マルチレイヤー・モジュラー・スイッチ

SwitchBlade® 7800S
SwitchBlade® 5400S

SB-7800S・SB-5400S ソフトウェアマニュアル

解説書 Vol.2

Ver. 10.7 対応

613-000108 Rev.J 080731

Allied Telesis

■対象製品

このマニュアルは SB-7800S および SB-5400S を対象に記載しています。また，SB-7800S のソフトウェアおよび SB-5400S のソフトウェアいずれも Ver. 10.7 の機能について記載しています。ソフトウェア機能は，基本ソフトウェア OS-SW および各種オプションライセンスによってサポートする機能について記載します。

■日本国外での使用について

弊社製品を日本国外へ持ち出されるお客様は、下記窓口へご相談ください。

TEL: 0120-860442

月～金（祝・祭日を除く）9:00 ～ 17:30

■商標一覧

■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。

■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：
SB-7804S-AC
SB-7808S-AC
SB-7816S-AC
SB-5402S-AC
SB-5404S-AC

■ご注意

弊社は、予告なく本書の一部または全体を修正、変更することがあります。
弊社は、改良のため製品の仕様を予告なく変更することがあります。

■マニュアルバージョン

2005 年 3 月 Rev.A 初版
2005 年 7 月 Rev.B
2006 年 1 月 Rev.C
2006 年 4 月 Rev.D
2006 年 5 月 Rev.E
2006 年 8 月 Rev.F
2007 年 6 月 Rev.G
2008 年 3 月 Rev.H
2008 年 7 月 Rev.J

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 SB-7800S および SB-5400S モデルを対象に記載しています。また，SB-7800S のソフトウェアおよび SB-5400S のソフトウェア，いずれも Ver. 10.7 の機能について記載しています。ソフトウェア機能は，基本ソフトウェア OS-SW および各種オプションライセンスによってサポートする機能について記載します。
操作を行う前にこのマニュアルをよく読み，書かれている指示や注意を十分に理解してください。また，このマニュアルは必要なときにすぐ参照できるよう使いやすい場所に保管してください。
なお，このマニュアルでは特に断らないかぎり SB-7800S と SB-5400S に共通の機能について記載しますが，どちらかの機種固有の機能については以下のマークで示します。

【SB-7800S】:

SB-7800S でサポートする機能です。SB-5400S はサポートしない機能または該当しない記述です。

【SB-5400S】:

SB-5400S でサポートする機能です。SB-7800S はサポートしない機能または該当しない記述です。

また，このマニュアルでは特に断らないかぎり基本ソフトウェア OS-SW の機能について記載しますが，各種オプションライセンスでサポートする機能を以下のマークで示します。

【OP-BGP】:

SB-7800S と SB-5400S のオプションライセンス OP-BGP でサポートする機能です。

【OP-ISIS】:

SB-7800S と SB-5400S のオプションライセンス OP-ISIS でサポートする機能です。

【OP-MLT】:

SB-7800S と SB-5400S のオプションライセンス OP-MLT でサポートする機能です。

【OP-ADV】:

SB-7800S と SB-5400S のオプションライセンス OP-ADV でサポートする機能です。

【OP-OSPF(SB-5400S)】:

SB-7800S では基本ソフトに含む機能ですが，SB-5400S はオプションライセンス OP-OSPF でサポートする機能です。

■このマニュアルの訂正について

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

■対象読者

SB-7800S または SB-5400S 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

■マニュアルの構成

「SB-7800S・SB-5400S ソフトウェアマニュアル　解説書」は Vol.1 および Vol.2 に分かれています。
「SB-7800S・SB-5400S ソフトウェアマニュアル　解説書 Vol.2」は，次に示す編と付録から構成されています。

第 1 編　QoS

SB-7800S および SB-5400S が行っている QoS 制御，Diff-serv 機能などについて説明しています。

第 2 編　レイヤ 2 認証

OSI 階層モデルの第 2 レイヤで認証を行う IEEE 802.1X について説明しています。

第 3 編　高信頼性機能

高信頼性機能として冗長構成，GSRP，VRRP，CP 輻輳制御および IEEE802.3ah/UDLD について説明しています。

第 4 編　運用

ネットワーク管理，運用機能について説明しています。

第 5 編　システム構築のためのポイント

システム構築時に必要な，他機種および網・各種専用線サービスとの接続について説明しています。

付録 A　準拠規格

準拠している規格について説明しています。

付録 B　謝辞 (Acknowledgments)

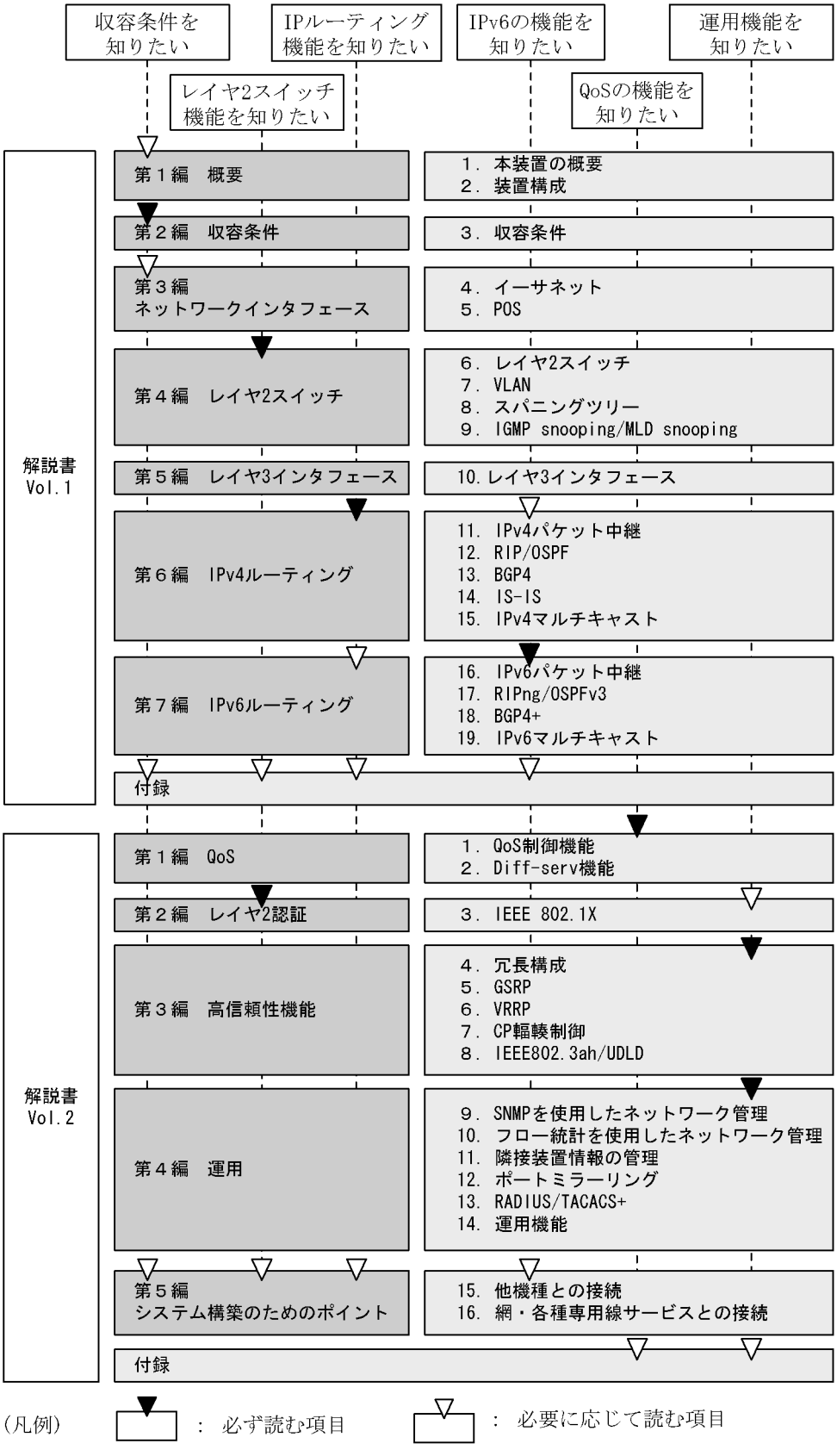
謝辞 (Acknowledgments) を掲載しています。

付録 C　用語解説

このマニュアルで使用している用語の意味を説明しています。

■読書手順

このマニュアルは次の手順でお読みいただくことをお勧めします。


収容条件を
知りたい
IPルーティング
機能を知りたい
IPv6の機能を
知りたい
運用機能を
知りたい
レイヤ2スイッチ
機能を知りたい
QoSの機能を
知りたい
解説書
Vol.1
第１編　概要
１．本装置の概要
２．装置構成
第２編　収容条件
３．収容条件
第３編
ネットワークインタフェース
４．イーサネット
５．POS
第４編　レイヤ2スイッチ
６．レイヤ2スイッチ
７．VLAN
８．スパニングツリー
９．IGMP snooping/MLD snooping
第５編　レイヤ3インタフェース
10.レイヤ3インタフェース
第６編　IPv4ルーティング
11．IPv4パケット中継
12．RIP/OSPF
13．BGP4
14．IS-IS
15．IPv4マルチキャスト
第７編　IPv6ルーティング
16．IPv6パケット中継
17．RIPng/OSPFv3
18．BGP4+
19．IPv6マルチキャスト
付録
解説書
Vol.2
第１編　QoS
１．QoS制御機能
２．Diff-serv機能
第２編　レイヤ2認証
３．IEEE 802.1X
第３編　高信頼性機能
４．冗長構成
５．GSRP
６．VRRP
７．CP輻輳制御
８．IEEE802.3ah/UDLD
第４編　運用
９．SNMPを使用したネットワーク管理
10．フロー統計を使用したネットワーク管理
11．隣接装置情報の管理
12．ポートミラーリング
13．RADIUS/TACACS+
14．運用機能
第５編
システム構築のためのポイント
15．他機種との接続
16．網・各種専用線サービスとの接続
付録
（凡例）
：　必ず読む項目
：　必要に応じて読む項目

■このマニュアルの URL

このマニュアルの内容は下記 URL に掲載しておりますので，あわせてご利用ください。
http://www.allied-telesis.co.jp/

■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。

●ハードウェアの構成，およびソフトウェアの機能を知りたい

解説書 Vol.1 (613-000107)	解説書 Vol.2 (613-000108)

●ハードウェアの設備条件，取扱方法を調べる

SB-7800S ハードウェア取扱説明書 (613-000105)	SB-5400S ハードウェア取扱説明書 (613-000106)

●コンフィグレーションの作成方法，設定例

コンフィグレーションガイド (613-000109)	コンフィグレーション コマンドレファレンス Vol.1 (613-000111)
	コンフィグレーション コマンドレファレンス Vol.2 (613-000112)

●運用管理方法，トラブルシュート →各コマンドの入力シンタックス，パラメータ詳細

運用ガイド (613-000110)	運用コマンドレファレンス Vol.1 (613-000113)
	運用コマンドレファレンス Vol.2 (613-000114)

→運用ログ詳細

メッセージ・ログレファレンス
(613-000115)

→MIB詳細

MIBレファレンス
(613-000116)

■このマニュアルでの表記

ABR	Available Bit Rate
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
ATM	Asynchronous Transfer Mode
AUX	Auxiliary
BCU	Basic management Control module
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol - version 4
BGP4+	Multiprotocol Extensions for Border Gateway Protocol - version 4
bit/s	bits per second *bpsと表記する場合もあります。
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
BSU	Basic packet Switching module
BU	Basic control Unit
CBR	Constant Bit Rate
CDP	Cisco Discovery Protocol
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
CP	multi layer Control Processor
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
Diff-serv	Differentiated Services
DIS	Draft International Standard/Designated Intermediate System
DLCI	Data Link Connection Identifier
DNS	Domain Name System
DR	Designated Router
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EFM	Ethernet in the First Mile
ES	End System
FCS	Frame Check Sequence
FDB	Filtering DataBase
FR	Frame Relay
FTTH	Fiber To The Home
GBIC	GigaBit Interface Converter
GFR	Guaranteed Frame Rate
GSRP	Gigabit Switch Redundancy Protocol
HDLC	High level Data Link Control
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
IIH	IS-IS Hello
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
IS	Intermediate System
IS-IS	Information technology - Telecommunications and Information exchange between systems - Intermediate system to Intermediate system Intra-Domain routeing information exchange protocol for use in conjunction with the Protocol for providing the Connectionless-mode Network Service (ISO 8473)
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Internal Spanning Tree
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
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MIB	Management Information Base
MPLS	Multi-Protocol Label Switching
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
NIF	Network Interface board
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
OSI	Open Systems Interconnection
OSINLCP	OSI Network Layer Control Protocol
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
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
POH	Path Over Head
POS	PPP over SONET/SDH
PPP	Point-to-Point Protocol
PPPoE	PPP over Ethernet
PRI	Primary Rate Interface
PSNP	Partial Sequence Numbers PDU
PSU	Packet Switching Module
PVC	Permanent Virtual Channel (Connection)/Permanent Virtual Circuit
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
REJ	REJect
RFC	Request For Comments

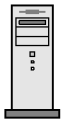
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RM	Routing Manager
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RQ	ReQuest
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SEL	NSAP SELector
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
SOH	Section Over Head
SONET	Synchronous Optical Network
SOP	System Operational Panel
SPF	Shortest Path First
SSAP	Source Service Access Point
STP	Spanning Tree Protocol
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
TLV	Type, Length, and Value
TOS	Type Of Service
TPID	Tag Protocol Identifier
TTL	Time To Live
UBR	Unspecified Bit Rate
UDLD	Uni-Directional Link Detection
UDP	User Datagram Protocol
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
VBR	Variable Bit Rate
VC	Virtual Channel/Virtual Call/Virtual Circuit
VCI	Virtual Channel Identifier
VLAN	Virtual LAN
VP	Virtual Path
VPI	Virtual Path Identifier
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queueing
WRED	Weighted Random Early Detection
WS	Work Station
WWW	World-Wide Web
XFP	10 gigabit small Form factor Pluggable

■図中で使用する記号の説明

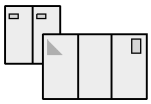
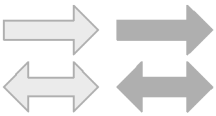
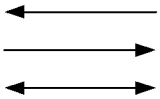
このマニュアルの図中で使用する記号を，次のように定義します。

●ﾜｰｸｽﾃｰｼｮﾝ，端末 ●入出力の動作 ●サーバ ●ファイル

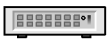
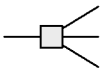




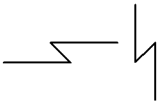

●ホストセンタ ●データの流れ ●その他の流れ ●工程，作業項目の流れ

●SB-7800S・SB-5400S ●一般ルータ ●イーサネット ●ネットワーク


●論理回線 ●通信回線



■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。

- 宛て（あて）
- 宛先（あてさき）
- 迂回（うかい）
- 鍵（かぎ）
- 個所（かしょ）
- 筐体（きょうたい）
- 桁（けた）
- 毎（ごと）
- 閾値（しきいち）
- 芯（しん）
- 溜まる（たまる）
- 必須（ひっす）
- 輻輳（ふくそう）
- 閉塞（へいそく）
- 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 1,024 バイト，1,024 ^{2} バイト，1,024 ^{3} バイト，1,024 ^{4} バイトです。

目次

第 1 編　QoS

目次

目次

解説書 Vol.1

第 1 編　概要

第 2 編　収容条件

第 3 編　ネットワークインタフェース

第 4 編　レイヤ 2 スイッチ

第 7 編　IPv6 ルーティング

1 QoS 制御

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。この章では本装置の QoS 制御機能について説明します。

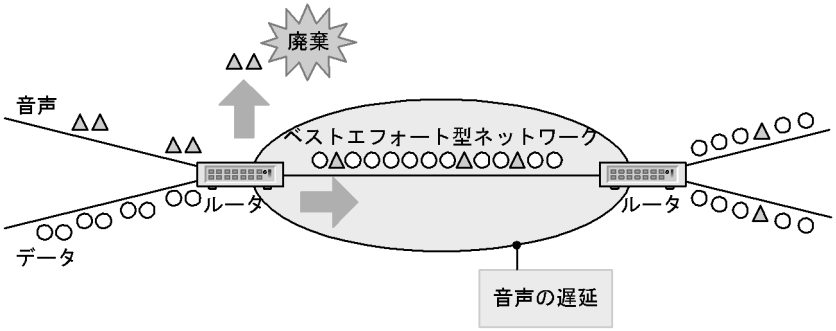
1.1 QoS 制御概説

QoS 制御とは，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する機能です。アプリケーションごとに要求される様々な通信品質を満たすために，QoS 制御を使いネットワーク資源を適切に分配する必要があります。

1.1.1 QoS 制御の必要性

なぜ QoS 制御が必要なのか，まずこの点を考えます。QoS 制御を使用しないベストエフォート型のネットワークの概念を次の図に示します。

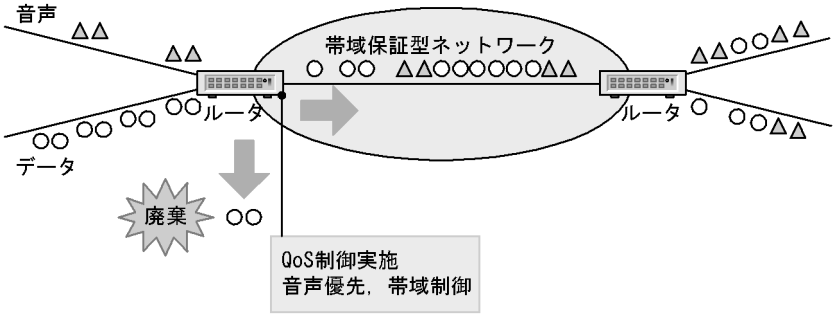
図 1-1 ベストエフォート型ネットワークの概念



ベストエフォート型の場合，ルータはトラフィックを「早い者順」に送信します。「図 1-1 ベストエフォート型ネットワークの概念」のようにデータトラフィックの負荷が高いと，データトラフィックの送信量が多くなるため，音声トラフィックの廃棄や遅延が発生します。

次に帯域保証型ネットワークの概念を次の図に示します。

図 1-2 帯域保証型ネットワークの概念



この図に示した QoS 制御を使用した帯域保証型ネットワークでは，音声トラフィックを優先的に送信したり，帯域制御を使用してデータトラフィックの出力量を制限したりすることができます。この結果，音声トラフィックの遅延を最小限に抑え，また，データトラフィックを帯域に応じて適切に送信できます。

1.1.2 トラフィック種別と通信品質

トラフィック種別に対応する代表的な用途および通信品質を次の表に示します。

表 1-1 トラフィック種別に対応する代表的な用途および通信品質

トラフィック種別	用途	要求品質
音声	IP 電話	低遅延，低揺らぎ（実時間型）
映像	VoD	低遅延，最低帯域監視
データ （帯域保証型）	基幹業務，重要データ	最低帯域監視
データ （ベストエフォート型）	Web アクセス，ファイル転送， バックアップ処理	余剰帯域

1.1.3 QoS 制御のメリット

QoS 制御を使用することで，次に示すメリットがあります。

● **通信品質の向上**

トラフィックの要求品質に応じた QoS 制御を適用することによって，優先トラフィックの通信品質を向上できます。例えば，データトラフィックより遅延に敏感な音声トラフィックを優先的に出力することによって，音声通信の品質を良くすることができます。

● **装置・回線コストの低減**

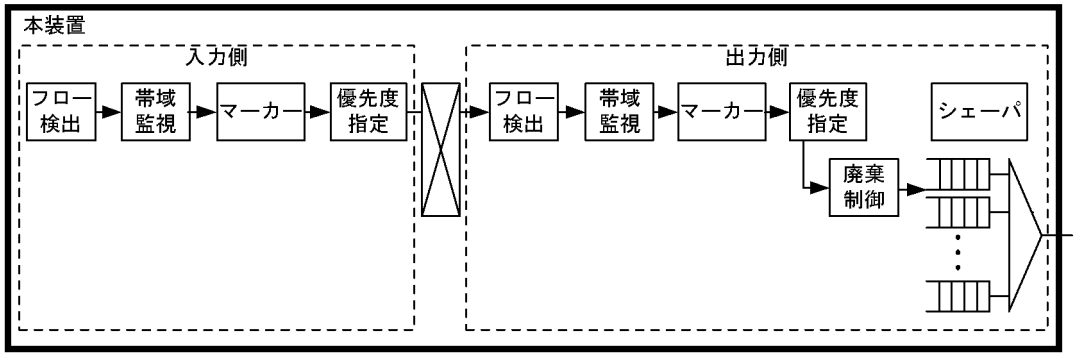
トラフィック量が増大しても，現状の装置・回線を維持したまま，重要なトラフィックの通信品質を向上できます。

今までは通信品質を改善するために，輻輳ポイントで回線を増強する方法を取ってきました。しかし，ネットワークの大規模化が進み，トラフィック量が増え続ける状況を考慮すると，回線増強だけでは限界があります。そこで，回線増強だけなく QoS 制御も併用するという方法が必要になります。

1.2 QoS 制御構造

本装置の QoS 制御の機能ブロックを次の図に示します。

図 1-3 本装置の QoS 制御の機能ブロック



図に示した機能ブロックの概要を次の表に示します。

表 1-2 機能ブロックの概要

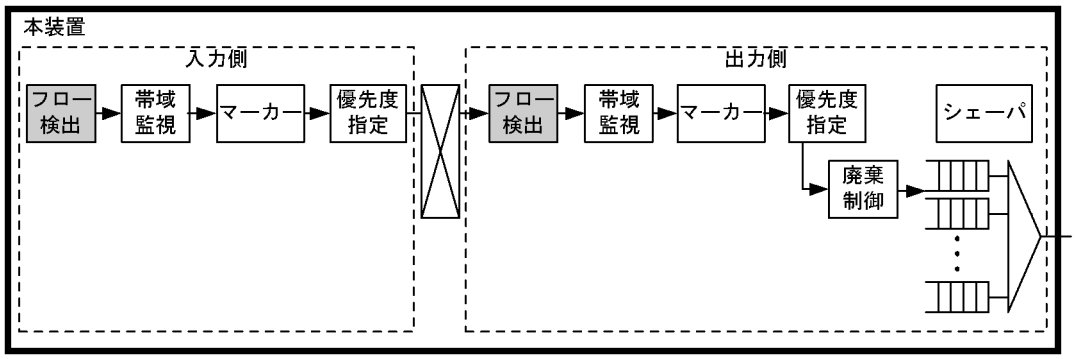
機能ブロック	機能概要
フロー検出	プロトコル種別や IP アドレス，ポート番号などの条件に一致するフローを検出します。
帯域監視	フローごとに帯域を監視して，帯域を超えたフローに対してペナルティを与えます。
マーカー	IP ヘッダ内の DSCP や Tag-VLAN ヘッダのユーザ優先度の値を書き換える機能です。
優先度指定	フローをキューイングするキュー番号や，廃棄されやすさを示すキューイング優先度を指定します。
廃棄制御	パケットの優先度とキューの状態に応じて，該当パケットをキューイングするか廃棄するかを制御します。廃棄制御は出力側だけの機能です。
シェーパ	各キューからのパケットの出力順序および出力帯域を制御します。シェーパは出力側だけの機能です。

機能ブロックの詳細について，次の節から説明します。

1.3 フロー検出

フロー検出は，パケットの一連の流れであるフローを IP ヘッダや TCP ヘッダなどの条件に基づいて検出する機能です。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 1-4 フロー検出の位置づけ



（凡例）：この節で説明する機能ブロック

本装置がサポートするフロー検出条件を次の表に示します。

表 1-3 フローの検出条件

ヘッダ種別	設定項目	レイヤ 2 スイッチ中継パケット			IPv4 中継パケット	IPv6 中継パケット	項目設定
		右記以外	IPv4	IPv6			
MAC	送信元 MAC アドレス	○	○	○	○※1	○※1	MAC アドレスを単一指定，またはマスク指定できます。
	宛先 MAC アドレス	○	○	○	○※1	○※1	MAC アドレスを単一指定，またはマスク指定できます。
	イーサネットタイプ	○ (0x0800, 0x86dd 以外)	○ (0x0800)	○ (0x86dd)	○※1 (0x0800)	○※1 (0x86dd)	IPv4，IPv6，IPX などのプロトコル種別を指定します。
	ユニキャストフラッディングフレーム識別子	○	○	○	○※1	○※1	フラッディングされたフレームのうち，宛先 MAC アドレスがユニキャストアドレスのフレームを検出します。出力側だけ指定できます。
Tag-VLAN	VLAN ID	○	○	○	○※1	○※1	VLAN 番号
	ユーザ優先度	○	○	○	○	○	優先度情報。ソフトウェア中継※2 時入力側で書き換えたユーザ優先度を出力側で検出できません。
IP	IP ユーザデータ長	-	○	○	○	○	IP ユーザデータの上限値または下限値
	上位プロトコル	-	○	○	○	○	TCP，UDP などを示す番号
	送信元 IP アドレス	-	○	○	○	○	アドレスを単一指定，範囲指定，またはサブネット指定できます。※3

ヘッダ種別	設定項目	レイヤ 2 スイッチ中継パケット			IPv4 中継パケット	IPv6 中継パケット	項目設定
		右記以外	IPv4	IPv6			
	宛先 IP アドレス	-	○	○	○	○	アドレスを単一指定，範囲指定，またはサブネット指定できます。※3
	DSCP	-	○	○	○	○	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
	プレシデンス	-	○	○	○	○	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 3 ビット
	フラグメント識別子	-	○	-	○	-	2 番目以降のフラグメントパケットを検出します。
TCP	送信元ポート番号	-	○	○	○	○	送信元ポート番号を単一指定，または範囲指定できます。
	宛先ポート番号	-	○	○	○	○	宛先ポート番号を単一指定，または範囲指定できます。
	ACK フラグ	-	○	○	○	○	ACK フラグが 1 のパケットを検出します。
	SYN フラグ	-	○	○	○	○	SYN フラグが 1 のパケットを検出します。
UDP	送信元ポート番号	-	○	○	○	○	送信元ポート番号を単一指定，または範囲指定できます。
	宛先ポート番号	-	○	○	○	○	宛先ポート番号を単一指定，または範囲指定できます。
ICMP	ICMP タイプ	-	○	-	○	-	Echo Request/Echo Reply/ Destination Unreachable などを示す番号
	ICMP コード	-	○	-	○	-	Net Unreachable などの ICMP タイプに対する詳細コードを示す番号
ICMPv6	ICMPv6 タイプ	-	-	○	-	○	Echo Request/Echo Reply/ Destination Unreachable などを示す番号
	ICMPv6 コード	-	-	○	-	○	不明な IPv6 オプションなどの ICMPv6 タイプに対する詳細コードを示す番号
IGMP	IGMP タイプ	-	○	-	○	-	Membership Query などを示す番号

（凡例） ○：該当する　-：該当しない

注※ 1

出力側のインタフェースで，送信元 MAC アドレス，宛先 MAC アドレス，イーサネットタイプ，および VLAN ID で IPv4，IPv6 中継パケットを検出することはできません。

注※ 2

ARP 未解決，NDP 未解決，IP オプション付き，MTU オーバ検出のパケットです。

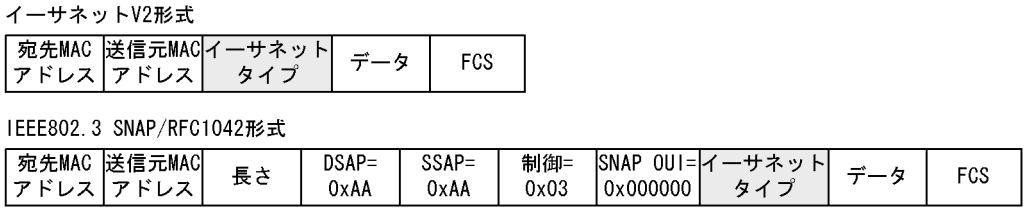
注※ 3

コンフィグレーションコマンド flow qos の pd_prefix 指定時は，IPv6 DHCP サーバ機能によって，指定したインタフェースで配布するプレフィックスアドレスでのフロー検出ができます。なお，プレフィックスの配布・未配布

とは連携しないで，コンフィグレーションに設定したプレフィックスアドレスを該当フローリスト情報に自動設定します。

本装置は，イーサネットタイプとしてイーサネット V2 形式と，IEEE802.3 の SNAP/RFC1042 形式のイーサネットフレームのイーサネットタイプを検出できます。イーサネットタイプの位置を次の図に示します。

図 1-5　イーサネットタイプの位置



ユニキャストフラッディングフレーム識別子 (unicast_flood) は，本装置がフラッディングしたフレームのうち，宛先 MAC アドレスがユニキャストアドレスのフレームを検出するための条件です。フラッディングとは，フレームを受信した物理ポートを除く同一 VLAN 内の全ポートへ，フレームを転送する動作です。このフラッディングが頻繁に発生すると，フラッディングフレームが回線帯域を消費するため，通常通信の帯域が圧迫されるという問題が出てきます。そこでフロー検出機能と帯域監視機能を連携させて，検出したフラッディングフレームの出力量を制限することで，この問題を回避できます。

1.3.1　フロー検出機能の運用について

フロー検出機能では，フロー検出条件モードおよびフロー検出条件オプションで運用方法を選択できます。

(1) フロー検出条件モード

フロー検出条件モードでは，次の表に示す二つの運用方法を選択できます。なお，選択した運用方法はフィルタリング機能も同じ運用方法となります。

表 1-4　フロー検出条件モードで選択できる運用方法

項番	運用方法	フロー動作	フロー検出条件モードの指定方法
1	きめ細かいフロー検出条件を指定する	MAC，IP ヘッダなどを検出条件としてパケット検出が可能。	フロー検出条件モードの指定なし
2	パケット中継性能を劣化させない	<Portlist> 指定では，L2 スイッチ中継を対象とし，<Interface Name> 指定では，IPv4，IPv6 中継パケットを対象としたパケット検出が可能。	フロー検出条件モード 1 (retrieval_mode_1) を指定

次の表にフロー検出条件モードと対応可能 PSU，BSU の関係を示します。

表 1-5 フロー検出条件モードと対応可能 PSU，BSU の関係

フロー検出条件モード	SB-7800S で対応可能な PSU	SB-5400S で対応可能な BSU
指定なし	PSU-1 PSU-12 PSU-2 PSU-22 PSU-33 PSU-43	BSU-C1 BSU-C2 BSU-S1 BSU-S2
フロー検出条件モード 1	PSU-12 PSU-22 PSU-33 PSU-43	BSU-C1 BSU-C2 BSU-S1 BSU-S2

(a) フロー検出条件モード 1

パケット中継性能を劣化させることなく，フロー検出機能を運用したい場合には，コンフィグレーションコマンド flow で，フロー検出条件モード 1 を指定します。

フロー検出条件モード 1 を使用する場合は，対象 PSU に「表 1-5 フロー検出条件モードと対応可能 PSU，BSU の関係」で示す PSU を実装してください。フロー検出条件モード 1 をサポートしていない PSU に対してフロー検出条件モード 1 を設定した場合，フローフィルタ機能，フロー QoS 機能のコンフィグレーションは編集・表示できますが，該当 PSU におけるフローフィルタ機能，フロー QoS 機能は動作しません。

フロー検出条件モード 1 指定時，設定した入出力インタフェースごと (<Portlist> 指定，または <Interface Name> 指定) に指定可能なフロー検出条件を「表 1-6 フロー検出条件モード 1 時のフロー検出条件」に示します。

なお，フィルタリング機能もフロー検出条件モード 1 で動作します。フロー検出条件モード 1 指定時，フィルタリング機能で指定可能なフロー検出条件と動作指定は，「解説書 Vol.1 11.6.3 フィルタリングの運用について」，「解説書 Vol.1 16.6.3 フィルタリングの運用について」を参照してください。

表 1-6 フロー検出条件モード 1 時のフロー検出条件

ヘッダ種別	設定項目	<Portlist> 指定		<Interface Name> 指定	
		L2 スイッチ中継パケット		IPv4 中継パケット	IPv6 中継パケット
		右記以外	IPv4，IPv6		
MAC	送信元 MAC アドレス	○	○	-	-
	宛先 MAC アドレス	○	○	-	-
	イーサネットタイプ	○	○	-	-
	フラッディングフレーム識別子	○※	○※	-	-
Tag-VLAN	VLAN ID	○	○	-	-
	ユーザ優先度	○	○	○	○
IP	IP ユーザデータ長	-	-	○	○
	上位プロトコル	-	-	○	○
	送信元 IP アドレス	-	-	○	○
	宛先 IP アドレス	-	-	○	○

ヘッダ種別	設定項目	<Portlist> 指定		<Interface Name> 指定	
		L2 スイッチ中継パケット		IPv4 中継パケット	IPv6 中継パケット
		右記以外	IPv4，IPv6		
	DSCP	-	○	○	○
	プレシデンス	-	○	○	○
	フラグメント識別子	-	-	○	-
TCP	送信元ポート番号	-	-	○	○
	宛先ポート番号	-	-	○	○
	ACK フラグ	-	-	○	○
	SYN フラグ	-	-	○	○
	セッション維持	-	-	○	○
UDP	送信元ポート番号	-	-	○	○
	宛先ポート番号	-	-	○	○
ICMP	ICMP タイプ	-	-	○	-
	ICMP コード	-	-	○	-
ICMPv6	ICMPv6 タイプ	-	-	-	○
	IGMPv6 コード	-	-	-	○
IGMP	IGMP タイプ	-	-	○	-

(凡例) ○：指定可 -：指定不可
注※ 出力側だけ指定可能です。

次にフロー検出条件モード 1 を使用した場合の <Portlist> 指定，<Interface Name> 指定ごとの検出可能なパケットを示します。

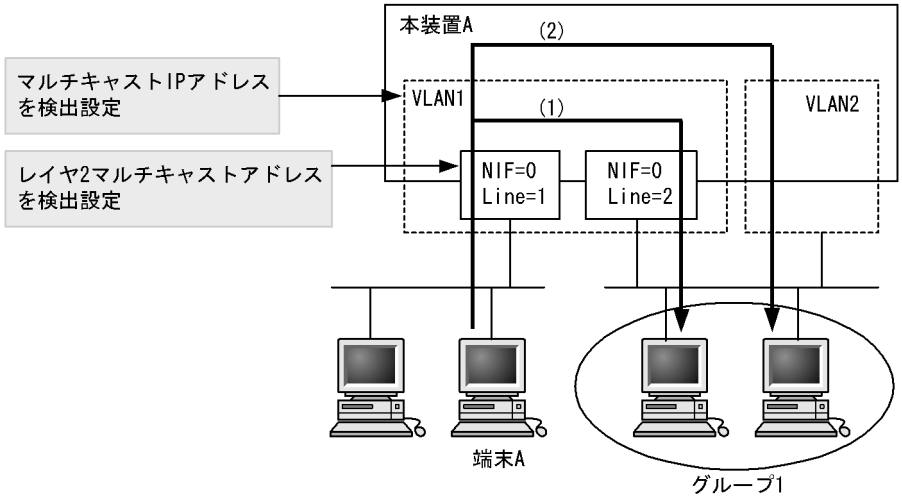
表 1-7 検出可能パケット種別一覧

フロー指定方法	パケット種別
<Portlist> 指定	レイヤ 2 スイッチ中継パケット※ IPv4，IPv6 中継パケット※
<Interface Name> 指定	IPv4，IPv6 中継パケット※

注※

- 帯域監視機能を使用した場合，<Portlist> 指定時は，レイヤ 2 スイッチ中継パケットだけを対象とし，<Interface Name> 指定時は，IPv4，IPv6 中継パケットだけを対象とします。
- 宛先 MAC アドレスがレイヤ 2 マルチキャストアドレス，かつ宛先 IP アドレスがマルチキャスト IP アドレスのパケットは，本装置でレイヤ 2 スイッチ中継および IPv4，IPv6 中継の両方を実施します (次に示す図の (1)，(2))。したがって，(1) のレイヤ 2 スイッチ中継パケットをフロー検出する場合は，<Portlist> 指定で宛先 MAC アドレス検出条件にレイヤ 2 マルチキャストアドレスを指定して，(2) の IPv4，IPv6 中継パケットをフロー検出する場合は <Interface Name> 指定で，宛先 IP アドレス検出条件にマルチキャスト IP アドレスを指定してください。

図 1-6 マルチキャストパケット中継例



(2) フロー検出条件オプション

フロー検出条件オプションでは，次の表に示す二つの運用方法を選択できます。なお，選択した運用方法はフィルタリング機能も同じ運用方法となります。

表 1-8 フロー検出条件オプションで選択できる運用方法

項番	運用方法	フロー動作	フロー検出条件オプションの指定方法
1	中継パケットでフロー検出する	中継パケットでだけフロー検出可能	フロー検出条件オプションの指定なし
2	中継パケットおよび本装置宛パケット※でフロー検出したい	中継パケットおよび本装置宛パケット※でフロー検出可能	フロー検出条件オプション 1 (retrieval_option_1) を指定

注※

フロー検出条件オプション 1 指定時にフロー検出対象に加わる本装置宛パケットは以下に該当するパケットです。したがって，フロー検出条件オプション 1 を指定しない場合，以下に該当する本装置宛パケットはフロー検出対象外です。

- 宛先 MAC アドレスがブロードキャストアドレスであるパケット
- 宛先 MAC アドレスがマルチキャスト MAC アドレスまたは自 MAC アドレスである非 IP パケット
- 送信元 IP アドレスまたは宛先 IP アドレスがリンクローカルアドレスであるパケット

次の表にフロー検出条件モードと対応可能 PSU，BSU の関係を示します。

表 1-9 フロー検出条件オプションと対応可能 PSU，BSU の関係

フロー検出条件オプション	SB-7800S で対応可能な PSU	SB-5400S で対応可能な BSU
指定なし	PSU-1 PSU-12 PSU-2 PSU-22 PSU-33 PSU-43	BSU-C1 BSU-C2 BSU-S1 BSU-S2
フロー検出条件オプション 1	PSU-12 PSU-22 PSU-33 PSU-43	BSU-C1 BSU-C2 BSU-S1 BSU-S2

(a) フロー検出条件オプション 1

本装置宛パケット（「表 1-8　フロー検出条件オプションで選択できる運用方法」の注参照）でもフロー検出機能を運用したい場合には，コンフィグレーションコマンド flow で，フロー検出条件オプション 1 を指定します。フロー検出条件オプション 1 を使用する場合は，対象 PSU，対象 BSU に「表 1-9　フロー検出条件オプションと対応可能 PSU，BSU の関係」で示す対応可能 PSU，BSU を実装してください。なお，フィルタリング機能もフロー検出条件オプション 1 で動作します。また，フロー検出条件オプション 1 の指定は，フロー検出条件モードと同時に設定することができます。

注

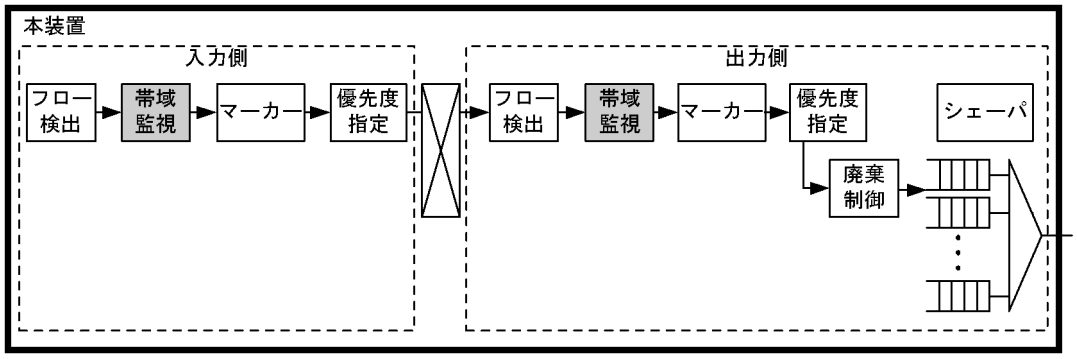
EAPOL，LACP，BPDU，CDP，OADP，LLDP，GSRP のパケットをフロー検出するコンフィグレーション flow qos の設定は，次のインタフェースまたは物理ポートに指定してください。

- Tag-VLAN 連携回線の untagged の論理インタフェース
- VLAN 回線の untagged ポートが属する VLAN インタフェース

1.4 帯域監視機能 (UPC 機能)

帯域監視機能 (UPC 機能) は，フロー検出機能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 1-7 帯域監視機能の位置づけ



（凡例）：この節で説明する機能ブロック

この機能は，フロー検出機能が検出したフローの帯域をパケット長 (次の表を参照してください) を用いて監視し，あらかじめ設定した監視帯域以上のパケットにペナルティを科す機能です。

表 1-10 回線種別ごとでの帯域監視の対象とするパケット長

回線種別	帯域監視の対象とするパケット長
イーサネット	MAC アドレスから FCS まで
POS【SB-7800S】	PPP ヘッダから FCS まで

監視帯域内として中継するパケットを「遵守パケット」，監視帯域以上としてペナルティを科すパケットを「違反パケット」といいます。

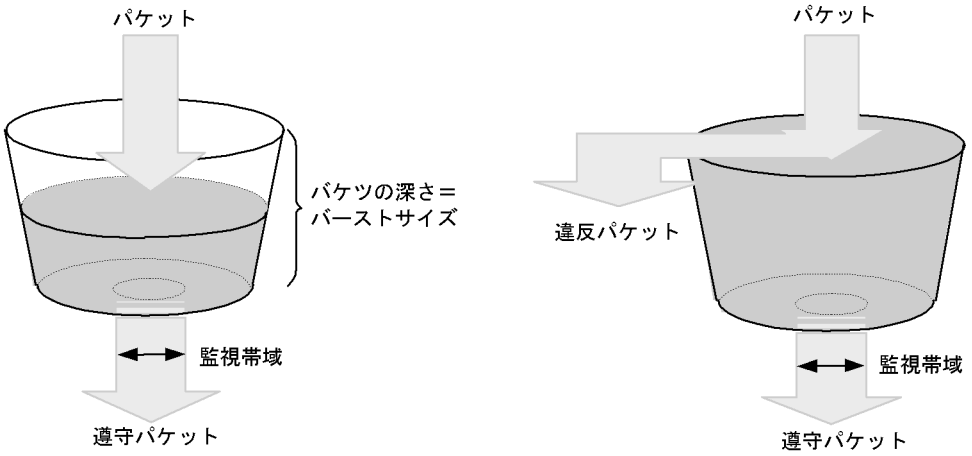
違反パケットに科されるペナルティは，最大帯域制御を用いた場合には，パケットを廃棄します。最低帯域監視を用いた場合には，キューイング優先度の変更，パケットのユーザ優先度の変更，またはパケットの DSCP 値の変更をして，次に説明するマーカーへ指示を出します。

帯域監視機能は，設定される監視帯域値とバーストサイズに基づいて，各フローの帯域監視を行います。監視帯域値とは，そのフローの中継を許可する，一定時間の平均帯域です。バーストサイズとは，監視トラフィックの一時的な揺らぎを許容するための値で，平均帯域を超過して遵守パケットと判定される最大バイト数です。

フロー検出で検出したパケットが監視帯域を遵守しているか違反しているかの判定には，次の図に示すように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。

バケツからは監視帯域分の水が漏れ，パケット送受信時にはパケット長分の水が注ぎ込まれます。例えば，最大帯域制御の場合，バケツからは，指定した監視帯域分の水が漏れ，パケット送受信時にはパケット長の水が注ぎ込まれます（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と，受信パケットを廃棄する違反パケットのペナルティを科します（図の右側の例）。あふれていない場合には中継します。水が一時的に多量に注ぎ込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。

図 1-8 Leaky Bucket アルゴリズムのモデル



バーストサイズのデフォルトは 3000 バイトですが，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，回線の MTU 長以上のバイト数で使用してください。

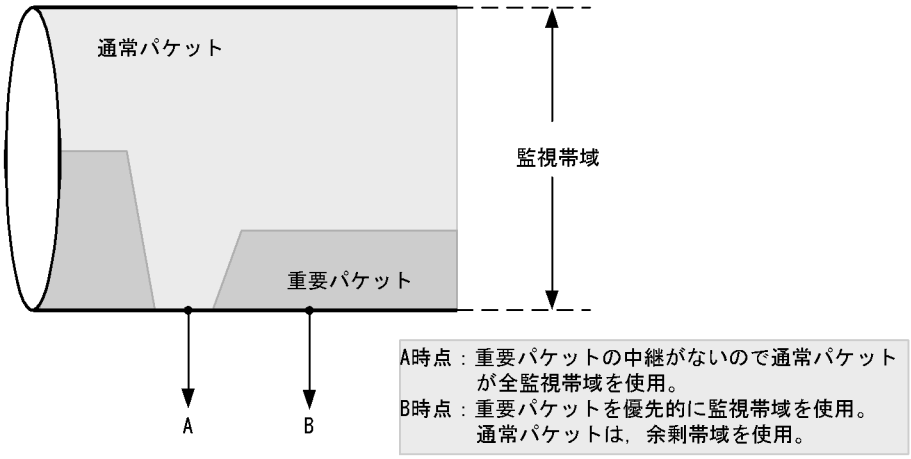
1.4.1 重要パケット保護機能

監視帯域内で，重要なパケットは優先的に監視帯域内パケットとして転送し，通常のパケットは重要なパケットが全監視帯域を使用して転送していない場合に監視帯域内パケットとして転送する機能です。

なお，SB-5400S の BSU-C1，BSU-S1 では使用できません。

重要パケット保護機能使用時の帯域使用状態を次の図に示します。

図 1-9 重要パケット保護機能使用時の帯域使用状態

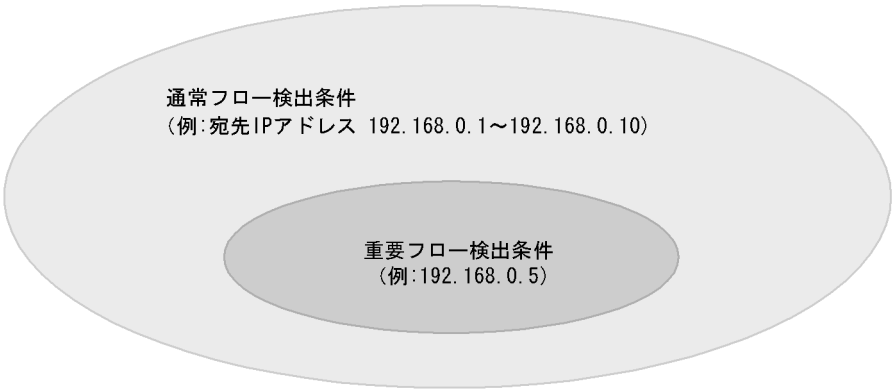


この機能は，帯域監視機能と併用して使用します。

重要パケットの指定方法は，フロー検出条件で，通常フロー検出条件の中の特に重要なパケットの検出条件を重要フロー検出条件に指定してください。

ただし，MAC 未学習のユニキャストフラッディングフレーム，VLAN 番号，フラグメント識別子は，重要フロー検出条件に指定できません。フロー検出条件指定概念図を次に示します。

図 1-10 フロー検出条件指定概念図



通常フロー検出条件に指定したパラメータは，重要フロー検出条件に同じパラメータの指定がない場合，重要フロー検出条件でも有効となります。

ただし，次の表に示す通常フロー検出条件を指定した場合は，重要フロー検出条件のパラメータ指定内容によって，重要フロー検出条件では無効（重要フロー検出条件としてパケット検出しない）となる場合があります。

表 1-11 重要フロー検出条件の設定内容

通常フロー検出条件指定パラメータ	重要フロー検出条件指定パラメータ	重要フロー検出条件のフロー検出条件内容
vlan untagged	ユーザ優先度 (user_priority)	vlan untagged は重要フロー検出条件では無効となります。重要フロー検出条件は，ユーザ優先度が有効となります。
フラグメント識別子 (fragments)	4 層 (TCP，UDP，ICMP，IGMP) の検出条件	フラグメント識別子は重要フロー検出条件では無効となります。重要フロー検出条件は，4 層の検出条件が有効となります。
DSCP	プレシデンス	DSCP は重要フロー検出条件では無効となります。重要フロー検出条件は，プレシデンスが有効となります。
プレシデンス	DSCP	プレシデンスは重要フロー検出条件では無効となります。重要フロー検出条件は，DSCP が有効となります。
IP ユーザデータ長上限値 (upper)	IP ユーザデータ長下限値 (lower)	IP ユーザデータ長上限値は重要フロー検出条件では無効となります。重要フロー検出条件は，IP ユーザデータ長下限値が有効となります。
IP ユーザデータ長下限値 (lower)	IP ユーザデータ長上限値 (upper)	IP ユーザデータ長下限値は重要フロー検出条件では無効となります。重要フロー検出条件は，IP ユーザデータ長上限値が有効となります。
TCP ヘッダの ACK フラグ (ack)	TCP ヘッダの SYN フラグ (syn)	ACK フラグ検出は重要フロー検出条件では無効となります。重要フロー検出条件は，SYN フラグ検出が有効となります。
TCP ヘッダの SYN フラグ (syn)	TCP ヘッダの ACK フラグ (ack)	SYN フラグ検出は重要フロー検出条件では無効となります。重要フロー検出条件は，ACK フラグ検出が有効となります。

1.4.2 UPC-RED

(1) 概要

UPC-RED 機能は，帯域監視機能を使用している応答・要求型プロトコル (例えば，TCP) の通信で，平均帯域を改善する機能です。ただし，プロトコルの特性によって，指定した監視帯域まで使用できない場合があります。

TCP プロトコルは，パケットが廃棄されると，ネットワーク内で輻輳が発生したと判断し，帯域を小さくします。これをスロースタートといいます。フロー内の多くの TCP コネクションが同時にスロースタートを開始すると，ネットワーク上のトラフィックが一気に少なくなります。

帯域監視を行っているフロー上で，この現象が発生すると，平均帯域が指定した監視帯域まで出力されず，本来得られるべきスループットがでません。

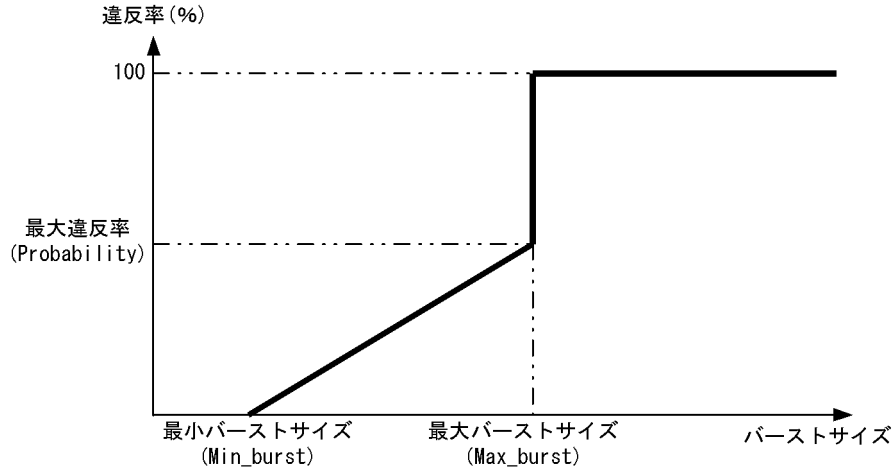
この問題は，UPC-RED 機能を使用することによって，改善されます。UPC-RED 機能は，TCP プロトコルが極端に帯域を小さくしてしまう状態になる前に，受信パケットの中からランダムにパケットを廃棄することによって，少し帯域を小さくさせる機能です。結果として平均帯域が小さくなることはなくなり，スループットが出なくなるという問題を改善します。

UPC-RED 機能は，最小バーストサイズ，最大バーストサイズ，廃棄率を用いて動作します。廃棄率とは，違反パケットと判定する確率です。バーストサイズと違反率の関係を次の図に示します。

この図を用いて，最大帯域制御を行っているフロー上で，UPC-RED 機能を使用した例で説明します。
UPC-RED 機能は，次の 1，2，3 の制御を行います。

1. 最小バーストサイズを超えるまでの間は，「遵守パケット」と判定し，中継します。
2. 最小バーストサイズを超え始めたとき (図中の最小バーストサイズ) から，受信パケットの中から違反率に基づき，幾つかのパケットを選び，「違反パケット」と判定し，廃棄します。
3. 最大バーストサイズを超えると (図中の最大バーストサイズ) すべての受信パケットを「違反パケット」と判定し，すべての受信パケットを廃棄します。

図 1-11　バーストサイズと違反率の関係



なお，UPC-RED 機能と最低帯域監視 (コンフィグレーションコマンド flow qos の min_rate) との組み合わせでは，最低帯域監視はパケットの廃棄を行わないため，UPC-RED 機能が有効に働きません。
UPC-RED 機能は最大帯域制御 (コンフィグレーションコマンド flow qos の max_rate) との組み合わせで使用してください。

（2） 使用方法

UPC-RED 機能は，設定される最小バーストサイズ，最大バーストサイズ，最大違反率の値に基づいて動作します。各設定値の最適な値は，監視帯域とラウンド・トリップ・タイム (RTT) に大きく依存します。

監視帯域，RTT ごとの設定推奨値を次の表に示します。この設定推奨値を基に，最小バーストサイズ，最大バーストサイズ，最大違反率を設定してください。

また，指定した監視帯域から，RTT を 50msec と仮定し，適切な最小バーストサイズ，最大バーストサイズ，最大違反率を自動で設定する機能も備えています。

なお，UPC-RED 機能使用時に平均帯域が監視帯域を大きく下回る場合，最小バーストサイズと最大バーストサイズを大きくし，最大違反率を小さくするように設定すると，平均帯域が改善される場合があります。

注

表で，Mbyte，kbyte 単位で示す値は，小数点以下第一位を切り上げた値です。

表 1-12　最大違反率，最大 / 最小バーストサイズの推奨値

監視帯域 (bps)	RTT(msec)							
	10		20		50		100	
	最大違反率 (%)	バーストサイズ (byte)	最大違反率 (%)	バーストサイズ (byte)	最大違反率 (%)	バーストサイズ (byte)	最大違反率 (%)	バーストサイズ (byte)
128k	100	4500 1500	100	7500 3000	100	18k 4500	100	36k 11k
256k	100	7500 3000	100	15k 4500	100	36k 11k	100	71k 21k
512k	100	15k 4500	100	28k 7500	100	72k 21k	100	147k 46k
1M	100	28k 7500	100	55k 17k	100	143k 44k	83.5	307k 112k
2M	100	55k 17k	100	113k 34k	83.5	307k 112k	34.5	704k 313k
5M	100	143k 44k	83.5	307k 112k	26.5	935k 447k	12	2434k 1457k
10M	83.5	307k 112k	34.5	704k 313k	12	2434k 1457k	6	7127k 5173k
20M	34.5	704k 313k	15.5	1766k 985k	6	7127k 5173k	3	23M 19M
50M	12	2434k 1457k	6	7127k 5173k	2.5	34M 30M	1	124M 114M
100M	8.5	3441k 2060k	4	10M 7316k	1.5	49M 42M	1	175M 161M
200M	6	4865k 2913k	3	14M 11M	1	68M 59M	0.5	247M 228M
500M	4	7692k 4605k	2	23M 16M	0.5	108M 93M	0.5	256M 237M
1G	2.5	11M 6512k	1.5	32M 23M	0.5	152M 131M	0.5	256M 237M
2G	2	16M 9209k	1	45M 32M	0.5	215M 185M	0.5	256M 237M

監視帯域 (bps)	RTT(msec)							
	10		20		50		100	
	最大違反率 (%)	バーストサイズ (byte)	最大違反率 (%)	バーストサイズ (byte)	最大違反率 (%)	バーストサイズ (byte)	最大違反率 (%)	バーストサイズ (byte)
5G	1	24M 15M	0.5	72M 51M	0.5	256M 221M	0.5	256M 237M
10G	1	34M 21M	0.5	99M 72M	0.5	256M 221M	0.5	256M 237M

注　バーストサイズの上段は最大バーストサイズ，下段は最小バーストサイズを示します。

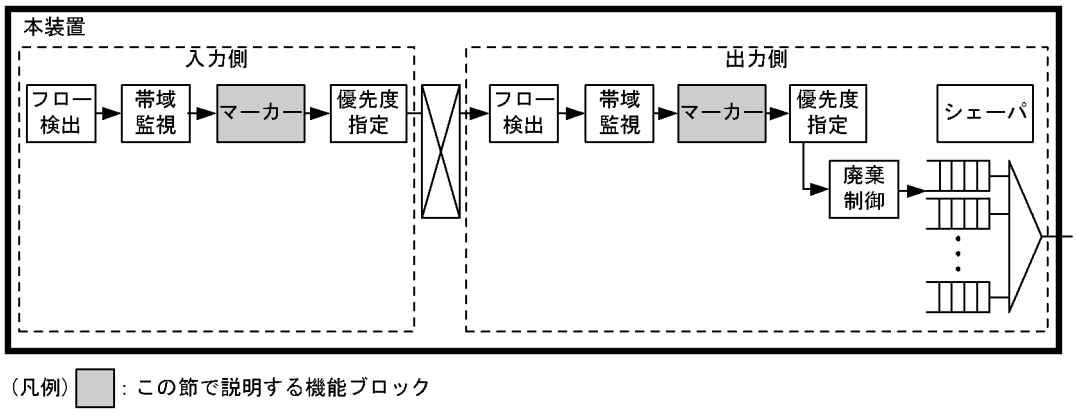
（3） 注意事項

- PSU-1，または PSU-2 は UPC-RED 機能をサポートしていません。

1.5 マーカー

マーカーは，Tag-VLAN ヘッダ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 1-12 マーカーの位置づけ



（凡例）：この節で説明する機能ブロック

（1） DSCP 書き換え

検出したフローの TOS フィールド（IPv4 ヘッダ）またはトラフィッククラスフィールド（IPv6 ヘッダ）の上位 6 ビットを書き換えます。ユニキャスト，およびマルチキャストパケットに対して，入力側と出力側で DSCP 値の書き換えができます。

この機能を利用することによって，検出したフローのユーザ優先度を DSCP 値に対応づけることができます。例えば，ユーザ優先度が 7 のフローに対して DSCP を 63 に設定できます。

また，帯域監視機能ブロックからの指示によって，最低帯域を超えたフローの DSCP を書き換えることができます。例えば最低帯域を超えたフローに対して，DSCP を 0 に設定できます。

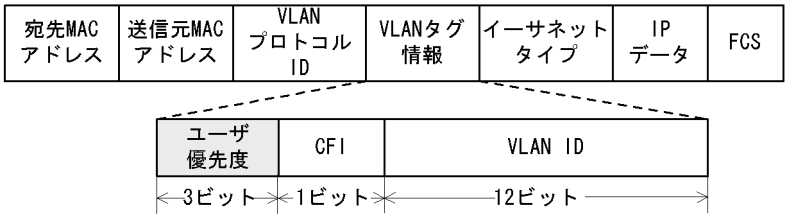
なお，DSCP への書き換えは，レイヤ 3 中継の送受信側およびレイヤ 2 中継の受信側で動作します。

DSCP 書き換えを行わない場合，レイヤ 2 中継およびレイヤ 3 中継では受信時の DSCP で送信します。

（2） ユーザ優先度書き換え

検出したフローの Tag-VLAN ヘッダ内にあるユーザ優先度を書き換えます。ユニキャスト，およびマルチキャストフレームに対して，入力側と出力側でユーザ優先度の書き換えができます。ユーザ優先度は次の図に示すように，VLAN タグ情報フィールドの先頭の 3 ビットを指します。

図 1-13 Tag-VLAN のヘッダフォーマット



この機能を利用することによって，検出したフローの DSCP 値をユーザ優先度に対応付けることができます。例えば，DSCP が 63 のフローに対してユーザ優先度を 7 に設定できます。

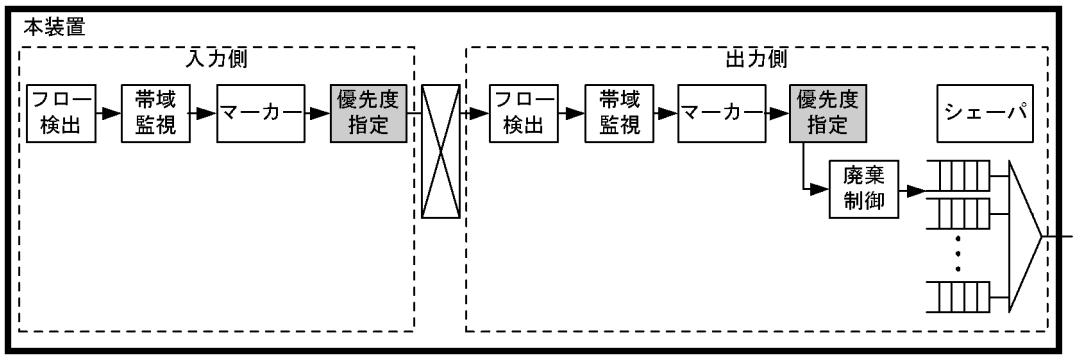
なお，ユーザ優先度の書き換えを使用することなく，受信した Tag-VLAN パケットを別の VLAN ID を持つ Tag-VLAN へ中継すると，出力するパケットのユーザ優先度はデフォルトの 0 となります。

また，ユーザ優先度の書き換えを使用せずにレイヤ 2 中継を行った場合，受信時のユーザ優先度で送信します。レイヤ 3 中継を行った場合，ユーザ優先度はデフォルトの 0 に書き換えます。

1.6 優先度決定

優先度決定には，検出したフローに対して明示的に優先度を指定する方法，DSCP に基づく優先度を指定する方法（DSCP マッピング），およびアグリゲートキュー番号指定の 3 種類があります。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 1-14 優先度決定の位置づけ



（凡例）：この節で説明する機能ブロック

(1) フローに基づく優先度決定

コンフィグレーションのフロー情報によって，パケットに対する優先度を決定できます。優先度には，どのキューにフローをキューイングするかを示す出力優先度と，廃棄されやすさを示すキューイング優先度の二つがあります。出力優先度は数字が大きいほど優先度が高く，キューイング優先度は数字が大きいほど廃棄されにくいことを示します。

