートする情報

項番	名称	説明
1	Device ID	装置を一意に識別する識別子
2	Address	CDP PDU を送信するポートに関連するアドレス
3	Port ID	CDP PDU を送信するポートの識別子
4	Capabilities	装置の機能
5	Version	ソフトウェアバージョン
6	Platform	プラットフォーム
7	Duplex	CDP PDU を送信するポートの Duplex 情報

16.1.3 OADP 使用時の注意事項

(1) この機能を設定した装置間にこの機能をサポートしない別装置を接続した場合

次に示す構成とした場合、隣接装置との接続状態を正確に把握しにくい状態になります。

- スイッチを経由して接続した場合、スイッチは OADP の配布情報を中継します。そのため、直接接続していない装置間で隣接情報として配布情報を受信できるので、直接接続されている装置間の情報と区別が付かなくなります。
- ルータを経由して接続した場合、OADP の配布情報はルータで廃棄されるため OADP 機能を設定した装置間では受信できません。

(2) 隣接装置の最大数について

装置当たり最大 100 の隣接装置情報を収容できます。最大数を超えた場合、受信した配布情報は廃棄されます。受信済みの隣接装置情報がタイムアウトで削除される時間を確保するために廃棄状態は一定時間継続されます。時間は、最大収容数の閾値以上になった隣接装置情報の保持時間と同じです。

(3) OADP を使用するポートの VLAN について

OADP はポートに設定されている VLAN 上で OADP PDU を送受信します。VLAN を無効 (state suspend コマンド) に設定するとその VLAN では OADP は動作しません。

(4) CDP を実装した装置と接続した場合について

トランクポートで CDP を実装した装置と接続した場合は、そのポートのネイティブ VLAN を無効 (state suspend コマンド) にしないでください。無効に設定した場合、CDP PDU は本装置で廃棄されます。

(5) CDP を実装した装置間にあった L2 スイッチと本装置とを交換した場合について

CDP を実装した装置の間にあった（CDP を透過する）L2 スイッチを本装置に置き換えた場合に、本装置で CDP 受信機能を設定 (oadp cdp-listener コマンド) すると、本装置が CDP PDU を受信して透過しなくなるため、CDP を実装した装置同士がお互いを認識できなくなります。CDP 受信機能を設定 (oadp cdp-listener コマンド) しなければ、本装置は CDP PDU を受信しないで透過するので、装置を置き換える前と同様に CDP を実装した装置同士がお互いを認識できます。

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

OADP 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
oadp cdp-listener	CDP 受信機能を有効にします。
oadp enable	ポートおよびリンクアグリゲーションで OADP 機能を有効にします。
oadp hold-time	本装置が送信する OADP 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。
oadp ignore-vlan	指定した VLAN ID から受信する OADP フレームを無視する場合に指定します。
oadp interval-time	本装置が送信する OADP フレームの送信間隔を指定します。
oadp run	装置全体で OADP 機能を有効にします。

16.2.2 OADP の設定

(1) OADP 機能の設定

[設定のポイント]

OADP 機能のコンフィグレーションは装置全体で機能を有効にする設定と、実際に運用するポートで有効にする設定が必要です。

OADP を使用したいポートがリンクアグリゲーションを構成している場合は、ポートチャネルインターフェースに対して設定します。

ここでは、gigabitethernet 0/1において OADP 機能を運用させます。

[コマンドによる設定]

1. **(config)# oadp run**

装置全体で OADP 機能を有効にします。

2. **(config)# interface gigabitethernet 0/1**

ポート 0/1 のイーサネットインターフェースコンフィグレーションモードに移行します。

3. **(config-if)# oadp enable**

ポート 0/1 で OADP 機能の動作を開始します。

[注意事項]

OADP は、設定したポートで有効な VLAN 上で動作します。suspend に設定されている VLAN では OADP は動作しません。

(2) OADP フレームの送信間隔、保持時間の設定

[設定のポイント]