なお，一つの動作指定には，フローに基づく優先度指定または DSCP マッピングのどちらかを選択して設定します。

- フローを受信または送信する際，「表 1-13 出力優先度とキューイング優先度の決定について」に従って，出力優先度およびキューイング優先度が決定します。ただし，本装置が生成するパケットは「表 1-13 出力優先度とキューイング優先度の決定について」の項番 3 に従って優先度が決定します。
- キューイング優先度は，「表 1-13 出力優先度とキューイング優先度の決定について」で決定したキューイング優先度を基に「表 1-22 決定したキューイング優先度と NIF 種別による対応キューイング優先度【SB-7800S】」および「表 1-24 決定したキューイング優先度と NIF 種別による対応キューイング優先度【SB-5400S】」に従って，NIF 種別ごとの対応キューイング優先度を決定します。

表 1-13 出力優先度とキューイング優先度の決定について

項番	フローの受信側の動作	フローの送信側の動作	出力優先度とパケットを積むキュー番号の決定方法	キューイング優先度の決定方法
1	フロー検出し，コンフィグレーションのフロー情報で出力優先度，キューイング優先度の指定あり	フロー検出し，コンフィグレーションのフロー情報で出力優先度，キューイング優先度の指定あり	1. 送信側でフロー検出したフロー情報に指定した出力優先度に従う。※1 2. 1. で決定した出力優先度を基に「表 1-19 送信側で決定した出力優先度に対応する出力先インタフェースのキュー番号」に従い，キュー番号が決定する。※2	送信側でフロー検出したフロー情報に指定したキューイング優先度に従う。※2

項番	フローの受信側の動作	フローの送信側の動作	出力優先度とパケットを積むキュー番号の決定方法	キューイング優先度の決定方法
		フロー検出し，コンフィグレーションのフロー情報で出力優先度，キューイング優先度の指定がない	1. 「表 1-14　出力優先度，キューイング優先の指定無しの場合の出力優先度」の項番 2 に従い，出力優先度が決定する。※2 2. 1. で決定した出力優先度が積まれるキュー番号となる。	送信側でキューイング優先度の明示的な指定がないため，キューイング優先度は 4 に決定する。※2
		フロー検出されない（どのコンフィグレーションのフロー情報にも一致しない）	1. 受信側でフロー検出したフロー情報に指定した出力優先度に従う。 2. 1. で決定した出力優先度を基に「表 1-18　受信側で決定した出力優先度に対応する出力先インタフェースのキュー番号」に従い，キュー番号が決定する。※3	受信側でフロー検出したフロー情報に指定したキューイング優先度に従う。※3
2	フロー検出し，コンフィグレーションのフロー情報で出力優先度，キューイング優先度の指定がない	フロー検出し，コンフィグレーションのフロー情報で出力優先度，キューイング優先度の指定あり	1. 送信側でフロー検出したフロー情報に指定した出力優先度に従う。 2. 1. で決定した出力優先度を基に「表 1-19　送信側で決定した出力優先度に対応する出力先インタフェースのキュー番号」に従い，キュー番号が決定する。※2	送信側でフロー検出したフロー情報に指定したキューイング優先度に従う。※2
		フロー検出し，コンフィグレーションのフロー情報で出力優先度，キューイング優先度の指定がない	1. 「表 1-14　出力優先度，キューイング優先の指定無しの場合の出力優先度」の項番 2 に従い，出力優先度が決定する。※2 2. 1. で決定した出力優先度が積まれるキュー番号となる。	送信側でキューイング優先度の明示的な指定がないため，キューイング優先度は 4 に決定する。※3
		フロー検出されない（どのコンフィグレーションのフロー情報にも一致しない）	1. 「表 1-14　出力優先度，キューイング優先の指定無しの場合の出力優先度」の項番 1 に従い，出力優先度が決定する。※3 2. 1. で決定した出力優先度が積まれるキュー番号となる。	受信側でキューイング優先度の明示的な指定がないため，キューイング優先度は 4 に決定する。※3
3	フロー検出されない（どのコンフィグレーションのフロー情報にも一致しない）	フロー検出し，コンフィグレーションのフロー情報で出力優先度，キューイング優先度の指定あり	1. 送信側でフロー検出したフロー情報に指定した出力優先度に従う。※2 2. 1. で決定した出力優先度を基に「表 1-19　送信側で決定した出力優先度に対応する出力先インタフェースのキュー番号」に従い，キュー番号が決定する。※2	送信側でフロー検出したフロー情報に指定したキューイング優先度に従う。※2
		フロー検出し，コンフィグレーションのフロー情報で出力優先度，キューイング優先度の指定がない	1. 「表 1-14　出力優先度，キューイング優先の指定無しの場合の出力優先度」の項番 2 に従い，出力優先度が決定する。※2 2. 1. で決定した出力優先度が積まれるキュー番号となる。	送信側でキューイング優先度の明示的な指定がないため，キューイング優先度は 4 に決定する。※2

項番	フローの受信側の動作	フローの送信側の動作	出力優先度とパケットを積むキュー番号の決定方法	キューイング優先度の決定方法
		フロー検出されない（どのコンフィグレーションのフロー情報にも一致しない）	1. 「表 1-15　デフォルトの出力優先度とキューイング優先度」に従い，出力優先度が決定する。※3 2. 1. で決定した出力優先度が積まれるキュー番号となる。	「表 1-15　デフォルトの出力優先度とキューイング優先度」に従い，キューイング優先度が決定する。※3

注※ 1

出力側にコンフィグレーションのフロー情報を指定し，かつ出力先インタフェースのスケジューリング種別が LLQ+3WFQ または階層化シェーパ機能を使用している場合は，ポートリストの指定で出力優先度を 1 ～ 4 に指定してください。なお，出力優先度が 5 ～ 8 に指定された場合，出力優先度は 4 として動作します。

注※ 2

ディストリビューション送信キューがある NIF では，決定した出力優先度およびキューイング優先度は送信側のディストリビューション送信キュー，送信キューで動作します。

NIF 種別による優先度指定の詳細については，「1.9　NIF 種別と QoS 制御機能との対応」を参照してください。

また，送信側のディストリビューション送信キューおよび送信キューについては，「図 1-20　レガシーシェーパ（ディストリビューションスケジューリング使用）の概念」を参照してください。

注※ 3

ディストリビューション送信キューがある NIF では，決定した出力優先度およびキューイング優先度は送信側のディストリビューション送信キューだけで動作します。

表 1-14　出力優先度，キューイング優先の指定無しの場合の出力優先度

項番	完全優先，ラウンドロビン			LLQ+3WFQ	階層化シェーパ
	8 キュー	4 キュー	2 キュー		【SB-7800S】
1	4	2	1	2	2
2	4	2	1	2	2

表 1-15　デフォルトの出力優先度とキューイング優先度

パケット種別	出力優先度					キューイング優先度
	完全優先，ラウンドロビン			LLQ+3WFQ	階層化シェーパ	
	8 キュー	4 キュー	2 キュー		【SB-7800S】	
本装置が生成する ARP・ルーティングプロトコル・SNMP パケット（本装置が生成するエラー通知パケット（ICMP，ICMPv6）を除く）。詳細を「表 1-16　本装置が生成する IPv4 パケット」，「表 1-17　本装置が生成する IPv6 パケット」に示します。	8	4	2	4	4	4
本装置が中継するパケット	4	2	1	2	2	4
本装置が生成するエラー通知パケット（ICMP，ICMPv6）	4	2	1	2	2	1

本装置が生成する IPv4 パケットを次の表に示します。

表 1-16 本装置が生成する IPv4 パケット

パケット名称	プロトコル (番号)	ポート番号	タイプ番号	備考
Echo Reply	ICMP(1)	-	0	エコー応答 (ping)
Echo		-	8	エコー要求 (ping)
Membership Query	IGMP(2)	-	17※3	メンバーシップ要求
Version1 Membership Report	IGMP(2)	-	18※3	バージョン 1 のメンバーシップ報告
ftp	TCP(6)	20，21※1	-	-
telnet		23※1	-	-
time		37※1	-	-
bgp		179※1	-	-
rlogin		513※1	-	-
smtp		25	-	-
TACACS		49	-	コンフィグレーションでポート番号が変更可能
echo	UDP(17)	7※2	-	-
time		37※2	-	-
bootps/bootpc		67，68※2	-	DHCP
ntp		123※2	-	-
snmp		161※2	-	-
sysylog		514※2	-	-
rip		520※2	-	-
RADIUS		1812，1813	-	コンフィグレーションでポート番号が変更可能
ospf	89	-	-	-
pim	103	-	-	-
vrrp	112	-	-	-

(凡例) - : 該当しない

注※ 1

送信元ポート番号および宛先ポート番号のどちらかがこのポート番号です。

注※ 2

送信元ポート番号がこのポート番号です。

注※ 3

IGMP バージョンと IGMP タイプを合わせたものがこのタイプ番号です。

本装置が生成する IPv6 パケットを次の表に示します。

表 1-17　本装置が生成する IPv6 パケット

パケット名称	プロトコル (番号)	ポート番号	タイプ番号	備考
Echo Reply	ICMPv6(58)	-	129	エコー応答 (ping)
Echo		-	128	エコー要求 (ping)
Multicast Listner Query		-	130	IPv6 マルチキャストグループの参加問い合わせ
RA		-	134	-
NDP		-	135，136	-
Redirect		-	137	-
ftp	TCP(6)	20，21 ※ 1	-	-
telnet		23 ※ 1	-	-
time		37 ※ 1	-	-
TACACS		49	-	コンフィグレーションでポート番号の変更可能
bgp4+		179 ※ 1	-	-
rlogin		513 ※ 1	-	-
echo	UDP(17)	7 ※ 2	-	-
time		37 ※ 2	-	-
ntp		123 ※ 2	-	-
snmp		161 ※ 2	-	-
sysylog		514 ※ 2	-	-
ripng		521 ※ 2	-	-
RADIUS		1812,1813	-	コンフィグレーションでポート番号の変更可能
ospfv3	89	-	-	-
pim	103	-	-	-
vrrp	112	-	-	-

(凡例)　- : 該当しない

注※ 1

送信元ポート番号および宛先ポート番号のどちらかがこのポート番号です。

注※ 2

宛先ポート番号がこのポート番号です。

表 1-18　受信側で決定した出力優先度に対応する出力先インタフェースのキュー番号

スケジューリング種別		完全優先，ラウンドロビン			LLQ+3WFQ
キュー数		8	4	2	4
出力優先度	1	1	1	1	1
	2	2			
	3	3	2		2

スケジューリング種別		完全優先，ラウンドロビン			LLQ+3WFQ
キュー数		8	4	2	4
	4	4			
	5	5	3	2	3
	6	6			
	7	7	4		4
	8	8			

表 1-19　送信側で決定した出力優先度に対応する出力先インタフェースのキュー番号

スケジューリング種別		完全優先，ラウンドロビン			LLQ+3WFQ	階層化シェーパ 【SB-7800S】
キュー数		8	4	2	4	4
出力優先度	1	1	1	1	1	1
	2	2			2	2
	3	3	2		3	3
	4	4			4	4
	5	5	3	2		
	6	6				
	7	7	4			
	8	8				

（2） DSCP マッピング

DSCP 値に基づき，フローの出力優先度とキューイング優先度を決定します。DSCP は TOS フィールドまたはトラフィッククラスフィールドの上位 6 ビットのことです。なお，一つの動作指定には，フローに基づく優先度指定または DSCP マッピングのどちらかを選択して設定します。

インタフェース名指定の出力側 (Outbound) に DSCP マッピングを指定した場合，出力先インタフェースのスケジューリングに LLQ+3WFQ を指定しないでください。

DSCP 値に対応する出力優先度とキューイング優先度を次の表に示します。

なお，この表に基づいて決定した出力優先度が積まれるキュー番号となります。

例えば，検出したフローの DSCP 値が 7 の場合，出力優先度は 1，キューイング優先度は 4 と自動で決まります。また，検出したフローの DSCP 値が 10 の場合，出力優先度は 2，キューイング優先度は 4 に自動で決まります。

表 1-20　DSCP 値に対応する出力優先度とキューイング優先度

DSCP 値	出力優先度			キューイング優先度
	8 キュー	4 キュー， LLQ+3WFQ， 階層化シェーパ **【SB-7800S】**	2 キュー	
0 ～ 7	1	1	1	4
8 ～ 9	2			1
10 ～ 11				4
12 ～ 13				3
14 ～ 15				2
16 ～ 17	3	2		1
18 ～ 19				4
20 ～ 21				3
22 ～ 23				2
24 ～ 25	4			1
26 ～ 27				4
28 ～ 29				3
30 ～ 31				2
32 ～ 33	5	3	2	1
34 ～ 35				4
36 ～ 37				3
38 ～ 39				2
40 ～ 47	6			1
48 ～ 55	7	4		1
56 ～ 63	8			1

キューイング優先度については，「表 1-20　DSCP 値に対応する出力優先度とキューイング優先度」で決定したキューイング優先度を基に「表 1-22　決定したキューイング優先度と NIF 種別による対応キューイング優先度【SB-7800S】」および「表 1-24　決定したキューイング優先度と NIF 種別による対応キューイング優先度【SB-5400S】」に従って，NIF 種別ごとの対応キューイング優先度を決定します。

（3）アグリゲートキュー番号指定【SB-7800S】

後述する階層化シェーパ機能のアグリゲートキューを指定します。出力側だけの機能です。階層化シェーパ機能をサポートしていない NIF に設定したインタフェースで，アグリゲートキュー番号を指定した場合，無視されます。また，階層化シェーパ機能をサポートしている NIF に設定したインタフェースで，アグリゲートキュー番号を指定した場合，コンフィグレーションの階層化シェーパ情報で該当アグリゲートキュー番号を指定する必要があります。指定しない場合は，該当アグリゲートキュー番号でパケットが廃棄されますのでご注意ください。

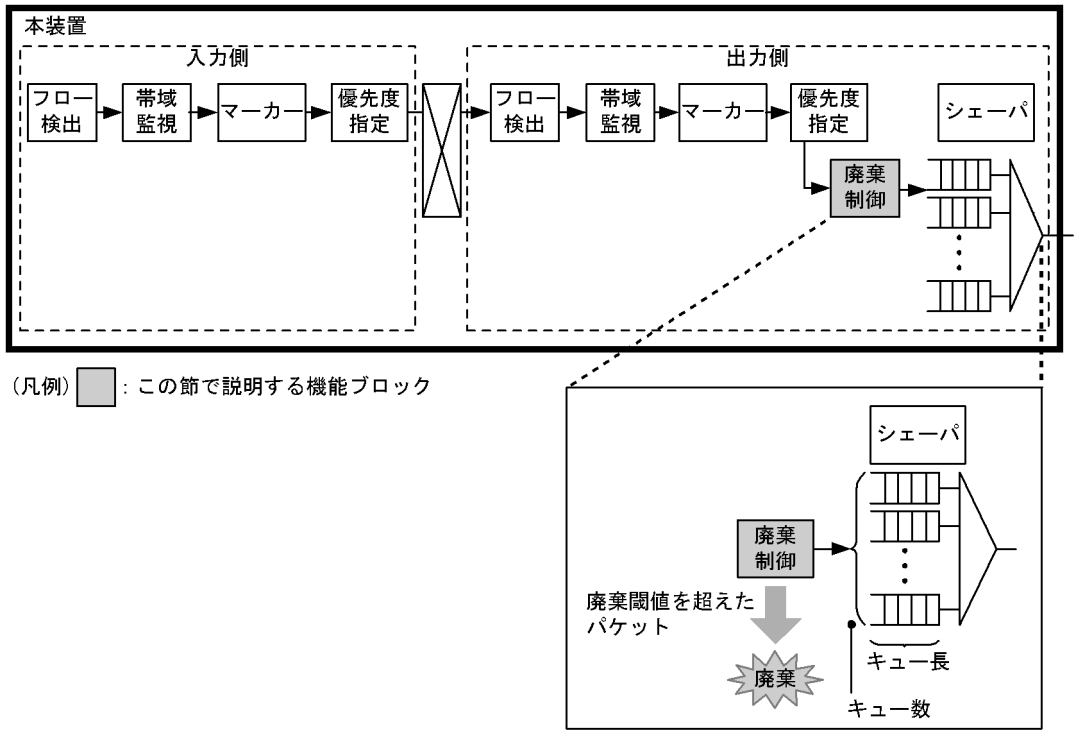
項目		仕様
アグリゲートキュー番号	初期値※	デフォルトキュー
	値の範囲	1 ～ 1023

注※　出力回線において階層化シェーパ機能が動作しているときに本パラメータを省略した場合，またはフロー検出のコンフィグレーションに一致しない場合

1.7 廃棄制御

この節では廃棄制御について説明します。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 1-15 廃棄制御の位置づけ



廃棄制御は，パケットの優先度とキューの状態に応じて，該当パケットをキューイングするか廃棄するかを制御します。キューにパケットが滞留している場合，同じ出力優先度でも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。なお，廃棄制御は出力側だけの機能です。

また，「図 1-15 廃棄制御の位置づけ」に示すとおり，一つのキューにキューイングできる最大のパケット数を「キュー長」，一つのインタフェースが保有するキューの最大数を「キュー数」と呼びます。

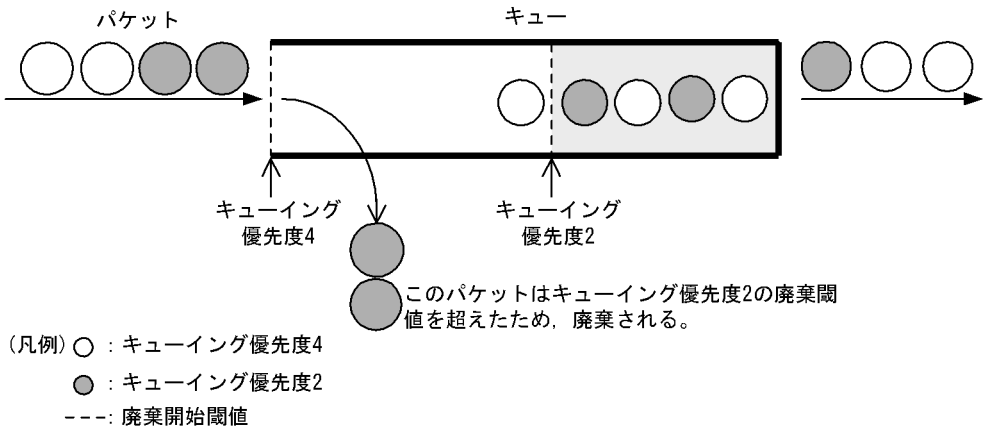
本装置は廃棄制御として，テールドロップおよび WRED の機能を提供します。

1.7.1 テールドロップ

キュー長が廃棄閾値を超えると，パケット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変えることができます。テールドロップの概念を次の図に示します。

この図に示すとおり，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 のパケットをすべて廃棄します。

図 1-16 テールドロップの概念



次に，廃棄閾値のデフォルト値を示します。デフォルト値は NIF 種別によって異なります。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。

（1） SB-7800S の場合

表 1-21 NIF 種別と廃棄閾値との対応【SB-7800S】

項番	NIF 種別		キューイング優先度に対する廃棄閾値			
			1	2	3	4
1	NE10G-1ER NE10G-1LW NE10G-1EW NE10G-1RX NE1G-12TA NE1G-12SA NE1G-6GA NP192-1S NP192-1S4 NP48-4S NEMX-12 S12-1G48T S12-1G48S S22-10G4RX S33-10G4RX		40%	60%	85%	100%
2	NE1G-48T	ディストリビューション送信キュー	40%	60%	85%	100%
		送信キュー	75%		100%	
3	NE1GSHP-4S NE1GSHP-8S		50%		100%	

注 表中のヘッダ部の数字 1 ～ 4 は，キューイング優先度を示します。

上記表における項番 1 の NIF は，1%単位に廃棄閾値をカスタマイズすることができます。項番 2 の NIF は，廃棄閾値が固定です。項番 3 の NIF は，3 種類のモードから廃棄閾値を選択することができます。

また，項番 2 の NIF における送信キューのキューイング優先度の廃棄閾値は，2 クラスだけサポートします。

「1.6 優先度決定」で決定したキューイング優先度について NIF 種別ごとで使用するキューイング優先度

のマッピングを次の表に示します。

表 1-22 決定したキューイング優先度と NIF 種別による対応キューイング優先度【SB-7800S】

決定したキューイング優先度	対応するキューイング優先度			
	NIF 種別			
	NE10G-1ER NE10G-1LW NE10G-1EW	NE1G-48T		NE1GSHP-4S NE1GSHP-8S
	NE10G-1RX NE1G-12TA NE1G-12SA NE1G-6GA NP192-1S NP192-1S4 NP48-4S MEMX-12 S12-1G48T S12-1G48S S22-10G4RX S33-10G4RX	ディストリビューション送信キュー	送信キュー	
1	1	1	1	1
2	2	2		
3	3	3	2	2
4	4	4		

（2） SB-5400S の場合

表 1-23 NIF 種別と廃棄閾値との対応【SB-5400S】

項番	NIF 種別		キューイング優先度に対する廃棄閾値			
			1	2	3	4
1	NF1G-6G NFMX-34（32，33 ポート）		40%	60%	85%	100%
2	NF100-48TA NF1G-48T NF1G-32S	ディストリビューション送信キュー	40%	60%	85%	100%
	NFMX-44 NFMX-34（0 ～ 31 ポート）	送信キュー	75%		100%	

注 表中のヘッダ部の数字 1 ～ 4 は，キューイング優先度を示します。

上記表における項番 1 の NIF は，1%単位に廃棄閾値をカスタマイズすることができます。項番 2 の NIF は，廃棄閾値が固定です。

また，項番 2 の NIF における送信キューのキューイング優先度の廃棄閾値は，2 クラスだけサポートします。

「1.6 優先度決定」で設定したキューイング優先度について NIF 種別ごとで使用するキューイング優先度のマッピングを次の表に示します。

表 1-24 決定したキューイング優先度と NIF 種別による対応キューイング優先度【SB-5400S】

決定したキューイング優先度	対応するキューイング優先度		
	NIF 種別		
	NF1G-6G NFMX-34 (32,33 ポート)	NF100-48TA NF1G-48T NF1G-32S NFMX-44 NFMX-34（0 ～ 31 ポート）	
		ディストリビューション送信キュー	送信キュー
1	1	1	1
2	2	2	
3	3	3	2
4	4	4	

1.7.2 WRED

WRED(Weighted Random Early Detection) は，キュー長が廃棄閾値を超えるとランダムにパケットを廃棄する機能です。パケットが廃棄されることによって，TCP を使用するアプリケーションはパケットの再送とトラフィック量を減らします。テールドロップを利用したときに一斉にパケットの廃棄が発生すると，複数の TCP アプリケーションが一斉にパケットを再送するため，回線帯域を有効に活用できなくなるという問題を，WRED を使用することで回避できます。

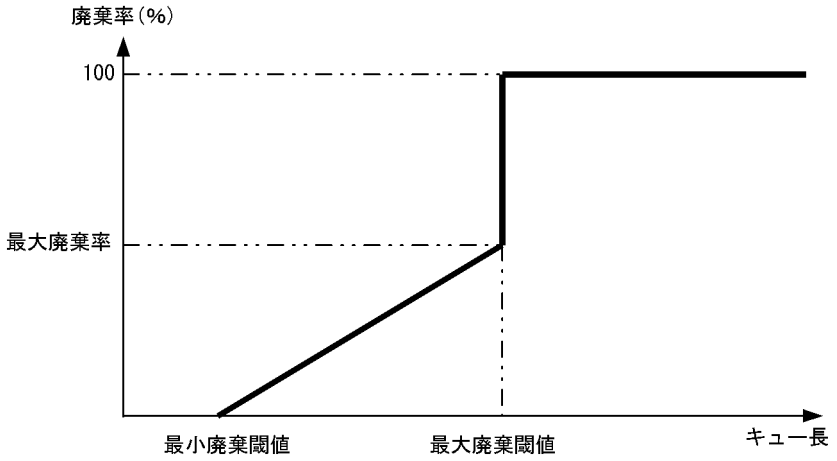
WRED が使用可能な NIF については，「1.9 NIF 種別と QoS 制御機能との対応」を参照してください。

(1) WRED の機能詳細

最小廃棄閾値と最大廃棄閾値を設定し，最大廃棄閾値を超えたパケットをすべて廃棄します。また，最大廃棄率を設定することによって，最小廃棄閾値と最大廃棄閾値の範囲内でランダムにパケットを廃棄します。

WRED を使用した際のキュー長に対する廃棄率の概念図を次の図に示します。また，各廃棄クラスの閾値を「表 1-25 廃棄閾値と最大廃棄率の初期値」に示します。

図 1-17 キュー長に対する廃棄率の概念図



1. 最小廃棄閾値を超えるまでの間は，通常に中継します。
2. 最小廃棄閾値を超え始めたとき，送信パケットの中からいくつかのパケットを最大廃棄率に応じて廃棄します。
3. 最大廃棄閾値を超えると，すべての送信パケットを廃棄します。

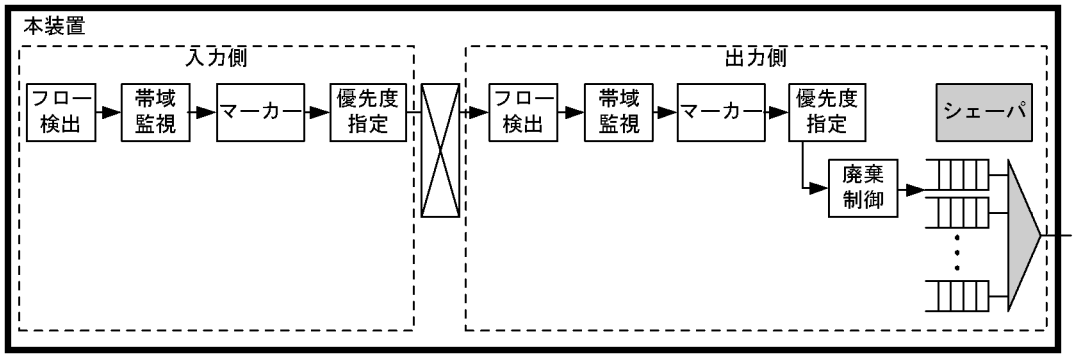
表 1-25　廃棄閾値と最大廃棄率の初期値

キューイング優先度	最小廃棄閾値 / 最大廃棄閾値 (%)	最大廃棄率 (%)
1	0/40	10
2	40/60	10
3	60/85	10
4	85/100	10

1.8 シェーパ

シェーパは，パケッ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 1-18 シェーパの位置づけ



本装置で提供するシェーパは，PSU(SB-5400S では BSU) に標準で備わっている**レガシーシェーパ**と，ネットワークインタフェース NE1GSHP-4S または NE1GSHP-8S を必要とする**階層化シェーパ【SB-7800S】**の 2 種類があります。

1.8.1 レガシーシェーパ

レガシーシェーパは次の図に示すとおり，物理回線の帯域をシェーピングするポート帯域制御と，どのキューにあるパケットを次に送信するかを決めるスケジューリングから構成されます。レガシーシェーパ（ディストリビューションスケジューリング未使用）の概念，レガシーシェーパ（ディストリビューションスケジューリング使用）の概念を次の図に示します。ディストリビューションスケジューリングの詳細については，「(3) ディストリビューションスケジューリング」を参照してください。

図 1-19 レガシーシェーパ（ディストリビューションスケジューリング未使用）の概念

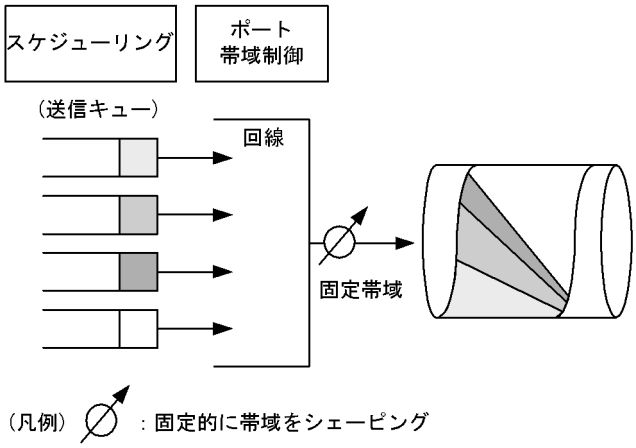
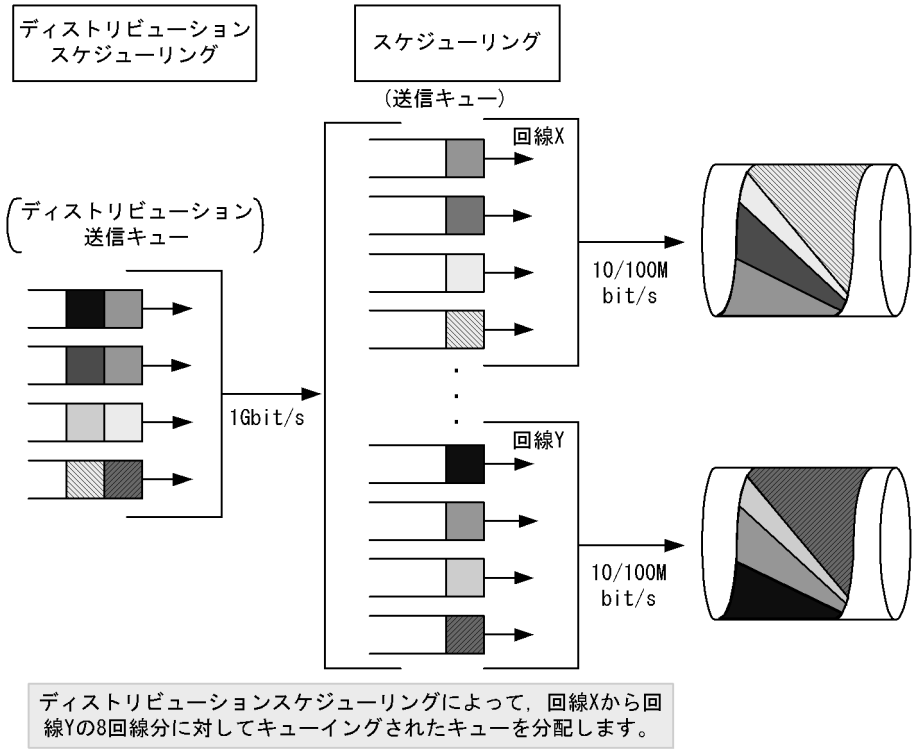


図 1-20 レガシーシェーパ（ディストリビューションスケジューリング使用）の概念



(1) 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，回線全体の送信帯域を回線速度以下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 500Mbit/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 500Mbit/s 以下に抑えてパケットを送信できます。物理帯域と契約帯域の差による輻輳を回避できます。

回線種別に対するポート帯域制御の帯域範囲と設定単位を次の表に示します。この仕様は回線種別によって異なります。設定可能な NIF 種別については，「1.9 NIF 種別と QoS 制御機能との対応」を参照してください。

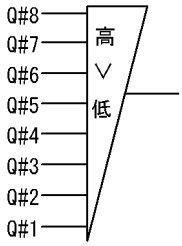
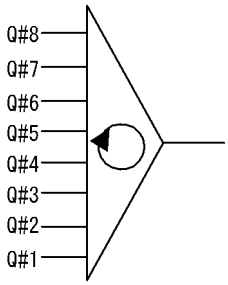
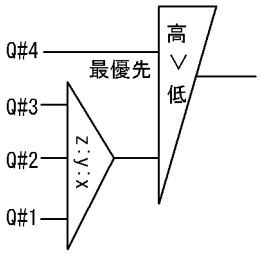
表 1-26 回線種別に対するポート帯域制御の帯域範囲と設定単位

回線種別	帯域の範囲	設定単位
10GBASE-R【SB-7800S】 10GBASE-W【SB-7800S】 OC-192C/STM-64 POS【SB-7800S】	10M ～ 10Gbit/s	1Mbit/s
1000BASE-X 1000BASE-T	1M ～ 1Gbit/s	
100BASE-TX(全二重)	500k ～ 100Mbit/s	100kbit/s
10BASE-T(全二重)	500k ～ 10Mbit/s	
OC-48c/STM-16 POS【SB-7800S】	10M ～ 2400Mbit/s	1Mbit/s

(2) スケジューリング

スケジューリングには，3 種類の方式があります。スケジューリングの動作仕様を次の表に示します。

表 1-27 スケジューリングの動作仕様

スケジューリング種別	概念図	動作説明	適用例
完全優先		ポート当たり 8 キュー。複数のキューにパケットが存在する場合，優先度の高いキューから常にパケットを送信します。完全優先制御がスケジューリングのデフォルトです。	トラフィックの優先順を完全に遵守する場合
ラウンドロビン		ポート当たり 8 キュー。複数のキューにパケットが存在する場合，順番にキューを参照し，パケットを送信します。パケット長に関わらず，パケット数が均等になるように制御します。	データ系トラフィックだけの場合
LLQ+3WFQ		最優先キュー付き，重み付き均等保証。ポート当たり 4 キュー。最優先キューがキュー 4(左図 Q#4) と，重み付き帯域均等キューが三つ (左図 Q#1，Q#2，Q#3)。Q#4 にパケットが存在する場合，最優先でパケットを送信します。Q#4 が使用していない残りの帯域を設定した x:y:z の比に応じて Q#1，Q#2，Q#3 からパケットを送信します。	LLQ に音声，WFQ にデータ系トラフィック

スケジューリングの仕様を次の表に示します。

表 1-28 スケジューリングの仕様

項目		仕様	内容
キュー数	完全優先 ラウンドロビン	8	-
	LLQ+3WFQ	4	使用可能な NIF 種別については，「1.9 NIF 種別と QoS 制御機能との対応」を参照してください。
キュー長		非公開（固定値）	キュー数を変更することで，キュー長を拡張できます。 使用可能な NIF 種別については，「1.9 NIF 種別と QoS 制御機能との対応」を参照してください。
シェーピング対象のフレーム長	イーサネット	84 ～ 1538 バイト	フレーム間ギャップ，プリアンブル，FCS を含みます。
		84 ～ 9616 バイト	フレーム間ギャップ，プリアンブル，FCS を含みます。Jumbo フレーム設定時。
	POS	12 ～ 9222 バイト	開始／終了フラグ，FCS を含みます。

項目		仕様	内容
LLQ+3WFQ	キュー 1 ～ 3 の重み	1 ～ 100%	1%単位で指定。キュー 1 ～ 3 の重み x,y,z について次の条件を満たすように設定してください。 x+y+z ≦ 100

(凡例) -: 該当しない

(3) ディストリビューションスケジューリング

ディストリビューション送信キューを搭載する NIF 種別を次の表に示します。

表 1-29 ディストリビューション送信キューを搭載する NIF 種別【SB-7800S】

項番	対象 NIF の略称
1	NE1G-48T
2	NE1GSHP-4S
3	NE1GSHP-8S

表 1-30 ディストリビューション送信キューを搭載する NIF 種別【SB-5400S】

項番	対象 NIF の略称
1	NF100-48TA
2	NF1G-48T
3	NF1G-32S
4	NFMX-44
5	NFMX-34（だたし，0 ～ 31 ポートだけ）

ディストリビューションスケジューリングは，スケジューリング動作を完全優先固定で動作します。スケジューリング動作を変更することはできません。

廃棄制御はテールドロップで動作します。詳細については，「1.7.1 テールドロップ」を参照してください。

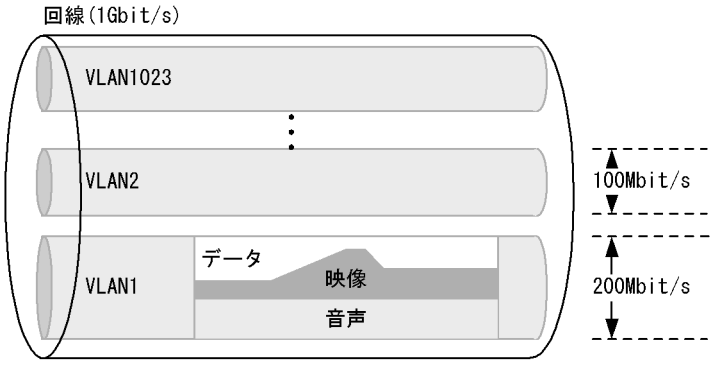
ディストリビューション送信キューにキューイングされたパケットは，優先度の高いキューから送信キューへキューイングされます。このため，ディストリビューション送信キューのキューに滞留が発生すると，送信キューのスケジューリング動作でラウンドロビンを選択していても完全優先の優先順で送信されます。

階層化シェーパ NIF においても，4WFQ の重みを均等に設定した場合は同様の動作となります。

1.8.2 階層化シェーパ【SB-7800S】

階層化シェーパは，次の図に示すとおり，Tag-VLAN 連携回線などのユーザごとに帯域を確保できます。回線が輻輳状態でも，ユーザごとに割り当てた帯域を保証できます。さらに，ユーザ内のアプリケーション種別ごとに優先制御および帯域制御を行うことができます。

図 1-21 階層化シェーパの概念



階層化シェーパは，次に示す三つの制御ブロックから構成されます。

1. ポート帯域制御：回線全体の送信帯域を回線速度以下にシェーピングする
2. アグリゲートキュー帯域制御：ユーザごとに帯域制御を実行する
3. スケジューリング：ユーザ単位で保有する四つのキューの内，どのキューにあるパケットを次に送信するかを決定する

ポート帯域制御は，「1.8.1 レガシーシェーパ （1）ポート帯域制御」と同様の機能です。次に，アグリゲートキュー帯域制御とスケジューリングを説明します。

（1） アグリゲートキュー帯域制御

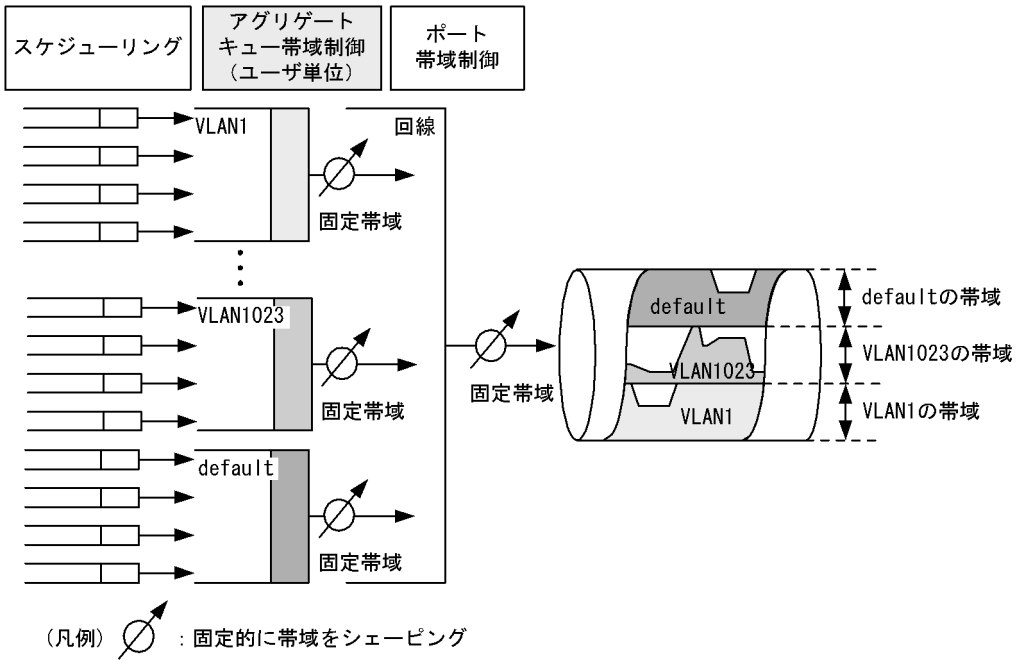
（a） 制御方式

アグリゲートキュー帯域制御には，RLQ(Rate Limited Queueing) 方式と RGQ(Rate Guaranteed Queueing) 方式の 2 種類の制御方式があります。

RLQ はユーザごとに固定帯域を割り当てる方式です。RLQ の概念を次の図に示します。この図は，左側に階層化シェーパの構造図を，右側に回線内におけるトラフィックの状態変化を示しています。アグリゲートキュー帯域制御は四つのキューを保持しています。スケジューリングを実施した後のトラフィックをシェーピングします。

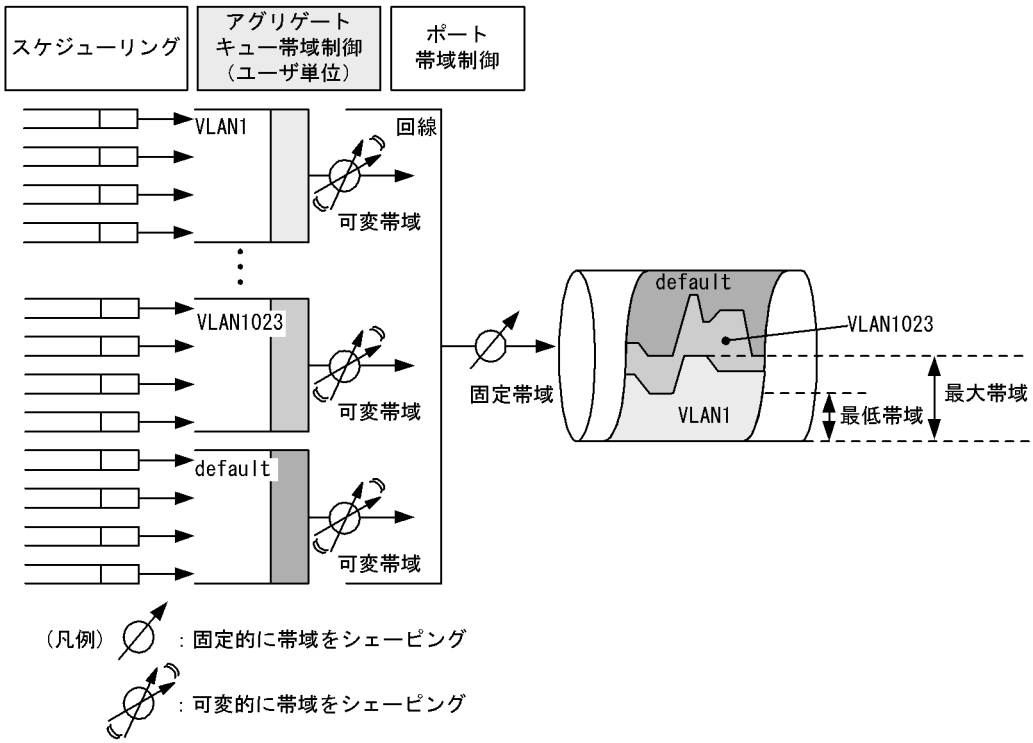
この図に示すように，VLAN1 は VLAN1023 と default のトラフィックの影響を受けず，常に帯域を確保できます。ただし，回線内で使用していない帯域 (余剰帯域) があっても，その帯域をほかのユーザが使用することはできません。また，ユーザごとに割り当てた帯域の合計は，ポート帯域制御の帯域値以内を満たす必要があります。

図 1-22 RLQ の概念



RGQ はユーザごとに最低帯域を保証する方式です。回線に余剰帯域がある場合，ユーザごとに設定した最大帯域まで余剰帯域を割り当てることができます。RGQ の概念を次の図に示します。

図 1-23 RGQ の概念



余剰帯域は，デフォルトではユーザ間で均等に分配します。また，設定によってユーザ単位に余剰帯域の分配比率（重み）を決めることができます。分配比率に応じた余剰帯域の計算例を次の表に示します。こ

の表ではポート帯域制御によって回線帯域を 900Mbit/s にシェーピングする場合を想定します。計算を簡単にするため，ユーザ数を三つにします。

表 1-31　余剰帯域の計算例

割り当てユーザ	入力帯域 (Mbit/s)	最低帯域 (Mbit/s)	最大帯域 (Mbit/s)	余剰帯域分配比率	余剰帯域※ (Mbit/s)	実際の送信帯域 (Mbit/s)
VLAN1	400	200	900	3	150	350
VLAN2	350	200	900	2	100	300
VLAN1023	250	200	900	1	50	250

注※　回線内の余剰帯域＝回線帯域 - 各ユーザごとの最低帯域の合計
＝ 900-(200 ＋ 200 ＋ 200) ＝ 300(Mbit/s)
VLAN1 の余剰帯域＝ 300 × (3 ÷ (3 ＋ 2 ＋ 1)) ＝ 150(Mbit/s)
VLAN2 の余剰帯域＝ 300 × (2 ÷ (3 ＋ 2 ＋ 1)) ＝ 100(Mbit/s)
VLAN1023 の余剰帯域＝ 300 × (1 ÷ (3 ＋ 2 ＋ 1)) ＝ 50(Mbit/s)

(b) アグリゲートキュー帯域制御の仕様

アグリゲートキュー帯域制御の仕様を次の表に示します。

表 1-32　アグリゲートキュー帯域制御の仕様

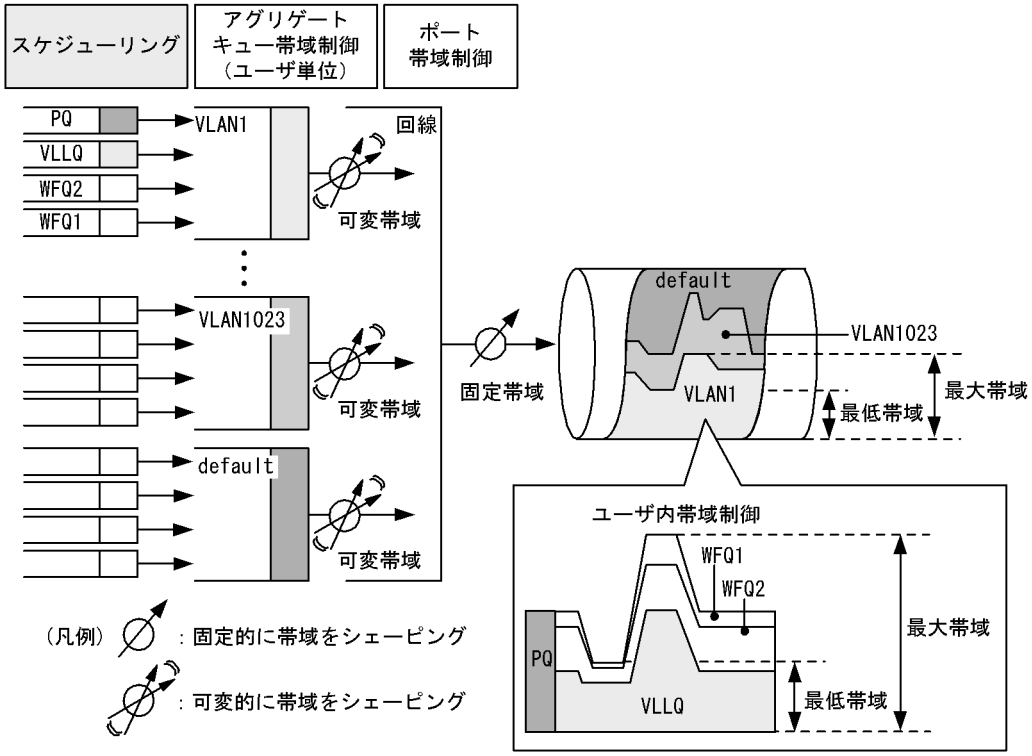
項目		仕様	内容
アグリゲートキュー数		16384/ 装置	-
		1024/ 回線	デフォルトのアグリゲートキューを含みます。
RLQ	最大帯域	240kbit/s ～ 1Gbit/s	1kbit/s 単位で指定できます。
RGQ	最大帯域		
	最低帯域		
	余剰帯域分配方式	ユーザ間均等 (デフォルト)	-
		重み　1 ～ 50	ユーザごとに重みに応じて余剰帯域を分配します。
デフォルトのアグリゲートキュー		1/ 回線	フロー検出条件で検出されないパケットが割り当てられるキュー。

(凡例)　- : 該当しない

(2) スケジューリング

スケジューリングは，どのキューにあるパケットを次に送信するかを決めます。スケジューリングの概念を次の図に示します。この図は，アグリゲートキュー帯域制御として RGQ 方式を使用し，スケジューリングとして PQ+LLQ+2WFQ 方式を使用した帯域制御の様子を示しています。合わせて，VLAN1 内の帯域制御の様子を示します。本装置の特徴である PQ+LLQ+2WFQ 方式の動作を，次の図を使って説明します。なお，スケジューリングは，PQ+LLQ+2WFQ のほかに 3 種類の方式がありますが，それらは「表 1-33　スケジューリングの動作仕様」にまとめて説明します。

図 1-24 スケジューリングの概念

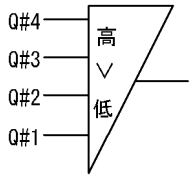


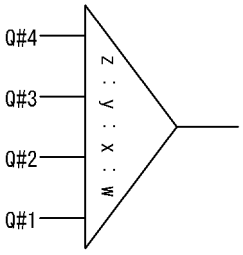
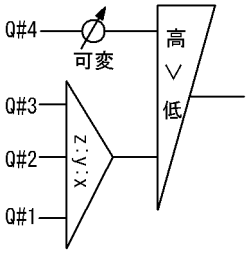
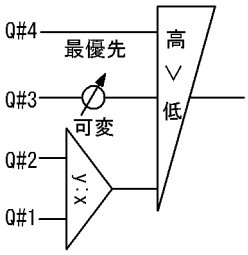
PQ+LLQ+2WFQ 方式は，PQ(Priority Queueing) と LLQ(Low Latency Queueing)，二つの WFQ(Weighted Fair Queueing) から構成されます。PQ は常に最優先でパケットを出力します。PQ の動作は，「図 1-24 スケジューリングの概念」のユーザ内帯域制御に示すように，ユーザごとの帯域が変動しても，優先的に出力できる点が特徴です。

LLQ は，PQ が動作していないときの帯域に対して，最低保証帯域の範囲内で WFQ のキューより優先的にパケットを出力します。また，RGQ 方式のようにユーザ単位に余剰帯域が割り当てられると，その余剰に応じて確保できる帯域が変動するという特徴があります。このキューを VLLQ(Variable LLQ) と呼びます。

最後に二つの WFQ は，VLLQ が使用しない残りの帯域を，設定した重みに応じて使用します。

表 1-33 スケジューリングの動作仕様

機能名	概念図	動作説明	適用例
完全優先		完全優先制御。複数のキューにパケットが存在する場合，優先度の高いキューから常にパケットを送信します。	トラフィックの優先順を完全に遵守する場合

機能名	概念図	動作説明	適用例
4WFQ		重み付き均等保証。ポート当たり 4 キュー。帯域を，設定した w:x:y:z の比に応じて Q#1，Q#2，Q#3，Q#4 からパケットを送信します。	データ系トラフィックだけの帯域制御
VLLQ+3WFQ		最優先キュー付き，重み付き均等保証。ポート当たり 4 キュー。最優先キューがキュー 4(左図 Q#4) と，重み付き帯域均等キューが三つ (左図 Q#1，Q#2，Q#3)。 Q#4 にパケットが存在する場合，最低保証帯域の範囲内でパケットを送信します (VLLQ)。 Q#4 が使用していない残りの帯域を設定した x:y:z の比に応じて Q#1，Q#2，Q#3 からパケットを送信します。なお，この方式で VLLQ の最低保証帯域を 100%に設定すると，レガシーシェーパの LLQ+3WFQ と同等になります。	VLLQ に映像，WFQ にデータ系トラフィック
2LLQ+2WFQ (PQ+VLLQ+2WFQ)		最優先キュー付き，重み付き均等保証。ポート当たり 4 キュー。最優先キューが二つ (左図 Q#3，Q#4)，重み付き帯域均等キューが二つ (左図 Q#1，Q#2)。 Q#4 は，常に最優先で出力します (PQ)。Q#3 は，Q#4 が使用していない残りの帯域を使用して，最低保証帯域の範囲内で優先的にパケットを出力します (VLLQ)。 Q#1 と Q#2 は，Q#3 と Q#4 が使用していない残りの帯域を，設定した x:y の比に応じてパケットを送信します。	PQ に音声，VLLQ に映像，WFQ にデータ系トラフィック

スケジューリングの仕様を次の表に示します。

表 1-34　スケジューリングの仕様

項目		仕様	内容
帯域制御対象パケット		すべてのパケット	-
キュー数		4	-
キュー長		0 ～ 4000※	設定によって変更できます。
フレーム長		84 ～ 2056B	シェーピング対象のフレーム長。フレーム間ギャップ，プリアンブル，FCS を含みます。
4WFQ	キュー 1 ～ 4	1 ～ 100%	1%単位で指定します。キュー 1 ～ 4 の重みである w，x，y，z について次の条件を満たすように設定してください。 w+x+y+z ≦ 100 w ≦ x ≦ y ≦ z
VLLQ+3WFQ	キュー 4（VLLQ）	10 ～ 100%	最低保証帯域に対し 10%単位の比率で指定します。

項目		仕様	内容
	キュー 1 ～ 3	1 ～ 100%	1%単位で指定。キュー 1 ～ 3 の重みである x，y，z について次の条件を満たすように設定してください。 x+y+z ≦ 100 x ≦ y ≦ z
2LLQ+2WFQ	キュー 4 PQ	-	完全優先制御を指定
	キュー 3(VLLQ)	10 ～ 100%	最低保証帯域に対し 10%単位の比率で指定します。
	キュー 1 ～ 2	1 ～ 100%	1% 単位で指定します。キュー 1 ～ 2 の重みである x，y について次の条件を満たすように設定してください。 x+y ≦ 100 x ≦ y

（凡例） -：該当なし

注※ 各キューにはキュー長が未設定時はデフォルト値が割り当てられます。送信キューごとのデフォルトキュー長を次の表に示します。

表 1-35 送信キューごとのデフォルトキュー長

送信キュー番号	デフォルトキュー長
1	120
2	100
3	80
4	50

次に，ユーザ単位内の各キューが確保する帯域値の変化を具体的に説明します。説明は，次の表に示すキューの設定値を例として取り上げます。

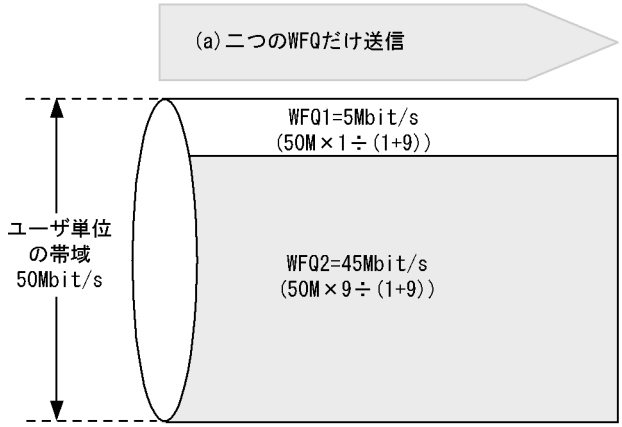
表 1-36 キューに対する設定値

キュー種別	設定値
VLLQ	90%
WFQ2	9%
WFQ1	1%

なお，説明を簡単にするため，ユーザ単位に割り当てられた帯域は固定値 50Mbit/s とします。パケットのトラフィックパターンを 2 種類に分けて，各キューが確保する帯域値の相違を次に示します。

● パターン (a)

図 1-25　各キューが確保する帯域値の相違 (二つの WFQ だけ送信)



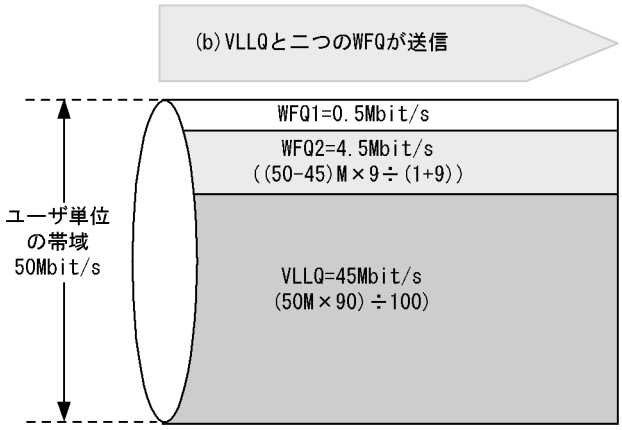
WFQ が動作するキューだけパケットの入力があるトラフィックパターンです。二つの WFQ は，ユーザ単位に割り当てられた帯域（ユーザ帯域と呼ぶ）である 50Mbit/s を設定した重みに応じて分け合います。例えば WFQ2 が確保する帯域は，次の計算で求まります。

```
WFQ2＝ユーザ帯域×WFQ2の重み÷(WFQ1の重み＋WFQ2の重み)
    ＝50M×9÷(1+9)
    ＝45Mbit/s
```

WFQ1 も同様の計算によって，5Mbit/s の帯域を確保します。

● パターン (b)

図 1-26　各キューが確保する帯域値の相違 (VLLQ と二つの WFQ が送信)



VLLQ と WFQ が動作するキューに対してパケットの入力があるトラフィックパターンです。まず優先度の高い VLLQ へ帯域を割り当て，残りの帯域を WFQ で分け合います。VLLQ は，ユーザ帯域 50Mbit/s のうち，最低保証帯域の重み 90%分，つまり 45Mbit/s の帯域を確保します。一方，二つの WFQ は，VLLQ が使用しない残りの帯域を設定した重みに応じて分け合います。WFQ2 が確保する帯域は，次の計算で求まります。

```
WFQ2＝(ユーザ帯域-VLLQの帯域)×WFQ2の重み÷(WFQ1の重み＋WFQ2の重み)
    ＝(50M-45M)×9÷(1+9)
    ＝4.5Mbit/s
```

WFQ1 も WFQ2 と同様の計算によって，0.5Mbit/s の帯域を確保します。

(3) ユーザ優先度書き換え機能

この機能は，キューイングしたパケットを出力するときに，パケットのユーザ優先度を書き換えます。この機能には 2 種類のモードがあり，装置で一つのモードを選択します。ユーザ優先度書き換え機能の仕様を次の表に示します。なお，デフォルトは，ユーザ優先度を書き換えません。

表 1-37　ユーザ優先度書き換え機能の仕様

モード	仕様
ユーザ優先度保存 (デフォルト)	ユーザ優先度の書き換えを行いません。マーカー機能によってユーザ優先度書き換えた場合，書き換えた値がそのまま出力されます。このモードが装置としてのデフォルトとなります。
ユーザ優先度クリア	ユーザ優先度をデフォルト値 0 に書き換えます。

この機能は，マーカーを実行した後に動作します。そのためモードとしてユーザ優先度クリアまたはユーザ優先度書き換えを選択した場合，マーカーで書き換えたユーザ優先度が，再度書き換わります。

(4) キュー長指定機能

この機能は，「CSW 側受信キュー (from_CSW キュー)」および「NIF 側送信キュー (ディストリビューションキュー)」のキュー長 (バッファ) を任意の値に設定できます。キュー長を変更することによって，当該回線から送信されるバーストトラフィックに対するキュー溢れを回避することができます。

なお本機能は，NE1GSHP-8S だけ設定可能です。

キュー長指定が対象となるキューの位置付けを次の図に，設定可能なキュー長を「表 1-38　設定可能なキュー長」に示します。

図 1-27　対象となるキューの位置付け

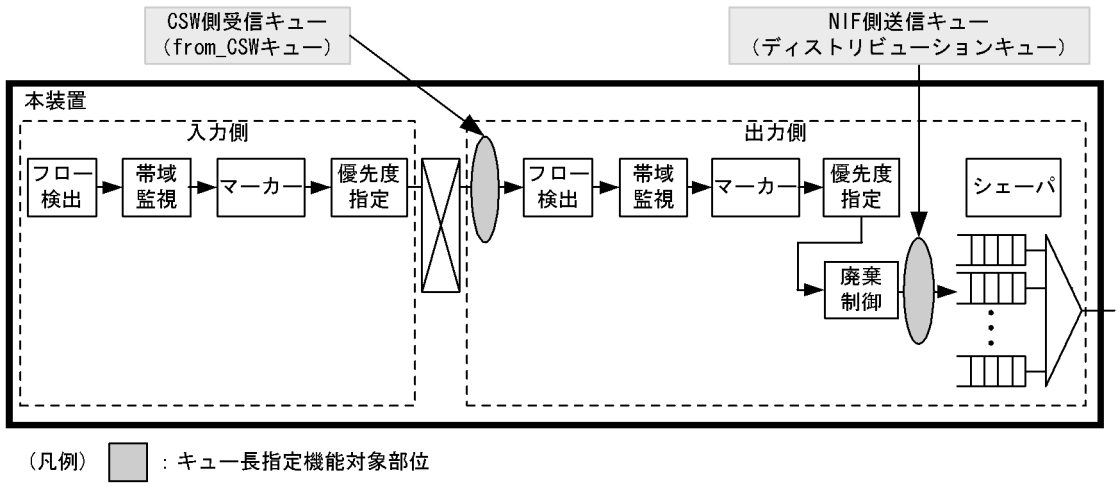


表 1-38　設定可能なキュー長

キュー種別	指定可能キュー長	条件
CSW 受信側キュー (from_CSW キュー)	128 / 256 / 512 / 1024	受信キュー数が四つあるため，4 キューのサイズ合計が 1536 を超えないこと

キュー種別	指定可能キュー長	条件
NIF 側送信キュー (ディストリビューションキュー)	2048 / 4096 / 8192 / 16384	送信キュー数が四つあるため，4 キューのサイズ合計が 32768 を超えないこと

1.9 NIF 種別と QoS 制御機能との対応

SB-7800S の NIF 種別と QoS 制御機能との対応を次の表の (1/3) ～ (3/3) に示します。

表 1-39 NIF 種別と QoS 制御機能との対応 (1/3)【SB-7800S】

NIF 種別	機能									
	フロー検出	帯域監視	マーカー	優先度指定			廃棄制御			
				出力優先	DSCP マップ	キュー数指定	テールドロップ		WRED	閾値の変更
							2 クラス	4 クラス		
NE10G-1ER NE10G-1LW NE10G-1EW NE10G-1RX NE1G-12TA NE1G-12SA NE1G-6GA NEMX-12 S12-1G48T S12-1G48S S22-10G4RX S33-10G4RX	○	○	○	○	○	○	-	○	○	○
NE1G-48T	○	○	○	○※4	○※4	○	○	-	-※1	-
NE1GSHP-4S	○	○	○	○※4	○※4	-	○	-	-	○
NE1GSHP-8S	○	○	○	○※4	○※4	-	○	-	-	○
NP192-1S4 NP48-4S NP192-1S	○※2	○	○※3	○	○	○	-	○	○	○

(凡例) ○：該当する -：該当しない

注※ 1

WRED を指定した場合はログメッセージを表示しテールドロップで動作します。

注※ 2

MAC ヘッダ検出条件は指定できません。

注※ 3

ユーザ優先度書き換えはできません。

注※ 4

Inbound で設定した場合，ディストリビューション送信キューに反映されます。以降の送信キューについては，Outbound へのフロー QoS 情報設定で対応してください。

表 1-40 NIF 種別と QoS 制御機能との対応 (2/3)【**SB-7800S**】

NIF 種別	機能						
	シェーパ						
	レガシーシェーパ				階層化シェーパ		
	ポート帯域制御	スケジューリング			ポート帯域制御	アグリゲートキュー帯域制御	
		PQ	RR	LLQ		RLQ	RGQ
NE10G-1ER NE10G-1LW NE10G-1EW NE10G-1RX NE1G-12TA NE1G-12SA NE1G-6GA NEMX-12 S12-1G48T S12-1G48S S22-10G4RX S33-10G4RX	○	○	○	○	-	-	-
NE1G-48T	-	○	○	-※1	-	-	-
NE1GSHP-4S	-	-	-	-	○※2	○※2	○※2
NE1GSHP-8S	-	-	-	-	○※2	○※2	○※2
NP192-1S4 NP48-4S NP192-1S	○	○	○	○	-	-	-

(凡例) ○：該当する -：該当しない

PQ：Priority Queuing（完全優先） RR：Round Robin（ラウンドロビン）

LLQ：Low Latency Queuing（LLQ ＋ 3WFQ）

RLQ：Rate Limited Queuing RGQ：Rate Guaranteed Queuing

注※ 1

LLQ を指定した場合は，ログメッセージを表示し PQ で動作します。

注※ 2

NE1GSHP-4S または NE1GSHP-8S を使用する場合は，必ずコンフィグレーションコマンド shaper を設定してください。

表 1-41 NIF 種別と QoS 制御機能との対応 (3/3)【SB-7800S】

NIF 種別	機能				
	シェーパ				
	階層化シェ - パ				
	スケジューリング				キュー長指定
	PQ	LLQ+3WFQ	2LLQ+2WFQ	4WFQ	
NE10G-1ER NE10G-1LW NE10G-1EW NE10G-1RX NE1G-12TA NE1G-12SA NE1G-6GA NEMX-12 S12-1G48T S12-1G48S S22-10G4RX S33-10G4RX	-	-	-	-	-
NE1G-48T	-	-	-	-	-
NE1GSHP-4S	○※	○※	○※	○※	-
NE1GSHP-8S	○※	○※	○※	○※	○
NP192-1S4 NP48-4S NP192-1S	-	-	-	-	-

(凡例) ○：該当する -：該当しない

PQ：Priority Queuing（完全優先） LLQ：Low Latency Queuing

WFQ：Weighted Fair Queueing

注※ NE1GSHP-4S または NE1GSHP-8S を使用する場合は，必ずコンフィグレーションコマンド shaper を設定してください。

SB-5400S の NIF 種別と QoS 制御機能との対応を次の表の (1/2) と (2/2) に示します。

表 1-42 NIF 種別と QoS 制御機能との対応 (1/2)【SB-5400S】

NIF 種別		機能									
		フロー検出	帯域監視	マーカー	優先度指定			廃棄制御			
					出力優先	DSCP マップ	キュー数指定	テールドロップ		WRED	閾値の変更
								2 クラス	4 クラス		
NF1G-6G		○	○	○	○	○	○	-	○	○	○
NF100-48TA		○	○※2	○	○※2	○※2	○	○	-	-※1	-
NF1G-48T NF1G-32S NFMX-44		○	○※2	○	○※2	○※2	○	○	-	-※1	-
NFMX-34	0 ～ 31 ポート	○	○※2	○	○※2	○※2	○	○	-	-※1	-

NIF 種別		機能									
		フロー検出	帯域監視	マーカー	優先度指定			廃棄制御			
					出力優先	DSCPマップ	キュー数指定	テールドロップ		WRED	閾値の変更
								2クラス	4クラス		
	32,33ポート	○	○	○	○	○	○	-	○	-※1	-

（凡例） ○：該当する -：該当しない

注※ 1

WRED を指定した場合はログメッセージを表示しテールドロップで動作します。

注※ 2

Inbound で設定した場合，ディストリビューション送信キューに反映されます。以降の送信キューについては，Outbound へのフロー QoS 情報設定で対応してください。

表 1-43 NIF 種別と QoS 制御機能との対応 (2/2)【SB-5400S】

NIF 種別		機能					
		シェーパ					
		レガシーシェーパ				階層化シェーパ	キュー長指定
		ポート帯域制御	スケジューリング				
			PQ	RR	LLQ		
NF1G-6G		○	○	○	○	-	-
NF100-48TA		-	○	○	-※	-	-
NF1G-48T NF1G-32S NFMX-44		-	○	○	-※	-	-
NFMX-34	0～31ポート	-	○	○	-※	-	-
	32,33ポート	○	○	○	○	-	-

（凡例） ○：該当する -：該当しない

PQ：Priority Queuing（完全優先） RR：Round Robin（ラウンドロビン）

LLQ：Low Latency Queuing（LLQ ＋ 3WFQ）

注※ LLQ を指定した場合は，ログメッセージを表示し PQ で動作します。

1.10 QoS 制御機能とパケット中継方式との対応

QoS 制御機能は，パケット中継方式によってサポートする機能が異なります。QoS 制御機能とパケット中継方式の対応を次の表に示します。

表 1-44 QoS 制御機能とパケット中継方式との対応

QoS 制御機能			レイヤ 2 スイッチ中継		IPv4，IPv6 中継	
大項目	小項目		受信側	送信側	受信側	送信側
フロー検出	MAC ヘッダ	送信元 MAC アドレス	○	○	○	○※1
		宛先 MAC アドレス	○	○	○	○※1
		イーサネットタイプ	○	○	○	-
	Tag-VLAN ヘッダ	ユーザ優先度	○	○※2	○	○※3
		VLAN ID	○	○	○	○※4
	IP ヘッダ※5		○	○	○	○
	レイヤ 4 ヘッダ (TCP/UDP など)※5		○	○	○※6, ※7	○※6, ※7
帯域監視	違反時パケット廃棄		○	○	○	○
	違反時キューイング優先度変更		○	○	○	○
	違反時ユーザ優先度書き換え		○	○	○	○
	違反時 DSCP 値書き換え		○※8	-	○	○
マーカー	ユーザ優先度書き換え		○	○	○	○
	DSCP 書き換え		○※8	-	○	○
優先度指定			○	○	○	○
廃棄制御			-	○	-	○
シェーパ			-	○	-	○

(凡例) ○：サポート　-：未サポート

注※1

特定の MAC アドレスのフロー検出は未サポートです。すべての MAC アドレスをフロー検出すること (コンフィグレーションコマンド flow qos での MAC アドレスに any と指定) ができます。

注※2

レイヤ 2 スイッチ中継で，送信側でのユーザ優先度で検出を指定したときは，次のようになります。

- 受信側で VLAN-Tag 無しフレームを受信した場合
  受信側でユーザ優先度の書き換えを実施しなかった場合は，ユーザ優先度 0 で検出します。
  受信側でユーザ優先度の書き換えを実施した場合は，受信側で書き換えたユーザ優先度で検出します。
- 受信側で VLAN-Tag 付きフレームを受信した場合
  受信側でユーザ優先度の書き換えを実施しなかった場合は，受信時のユーザ優先度で検出します。
  受信側でユーザ優先度の書き換えを実施した場合は，受信側で書き換えたユーザ優先度で検出します。

注※3

IPv4，IPv6 中継で，送信側でユーザ優先度のフロー検出を指定したときは，次のようになります。

- 受信側でユーザ優先度の書き換えを実施しなかった場合は，ユーザ優先度 0 で検出します。
- 受信側でユーザ優先度の書き換えを実施した場合は，受信側で書き換えたユーザ優先度で検出します。

注※4

インタフェース名指定で，Tag-VLAN 連携回線の場合，VLAN ID で QoS 制御可能です。この場合，VLAN ID をフロー検出条件として指定する必要はありません。Tag-VLAN 連携回線以外のインタフェースおよび物理ポートでは，未サポートです。

注※ 5

Tag-VLAN ヘッダが 2 個までの場合です。3 個以上の場合は未サポートです。

注※ 6

2 番目以降のフラグメントパケットは未サポートです。詳細は，「1.11.5　フラグメントパケットの注意事項」を参照してください。

注※ 7

暗号ペイロードオプションまたは認証オプションが付加されているパケットは未サポートです。また，暗号ペイロードオプションまたは認証オプション以外の拡張ヘッダ付きパケットの場合は，本装置で「パケットのレイヤ 4 ヘッダが見える，見えない」でソフトウェア中継，ハードウェア中継が選択されます。詳細は，「1.11.4　IPv6 パケットをレイヤ 4 ヘッダ検出条件でフロー検出する場合の注意事項」を参照してください。

注※ 8

IP ヘッダが不正，または IPv4 オプションヘッダがある場合，DSCP 値書き換えは未サポートです。

1.11 QoS 制御使用時の注意事項

1.11.1 優先度設定時の注意点

1. 双方向通信を行うときに，シェーパのスケジューリングとして完全優先を選択した場合は，両方向のフローに対して優先度の設定をする必要があります。
2. 出力優先度およびキューイング優先度は，本装置から出力されるパケットだけが有効です。このため，入力側で検索条件に一致したパケットに出力優先度およびキューイング優先度の書き換えを指定した場合でも，本装置宛のプロトコル制御パケットでは，出力優先度およびキューイング優先度は書き換わりません。したがって，本装置宛のプロトコル制御パケットの本装置における処理優先度は変わりません。
3. リンクアグリゲーション，VLAN，リンクアグリゲーション内の Tag-VLAN 連携回線のインタフェース名に対して，優先度機能を使用する場合は，フロー検出したフローの出力先のすべてのポートを同じスケジューリングにしてください。

1.11.2 CP 処理負荷と QoS 制御の関係

収容条件以内で使用する場合，「図 1-28　通常のケース (収容条件以内で，性能範囲内での使用)」に示すような QoS 制御 (廃棄制御，シェーパなど) を行います。しかし，収容条件を超えた状況で CP に高負荷が発生した場合，「図 1-29　高負荷によるパケット廃棄発生で QoS 制御が機能しないケース」に示すように送信パケットが廃棄されて期待する QoS 制御結果が得られないケースがあります。

図 1-28　通常のケース (収容条件以内で，性能範囲内での使用)

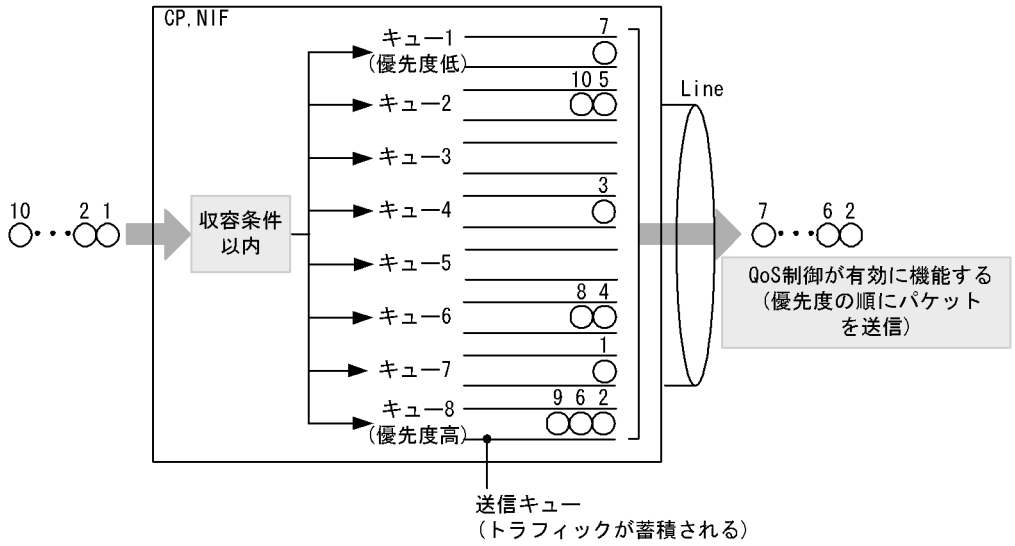
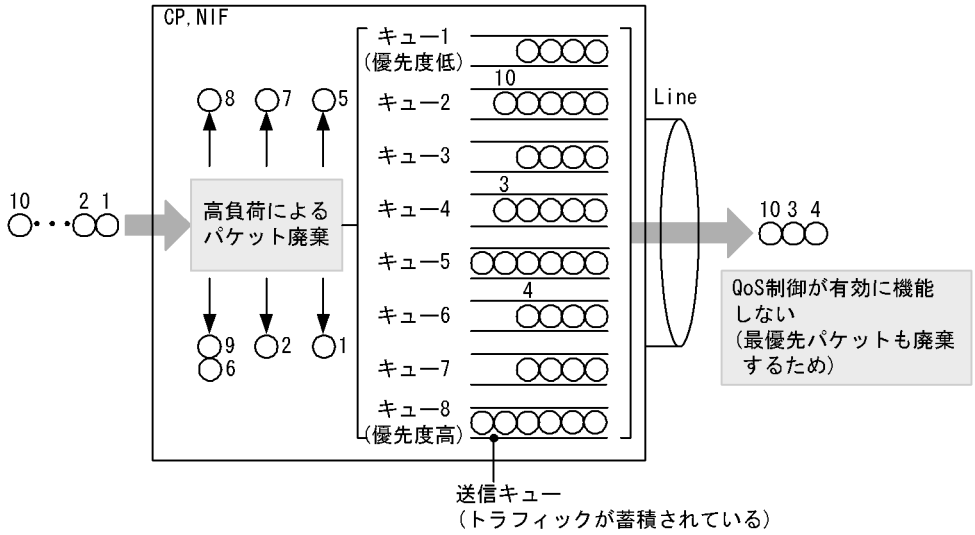


図 1-29 高負荷によるパケット廃棄発生で QoS 制御が機能しないケース



CP に高負荷が発生する要因を次に示します。これらの要因によって CP に高負荷が発生すると，QoS 制御が正常に機能しなくなる場合があるので注意してください。

- CP のソフトウェア処理によるもの
- IP フラグメントが多発する場合
- IP ヘッダオプションを利用したパケットを多数受信および中継する場合
- 収容条件を超えた状況で使用している場合

本装置の収容条件は，「解説書 Vol.1　3. 収容条件」を参照してください。

1.11.3 レイヤ 2 スイッチ中継での IPv4 オプション付きパケットをフロー検出する場合の注意事項

レイヤ 2 スイッチ中継で，IPv4 オプション付きパケットを受信し，フロー検出条件としてポート番号などのレイヤ 4 ヘッダ検出条件を設定している場合：

1. パケットのレイヤ 4 ヘッダが見えるとき（次の表を参照してください）
   ハードウェア処理によって QoS 制御を実行します。
2. パケットのレイヤ 4 ヘッダが見えないとき（次の表を参照してください）
   QoS 制御を行わずに受信パケットを中継します。

表 1-45 受信側でのレイヤ 4 ヘッダ判別可否パターン

受信パケット			レイヤ 4 ヘッダ内のフィールド	
レイヤ 3 ヘッダ	レイヤ 2 ヘッダ		TCP/UDP ※1 ICMP/IGMP ※2	TCP CODEBIT
IPv4 オプションなし	POS【SB-7800S】		○	○
	Ethernet V2	Tag なし	○	○
		Tag 付き (Tag 数 1)	○	○
		Tag 付き (Tag 数 2)	○	○
	IEEE802.3	Tag なし	○	○

受信パケット			レイヤ 4 ヘッダ内のフィールド	
レイヤ 3 ヘッダ	レイヤ 2 ヘッダ		TCP/UDP ※ 1 ICMP/IGMP ※ 2	TCP CODEBIT
		Tag 付き (Tag 数 1)	○	○
		Tag 付き (Tag 数 2)	○	○
IPv4 オプションあり	POS【SB-7800S】		○	×
(8byte 以下)	Ethernet V2	Tag なし	○	×
		Tag 付き (Tag 数 1)	○	×
		Tag 付き (Tag 数 2)	○	×
	IEEE802.3	Tag なし	○	×
		Tag 付き (Tag 数 1)	○	×
		Tag 付き (Tag 数 2)	○	×
IPv4 オプションあり	POS【SB-7800S】		×	×
(9byte 以上)	Ethernet V2	Tag なし	×	×
		Tag 付き (Tag 数 1)	×	×
		Tag 付き (Tag 数 2)	×	×
	IEEE802.3	Tag なし	×	×
		Tag 付き (Tag 数 1)	×	×
		Tag 付き (Tag 数 2)	×	×

(凡例) ○ : 該当フィールドの検出可　× : 該当フィールドの検出不可
注※ 1　: 送信元ポート番号 , 宛先ポート番号
注※ 2　: Type,Code

表 1-46　送信側でのレイヤ 4 ヘッダ判別可否パターン

送信パケット			レイヤ 4 ヘッダ内のフィールド	
レイヤ 3 ヘッダ	レイヤ 2 ヘッダ		TCP/UDP ※ 1 ICMP/IGMP ※ 2	TCP CODEBIT
IPv4 オプションなし	POS【SB-7800S】		○	○
	Ethernet V2	Tag なし	○	○
		Tag 付き (Tag 数 1)	○	○
		Tag 付き (Tag 数 2)	○	○
	IEEE802.3	Tag なし	○	○
		Tag 付き (Tag 数 1)	○	○
		Tag 付き (Tag 数 2)	○	○
IPv4 オプションあり	POS【SB-7800S】		○	×
(8byte 以下)	Ethernet V2	Tag なし	○	×
		Tag 付き (Tag 数 1)	○	×
		Tag 付き (Tag 数 2)	○	×
	IEEE802.3	Tag なし	○	×

送信パケット			レイヤ 4 ヘッダ内のフィールド	
レイヤ 3 ヘッダ	レイヤ 2 ヘッダ		TCP/UDP ※1 ICMP/IGMP ※2	TCP CODEBIT
		Tag 付き (Tag 数 1)	○	×
		Tag 付き (Tag 数 2)	○	×
IPv4 オプションあり (9byte 以上)	POS【SB-7800S】		×	×
	Ethernet V2	Tag なし	×	×
		Tag 付き (Tag 数 1)	×	×
		Tag 付き (Tag 数 2)	×	×
	IEEE802.3	Tag なし	×	×
		Tag 付き (Tag 数 1)	×	×
		Tag 付き (Tag 数 2)	×	×

(凡例) ○ : 該当フィールドの検出可　× : 該当フィールドの検出不可
注※ 1　: 送信元ポート番号 , 宛先ポート番号
注※ 2　: Type,Code

1.11.4 IPv6 パケットをレイヤ 4 ヘッダ検出条件でフロー検出する場合の注意事項

1. 暗号ペイロードオプションまたは認証オプションが付加されているパケットを受信した場合，ポート番号などのレイヤ 4 ヘッダ条件で検出することはできません。
2. 暗号ペイロードオプションまたは認証オプション以外の拡張ヘッダ付きパケットや，拡張ヘッダがないパケットを受信し，フィルタリングのフロー検出条件としてポート番号などのレイヤ 4 ヘッダ検出条件を設定している場合：
   1. パケットのレイヤ 4 ヘッダが見えるとき (次の表を参照してください)
      ハードウェア処理によって QoS 制御を実行します。
   2. パケットのレイヤ 4 ヘッダが見えないとき (次の表を参照してください)
      レイヤ 3 中継の場合は，ソフトウェア処理によってフィルタリングを実行します。レイヤ 2 スイッチ中継の場合は，フィルタリングで指定した動作を行わず，受信パケットを中継します。

表 1-47　受信側でのレイヤ 4 ヘッダ判別可否パターン

受信パケット			レイヤ 4 ヘッダ内のフィールド	
レイヤ 3 ヘッダ	レイヤ 2 ヘッダ		TCP/UDP ※1 ICMP/IGMP ※2	TCP CODEBIT
IPv6 拡張ヘッダなし	POS【SB-7800S】		○	○
	Ethernet V2	Tag なし	○	○
		Tag 付き (Tag 数 1)	○	○
		Tag 付き (Tag 数 2)	○	○
	IEEE802.3	Tag なし	○	○
		Tag 付き (Tag 数 1)	○	○
		Tag 付き (Tag 数 2)	○	○

受信パケット			レイヤ 4 ヘッダ内のフィールド	
レイヤ 3 ヘッダ	レイヤ 2 ヘッダ		TCP/UDP ※ 1 ICMP/IGMP ※ 2	TCP CODEBIT
IPv6 拡張ヘッダあり (拡張ヘッダ 8byte 以下)	POS【SB-7800S】		○	○
	Ethernet V2	Tag なし	○	○
		Tag 付き (Tag 数 1)	○	○
		Tag 付き (Tag 数 2)	○	○
	IEEE802.3	Tag なし	○	○
		Tag 付き (Tag 数 1)	○	○
		Tag 付き (Tag 数 2)	○	○
IPv6 拡張ヘッダあり (拡張ヘッダ 9byte 以上)	POS【SB-7800S】		×	×
	Ethernet V2	Tag なし	×	×
		Tag 付き (Tag 数 1)	×	×
		Tag 付き (Tag 数 2)	×	×
	IEEE802.3	Tag なし	×	×
		Tag 付き (Tag 数 1)	×	×
		Tag 付き (Tag 数 2)	×	×

(凡例) ○ : 該当フィールドの検出可　× : 該当フィールドの検出不可

注※ 1　: 送信元ポート番号 , 宛先ポート番号

注※ 2　: Type,Code

表 1-48　送信側でのレイヤ 4 ヘッダ判別可否パターン

送信パケット			レイヤ 4 ヘッダ内のフィールド	
レイヤ 3 ヘッダ	レイヤ 2 ヘッダ		TCP/UDP ※ 1 ICMP/IGMP ※ 2	TCP CODEBIT
IPv6 拡張ヘッダなし	POS【SB-7800S】		○	○
	Ethernet V2	Tag なし	○	○
		Tag 付き (Tag 数 1)	○	○
		Tag 付き (Tag 数 2)	○	○
	IEEE802.3	Tag なし	○	○
		Tag 付き (Tag 数 1)	○	○
		Tag 付き (Tag 数 2)	○	×
IPv6 拡張ヘッダあり (拡張ヘッダ 8byte 以下)	POS【SB-7800S】		○	○
	Ethernet V2	Tag なし	○	○
		Tag 付き (Tag 数 1)	○	○
		Tag 付き (Tag 数 2)	○	×
	IEEE802.3	Tag なし	○	×

送信パケット			レイヤ 4 ヘッダ内のフィールド	
レイヤ 3 ヘッダ	レイヤ 2 ヘッダ		TCP/UDP ※1 ICMP/IGMP ※2	TCP CODEBIT
		Tag 付き (Tag 数 1)	○	×
		Tag 付き (Tag 数 2)	×	×
IPv6 拡張ヘッダあり (拡張ヘッダ 9byte 以上)	POS【SB-7800S】		×	×
	Ethernet V2	Tag なし	×	×
		Tag 付き (Tag 数 1)	×	×
		Tag 付き (Tag 数 2)	×	×
	IEEE802.3	Tag なし	×	×
		Tag 付き (Tag 数 1)	×	×
		Tag 付き (Tag 数 2)	×	×

(凡例) ○：該当フィールドの検出可　×：該当フィールドの検出不可

注※1　：送信元ポート番号 , 宛先ポート番号

注※2　：Type,Code

1.11.5　フラグメントパケットの注意事項

IP のフラグメントパケットを 4 層（TCP，UDP，ICMP，IGMP）のフロー検出条件にて QoS 制御を実施した場合，2 番目以降のフラグメントパケットはレイヤ 4 ヘッダがパケット内にないため，同じフロー検出条件では検出できません。フラグメントパケットを含めた QoS 制御を実施する場合は，フロー検出条件に L3 条件を指定するようにしてください。

1.11.6　帯域監視機能使用時の注意事項

1. 複数のフローで帯域監視機能を使用している場合，各フローで指定した監視帯域値の合計が，出力回線，または出力キューの帯域値以内となる様に，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. フロー検出条件オプション 1 機能を指定し，かつ入力側で QoS の帯域監視機能を運用している場合，本装置宛のプロトコル制御パケットも帯域監視対象となります。したがって，フロー検出条件オプション 1 指定時，本装置宛のプロトコル制御パケットも最大監視帯域違反として廃棄される場合があります。このため，フロー検出条件オプション 1 機能指定時は，本装置宛のプロトコル制御パケットを考慮した最大帯域を確保する必要があります。フロー検出条件オプション 1 機能指定時にフロー検出対象に加わるパケットについては，「1.3.1　フロー検出機能の運用について　(2) フロー検出条件オプション」を参照してください。
4. 最低帯域違反ペナルティによる出力優先度およびキューイング優先度は，本装置から出力されるパケットだけが有効です。このため，入力側で検索条件に一致したパケットに出力優先度およびキューイング優先度の書き換えを指定した場合でも，本装置宛のプロトコル制御パケットでは，最低帯域違反ペナルティによる出力優先度およびキューイング優先度は書き換わりません。したがって，本装置宛のプロトコル制御パケットの本装置における処理優先度は変わりません。

1.11.7 TCP パケットに対する契約帯域監視機能の使用

帯域監視によって契約帯域を超えるパケットを廃棄する，という設定をした場合には，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。TCP を使用したデータ系通信に対して帯域を制限したい場合は，「1.8 シェーパ」に示したシェーパ機能，「1.4.2 UPC-RED」に示した UPC-RED 機能を使用することをお勧めします。

上記機能を使用できず，帯域監視機能を使用する場合には，帯域監視の結果「パケットを廃棄する」ではなく，「パケット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」ようにしてください。このモードにすると，契約帯域を超えてもすぐ廃棄されず，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。

1.11.8 レガシーシェーパ機能使用時の注意事項

リンクアグリゲーション，VLAN，リンクアグリゲーション内の Tag-VLAN 連携回線に属するポートに対してスケジューリングを設定する場合は，該当インタフェースに属するすべてのポートを同じスケジューリングにしてください。

1.11.9 階層化シェーパを使用する上での注意点【SB-7800S】

1. ARP などの制御系パケットの送信時や回線テストの実施時には，デフォルトのアグリゲートキューを使用します。したがって，階層化シェーパ機能を設定した物理回線のデフォルトアグリゲートキューに帯域を割り当てるように設定してください。

1.11.10 フロー QoS 統計情報の表示について

下記条件を満たすコンフィグレーション flow qos を指定した物理ポートまたはインタフェースが，show vlan コマンドでの Port Information の表示において Blocking 状態の場合，最大帯域違反したパケットのフロー QoS 統計情報は採取されません。

- 条件 1
  フロー検出条件オプション 1 を指定
- 条件 2
  コンフィグレーション flow qos で EAPOL，LACP，BPDU，CDP，OADP，LLDP，GSRP のパケットをフロー検出して最大帯域監視を設定

2 Diff-serv 機能

Diff-serv 機能は IP ネットワーク上の QoS 制御技術の一つです。この章では Diff-serv 機能について説明します。

2.1 Diff-serv 概説

2.1.1 Diff-serv の機能

Diff-serv(Differentiated Services) 機能は，IP ネットワーク上の QoS 制御技術の一つです。従来の QoS 技術はパケットの TCP/IP ヘッダからフローを検出して優先度を決定していましたが，この技術ではインターネットのバックボーンのように多数のユーザのフローが集中する大規模な IP ネットワークには適用できませんでした。しかし，Diff-serv 機能を使用すれば，ネットワークの境界ルータで設定した条件に一致する IP フローを検出し，このフローの IP ヘッダ内 DS Field の上位 6 ビットである DSCP(Differentiated Services Code Point) に，ドメイン内で行う制御の内容をビットパターンとして集約し転送します。後続のルータは，DSCP だけを参照して優先制御などを行うため，高速にパケット転送を行うことができます。このようなシンプルなアーキテクチャを使用し，ISP での契約サービスの差別化や，各種アプリケーションのサービスの差別化など，ポリシーベースのサービスを行えます。

（1） Diff-serv のネットワークモデル

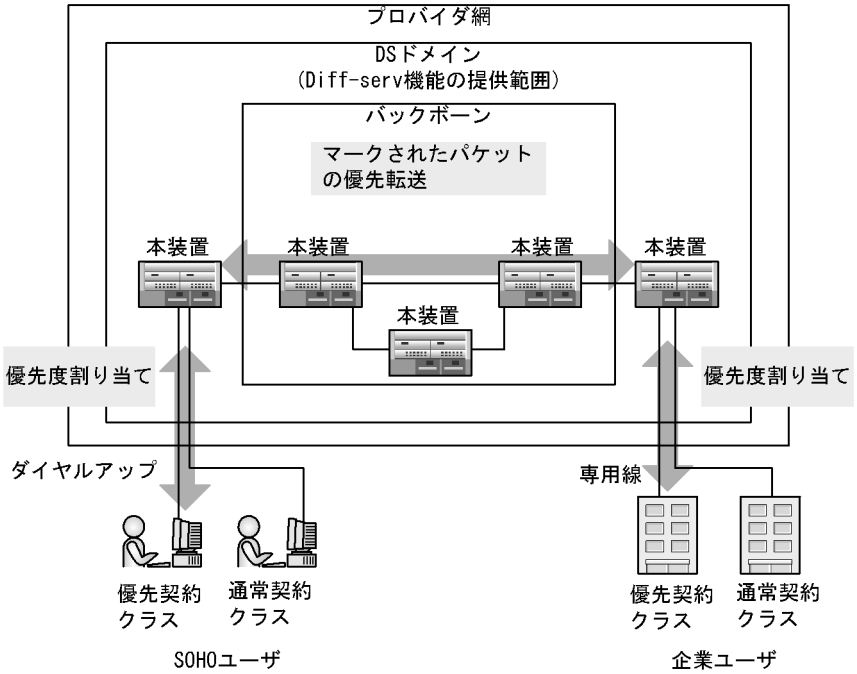
Diff-serv 機能を使用するネットワークを **DS ドメイン**と呼びます。この DS ドメインは境界に位置する**バウンダリノード**とコアに位置する**インテリアノード**から構成されます。フロー数が少なく回線速度が比較的低速のバウンダリノードは Diff-serv 機能の全機能を備えています。一方，高速で多数のフロー数を抱えるインテリアノードは簡易な機能を備えます。

バウンダリノードはネットワークの境界ルータに当たり，フローを識別して DSCP へ集約して DSCP に基づいて転送動作を行います。ここでバウンダリノードがパケットに対して行うマーキングを**ネットワークマーキング**と呼びます。また，ユーザがあらかじめパケットに DSCP を付けて転送する場合は，バウンダリノードが契約帯域の監視および送信制御だけを行います。この，ユーザがあらかじめパケットに対して行うマーキングを**ユーザマーキング**と呼びます。

インテリアノードはネットワークのバックボーンのルータに当たり，DSCP に基づいた転送動作だけを行います。この優先転送動作を，PHB(Per Hop Behavior) と呼びます。

Diff-serv 機能の概要を次の図に示します。

図 2-1　Diff-serv 機能の概要



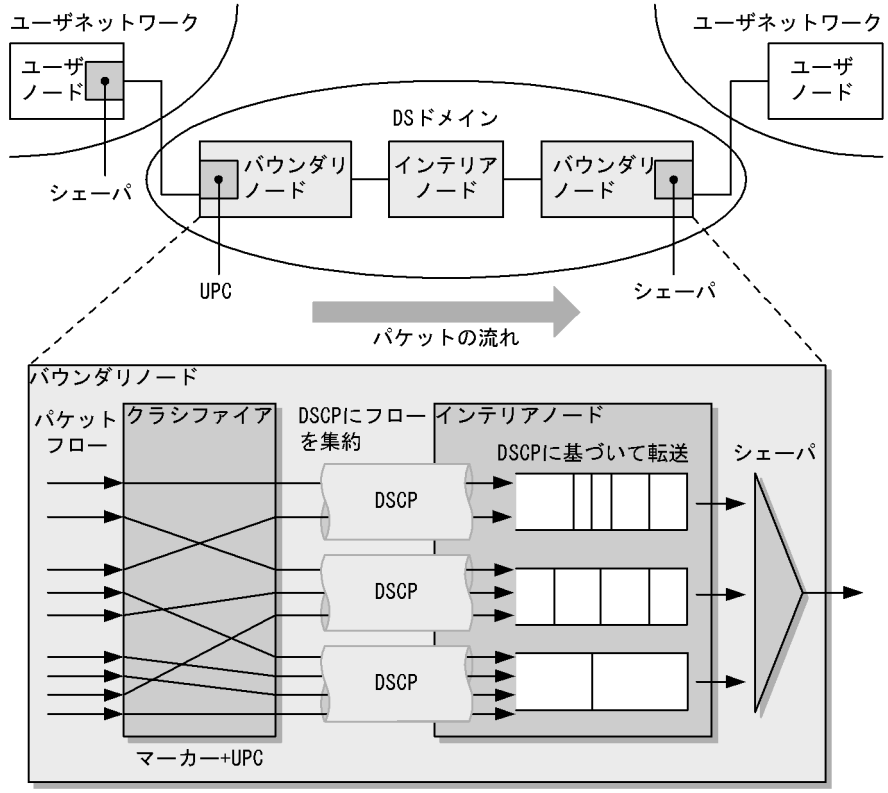
(2) バウンダリノードおよびインテリアノードの機能

バウンダリノードおよびインテリアノードでの，Diff-serv の機能について説明します。

- バウンダリノードの機能
  TCP/IP ヘッダからフローを識別し，個々のユーザとの契約に基づいて DSCP へ分類・集約する**クラシファイア**，IP ヘッダの DS フィールドに DSCP 値を書き込む**マーカー**，ユーザとの契約帯域を DSCP ごとに監視する UPC，送信帯域を制御する**シェーパ**機能があります。
- インテリアノードの機能
  インテリアノードはパケットヘッダ内の DSCP に基づいて優先転送だけを行います。

バウンダリノードおよびインテリアノードの機能を次の図に示します。

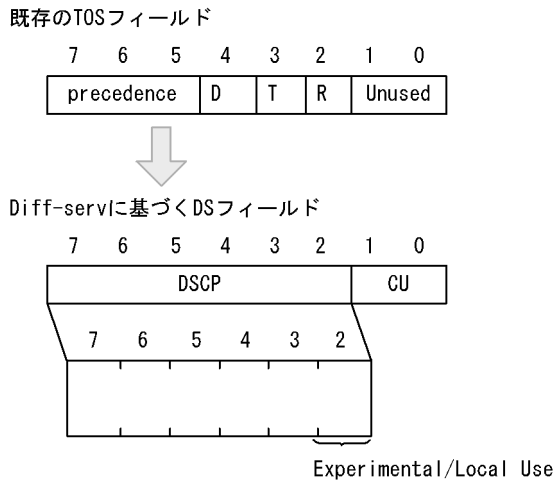
図 2-2 バウンダリノードおよびインテリアノードの機能



(3) DS フィールドと DSCP

Diff-serv では，既存の IP ヘッダ内の TOS フィールドを DS フィールドとして再定義しています。既存の TOS フィールドのフォーマットと，Diff-serv で使用する DS フィールドのフォーマットを次の図に示します。

図 2-3 TOS フィールドと DS フィールド



（凡例） D : Delay
T : Throughput
R : Reliability
DSCP : Differentiated Services Code Point
CU : Current Unused

Diff-serv の DSCP は，6 ビットのフィールドを持っていますが，最下位ビットは，RFC で Experimental/Local Use と規定しています。また，DSCP 値の上位 3 ビットを Class selector として使用することで，既存の TOS フィールドとの互換性を取っています。

（4） Diff-serv の導入手順

Diff-serv の導入時に必要な情報について概要を示します。DS ドメイン内には，バウンダリノードとインテリアノードの 2 種類のルータがあります。DS ドメイン内で一貫したサービスを行うためには，次に示す項目を決定する必要があります。

- STEP1
  バウンダリノードでは次の項目を決定します。
  - DS ドメイン内の DSCP と転送動作の対応づけ
  - 各ルータの転送動作
  - 各出力インタフェースの優先制御方法

  インテリアノードでは，DS ドメイン内の DSCP と転送動作の対応づけを決定します。これらの決定項目は DS ドメイン全体に対するものです。
- STEP2
  バウンダリノードでは各フローの DSCP との対応づけと帯域制御を決定します。これは，ユーザごとに決定します。インテリアノードでは決定する項目はありません。

2.1.2 Diff-serv の QoS サービス

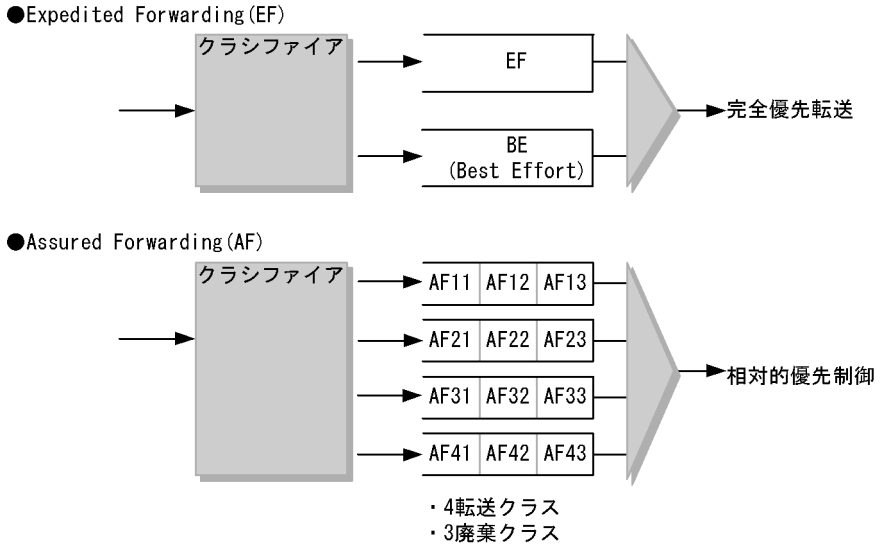
Diff-serv 機能が目標とする QoS サービスは，PHB と対応して標準化されています。Diff-serv の目標とする QoS サービスを次の表に示します。

表 2-1 Diff-serv の目標とする QoS サービス

サービス	特長	説明	対応する PHB
仮想専用線サービス	固定帯域保証	仮想専用線サービスの実現を目標とし，EF の DSCP を持ったパケットを他 DSCP のパケットより優先して転送し，固定帯域を保証します。	Expedited Forwarding (EF) 完全優先転送 (RFC 2598)
オリンピックサービス	相対的 QoS	オリンピックサービスの実現を目標とし，金，銀，銅の 3 種類のクラスを持ち，クラス間で相対的な QoS サービスを使用できます。	Assured Forwarding (AF) 相対的優先転送 (RFC 2597)

Diff-serv の目標とする QoS サービスを次の図に示します。

図 2-4 Diff-serv の目標とする QoS サービス



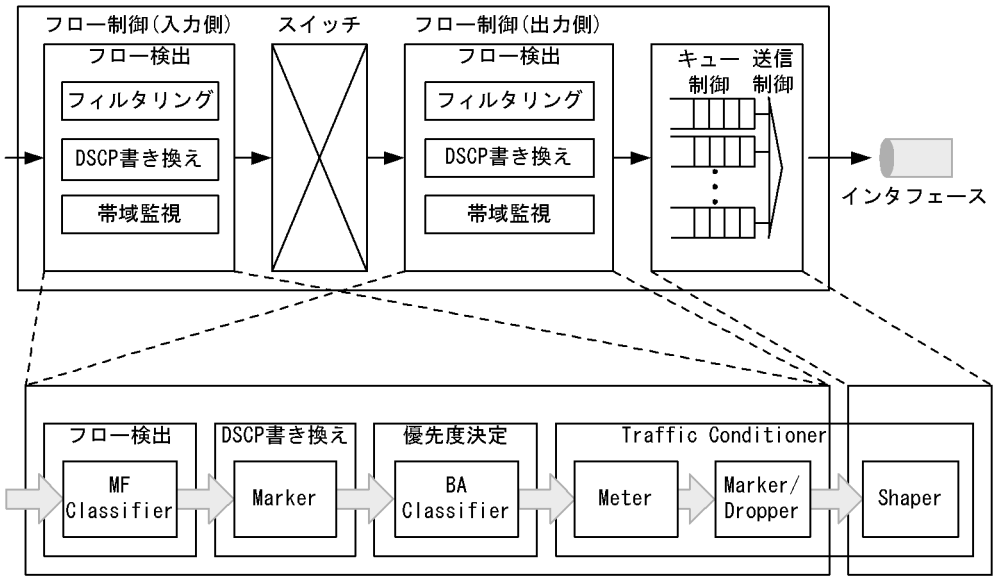
2.1.3 Diff-serv の制御仕様

本装置の Diff-serv の制御仕様は，RFC2475 に準拠しており，対象プロトコルは IP です。

2.2 Diff-serv の機能ブロック

本装置の Diff-serv の機能は，「1.2 QoS 制御構造」で示した，フロー制御，キュー制御，送信制御の 3 ブロックを使用して実現します。これらのブロックの内 RFC で Diff-serv ノードの必要機能として規定している MF Classifier(Multi Field Classifier)，Marker，BA Classifier(Behavior Aggregate Classifier)，Meter，Dropper は，フロー制御ブロックで，Shaper はキュー制御ブロックと送信制御ブロックで制御します。また，キュー制御および送信制御は，PHB(Per Hop Behavior) を決定します。本装置の Diff-serv 機能ブロックを次の図に示します。

図 2-5 本装置の Diff-serv 機能ブロック



各機能ブロックの説明を次の表に示します。

表 2-2 各機能ブロックの説明

機能ブロック		機能
MF Classifier		コンフィグレーションで指定するフロー識別条件によって IP フローの検出を行います。
Marker		MF Classifier で検出した IP フローのすべてのパケットに対して，コンフィグレーションで指定した DSCP 値のマーキングを行います。
BA Classifier		入力パケットの DSCP 値によって，出力優先度とキューイング優先度を決定します。
TrafficConditioner	Meter	IP フロー単位または DSCP 単位に使用している帯域の監視を行い，使用中の帯域を Marker，Shaper，Dropper に通知します。
	Marker	違反帯域のパケットに対して，コンフィグレーションで指定した DSCP 値のマーキングを再度行います。
	Dropper Shaper	Meter から通知される使用中帯域の状態に基づいて，違反帯域のパケットに対して帯域の調整動作を行います。

2.2.1 フロー制御

フロー制御は入力側と出力側の 2 か所で行います。

（1） MF Classifier(Multi Field Classifier)

MF Classifier は，あらかじめコンフィグレーションで指定された条件で IP フローを検出します。コンフィグレーションで指定できる IP フローの識別条件と指定方法については，「1.3　フロー検出」を参照してください。

（2） Marker

Marker は，MF Classifier で検出した IP フローの 6 ビットの DS フィールドを書き換えます。また，帯域監視中の違反パケットに対するペナルティ動作としても DS フィールドを書き換えます。

（3） BA Classifier(Behavior aggregate Classifier)

BA Classifier は，入力インタフェースからのパケットか，装置内の Marker によってマーキングされたパケットの DS フィールドの値によって出力優先度とキューイング優先度を決定します。

（4） Traffic Conditioner

Traffic Conditioner には Meter，Marker，Shaper，Dropper の機能があります。これらの機能は，IP フローの帯域を監視して，違反帯域のパケットに対して帯域の調整動作を行います。具体的な調整動作を次に示します。

● Meter
IP フローの帯域を監視し，現在使用中の帯域を Marker，shaper，Dropper に通知します。

● Marker，Dropper
Meter から通知される現在使用中の帯域に対して，コンフィグレーションで設定した契約帯域以上のフローを受信したときに調整動作を行います。

● Shaper
帯域分配などの送信制御を行います。詳細は，「1.8　シェーパ」を参照してください。

中継動作はあらかじめコンフィグレーションで設定しておきます。

- パケットを廃棄する。
- パケットの優先度を下げるために DSCP 値に変更する。
- パケットのキューイング優先度に変更する。

Traffic Conditioner の帯域監視は，コンフィグレーションで設定する監視帯域レートによって，監視時間が一意に決まります。このため，契約帯域に違反したフローは出力が契約帯域以下になる場合があります。

2.2.2　キュー制御

「1.7　廃棄制御」を参照してください。

2.2.3　送信制御

「1.8　シェーパ」を参照してください。

2.2.4　機能ブロックとコンフィグレーションコマンドの対応

本装置で Diff-serv を行うには，QoS フロー情報を使用して各機能ブロックに情報を設定します。機能ブロックに対応するコンフィグレーションコマンドを次の表に示します。

表 2-3 機能ブロックに対応するコンフィグレーションコマンド

Diff-serv の機能ブロック		本装置のコンフィグレーションコマンド	
ブロック名称	機能	エントリ名称	パラメータ名称
MFClassifier	フロー検出	flow qos	{ip | <protocol No.> | tcp | udp | icmp | igmp |icmp6}
			upper <Length>
			lower <Length>
			dscp <DSCP>
			<IP_Source>
			<IP_Destination>
			<Port_Source>
			<Port_Destination>
			<ICMP_Type>
			<ICMP_Code>
			<IGMP_Type>
Marker	DSCP マーキング		replace_dscp <DSCP>
	DSCP マッピング		dscp_map
BA Classifier	フロー検出		dscp
	優先クラス決定		priority <Level>
			discard <Level>
Meter/Dropper	違反検出		max_rate
			min_rate
	違反パケットへの対応		penalty_discard <Level.>
			penalty_dscp <DSCP.>
Shaper	送信制御	qos-queue-list	priority
			round_robin
			llq+3wfq
		shaper	priority
			llq+3wfq
			2llq+2wfq
			4wfq

DSCP 値と各クラスのマッピング例を次の図に示します。

図 2-6　DSCP 値と各クラスのマッピング例

	出力優先度	高 ← キューイング優先度 → 低			
		Discard クラス4	Discard クラス3	Discard クラス2	Discard クラス1
高	Priorityクラス8				
	Priorityクラス7				
	Priorityクラス6				101110
					46
	Priorityクラス5	100010	100100	100110	
		34	36	38	
	Priorityクラス4	011010	011100	011110	
		26	28	30	
	Priorityクラス3	010010	010100	010110	
		18	20	22	
	Priorityクラス2	001010	001100	001110	
		10	12	14	
低	Priorityクラス1	000000			
		0			

（凡例）

DSCP値(2進数)
DSCP値(10進数)

□：EFの推奨値　　■：Best Effortの推奨値

■：AFの推奨値

注1　出力優先度が大きいほど，パケットを優先的に送出する。
注2　キューイング優先度が高いパケットほど廃棄しない。

2.3 コンフィグレーション作成時の注意事項

本装置は，「表 2-3 機能ブロックに対応するコンフィグレーションコマンド」で示したように，QoS 情報のコンフィグレーションコマンドによって Diff-serv に対応できます。

2.3.1 コンフィグレーション作成パターン

QoS 情報の Diff-serv の代表的な設定パターンを次に示します。

- パターン 1：ネットワークマーキングでの入力側バウンダリノード
- パターン 2：ユーザマーキングでの入力側バウンダリノード
- パターン 3：インテリアノードおよび出力側バウンダリノード

Diff-serv のコンフィグレーション作成パターンを次の表に示します。

表 2-4 Diff-serv のコンフィグレーション作成パターン

定義パターン	inbound					outbound
	MF	Marker	BA	Meter	Dropper	
パターン 1	Q	Q	Q	Q	Q	-
パターン 2	-	-	Q	Q	Q	-
パターン 3	-	-	Q	-	-	-

（凡例） Q：flow qos で定義する -：規格外である

Diff-serv のコンフィグレーションを行う場合は，フローに対して Inbound 側の各エントリを使用しますが，次の場合は，Outbound 側エントリを使用してください。

- Outbound 側でユーザごとに QoS 制御する場合

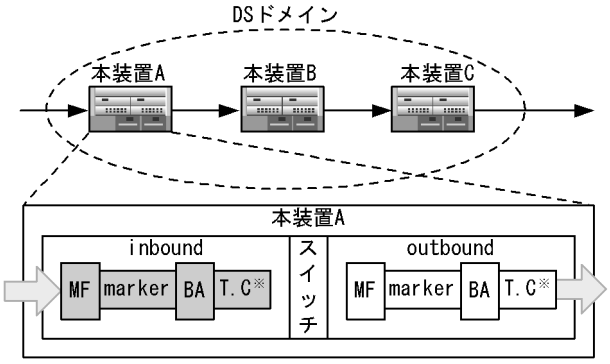
2.3.2 適用例

設定パターンごとの DS ドメイン内の本装置の位置づけと想定される適用例を，次に示します。

（1） パターン 1 の適用例

ネットワークマーキングを行うときの入力側バウンダリノードで，DS ドメイン外からのフローに対して対応する DSCP をマーキングし，マーキングした単位に帯域監視を行う場合に，パターン 1 を使用します。本装置の位置づけと適用例を次の図に示します。

図 2-7 本装置の位置づけと適用例 (パターン 1)

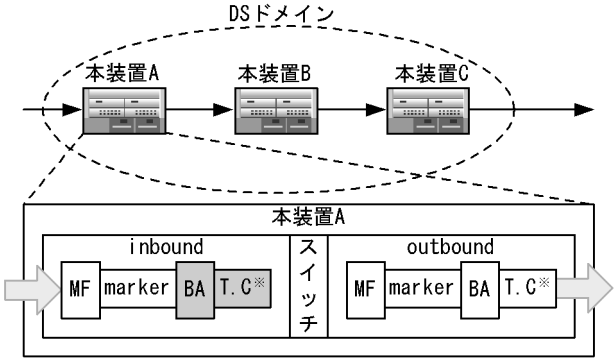


注※ T.C : Traffic Conditioner

(2) パターン 2 の適用例

ユーザマーキングを行うときの入力側バウンダリノードで，DSCP 単位に帯域監視を行う場合に，パターン 2 を使用します。また，ネットワークマーキングで DSCP のマーキングを行わない場合もこのパターンを使用します。本装置の位置づけと適用例を次の図に示します。

図 2-8 本装置の位置づけと適用例 (パターン 2)

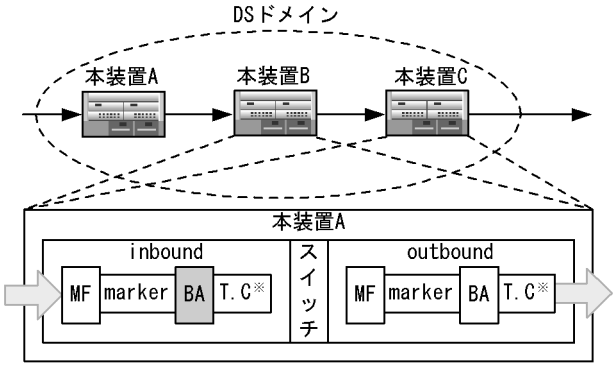


注※ T.C : Traffic Conditioner

(3) パターン 3 の適用例

ユーザマーキングを行うときの入力側バウンダリノードで，DSCP 単位に帯域監視を行う場合に，パターン 3 を使用します。また，ネットワークマーキングで DSCP のマーキングを行わない場合もこのパターンを使用します。本装置の位置づけと適用例を次の図に示します。

図 2-9　本装置の位置づけと適用例 (パターン 3)



注※　T.C：Traffic Conditioner

3 IEEE 802.1X

IEEE 802.1X は OSI 階層モデルの第 2 レイヤで認証を行う機能です。この章では IEEE 802.1X の概要について説明します。

3.1 IEEE 802.1X 概説

IEEE 802.1X は，不正な LAN 接続を規制する機能です。バックエンドに認証サーバ (一般的には RADIUS サーバ) を設置し，認証サーバによる端末の認証が通過した上で，本装置の提供するサービスを利用可能にします。

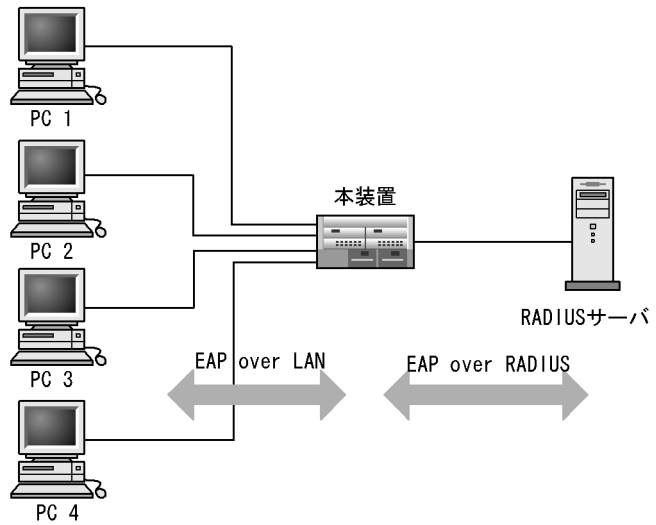
IEEE 802.1X の構成要素と動作概略を次の表に示します。

表 3-1 構成要素と動作概略

構成要素	動作概略
本装置 (Authenticator)	端末の LAN へのアクセスを制御します。また，端末と認証サーバ間で認証情報のリレーを行います。端末と本装置間の認証処理に関わる通信は EAP Over LAN(EAPOL) で行います。本装置と認証サーバ間は EAP Over RADIUS を使って認証情報を交換します。なお，本章では，「本装置」または「Authenticator」と表記されている場合，本装置自身と本装置に搭載されている Authenticator ソフトウェアの両方を意味します。
端末 (Supplicant)	EAPOL を使用して端末の認証情報を本装置とやりとりします。なお，本章では，「端末」または「Supplicant」と表記されている場合，端末自身と端末に搭載されている Supplicant ソフトウェアの両方を意味します。「Supplicant ソフトウェア」と表記されている場合，Supplicant 機能を持つソフトウェアだけを意味します。
認証サーバ (Authentication Server)	端末の認証を行います。認証サーバは端末の認証情報を確認し，本装置の提供するサービスへのアクセスを要求元の端末に許可すべきかどうかを本装置に通知します。

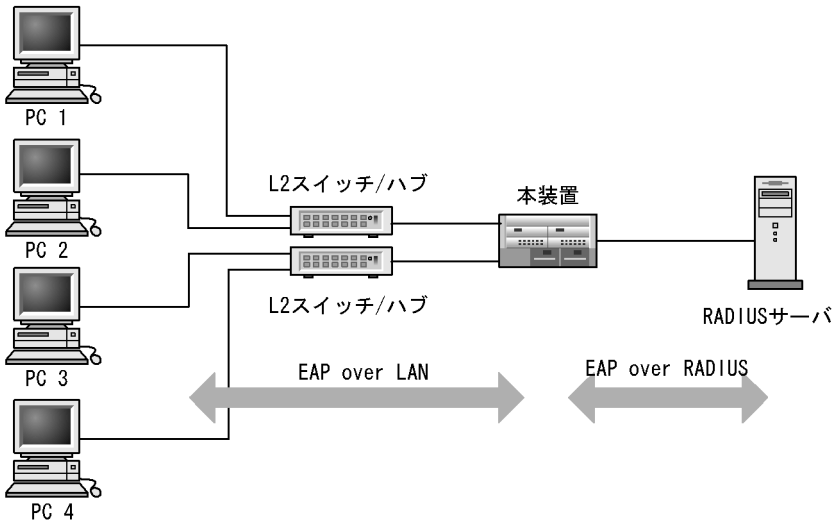
標準的な IEEE 802.1X の構成では，本装置のポートに直接端末を接続して運用します。本装置を使った IEEE 802.1X 基本構成を次の図に示します。

図 3-1 IEEE 802.1X 基本構成



また，本装置では一つのポートで複数の端末の認証を行う拡張機能をサポートしています (マルチモードおよび端末認証モード)。本拡張機能を使用した場合，端末と本装置間に L2 スイッチやハブを配置することにより，ポート数によって端末数が制限を受けない構成が可能です。本構成を行う場合，端末と本装置間に配置する L2 スイッチは EAPOL を透過する必要があります。その場合の構成を次の図に示します。

図 3-2　端末との間に L2 スイッチを配置した IEEE 802.1X 構成



3.2 サポート機能

サポートする機能を以下に示します。

(1) 認証動作モード

本装置でサポートする認証動作モード(PAE モード)は Authenticator です。本装置が Supplicant として動作することはありません。

(2) 認証方式

本装置でサポートする認証方式は RADIUS サーバ認証です。

端末から受信した EAPOL パケットを EAPoverRADIUS に変換し，認証処理は RADIUS サーバで行います。

RADIUS サーバは EAP 対応されている必要があります。

本装置が使用する RADIUS の属性名を次の表に示します。

表 3-2 認証で使用する属性名

属性名	type 値	解説	パケットタイプ
User-Name	1	認証されるユーザ名。	Request
NAS-IP-Address	4	認証を要求している，Authenticator（本装置）の IP アドレス。 ローカルアドレスが設定されている場合はローカルアドレス，ローカルアドレスが設定されていない場合は送信インタフェースの IP アドレスになります。	Request
NAS-Port	5	Supplicant を認証している Authenticator の物理ポート番号を表す。	Request
Service-Type	6	提供するサービスタイプ。	Request Accept
Framed-MTU	12	Supplicant ～ Authenticator 間の最大フレームサイズ。	Request
Reply-Message	18	ユーザに表示されるメッセージ。	Challenge Accept Reject
State	24	Authenticator と RADIUS サーバ間の State 情報の保持を可能にする。	Request Challenge
Session-Timeout	27	Supplicant へ送信した EAP-Request に対する応答待ちタイムアウト値。	Challenge
Called-Station-Id	30	ブリッジやアクセスポイントの MAC アドレス。	Request
Calling-Station-Id	31	Supplicant の MAC アドレス（大文字 ASCII, "-" 区切り）。	Request
NAS-Identifier	32	Authenticator を識別する文字列。	Request
NAS-Port-Type	61	Authenticator がユーザ認証に使用している，物理ポートのタイプ。	Request
Tunnel-Type **【SB-7800S】**	64	トンネル・タイプ。VLAN 単位認証（動的）モードでだけ意味を持ち，VLAN(13) を設定。	Accept

属性名	type 値	解説	パケットタイプ
Tunnel-Medium-Type **【SB-7800S】**	65	トンネルを作成する際のプロトコル。 VLAN 単位認証（動的）モードでだけ意味を持ち，IEEE802(6) を設定。	Accept
Connect-Info	77	Supplicant のコネクションの特徴を示す。	Request
EAP-Message	79	EAP パケットをカプセル化する。	Request Challenge Accept Reject
Message-Authenticator	80	RADIUS/EAP パケットを保護するために使用する。	Request Challenge Accept Reject
Tunnel-Private-Group-ID **【SB-7800S】**	81	VLAN を識別する文字列。Accept 時は，認証済みの Supplicant に割り当てる VLAN を意味する。 VLAN 単位認証（動的）モードでだけ意味を持ち，次に示す文字列が対応する。 (1)VLAN ID を示す文字列 (2)"VLAN"+VLAN ID を示す文字列 文字列にスペースを含んではいけない（含めた場合 VLAN 割り当ては失敗する）。 （設定例） VLAN10 の場合 (1) の場合　"10" (2) の場合　"VLAN10"	Accept
Acct-Interim-Interval	85	Interim パケット送信間隔。	Accept
NAS-Port-Id	87	Supplicant を認証する Authenticator のポートを識別するために使用する。NAS-Port-Id は，可変長のストリングであり，NAS-Port が長さ 4 オクテットの整数値である点で NAS-Port と異なる。	Request

（3） 認証アルゴリズム

本装置でサポートする認証アルゴリズムを次の表に示します。

表 3-3　サポートする認証アルゴリズム

認証アルゴリズム	概要
EAP-MD5-Challenge	UserPassword とチャレンジ値の比較を行う。
EAP-TLS	証明書発行モジュールを使用した認証方式。
EAP-PEAP	EAP-TLS トンネル上で，他の EAP 認証アルゴリズムを用いて認証する。
EAP-TTLS	EAP-TLS トンネル上で，他方式（EAP，PAP，CHAP など）の認証アルゴリズムを用いて認証する。

（4） RADIUS Accounting 機能

本装置は RADIUS Accounting 機能をサポートします。この機能は IEEE 802.1X 認証にて認証許可となった端末へのサービス開始やサービス停止のタイミングでユーザアカウンティング情報を送信し，利用状況追跡を行えるようにするための機能です。RADIUS Authentication サーバと RADIUS Accounting サーバを別のサーバに設定することによって，認証処理とアカウンティング処理の負荷を分散させることができます。

RADIUS Accounting 機能を使用する際に，RADIUS サーバに送信される情報を次の表に示します。

表 3-4 RADIUS Accounting がサポートする属性

属性名	type 値	解説	アカウンティング要求種別による送信の有無		
			Start	Stop	Interim-Update
User-Name	1	認証されるユーザ名。	○	○	○
NAS-IP-Address	4	認証を要求している，Authenticator（本装置）の IP アドレス。 ローカルアドレスが設定されている場合はローカルアドレス，ローカルアドレスが設定されていない場合は，送信インタフェースの IP アドレスになります。	○	○	○
NAS-Port	5	Supplicant を認証している Authenticator の物理ポート番号を表す。	○	○	○
Service-Type	6	提供するサービスタイプ。	○	○	○
Calling-Station-Id	31	Supplicant の MAC アドレス (大文字 ASCII, "-" 区切り)。	○	○	○
NAS-Identifier	32	Authenticator を識別する文字列。	○	○	○
Acct-Status-Type	40	Accounting 要求種別 Start(1),Stop(2),Interim-Update(3)	○	○	○
Acct-Delay-Time	41	Accounting 情報送信遅延時間	○	○	○
Acct-Input-Octets	42	Accounting 情報 (受信オクテット数)。 0 固定。	-	○	○
Acct-Output-Octets	43	Accounting 情報 (送信オクテット数)。 0 固定。	-	○	○
Acct-Session-Id	44	Accounting 情報を識別する ID。	○	○	○
Acct-Authentic	45	認証方式 (RADIUS(1),Local(2),Remote(3))	○	○	○
Acct-Session-Time	46	Accounting 情報 (セッション持続時間)	-	○	○
Acct-Input-Packets	47	Accounting 情報 (受信パケット数)。 0 固定。	-	○	○
Acct-Output-Packets	48	Accounting 情報 (送信パケット数)。 0 固定。	-	○	○
Acct-Terminate-Cause	49	Accounting 情報 (セッション終了要因) 詳細は「表 3-5 Acct-Terminate-Cause での切断要因」を参照のこと。 (User Request (1), Lost Carrier (2), Admin Reset (6), Supplicant Restart (19), Reauthentication Failure (20), Port Reinitialized (21), Port Administratively Disabled(22))	-	○	-
NAS-Port-Type	61	Authenticator がユーザ認証に使用している，物理ポートのタイプ。	○	○	○