OADP フレームの送信間隔を変更すると、装置の情報の変更が反映される時間を調整できます。送信間隔を短くすると変更が早く反映される一方で、自装置、隣接装置の負荷が高まる場合があります。送信間隔を長くすると負荷は低くなりますが変更の反映が遅くなります。通常、本設定は変更する必要はありません。

[コマンドによる設定]

1. **(config) # oadp interval-time 60**

OADP フレームの送信間隔を 60 秒に設定します。

2. **(config) # oadp hold-time 180**

本装置が送信した情報を隣接装置が保持する時間を 180 秒に設定します。

(3) CDP 受信機能の設定

[設定のポイント]

CDP 受信機能を有効にすると、OADP が動作しているすべてのポートで CDP 受信機能が動作します。

ここでは、gigabitethernet 0/1 において CDP 受信機能を運用させます。

[コマンドによる設定]

1. **(config) # interface gigabitethernet 0/1**

ポート 0/1 のイーサネットインターフェースコンフィグレーションモードに移行します。

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

ポート 0/1 で OADP 機能を有効にします。

3. **(config-if) # exit**

イーサネットインターフェース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モードに戻ります。

4. **(config) # oadp cdp-listener**

CDP 受信機能を有効にします。OADP が動作しているポートで CDP 受信機能が動作します。

(4) OADP フレームを無視する VLAN の設定

[設定のポイント]

OADP は、トランクポートでは VLAN tag を使用して 1 ポートに複数の OADP フレームを送受信します。トランクポートに所属している VLAN 数が増えると隣接装置情報も増加し、装置への負荷が増加します。受信した OADP フレームを無視する VLAN を設定することで装置への負荷を抑えられます。

[コマンドによる設定]

1. **(config) # oadp ignore-vlan 10-20**

VLAN10 ~ 20 で受信した OADP フレームを無視します。

16.3 オペレーション

16.3.1 運用コマンド一覧

OADP 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 oadp	OADP/CDP の設定情報および隣接装置情報を表示します。
show oadp statistics	OADP/CDP 統計情報を表示します。
clear oadp	OADP/CDP の隣接情報をクリアします。
clear oadp statistics	OADP/CDP の統計情報をクリアします。
restart oadp	OADP プログラムを再起動します。
dump protocols oadp	OADP 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。

16.3.2 OADP 情報の表示

OADP 情報の表示は、運用コマンド show oadp で行います。show oadp コマンドは、OADP の設定情報とポートごとの簡易的な情報を示します。show oadp detail コマンドは、隣接装置の詳細な情報を表示します。

図 16-2 show oadp コマンドの実行結果

```
> show oadp
Date 2010/12/01 15:30:00 UTC
OADP/CDP status: Enabled/Disabled   Device ID: OADP-1
Interval Time: 60      Hold Time: 180
ignore vlan: 2-4,10
Enabled Port: 0/1-5,16,20
                           CH 10

Total Neighbor Counts=2
Local      VID Holdtime Remote      VID Device ID      Capability Platform
0/1        0     35 0/8          0  OADP-2        RS          PF5240F-48T4XW
0/16       0      9 0/1          0  OADP-3        S           PF5240R-48T4XW

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater
>
```