属性名	type 値	解説	アカウンティング要求種別による送信の有無		
			Start	Stop	Interim-Update
NAS-Port-Id	87	Supplicant を認証する Authenticator のポートを識別するために使用する。NAS-Port-Id は，可変長のストリングであり，NAS-Port が長さ 4 オクテットの整数値である点で NAS-Port と異なる。	○	○	○

（凡例） ○：送信する　-：送信しない

表 3-5　Acct-Terminate-Cause での切断要因

値	切断要因	解説
1	User Request	Supplicant からの要求で切断した。
2	Lost Carrier	モデムのキャリア信号がなくなった。
6	Admin Reset	管理者の意思で切断した。
19	Supplicant Restart	Supplicant のステートマシンが初期化された。
20	Reauthentication Failure	再認証失敗した。
21	Port Reinitialized	ポートの MAC が再初期化された。
22	Port Administratively Disabled	ポートが管理的に無効にされた。

3.3 拡張機能概要

本装置では，標準的な IEEE 802.1X に対して機能拡張を行っています。拡張機能の概要を以下に示します。

3.3.1 認証モード

本装置の IEEE 802.1X 機能では，三つの基本認証モードとその下に三種類の認証サブモードを設けています。基本認証モードは，認証制御を行う単位を示し，認証サブモードは認証のさせ方を指定します。また，基本認証モードと認証サブモードに対して設定可能なオプションを設けています。各認証モードの関係を次の表に示します。

表 3-6 認証モードとオプションの関係

基本認証モード	認証サブモード	認証オプション
ポート単位認証	シングルモード	-
	マルチモード	-
	端末認証モード	認証除外端末オプション
		認証端末数制限オプション
VLAN 単位認証（静的）	シングルモード	認証除外ポートオプション
	マルチモード	認証除外ポートオプション
	端末認証モード	認証除外端末オプション
		認証除外ポートオプション
		認証端末数制限オプション
VLAN 単位認証（動的） **【SB-7800S】**	端末認証モード	認証除外端末オプション
		認証端末数制限オプション

（凡例） -：該当なし

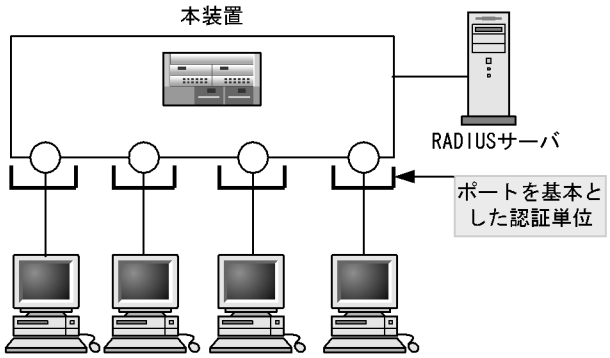
本装置の IEEE 802.1X 機能においては，リンクアグリゲーショングループについても一つの束ねられたポートとして扱います。この機能での「ポート」の表現には通常のポートとリンクアグリゲーショングループを含むものとします。

（1） 基本認証モード

本装置でサポートする基本認証モードを以下に示します。

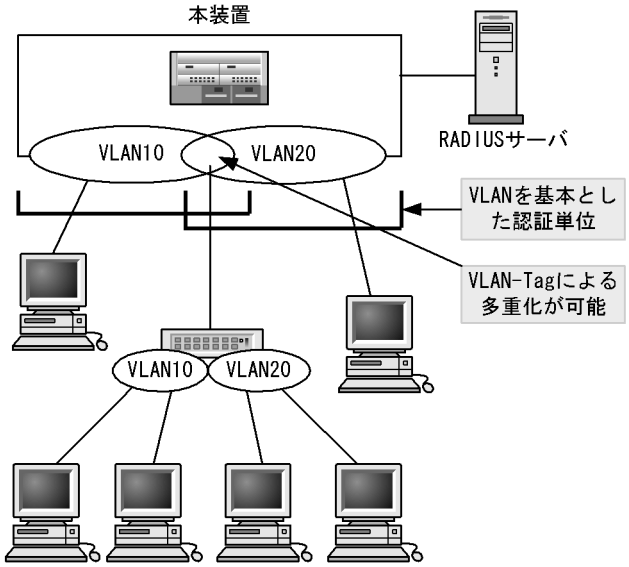
- ポート単位認証モード
  認証の制御を物理ポートもしくはリンクアグリゲーショングループに対して行います。IEEE 802.1X の標準的な認証単位です。この認証モードでは IEEE802.1Q VLAN-Tag の付与された EAPOL フレームを扱うことはできません。IEEE802.1Q VLAN-Tag の付与された EAPOL フレームを受信すると廃棄します。コンフィグレーションコマンド dot1x の port サブコマンドで設定します。
  ポート単位認証の動作イメージを次の図に示します。

図 3-3 ポート単位認証の動作イメージ



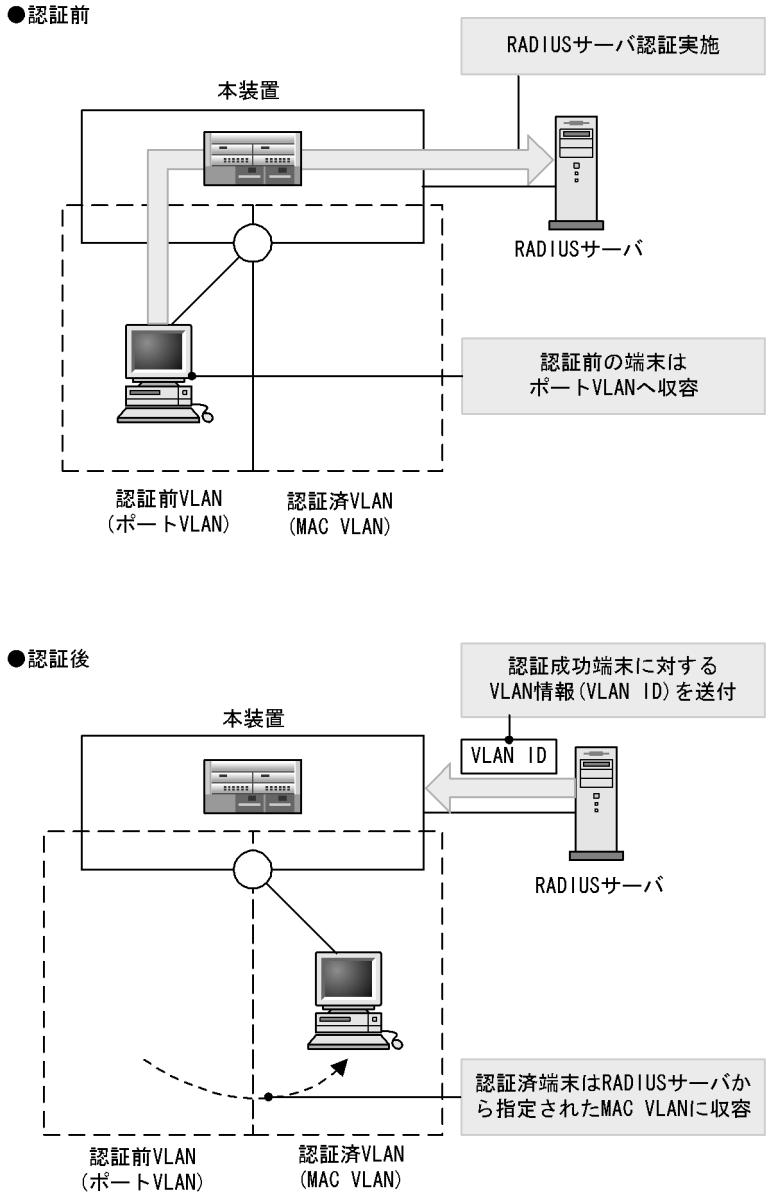
- VLAN 単位認証（静的）モード
  認証の制御を VLAN に対して行います。IEEE802.1Q VLAN-Tag の付与された EAPOL フレームを扱うことができます。端末と本装置の間に L2 スイッチを配置し，L2 スイッチを用いて IEEE802.1Q VLAN-Tag の付与を行う場合に使用します。Tag の付与されていない EAPOL については，ポートに Untagged で設定されている VLAN で受信したと認識します。コンフィグレーションコマンド dot1x の target-vlan サブコマンドで設定します。
  VLAN 単位認証（静的）の動作イメージを次の図に示します。

図 3-4 VLAN 単位認証（静的）の動作イメージ



- VLAN 単位認証（動的）モード**【SB-7800S】**
  認証の制御を MAC VLAN に所属する端末に対して行います。IEEE802.1Q VLAN-Tag の付与された EAPOL フレームを扱うことができません。このフレームを受信した場合破棄します。
  MAC VLAN に対応していない PSU ボードでは，本モードはサポートしません。
  指定された MAC VLAN の Untagged が動的認証対象となり，Tagged で設定された場合，認証除外ポートとして扱われます。
  認証に成功した端末は，認証サーバである RADIUS サーバからの VLAN 情報（MAC VLAN の VLANID）に従い，動的に VLAN の切り替えを行います。コンフィグレーションコマンド dot1x の target-vlan dynamic サブコマンドで設定します。
  VLAN 単位認証（動的）動作イメージを次の図に示します。

図 3-5 VLAN 単位認証（動的）の動作イメージ



(2) 認証サブモード

基本認証モードに対して設定する認証サブモードを以下に示します。

- シングルモード
  一つの認証単位内に一つの端末だけ認証して接続するモードです。IEEE 802.1X の標準的な認証モードです。最初の端末が認証している状態でほかの端末からの EAP を受信すると，そのポートの認証状態は未認証状態に戻り keep-unauth サブコマンドで指定された時間が経過した後に認証シーケンスの再開を行います。コンフィグレーションコマンド dot1x の access-control single サブコマンドで設定します。
- マルチモード
  一つの認証単位内に複数端末の接続を許容しますが，認証対象の端末はあくまで最初に EAP を受信した 1 端末だけのモードです。最初に認証を受けた端末の認証状態に応じて，その他の端末のパケットを疎通するかどうかが決まります。最初の端末が認証されている状態でほかの端末の EAP を受信すると

無視します。コンフィグレーションコマンド dot1x の access-control multi サブコマンドで設定します。

- 端末認証モード
  一つの認証単位内に複数端末の接続を許容し，端末ごと（送信元 MAC アドレスで識別）に認証を行うモードです。端末が認証されている状態でほかの端末の EAP を受信すると，EAP を送信した端末との間で個別の認証シーケンスが開始されます。コンフィグレーションコマンド dot1x の access-control supplicant サブコマンドで設定します。

（3） 認証モードオプション

認証モード／認証サブモードに対するオプション設定を以下に示します。

- 認証除外端末オプション
  スタティック MAC アドレス登録機能によって MAC アドレスが設定された端末については認証を不要とし，疎通を許可するオプション設定です。Supplicant 機能を持たないプリンタなどの装置やサーバの様な認証が不要な端末を，端末単位で認証対象から除外したいときに使用します。ポート単位認証および VLAN 単位認証（静的）では，コンフィグレーションコマンド fdb の static-entry サブコマンドで設定します。
  VLAN 単位認証（動的）では，コンフィグレーションコマンド vlan の mac-address サブコマンドで設定します。端末認証モードの場合だけ使用可能です。**【SB-7800S】**
- 認証除外ポートオプション
  特定の物理ポート番号もしくはリンクアグリゲーション ID を指定することで，その物理ポートもしくはリンクアグリゲーショングループ配下の端末については認証を不要とし，疎通を許可するオプション設定です。VLAN 単位認証（静的）モードを使用しているときに，認証対象となる VLAN の中に認証対象外としたいポートがある場合に使用します。コンフィグレーションコマンド dot1x の force-authorized-port サブコマンドで設定します。VLAN 単位認証（静的）モードの場合だけ使用可能です。
- 認証端末数制限オプション
  認証単位内に収容する最大認証端末数を制限するオプション設定です。コンフィグレーションコマンド dot1x の max-supplicant サブコマンドで設定します。端末認証モードだけで有効です。認証単位ごとの設定値を次の表に示します。

表 3-7　認証端末数制限オプション

認証モード	初期値	最小値	最大値
ポート単位認証	256	1	256
VLAN 単位認証（静的）	256	1	256
VLAN 単位認証（動的）	8,192	1	8,192

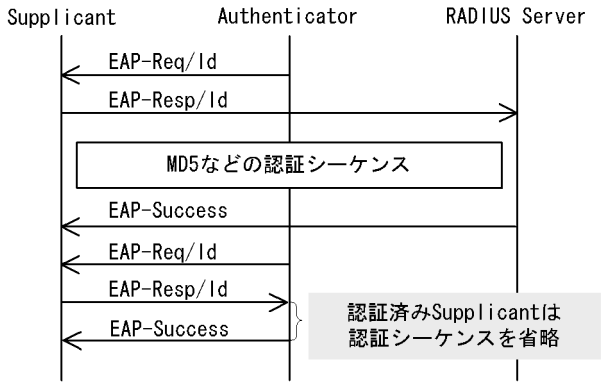
- 端末検出動作切り替えオプション
  端末の認証開始を誘発するために，本装置は tx-period サブコマンドで指定された間隔で EAP-Req/Id をマルチキャストで送信します。認証モードが端末認証モードの場合，認証単位に複数の端末が存在する可能性があるため，本装置ではすべての端末の認証が完了するまで EAP-Req/Id の送信を継続することをデフォルトの動作としています。このとき，認証単位当たりの端末数が増えると EAP-Req/Id に応答した端末の認証処理で装置に負荷を掛けるおそれがあるため，認証済み端末からの応答には認証シーケンスを一部省略することで，装置の負荷を軽減しています。
  ただし，使用する Supplicant ソフトウェアの種類によっては，認証シーケンスの省略によって認証済み端末の通信が途切れる問題が発生することがあります。そのため，認証済み端末に対する動作を切り替えるオプションを用意しています。本オプションは supplicant-detection サブコマンドで選択を行い，次に示す三種類の動作を指定できます。

- shortcut（認証済み端末に対する認証シーケンスを省略する：デフォルト）
- disable（認証済み端末が存在する場合は EAP-Req/Id の送信を停止する）
- full（認証済み端末に対する認証シーケンスを省略しない）

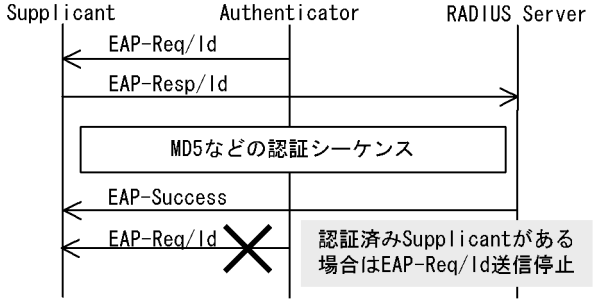
本オプションは端末認証モードだけで有効です。それぞれの動作シーケンスを次の図に示します。

図 3-6　shortcut，disable，full の EAP-Req/Id のシーケンス

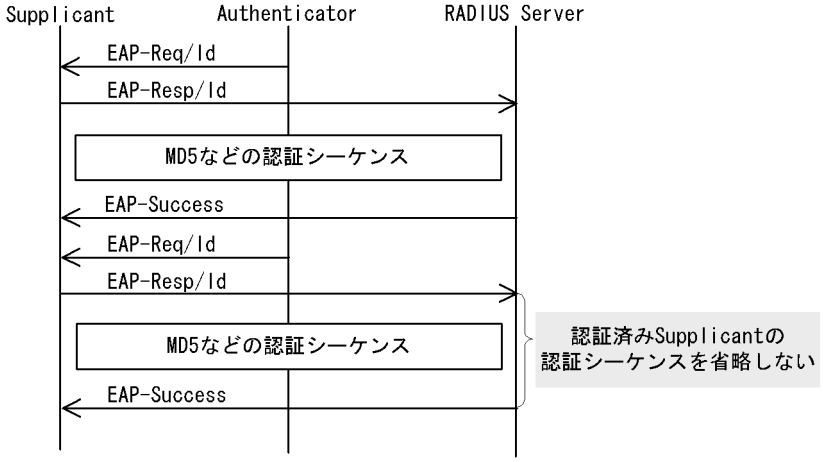
●shortcut指定時のシーケンス（デフォルト）



●disable指定時のシーケンス



●full指定時のシーケンス



3.3.2　端末要求再認証抑止機能

端末から送信される EAPOL-Start フレームを契機とする再認証処理を抑止する機能です。多数の端末か

ら短い間隔で再認証要求が行われるような場合に，再認証処理のために本装置の負荷が上昇するのを防ぎます。本設定が行われている場合，端末の再認証は本装置が reauth-period サブコマンドで指定された時間間隔で行う定期的な再認証処理で行われます。コンフィグレーションコマンド dot1x の ignore-eapol-start サブコマンドで設定します。

3.3.3 RADIUS サーバ接続機能

（1） RADIUS サーバとの接続

RADIUS サーバは最大四つまで指定でき，一つの RADIUS サーバとの接続に失敗したときは順次これらの RADIUS サーバとの接続を試みます。すべての RADIUS サーバとの接続に失敗した場合，端末に EAP-Failure を送信して認証処理を終了します。

プロトコル処理の途中で通信タイムアウトを検出した場合，いったん端末に EAP-Failure を送信し，認証処理を最初からやり直します。

IEEE 802.1X で使用する RADIUS サーバとの接続は，認証の対象外となっているポートを使用してください。

（2） VLAN 単位認証（動的）で VLAN を動的に割り当てるときの設定【SB-7800S】

SB-7800S でサポートする VLAN 単位認証（動的）で VLAN の動的割り当てを実施する場合，RADIUS サーバへ次に示す属性を設定する必要があります。

- Tunnel-Type
- Tunnel-Medium-Type
- Tunnel-Private-Group-Id

詳細については，「表 3-2　認証で使用する属性名」を参照してください。

（3） RADIUS サーバでの本装置の識別の設定

RADIUS プロトコルでは RADIUS クライアント（NAS）を識別するキーとして，要求パケットの送信元 IP アドレスを使用するよう規定されています。本装置では要求パケットの送信元 IP アドレスとして，次に示すアドレスを使用します。

- コンフィグレーションコマンド local-address によってローカルアドレスが設定されている場合は，ローカルアドレスを送信元 IP アドレスとして使用します。
- ローカルアドレスが設定されていない場合は，送信インタフェースの IP アドレスを使用します。

本装置にローカルアドレスが設定されている場合，RADIUS サーバに登録する本装置の IP アドレスとして，ローカルアドレスで指定した IP アドレスを指定してください。RADIUS サーバと通信する送信インタフェースが特定できない場合であっても，ローカルアドレスを設定することによって，RADIUS サーバに設定する本装置の IP アドレスを特定できるようになります。

3.3.4 EAPOL フォワーディング機能

本装置で IEEE 802.1X を動作させない場合に，EAPOL フレームを中継する機能です。EAPOL フレームは宛先 MAC アドレスが IEEE802.1D で予約されているアドレスであるため通常は中継を行いませんが，IEEE 802.1X が使用されていない場合はこの機能によって中継が可能です。ほかの Authenticator と端末の間の L2 スイッチとして本装置を使用する場合に設定します。詳細は，「解説書 Vol.1　7.5.6(2) EAPOL フォワーディング機能」を参照してください。

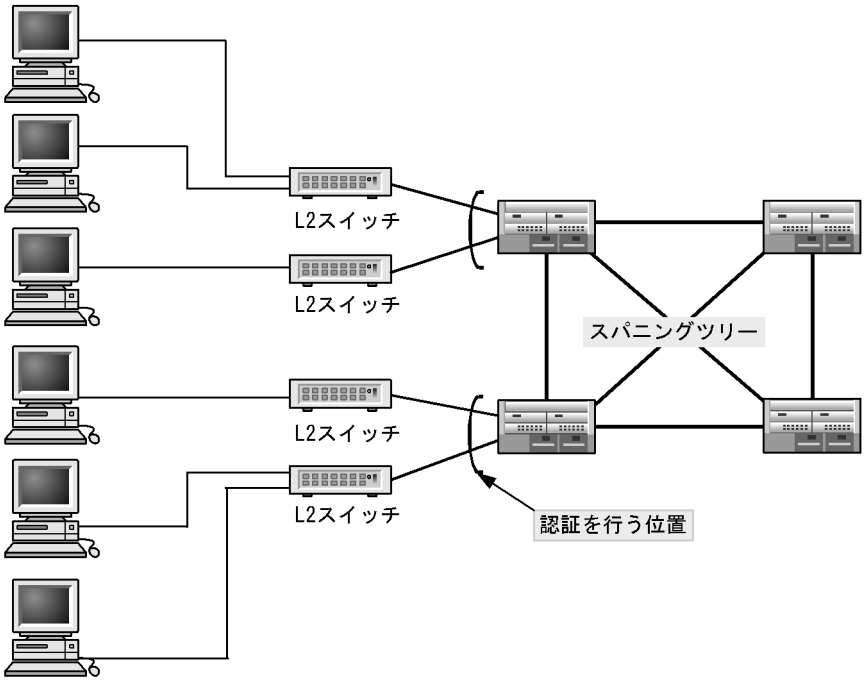
3.3.5 冗長化との組み合わせ

(1) スパニングツリー機能との共存について

端末を接続するエッジポートでの認証，およびルートブリッジでの認証が行えます。それ以外の位置ではスパニングツリーとの共存はできません。スパニングツリーに関するトポロジー計算は，IEEE 802.1X を意識せずに計算します。

スパニングツリーと共存可能な構成例を次の図に示します。

図 3-7 スパニングツリーと共存可能な構成例



3.3.6 認証デフォルト VLAN 機能【SB-7800S】

認証デフォルト VLAN 機能は，802.1X に未対応などの理由によって MAC VLAN に収容できない端末をポート VLAN に収容する機能です。VLAN 単位認証（動的）に設定したポートに対してポート VLAN またはデフォルト VLAN が設定されている場合，その VLAN は認証デフォルト VLAN として動作します。次に示すような場合，端末は認証デフォルト VLAN に収容されます。

- 802.1X 未対応の端末。
- 認証前の 802.1X 対応の端末。
- 認証または再認証に失敗した端末。
- RADIUS サーバから指定された VLAN ID がコンフィグレーションで指定されていない場合。
- RADIUS サーバから指定された VLAN ID が MAC VLAN でない場合。

3.4 IEEE 802.1X 使用時の注意事項

（1） GSRP 機能との共存について

GSRP 機能と IEEE 802.1X 機能は共存できません。

（2） VRRP との共存について

VRRP 機能と IEEE802.1X 機能は共存できません。

（3） MAC アドレス学習数制限機能との共存について

該当物理ポートが IEEE 802.1X ポート単位認証に設定されている場合にだけ共存設定できます。ほかのモードではできません。

（4） デフォルト VLAN 機能との共存について

デフォルト VLAN には IEEE 802.1X VLAN 単位認証を設定できません。

（5） プロトコル VLAN 機能との共存について

プロトコル VLAN には IEEE 802.1X 機能を設定できません。

（6） Tagged ポートとの共存について

Tagged ポートを含む VLAN には VLAN 単位認証（静的）が設定できます。Tagged ポートにポート単位認証は設定できません。

VLAN 単位認証（動的）では，Tagged ポートは認証除外ポートとして扱われます。**【SB-7800S】**

（7） ハイブリッドリンク機能との共存について

Untagged，Tagged が混在するポートを含む VLAN にも VLAN 単位認証（静的）が設定できます。ポート単位認証は設定できません。

VLAN 単位認証（動的）は設定できません。**【SB-7800S】**

（8） VLAN トンネリング機能との共存について

VLAN トンネリング機能と IEEE 802.1X 機能は共存できません。正しく認証が行えません。

（9） 未定義フレーム廃棄機能との共存について

IEEE 802.1X 機能の設定をしたポート（VLAN 単位認証（静的）の場合は，その VLAN に属するポート）で VLAN が決定できないフレームを受信した場合デフォルト VLAN で転送されます。デフォルト VLAN で転送せずに廃棄したい場合は，未定義フレーム廃棄機能を該当ポートに設定してください。

VLAN 単位認証（動的）とは共存できません。**【SB-7800S】**

未定義フレーム廃棄機能については，「解説書 Vol.1　7.1.5 未定義フレーム廃棄機能」を参照してください。

（10）アップリンク VLAN 機能・アップリンクブロック機能との共存について

アップリンク VLAN 機能またはアップリンクブロック機能を設定した VLAN に対して 802.1X 認証を設定

している場合，該当 VLAN に所属するポートに接続する認証済端末の通信が一時的に遮断されることがあります。これは次に示す (a)，(b) のどちらかの条件を満たす場合に発生します。

(a) 該当する VLAN で，次のどれかに当てはまるコンフィグレーション変更を行った

- アップリンク VLAN 機能の strict モードを追加または削除した場合
- アップリンクブロック機能を追加または削除した場合
- 設定されているアップリンク VLAN 機能の strict モードを loose モードへ，または loose モードを strict モードへ変更した場合
- アップリンクポートもしくはブロックポートを追加または削除した場合

(b) 該当する VLAN で，設定されているアップリンクポートもしくはブロックポートが，リンクアップまたはリンクダウンした

（11）OADP，CDP 機能との共存について

OADP，CDP の透過モードは共存できません。

（12）ルータポート機能との共存について

ルータポートに IEEE 802.1X 機能の設定はできません。

（13）MAC 学習 ON/OFF 機能との共存について

IEEE 802.1X 設定をしたポート /VLAN は MAC 学習 OFF には設定できません。

（14）系切替時の引き継ぎ情報について

SB-7800S では運用系と待機系を切り替えた場合，認証されている MAC アドレスを引き継ぎます。
SB-5400S では引き継ぎは行いません。認証されている MAC アドレス以外の情報は引き継ぎを行いません。

LACP リンクアグリゲーションモードを使用している場合，そのリンクアグリゲーションで認証を行った MAC アドレス情報は引き継ぎを行いません。スタティックリンクアグリゲーションモードを使用している場合は引き継ぎを行います。

（15）フロー統計機能 (sFlow 統計 /NetFlow 統計) との共存について

802.1X ポート単位認証を動作させているポートおよび VLAN 単位認証を動作させている VLAN 内の各ポートに対して，フロー統計機能 (sFlow 統計 /NetFlow 統計) で情報収集を行う際，一部統計情報を誤って採取する場合があります。802.1X 認証機能によって送信元の端末が未認証状態であり，該当端末からのフレームを廃棄しているにもかかわらず，フロー統計機能で一部統計採取されます。以下に発生条件を示します。以下の (a)(b) の条件を同時に満たす場合に発生します。

(a) 認証サブモード

認証サブモードを端末認証モードもしくはシングルモードに設定している場合

(b) 対象となるフレームの種類

- IPv6 フレームで，宛先アドレスがリンクローカルアドレス
- OSPF や BGP などのレイヤ 3 にかかわる自装置宛の制御フレーム

（16）VLAN 単位認証（動的）モードをサポートする PSU について【SB-7800S】

VLAN 単位認証（動的）をサポートする PSU は，MAC VLAN 機能をサポートした PSU ボードだけです。対応する PSU ボードについては，「解説書 Vol.1　7.4.5 MAC VLAN サポートの PSU について」を

参照してください。

（17）VLAN 単位認証（動的）モードでのエージング時間の設定について【SB-7800S】

VLAN 単位認証（動的）モードを使用する場合，radius-vlan サブコマンドで指定する VLAN と認証デフォルト VLAN として使用する VLAN については，FDB エントリのエージング時間に 0（無限）を指定しないでください。0（無限）を指定すると，端末の所属する VLAN が切り替わったときに，切り替わる前の VLAN の FDB エントリがエージングで消去されずに残り続けるため，不要な FDB エントリが蓄積することになります。切り替わる前の VLAN に不要な FDB エントリが蓄積した場合は，clear fdb コマンドで消去してください。

（18）MAC VLAN との共存について【SB-7800S】

VLAN 単位認証（動的）だけが共存できます。

MAC VLAN で指定されたポートに対するポート単位認証および MAC VLAN に対する VLAN 単位認証（静的）での共存はできません。

（19）supplicant-detection サブコマンドについて

supplicant-detection サブコマンドで指定するオプションと Supplicant ソフトウェアの組み合わせには以下の注意事項があります。

（a） shortcut

装置の負荷を低減するため，認証済み端末に対する EAP-Req/Id 契機の認証シーケンスを一部省略します。一部の Supplicant ソフトウェアを本モードで使用すると，EAP-Req/Id による認証時に認証済み端末との通信が途切れる場合があります。そのときに，使用する Supplicant ソフトウェアが EAP-Start を自発的に送信できる場合は disable を指定してください。自発的に EAP-Start を送信できない場合は full を指定してください。full を指定した場合は接続できる端末数に制限が発生しますので注意してください。

（b） disable

認証済み端末が存在する場合は EAP-Req/Id の送信を停止します。自発的に EAP-Start を送信しない Supplicant ソフトウェアで本モードを使用すると，認証開始の契機がなくなるため認証を開始できません。Windows 標準の Supplicant ソフトウェアはデフォルトでは自発的に EAP-Start を送信しませんが，レジストリ SupplicantMode の値を変更することによってこの動作を変更できます。レジストリの詳細については，Microsoft 社の WWW サイトあるいは公開技術文書を参照してください。レジストリの設定を失敗すると Windows が立ち上がらなくなるおそれがありますので注意してください。また，レジストリを変更する場合は必ずレジストリのバックアップを取ることをお勧めします。

（c） full

認証済み端末に対する EAP-Req/Id 契機の認証シーケンスを省略しません。本モードでは，認証単位ごとに接続できる端末数が，SB-7800S の場合 30 台，SB-5400S の場合 25 台に制限されます。この台数を超える端末を接続した場合，本装置に負荷が掛かり認証処理の取りこぼしが発生し，認証済み端末との通信が途切れることがあります。本モードは自発的に EAP-Start を送信しない Supplicant ソフトウェアと，認証シーケンスを省略すると問題の発生する Supplicant ソフトウェアを混在して使用する場合に指定してください。

（20）タイマ値のオンラインコンフィグレーション変更について

オンラインコンフィグレーションの変更によって，タイマ値（tx-period，reauth-period，supp-timeout，

quiet-period，keep-unauth）を変更した場合，変更した値が実際にタイマに反映されるのは，各認証単位で現在動作中のタイマがタイムアウトして 0 になったときです。すぐに変更を反映させたい場合には，運用コマンド「clear dot1x auth-state」を使用して認証状態をいったん解除してください。

（21）tx-period および reauth-period の設定値について

tx-period および reauth-period の設定値は，次に示す式の値に基づいて設定してください。この式で決定される値よりも小さな値を設定した場合，端末の認証状態が安定しないことがあります。

- SB-7800S の場合
  tx-period ≧（装置で認証を行う総端末数÷ 30）× 2
  reauth-period ＞ tx-period
- SB-5400S の場合
  tx-period ≧（装置で認証を行う総端末数÷ 25）× 2
  reauth-period ＞ tx-period

（22）端末と本装置の間にＬ２機能を持つスイッチを配置する場合について

本装置から送信される EAPOL フレームに対する端末からの応答は一般的にマルチキャストとなるため，端末と本装置の間に L2 機能を持つスイッチ（以降，L2 スイッチと表記します）を配置する場合，端末からの応答による EAPOL フレームは L2 スイッチの同一 VLAN のすべてのポート※へ転送されます。したがって，L2 スイッチの VLAN を次のように定義すると，同一端末からの EAPOL フレームが本装置の複数のポートへ届き，複数のポートで同一端末に対する認証処理が行われるようになります。そのため，認証動作が不安定になり，通信が切断されたり，認証ができなくなったりします。

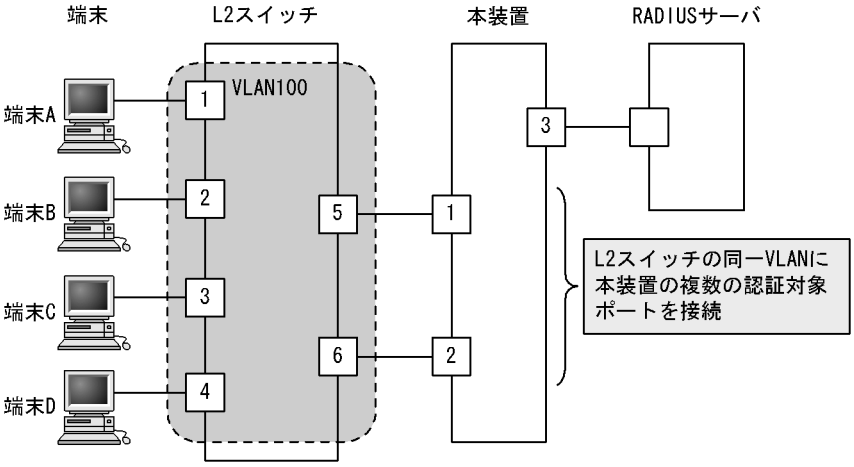
注※
リンクアグリゲーションの場合，リンクアグリゲーショングループを 1 ポートとみなします。

- L2 スイッチの同一 VLAN に設定されているポートを，本装置の認証対象となっている複数のポートに接続した場合（下図の禁止構成例参照）
- L2 スイッチの同一 VLAN に設定されているポートを，複数の本装置の認証対象となっているポートに接続した場合（下図の禁止構成例参照）

端末と本装置の間に L2 スイッチを配置する場合の禁止構成例を次の図に示します。

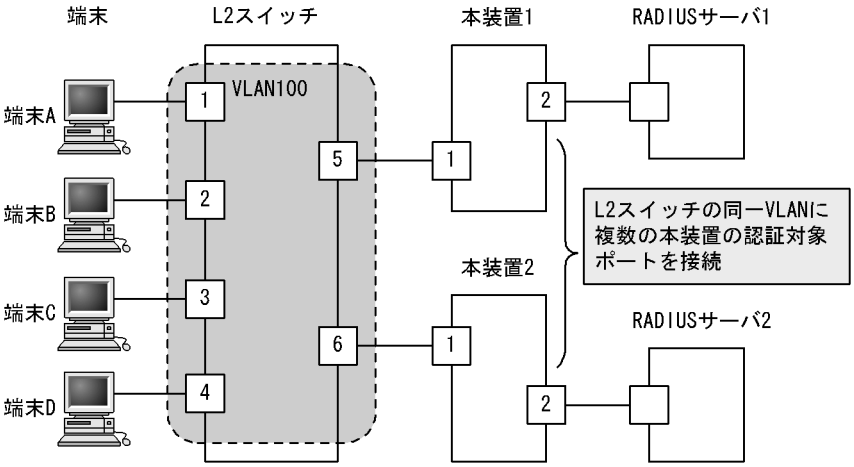
図 3-8　禁止構成例

・L2スイッチの同一VLANに本装置の複数の認証対象ポートを接続した例



本構成の場合，本装置から送信したEAPOLフレームに対して，認証対象端末A，B，C，Dからの応答フレームが本装置の認証対象ポート1，2に転送されてしまいます。これによって，本装置の認証ポート1，2では同一端末に対する認証処理が実行されます。各認証ポートでは，認証する端末が他ポートで認証されている場合，他ポートの認証状態を解除して，自ポートでの認証処理を行います。その結果，他ポートで認証済みである端末の通信が遮断されます。

・L2スイッチの同一VLANに複数の本装置の認証対象ポートを接続した例

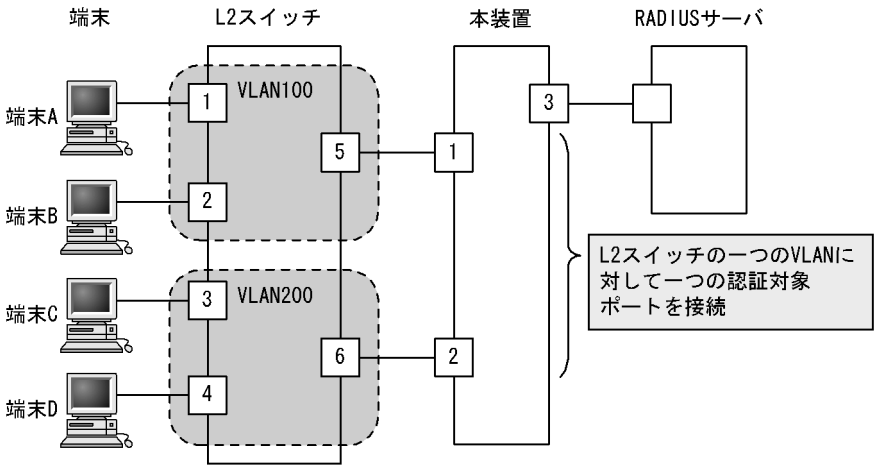


本構成の場合，認証対象端末から送られたEAPOL-Startフレームがマルチキャストで本装置1および本装置2に送信されます。このEAPOL-Startフレームを受信した本装置1，本装置2で認証処理が行われて，一つの端末に対して本装置1および本装置2で認証済み状態になる場合があります。

端末と本装置の間に L2 スイッチを配置する場合の正しい構成例を次の図に示します。

図 3-9 正しい構成例

・L2スイッチの一つのVLANに本装置の一つの認証対象ポートを接続した例



本構成の場合，本装置からのEAPOLフレームに対する認証対象端末A，Bからの応答フレームは，本装置のポート1だけに送信されます。一方，認証対象端末C，Dからの応答フレームは，本装置のポート2だけに送信されるため，同一端末に対して，
複数の認証対象ポートでの認証処理は発生しません。

4 冗長構成

この章では本装置の冗長構成について説明します。

4.1 冗長構成概説

SB-7800S では装置の信頼性を向上するために電源ユニット (PS) および基本制御モジュール (BCU) を冗長化できます。SB-5400S では装置の信頼性を向上するために電源ユニット (PS)，基本制御モジュール (BCU) および基本スイッチングモジュール (BSU) を冗長化できます。装置ごとの冗長化を次の表に示します。

表 4-1 装置ごとの冗長化

項目	SB-7804S	SB-7808S	SB-7816S	SB-5402S	SB-5404S
電源冗長化	○	○	○	○	○
基本制御モジュール (BCU) 冗長化	×	○	○	×	○※
基本スイッチングモジュール (BSU) 冗長化	-	-	-	×	○※

(凡例) ○：冗長化できる ×：冗長化できない -：BSU 実装不可
注※ SB-5404S では，基本制御モジュールと基本スイッチングモジュールを同時に冗長化します。基本制御モジュールだけや基本スイッチングモジュールだけの冗長化はできません。

4.1.1 電源ユニット (PS)

SwitchBlade7800S シリーズおよび SwitchBlade5400S シリーズは複数個の PS から構成され，装置ごとに必要な電源個数が異なります。装置と電源数の対応について次の表に示します。PS の実装数が基本構成時の電源数を超え PS 冗長時の電源数に満たない場合は，冗長電源部の異常として取り扱います。PS を冗長して運用する場合は表で示す電源数が必要となります。

表 4-2 必要電源数

装置モデルと PSU 内蔵型 高密度ポート NIF の搭載有無		PS 基本構成時	PS 冗長時
SB-7804S-AC	搭載なし	1	2 または 3※
	搭載あり	2	3
SB-7808S-AC	搭載なし	2	4
	搭載あり	3	4
SB-7816S	搭載なし	2	4
	搭載あり	2	4
SB-7804S-DC	搭載なし	1	2
	搭載あり	1	2
SB-7808S-DC	搭載なし	1	2
	搭載あり	1	2
SB-5402S	-	1	2
SB-5404S	-	2	4

(凡例) -：該当なし
注※ 電源を 2 個実装することで冗長構成になりますが，POW2 を実装した場合は電源を 3 個実装することで冗長構成になります。

電源に障害が発生し電力供給が停止した場合は，自動的に残りの電源で負荷バランスを行い，電源を安定

して供給できます。また，障害となった電源は装置を運用したまま交換できます。

本装置には電源ユニットの実装状態を監視する電源ユニットの運用モードがあり，運用モードには‘auto’と‘redundancy’の二つのモードがあります。何も設定していない状態 (デフォルト) である‘auto’モードは，電源の実装状態に合わせて運用したい場合に使用します。本装置の立ち上げに必要な電源数 (基本構成) のまま運用を行う場合や，基本構成から冗長構成に変更する場合，冗長構成から基本構成に変更する場合など，電源数の増減に自動的に対応します。

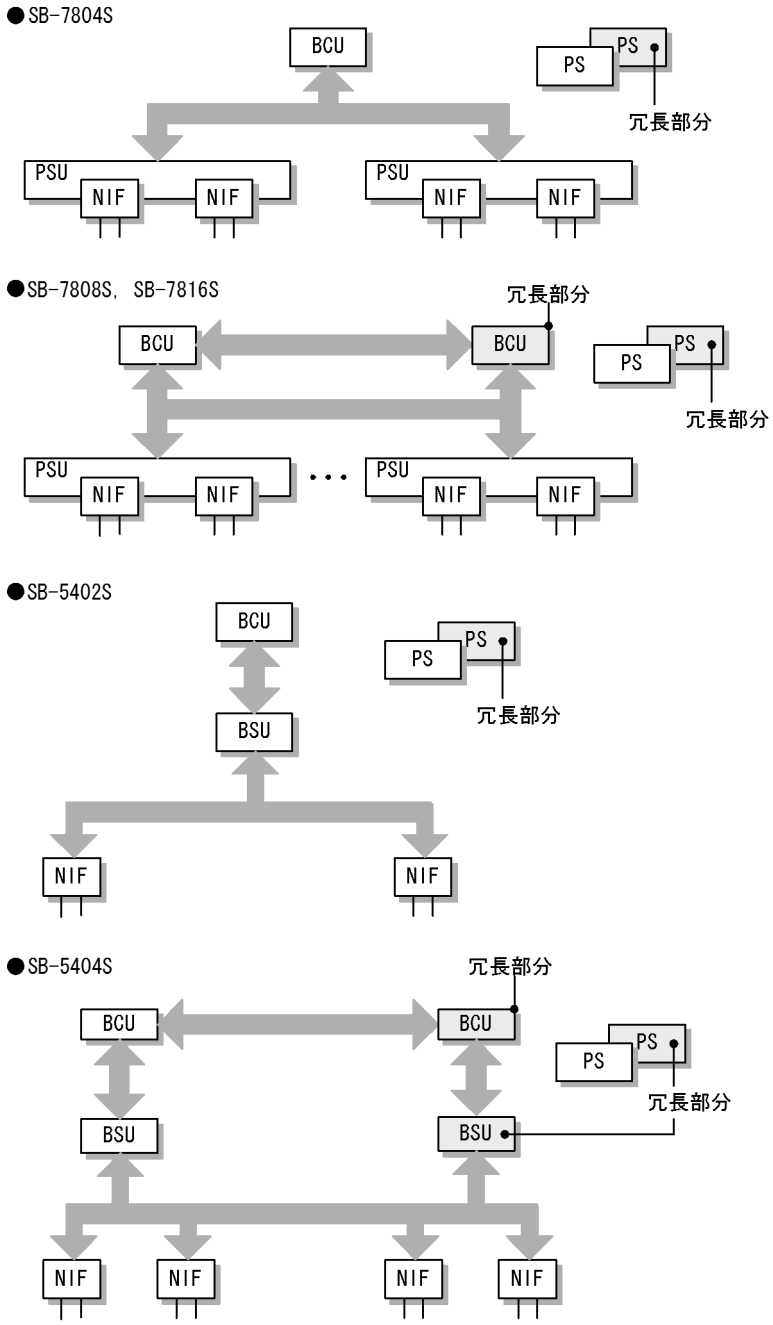
電源の冗長構成で運用を継続したい場合には‘redundancy’モードを使用することをお勧めします。‘redundancy’に設定した場合，電源ユニットが冗長構成でなくなったときに (立ち上げ時に未実装の電源があった場合または運用中に電源を抜去した場合)‘E8 POW 00000102 2200:000000000000 Power unit isn't redundantly mounted. (電源が冗長実装ではありません。)’のログを出力し，冗長構成でなくなったことを警告します。SB-5400S の場合，‘E8 POW 00000102・・・’の 'POW' の部分は 'PS' になります。

電源ユニットの運用モードについては，運用コマンド set mode の記述を参照してください。

4.1.2 基本制御モジュール (BCU)

SB-7808S，SB-7816S および SB-5404S は基本制御モジュールの冗長構成ができます。また，SB-5404S では基本スイッチングモジュールの冗長構成ができます。装置の冗長構成部分を次の図に示します。

図 4-1　装置の冗長構成部分



4.2 基本制御モジュールおよび基本スイッチングモジュールの二重化

本装置の制御とルーティング情報，スイッチング情報を処理する基本制御モジュール (BCU) および基本スイッチングモジュール (BSU) は，二重化による冗長構成にできます。冗長構成によって，障害に対する信頼性を高めます。冗長構成にすれば BCU 障害発生時でも BCU がサポートするルーティング機能，スイッチング機能の復旧を短期間に行えます。このため，PSU や BSU での中継処理に対する影響を極力抑えることができます。

本装置の初期導入時は，SB-7800S では BCU の実装枚数が 1 枚であれば一重化で動作し , 実装枚数が 2 枚であれば系切替が可能な状態 (待機系 BCU，CP が起動完了) になったとき，‘System mode changed from simplex to duplex.’のログを表示して，二重化で動作します。実装枚数が 2 枚でも待機系 BCU，CP が起動完了していない場合，一重化で動作します。

SB-5400S では BCU と BSU の実装枚数が 1 枚ずつであれば一重化で動作し，実装枚数が 2 枚ずつであれば系切替が可能な状態 (待機系 BCU，CP，BSU が起動完了) になったとき，‘System mode changed from simplex to duplex.’のログを表示し，二重化で動作します。実装枚数が 2 枚ずつでも待機系 BCU，CP，BSU が起動完了していない場合，一重化で動作します。

それぞれの動作を固定で行いたい場合は，冗長動作モードで設定してください。冗長動作モードの設定については，運用コマンド set mode の記述を参照してください。

二重化によって冗長構成で運用を開始すると，SB-7800S では BCU0 が運用系として動作し，BCU1 は待機系として動作します。SB-5400S では BCU0・BSU0 が運用系として動作し，BCU1 と BSU1 は待機系として動作します。これらの実装位置については，「解説書 Vol.1　2.1 本装置のモデル」を参照してください。

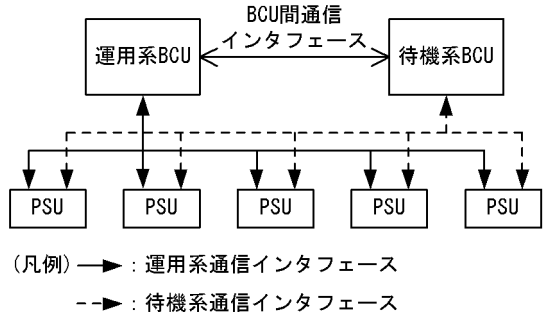
CSW モードを double_fixed に設定していた場合，BCU の冗長構成機能は動作せず，一重化として動作します。CSW モードの詳細は，「解説書 Vol.1　2.4 CSW 動作モード（CSW モード）【SB-7800S】」を参照してください。**【SB-7800S】**

4.2.1 冗長構成での動作

(1) 冗長構成

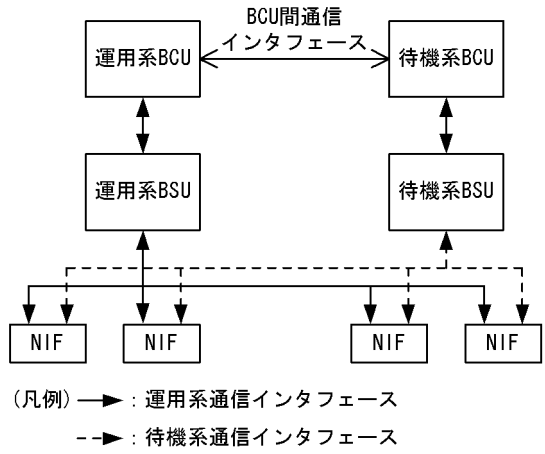
SB-7800S では，運用系および待機系の BCU はそれぞれ独立したインタフェースで PSU と接続しています。PSU から見て接続先の BCU が運用系の場合は，該当する BCU との通信が有効になります。待機系の場合，インタフェースは無効となります。BCU と PSU の冗長構成でのインタフェースの関係を次の図に示します。

図 4-2 BCU-PSU 間の冗長構成でのインタフェース



SB-5400S では，運用系および待機系の BSU はそれぞれ独立したインタフェースで NIF と接続しています。NIF から見て接続先の BSU が運用系の場合は，該当する BSU との通信が有効になります。待機系の場合，インタフェースは無効となります。BSU と NIF の冗長構成でのインタフェースの関係を次の図に示します。

図 4-3 BSU-NIF 間の冗長構成でのインタフェース



（2） 二重化での動作開始

装置の起動時には，SB-7800S では二重化を構成する二つの BCU が，SB-5400S では二重化を構成する二つの BCU または BSU が，それぞれ運用系および待機系として起動します。運用系に障害が発生した場合，すぐ待機系に装置の制御権を渡すとともに障害部位を再初期化します。待機系は障害になった運用系の代わりに新運用系となって装置の制御を引き継ぎます。障害が発生した旧運用系が，再初期化によって障害が回復した場合には，運用系には戻らないで新待機系として待機状態になります。

（3） 装置起動時の待機系および運用系との整合性確認

装置起動時に待機系は運用系からソフトウェアのバージョン，ソフトウェアライセンスキー，およびスタートアップコンフィグレーションファイルに関する情報を取得して比較します。比較した情報に差異がある場合は，冗長動作モードによって PSU や BSU の再起動による一時的な通信断や，装置として二重化運用を抑止します。これによって，系切替発生時に運用状態が不一致のために発生する運用障害を防ぎます。

（4） 運用系および待機系の状態表示

運用系 BCU を介して待機系 BCU の状態を参照できます。参照できる情報は SB-7800S では待機系 BCU

の LED 状態および障害情報，SB-5400S では待機系 BCU または BSU の LED 状態および障害情報です。ただし，待機系 BCU が障害の場合は状態を参照できません。

（5） コマンドによる系切替実行および系切替の抑止

コマンドを使用して任意の時点で運用系と待機系を切り替える機能をサポートします。また，系切替の抑止もできます。

4.2.2 系切替時の動作

（1） 系切替時の引き継ぎ情報

SB-7800S では運用系と待機系を切り替えた場合，次に示す情報を引き継ぎます。

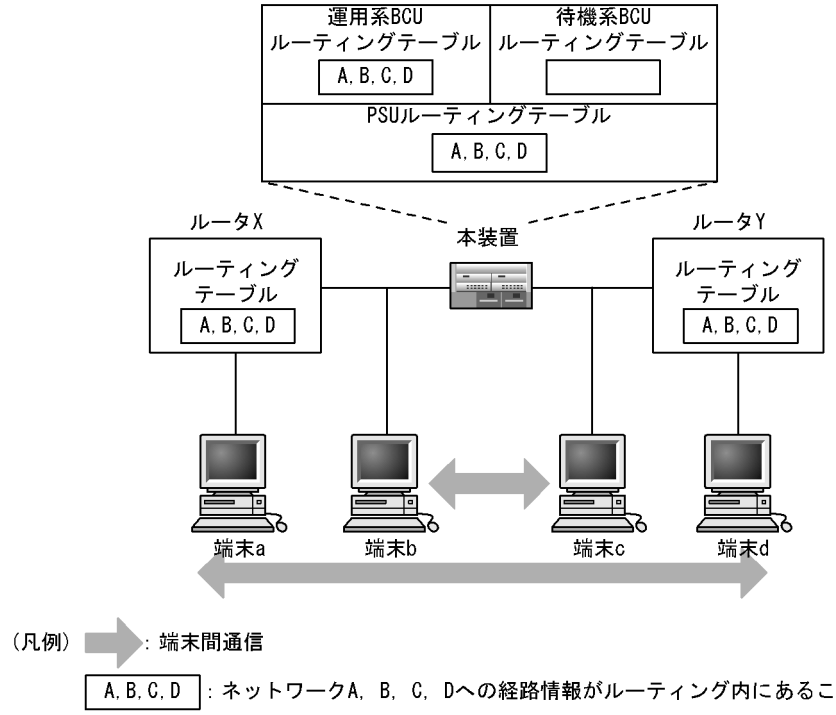
SB-5400S では運用系と待機系を切り替えても FDB エントリ情報およびルーティングエントリ情報の引き継ぎはしません。

- **旧運用系 BCU に障害が発生するまでに処理した FDB エントリ情報**
- **旧運用系 BCU に障害が発生するまでに処理したルーティングエントリ情報**
  - 本装置の動作
    SB-7800S では旧運用系 BCU に障害が発生した時点までのルーティングエントリ情報は，新運用系がルーティング処理動作を開始するまでの間，装置内に保持されています。したがって，障害時点で装置を介して行っている通信はそのまま保証されます。旧運用系から新運用系への引き継ぎ処理中に発生した経路更新情報は，新運用系への切替後にルーティングエントリ情報に反映されます。
    SB-5400S では旧運用系 BCU または BSU に障害が発生した時点までのルーティングエントリ情報は新運用系に引き継がれません。したがって，新運用系へ切替後にルーティングエントリ情報を再学習するまで通信が停止します。
  - 経路情報を交換している相手装置の動作
    相手装置は一時的に本装置と経路情報を交換できなくなるため，通信断となります。旧運用系から新運用系への切替後，経路情報の交換を再開すれば通信が復旧します。
- **close コマンドによる閉塞状態情報**
  旧運用系から新運用系への移行時に，SB-7800S では PSU，NIF および回線，SB-5400S では NIF および回線の閉塞運用状態を引き継ぐことによって，制御上の不一致発生を回避します。

（2） BCU 切替時の本装置と相手装置の中継動作【SB-7800S】

BCU 切替時の本装置と相手装置の中継動作について概要を説明します。BCU の切替を次の図に示します。

図 4-4 BCU の切替



この図では端末 a と d，b と c がルータ X，Y，本装置を介して通信している例です。使用しているルーティングプロトコル (RIP，OSPF，BGP4，IS-IS，RIPng，OSPFv3，BGP4+) によって相手ルータの動作が異なります。次にルーティングプロトコルごとの BCU 切替について説明します。

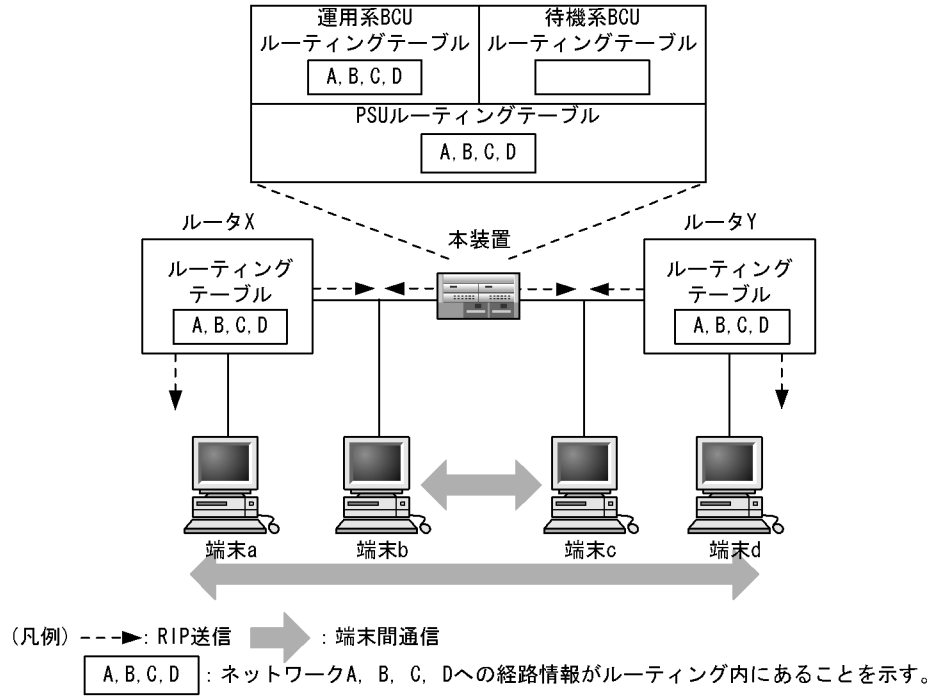
(a) ルーティングプロトコルに RIP，RIPng を使用している場合

RIP と RIPng では相手ルータの動作が同じなので RIP を例に説明します。

● 系切替前

端末 a と d，b と c が通信を行っています。また，本装置，ルータ X，ルータ Y はお互い RIP の送受信を行い，ルーティング情報をやり取りします。RIP 系切替前を次の図に示します。

図 4-5 BCU 切替 (RIP 系切替前)

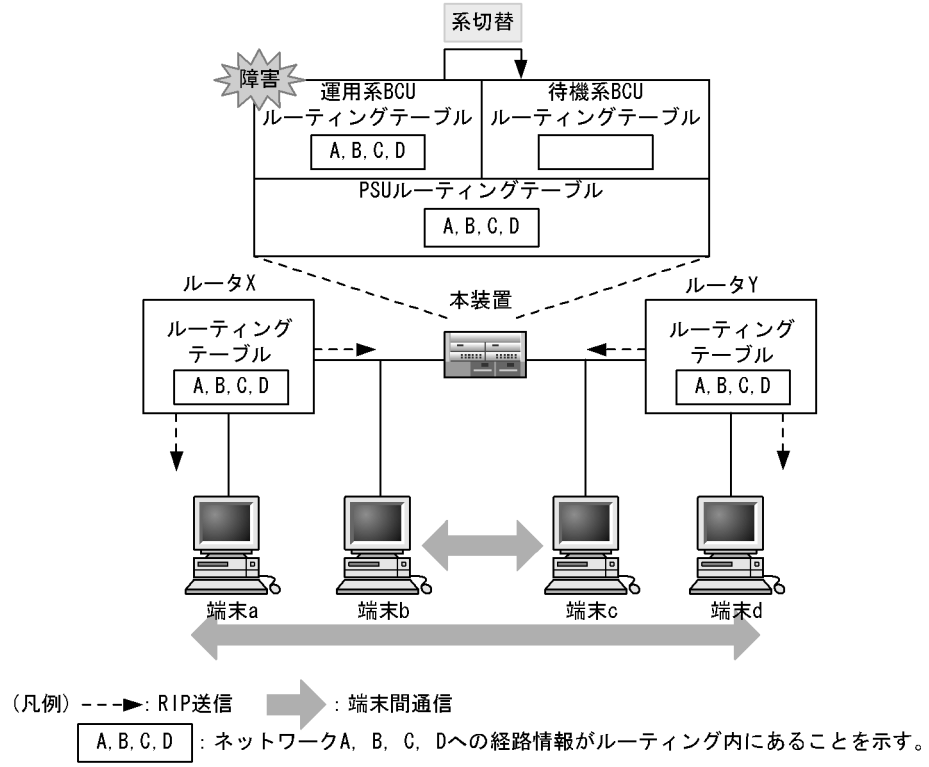


● 系切替発生

本装置の運用系に障害が発生して系切替を行います。新待機系 BCU のルーティングテーブルは初期化されます。新運用系 BCU のルーティングテーブルはルーティングプロトコルの学習が始まっていないため，まだエントリはありません。PSU のルーティングテーブルを系切替によって初期化しません。また，ルータ X，Y も本装置のダウンを検出しないため，端末 a と d，b と c の通信は継続します。

RIP 系切替発生を次の図に示します。

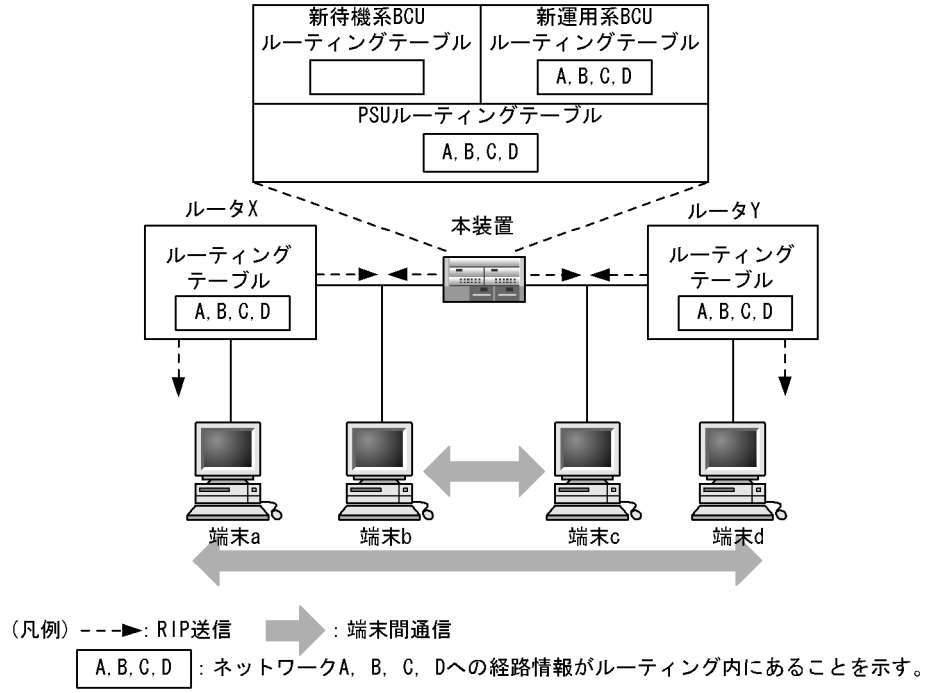
図 4-6 BCU 切替 (RIP 系切替発生)



● 系切替後

本装置はルータ X，Y が本装置のダウンを検出する前に系切替を完了して RIP のやり取りを再開します。ルータ X，Y が送信する RIP を受信し，ルーティングテーブルを再学習します。PSU，ルータ X，Y のルーティングテーブルが変化しないため，端末 a と d，b と c の通信は継続しています。RIP 系切替後を次の図に示します。

図 4-7 BCU 切替 (RIP 系切替後)



(b) ルーティングプロトコルに OSPF，BGP4，IS-IS，OSPFv3，BGP4+ を使用している場合

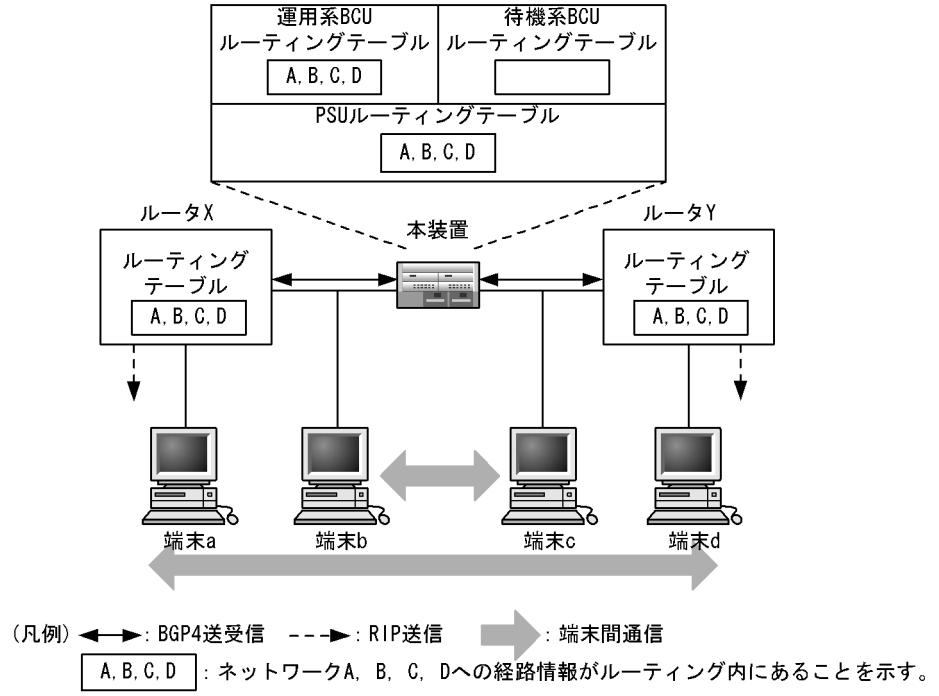
RIP/RIPng 以外のプロトコルには，隣接ルータとの接続切断を検出する機能があります。グレースフル・リスタート機能を使用していない場合，本装置が系切替すると，隣接ルータでは以前の接続が切断したものと認識します。この結果，隣接ルータがパケット転送を停止するため，本装置を経由する通信が一時的に停止します。グレースフル・リスタートを使用する場合については，「(c) グレースフル・リスタートを使用する場合」を参照してください。

以下，OSPF，BGP4，IS-IS，OSPFv3，BGP4+ では相手ルータの動作が同じなので BGP4 を例に説明します。

● 系切替前

端末 a と d，b と c が通信を行っています。また，本装置，ルータ X，ルータ Y はお互い BGP4 の送受信を行い，ルーティング情報をやり取りします。BGP4 系切替前を次の図に示します。

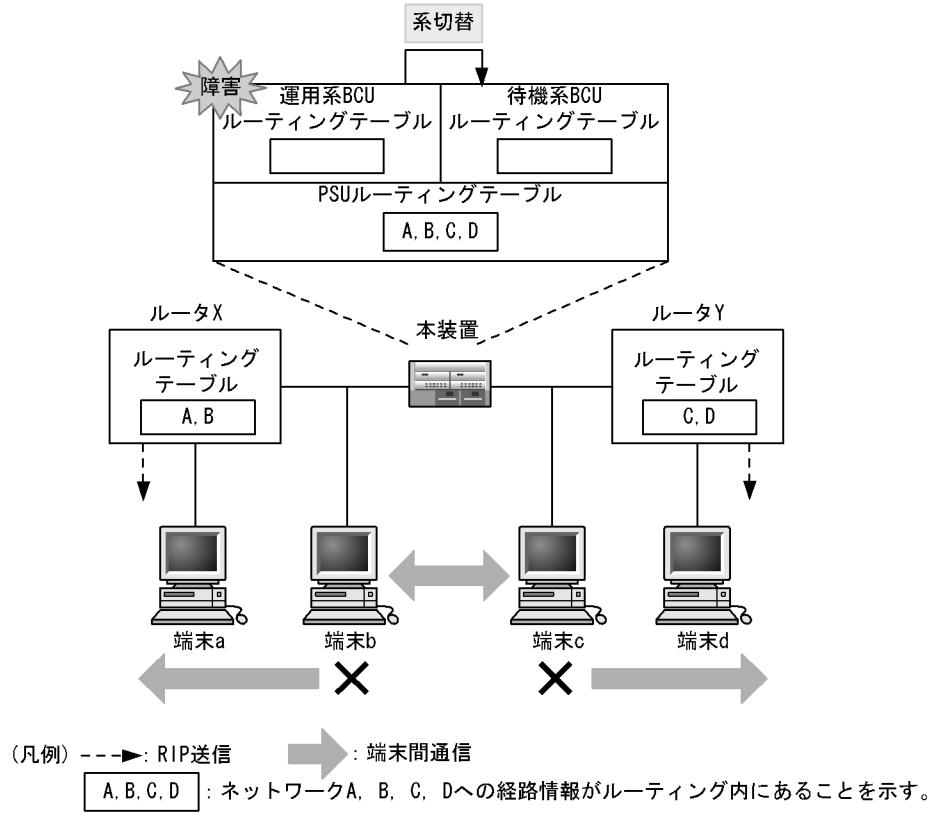
図 4-8 BCU 切替 (BGP4 系切替前)



● 系切替発生

本装置の運用系に障害が発生して系切替を行います。新待機系 BCU のルーティングテーブルは初期化されます。新運用系 BCU のルーティングテーブルはルーティングプロトコルの学習が始まっていないため，まだエントリはありません。PSU のルーティングテーブルは系切替によって再初期化しないため，端末 b と c の通信は継続します。端末 a と d の通信は，本装置とルータ X，Y の BGP4 の TCP セッションが切れ，ルータ X，Y のルーティングテーブルが削除されるので停止します。BGP4 系切替発生を次の図に示します。

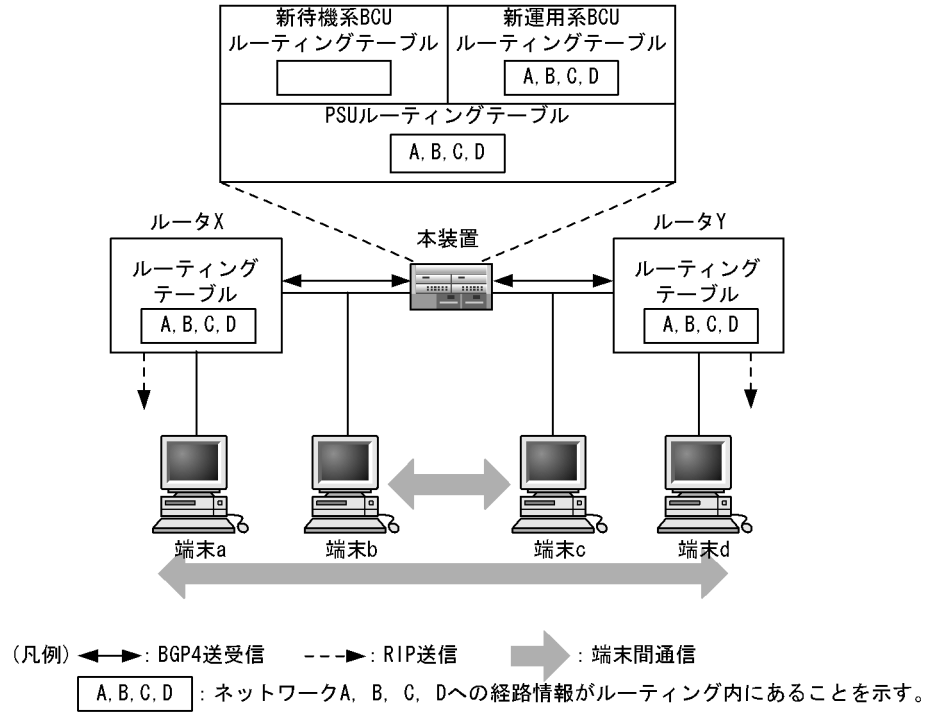
図 4-9 BCU 切替 (BGP4 系切替発生)



● 系切替後

本装置は系切替完了後，TCP セッションを確立して BGP4 のやり取りを再開し，ルーティングテーブルを再学習します。ルータ X，Y でもルーティングテーブルを再学習します。PSU のルーティングテーブルは系切替によって再初期化しないため，端末 b と c の通信は継続します。端末 a と d の通信は，ルータ X，Y のルーティングテーブルの再学習によって再開します。BGP4 系切替後を次の図に示します。

図 4-10 BCU 切替 (BGP4 系切替後)



ルーティングテーブルの再学習を完了するまでの目安時間は，経路交換開始時間と経路情報数に依存する経路交換時間・経路計算時間の合計です。本装置のデフォルト値でプロトコルが動作した場合の経路交換開始時間を次に示します。

- OSPF の経路交換開始時間は，系切替後約 40 秒です。(対向ルータとのインタフェースがイーサネットの場合)
- BGP4 の経路交換開始時間は，系切替後約 90 ～ 130 秒です。

(c) グレースフル・リスタートを使用する場合

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

「(b) ルーティングプロトコルに OSPF，BGP4，IS-IS，OSPFv3，BGP4+ を使用している場合」で説明したように，装置の BCU が系切替したとき，隣接ルータでは以前の接続が切断したものと認識して，経路を削除するため，ネットワーク全体では通信が停止します。

グレースフル・リスタートでは，この問題を解決して切替時の通信停止時間を短縮します。具体的には以下の方法によって解決します。

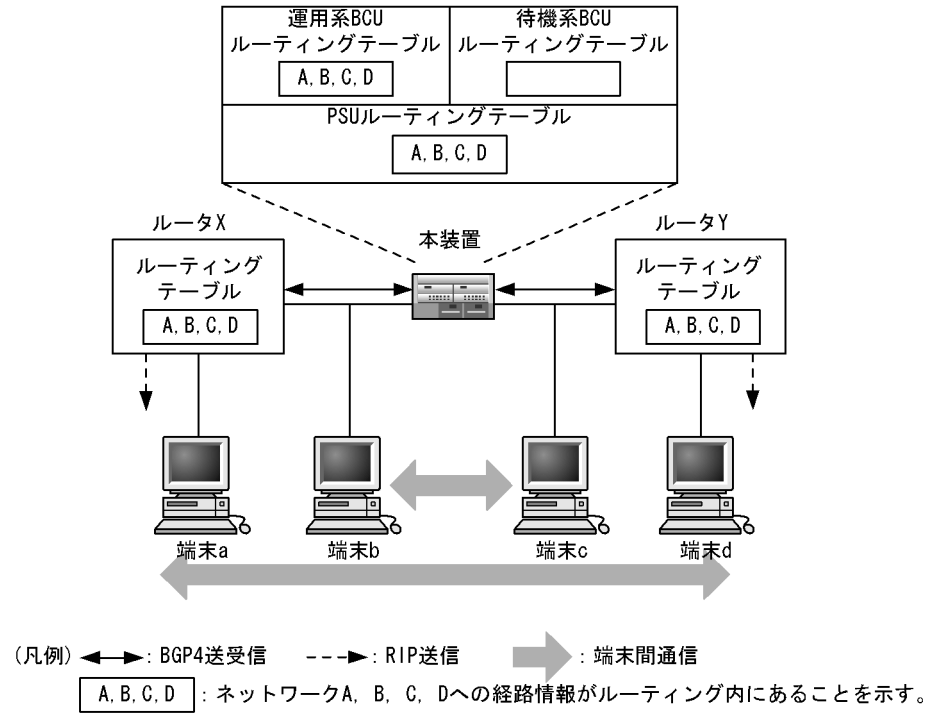
- 隣接ルータに，グレースフル・リスタートを補助する機能を用意します。グレースフル・リスタートによる接続要求を受け取ったときに，以前の接続を切断して再接続するのではなく，以前の接続を継続しているものと認識する機能を追加します。これによって，ルーティングプログラム切替時にも隣接ルータとの接続が切断しなくなるため，隣接ルータも経路を保持したまま動作します。
- 経路学習・経路広告の処理順序を固定します。グレースフル・リスタートでは，まず隣接ルータから経路情報を学習し，経路を学習し終わってから経路広告を開始します。これにより，経路広告時にはすべての経路を広告するため，一部経路しか広告しないことによって隣接ルータから経路が消えることがなくなります。

以下，グレースフル・リスタートを使用している場合の動作を説明します。OSPF，BGP4，IS-IS，OSPFv3，BGP4+ では相手ルータの動作が同じなので BGP4 を例に説明します。

● 系切替前

次の図に，系切替前の通信状態を示します。端末 a と d，b と c が通信を行っています。また，本装置，ルータ X，ルータ Y はお互い BGP4 の送受信を行い，ルーティング情報を交換します。本装置にはグレースフル・リスタート機能が動作するように設定しておきます。また，ルータ X・ルータ Y にはグレースフル・リスタートの補助機能が動作するように設定しておきます。

図 4-11 グレースフル・リスタート (系切替前)

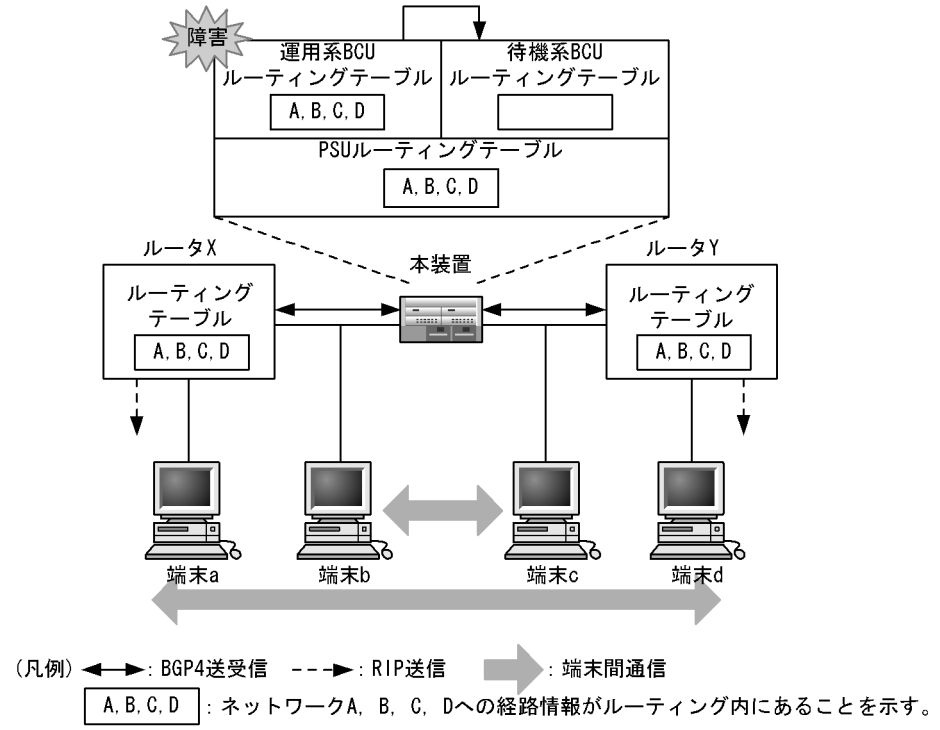


● 系切替発生

次の図に，系切替中の通信状態を示します。

本装置の運用系に障害が発生して系切替を行います。新待機系 BCU のルーティングテーブルは初期化されます。新運用系 BCU のルーティングテーブルはルーティングプロトコルの学習が始まっていないため，まだエントリはありません。PSU の経路は，すべて系切替前ルーティングテーブルに移動します。系切替前ルーティングテーブルに経路が残っているので，端末 b と c の通信は継続します。本装置とルータ X，ルータ Y の BGP4 の TCP セッションは切断されますが，グレースフル・リスタートの補助機能が働くので，ルータ X，ルータ Y のルーティングテーブルは削除されません。このため，端末 a と d の通信も継続します。

図 4-12 グレースフル・リスタート (系切替中)

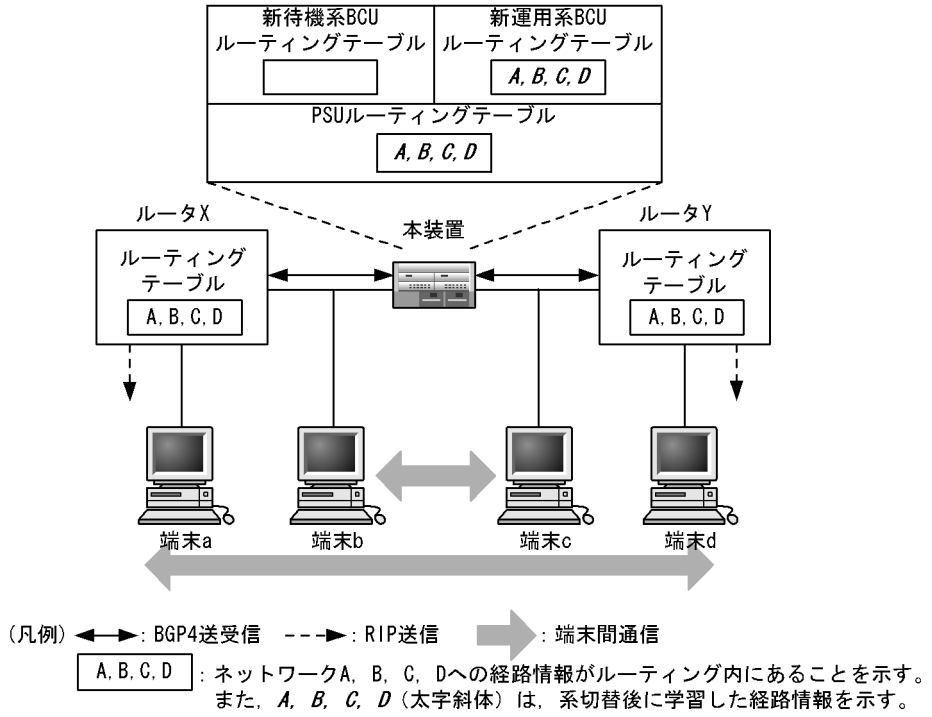


● 経路学習

次の図に，グレースフル・リスタート経路学習時の通信状態を示します。

本装置は系切替完了後，TCP セッションを確立して BGP4 の通信を再開します。このとき，まずルータ X，ルータ Y からの経路学習を行い，通常のルーティングテーブルに学習経路を上書きします。この間，系切替前，系切替後どちらかの経路が本装置の PSU に存在しており，またルータ X，ルータ Y すべて系切替前の経路を保持しているので，端末 a と d の通信，端末 b と c の通信両方とも継続します。

図 4-13 グレースフル・リスタート (経路学習)



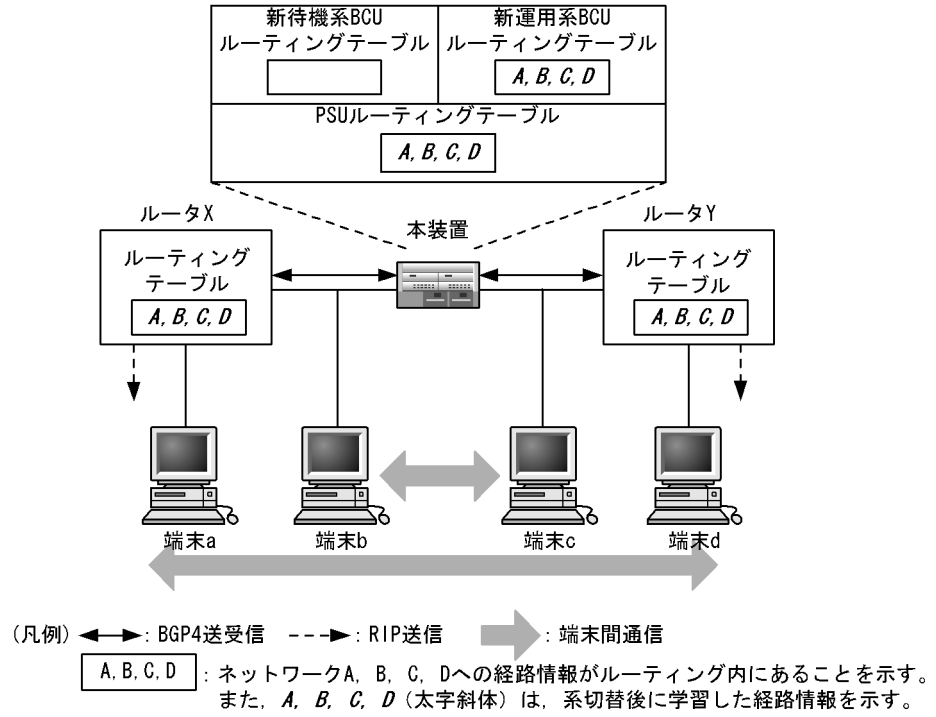
● 経路広告

次の図に，グレースフル・リスタート経路広告時の通信状態を示します。

本装置が経路学習を完了したら，系切替前からあった経路を削除し，ルータ X，ルータ Y への経路広告を開始します。ルータ X，ルータ Y では，この広告経路によって系切替前に学習した経路を上書きします。この間も端末 a と d の通信は継続します。

本装置の経路広告が完了したら，通常の BGP4 の運用状態に戻ります。

図 4-14 グレースフル・リスタート (経路広告)



[注意事項]

1. グレースフル・リスタート一般の適用範囲については，「解説書 Vol.1　12.8 グレースフル・リスタートの概要」を参照してください。
2. 各プロトコル固有のグレースフル・リスタートの方式・動作・適用範囲については，以下を参照してください。
   OSPF :「解説書 Vol.1　12.5.9 グレースフル・リスタート」
   BGP4 :「解説書 Vol.1　13.3.11 グレースフル・リスタート」
   IS-IS :「解説書 Vol.1　14.2.8 グレースフル・リスタート」
   OSPFv3 :「解説書 Vol.1　17.5.8 グレースフル・リスタート」
   BGP4+ :「解説書 Vol.1　18.3.11 グレースフル・リスタート」
3. PSU の経路保持時間を，グレースフル・リスタートの経路学習時間よりも長くなるように設定してください。経路保持時間のほうが短い場合，系切替後の新しい経路を学習する前に切替前の経路を削除するので，通信が停止します。

(d) マルチキャストルーティングプロトコルに PIM-SM を使用している場合【OP-MLT】

IPv4 PIM-SM，IPv4 PIM-SSM，IPv6 PIM-SM，IPv6 PIM-SSM，PIM-DM，DVMRP では動作が同じなので，IPv4 PIM-SM を例に説明します。

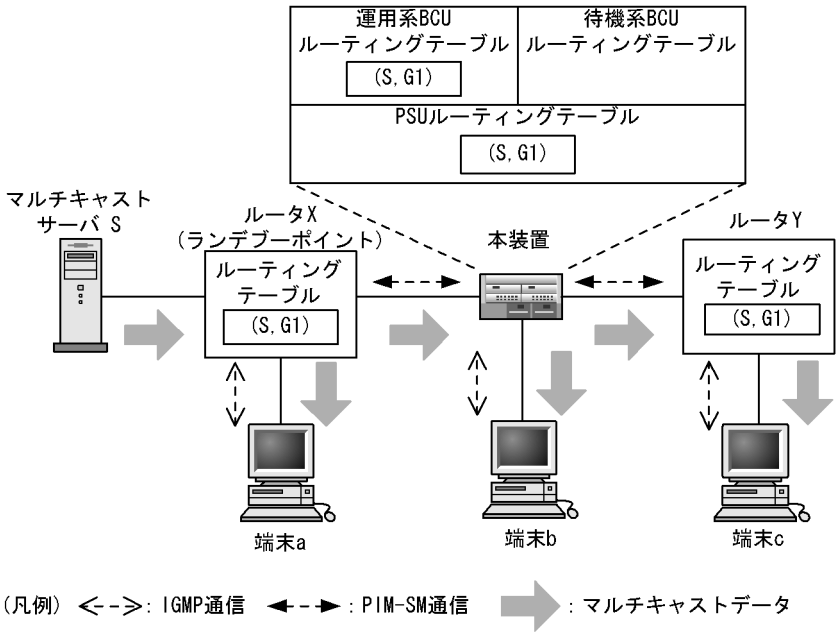
IPv6 PIM-SM，IPv6 PIM-SSM の場合は IGMP が MLD となります。また，IPv4 PIM-SSM，IPv6 PIM-SSM，IPv4 PIM-DM，DVMRP にはランデブーポイントは存在しません。

IPv4 PIM-SM，IPv6 PIM-SSM は系切替時に通信を継続できる nonstop forwarding 機能をサポートしています。nonstop forwarding 機能については「(e) マルチキャストルーティングプロトコルに PIM-SM (nonstop forwarding 機能) を使用している場合【OP-MLT】」を参照してください。

● 系切替前
マルチキャストサーバ S がマルチキャストグループアドレス (G1) 宛にデータを配信します。

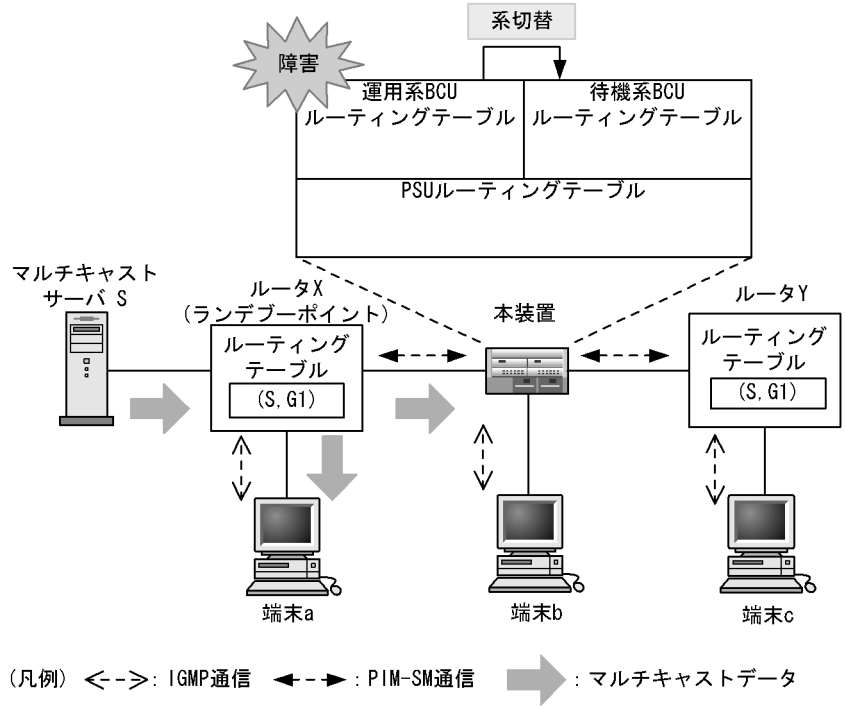
ランデブーポイントをルータ X とし，端末 a，b，c が IGMP によってグループ G1 に参加し，本装置，ルータ X，ルータ Y は PIM-SM の送受信を行いマルチキャストルーティング情報を作成します。
PIM-SM 系切替前を次の図に示します。
マルチキャストサーバ S が送信するマルチキャストデータは端末 a，b，c に配信されています。

図 4-15　BCU 切替 (PIM-SM 系切替前)



● 系切替発生
本装置運用系に障害が発生して系切替を行います。新待機系 BCU のマルチキャストルーティングテーブルを初期化します。
新運用系 BCU のマルチキャストルーティングテーブルと PSU のルーティングテーブルも系切替により初期化します。したがって，マルチキャストサーバ S が配信するマルチキャストデータは端末 a には配信されますが，端末 b，c には配信されません。
この状態から新運用系のマルチキャスト学習が始まります。
PIM-SM 系切替発生を次の図に示します。

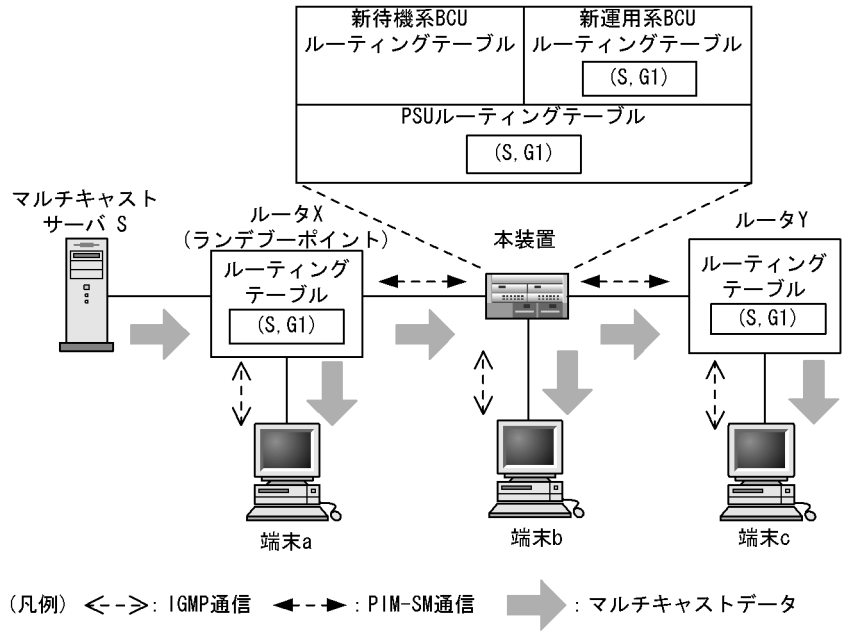
図 4-16　BCU 切替 (PIM-SM 系切替発生)



● 系切替後

本装置はルータ X，Y が本装置のダウンを検出する前に系切替を完了して，PIM-SM のやり取りを再開します。ルータ X，Y が送信する PIM-SM を受信し，マルチキャストルーティングテーブルを再学習します。また，端末 b と IGMP のやり取りを再開し，マルチキャスト G1 への参加の再認識を行い，マルチキャスト中継が再開し，マルチキャストデータを端末 a，b，c に配信します。PIM-SM 系切替後を次の図に示します。

図 4-17　BCU 切替 (PIM-SM 系切替後)



マルチキャスト中継が再開するまでの目安時間は経路交替開始時刻と経路情報数に依存する系切替時

間・対向装置認識時間・経路交換時間・経路計算時間の合計です。系切替時間はコンフィグレーションの量によって変化します。系切替発生時のマルチキャスト中継再開までの時間を次に示します。

- IPv4 PIM-SM/IPv6 PIM-SM のマルチキャスト中継再開時間は系切替およびユニキャスト経路再学習後 0 ～ 215 秒です。ただし，本装置がランデブーポイント (兼 BSR) の場合は 60 ～ 245 秒です。
- IPv4 PIM-SSM/IPv6 PIM-SSM のマルチキャスト中継再開時間は系切替およびユニキャスト経路再学習後 0 ～ 155 秒です。
- IPv4 PIM-DM のマルチキャスト中継再開時間は系切替およびユニキャスト経路再学習後 0 ～ 30 秒です。
- DVMRP のマルチキャスト中継再開時間は系切替後 0 ～ 70 秒です。

（e） マルチキャストルーティングプロトコルに PIM-SM（nonstop forwarding 機能）を使用している場合【OP-MLT】

IPv4 PIM-SM，IPv6 PIM-SSM は系切替時に通信を継続することが可能な nonstop forwarding 機能をサポートしています。

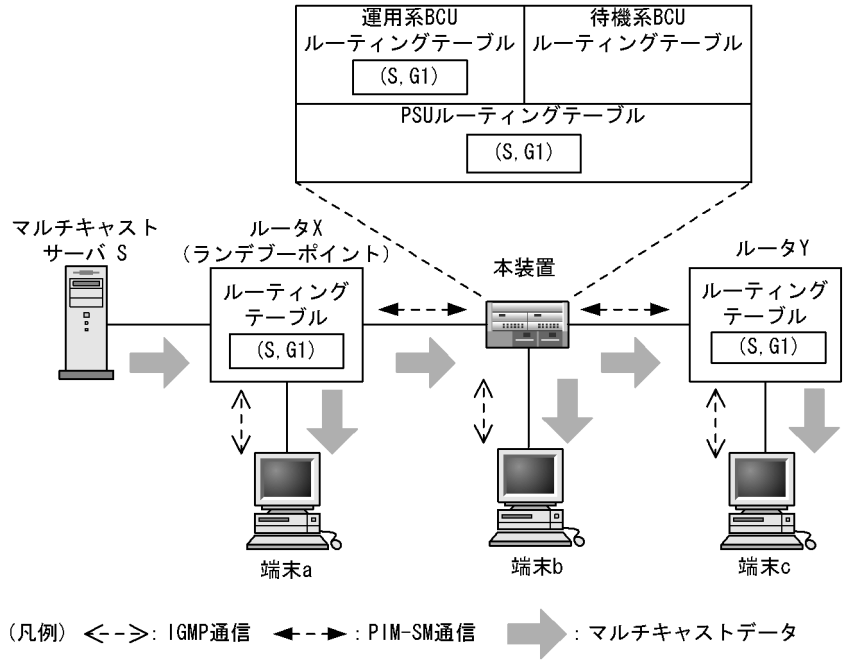
本機能は，コンフィグレーションで nonstop-forwarding 設定をした場合だけ有効です。
nonstop-forwarding 設定をしない場合は，「(d) マルチキャストルーティングプロトコルに PIM-SM を使用している場合【OP-MLT】」と同様の動作となります。

IPv4 PIM-SM，IPv6 PIM-SSM では動作が同じなので，IPv4 PIM-SM を例に nonstop forwarding 機能について説明します。

IPv6 PIM-SSM の場合は，IGMP が MLD となりランデブーポイントは存在しません。

● 系切替前
マルチキャストサーバ S がマルチキャストグループアドレス (G1) 宛にデータを配信します。
ランデブーポイントをルータ X とし，端末 a，b，c が IGMP によってグループ G1 に参加し，本装置，ルータ X，ルータ Y は PIM-SM の送受信を行いマルチキャストルーティング情報を作成します。
PIM-SM 系切替前を次の図に示します。
マルチキャストサーバ S が送信するマルチキャストデータは端末 a，b，c に配信されています。

図 4-18 BCU 切替（PIM-SM 系切替前）

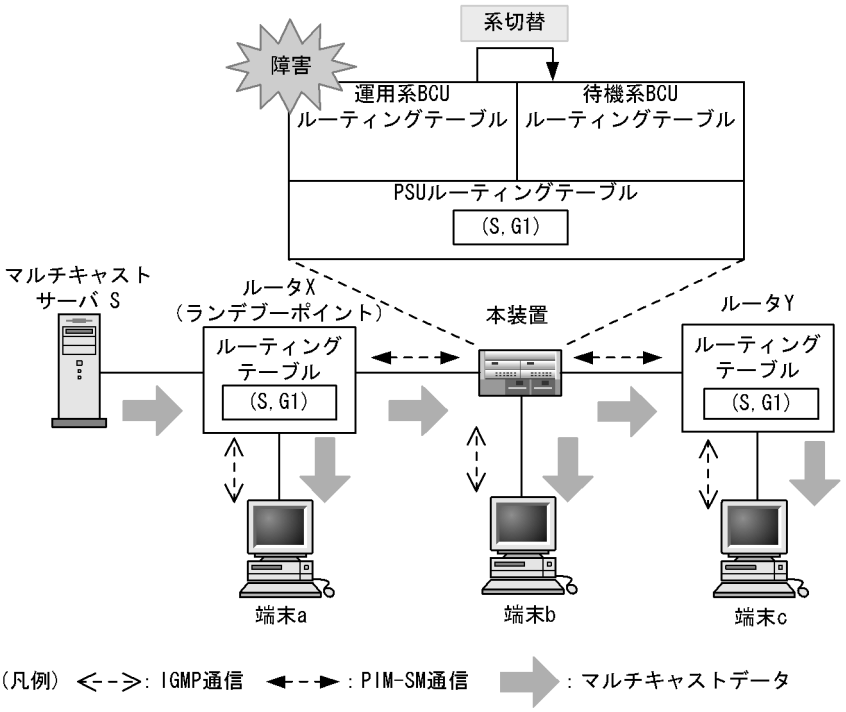


● 系切替発生

本装置運用系に障害が発生して系切替を行います。新待機系 BCU のマルチキャストルーティングテーブルは初期化されます。新運用系 BCU のマルチキャストルーティングテーブルはマルチキャストルーティングプロトコルの学習が始まっていないため，まだエントリはありません。PSU のルーティングテーブルを系切替によって初期化しません。また，ルータ X，Y も本装置のダウンを検出しないため，マルチキャストサーバ S から端末 a，b，c への配信は継続します。

PIM-SM 系切替発生を次の図に示します。

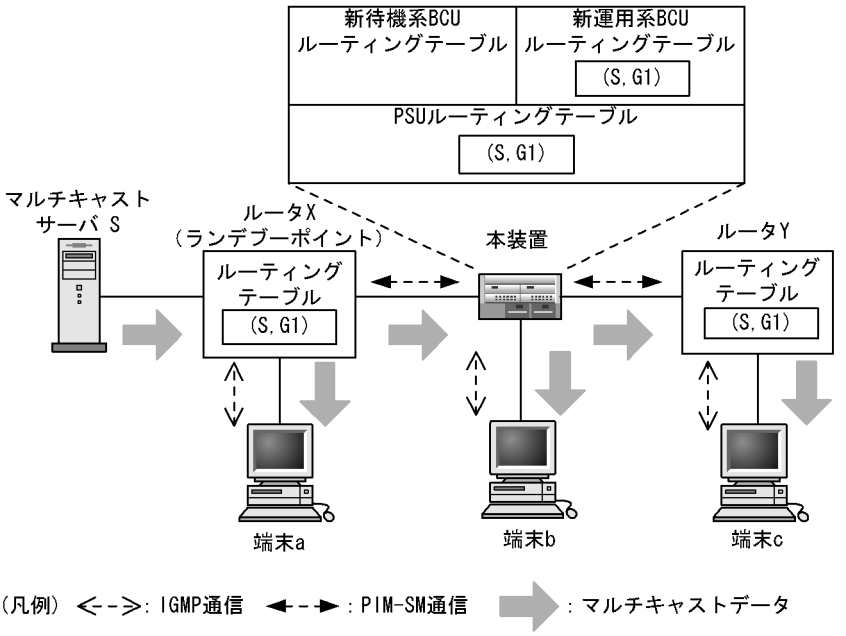
図 4-19 BCU 切替（PIM-SM 系切替発生）



● 系切替後

本装置はルータ X，Y が本装置のダウンを検出する前に系切替を完了して，PIM-SM のやり取りを再開します。ルータ X，Y が送信する PIM-SM を受信し，マルチキャストルーティングテーブルを再学習します。また，端末 b と IGMP のやり取りを再開し，マルチキャスト G1 への参加の再認識を行います。PSU，ルータ X，ルータ Y のマルチキャストルーティングテーブルが変化しないため，マルチキャストサーバ S から端末 a，b，c への配信は継続しています。再学習完了後，本装置は未学習のマルチキャスト中継エントリを PSU から削除します。PIM-SM 系切替後を次の図に示します。

図 4-20 BCU 切替（PIM-SM 系切替後）



[注意事項]

1. IPv4 PIM-SM nonstop forwarding 機能についての注意事項は「解説書 Vol.1　15.6.1(3) PIM-SM の使用」を参照してください。
2. IPv6 PIM-SSM nonstop forwarding 機能についての注意事項は「解説書 Vol.1　19.6.1(3) IPv6 PIM-SSM」を参照してください。

(3) BCU および BSU 切替時の本装置と相手ルータの中継動作【SB-5400S】

本装置の運用系に障害が発生して系切替が発生した場合，旧運用系で保持していた BCU および BSU のルーティングテーブルは新運用系に引き継がれないで初期化されます。このため，系切替が完了しても相手ルータからルーティング情報を再学習するまで通信が停止します。

(4) コンフィグレーション不一致時の処理

一重化の運用中に運用系のコンフィグレーションを変更したあとで二重化運用に戻した場合，運用系と待機系でコンフィグレーションの差分が生じます。この状態では系切替発生時に運用上の動作矛盾が発生する可能性があります。このため，本装置では警告メッセージを出すとともに両系のコンフィグレーションの同期が取れるまで以降の系切替を抑止，または系切替後 PSU(SB-5400S では BSU) が再起動します。

また，立ち上げ時にコンフィグレーションの差分が生じた場合も同様の処理をします。この場合は，ユーザ操作 (コマンド) でコンフィグレーションの同期を取る必要があります。

4.3 冗長構成時の注意事項

4.3.1 運用系 BCU または BSU の保守

運用系 BCU または BSU を保守によって交換する場合は，運用系と待機系をコマンドで系切替させたあとで，交換部位を待機系として保守作業を実行してください。

4.3.2 二重化運用開始時の注意事項

(1) 二重化立ち上げ時の注意事項

二重化運用開始時は，SB-7800S では BCU0 が運用系として，BCU1 が待機系として動作します。SB-5400S では BCU0・BSU0 が運用系として，BCU1・BSU1 が待機系として動作します。このとき BCU0 に実装されている MC が故障している場合や，正しく実装されていない状態で運用を開始すると，BCU1 が運用系として動作するまで 7 分 30 秒～ 10 分かかります。MC に異常が認められない場合には，SB-7800S のときは BCU0 の，SB-5400S のときは BCU0 または BSU0 の交換または抜去をして，保守作業を実行してください。

(2) メモリ搭載に関する注意事項

BCU 二重化運用開始時は，BCU0 および BCU1 のメモリ実装数を同じにしてください。異なるメモリ実装で運用を開始すると，オンラインコンフィグレーション変更が不正に終了したリ，系切替時に BCU 障害が発生したりする場合があります。BCU0 および BCU1 のメモリ実装については show system コマンドを使って確認してください。

4.3.3 二重化運用時の RM イーサネット (SB-5400S ではリモートマネージメントポート) に関する注意事項

(1) 使用する管理用ポート

二重化運用の RM イーサネット (SB-5400S ではリモートマネージメントポート) は運用系だけ管理用ポートとして使用できます。待機系の管理用ポートは使用できません。

(2) インタフェースケーブル接続

RM イーサネット (SB-5400S ではリモートマネージメントポート) を使用する場合は運用系および待機系の RM イーサネットコネクタ (SB-5400S ではリモートマネージメントポート) にインタフェースケーブルを接続してください。

(3) インタフェース種別の注意事項

二重化運用の待機系の RM イーサネット (SB-5400S ではリモートマネージメントポート) には定義が反映されず動作しません。ただし，リンクに関してはハードウェアの仕様上 10BASE-T 半二重固定になります。

4.3.4 MC2 世代管理運用時の注意事項

2 世代管理運用は異なる内容の MC を MC スロットに実装して運用することになります。このため，基本制御モジュール (BCU および BSU) の二重化と併用して世代管理で装置を運用すると MC または MC ス

ロットの障害によって非優先の MC スロットに実装された MC で起動された場合，系切替時に通信断または系切替が抑止された状態で起動されることになります。また，優先 MC スロットの設定値は基本制御モジュール (BCU) 上に記憶されるため，基本制御モジュール (BCU) のオンライン中のボード交換時に再設定する必要があります。この場合，運用系の現用 MC と同一内容の MC だけで基本制御モジュール (BCU) を起動し，優先 MC スロットを設定してください。

4.3.5 レイヤ 3 機能使用時に BCU 二重化運用する場合の注意事項

BCU を二重化した装置でコンフィグレーションの vlan 情報に IP アドレスを定義してレイヤ 3 通信を行う場合，local-mac-address 情報を定義して運用してください。local-mac-address 情報を定義しない場合，BCU の系切替後にレイヤ 3 通信が一時的に途切れることがあります。特に，スパニングツリーもしくは GSRP を併用する場合，通信断時間が長くなることがあります。

4.3.6 レイヤ 2 機能使用時に BCU 二重化運用する場合の注意事項

BCU を二重化した装置で系切替が発生すると，リンクアグリゲーション（LACP），スパニングツリー，および GSRP はプロトコル情報を再構築します。再構築が終わるまで各プロトコルが動作しているポートはブロッキング状態になります。その間，レイヤ 2 通信は一時的に途切れます。また，VLAN やリンクアグリゲーションに IP アドレスを設定している場合は，VLAN インタフェースやリンクアグリゲーションインタフェースがダウンするため，レイヤ 3 通信も一時的に途切れます。

5 GSRP

GSRP は，レイヤ 2 およびレイヤ 3 で装置の冗長化を行う機能です。この章では GSRP の概要について説明します。

5.1 GSRP 概説

5.1.1 概要

GSRP(Gigabit Switch Redundancy Protocol) は，スイッチに障害が発生した場合でも，同一ネットワーク上の別スイッチを経由して通信経路を確保することを目的とした装置の冗長化を実現する機能です。

レイヤ 2 ではネットワークの冗長化を行うスパニングツリー，レイヤ 3 ではデフォルトゲートウェイの冗長化を行う VRRP が冗長化機能として利用できますが，GSRP を使うと，レイヤ 2 とレイヤ 3 の冗長化を一つの機能で同時に実現できます。

● レイヤ 2

2 台のスイッチ間で制御するため，スパニングツリーよりも装置間の切り替えが高速です。また，ネットワークのコアスイッチを多段にするような大規模な構成にも適しています。

● レイヤ 3

2 台のスイッチで同一の IP アドレスと MAC アドレスを持つことでデフォルトゲートウェイを冗長化します。PC などに対するデフォルトゲートウェイに GSRP を適用することで，PC などから上流のネットワークへの通信経路を冗長化できます。デフォルトゲートウェイの装置に障害が発生した場合でも同一の IP アドレス，MAC アドレスを引き継いで切り替えることで PC などからのデフォルトゲートウェイを経由した通信を継続できます。

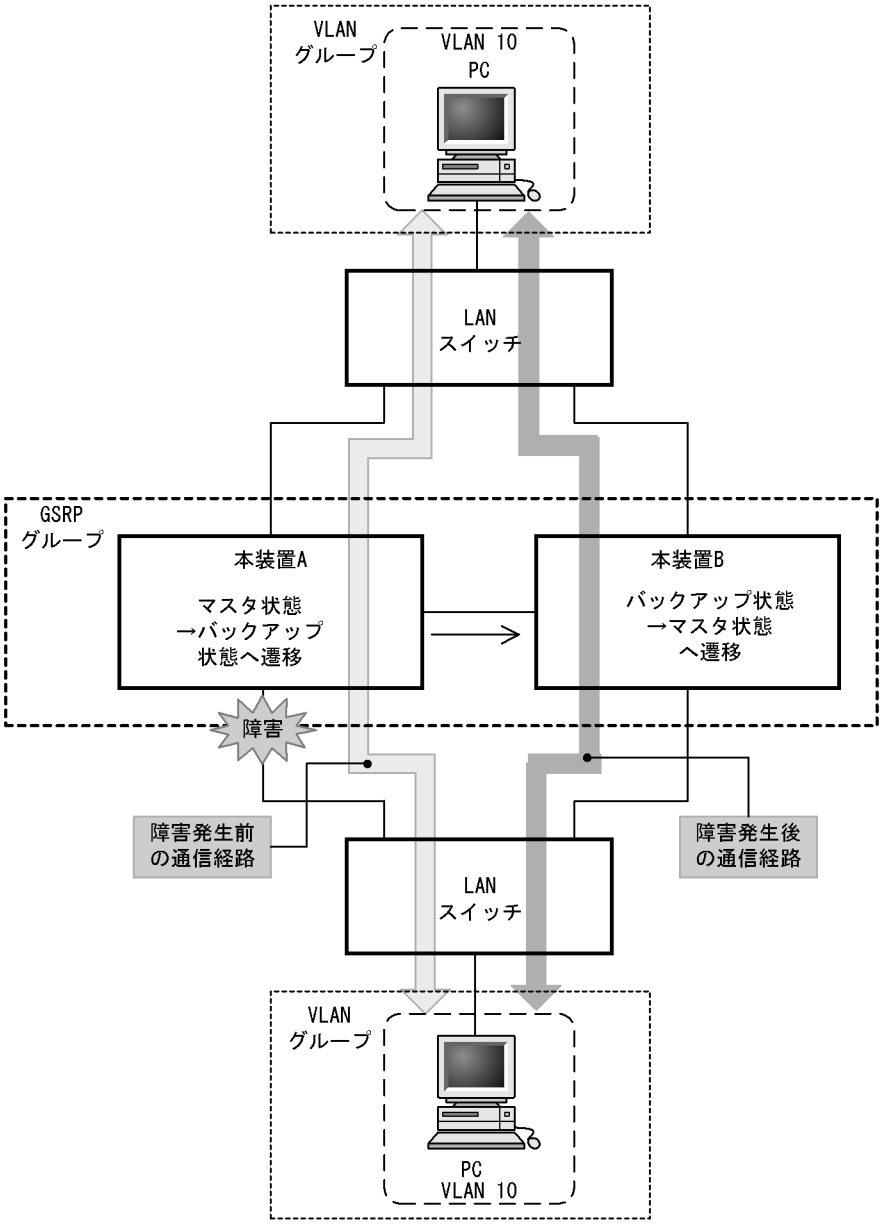
レイヤ 2 およびレイヤ 3 を同時に冗長化する機能の比較を次の表に示します。

表 5-1　レイヤ 2 およびレイヤ 3 を同時に冗長化する機能の比較

冗長化機能	説明
GSRP	• レイヤ 2 とレイヤ 3 の冗長化を一つの機能で実現しているため，管理が容易になる。 • 本装置独自仕様の機能のため他社装置との接続はできない。
スパニングツリー ＋ VRRP	• レイヤ 2 およびレイヤ 3 の両方で同時に冗長化を確保したい場合は，スパニングツリー，VRRP の両方の機能が必要である。 • 標準プロトコルのため，マルチベンダによるネットワークを構築できる。

GSRP によるレイヤ 2 の冗長化の概要を次の図に示します。

図 5-1 GSRP の概要



GSRP 機能を動作させる本装置 2 台をペアにしてグループを構成し，通常運用では片側がマスタ状態，もう一方がバックアップ状態として稼働します。マスタ状態の本装置 A はフレームをフォワーディングし，バックアップ状態の本装置 B はブロッキングします。回線障害や装置障害などが発生した場合，本装置 A，B 間でマスタ状態とバックアップ状態の切り替えを行います。これによって通信の継続が可能となります。

5.1.2 特徴

(1) 同時マスタ状態の回避

GSRP では本装置間を直接接続する回線上で状態確認用の制御フレームの送受信を行い，対向装置の状態を確認します。制御フレームの送受信が正常にできている間に回線障害などを検出した場合は，自動的に切り替えを行います。その際，本装置は，対向の本装置が確実にバックアップ状態として稼働中であるこ

とを確認した上でマスタ状態へ切り替わります。これにより 2 台の本装置が同時にマスタ状態となることを回避します。

また，装置障害などによって，制御フレームの送受信が正常にできなくなり，対向の本装置の状態が確認できない状態となった場合の切り替えは手動で行うことを基本とします。その理由は，対向の本装置がマスタ状態として稼働し続けている可能性があり，自動的にマスタ状態へ遷移したことによって，同時マスタ状態となることを回避するためです。運用者が障害の対応などを行い確実にマスタ状態へ切り替えても安全であると判断した上で，手動でマスタ状態へ切り替えることを想定しています。なお，手動による切り替えとは別に，本装置間を直接接続する回線のダウンを検出した場合には，対向装置障害と見なして自動的に切り替える機能もサポートしています。

(2) 制御フレームの送信範囲の限定

GSRP では，制御フレーム (GSRP Flush request) の送信範囲を限定し，不必要な個所へ送信されることを防止するため，制御フレームの送受信は指定した VLAN だけで行います。

5.1.3 サポート仕様

GSRP でサポートする項目と仕様を次の表に示します。

表 5-2 GSRP 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	○ (IPv4，IPv6)
装置当たりの GSRP グループ最大数		1
GSRP グループを構成する本装置の最大数		2
GSRP グループ当たりの VLAN グループ最大数		128
VLAN グループ当たりの VLAN 最大数		4095(SB-5400S の場合 4080)
GSRP Advertise フレーム送信間隔		0.5 ～ 60 秒の範囲で 0.5 秒単位
GSRP Advertise フレーム保有時間		1 ～ 120 秒の範囲で 1 秒単位
ロードバランス機能		○
バックアップ固定機能		○
ポートリセット機能		○
回線不安定時の連続切り替え防止機能		○

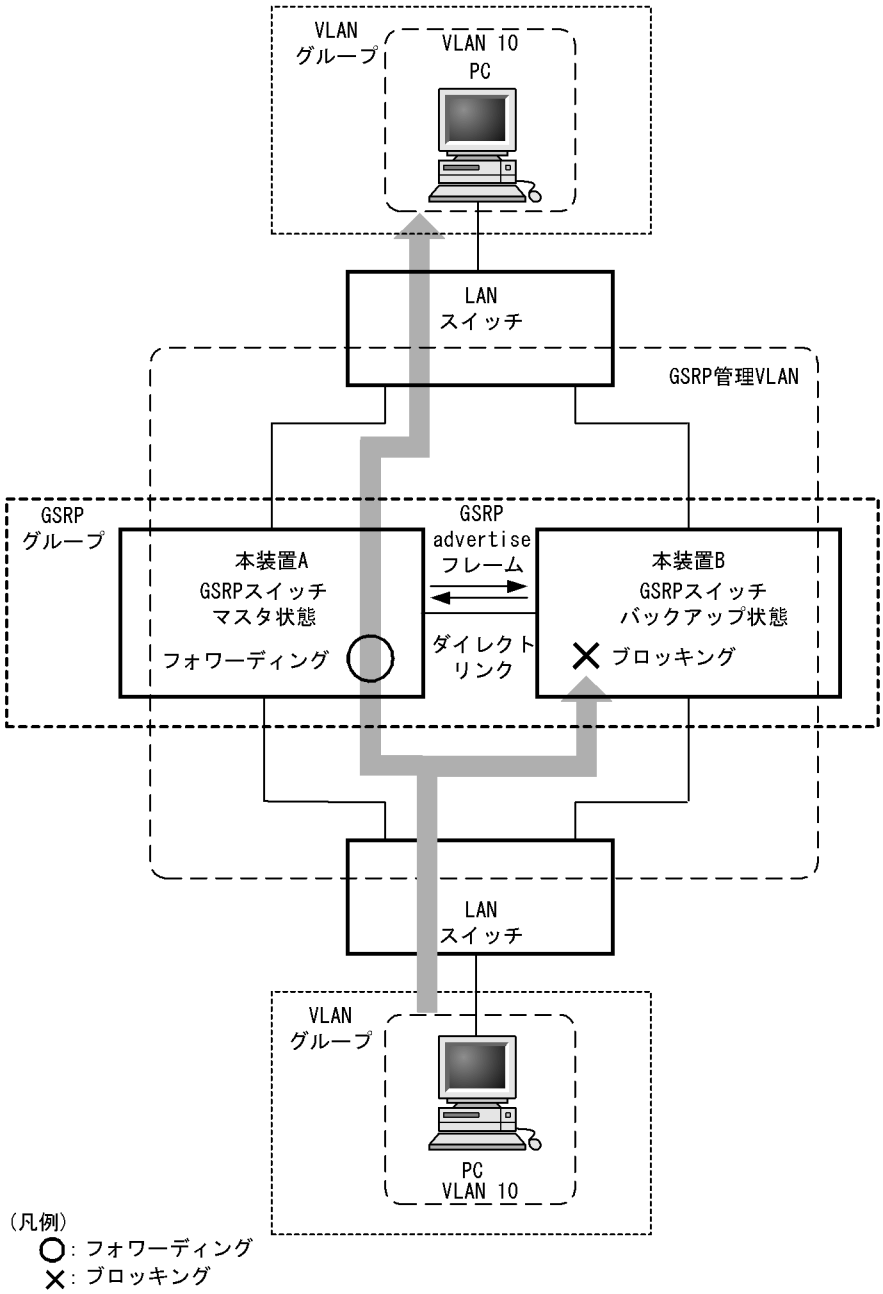
(凡例) ○：サポート

5.2 GSRP の基本原理

5.2.1 ネットワーク構成

GSRP を使用する場合の基本的なネットワーク構成を次の図に示します。

図 5-2 GSRP のネットワーク構成



GSRP の機能を動作させるスイッチを GSRP スイッチと呼びます。GSRP スイッチは 2 台のペアで GSRP グループを構成し，通常運用では片側がマスタ状態，もう一方がバックアップ状態として稼働します。GSRP ではこの 2 台の GSRP スイッチと周囲のスイッチとで三角形の構成を組むことを基本とします。

GSRP スイッチ同士の間は必ず回線を直接接続する必要があります。この GSRP スイッチ間の回線をダイレクトリンクと呼びます。

ダイレクトリンク上では GSRP Advertise フレームと呼ぶ状態確認用の制御フレームを送受信します。デフォルトの状態ではその他のデータフレームはブロッキングします。GSRP 制御対象外ポート設定するとデータフレームも送受信します。レイヤ 3 冗長切替機能を使用する場合，GSRP スイッチ間の通常データ中継のためにダイレクトリンクを使用する場合があり，その際にダイレクトリンクを GSRP 対象外ポートに設定します。詳細は「5.4　レイヤ 3 冗長切替機能」および「コンフィグレーションガイド　16.1.4 GSRP のレイヤ 3 冗長切替構成（RIP との組み合わせ）」を参照してください。

GSRP スイッチは GSRP Advertise フレームの送受信によって，互いの状態を確認し，マスタ状態，バックアップ状態の切り替え制御を行います。マスタ状態とバックアップ状態の切り替えは，VLAN グループと呼ぶ複数の VLAN をまとめた一つの論理的なグループ単位で行います。

マスタ状態の GSRP スイッチは指定された VLAN グループのフレームをフォワーディングしますが，バックアップ状態の GSRP スイッチではブロッキングします。

5.2.2　GSRP 管理 VLAN

GSRP を利用するネットワークでは，GSRP の制御フレームの送信範囲を限定するため，専用の VLAN の設定が必要です。この VLAN を GSRP 管理 VLAN と呼びます。GSRP ではこの GSRP 管理 VLAN 上だけで制御フレームを送受信します。

GSRP スイッチはマスタ状態へ遷移する際，周囲のスイッチに向けて FDB のクリアを要求するため，GSRP Flush request フレームと呼ぶ制御フレームを送信します。このため，GSRP 管理 VLAN には，ダイレクトリンクのポートだけでなく VLAN グループに参加させるすべての VLAN のポートを設定する必要があります。また，周囲のスイッチでも GSRP の制御フレームを受信できるよう GSRP 管理 VLAN と同一の VLAN の設定をしておく必要があります。

ただし，VLAN グループに参加させる VLAN のポートのうち，GSRP Flush request フレームの受信による FDB エントリのクリアをサポートしていないスイッチとの接続ポート，およびその対向のポートには，GSRP 管理 VLAN の設定は必要ありません。

5.2.3　GSRP の切り替え制御

GSRP スイッチで切り替えを行う際，フレームに対するフォワーディング，およびブロッキングの切り替え制御を行うだけでは，エンド - エンド間の通信は即座に再開できません。これは，周囲のスイッチの FDB において，MAC アドレスエントリが切り替え前にマスタ状態であった GSRP スイッチ向けに登録されたままであるためです。通信を即座に再開するためには，GSRP スイッチの切り替えと同時に，周囲のスイッチの FDB エントリをクリアする必要があります。

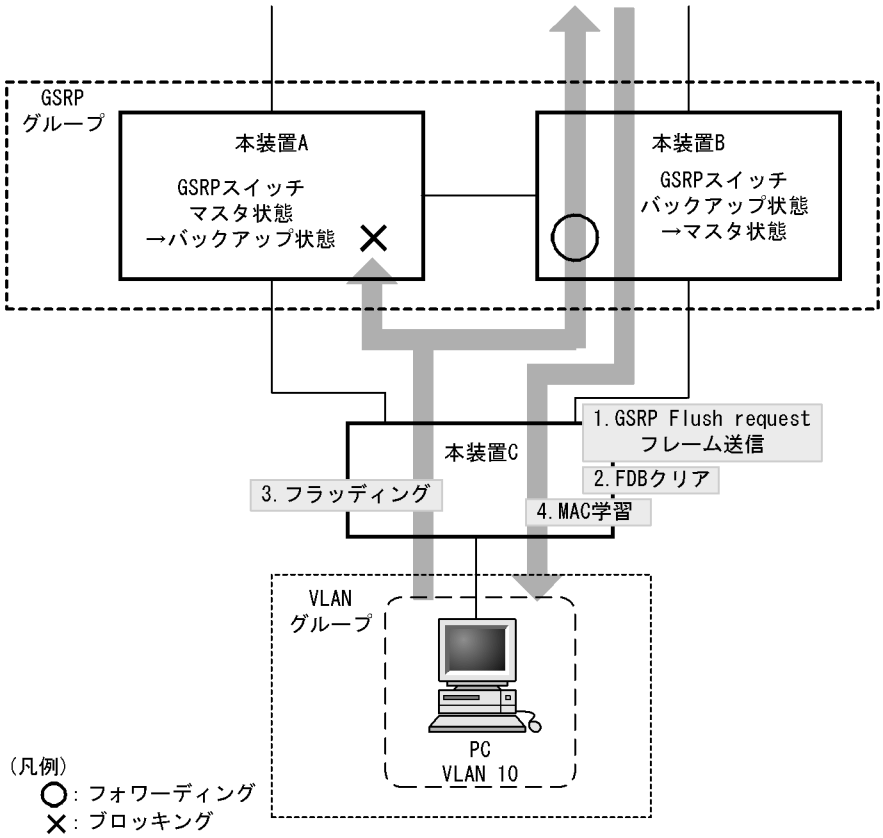
GSRP では，周囲のスイッチの FDB エントリをクリアする方法として下記をサポートしています。

（1） GSRP Flush request フレームの送信

GSRP では切り替えを行うとき，周囲のスイッチに対して FDB エントリのクリアを要求するため GSRP Flush request フレームと呼ぶ制御フレームを送信します。この GSRP Flush request フレームを受信して，自装置内の FDB のクリアを行うことのできるスイッチを GSRP aware と呼びます。本装置は特にコンフィグレーションの設定なしに，常に GSRP aware として動作します。GSRP aware は GSRP Flush request フレームをフラッディングします。一方，GSRP Flush Request フレームに対する機能をサポー

トしていないスイッチを GSRP unaware と呼びます。周囲のスイッチが GSRP unaware である場合は，「(2) ポートリセット機能」を使用する必要があります。GSRP Flush request フレームによる切り替え制御の概要を次の図に示します。

図 5-3　GSRP Flush request フレームによる切り替え制御の概要



1. 本装置 A と本装置 B との間で切り替えが行われ，本装置 B は GSRP Flush request フレームを本装置 C へ向けて送信します。
2. 本装置 C は GSRP Flush request フレームを受けて，自装置内の FDB をクリアします。
3. この結果，本装置 C 上は PC の送信するフレームに対して，MAC アドレスの学習が行われるまでフラッディングを行います。
   当該フレームは，マスタ状態である本装置 B を経由して宛先へフォワーディングされます。
4. 応答として PC 宛のフレームが戻ってくると，本装置 C は MAC アドレスの学習を行います。