図 16-3 show oadp detail コマンドの実行結果

```
> show oadp detail
Date 2010/12/01 15:30:00 UTC
OADP/CDP status: Enabled/Disabled Device ID: OADP-1
Interval Time: 60 Hold Time: 180
ignore vlan: 2-4,10
Enabled Port: 0/1-5,16,20

Total Neighbor Counts=2
-----
Port: 0/1 VLAN ID: 0
Holdtime : 6(sec)
Port ID : 0/8 VLAN ID(TLV): 0
Device ID : OADP-2
Capabilities : Router, Switch
Platform : PF5240F-48T4XW
Entry address(es):
    IP address : 192.16.170.87
    IPv6 address: fe80::200:4cff:fe71:5d1c
IfSpeed : 1G Duplex : FULL
Version : NEC PF5200 PF5240F-48T4XW-A [PF5240F-48T4XW] Switching software
Ver.S2.0.0.0 [OS-F3PA]
-----
Port: 0/16 VLAN ID: 0
Holdtime : 10(sec)
Port ID : 0/1 VLAN ID(TLV): 0
Device ID : OADP-3
Capabilities : Switch
Platform : PF5240R-48T4XW
Entry address(es):
    IP address : 192.16.170.100
IfSpeed : 1G Duplex : FULL
Version : NEC PF5200 PF5240R-48T4XW-A [PF5240R-48T4XW] Switching software
Ver.S2.0.0.0 [OS-F3PA]
-----
>
```


17 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物理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。

17.1 解説

17.2 コンフィグレーション

17.1 解説

17.1.1 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物理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ライザなどで受信することによって、トライフィックの監視や解析を行えます。

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 17-1 受信フレームのミラーリング

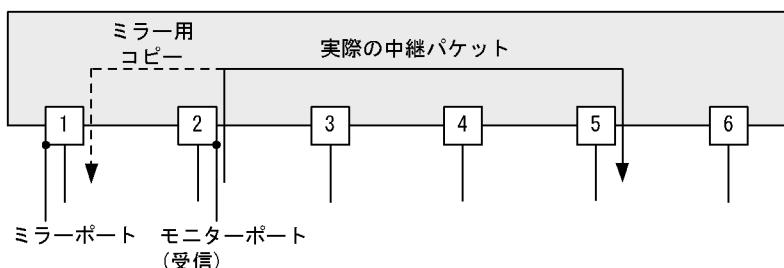
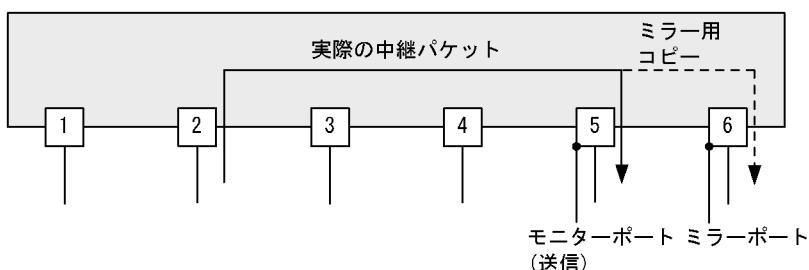


図 17-2 送信フレームのミラーリング



これらの図で示すとおり、トライフィックを監視する物理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物理ポートをミラーポートと呼びます。

ミラーポートからはミラーリングされたフレームだけ送信されます。それ以外の自発、自宛、中継フレームは廃棄されます。ただし、制御フレームが送信される設定をした場合、設定された制御フレームは送信されます。なお、ミラーリングしたフレームは、TTL (IPv4) またはホップリミット (IPv6) を減算しないで送信されます。

また、モニターポートとミラーポートは「多対一」の設定ができる、複数のモニターポートから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できます。ただし、モニターポートでコピーしたフレームを複数のミラーポートへ送信することはできません。

ポートミラーリングに関する運用コマンドはありません。ミラーポートに接続したアライザで、フレームがミラーリングされていることを確認してください。

17.1.2 ポートミラーリングの注意事項

(1) 他機能との共存

- モニターポートでは、ほかの機能は制限なく動作します。
- ミラーポートでは、VLAN 機能およびレイヤ 3 通信機能が使用できません。VLAN 機能を前提とするスパニングツリー、Ring Protocol、IGMP snooping/MLD snoopingなどの機能や、レイヤ 3 通信機能を前提とする SNMP、DHCP などの機能も使用できません。
- ミラーポートに制御フレームが送信される機能を設定すると、コピーされたフレームのほかに設定された制御フレームが送信されます。