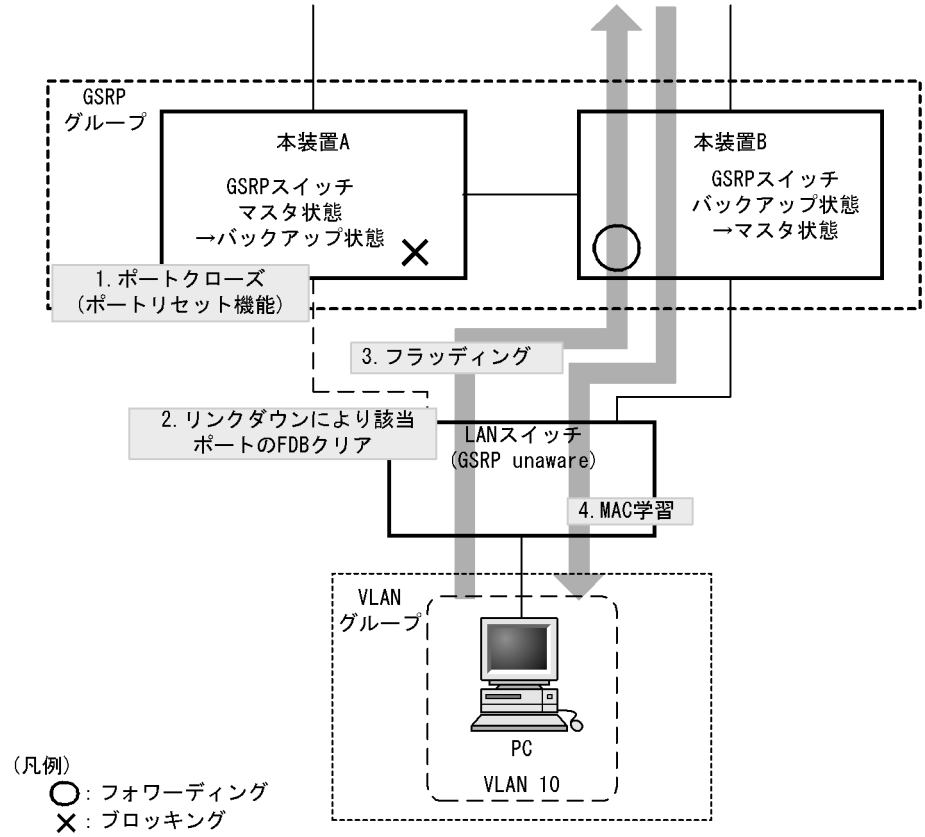
以後，本装置 C は PC からのフレームを本装置 B へ向けてだけフォワーディングするようになります。

(2) ポートリセット機能

ポートリセット機能は，GSRP スイッチにおいて周囲のスイッチと接続する物理ポートのリンクを一時的に切断する機能です。周囲のスイッチが GSRP unaware である場合に利用します。リンクの切断を検出したスイッチが該当物理ポート上で学習した MAC アドレスエントリを FDB からクリアする仕組みを利用します。

ポートリセット機能による切り替え制御の概要を次の図に示します。

図 5-4　ポートリセット機能による切り替え制御の概要



1. 本装置 A と本装置 B との間で切り替えが行われ，本装置 A はポートリセット機能によってリンクを切断します。
2. GSRP unaware である LAN スイッチ（以下，本説明内では単に GSRP unaware と表記します）はリンクダウンにより該当ポートの FDB をクリアします。
3. この結果，GSRP unaware は PC の送信するフレームに対して，MAC 学習されるまでフラッディングを行います。
   当該フレームは，マスタ状態である本装置 B を経由して宛先へフォワーディングされます。
4. 応答として PC 宛のフレームが戻ってくると，GSRP unaware は MAC の学習を行います。

以後，GSRP unaware は PC からのフレームを本装置 B へ向けてだけフォワーディングするようになります。

5.2.4　マスタ，バックアップの選択方法

（1）選択基準

GSRP スイッチは GSRP Advertise フレームを周期的に送受信し，当該フレームに含む VLAN グループ単位の選択基準の情報によって，VLAN グループ単位でマスタ，バックアップを決定します。GSRP でサポートするマスタ，バックアップの選択基準を次の表に示します。

表 5-3 GSRP でサポートするマスタ，バックアップの選択基準

項目	内容
アクティブポート数	装置内の VLAN グループに参加している全 VLAN(disable 状態の VLAN を除く) の物理ポートのうち，リンクアップしている物理ポートの数です。アクティブポート数の多いほうがマスタになります。リンクアグリゲーションを設定している場合は，リンクアグリゲーションを構成している全物理ポートを集約して 1 ポートとして換算します。
優先度	コンフィグレーションで指定する VLAN グループごとの優先度です。優先度の値の大きい方がマスタになります。
装置 MAC アドレス	装置の MAC アドレスです。MAC アドレス値の大きい方がマスタになります。

(2) 選択優先順

「(1) 選択基準」に示す選択基準の優先順をコンフィグレーションによって指定できます。指定できる順位を次に示します。

- アクティブポート数→優先度→装置 MAC アドレス （デフォルト）
- 優先度→アクティブポート数→装置 MAC アドレス

5.3 GSRP の動作概要

5.3.1 GSRP の状態

GSRP は五つの状態を持ち動作します。状態の一覧を次の表に示します。

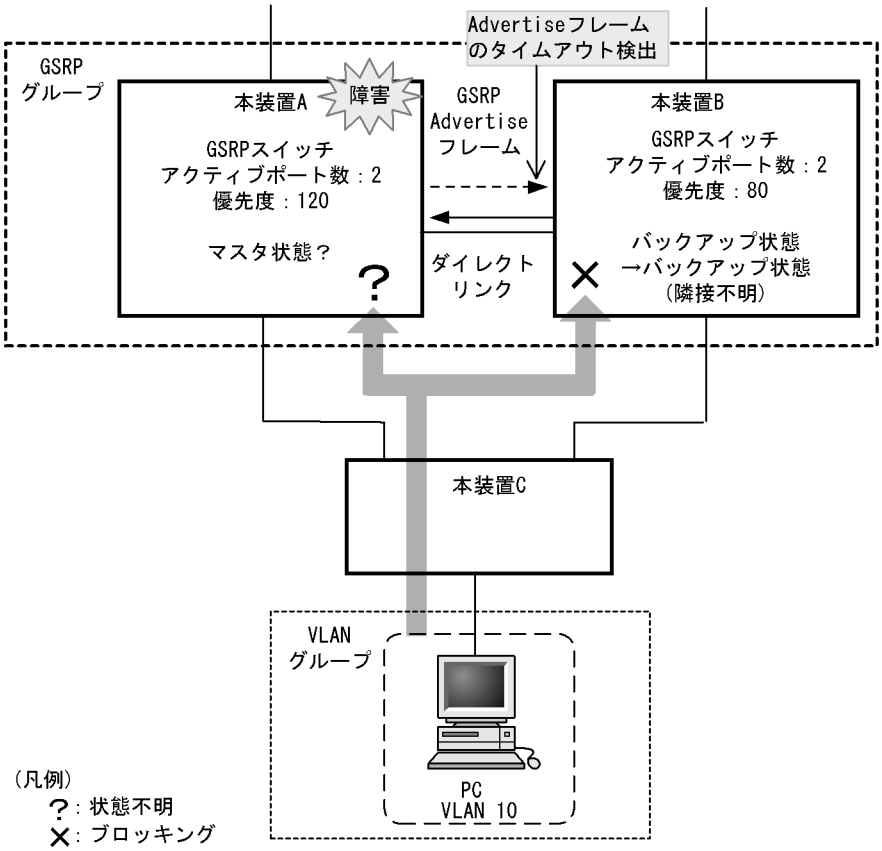
表 5-4 GSRP の状態一覧

状態	内容
バックアップ	バックアップ状態として稼働する状態です。バックアップ状態の GSRP スイッチは，VLAN グループ内の VLAN に対してポートごとにブロッキングします。GSRP 制御フレーム以外のフレームの中継は行わないため，MAC 学習は行いません。初期稼働時は必ずバックアップ状態から開始します。
バックアップ（マスタ待ち）	バックアップ状態からマスタ状態へ切り替わる際，対向の GSRP スイッチが確実にバックアップ状態，またはバックアップ（固定）状態であることを確認するための過渡的な状態です。バックアップ（マスタ待ち）状態では，バックアップ状態と同様，GSRP 制御フレーム以外のフレームの中継は行いません。
バックアップ（隣接不明）	バックアップ状態，およびバックアップ（マスタ待ち）状態で，対向の GSRP スイッチからの GSRP Advertise フレームの受信タイムアウトを検出した際に遷移する状態です。対向の GSRP スイッチはマスタ状態として稼働中の可能性があるため，GSRP Advertise フレームを再受信する，または運用コマンド（set gsrp master コマンド）によってマスタ状態へ遷移させる以外は，本状態で留まり続けます。バックアップ（隣接不明）状態では，バックアップ状態と同様，GSRP 制御フレーム以外のフレームの中継は行いません。
バックアップ（固定）	コンフィグレーション（コンフィグレーションコマンド gsrp の backup-lock サブコマンド）によって，強制的にバックアップ固定にされた状態です。コンフィグレーションが削除されるまで，本状態で留まり続けます。バックアップ（固定）状態では，バックアップ状態と同様，GSRP 制御フレーム以外のフレームの中継は行いません。
マスタ	マスタ状態として稼働する状態です。マスタ状態の GSRP スイッチは，VLAN グループ内の VLAN に対してポートごとにフォワーディングします。GSRP 制御フレームを含むすべてのフレームの中継を行い，MAC 学習を行います。

5.3.2 装置障害時の動作

次の図に装置障害時の動作例を示します。

図 5-5　装置障害時の動作



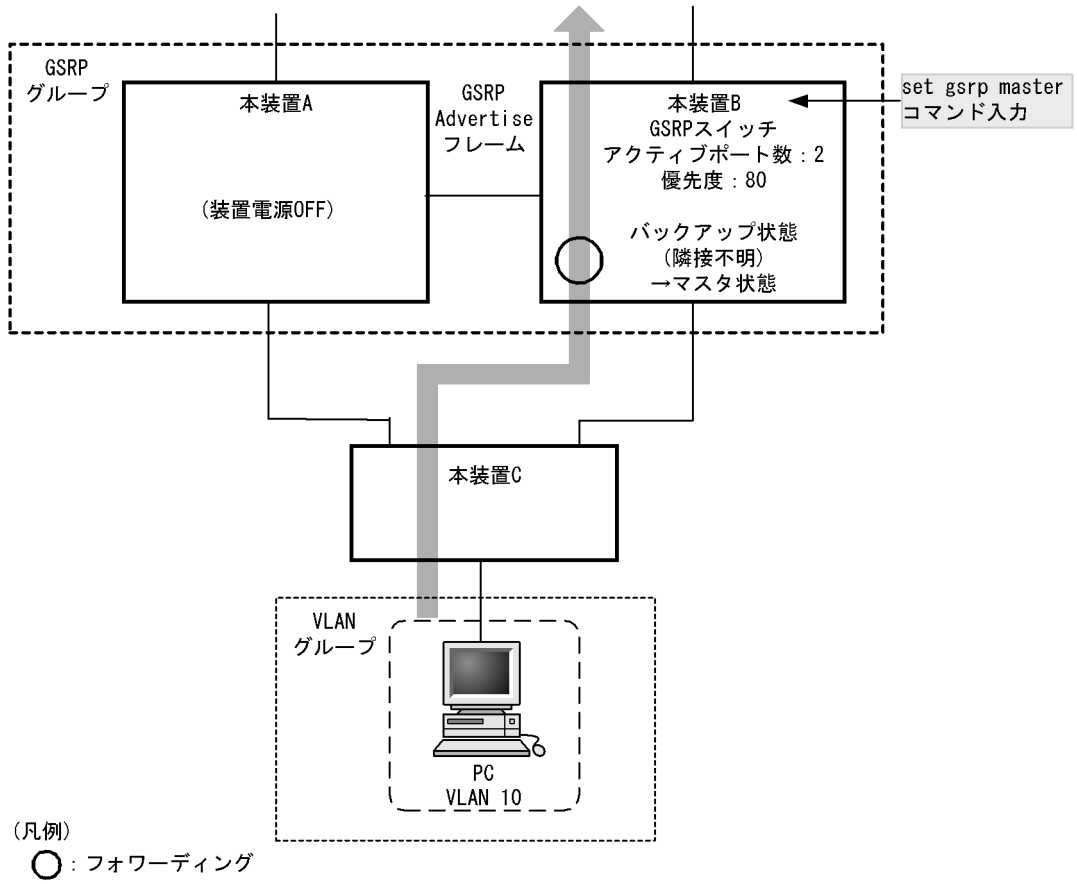
装置障害などが発生したことによって，マスタ状態の本装置 A が GSRP Advertise フレームを正常に送信できなくなった場合，本装置 B は本装置 A からの GSRP Advertise フレームの受信タイムアウトを検出します。このとき，本装置 B はバックアップ（隣接不明）状態に遷移します。バックアップ（隣接不明）状態では，バックアップ状態と同様，フレームの中継は行いません。バックアップ（隣接不明）状態になった場合，メッセージを出力し，運用者に対して装置の状態の確認を促します。

GSRP では，バックアップ（隣接不明）状態となった本装置 B をマスタ状態へ切り替える手段として手動で切り替える方法と，自動的に切り替える方法の二つをサポートしています。

● 手動による切り替え

GSRP では手動でマスタ状態へ切り替えるための運用コマンド（set gsrp master コマンド）をサポートしています。運用者は本装置 A のポートがブロッキングされていること，または装置が起動していないことを確認したうえで，本コマンドを使用することによって本装置 B をマスタ状態に遷移させることができます。set gsrp master コマンド入力後の動作を次の図に示します。

図 5-6　set gsrp master コマンド入力後の動作



● 自動での切り替え（ダイレクトリンク障害検出）

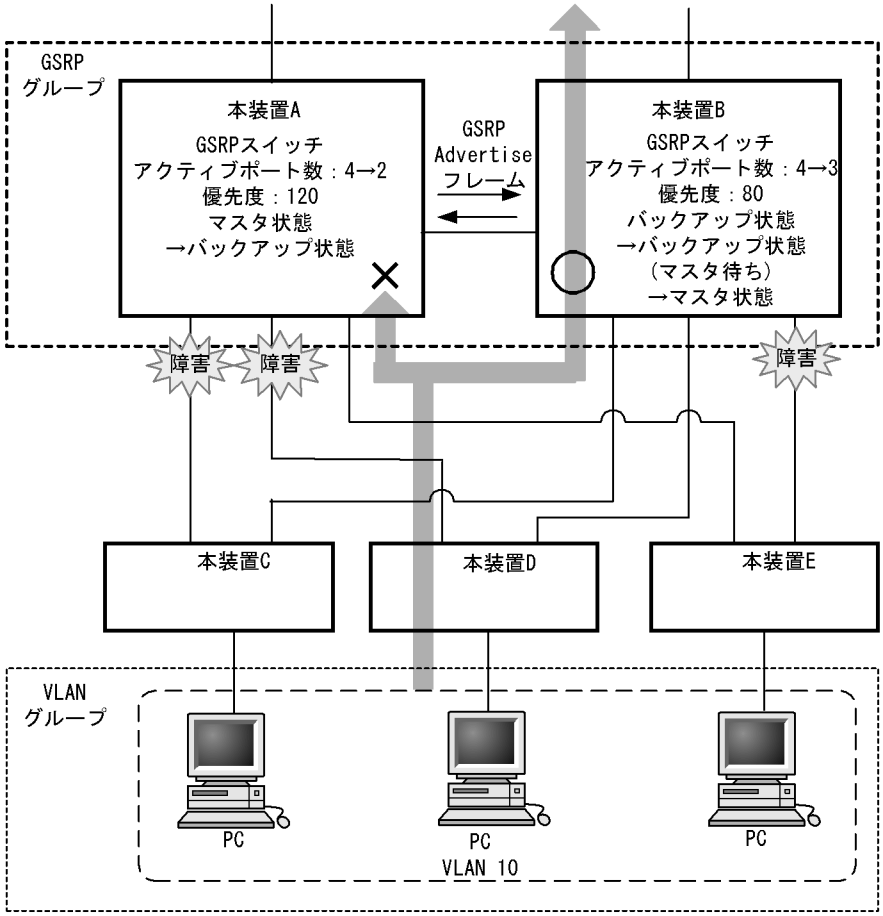
コンフィグレーションコマンド gsrp の no-neighbor-to-master サブコマンドで direct-down を指定することによって，バックアップ（隣接不明）状態に遷移した際，ダイレクトリンクのポートがダウン状態であれば，対向装置が装置障害状態であるとみなして，自動的にマスタ状態へ遷移します。

5.3.3　回線障害時の動作

(1) 回線障害時の動作例

次の図に回線障害時の動作例を示します。

図 5-7　回線障害時の動作例



この図では，本装置 A がマスタ状態，本装置 B がバックアップ状態として稼働している状況で，本装置 A と本装置 C，および本装置 D の間の回線と，本装置 B と本装置 E の間の回線で障害が発生した場合を示しています。本装置 A，および本装置 B で，マスタ，バックアップの選択優先順としてアクティブポート数を最優先とした設定をしている場合，本装置 B は，アクティブポート数が本装置 A よりも多くなるため，マスタになることを選択します。本装置 B は，マスタ状態へ遷移する前に，一旦バックアップ（マスタ待ち）状態へ遷移します。バックアップ（マスタ待ち）状態に遷移した本装置 B は，本装置 A からの GSRP Advertise フレームを待ちます。GSRP Advertise フレームを受信したら，本装置 A がバックアップ状態であることを確認したうえで，マスタ状態へ遷移します。なお，この図に示す例では，本装置 E はマスタ状態である本装置 B との間の回線が障害となっているため，通信ができなくなります。

(2) 回線不安定時の連続切り替え防止機能

GSRP では，マスタ状態とバックアップ状態の選択基準としてアクティブポート数を用います。このため，回線のアップ，ダウンが頻発するなど回線が不安定な状態となった場合にアクティブポート数の増減が多発し，結果マスタ状態とバックアップ状態の切り替えが連続して発生する可能性があります。

このため，GSRP では回線が安定化したことを運用者が確認できるまでの間，アップした回線のポートをアクティブポート数としてカウントしないようにするための遅延時間をコンフィグレーション（コンフィグレーションコマンド gsrp の port-up-delay サブコマンド）によって設定することが可能です。これに

よって，回線不安定時の不用意な切り替えを抑止することができます。

port-up-delay サブコマンドでは 1 から 43200 秒（12 時間）内で 1 秒単位に指定が可能です。また，infinity と設定することで，遅延時間を無限とすることも可能です。回線が安定したことを確認できた場合，port-up-delay サブコマンドで指定した遅延時間を待たずに即時にアクティブポート数としてカウントするための運用コマンド（clear gsrp port-up-delay コマンド）もサポートしています。

5.3.4 バックアップ固定機能

バックアップ固定機能によって，GSRP スイッチを強制的にバックアップ状態にすることができます。コンフィグレーション（コンフィグレーションコマンド gsrp の backup-lock サブコマンド）によって，バックアップ（固定）状態になり，コンフィグレーションが削除されるまで本状態で留まり続けます。バックアップ（固定）状態では，バックアップ状態と同様，GSRP 制御フレーム以外のフレームの中継は行いません。

GSRP では，マスタ状態とバックアップ状態の選択要因としてアクティブポート数を使います。アクティブポート数は VLAN グループに所属している VLAN のポート数であり，VLAN にポートを追加するときや，ネットワーク構成を変更するときはアクティブポート数の増減が伴います。このようなとき，通常はマスタ状態およびバックアップ状態の両方の装置に同じ変更が反映されますが，作業中，一時的にバックアップ状態の装置のアクティブポート数がマスタ状態の装置を超えると，マスタ状態とバックアップ状態の切り替えが発生します。

マスタ状態とバックアップ状態の選択基準に関わる設定や構成を変更する際に，作業の完了が確認できるまでの間は強制的にバックアップ状態にすることで安全に構成変更を行うことができます。これによって，設定や構成の変更作業時に GSRP の切り替えが発生することを回避できます。

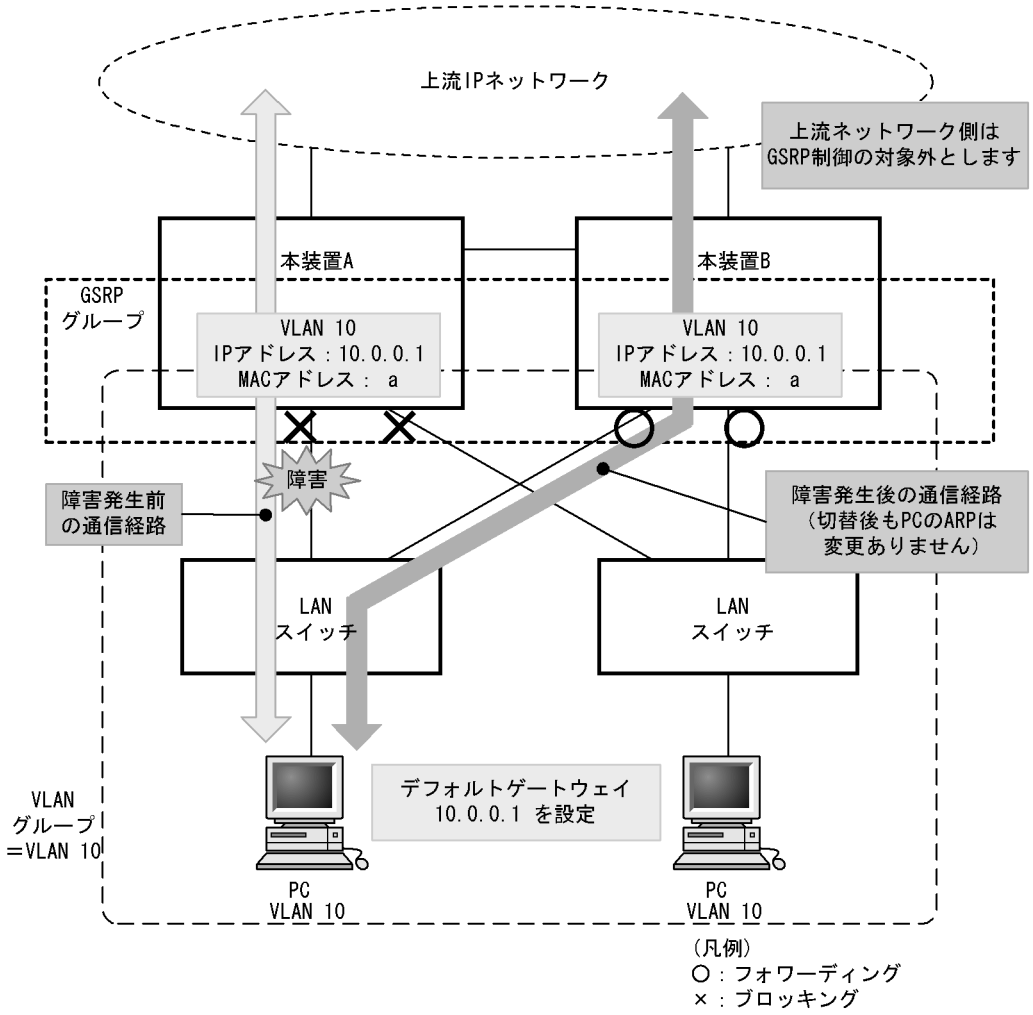
5.4 レイヤ 3 冗長切替機能

5.4.1 概要

レイヤ 3 冗長切替機能は，2 台のスイッチが同一の IP アドレスと MAC アドレスを引き継いで切り替えることで PC などからのデフォルトゲートウェイを経由した通信を継続できるようにします。

GSRP レイヤ 3 冗長切替機能の概要を次に示します。なお，ここでは PC などを接続するネットワークを下流ネットワークと呼び，そこから IP 中継する先のネットワークを上流ネットワークと呼びます。GSRP のマスタ / バックアップ切り替えは下流ネットワーク側に反映します。

図 5-8 GSRP レイヤ 3 冗長切替機能の概要



（1） デフォルトゲートウェイの IP アドレス

GSRP で冗長化するデフォルトゲートウェイの IP アドレスは，2 台の GSRP スイッチで同じ VLAN に同じアドレスを設定します。マスタ状態の GSRP スイッチは VLAN がアップ状態となり，デフォルトゲートウェイとして IP 中継を行います。バックアップ状態の GSRP スイッチの VLAN はダウン状態となり IP 中継を行いません。

（2） デフォルトゲートウェイの MAC アドレス

GSRP で冗長化するデフォルトゲートウェイの MAC アドレスは GSRP のプロトコル専用の仮想 MAC アドレスを使用します。仮想 MAC アドレスは，VLAN グループ番号ごとに異なるアドレスを使用します。

マスタ状態の装置は，下流の LAN スイッチに仮想 MAC アドレスを学習させるために，仮想 MAC アドレスを送信元 MAC アドレスとした GSRP 制御フレームを定期的に送信します。

GSRP で使用する仮想 MAC アドレスを以下に示します。

VLAN グループ番号が 8 以下の場合は，次に示す方法で仮想 MAC アドレスを生成します。

図 5-9　GSRP レイヤ 3 冗長切替機能の仮想 MAC アドレスの生成方法 (VLAN グループ番号が 8 以下)

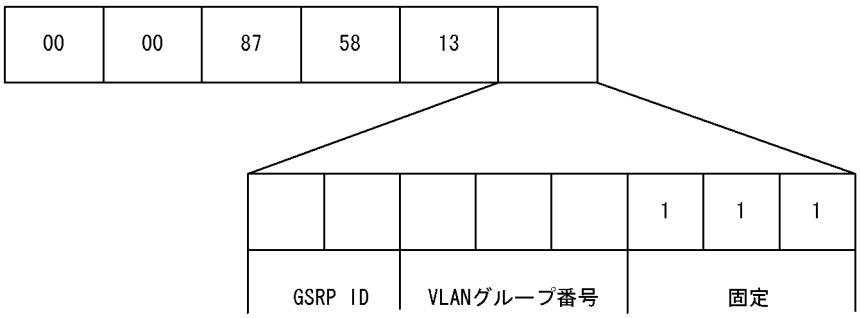


表 5-5　GSRP レイヤ 3 冗長切替機能の仮想 MAC アドレスの生成方法 (VLAN グループ番号が 8 以下)

項目	値
GSRP ID	GSRP ID 1 ～ 4 に対し，0 ～ 3 の値を設定します。レイヤ 3 冗長切替機能では，GSRP ID は 1 ～ 4 の値である必要があります。
VLAN グループ番号	VLAN グループ番号 1 ～ 8 に対し，0 ～ 7 の値を設定します。
固定（3 ビット）	最下位 3 ビットは 7 固定とします。

VLAN グループ番号が 9 以上の場合は，00:00:87:58:13:11 ～ 00:00:87:58:13:99 の範囲の仮想 MAC アドレスを，VLAN グループ番号 9 ～ 128 に順番に割り当てます。

5.4.2　上流ネットワーク障害時の切り替え

上流ネットワーク側は GSRP の制御対象から外し IP ルーティングを設定します。レイヤ 3 冗長切替機能を使用する場合，上流ネットワーク側の障害は IP ルーティング機能によって検出して経路を切り替えます。

上流ネットワーク側は，2 台の GSRP スイッチがどちらも上流ネットワークへ接続し，また一方のポートなどに障害が発生した場合はもう一方の GSRP スイッチを経由して通信を継続できるよう GSRP スイッチ間の通信経路も確保します。

上流ネットワークの障害に対応した設定の概要と，障害時の通信経路の例を，次の図に示します。

図 5-10　上流ネットワークの障害に対応した設定

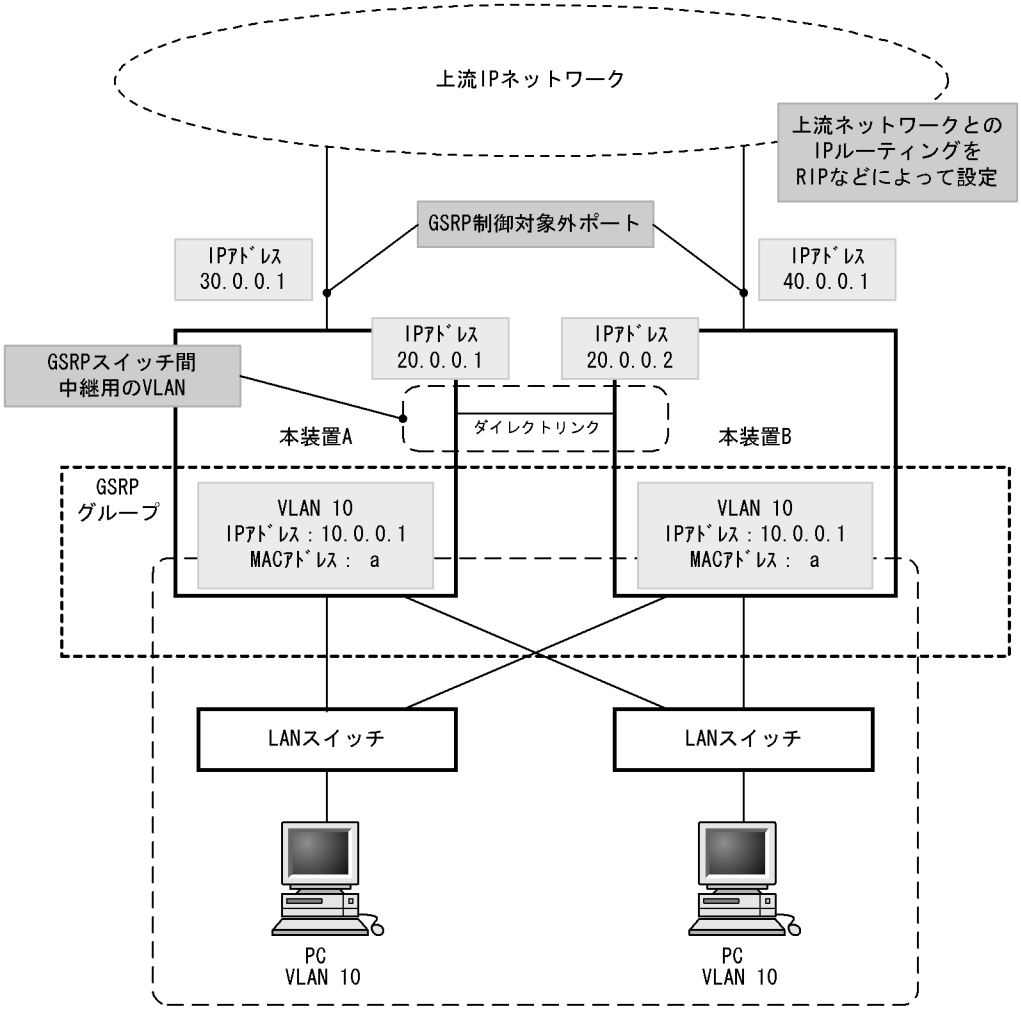
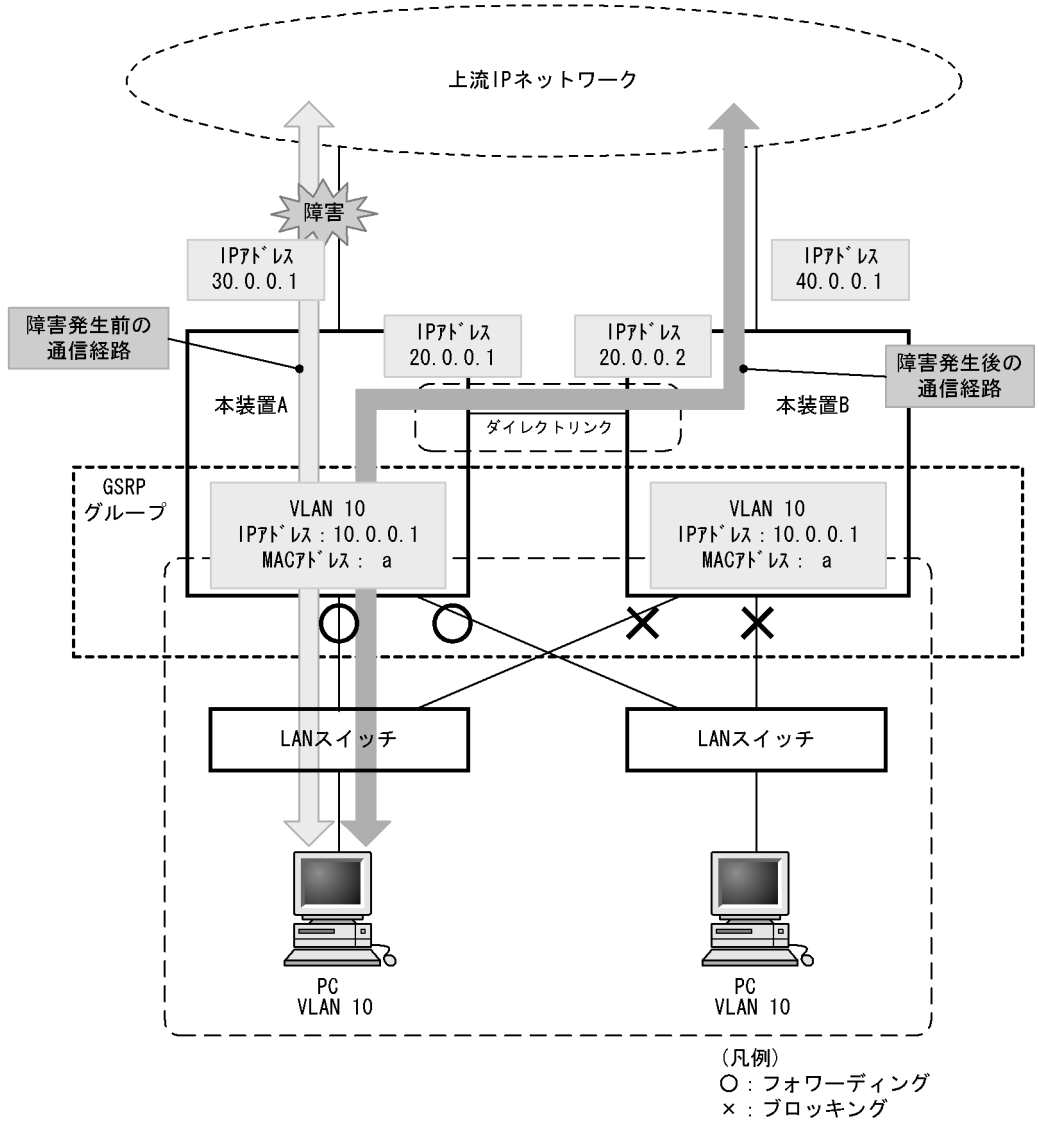


図 5-11　上流ネットワークの障害発生時の通信経路



（1） 上流ネットワーク側のポートの設定

上流ネットワーク側のポートは GSRP 制御対象外ポート（コンフィグレーションコマンド gsrp-exception-port）として設定し，マスタ / バックアップどちらの状態においても通信可能なポートとします。そこに IP アドレスおよび IP ルーティングを設定することで上流ネットワークと接続します。

IP ルーティングは，2 台の GSRP スイッチがどちらも上流ネットワークと通信できるよう設定します。また，上流ネットワーク向けの障害が検出できるよう，ダイナミックルーティングもしくはスタティックルーティングの動的監視機能を設定します。

（2） GSRP スイッチ間の設定

上流ネットワークとは 2 台の GSRP スイッチ両方を通信可能な状態とするため，バックアップ側の GSRP スイッチに上流ネットワークからパケットが届く場合があります。そのようなパケットをマスタ側の GSRP スイッチに中継するために，GSRP スイッチ間にレイヤ 3 での通信経路を設定します。

GSRP スイッチ間はダイレクトリンクを接続し GSRP 管理 VLAN 上で GSRP Advertise フレームのやり

とりをします。このダイレクトリンク上に GSRP 管理 VLAN 以外の VLAN と IP ルーティングを設定することで，GSRP スイッチ間の中継ができます。ただし，下流からのトラフィックを直接上流ネットワークに中継するために，GSRP スイッチ間を中継する経路は優先度の低い経路となるよう IP ルーティングを設定してください。

なお，このような上流ネットワークの設定を含めたレイヤ 3 冗長切替機能の設定例は，「コンフィグレーションガイド　16.1 GSRP」を参照してください。

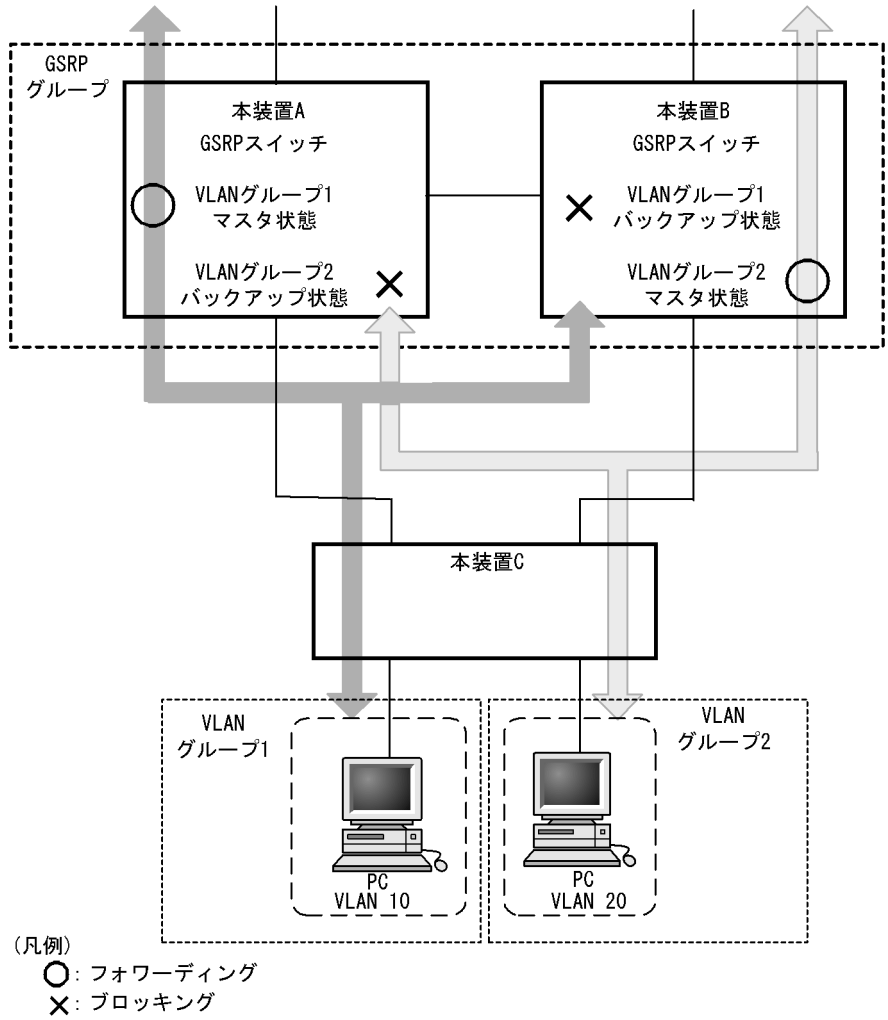
5.5 GSRP のネットワーク設計

5.5.1 VLAN グループ単位のロードバランス構成

GSRP では，VLAN グループ単位にマスタ状態，バックアップ状態の状態管理を行います。1 台の GSRP スイッチで最大 128 個の VLAN グループまで設定が可能です。複数の VLAN グループを同居させることで，VLAN グループ単位のロードバランス構成をとり，トラフィックの負荷分散を図ることが可能です。ロードバランス構成の概要を次の図に示します。

この図では，本装置 A が VLAN グループ 1 に対してマスタ状態，VLAN グループ 2 に対してバックアップ状態で動作，また本装置 B が VLAN グループ 1 に対してバックアップ状態，VLAN グループ 2 に対してマスタ状態で動作している例を示しています。

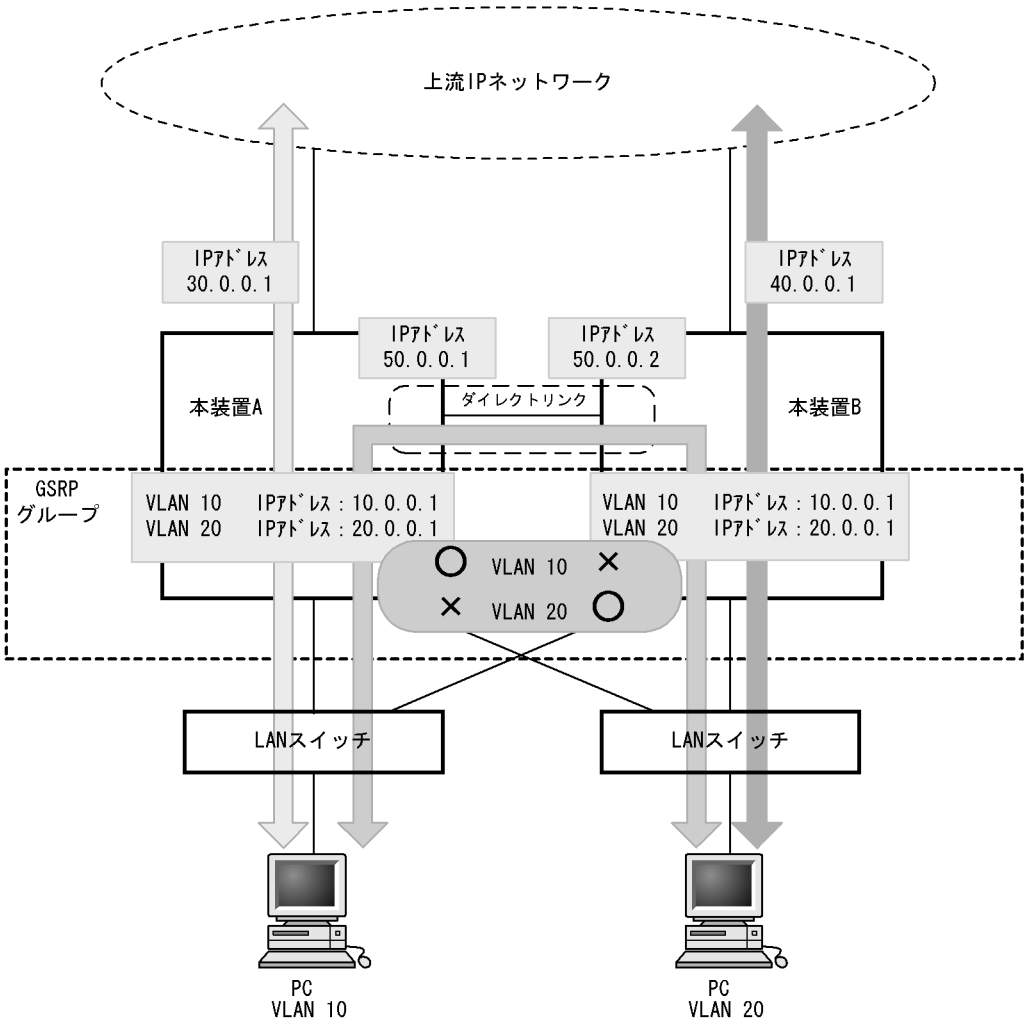
図 5-12 ロードバランス構成



レイヤ 3 冗長切替機能でロードバランス構成をとると，異なる装置がマスタ状態の VLAN 間で通信するためには GSRP スイッチ間で通信経路を確保する必要があります。この通信は，「5.4.2 上流ネットワーク障害時の切り替え」で示したダイレクトリンク上の VLAN で行います。レイヤ 3 冗長切替を使用する場合のロードバランス構成の概要を次の図に示します。

この図では，本装置 A が VLAN 10 に対してマスタ状態，本装置 B が VLAN 20 に対してマスタ状態で動作しています。上流 IP ネットワークへの通信はそれぞれマスタ状態の装置を経由します。VLAN10 と VLAN20 の間での通信はダイレクトリンク上の VLAN を経由します。

図 5-13　レイヤ 3 冗長切替機能使用時のロードバランス構成

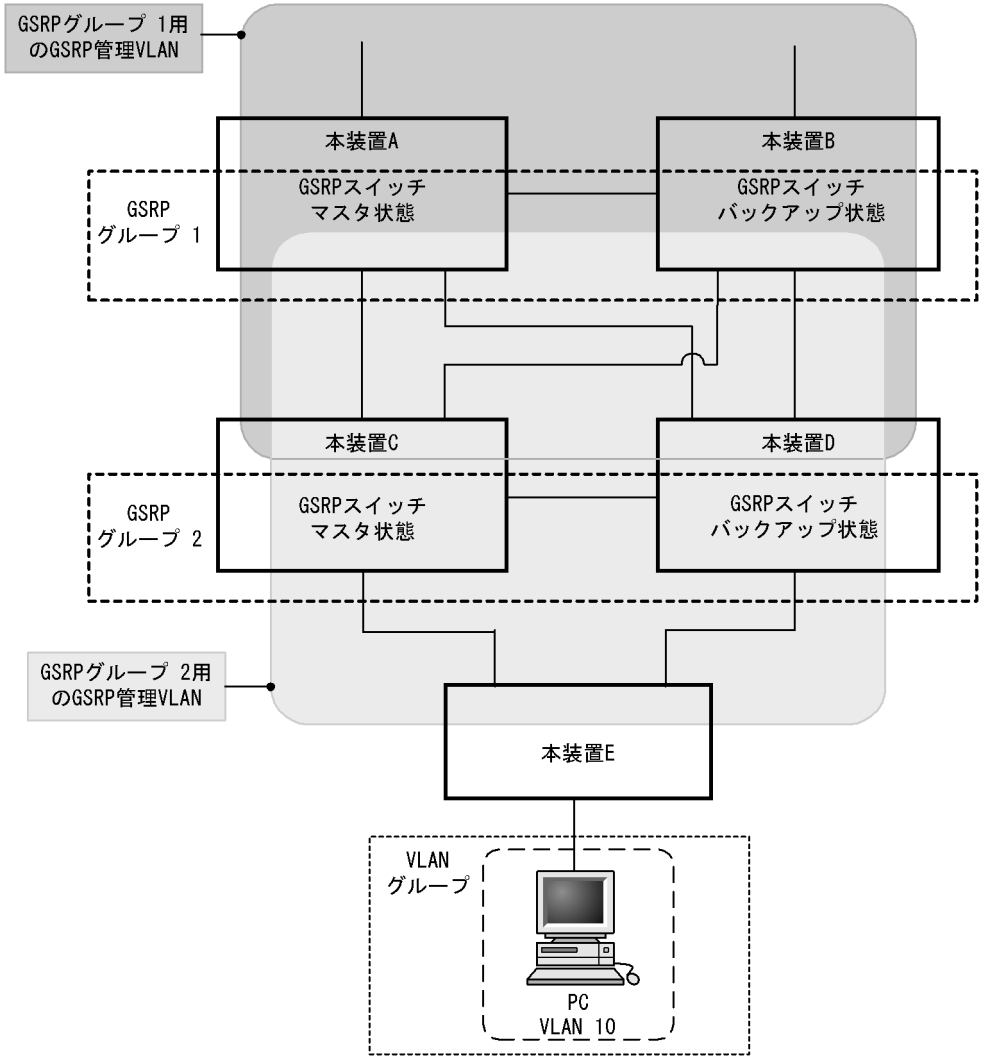


（凡例）○：マスタ状態
　　×：バックアップ状態

5.5.2　GSRP グループの多段構成

GSRP では，同一のレイヤ 2 ネットワーク内に複数の GSRP グループを多段にした構成をとることが可能です。これによって大規模ネットワークでも，冗長性を確保することができます。GSRP グループを多段構成にする場合，GSRP の制御フレームの送信範囲を限定するため，GSRP グループごとに GSRP 管理 VLAN を設定します。GSRP グループの多段構成の概要を次の図に示します。

図 5-14 GSRP グループの多段構成



この図では，本装置 A と本装置 B で GSRP グループ 1 を，本装置 C と本装置 D で GSRP グループ 2 を構成した場合を示しています。各 GSRP グループはそれぞれ独立して動作するため，ある GSRP グループでマスタ状態とバックアップ状態の切り替えが発生しても，ほかの GSRP グループでの動作には影響しません。GSRP 管理 VLAN は GSRP スイッチを中心に周囲のスイッチを含めた VLAN として設定します。

5.6 GSRP 使用時の注意事項

（1） GSRP と VRRP 機能との混在利用について

同一装置内で VRRP 機能と GSRP 機能は同時に使用できません。

（2） ポートリセット機能を使用する場合について

ポートリセット機能を設定した物理ポートと対向のスイッチとの間に伝送装置などを設置した場合，対向のスイッチで正しくポートのリンクダウンを検出できない可能性があります。ポートリセット機能を使用する場合は，対向のスイッチでポートのリンクダウンが直接検出できるようにネットワークの設計を行うようお願いします。

（3） ポートリセット機能をロードバランス構成で使用する場合について

同一の物理ポートを複数の VLAN グループで共有し，かつその物理ポートに対してポートリセット機能を設定した場合，ある VLAN グループでマスタ状態からバックアップ状態に切り替わった際，別の VLAN グループではマスタ状態として稼働しているにもかかわらずポートのリンクをダウンさせるため通信断となります。このダウンによる一時的な通信断を回避したい場合は，複数の VLAN グループで同一の物理ポートを共有しないようにネットワークの設計を行うようお願いします。

ポートリセット機能によって一時的にダウンさせているポートは，マスタ，バックアップの選択ではアクティブポートとして扱います。マスタ状態として稼働している VLAN グループのマスタ，バックアップの選択には影響しません。

（4） GSRP 使用時の VLAN 構成について

GSRP 使用時は，すべての VLAN が GSRP によって制御されます。そのため，VLAN グループに属していない VLAN ポートは，ブロッキング状態になります。

（5） ダイレクトリンク障害検出機能について

ダイレクトリンクで本装置との間に伝送装置などを設置した構成で伝送装置の障害が発生した場合，マスタ状態で稼働中の本装置は正常に動作しているにもかかわらず，バックアップ状態で稼働中の別の本装置は対向の本装置で障害が発生したと認識し，自動でマスタ状態へ切り替わる可能性があります。この結果，2 台の本装置で同時にマスタ状態となります。また，ダイレクトリンクの回線の片線切れ障害が発生した場合でも同様の現象が発生する可能性があります。このため，コンフィグレーションコマンド gsrp の no-neighbor-to-master サブコマンドで direct-down を指定する場合は，ダイレクトリンクを冗長構成にし，複数経路で GSRP advertise フレームの送受信ができるようネットワークの設計を行うようお願いします。なお，ダイレクトリンクを冗長構成にするためには，リンクアグリゲーションを使用する方法，通常の回線を複数使用する方法などがありますが，どちらも効果は同じです。また，レイヤ 3 冗長切替機能でダイレクトリンク上の VLAN を通信に用いる場合，ダイレクトリンクを冗長構成にするときはリンクアグリゲーションを使用してください。

バックアップ（隣接不明）状態からマスタ状態に遷移する動作モードを direct-down に設定した場合，ダイレクトリンクに指定したすべてのポートが障害状態になると，マスタとして動作を開始します。ただし，次に示す動作後，ダイレクトリンクに指定したポートで GSRP Advertise フレームを 1 度も受信していない場合，バックアップ（隣接不明）状態のまま待機し続けます。マスタとして動作させたい場合，マスタ遷移コマンド（運用コマンド set gsrp master）を入力してください。

- 装置起動
- 系切替

- reload cp コマンド
- restart vlan コマンド
- restart gsrp コマンド
- no-neighbor-to-master サブコマンドで direct-down を指定
- direct-link サブコマンドによるダイレクトリンクポートの設定
- copy backup-config コマンドによるランニングコンフィグレーションへの反映

（6） GSRP 使用時のネットワークの構築について

GSRP を利用するネットワークは基本的にループ構成となります。フレームのループを防止するため，GSRP を使用するネットワークの構築時には，次に示すような対応をお願いします。

- GSRP のコンフィグレーションを設定する際，事前に本装置から回線を外すか，閉塞状態にしてください。または，周囲のスイッチにおいて回線を外しておいてください。コンフィグレーション設定後，GSRP の状態遷移が安定した後，回線を接続してください。
- GSRP グループを構成する 2 台の本装置のうち 1 台だけを起動させて，コンフィグレーションを設定し，バックアップ状態に切り替わったことを確認した後，もう一方の GSRP スイッチを起動してコンフィグレーションを設定してください。
- バックアップ固定機能を使って片方の GSRP スイッチを強制的にバックアップ状態にし，その状態でコンフィグレーションを設定してください。

（7） GSRP unaware での GSRP の制御フレームの中継について

GSRP スイッチの周囲のスイッチが GSRP unaware である場合，GSRP の制御フレームはフラッディングされます。この結果，トポロジー上，不必要なところまで制御フレームが中継されていく可能性があります。制御フレームの不必要な中継を防止するため，GSRP unaware でも GSRP 管理 VLAN を正しく設定してください。

（8） GSRP Flush request フレームの中継について

GSRP aware は GSRP Flush request フレームをフラッディングします。GSRP aware によって GSRP Flush request フレームを中継させるネットワーク構成では，GSRP aware のソフトウェアバージョンを Ver.10.5 以降にする必要があります。GSRP スイッチは GSRP Flush request フレームをフラッディングしないので，GSRP グループの多段構成などで GSRP スイッチによって GSRP Flush request フレームを中継させる構成はできません。

（9） GSRP 使用時の本装置のリモート管理について

GSRP を使用する場合，装置のリモート管理には以下のどれかを使用してください。

- RM イーサネット（SB-5400S ではリモートマネージメントポート）
- GSRP 制御対象外ポート（コンフィグレーションコマンド gsrp-exception-port で指定したポート）
- ルータポート

なお，リモート管理に用いる IP アドレスは装置ごとに異なる IP アドレスを設定してください。

（10） 相互運用

GSRP は，本装置独自仕様の機能です。Extreme Networks 社 LAN スイッチに搭載されている ESRP(Extreme Standby Router Protocol) および Foundry Networks 社 LAN スイッチに搭載されている VSRP(Virtual Switch Redundant Protocol) とは相互運用できません。

（11）BCU 過負荷時

BCU が過負荷状態となった場合，本装置が送受信する GSRP advertise フレームの廃棄または処理遅延が発生し，タイムアウトのメッセージ出力や，状態遷移が発生する場合があります。過負荷状態が頻発する場合には，GSRP advertise フレームの送信間隔，および保有時間を大きい値に設定して運用してください。

（12）BCU 二重化時

BCU 二重化構成の本装置で，GSRP の状態遷移を装置 MAC アドレスの値によってマスタ／バックアップを選択するように使用する場合，BCU 障害などで BCU の切り替えが発生すると，装置 MAC アドレスが旧運用系の BCU が保有する装置 MAC アドレスから新運用系の BCU の装置 MAC アドレスに変更されます。このため，BCU 切り替えによって GSRP の状態遷移が発生する可能性があります。BCU 二重化構成で GSRP を使用する場合は，装置管理情報 のコンフィグレーションコマンド local-mac-address によって装置 MAC アドレスを固定に設定して運用してください。

（13）BCU 二重化構成でポートリセット機能を使用する場合について

ある VLAN グループがマスタ状態からバックアップ状態に切り替わった際，ポートリセット機能によってポートをダウンさせているときに，BCU 障害などで BCU 切り替えが発生すると，新運用系で当該ポートがダウンのままになることがあります。その場合，free コマンドによって当該 Line を運用状態にしてください。

（14）VLAN グループ番号に関する注意

次に示すハードウェアが装置上に一つでも搭載されている場合，9 以上の VLAN グループ番号は使用できません。

SB-7800S の場合

NE1GSHP-4S，NE1GSHP-8S，NE10G-1ER，NE10G-1EW，または NE10G-LW の NIF のどれかを使用する場合。
上記を除く NIF を使用する場合は 9 以上の VLAN グループ番号を使用できます。

SB-5400S の場合

BSU-C1，または BSU-S1 のどちらかの BSU を使用する場合。
上記を除く BSU を使用する場合は 9 以上の VLAN グループ番号を使用できます。

また，レイヤ 3 冗長切替機能使用時に 9 以上の VLAN グループ番号を設定すると，GSRP の多段構成などで GSRP グループが異なる場合でも，同じ MAC アドレスが設定されます。

対向装置および GSRP aware のソフトウェアバージョンが Ver.10.1 以前の場合，9 以上の VLAN グループ番号は使用できません。

（15）仮想 MAC アドレスの学習について

レイヤ 3 冗長切替機能使用時，GSRP で冗長化するデフォルトゲートウェイの MAC アドレスは仮想 MAC アドレスを使用します。これに対し，IP 中継および本装置が自発的に送信するパケット / フレームの送信元 MAC アドレスは，仮想 MAC アドレスではありません。装置 MAC アドレス，または VLAN ごとの MAC アドレスになります。

GSRP では，GSRP スイッチをデフォルトゲートウェイとする装置に仮想 MAC アドレスを学習させるため，GSRP 制御フレームを定期的に送信しています。GSRP 制御フレームは，送信元 MAC アドレスを仮

想 MAC アドレスとした非 IP のユニキャストフレームです。

GSRP スイッチをデフォルトゲートウェイとするすべての装置に GSRP 制御フレームが転送されるネットワーク設計を行ってください。

6 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エンドホスト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 の機能について説明します。

6.1 VRRP 概説

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的なルータを定義できます。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。

(1) VRRP でサポートしている項目

VRRP でサポートしている項目を次の表に示します。

表 6-1 VRRP でサポートしている項目

項目		内容
対象インタフェース		イーサネット，VLAN
対象プロトコル		IPv4，IPv6
装置当たりの仮想ルータ最大数		255
インタフェース当たりの仮想ルータ最大数		255※1,※3
仮想ルータ当たりの IP アドレス数		1
パケット認証方式	なし	○
	テキストパスワード	○
	IP 認証ヘッダ	-
優先度制御		○
自動切り戻し (Preempt Mode)		○ (on/off で設定する)
アクセプトモード（Accept Mode）		○ (on/off で設定する)
制御パケット送信間隔		1 ～ 255 秒の範囲で指定できます。
装置切り替え時間		4 秒※2

(凡例) ○：サポートしている -：サポートしていない

注※ 1

仮想ルータが使用する MAC アドレスは仮想ルータごとに自動的に割り当てられます。

注※ 2

制御パケットの送信間隔が 1 秒 (デフォルト) の場合の装置切り替え時間。

IPv4 および virtual-router のパラメータで「ietf-ipv6-spec-01-mode」を指定したときの装置の切り替え時間は (パケット送信間隔× 3 ＋ 1) 秒になります。virtual-router のパラメータで「ietf-ipv6-spec-07-mode」を指定した場合，装置切り替え時間の計算方法は (パケット送信間隔× 3 + (((256 - 優先度) ×パケット送信間隔) ÷ 256)) に変更になります。エンド - エンド間の通信再開には，通信経路上のルータ装置で経路情報の再計算時間を含める必要があります。

注※ 3

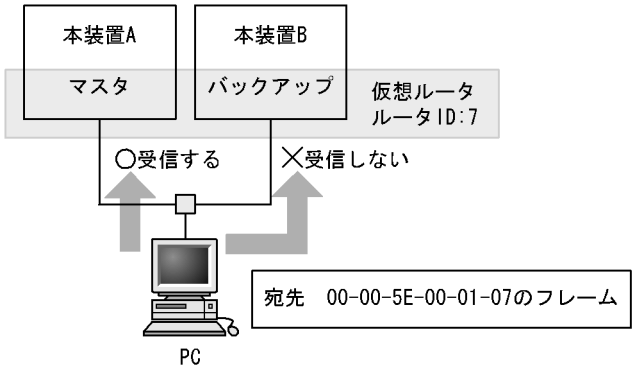
SB-7800S の場合，搭載されている NIF 種別については，最大数の 255 まで登録できません。定義不可能な NIF については，「6.12 VRRP 使用時の注意事項 (13) 仮想ルータ ID(VRID)」を参照してください。

SB-5400S の場合，搭載されている BSU 種別については，最大数の 255 まで登録できません。定義不可能な BSU については，「6.12 VRRP 使用時の注意事項 (13) 仮想ルータ ID(VRID)」を参照してください。

6.2 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 アドレスを持ちます。仮想ルータの MAC アドレスは，00-00-5E-00-01-{仮想ルータの ID} に決められており，仮想ルータの ID から自動的に生成されます。マスタ状態のルータは仮想 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，バックアップ状態のルータは仮想 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。マスタ状態のルータは仮想 MAC 宛てフレームを受信すると，自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。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。

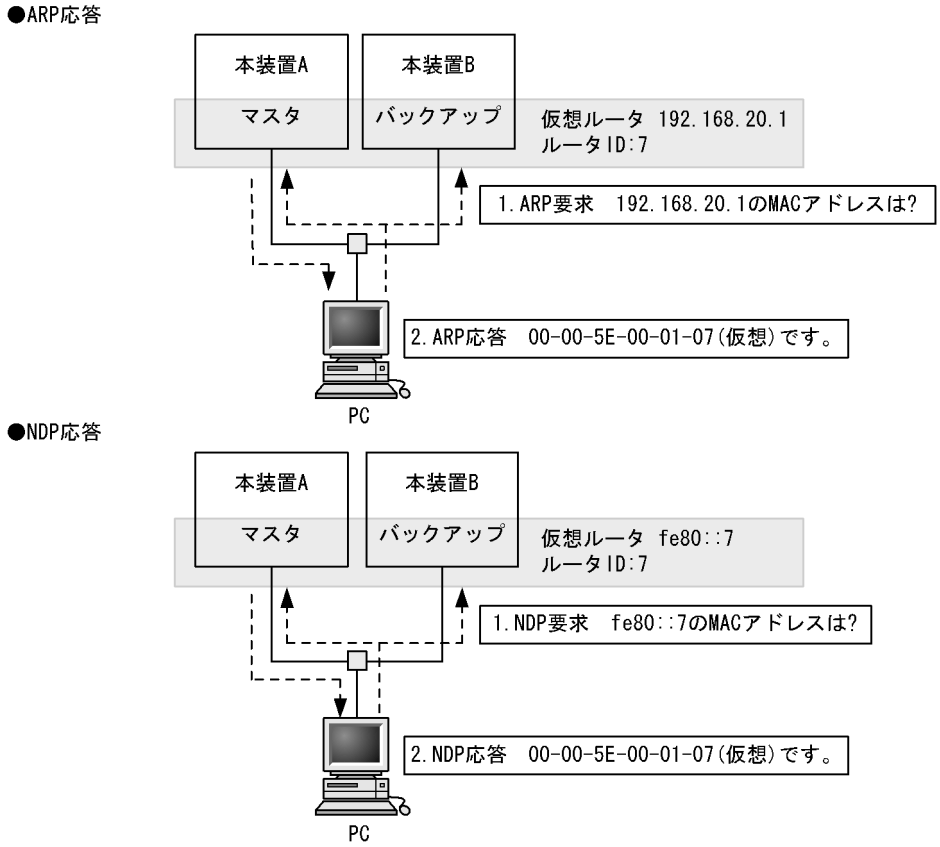
図 6-1 仮想 MAC アドレス宛てフレームの受信



VRRP では仮想 MAC アドレス宛てフレームが切り替えの対象になります。マスタとバックアップが切り替わった後で通信を継続できるのは仮想 MAC アドレス宛てフレームに限定されます。「図 6-1 仮想 MAC アドレス宛てフレームの受信」の場合，PC は仮想 MAC アドレスを宛先としてフレームの送信を行わなければなりません。

仮想ルータは仮想ルータの IP アドレスを持ちます。マスタ状態のルータは，仮想ルータの 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，常に仮想ルータの 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 6-2　仮想 MAC アドレスによる ARP 応答および NDP 応答



仮想ルータをデフォルトルータとして使用する PC などのホストは，自 ARP キャッシュテーブル内に仮想ルータの IP アドレス宛てのフレームは仮想 MAC アドレス宛てに送信するように学習します。このように学習されたホストは常に仮想ルータへ送信するときに仮想 MAC アドレスを宛先に指定してフレームの送信を行うようになるため，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。

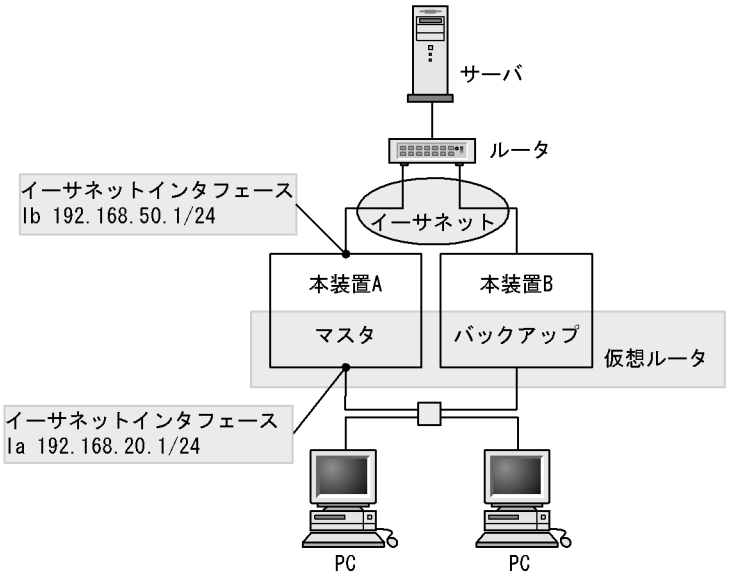
6.3 障害監視インタフェース

VRRP では仮想ルータを設定したインタフェースの障害時に，マスタルータを装置単位で切り替えます。しかし，仮想ルータが設定されていないそのほかのインタフェースに障害が発生した場合には切り替えません。本装置では独自の付加機能として他インタフェースを監視して，他インタ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。このインタフェースを障害監視インタフェースといいます。

障害監視インタフェースがダウンしたとき，仮想ルータの優先度の扱いは 2 通りあります。一つは , 障害監視インタフェースがダウンしたときに仮想ルータの優先度をあらかじめ設定しておいた優先度 (Critical Priority) に変更して運用します。もう一つは，障害監視インタフェースがダウンしたときにあらかじめ障害監視インタフェースに設定された，優先度減算値 (Down Priority) を仮想ルータの優先度から減算し運用します。前者の場合，障害監視インタフェースは一つしか設定できませんが，VRRP ポーリング機能を使用することができます。後者の場合，障害監視インタフェースを複数設定することができます。ただし，VRRP ポーリング機能は使用できません。

仮想ルータの優先度障害監視インタフェースを次の図に示します。

図 6-3 障害監視インタフェース



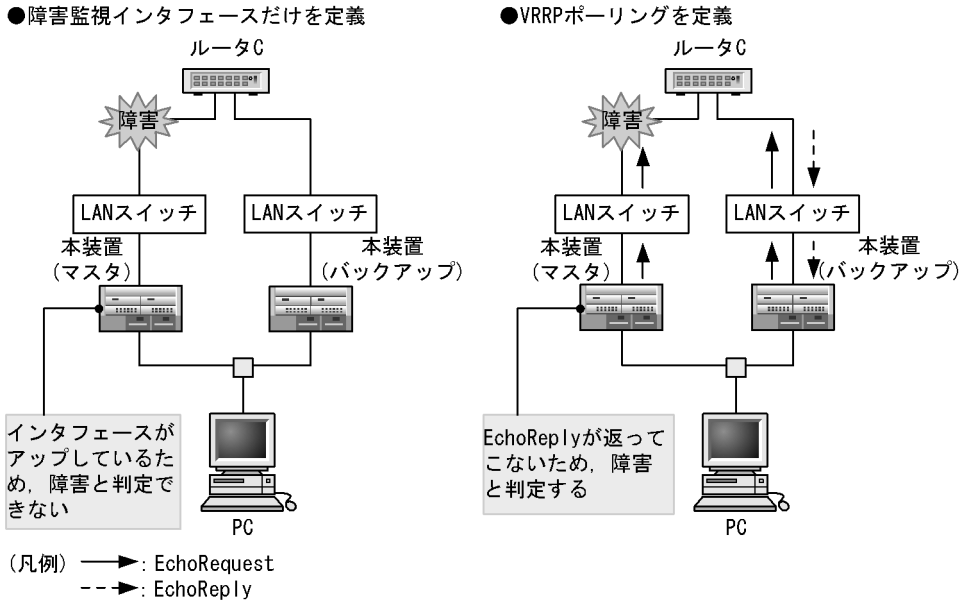
この図を例にして説明します。本装置 A には Ia というイーサネットインタフェースと Ib というイーサネットインタフェースの二つが定義されています。仮想ルータはインタフェース Ia に設定されています。通常の VRRP の動作ではイーサネット回線の障害によってインタフェース Ib がダウンしても，仮想ルータの動作には影響を与えません。しかし，本装置では障害監視インタフェース (Critical Interface) と障害監視インタフェースダウン時の優先度 (Critical Priority)，または優先度を下げる値 (Down Priority) を指定することによって，仮想ルータの動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フェースを Ib，そして障害監視インタフェースダウン時の優先度を 0 に設定した場合，インタフェース Ib のダウン時には自動的マスタが本装置 A から本装置 B へ切り替わります。

6.4 VRRP ポーリング

障害監視インタフェースでは，インタフェースのダウンで検出できるレベルの障害しか監視することができないため，ルータをまたいだ先の障害は検出できません。本装置では，障害監視インタフェースに対して VRRP ポーリングを使用することで，ルータをまたいだ先の障害でも検出できます。なお，VRRP ポーリングは障害監視インタフェースを複数設定した場合は，使用できません。VRRP ポーリングを定義した場合と定義していない場合の比較を次の図に示します。

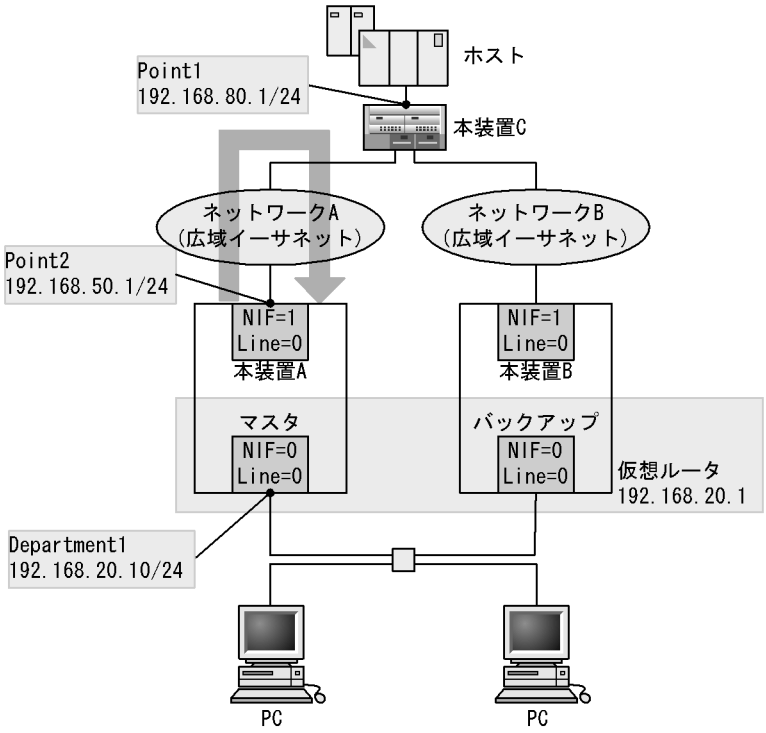
図 6-4 VRRP ポーリングを定義した場合と定義していない場合の比較



6.4.1 VRRP ポーリングの概要

VRRP ポーリングは，コンフィグレーションによって指定された IP アドレス宛てに ICMP Echo パケットによるポーリングを行い，疎通状態を監視します。ICMP Echo パケットは RFC 標準であるため，宛先 IP アドレスに指定する相手装置が本装置である必要はありません。ただし，ICMP Echo パケットに対して応答を返す必要があります。応答確認は ping コマンドを使用して行えます。応答がないため障害と判定した場合は，障害監視インタフェースと同様に仮想ルータの優先度を下げて運用します。VRRP ポーリングを次の図に示します。

図 6-5 VRRP ポーリング



「図 6-5 VRRP ポーリング」を例にして説明します。本装置 A には Department1 というイーサネットインタフェースと Point2 というイーサネットインタフェースの二つが定義されています。仮想ルータは Department1 に設定されています。通常の障害監視インタフェースでは，ネットワーク上で発生した障害は検出できません。しかし，本装置では宛先 IP アドレス (target address) を指定して VRRP ポーリングを有効にすることによって，ネットワーク上で発生した障害をすぐ検出できます。また，ホスト側の本装置 C は static ポーリングを使用し，経路切り替えを行います。static ポーリングについては，「解説書 Vol.1 12.3.1(3) スタティック経路の動的監視」を参照してください。

「図 6-5 VRRP ポーリング」の，本装置 A の仮想ルータの障害監視インタフェースを Point2，障害監視インタフェースダウン時の優先度を 0，ポーリングの宛先 IP アドレスをルータ 1 の Point1 の IP アドレス (192.168.80.1) に設定した場合，ネットワーク上で障害が発生し応答が返らなくなると，自動的にマスタが本装置 A から本装置 B へ切り替わります。なお，障害検出時間または障害回復検出時間はコンフィグレーションによって変更できます。

障害監視インタフェースがダウンした場合，VRRP ポーリングは疎通不可能状態と判断し，インタフェースがアップするまで待機します。障害監視インタフェースがアップした時，再度ポーリングを始め，障害復旧検証によって疎通可能状態と判定した場合，切り戻しを行います。

6.4.2 VRRP ポーリング使用時の注意事項

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 6-6 送受信インタ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フェースが VRRP ポーリングを送信したインタフェースと一致しない場合があります。この場合，受信インタフェースチェックオプション (コンフィグレーションコマンド virtual-router の check-reply-interface サブコマンド) を指定することで，送信インタフェースと受信インタフェースをチェックできます。送信インタフェースと受信インタフェースが不一致

の場合に該当するパケットを廃棄します。なお，「図 6-7　自装置配下ではないネットワーク上のインタフェース不一致」のような自装置配下でないネットワーク上のインタフェースが不一致の場合は，保証しません。

図 6-6　送受信インタフェースが一致しない場合

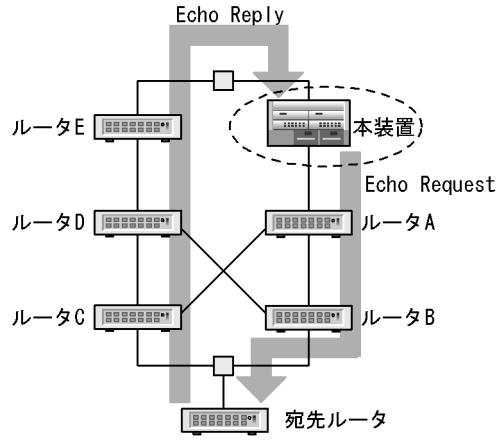
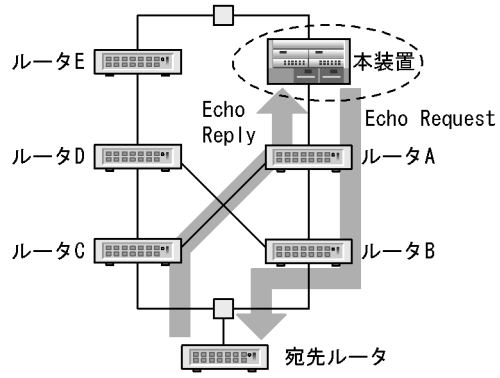


図 6-7　自装置配下ではないネットワーク上のインタフェース不一致

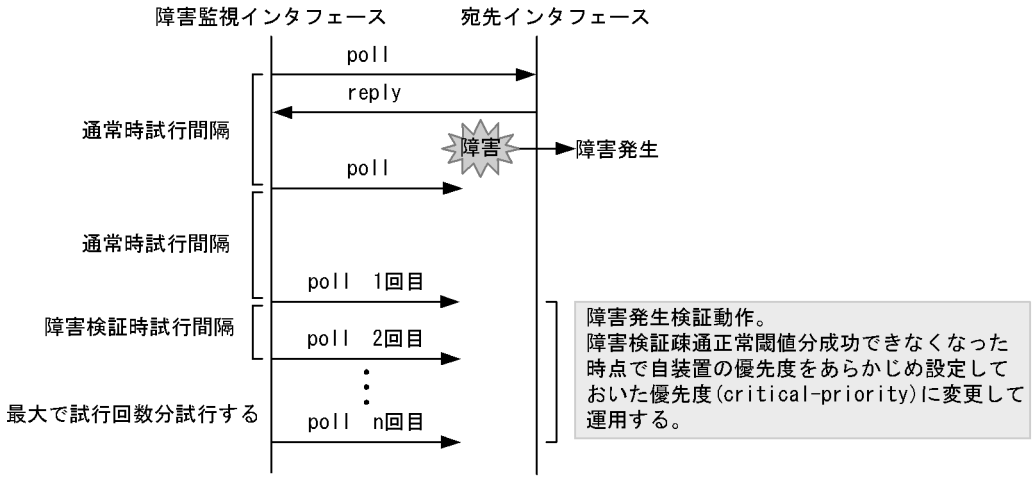


6.5 VRRP ポーリングの障害検出の仕組み

VRRP ポーリングの障害検出の仕組みについて説明します。VRRP ポーリングは通常時，通常時試行間隔 (コンフィグレーションコマンド virtual-router の check-status-interval サブコマンド) の指定値 (秒) でポーリングを行います。疎通可能状態である場合，応答が返らないままタイムアウトすると，障害発生検証を行います。

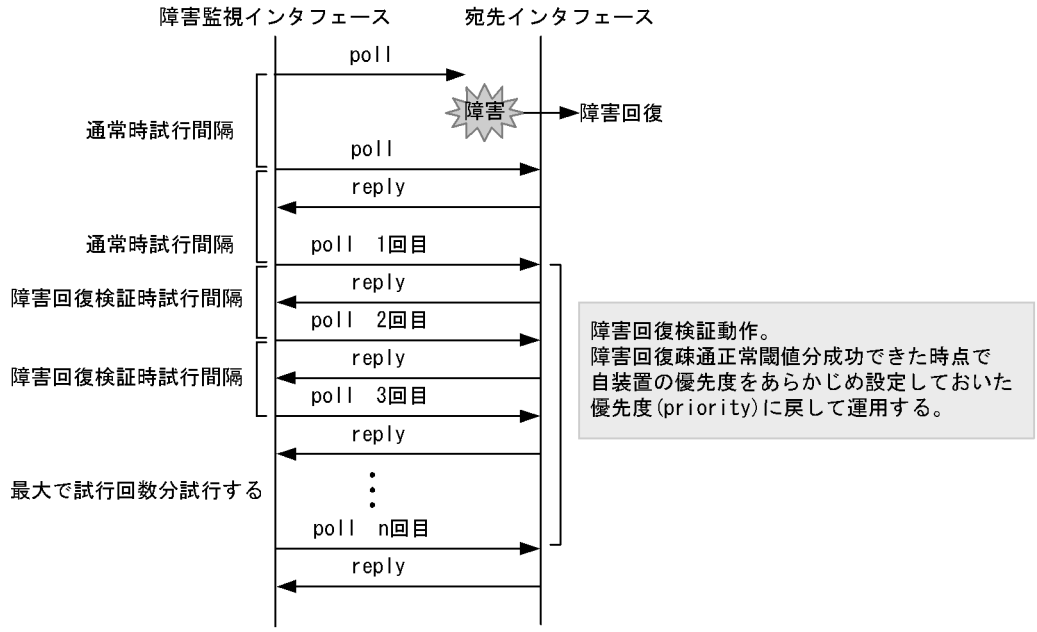
障害発生検証では，障害検証時試行間隔 (コンフィグレーションコマンド virtual-router の failure-detection-interval サブコマンド) の指定値 (単位：秒) で，試行回数 (コンフィグレーションコマンド virtual-router の check-trial-times サブコマンド) のポーリングを行います。このときに，障害検出疎通正常判定閾値 (コンフィグレーションコマンド virtual-router の failure-detection-times サブコマンド) で指定した回数分応答が返ってくるか判定し，この回数を満たせなくなった時点で障害と判定します。障害検出動作シーケンスを次の図に示します。

図 6-8　障害検出動作シーケンス



VRRP ポーリングの障害回復検出の仕組みについて説明します。VRRP ポーリングは通常時，通常時試行間隔で指定した間隔でポーリングを行います。疎通不可能状態である場合，応答が返ってくると障害回復検証を行います。障害回復検証では，障害回復検証時試行間隔 (コンフィグレーションコマンド virtual-router の recovery-detection-interval サブコマンド) の指定値 (単位：秒) で，試行回数分ポーリングを行います。このとき，障害回復疎通正常判定閾値 (コンフィグレーションコマンド virtual-router の recovery-detection-times サブコマンド) で指定した回数分応答が返ってくるか判定し，この回数を満たした時点で障害回復と判定します。障害回復動作のシーケンスを次の図に示します。

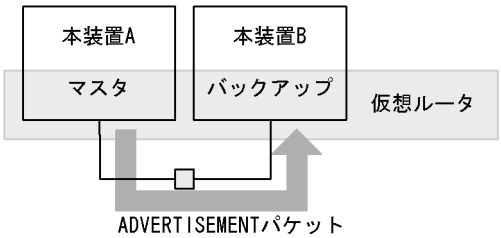
図 6-9　障害回復動作シーケンス



6.6 障害検出の仕組み

マスタ状態の本装置は定期的な周期（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イーサネットインタフェースから送信します。バックアップ状態のルータはマスタ状態のルータが送信する ADVERTISEMENT パケットを受信することによって，マスタ状態のルータに障害がないことを確認します。ADVERTISEMENT パケットの送信を次の図に示します。

図 6-10 ADVERTISEMENT パケットの送信



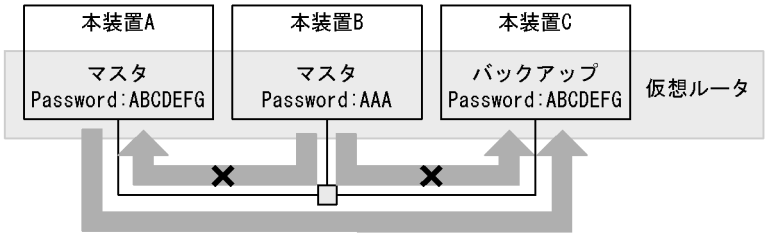
マスタ状態となっている本装置に障害が発生した場合，ADVERTISEMENT パケットを送信できません。例えば，本装置全体がダウンしてしまった場合や，仮想ルータが設定されているイーサネットインタフェースからパケットを送信できなくなるような障害が発生した場合，ケーブルの抜けなどの場合です。

バックアップ状態の本装置は一定の間 ADVERTISEMENT パケットをマスタ状態のルータから受信しなかった場合に，マスタルータに障害が発生したと判断し，バックアップからマスタへと状態を変化させます。

6.7 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，VRRP 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，(ルータ超えを伴う) 遠隔からの攻撃を防ぐことができます。また，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 6-11 パスワードの不一致



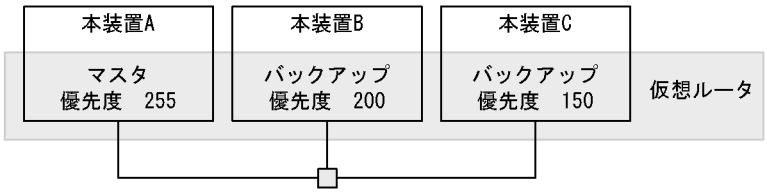
この図の例では本装置 B のパスワードが本装置 A および本装置 C と異なっているため，本装置 B から送信された ADVERTISEMENT パケットを本装置 A や本装置 C が受け取っても廃棄します。この場合，本装置 C は本装置 A からの ADVERTISEMENT パケットだけを受信して処理します。

6.8 マスタルータの選出方法

6.8.1 優先度

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

図 6-12 マスタ状態のルータの選出



この図の場合，優先度が最も高い本装置 A がマスタ状態になります。本装置 A がダウンした場合は，次に優先度の高い本装置 B がマスタ状態へと変化します。本装置 A と本装置 B の両方がダウンした場合にだけ本装置 C がマスタ状態になります。

優先度の同じ仮想ルータが存在する場合はどちらかがマスタ状態になります。どちらがマスタ状態になるかは不定であるため，マスタ状態になる装置を明確に制御したい場合は，異なる優先度を指定してください。

6.8.2 自動切り戻し

VRRP では自ルータよりも優先度の低い VRRP ルータがマスタ状態になっていることを検出すると，優先度の高いバックアップルータが自動的にマスタへ状態を変化させます。逆に，マスタ状態のルータが自分より優先度の高い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 6-12 マスタ状態のルータの選出」の構成を例にしてみると，本装置 A と本装置 B がダウンした状態で本装置 C がマスタ状態になっている状態から，本装置 B が復旧すると，本装置 C よりも優先度の高い本装置 B がマスタ状態に変化し，本装置 C がマスタ状態からバックアップ状態を変化させることになります。

この自動切り戻しの機能を抑止する設定もできます。自動的に切り戻しさせたくない場合には 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，バックアップ状態のルータが自ルータよりも優先度の低いルータがマスタ状態になっていることを検出しても，マスタ状態へと変化させることはありません。ただ，自装置が IP アドレスの所有者 (優先度が 255 のとき) は切り戻しの抑止は有効になりません。

6.8.3 自動切り戻し抑止

本装置では，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 通りの方法があります。

(1) 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，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，バックアップ状態のルータが自ルータよりも優先度の低いルータがマスタ状態になっていることを検出しても，マスタ状態へ変化させることはありません。

ただし，マスタ状態のルータの障害などによって，一定時間（ADVERTISEMENT 送信間隔× 3 ＋ 1 秒）ADVERTISEMENT パケットを受信しなかった場合は，バックアップ状態からマスタ状態に遷移します。

（2） PREEMPT モード OFF によるマスタ状態遷移の時間監視 (preempt-mode-off-timer)

自動切り戻し抑止中状態（PREEMPT モード OFF）のバックアップ中にマスタ状態のルータから ADVERTISEMENT パケットを受信しなかった場合に，切り戻しを遅延させたいときに使用してください。マスタ装置のダウンを検出し，本タイマ値の経過後，マスタ状態に遷移します。

切り戻し時間は次のようになります。

（ADVERTISEMENT 送信間隔× 3 ＋ 1）（秒）＋本タイマ値（秒）

コンフィグレーションの設定によって，1 ～ 65535 秒の範囲で設定できます。

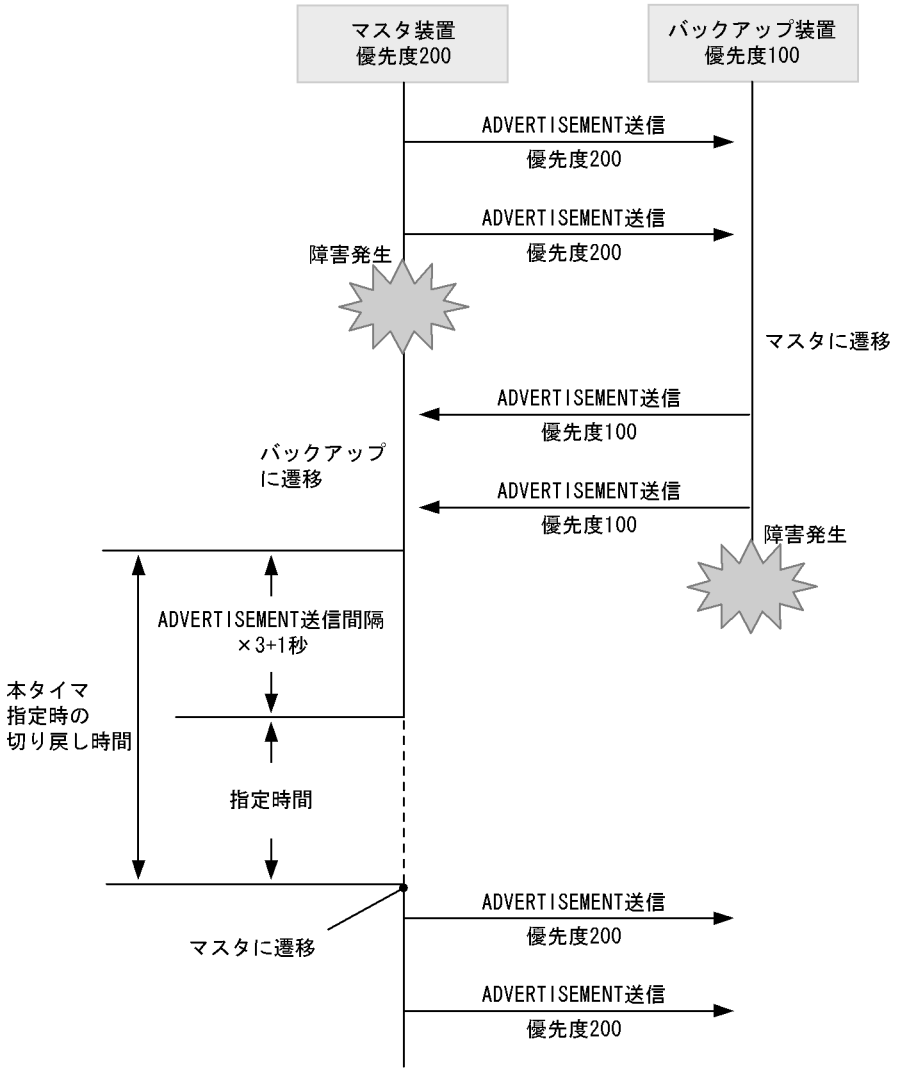
本タイマ監視中に再度，自ルータより優先度の低い ADVERTISEMENT パケットを受信した場合は，タイマ監視を中断し，バックアップ状態を維持します。また，自ルータより優先度の高い ADVERTISEMENT パケットを受信した場合も，タイマ監視を中断し，バックアップ状態を維持します。

また，二重化構成で，運用系と待機系でタイマ時間の同期は行いません。このため，本体タイマ監視中に系切替が発生した場合，新運用系で最初からタイマ監視を行います。

自動切り戻し抑止中状態に本タイマを設定した場合，システム立ち上げ時に対向装置が存在しないと，タイマ監視によるバックアップ状態を維持します。また，本来マスタとなるべき装置とバックアップになるべき装置に，自動切り戻し抑止中状態で本タイマを設定し，同時にシステムを立ち上げるとダブルバックアップになります。この場合，swap vrrp コマンドでマスタ状態に遷移させてください。

本タイマを指定したときの切り戻し時間を次に示します。

図 6-13　本タイマを指定したときの切り戻し時間



「表 6-2　自動切り戻し抑止状態で本タイマを使用した場合と，使用しない場合の状態遷移」に自動切り戻し抑止状態で本タイマを使用した場合と，使用しない場合の状態遷移を示します。

表 6-2　自動切り戻し抑止状態で本タイマを使用した場合と，使用しない場合の状態遷移

イベント	自装置 Backup 状態 preempt-mode-off	
	preempt-mode-off-timer あり	preempt-mode-off-timer なし
自優先度より高い ADVERTISEMENT 受信	Backup 状態のまま	Backup 状態のまま
自優先度より低い ADVERTISEMENT 受信	Backup 状態のまま	Backup 状態のまま
ADVERTISEMENT 未受信	Backup 状態のまま	Master 状態に遷移
preempt-mode-off-timer タイムアウト	Master 状態に遷移	-

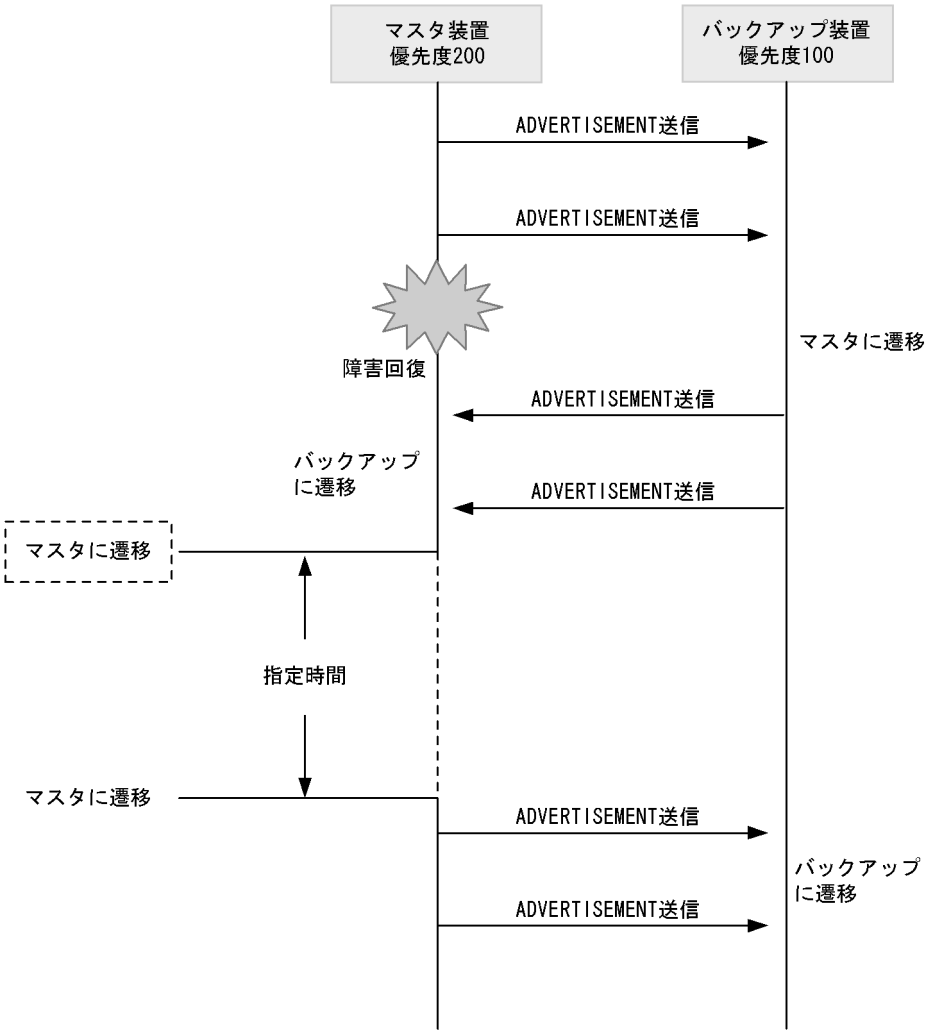
（凡例）-：該当なし

なお，本タイマは，自動切り戻し抑止中のマスタ装置に障害が発生し，回復した場合に，本装置間にあるスイッチなどの状態によって，対向装置から ADVERTISEMENT パケットを一時的に受信できないとき，マスタ - バックアップの切り替えが発生しないようにするためのタイマです。

（3） 抑止タイマ (Master Transition Delay) による抑止

本機能は，マスタ装置が故障などによってバックアップ状態になった場合に，自動切り戻し（preempt mode on）でマスタ状態に遷移する時間を，任意の時間遅延させる機能です。この機能によって，自動切り戻し（preempt-mode-on）でマスタ - バックアップの切り替えが頻繁に発生することを防ぐことができます。

図 6-14　抑止タイマによるマスタ状態遷移



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，抑止タイマを設定してください。コンフィグレーションの設定によって 1 ～ 65535 秒の範囲で設定可能です。

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。

どちらの方法についても，自装置が 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。また，マスタ装置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，かつ残った装置の中で自装置の優先度が最も高いことを検出した場合には，マスタ状態に遷移します。

6.8.4 コマンドによる切り戻し

自動切り戻し抑止中状態で，swap コマンドによって本装置の切り戻し処理を起動することができます。

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，本コマンドを指定することで，コマンド指定時にマスタとして稼働していた装置よりもコマンドを指定した装置の優先度が高い場合には，コマンドを指定した装置がマスタ状態に遷移します。

また，自動切り戻し抑止中状態で，preempt-mode-off-timer によるバックアップ監視中（対向装置から ADVERTISEMENT パケットを受信していない状態）に本コマンドを指定することでマスタに遷移します。

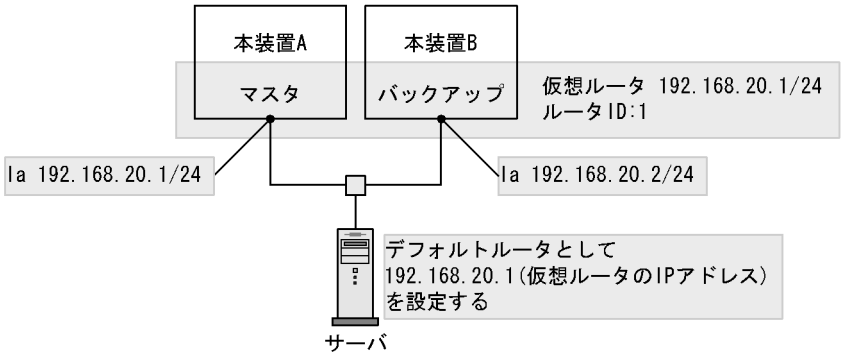
（注意：強制的にマスタ状態に遷移するコマンドではありません。）

6.9 ネットワーク構成例

6.9.1 VRRP による構成例

VRRP によるネットワーク構成例を次の図に示します。

図 6-15 VRRP によるネットワーク構成例



この図の構成では同一のイーサネットセグメント内に設置された本装置 2 台を使用して，仮想的なルータを設定しています。実際には 2 台のルータのどちらかがマスタ状態となり，マスタ状態のルータが仮想ルータをシミュレートします。

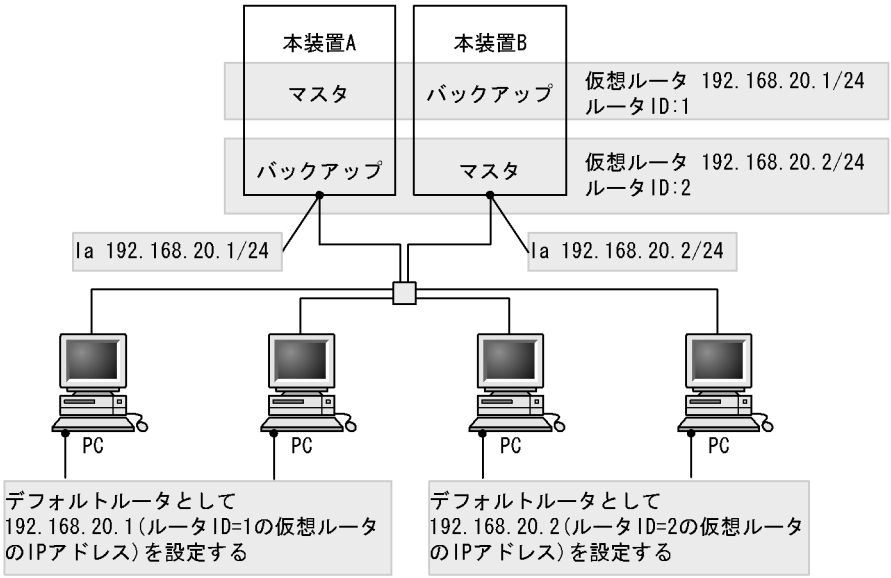
一方，バックアップ状態となったルータはマスタ状態のルータを監視します。マスタ状態のルータに障害が発生して通信を継続させることができなくなった場合，バックアップ状態で待機しているルータがマスタ状態のルータの障害を検出して，自身がマスタに状態を変化させて仮想ルータをシミュレートします。

仮想ルータには IP アドレスが設定されます。仮想ルータの IP アドレスをデフォルトルータとして指定しているサーバはマスタ状態のルータの切り替えを意識しないで通信を継続できます。

6.9.2 負荷分散の例

負荷分散の例を次の図に示します。

図 6-16　負荷分散の例



この図の例では同一のイーサネットセグメントに対して 2 個の仮想ルータを設定しています。配下の 4 台の PC のうち，2 台は仮想ルータ 1(ルータ ID:1 の仮想ルータ) をデフォルトルータに設定し，残りの 2 台は仮想ルータ 2(ルータ ID:2 の仮想ルータ) をデフォルトルータに設定しています。仮想ルータ 1 のマスタルータは本装置 A，仮想ルータ 2 のマスタルータは本装置 B になっているため，通常の運用時 (どちらのルータにも障害がない場合) には 2 台の本装置を使用して負荷分散を行えます。

本構成では，どちらかの装置に障害が発生しても，配下の 4 台の PC にすべて通信経路を確保できます。例えば，本装置 A に障害が発生した場合には仮想ルータ 1 のマスタが本装置 A から本装置 B へ移り，逆に本装置 B に障害が発生した場合には仮想ルータ 2 のマスタが本装置 B から本装置 A へ移ります。デフォルトルータをどちらかの仮想ルータに設定している PC はマスタ状態のルータが存在する間，通信を継続できます。

6.10 アクセプトモード（Accept mode）

アクセプトモードを設定することで，マスタ状態の仮想ルータが，アドレス所有者でなくても，IP パケットを受信できます。

6.11 IPv6 VRRP ドラフト対応

(1) テキストパスワード領域の有無

本装置は IPv6 VRRP ドラフトに対応していて，ADVERTISEMENT パケットにテキストパスワード領域を付けて送信するかどうかを選択できます。

送信時にテキストパスワード領域を付けるかどうかで ADVERTISEMENT パケットのフォーマットが異なるため，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てしまいます。これによって，お互いがマスタ状態になり，その状態が解消されません。そのため，VRRP を組む装置間では，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。

IPv6 VRRP ドラフト非対応 (ietf-ipv6-spec-07-mode パラメータ未サポート) のソフトウェアバージョンの場合は，テキストパスワード領域を付けて送信します。

(2) 装置切り替え時間計算方法変更

マスタからの ADVERTISEMENT パケットを一定時間受信しなかった場合，バックアップからマスタへと状態を変化させますが，より優先度の高い VRRP からマスタに遷移するように，装置切り替え時間の計算に各 VRRP の優先度を含めて計算をしています。

IPv6 の装置切り替え時間の計算には，各 VRRP の優先度のほかに，パケット送信間隔も含まれます。

新しい計算式は，「表 6-1　VRRP でサポートしている項目」の注※ 2 を参照してください。

6.12 VRRP 使用時の注意事項

（1） サポートプロトコル

VRRP 機能を使用できるプロトコルは IPv4 および IPv6 だけです。また，仮想ルータを構成する複数のルータ間は VRRP を使用するプロトコルによって相互に通信できる必要があります。

なお，規格上 IPv6 の場合，仮想ルータへはリンクローカルアドレスだけ設定可能ですが，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を含む）も設定可能です。

（2） VRRP ルータに対する通信

VRRP ルータに対する通信 (ping，ping ipv6，telnet，ftp など) はルータのインタフェースに割り当てられている実 IP アドレス宛てで行う必要があります。仮想ルータの IP アドレスの場合，実 IP アドレスと仮想ルータの IP アドレスが同一であるアドレス所有者のルータがマスタ状態のときには通信できますが，それ以外の場合には通信できません。

ただし，アクセプトモードを設定した場合は，IPv4 の ping 通信が可能です。

（3） traceroute，traceroute ipv6 コマンド

VRRP ルータから送信される IP パケットの送信元アドレスは仮想ルータの IP アドレスではなく，ルータの実 IP アドレスです。そのため，配下のホストから仮想ルータを通過する宛先アドレスに対して traceroute または traceroute ipv6 コマンドを実行した場合，マスタ状態となっている VRRP ルータの実 IP アドレスが経路中のルータの IP アドレスとして表示されます。

（4） proxy ARP

VRRP を設定しているイーサネットインタフェースから proxy ARP による応答を行う場合，仮想ルータの MAC アドレスを使用して応答します。物理的に割り当てられる MAC アドレスでは応答しません。

（5） proxy NDP

VRRP を設定しているイーサネットインタフェースから proxy NDP による応答を行う場合，物理的に割り当てられる MAC アドレスを使用して応答します。

（6） ICMP Redirect，ICMPv6 Redirect

VRRP を設定しているインタフェース上では ICMP Redirect および ICMPv6 Redirect メッセージの送信は抑止されます。

（7） 障害監視インタフェース

障害監視インタフェースには IP の定義を行ってください。障害監視インタフェースダウン時の優先度を 0(デフォルト) に設定した場合に障害監視インタフェースがダウンすると，VRRP を設定しているインタフェースもダウン状態になります。また，障害監視インタフェースを複数設定している場合，仮想ルータの優先度からダウンした障害監視インタフェースの優先度を下げる値の合計を減算した結果，優先度が 0 となった場合も同様に，VRRP を設定しているインタフェースもダウン状態になります。同一回線内に複数の VLAN インタフェースを収容している場合，VRRP を設定している VLAN インタフェースだけがダウン状態になります。同一回線内のほかの VLAN インタフェースは影響を受けません。

一つのインタフェースに複数の VRRP 定義を行う場合で，各 VRRP 定義に対してそれぞれ個別の障害監

視インタフェースを定義し，その障害監視インタフェースダウン時の優先度を 0 とした場合，該当するインタフェースに定義されている VRRP の障害インタフェースのうち一つでもダウン状態になると，そのインタフェースはそのほかの障害監視インタフェースの状態に関係なくダウン状態になります。その場合，同一インタフェースに定義されているそのほかの VRRP の動作にも影響が発生するため，障害監視インタフェースダウン時の優先度を 0 とする障害監視インタフェースの指定を行う場合，一つのインタフェースには一つの VRRP を定義することをお勧めします。

一つのインタフェースに複数の VRRP を定義し，障害監視インタフェースダウン時の優先度を 0 とする障害監視インタフェースを指定する場合，各 VRRP の障害監視インタフェース定義にはすべて同一のインタフェースを指定してください。

（8）VRRP ポーリング

VRRP ポーリングは，障害監視インタフェースを送信インタフェースとします。障害監視インタフェースの IP アドレスと宛先 IP アドレスは，相互に通信できる IP アドレスを設定してください。相互に通信できない IP アドレスを設定した場合は，VRRP ポーリングは障害と判定します。

コンフィグレーションで指定する障害監視インタフェースと，宛先 IP アドレスまでの経路は，ルーティングテーブルに依存します。ルーティングプロトコルによって正しい経路を設定してください。

受信インタフェースチェックオプション (コンフィグレーションコマンド virtual-router の check-reply-interface サブコマンド) を指定している場合，送信インタフェースと受信インタフェースが不一致の場合はパケットを破棄します。このため，通信可能状態でも障害と判定する場合があります。受信インタフェースチェックオプションはデフォルトでは無効です。

VRRP ポーリングが送信する ICMP パケットは自装置内では優先されますが，他ルータでは優先されません。このため，ネットワーク過負荷時に障害と判定する場合があります。これを回避するには，VRRP ポーリングのパケットを QoS などで優先するように設定してください。

（9）DHCP/BOOTP リレーエージェント機能との共存

DHCP/BOOTP リレーエージェント機能と VRRP 機能を同一インタフェースで同時に運用する場合は，DHCP/BOOTP サーバで，DHCP/BOOTP クライアントゲートウェイアドレス (ルータオプション) を本装置に設定した仮想ルータアドレスに設定する必要があります。設定方法の詳細については，「コンフィグレーションガイド　8.4.6 DHCP/BOOTP リレーと VRRP 連携」を参照してください。

（10）IP フィルタリング

VRRP を設定したインタフェースで，VRRP の ADVERTISEMENT パケットを廃棄するフィルタリングを設定しないでください。VRRP の ADVERTISEMENT パケットは，IPv4 の場合は宛先アドレスが 224.0.0.18，送信元アドレスがマスタルータの実 IPv4 アドレスに，IPv6 の場合は宛先アドレスが ff02::12，送信元アドレスがマスタルータのリンクローカルアドレスに，プロトコル番号は IPv4 および IPv6 ともに 112 になります。

（11）高負荷時

仮想ルータを多数設定したとき，VRRP の ADVERTISEMENT パケットの送信間隔がデフォルト値（1 秒）の場合は，マスタ／バックアップの関係が切り替わることがあります。その場合は，ADVERTISEMENT パケットの送信間隔を調整してください。

ADVERTISEMENT パケットの送信間隔の目安値は次のように計算してください。

VRRP 数×物理インタフェース数÷ 200 ＜＝ ADVERTISEMENT パケットの送信間隔（端数切り上げ）

- VRRP 数
  コンフィグレーションに定義してある VRRP の数
- 物理インタフェース数
  VRRP を定義してあるインタフェースに複数の物理インタフェースを定義している場合，その中の最も多い物理インタフェースの数

表 6-3　ADVERTISEMENT パケットの送信間隔（参考値）

物理インタフェース数	VRRP 数							
	1	5	10	50	100	150	200	255
1	1	1	1	1	1	1	1	2
5	1	1	1	2	3	4	5	7
10	1	1	1	3	5	8	10	13

注　単位は秒です。

なお，この値はあくまでも目安であり，ネットワークの運用方法によっては目安値以上で ADVERTISEMENT パケットの送信が必要な場合もあります。また，環境によっては目安値よりも小さい間隔で利用できる場合もありますので，事前に評価した上でご使用ください。

また，copy mc コマンドや ppupdate コマンド実行時には，RM の CPU 使用率が上昇しマスタ／バックアップの関係が切り替わる場合があります。CPU 高負荷時の切り替えを抑止したい場合は，ADVERTISEMENT パケットの送信間隔を調整してください。

（12）相互運用

Cisco 社ルータに搭載されている HSRP(Hot Standby Router Protocol) とは相互運用できません。

（13）仮想ルータ ID(VRID)

SB-7800S の場合

NE1GSHP-4S，NE10G-1ER，NE10G-1EW，NE10G-LW のどれかの NIF を使用し，同一物理ポート内に複数の仮想ルータを定義する場合，VRID の指定に下記制限事項がありますので注意願います。
VRID は (1 ～ 7)(8 ～ 15)(16 ～ 23)...(248 ～ 255) の 8 個幅の 32 グループに分けられ，同一物理ポート内には既に定義済みの VRID と同じグループに属する VRID は設定できません。例えば，VRID1 の仮想ルータを定義したポートでは 2 個目の仮想ルータに VRID2 ～ 7 を指定することはできません。VRID8 ～ 255 の中から選択してください。なお，異なる物理ポートであれば，VRID1 ～ 7 は使用可能です。
上記 NIF 以外を使用した場合は上記制限事項が解除されます。
8 個幅の同じグループに複数の仮想ルータが設定されているコンフィグレーションで上記未対応 NIF を使用し起動した場合，仮想ルータをすべて削除し再設定するか，対応 NIF に交換してください。

SB-5400S の場合

BSU-C1，BSU-S1 のどれかの BSU を使用し，同一物理ポート内に複数の仮想ルータを定義する場合，VRID の指定に下記制限事項がありますので注意願います。
VRID は (1 ～ 7)(8 ～ 15)(16 ～ 23)...(248 ～ 255) の 8 個幅の 32 グループに分けられ，同一物理ポート内には既に定義済みの VRID と同じグループに属する VRID は設定できません。例えば，VRID1 の仮想ルータを定義したポートでは 2 個目の仮想ルータに VRID2 ～ 7 を指定することはできません。

VRID8 ～ 255 の中から選択してください。なお，異なる物理ポートであれば，VRID1 ～ 7 は使用可能です。
上記 BSU 以外を使用した場合は上記制限事項が解除されます。
8 個幅の同じグループに複数の仮想ルータが設定されているコンフィグレーションで上記未対応 BSU を使用し起動した場合，仮想ルータをすべて削除し再設定するか，対応 BSU に交換してください。

（14）コンフィグレーションを削除する場合

VRRP のコンフィグレーションを削除した場合，本装置に接続されていたホストが一時的に通信不可となる場合があります。ホストの ARP/NDP エントリに本装置の IP に対して仮想 MAC を学習していた場合，通信不可となります。復旧するにはホストの ARP/NDP エントリをクリアしてください。

（15）アクセプトモードを使用するときの注意事項

アクセプトモードは IPv4 および IPv6 の Ping 応答に使用することを前提としています。そのほかのアプリケーション（telnet，ftp，SNMP など）は，サポートしていません。

（16）IPv6 送信タイプ指定時の注意事項

IPv6 の送信タイプで ietf-ipv6-spec-07-mode の設定を行うためには，VRID の設定に制限のない NIF を使用してください。VRID の設定に制限のある NIF については，「（13）仮想ルータ ID(VRID)」を参照してください。

7 CP 輻輳制御

この章では，本装置の CP 輻輳制御について説明します。

7.1 機能概要

レイヤ 2 スイッチにおいて，特定の VLAN がネットワークの設定誤りなどでループ構成になっている場合，ARP 要求フレームやルーティング制御プロトコルフレームなどが VLAN 内を周回し，いわゆるブロードキャストストームが発生します。これによって自宛のフレーム受信処理が多発すると装置輻輳が発生し，本来正常に動作していた通信にも影響を及ぼすことがあります。本装置では，このような場合でも正常に動作している VLAN への影響を抑えるための輻輳制御機能を実装しています。この輻輳制御は BCU 内の CP で行うため CP 輻輳制御と呼びます。

CP 輻輳制御は，ブロードキャストを含む自装置宛のフレームの輻輳を検知すると，該当するポートの通信を一時的に停止し，輻輳の要因となるフレームを受信しないようにします。一定時間のあとに通信を再開させ，以降このような制御を輻輳が発生している間繰り返します。この制御によって，ブロードキャストストームが発生しても，正常に動作している VLAN を収容しているポートの自宛通信への影響を抑えることができます。また，抑止制御の対象にしたポートは，一時的に通信を停止した場合も外部的には閉塞していない状態として見せます。そのため，レイヤ 2 のプロトコル制御フレーム（BPDU，LACP など）は通信を停止せず，スパニングツリーやリンクアグリゲーションの構成に影響を与えません。

7.2 動作概要

(1) 制御手順

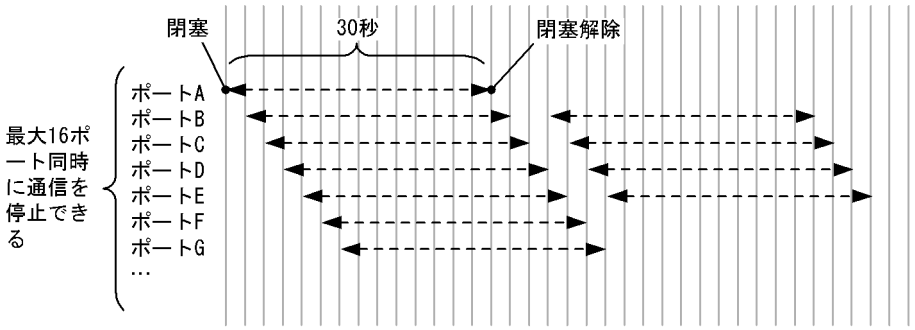
CP 輻輳制御の動作概要手順を次に示します。

1. コンフィグレーションで CP 輻輳制御の動作可否と制御時間を設定できます。動作可能に設定すると，CP 輻輳制御を開始します。
2. CP 部のフレーム受信キューのあふれを 1 秒周期で監視します。あふれを検出すると，たまっているキューがどこのポートから受信したものが多いかをチェックし，最大 16 ポート※1 を制御対象に選びます。
3. 制御対象となったポートは制御時間の間，通信を停止します。制御時間経過後に通信を再開※2 し，次の 1 秒後に該当するポートからの受信で輻輳が発生していなければそのポートを制御対象から外します。輻輳が続いていれば，該当するポートを引き続き制御対象として再度制御時間の間，通信を停止します。
4. 輻輳が継続する間，上記を繰り返し，断続的に輻輳しているポートの通信停止，通信停止解除を繰り返します※3。

注※ 1

閉塞中も CP 部のフレーム受信キューあふれを監視して，最大 16 ポートまで通信を停止します。同時に通信を停止する処理の流れを次の図に示します。

図 7-1 同時に通信を停止する処理の流れの例（CP 輻輳制御時間が 30 秒の場合）



注※ 2

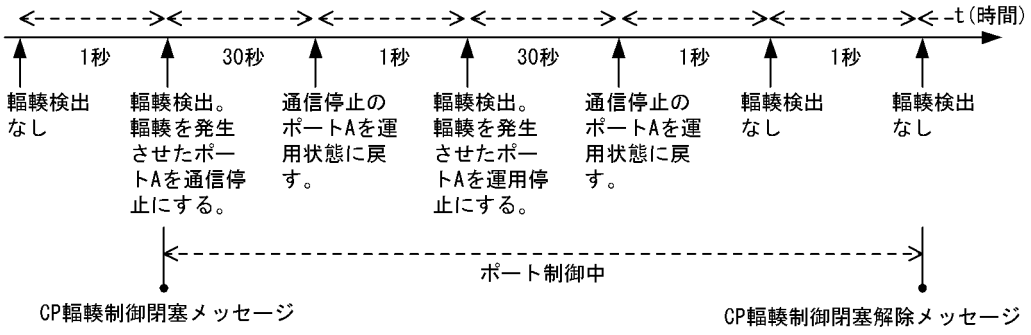
制御時間が経過しなくても，次のイベントが発生した契機で通信を再開します。

- 運用コマンド no cp congestion-control で，輻輳による閉塞状態を解除したとき
- 回線状態が運用中（正常動作中）から，ほかの状態に変化したとき
- コンフィグレーションコマンド congestion-control のパラメータについて設定，変更，または削除をしたとき
- 系切替したとき

注※ 3

断続的に輻輳しているポートの通信停止，通信停止解除を繰り返す場合，CP 輻輳制御閉塞メッセージおよび CP 輻輳制御閉塞解除メッセージは次の図に示すタイミングで出力します。

図 7-2 CP 輻輳制御メッセージ出力タイミングの例（CP 輻輳制御時間が 30 秒の場合）



（2） サポート項目一覧

CP 輻輳制御のサポート項目一覧を次に示します。

表 7-1 CP 輻輳制御のサポート項目一覧

項目	サポート内容
制御対象となるポート	• 装置で動作中の全ポート対象 ただし，同時に制御対象となるのは最大 16 ポートまでです。
通信停止する単位	• 物理ポート単位 ハイブリッドリンクの場合は，多重している全 VLAN の該当ポートの通信が停止します。 リンクアグリゲーションの場合も通信停止する単位は物理ポート単位です。
通信停止するフレーム	• 該当ポートの全通信 ただし，レイヤ 2 プロトコル制御フレームは対象外です（BPDU，LACP，LLDP，EAPOL など）。 • PPP 制御フレームを含む全フレーム（POS 回線の場合）
通信停止する時間	• 10 秒～ 86400 秒，または無限（コンフィグレーションコマンド congestion-control の control-time の時間）
輻輳チェック対象フレーム	• ブロードキャスト • 制御系マルチキャスト • 自宛ユニキャスト 上記を一括で監視します。

7.3 使用時の注意

- 自宛であっても ARP/NDP の未解決のパケット，IP-Option 拡張ヘッダ付きパケット，IP-TTL オーバのパケット，DHCP ブロードキャストのパケットなど，通常の通信で一時的に CP 輻輳する可能性があるものは輻輳監視から除外しています。
- ブロードキャストストームが発生したり，過度の自宛フレームを受信したりして CP 輻輳となると，本機能が動作します。ただし，ブロードキャストストームではなく，複数のポートから過度の自宛フレームを受信して CP 輻輳を検知した場合は，本機能が動作しないときがあります。
- POS 回線で輻輳が発生し制御対象になった場合，該当する POS 回線の PPP コネクションが切断され，インタフェースがダウンすることがあります。**【SB-7800S】**
- 本機能を使用する場合は，OSPF や OSPFv3 の収容条件の最大隣接ルータ数の半分でネットワーク設計をしてください。
- ポートの閉塞時，閉塞解除時に運用ログとして CP 輻輳制御メッセージを出力します。
- 本機能を使用しても，次に示す条件のどれかに該当する場合，CP 輻輳メッセージを出力します。
  1. 輻輳チェック対象フレーム以外のフレームで輻輳が発生している場合
  2. 輻輳制御可能なポート数（16 ポート）を超えて輻輳が発生している場合
  3. 輻輳制御しているポートが 8 ポート以上連続して通信停止を解除した場合
- 本機能を使用しても輻輳状態が改善されない場合は，フロー検出（フロー検出条件モード 1）との併用をお勧めします。併用可能なパッケージに関しては，「表 1-5　フロー検出条件モードと対応可能 PSU, BSU の関係」を参照してください。

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 IEEE802.3ah/UDLD 機能

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ない，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となり，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そのポートを閉塞することによって未然に防げます。

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とられています。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ます。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。

イーサネットケーブルで接続された片方の装置側のポートに障害検出モードを設定することで，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。障害検出モー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，そのポートの閉塞処理を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するポートでの運用を停止します。

8.1.2 サポート機能

IEEE802.3ah/UDLD 機能でサポートする IEEE802.3ah/OAM 機能を次の表に示します。

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を行うことができず，障害検出モード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，障害検出モー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，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。

9 SNMP を使用したネットワーク管理

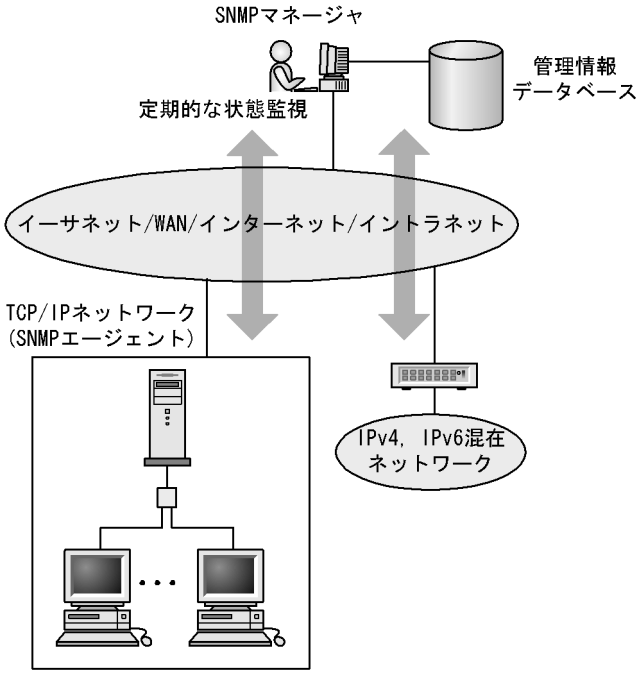
この章では本装置の SNMP エージェント機能についてサポート仕様を中心に説明します。

9.1　SNMP 概説

9.1.1　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。

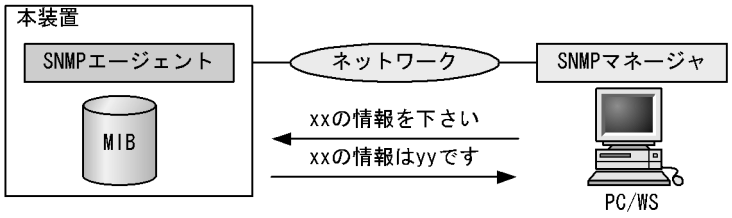
図 9-1　ネットワーク管理の概要



9.1.2　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 9-2　MIB 取得の例

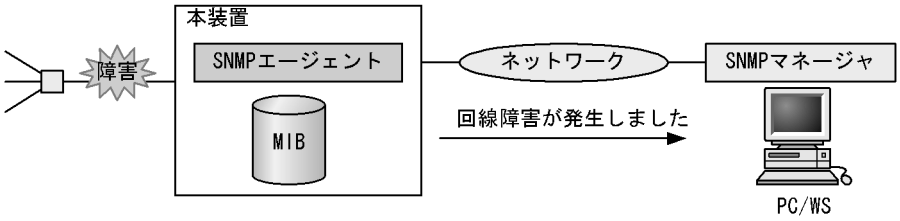


本装置の運用コマンドには MIB 情報を表示するための SNMP コマンドがあります。このコマンドは，自装置およびリモート装置の SNMP エージェントの MIB を表示します。ただし，ネットワーク管理を効率よく行うためには，SNMP マネージャを購入して運用することをお勧めします。

本装置では，SNMPv1(RFC1157)，SNMPv2(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，SNMPv2，または SNMPv3 プロトコルで使用してください。

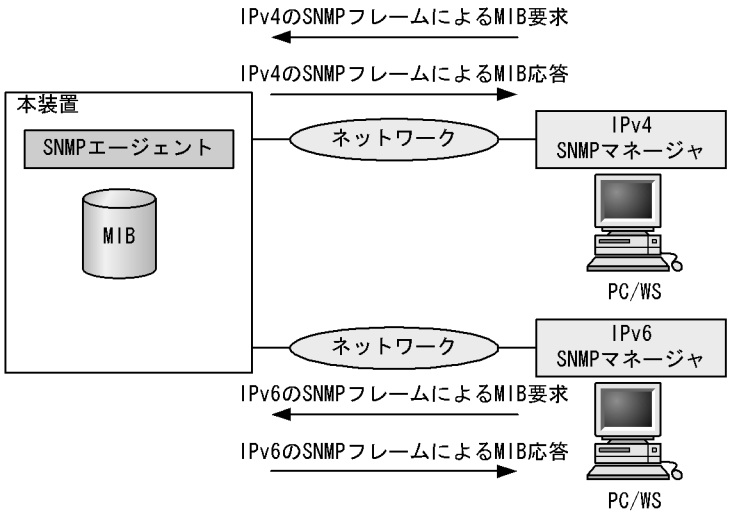
また，SNMP エージェントは**トラップ** (Trap) と呼ばれるイベント通知 (主に障害発生の情報など) 機能があります。SNMP マネージャは，トラップを受信することで定期的に装置の状態変化を監視しなくても変化を知ることができます。ただし，トラップは UDP を使用しているため，装置から SNMP マネージャに対するトラップが到達確認できません。そのため，ネットワークの輻輳などによって，トラップがマネージャに到達しない場合があります。トラップの例を次の図に示します。