(2) ポートミラーリング使用時の注意事項

- ポートミラーリングでコピーしたフレームは、ミラーポートの回線帯域を超えて出力することはできません。
- 受信したフレームの FCS が不正な場合、該当フレームはミラーリングされません。
- モニターポートに対して、フィルタ /QoS 制御やストームコントロールを設定できますが、ポートミラーリング機能には影響しません。
- 送信フレームのミラーリングでは、ハードウェアで中継するフレームだけをミラーリングします。ソフトウェアで送信するフレーム（自発、IP オプション付きパケットなど）はミラーリングしません。受信フレームのミラーリングでは、自宛フレームや IP オプション付きパケットなどを含めた、すべての受信フレームをミラーリングします。
- 送信フレームのミラーリングでは、1 セッションだけ設定できます。
- 送信フレームのミラーリングで複数モニターポートを設定し、そのすべてまたは一部のポートにフレームをフラッディングする場合、ミラーリングするフレームは次のようにになります。
 - 該当するポートが 0/1 ~ 0/24 および 0/49, 0/50 と、0/25 ~ 0/48 および 0/51, 0/52 にわたっている場合、2 個のフレームがミラーリングされます。
 - 上記以外の場合、1 個のフレームがミラーリングされます。
- 送信フレームのミラーリングでは、untagged フレームを送信する場合でも、送信フレームの VLAN の tag を持つ tagged フレームがミラーリングされます。
- 送信フレームのミラーリングでは、送信ポートに tag 変換機能が設定されていても、LAN 上で使用する VLAN tag ではなく、送信フレームの VLAN の tag を持つ tagged フレームがミラーリングされます。

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

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 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
monitor session	ポートミラーリングを設定します。

17.2.2 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。本装置では最大 4 組のモニターセッションを設定できます。

組み合わせごとに 1 から 4 のセッション番号を使用します。設定したモニターセッションを削除する場合は、設定時のセッション番号を指定して削除します。設定済みのセッション番号を指定すると、モニターセッションの設定内容は変更されて、以前のモニターセッションの情報は無効になります。

モニターポートには、通信で使用するポートを指定します。ミラーポートには、トライ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指定します。ミラーポートではポートミラーリング以外の通信はできません。

送信フレームのミラーリングおよび送受信フレームのミラーリングはセッション番号 1 のモニターセッションにだけ設定できます。

(1) 受信フレームのミラーリング

[設定のポイント]

設定できるインターフェースはイーサネットインターフェースです。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ーフェースを指定します。また、ミラーポートは vlan などを設定していないポートに設定します。

[コマンドによる設定]

```
1. (config)# monitor session 2 source interface gigabitethernet 0/1 rx destination
   interface gigabitethernet 0/5
```

アナライザをポート 0/5 に接続し、1G ビットイーサネットインターフェース 0/1 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]

設定できるインターフェースはイーサネットインターフェースです。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ーフェースを指定します。また、ミラーポートは vlan などを設定していないポートに設定します。セッション番号は 1 でなければなりません。

[コマンドによる設定]

```
1. (config)# monitor session 1 source interface gigabitethernet 0/2 tx destination
   interface gigabitethernet 0/6
```

アナライザをポート 0/6 に接続し、1G ビットイーサネットインターフェース 0/2 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]

設定できるインターフェースはイーサネットインターフェースです。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ーフェースを指定します。また、ミラーポートは `vlan`などを設定していないポートに設定します。セッション番号は 1 でなければなりません。

[コマンドによる設定]

```
1. (config)# monitor session 1 source interface gigabitethernet 0/3 both
   destination interface gigabitethernet 0/11
```

アナライザをポート 0/11 に接続し、1G ビットイーサネットインターフェース 0/3 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) 複数モニターポートのミラーリング

[設定のポイント]

複数のモニターポートをリスト形式で設定できます。設定済みのリストにポートを追加することや、削除することもできます。

[コマンドによる設定]

```
1. (config)# monitor session 1 source interface gigabitethernet 0/1-23,
   tengigabitethernet 0/49 both destination interface gigabitethernet 0/24
```

アナライザをポート 0/24 に接続し、1G ビットイーサネットインターフェース 0/1 から 0/23 および 10G ビットイーサネットインターフェース 0/49 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。

付録

付録 A 準拠規格

付録 A 準拠規格

付録 A.1 Diff-serv

表 A-1 Diff-serv の準拠規格および勧告

規格番号(発行年月)	規格名
RFC 2474(1998年12月)	Definition of the Differentiated Services Field(DS Field) in the IPv4 and IPv6 Headers
RFC 2475(1998年12月)	An Architecture for Differentiated Services
RFC 2597(1999年6月)	Assured Forwarding PHB Group
RFC 3246(2002年3月)	An Expedited Forwarding PHB (Per-Hop Behavior)
RFC 3260(2002年4月)	New Terminology and Clarifications for Diffserv

付録 A.2 VRRP

表 A-2 VRRP の準拠規格および勧告

規格番号(発行年月)	規格名
RFC 2787(1999年6月)	Definitions of Managed Objects for the Virtual Router Redundancy Protocol
RFC 3768(2004年4月)	Virtual Router Redundancy Protocol
draft-ietf-vrrp-ipv6-spec-02.txt (2002年3月)	Virtual Router Redundancy Protocol for IPv6
draft-ietf-vrrp-ipv6-spec-07.txt (2004年10月)	Virtual Router Redundancy Protocol for IPv6
draft-ietf-vrrp-unified-mib-04.txt (2005年9月)	Definitions of Managed Objects for the VRRP over IPv4 and IPv6

付録 A.3 IEEE802.3ah/UDLD

表 A-3 IEEE802.3ah/UDLD の準拠規格および勧告

規格番号(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.4 CFM

表 A-4 CFM の準拠規格および勧告

規格番号(発行年月)	規格名
IEEE802.1ag-2007(2007年12月)	Virtual Bridged Local Area Networks Amendment 5: Connectivity Fault Management

付録 A.5 SNMP

表 A-5 SNMP の準拠規格および勧告

規格番号(発行年月)	規格名
RFC 1155(1990年5月)	Structure and Identification of Management Information for TCP/IP-based Internets
RFC 1157(1990年5月)	A Simple Network Management Protocol (SNMP)
RFC 1213(1991年3月)	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC 1354(1992年7月)	IP Forwarding Table MIB
RFC 1493(1993年6月)	Definitions of Managed Objects for Bridges
RFC 1525(1993年9月)	Definitions of Managed Objects for Source Routing Bridges
RFC 1643(1994年7月)	Definitions of Managed Objects for the Ethernet-like Interface Types
RFC 1657(1994年7月)	Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2
RFC 1757(1995年2月)	Remote Network Monitoring Management Information Base
RFC 1850(1995年11月)	OSPF Version2 Management Information Base
RFC 1901(1996年1月)	Introduction to Community-based SNMPv2
RFC 1902(1996年1月)	Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1903(1996年1月)	Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1904(1996年1月)	Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1905(1996年1月)	Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1906(1996年1月)	Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1907(1996年1月)	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1908(1996年1月)	Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework
RFC 2233(1997年11月)	The Interfaces Group MIB using SMIv2
RFC 2452(1998年12月)	IP Version 6 Management Information Base for the Transmission Control Protocol
RFC 2454(1998年12月)	IP Version 6 Management Information Base for the User Datagram Protocol
RFC 2465(1998年12月)	Management Information Base for IP Version 6: Textual Conventions and General Group
RFC 2466(1998年12月)	Management Information Base for IP Version 6: ICMPv6 Group
RFC 2578(1999年4月)	Structure of Management Information Version 2 (SMIv2)
RFC 2579(1999年4月)	Textual Conventions for SMIv2
RFC 2580(1999年4月)	Conformance Statements for SMIv2
RFC 3410(2002年12月)	Introduction and Applicability Statements for Internet Standard Management Framework
RFC 3411(2002年12月)	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks

規格番号(発行年月)	規格名
RFC 3412(2002年12月)	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413(2002年12月)	Simple Network Management Protocol (SNMP) Applications
RFC 3414(2002年12月)	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3415(2002年12月)	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC 3416(2002年12月)	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
RFC 3417(2002年12月)	Transport Mappings for the Simple Network Management Protocol (SNMP)
RFC 3418(2002年12月)	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
RFC 3584(2003年8月)	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
RFC 3621(2003年12月)	Power Ethernet MIB

付録 A.6 SYSLOG

表 A-6 SYSLOG の準拠する規格および勧告

規格番号(発行年月)	規格名
RFC 3164(2001年8月)	The BSD syslog Protocol

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
RFC 3176(2001年9月)	InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks

付録 A.8 LLDP

表 A-8 LLDP の準拠規格および勧告

規格番号(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

索引

A

ADVERTISEMENT パケットの送出 159
ADVERTISEMENT パケットの認証 161
alarm グループ 248

C

CC 212
CCM 212
CDP でサポートする情報 292
CFM 201
CFM で使用するデータベース 220
CFM の運用コマンド一覧 228
CFM のコンフィグレーションコマンド一覧 224
Chassis ID (装置の識別子) 283
Chassis ID の subtype 一覧 283
Continuity Check 212

D

Down MEP 205

E

Emergency モード 99
Emergency リンクダウン 100
event グループ 248

G

GetBulkRequest オペレーション 239
GetNextRequest オペレーション 238
GetRequest オペレーション 237

H

history グループ 248

I

IEEE802.3ah/OAM 機能の運用コマンド一覧 184
IEEE802.3ah/UDLD 179
IEEE802.3ah/UDLD のコンフィグレーションコマンド一覧 182
IPv4/IPv6 SNMP マネージャからの MIB 要求と応答の例 234
IP アドレスによるオペレーション制限 242

L

L2 ループ検知 191
L2 ループ検知の運用コマンド一覧 199
L2 ループ検知のコンフィグレーションコマンド一覧 196
Linktrace 215
LLDP 281
LLDP 使用時の注意事項 285
LLDP でサポートする情報 282
LLDP の運用コマンド一覧 287
LLDP のコンフィグレーションコマンド一覧 286
LLDP の適用例 282
Loopback 214

M

MA 204
MEP 205
MIB オブジェクトの表し方 236
MIB 概説 235
MIB 構造 236
MIB 取得の例 233
MIB を設定できない場合の応答 240
MIP 207

O

OADP 289
OADP 使用時の注意事項 292
OADP でサポートする項目・仕様 291
OADP でサポートする情報 291
OADP の運用コマンド一覧 296
OADP のコンフィグレーションコマンド一覧 294
OpenFlow スイッチインスタンス 78, 81
OpenFlow 統計情報 111
OpenFlow プロトコル Features 通知機能 109
OpenFlow プロトコルコンフィグレーション機能 110
OpenFlow プロトコル制御ポート 105
OpenFlow 機能 73
OpenFlow 機能のオペレーションコマンド一覧 148
OpenFlow 機能のオペレーション 148
OpenFlow 機能の解説 81
OpenFlow 機能の概要 74
OpenFlow 機能のコンフィグレーション 133
OpenFlow機能のコンフィグレーションコマンド一覧 133
OpenFlow 機能の設定と運用 131

Organizationally-defined TLV extensions 284

P

Packet In 103

Packet Out 103

Port description (ポート種別) 284

Port ID (ポート識別子) 283

Port ID の subtype 一覧 283

Programmable Flow Switch の概要 77

Q

QoS 制御共通の運用コマンド一覧 27

QoS 制御共通のコンフィグレーションコマンド一覧
26

QoS 制御構造 22

QoS 制御の概要 21

QoS 制御の各機能ブロックの概要 22

R

RMON MIB 248

S

Secure Channel 92

SetRequest オペレーション 239

sFlow 統計 (フロー統計) 機能 261

sFlow 統計で使用する運用コマンド一覧 277

sFlow 統計で使用するコンフィグレーションコマンド
一覧 271

SNMP/RMON に関する運用コマンド一覧 255

SNMP/RMON に関するコンフィグレーションコマン
ド一覧 250

SNMPv1, SNMPv2C オペレーション 237

SNMPv3 オペレーション 243

SNMPv3 でのオペレーション制限 246

SNMPv3 による MIB アクセス許可の設定 251

SNMP エージェント 232

SNMP エンジン 234

SNMP エンティティ 234

SNMP オペレーションのエラーステータスコード
242

SNMP 概説 232

SNMP マネージャとの接続時の注意事項 249

SNMP を使用したネットワーク管理 231

statistics グループ 248

System description (装置種別) 284

System name (装置名称) 284

T

Time-to-Live (情報の保持時間) 283

Trap 247

U

Up MEP 205

V

Vendor 拡張メッセージ 121

VLAN 設定機能 115

VRRP 157

VRRP における障害検出の仕組み 159

VRRP の運用コマンド一覧 176

VRRP のコンフィグレーションコマンド一覧 169

VRRP のコンフィグレーションの流れ 170

VRRP ポーリング 163

あ

アクション 88

アクセプトモード 162

い

インデックス 236

え

エラーステータスコード 242

お

オペレーション 176

か

仮想 MAC 宛てフレームの受信 158

仮想 MAC アドレスによる ARP 応答および NDP 応
答 159

仮想ルータの MAC アドレスと IP アドレス 158

こ

コミュニティによるオペレーション 242

コミュニティによるオペレーション制限 241

コンフィグレーション [VRRP] 169

さ

サポート仕様 [OpenFlow 機能] 119

サポート仕様 [LLDP] 282

サポート仕様 [OADP] 291

し

- シェーパ 62
 自動切り戻しあとび自動切り戻しの抑止 160
 周期送信機能 118
 受信フレームのミラーリング 300
 障害監視インターフェース 163
 障害監視インターフェースと VRRP ポーリング 162
 障害監視インターフェースと VRRP ポーリングの設定 173

す

- ストームコントロール 187
 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 189

そ

- 送信制御 61
 送信フレームのミラーリング 300

た

- 帯域監視 39

と

- ドメイン 203
 トラップ 247
 トラップ概説 247
 トラップの例 233
 トラップフォーマット 247

ね

- ネットワーク管理 232

は

- 廃棄制御 69

ひ

- 標準 MIB 235

ふ

- フィルタ 1
 フィルタで使用する運用コマンド一覧 19
 フィルタで使用するコンフィグレーションコマンド一覧 14
 フィルタを使用したネットワーク構成例 2
 プライベート MIB 235

- プライマリ VLAN 205
 フロー検出 30
 フロー制御 29
 フローテーブル 79, 82
 フローテーブル制御 98

ほ

- ポートグループ機能 114
 ポートミラーリング 299
 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 302
 本装置のサポート MIB 237

ま

- マーカー 47
 マーカーの位置づけ 47
 マスターの選出方法 160
 マッチ条件 87
 マルチヒット機能 113

み

- ミラーポート 300
 ミラーリング 300

も

- モニターポート 300

ゆ

- ユーザ認証とプライバシー機能 234
 優先度 160
 優先度決定 54

ろ

- ログ出力機能 257
 ログ出力機能に関するコンフィグレーションコマンド一覧 259