図 9-3　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を行うことができます。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 9-4　IPv4/IPv6 SNMP マネージャからの MIB 要求と応答の例



9.1.3　SNMPv3

SNMPv3 は SNMPv2 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。

（1） 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。

（2） 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。

（3） 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 HMAC-MD5-96 および HMAC-SHA-96 を，プライバシープロトコルとして CBC-DES をサポートしています。

（4） 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定義できます。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 OID 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 include（MIB ビューに含む），または exclude（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，通知ビューとして設定できます。

9.2 MIB 概説

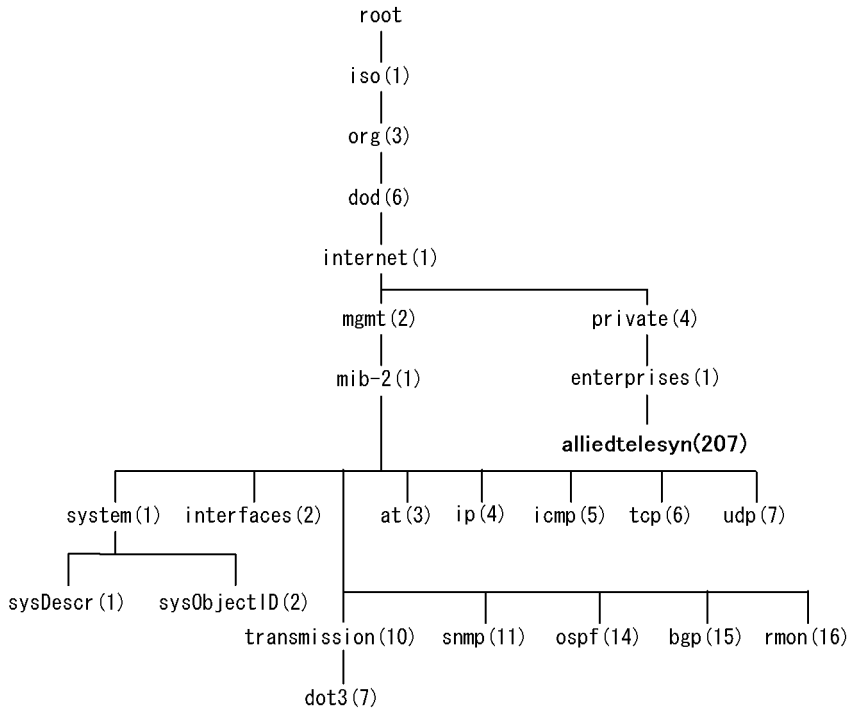
装置が管理し，SNMP マネージャに提供する MIB は，RFC で規定されたものと，装置の開発ベンダーが独自に用意する情報の 2 種類があります。

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まりありません。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。

9.2.1 MIB 構造

MIB の構造はツリー構造になっています。MIB はツリ - 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 9-5 MIB ツリーの構造例



9.2.2 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。

9.2.3 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フェースがあります。特定のインタフェースのタイプを調べるには，"2 番目のインタフェースのタイプ " 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,zzzzzz } となっている MIB のエントリは，xxxxx と yyyyy と zzzzzz 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。

9.2.4 本装置のサポート MIB

本装置では，装置の状態，インタフェースの統計情報，ルーティング情報，装置の機器情報など，ルータの管理に必要な 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いたします。

各 MIB の詳細については，「MIB レファレンス　1. サポート MIB の概要」を参照してください。

9.3　SNMP 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。

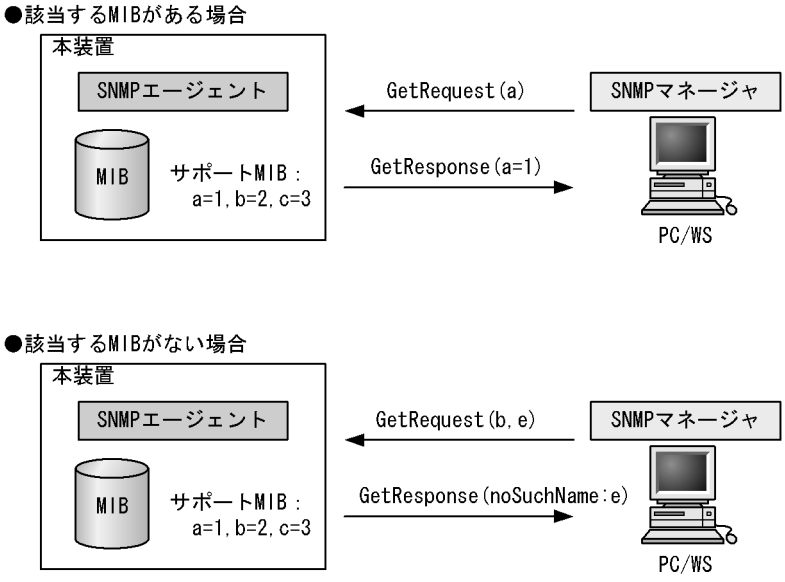
各オペレーションは SNMP マネージャから装置 (SNMP エージェント) に対して行われます。各オペレーションについて説明します。

9.3.1　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。

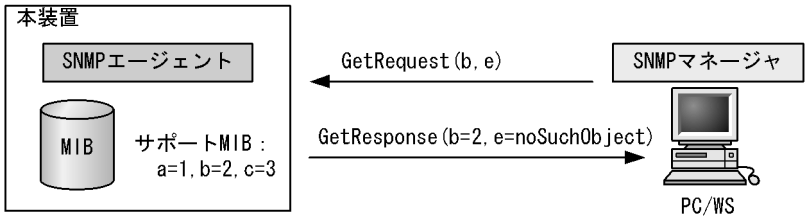
装置が該当する MIB を保持している場合，GetResponse オペレーションで MIB 情報を応答します。該当する MIB を保持していない場合は，GetResponse オペレーションで noSuchName を応答します。
GetRequest オペレーションを次の図に示します。

図 9-6　GetRequest オペレーション



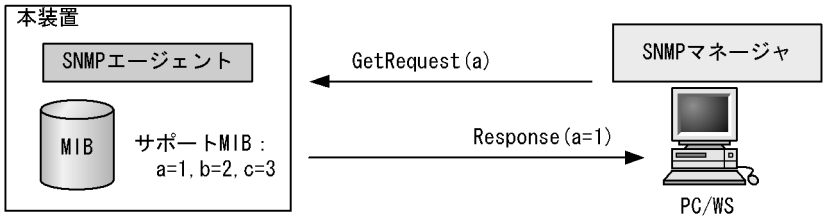
SNMPv2c では，装置が該当する MIB を保持していない場合は，GetResponse オペレーションで MIB 値に noSuchObject を応答します。SNMPv2 の場合の GetRequest オペレーションを次の図に示します。

図 9-7　GetRequest オペレーション (SNMPv2c)



SNMPv3 では，GetRequest オペレーションの応答として，GetResponse オペレーションではなく，Response オペレーションを使用します。SNMPv3 の場合の GetRequest オペレーションを次の図に示します。

図 9-8　GetRequest オペレーション (SNMPv3)

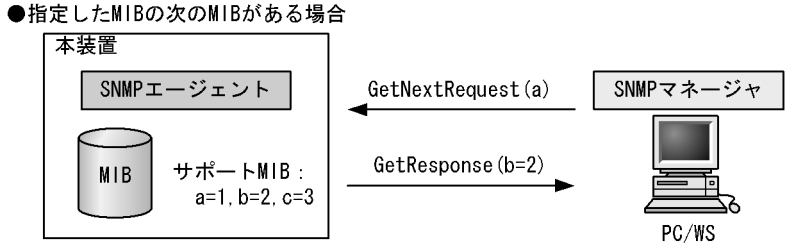


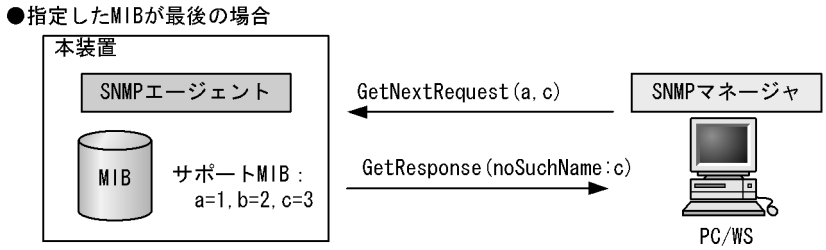
9.3.2　GetNextRequest オペレーション

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。GetResponse オペレーションを次の図に示します。

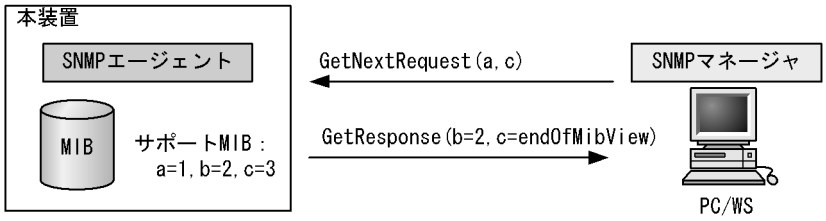
図 9-9　GetNextRequest オペレーション





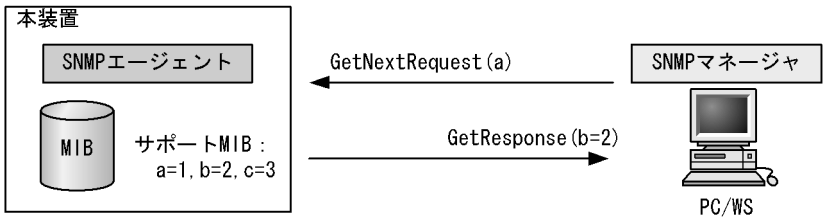
SNMPv2c の場合，指定した MIB が最後の場合は GetResponse で MIB 値に endOfMibView を応答します。SNMPv2 の場合の GetNextRequest オペレーションを次の図に示します。

図 9-10　GetNextRequest オペレーション (SNMPv2c)



SNMPv3 では，GetNextRequest オペレーションの応答として，GetResponse オペレーションではなく，Response オペレーションを使用します。SNMPv3 の場合の GetNextRequest オペレーションを次の図に示します。

図 9-11　GetNextRequest オペレーション (SNMPv3)

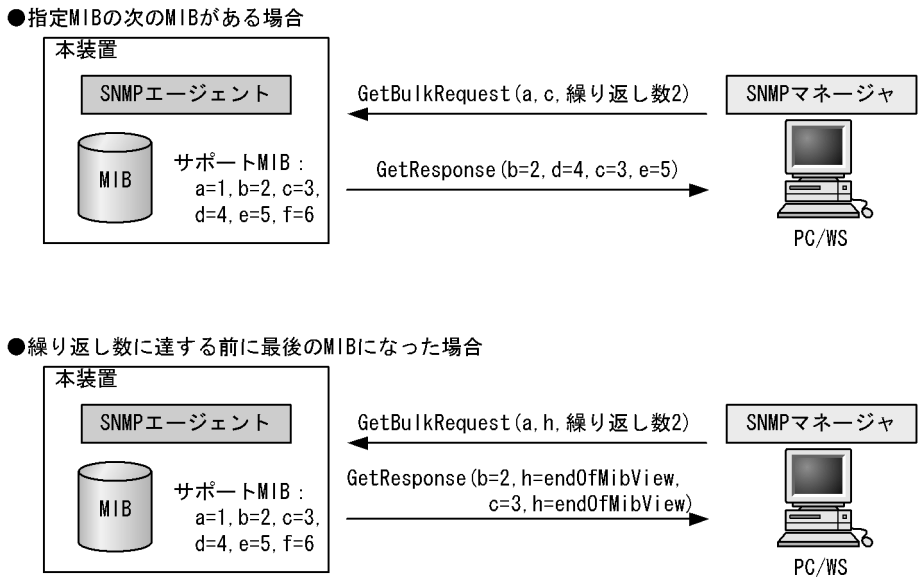


9.3.3　GetBulkRequest オペレーション

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。

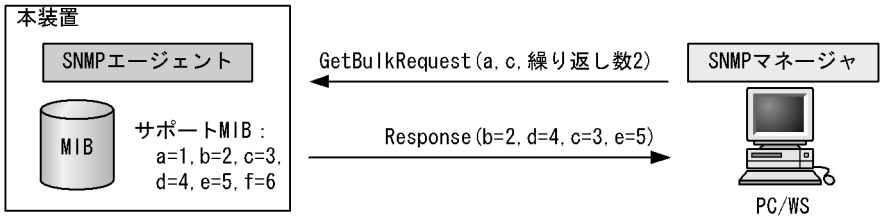
装置が，指定した MIB の次の項目から指定した繰り返し回数個分の MIB を保持している場合は，GetResponse オペレーションで MIB を応答します。指定した MIB が最後の場合，または繰り返し数に達する前に最後の MIB になった場合，GetResponse オペレーションで MIB 値に endOfMibView を応答します。GetNextRequest オペレーションを次の図に示します。

図 9-12　GetBulkRequest オペレーション



SNMPv3 では，GetBulkRequest オペレーションの応答として，GetResponse オペレーションではなく，Response オペレーションを使用します。SNMPv3 の場合の GetBulkRequest オペレーションを次の図に示します。

図 9-13　GetBulkRequest オペレーション (SNMPv3)

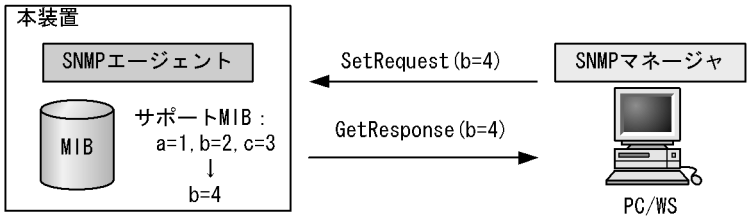


9.3.4　SetRequest オペレーション

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。

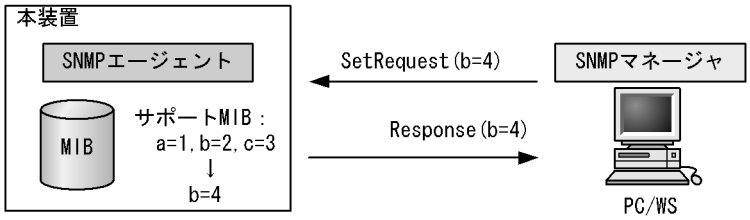
SetRequest オペレーションでは，設定する値と MIB を指定します。値を設定すると，GetResponse オペレーションで MIB と設定値を応答します。なお，本装置で SetRequest オペレーションが実行できる MIB は，MIB-II の system グループの MIB，interface グループの MIB，RMON の MIB，および SNMPv3 の MIB の一部です。SetRequest オペレーションを次の図に示します。

図 9-14 SetRequest オペレーション



SNMPv3 では，SetRequest オペレーションの応答として，GetResponse オペレーションではなく，Response オペレーションを使用します。SNMPv3 の場合の SetRequest オペレーションを次の図に示します。

図 9-15 SetRequest オペレーション (SNMPv3)



(1) MIB を設定できない場合の応答

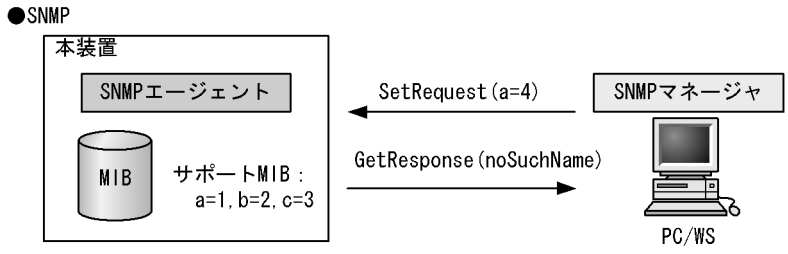
MIB を設定できないケースは，次に示す 3 通りです。

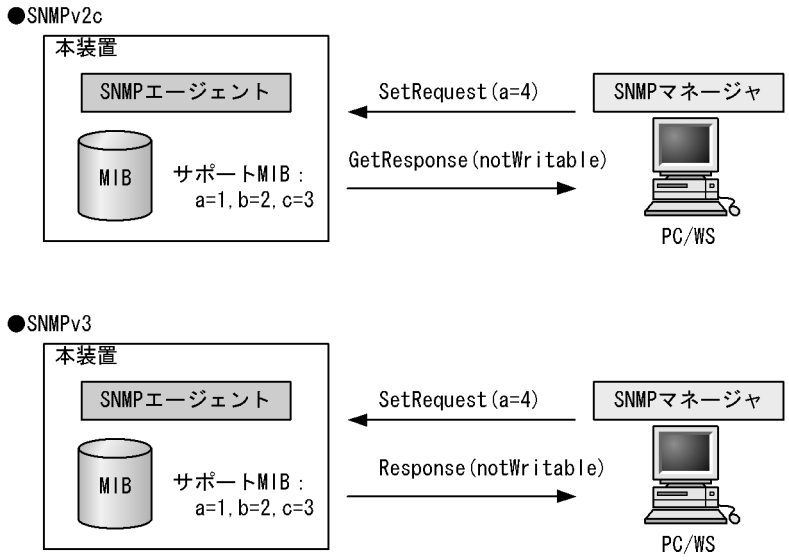
- MIB が読み出し専用の場合 (読み出し専用コミュニティに属するマネージャの場合も含む)
- 設定値が正しくない場合
- 装置の状態によって設定できない場合

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 を応答します。SNMPv2c の場合，MIB が読み出し専用の時は notWritable の GetResponse 応答をします。SNMPv3 の場合，MIB が読み出し専用の時は 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 9-16 MIB 変数が読み出し専用の場合の SetRequest オペレーション

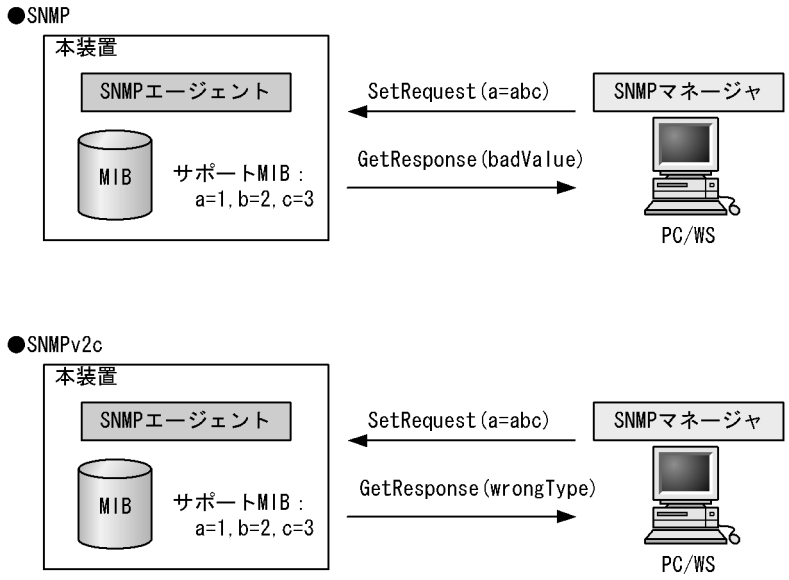


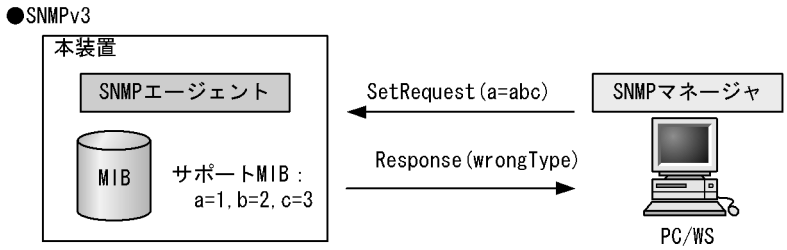


設定値のタイプが正しくない場合，badValue を応答します。SNMPv2c の場合，設定値のタイプが正しくない時は wrongType の GetResponse 応答をします。SNMPv3 の場合，設定値のタイプが正しくない時は wrongType の Response 応答をします。

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。

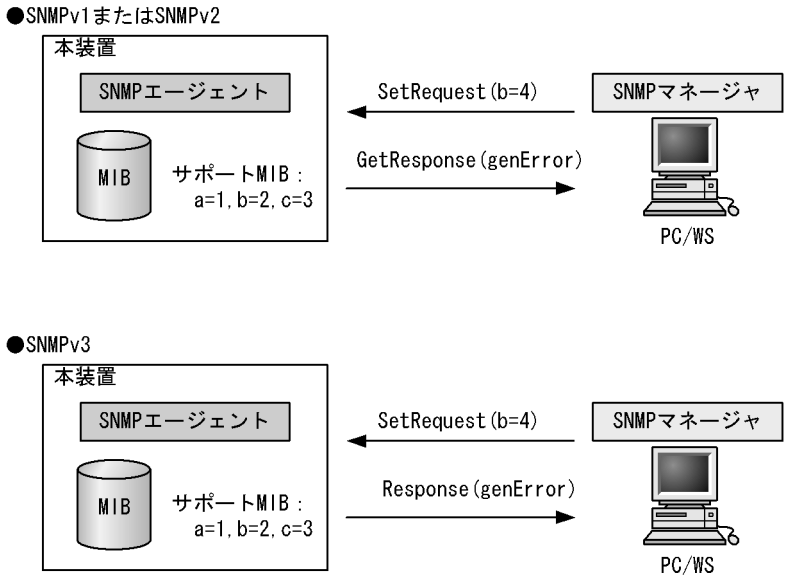
図 9-17　設定値のタイプが正しくない場合の SetRequest オペレーション例





装置の状態によって設定できない場合，GenError の GetResponse を応答します。SNMPv3 では，GetResponse ではなく，Response 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 9-18　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



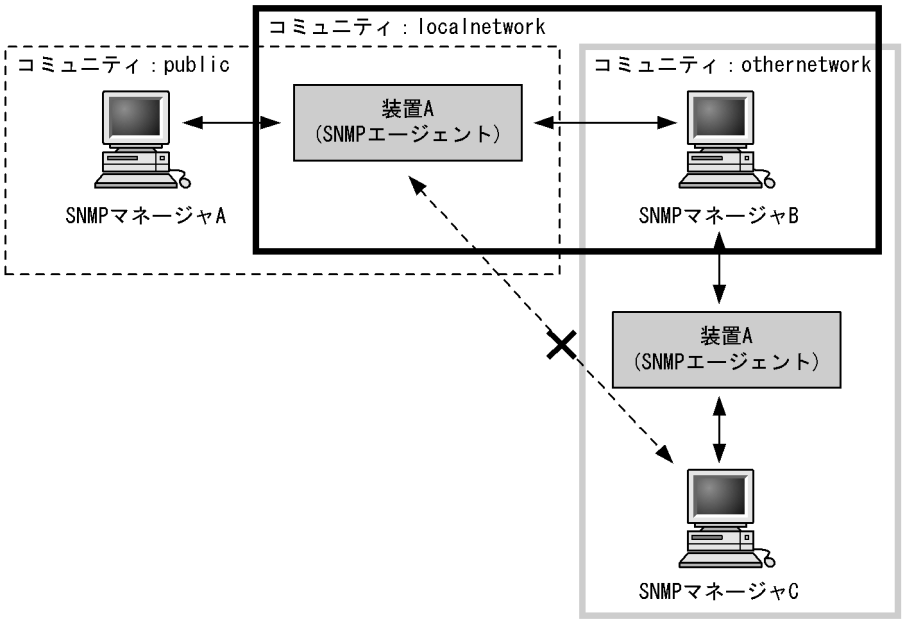
9.3.5　SNMP オペレーションの制限事項

SNMP オペレーションを実行するときには，次に示す制限事項に留意してください。

(1) 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 9-19 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。

(2) 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，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しています。本装置で SNMPv1 および SNMPv2c を使用するときは，コミュニティと SNMP マネージャの IP アドレス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。

(3) SNMPv3 でのオペレーション制限

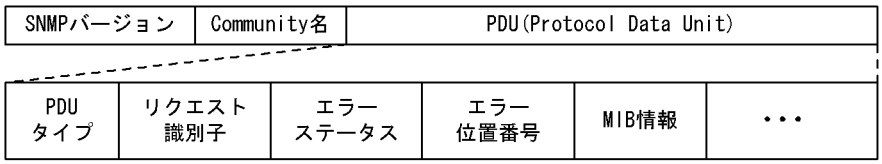
SNMPv1 および SNMPv2c ではコミュニティと SNMP マネージャの IP アドレスの組み合わせによって確認が行われるのに対し，SNMPv3 ではユーザ認証と MIB ビューによって MIB のオペレーションを制限します。本装置で SNMPv3 を使用するときは，SNMP セキュリティユーザ，MIB ビュー，およびセキュリティグループをコンフィグレーションコマンドで登録する必要があります。また，トラップを送信するには，SNMP セキュリティユーザ，MIB ビュー，通知フィルタ，および通知情報をコンフィグレーションコマンドで登録する必要があります。

9.3.6 SNMP オペレーションのメッセージフォーマット

(1) SNMPv1 オペレーション，SNMPv2c オペレーションのメッセージフォーマット

SNMPv1，SNMPv2c のオペレーションを行うメッセージフォーマットは，RFC1157 で規定されています。メッセージフォーマットの概要を次の図に示します。

図 9-20 SNMP オペレーションメッセージフォーマット



GetRequest，GetNextRequest，GetBulkRequest，SetRequest，GetResponse の各オペレーションのメッセージフォーマットは同じです。PDU タイプの値によってメッセージが区別されます。

オペレーション時は，オペレーションの種別を区別するために次の項目に値を設定して SNMP エージェントにメッセージを送信します。

- PDU タイプに種別を設定する
- フレーム送信シーケンス番号をリクエスト識別子に設定する
- オペレーションする MIB のオブジェクト ID を MIB 情報に設定する

PDU タイプコードを次の表に示します。

表 9-1 PDU タイプコード

オペレーション	コード
GetRequest	0xA0
GetNextRequest	0xA1
GetResponse	0xA2
SetRequest	0xA3
GetBulkRequest	0xA5

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 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 9-2 エラーステータスコード

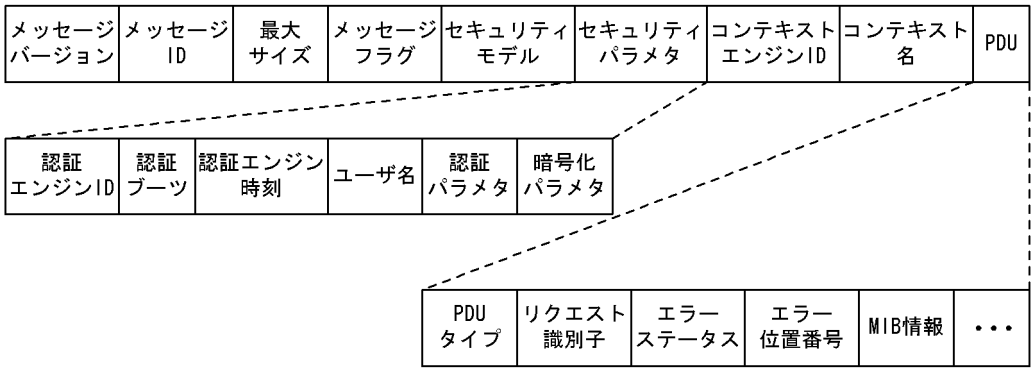
エラーステータス	コード	内容
noError	0	エラーはありません。
tooBig	1	データサイズが大きく PDU に値を設定できません。
noSuchName	2	指定 MIB がない，または書き込みできませんでした。
badValue	3	設定値が不正です。
readOnly	4	書き込みできませんでした（本装置では，応答することはありません）。
GenError	5	コード 0 ～ 4 以外のエラーが発生しました。
noAccess	6	アクセスできない MIB に対して set を行おうとしました。
wrongType	7	MIB で必要なタイプと異なるタイプが指定されました。
wrongLength	8	MIB で必要なデータ長と異なる長さが指定されました。
wrongEcoding	9	ASN.1 符号が不正でした。

エラーステータス	コード	内容
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	現在何か理由があっ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。
commitFaild	14	値の更新に失敗しました。
undoFaild	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。
notWriteable	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。

（2） SNMPv3 オペレーションのメッセージフォーマット

SNMPv3 のオペレーションを行うメッセージフォーマットは，RFC3416 で規定されています。メッセージフォーマットの概要を次の図に示します。

図 9-21　SNMPv3 オペレーションメッセージフォーマット



GetRequest，GetNextRequest，GetBulkRequest，SetRequest，Response，SNMPv2-Trap，Report の各オペレーションのメッセージフォーマットは同じです。PDU タイプの値によってメッセージが区別されます。

オペレーション時は，オペレーションの種別を区別するため，次の項目に値を設定して SNMP エージェントにメッセージを送信します。

- PDU タイプに種別を設定する。
- フレーム送信シーケンス番号をリクエスト識別子に設定する。
- オペレーションする MIB のオブジェクト ID を MIB 情報に設定する。

PDU タイプコードを次の表に示します。

表 9-3　PDU タイプコード

オペレーション	コード
GetRequest	0xA0
GetNextRequest	0xA1
Response	0xA2

オペレーション	コード
SetRequest	0xA3
GetBulkRequest	0xA5
SNMPv2-Trap	0xA7
Report	0xA8

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 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 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 9-4　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，応答することはありません)。
GenError	5	コード 0 ～ 4 以外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。
wrongEcoding	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	現在何か理由があっ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。
commitFaild	14	値の更新に失敗しました。
undoFaild	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。
notWriteable	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。

（3）SNMP オペレーションメッセージサイズの制限

本装置では 2048 バイトまでの SNMP オペレーションメッセージを処理します。2048 バイトを超える SNMP オペレーションメッセージは破棄されます。

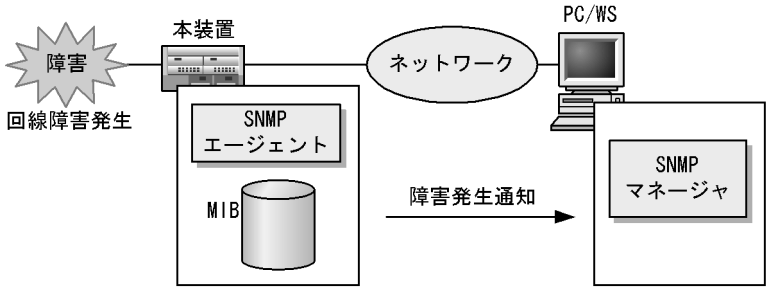
9.4 トラップ

9.4.1 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。

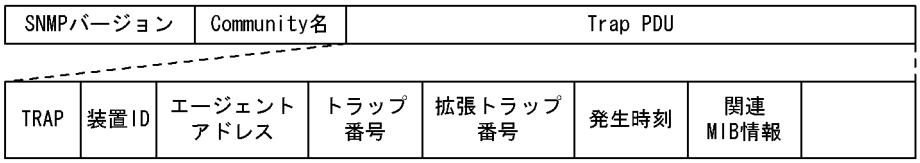
図 9-22 トラップの例



9.4.2 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 9-23 トラップフォーマット



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

9.4.3 サポートトラップ

本装置では，MIB-II トラップ，BGP トラップ，RMON トラップ，プライベートトラップの 4 種類をサポートしています。本装置がマネージャにトラップを通知するためには，コンフィグレーションコマンドでトラップを受信する SNMP マネージャのコミュニティ名，IP アドレスおよび受信するトラップのレベル (標準トラップだけか，プライベートトラップを含むか) を登録する必要があります。また，MIB-II トラップは使用している機能に関係なく，常に有効です。ほかのトラップは，機能を有効にすることでト

ラップが発行されます。

本装置が通知するトラップを次の表に示します。

表 9-5 本装置が通知するトラップ

トラップ種別	イベント通知概要
MIB-II トラップ	• 装置が起動しました。 • 装置の構成変化を検出しました。 • 回線のリンクダウンを検出しました。 • 回線のリンクダウンの回復を検出しました。 • 不正な SNMP マネージャからのアクセスを検出しました。
BGP トラップ	• BGP リンク確立を検出しました。 • BGP リンク断を検出しました。
RMON トラップ	• 特定の MIB の値が上方閾値超えを検出しました。 • 特定の MIB の値が下方閾値下回りを検出しました。
プライベートトラップ	• システム障害または警告メッセージの出力を検出しました。 • 待機系 BCU の状態変化を検出しました。

各トラップの詳細については「MIB レファレンス 4. サポート MIB トラップ」を参照してください。

9.5 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 が閾値に達した時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 と閾値を超えた時にログを記録する logTable グループ MIB があります。

eventTable グループ MIB は，閾値に達した時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。

RMON は，SNMP マネージャでも使用できますが，専用の RMON マネージャを使用すれば，より有効に RMON を活用できます。ただし，RMON マネージャによっては，本装置で使用できないものがありますので事前にテストしてから利用してください。

10 フロー統計を使用したネットワーク管理

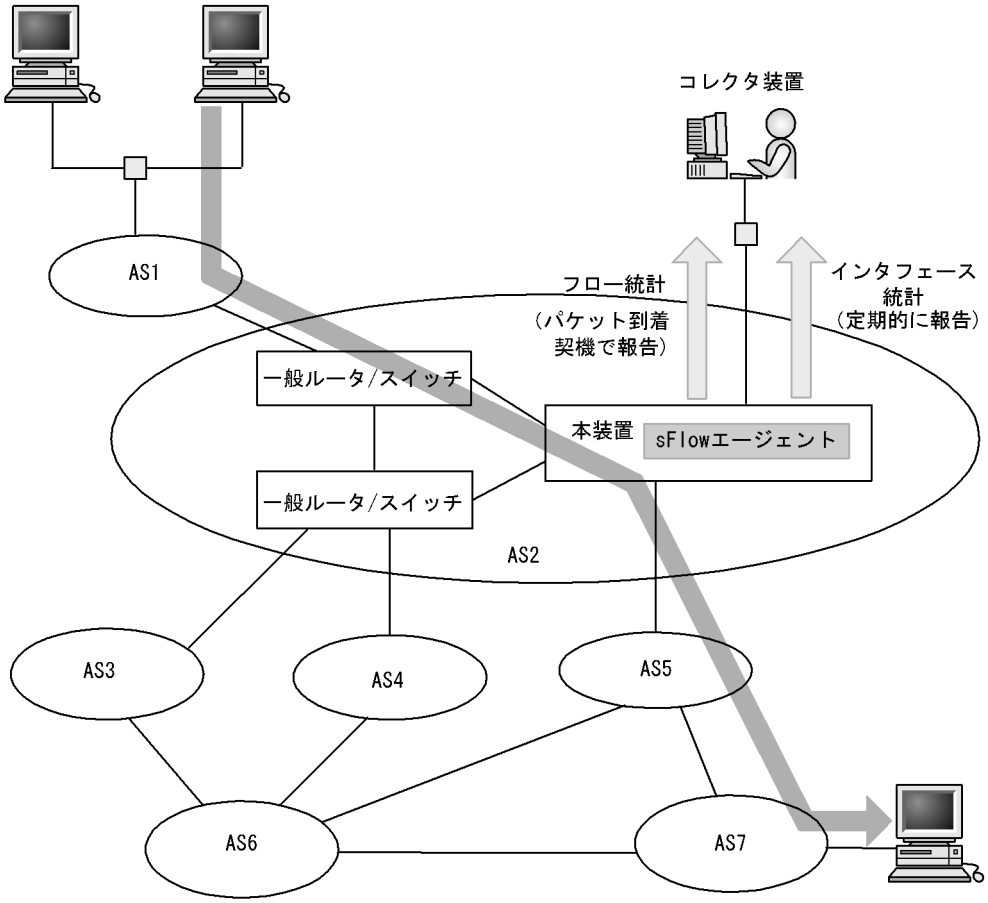
この章では本装置のフロー統計機能についてサポート仕様を中心に説明します。

10.1　sFlow 統計

10.1.1　sFlow 統計概説

sFlow 統計はエンド - エンドのトラフィック（フロー）特性や隣接するネットワーク単位のトラフィック特性の分析を行うため，ネットワークの上を流れるトラフィックを中継装置（ルータやスイッチ）でモニタする機能です。sFlow 統計は国際的に公開されているフロー統計プロトコル（RFC3176）でレイヤ 2 からレイヤ 7 までの統計情報をサポートしています。sFlow 統計情報（以降，sFlow パケット）を受け取り表示する装置を sFlow コレクタ（以降，コレクタ装置）と呼び，コレクタ装置に sFlow パケットを送付する装置を sFlow エージェントと呼びます。sFlow 統計を使ったネットワーク管理例を次の図に示します。

図 10-1　sFlow 統計のネットワーク管理例



（凡例）AS：Autonomous system

本装置の sFlow エージェントで収集する情報は，大きくフロー統計とインタフェース統計に分けられます。収集個所と収集内容を次の図に示します。

図 10-2　フロー統計とインタフェース統計

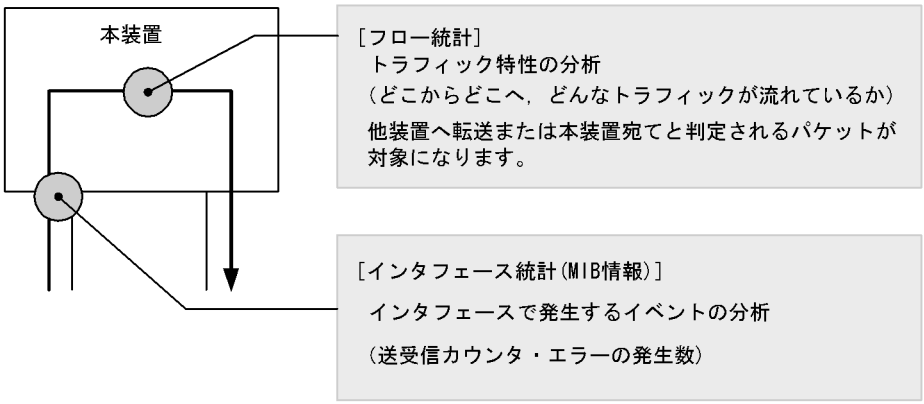
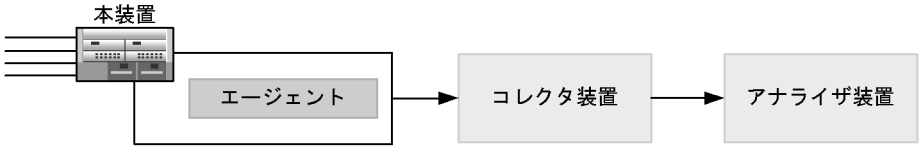


図 10-3　システム構成



本装置の sFlow エージェントでモニタされた情報はコレクタ装置に集められ，統計結果をアナライザ装置によってグラフィカルに表示することができます。したがって，sFlow 統計機能を利用していただくにはコレクタ装置とアナライザ装置を購入して運用する必要があります。

表 10-1　システム構成要素

項番	構成要素	役割り	備考
1	エージェント	統計情報を収集してコレクタ装置に送付します。	-
2	コレクタ装置	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装置に送付します。	アナライザ装置と一緒になっている場合もあります。
3	アナライザ装置	コレクタ装置から送付されるデータをグラフィカルに表示します。	-

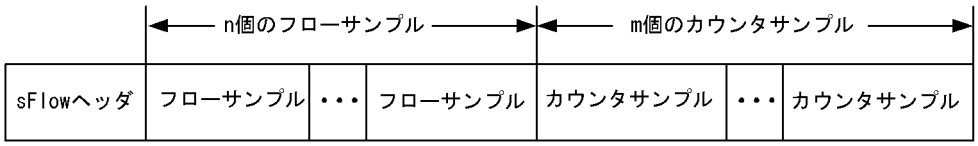
(凡例) -：該当なし

10.1.2　sFlow エージェント機能

本装置の sFlow エージェントは ,(1) 受信パケット（フレーム）をユーザ指定の割合でサンプルし，(2) サンプルしたパケット情報とインタフェース統計を sFlow パケットのフォーマットに整形して，(3) ユーザ指定のコレクタ装置に送付する機能があります。sFlow 統計ではサンプルしたパケット情報のことをフローサンプル，インタフェース統計をカウンタサンプルと呼びます。

コレクタ装置に通知するフォーマットは RFC3176 で規定されています。sFlow パケットのフォーマットを次の図に示します。

図 10-4　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 10-2　sFlow ヘッダのフォーマット

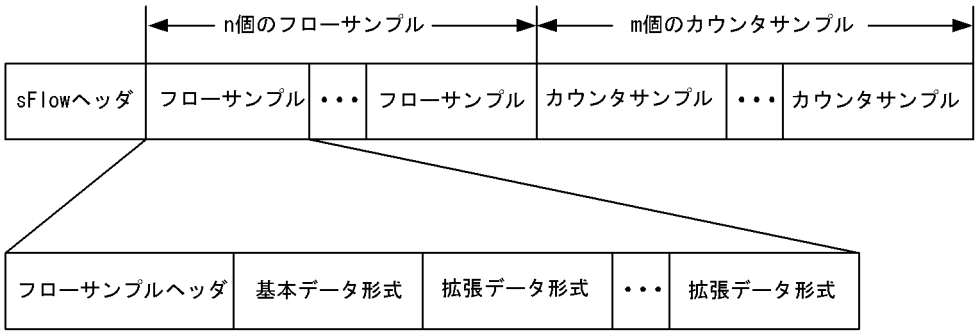
設定項目	説明	サポート
バージョン番号	sFlow パケットのバージョン（バージョン 2，4 サポート）	○
アドレスタイプ	sFlow エージェントの IP タイプ (IPv4=1, IPv6=2)	○
エージェント IP アドレス	sFlow エージェントの IP アドレス	○
シーケンス番号	sFlow パケットの生成ごとに増加する番号	○
生成時刻	現在の時間（装置の起動時からのミリセカンド）	○
サンプル数	この信号に含まれるサンプル（フロー・カウンタ）したパケット数（「図 10-4　sFlow パケットフォーマット」の例では n ＋ m が設定されます）	○

（凡例）　○：サポートする

10.1.3　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，コレクタ装置に通知するためのフォーマットです。フローサンプルにはモニタしたパケットに加えて，パケットには含まれていない情報（受信インタフェース，送信インタフェース，AS 番号など）も設定するため，詳細なネットワーク監視が行えます。フローサンプルのフォーマットを次の図に示します。

図 10-5　フローサンプルのフォーマット



（1） フローサンプルヘッダ

フローサンプルヘッダに設定する内容を次の表に示します。

表 10-3　フローサンプルヘッダのフォーマット

設定項目	説明	サポート
sequence_number	フローサンプルの生成ごとに増加する番号	○
source_id	フローサンプルの装置内の発生源（受信インタフェース）を表す SNMP Interface Index	○
sampling_rate	フローサンプルのサンプリング間隔	○
sample_pool	インタフェースに到着したパケットの総数	○
Drops	廃棄したフローサンプルの総数	○
Input	受信インタフェースの SNMP Interface Index。 インタフェースが不明な場合 0 を設定。	○
Output	送信インタフェースの SNMP Interface Index※1※2。送信インタフェースが不明な場合は 0 を設定。送信インタフェースが複数の場合（マルチキャストなど）は最上位ビットを立て，下位ビットが送信インタフェースの数を示します※3。	○

（凡例）　○：サポートする
注※ 1　ソフトウェア中継の場合は 0 になります。
注※ 2　フラディングパケットが対象になった場合は 0 が収集されます。
注※ 3　マルチキャストの場合，下位ビットは 0 固定です。

（2）基本データ形式

基本データ形式は HEADER 型と IPv4 型と IPv6 型の 3 種類があり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 HEADER 型です。IPv4 型，IPv6 型を使用したい場合はコンフィグレーションコマンドで設定してください。各形式のフォーマットを以降の表に示します。

表 10-4　HEADER 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 (HEADER 型 =1) ※	○
header_protocol	ヘッダプロトコル番号 (ETHERNET=1，PPP=7)	○
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ルした分のパケット長（デフォルト 128)	○
header<>	サンプルしたパケットの内容	○

（凡例）　○：サポートする
注※　IP パケットとして解析ができない場合は本フォーマットになります。

表 10-5　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	○

設定項目	説明	サポート
dst_port	宛先ポート番号	○
tcp_flags	TCP フラグ	○
TOS	IP のタイプオブサービス	○

(凡例) ○：サポートする

表 10-6 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	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

(3) 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，コレクタ装置に通知します。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 10-7 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	○※2
ルータ型	ルータ情報 (NextHop など) を収集する	○※1
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
ユーザ型	ユーザ情報 (TACACS/RADIUS 情報など) を収集する	○
URL 型	URL 情報 (URL 情報など) を収集する宛先 IP アドレス	○

(凡例) ○：サポートする
注※ 1 L2 中継時は sFlow パケットに設定されません。
注※ 2 L3 中継時は sFlow パケットに設定されません。

表 10-8 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 (SWITCH=1)	○
src_vlan	入力フレームの 802.1Q VLAN id	○
src_priority	入力フレームの 802.1p 優先度	○

設定項目	説明	サポート
dst_vlan	出力フレームの 802.1Q VLAN id	○※1※2
dst_priority	出力フレームの 802.1p 優先度	○※3

(凡例) ○：サポートする
注※1 Tag 変換機能を使用している場合，変換前の値が収集されます。
注※2 フラディングパケットが対象になった場合は 0 が収集されます。
注※3 入力フレームの 802.1p 優先度と同じ値が設定されます。

表 10-9 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 (ROUTER 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 IP アドレスのプレフィックスマスクビット	○
dst_mask	宛先 IP 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 10-10 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 (GATEWAY 型 =3)	○
as	本装置の AS 番号	○
src_as	送信元の AS 番号	○※1
src_peer_as	送信元への隣接 AS 番号	○※1※2
dst_as_path_len	AS 情報数 (1 固定)	○
dst_as_type	AS 経路種別 (2 : AS_SEQUENCE)	○
dst_as_len	AS 数 (2 固定)	○
dst_peer_as	宛先への隣接 AS 番号	○※1
dst_as	宛先の AS 番号	○※1
communities<>	本経路に関するコミュニティ※3	×
localpref	本経路に関するローカル優先※3	×

(凡例) ○：サポートする ×：サポートしない
注※1 送受信先がダイレクト経路の場合は，AS 番号が 0 で収集されます。
注※2 本装置から送信元へパケットを送信する場合に，隣接 AS 番号として扱っている値が本フィールドに入ります。本装置へ到着前に実際に通過した隣接 AS 番号と異なる場合があります。
注※3 未サポートのため 0 固定です。

表 10-11 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 (USER 型 =4) ※1	○

設定項目	説明	サポート
src_user_len	送信元のユーザ名の長さ	○
src_user<>	送信元のユーザ名	○
dst_user_len	宛先のユーザ名の長さ※2	○
dst_user<>	宛先のユーザ名※2	○

(凡例)　○：サポートする
注※1　RADIUS は宛先 UDP ポート番号 1812，TACACS は宛先 UDP ポート番号 49 が対象になります。
注※2　未サポートのため 0 固定です。

表 10-12　URL 型のフォーマット

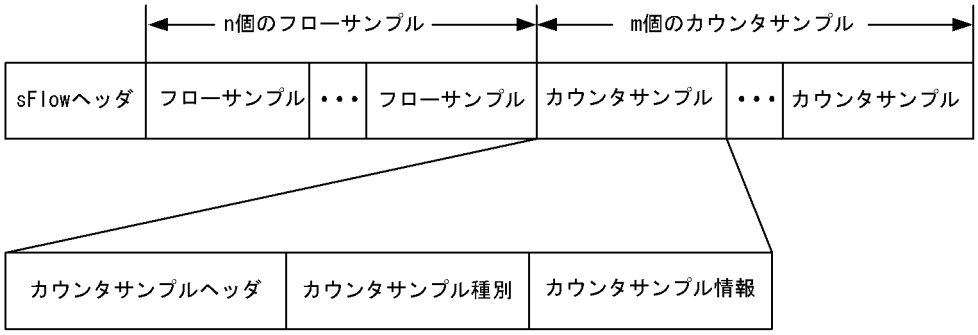
設定項目	説明	サポート
extended_information_type	拡張データ形式のタイプ (URL 型 =5)	○
url_direction	URL 情報源 (source address=1，destination address=2)	○
url_len	URL 長	○
url<>	URL 内容	○

(凡例)　○：サポートする

10.1.4　カウンタサンプル

カウンタサンプルは，インタフェース統計情報（到着したパケット数や，エラーの数など）を通知します。またインタフェースの種別よりコレクタ装置に通知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 10-6　カウンタサンプルのフォーマット



(1) 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 10-13　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 (インタフェース・VLAN 番号) を表す SNMP Interface Index	○
sampling_interval	コレクタ装置へのカウンタサンプルの送信間隔	○

(凡例) ○：サポートする

(2) カウンタサンプル種別

カウンタサンプル種別はインタフェース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 10-14 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)	×※
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)	×※
FDDI	FDDI 統計 (counters_type=4)	×※
100BaseVG	100BASE-VG ANY 統計 (counters_type=5)	×※
WAN	WAN 統計 (counters_type=6)	○
VLAN	VLAN 統計 (counters_type=7)	○

(凡例) ○：サポートする　×：サポートしない
注※　本装置で未サポートなインタフェースタイプのためです。

(3) 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）に従って通知されます。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 10-15 カウンタサンプル情報

設定項目	説明	サポート
GENERIC 統計	［RFC 2233 参照］	×
ETHERNET 統計	［RFC 2358 参照］	○※1
TOKENRING 統計	［RFC 1748 参照］	×
FDDI 統計	［RFC 1512 参照］	×
100BaseVG 統計	［RFC 2020 参照］	×
WAN 統計	［RFC 2233 参照］	○※2
VLAN 統計	［表 10-16　VLAN 統計フォーマットを参照］	○

(凡例) ○：サポートする　×：サポートしない

注※ 1
ifDirection，dot3StatsSymbolErrors は収集できません。

注※ 2
ifDirection は収集できません。ifInMulticastPkts，ifInBroadcastPkts，ifOutMulticastPkts，ifOutBroadcastPkts は 0 固定となります。

表 10-16 VLAN 統計フォーマット

設定項目	説明	サポート
vlan_id	VLAN ID	○
octets	オクテット数	○
ucastPkts	ユニキャストパケット数	○
multicastPkts	マルチキャストパケット数	○
broadcastPkts	ブロードキャストパケット数	○
discards	廃棄パケット数	○

(凡例) ○：サポートする

10.1.5 本装置での sFlow フロー統計の動作について

(1) sFlow フロー統計収集の対象パケットに関する注意点

- 本装置での sFlow のフロー統計は，受信時に他装置へ転送または自宛てと判定されるパケットを対象パケットとして扱います。
- 受信時に廃棄と判定されるパケット (Filter 機能で廃棄判定されるパケットなど) は，sFlow のフロー統計収集の対象外パケットとして扱います。ただし，QoS 機能の廃棄制御に従ってキューイング時に廃棄されるパケットは sFlow のフロー統計収集の対象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

- 本装置での sFlow 機能のフロー統計は，受信側でパケットをサンプルしてコレクタ装置に通知します。この性質上，送信インタフェース側に Filter 機能や QoS 機能を設定してパケットを廃棄する条件でも，コレクタ装置には中継しているように通知してしまいます。Filter 機能や QoS 機能と併用する場合は，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 フロー統計収集条件を次の表に示します。

表 10-17 他機能と併用時の sFlow フロー統計収集条件

機能	IN 側に設定	OUT 側に設定
Filter 機能	廃棄対象は収集されない	収集される
QoS 機能	帯域・優先度で制限される場合は収集されない	収集される

10.1.6 sFlow 統計に関する制限事項【SB-7800S】

(1) ハードに依存する制限事項

PSU-1，PSU-2 では，IP アドレスを定義していないインタフェースで受信したパケットを廃棄する場合，当該パケットを sFlow のサンプル対象パケットとして扱います。上記以外の PSU では非対象パケットとして扱います。

PSU-1，PSU-2 では，マルチキャストの定義を設定していないインタフェースで受信した IP アドレスがマルチキャストであるパケットを廃棄する場合，当該パケットを sFlow のサンプル対象パケットとして扱います。上記以外の PSU では非対象パケットとして扱います。ただし，IPv4 アドレスが 224.0.0.0/24，あるいは IPv6 アドレスが FF00::/12 のパケットは，sFlow のサンプル対象パケットとして扱います。

同一 PSU に NIF を 2 枚搭載して，sFlow が有効なポートを収容している NIF から，中継されるパケット

と廃棄されるパケットを混在して受信した場合，廃棄されたパケットをサンプルしてコレクタ装置に送信する場合があります。

BCU-SH8MS/BCU-SM8MS/BCU-SL8MS の場合に sFlow 統計機能で取り扱える IPv6 経路数は 16,384（16k）経路までです。

（2）ハードに依存しない制限事項

dot1x(IEEEE 802.1X 機能情報）構成情報を有効にしているポートに対して，sFlow 統計情報を有効にした場合，該当ポートで 802.1X として廃棄している自宛パケットが，sFlow 統計の対象パケットとして誤って採取する場合があります。

10.1.7　sFlow 統計に関する制限事項【SB-5400S】

（1）ハードに依存する制限事項

BSU-C1，BSU-S1 では，IP アドレスを定義していないインタフェースで受信したパケットを廃棄する場合，当該パケットを sFlow のサンプル対象パケットとして扱います。上記以外の BSU では非対象パケットとして扱います。

BSU-C1，BSU-S1 では，マルチキャストの定義を設定していないインタフェースで受信した IP アドレスがマルチキャストであるパケットを廃棄する場合，当該パケットを sFlow のサンプル対象パケットとして扱います。上記以外の BSU では非対象パケットとして扱います。ただし，IPv4 アドレスが 224.0.0.0/24，あるいは IPv6 アドレスが FF00::/12 のパケットは，sFlow のサンプル対象パケットとして扱います。

NIF を 2 枚以上※搭載して，sFlow が有効なポートを収容している NIF から，中継されるパケットと廃棄されるパケットを混在して受信した場合，廃棄されたパケットをサンプルしてコレクタ装置に送信する場合があります。

注※

2 枚搭載の場合は，実装位置が NIF 番号 0 または 1 に 1 枚実装，NIF 番号 2 または 3 に 1 枚実装される場合にだけ上記現象が発生します。

（2）ハードに依存しない制限事項

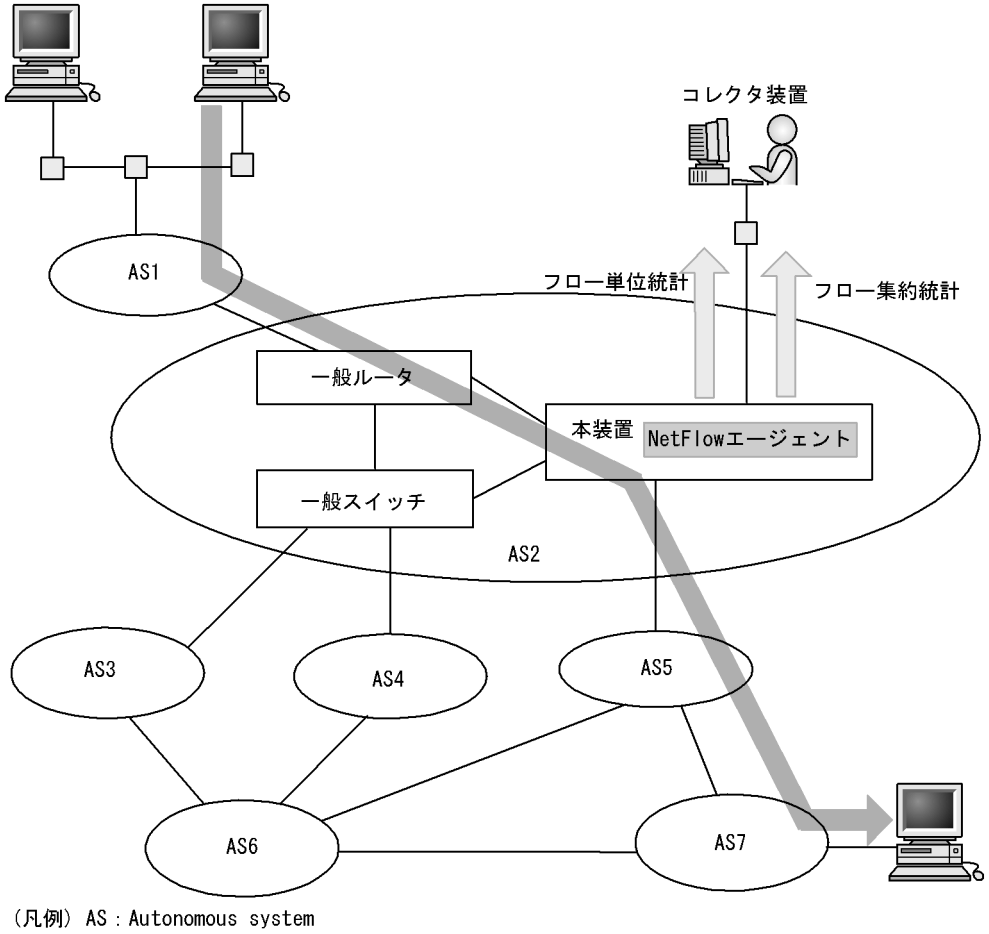
dot1x(IEEEE 802.1X 機能情報）構成情報を有効にしているポートに対して，sFlow 統計情報を有効にした場合，該当ポートで 802.1X として廃棄している自宛パケットが，sFlow 統計の対象パケットとして誤って採取する場合があります。

10.2　NetFlow 統計

10.2.1　NetFlow 統計概説

NetFlow 統計は，ネットワークを流れるトラフィックを本装置（NetFlow エージェント）でサンプリングしてモニタし，そのモニタした NetFlow 統計情報（以降，NetFlow パケット）を NetFlow コレクタと呼ばれる装置（以降，コレクタ装置）に集めて分析することによって，ネットワークの利用状況を把握する機能です。本装置のユーザ指定のポートに入ってくる IP パケットのレイヤ 3 とレイヤ 4 統計情報をコレクタ装置に通知することで，ネットワークの利用状況を把握でき，ネットワーク設備を計画的に増強したり，ネットワークのパフォーマンス低下を引き起こすアタックなどの異常を速やかに検知したりすることを可能にします。特徴としては sFlow 統計より情報を絞って収集しているため，低い負荷で運用が可能です。

図 10-7　NetFlow 統計のネットワーク構成例



本装置の NetFlow エージェントでモニタされた情報はコレクタ装置に集められ，統計結果をアナライザ装置によってグラフィカルに表示することができます。NetFlow 統計機能を利用していただくにはコレクタ装置とアナライザ装置を用意して運用する必要があります。

図 10-8　システム構成

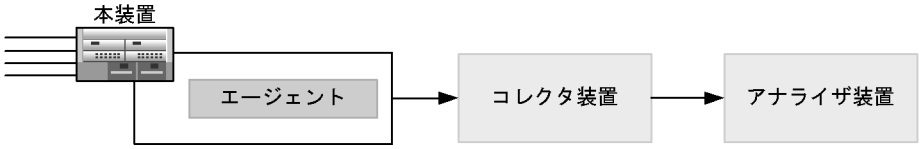


表 10-18　システム構成要素

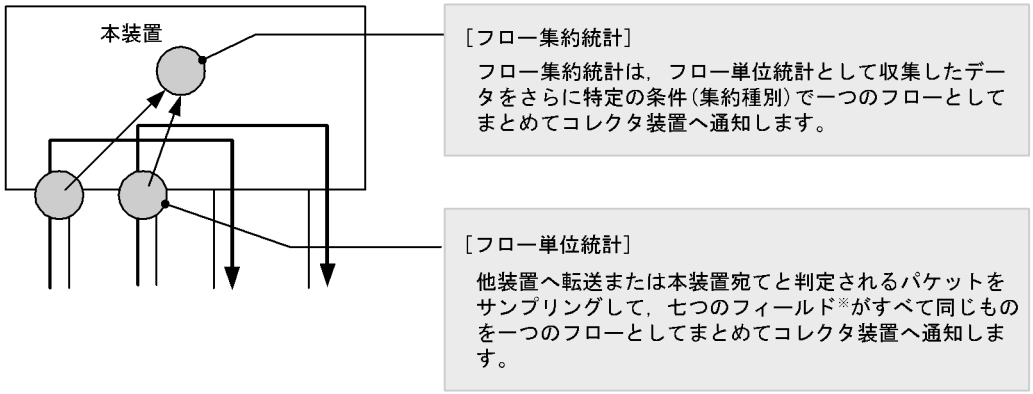
項番	構成要素	役割り	備考
1	エージェント	統計情報を収集してコレクタ装置に送付します。	-
2	コレクタ装置	エージェントから送付される統計情報を集計・編集・表示します。さらに，編集データをアナライザ装置に送付します。	アナライザ装置と一体になっている場合もあります。
3	アナライザ装置	コレクタ装置から送付されるデータをグラフィカルに表示します。	-

(凡例) - : 該当なし

10.2.2　NetFlow エージェント機能

本装置の NetFlow エージェントは，他装置へ転送または本装置宛てと判定されるパケットをユーザ指定の割合でサンプルし，サンプルしたパケット情報を NetFlow パケットのフォーマットに整形し，ユーザ指定のコレクタ装置に送付します。NetFlow パケットのフォーマットは Cisco Systems, Inc. によって規定されています。NetFlow エージェントで収集する情報には，フロー単位統計 (NetFlow datagram Version 5, Version 9) とフロー集約統計 (NetFlow datagram Version 8，Version 9) があります。収集個所と収集内容を「図 10-9　単位統計と集約統計」に示します。また，バージョンごとの特徴と推奨利用ネットワークを「表 10-19　NetFlow バージョンごとの特徴と推奨ネットワーク」に示します。

図 10-9　単位統計と集約統計



注※
発信元IPアドレス，宛先IPアドレス，発信元ポート番号，宛先ポート番号，プロトコルタイプ，TOS（タイプ オブ サービス），受信インタフェース。

本装置からコレクタ装置に対してフロー情報を通知する契機は以下の四つがあります。

- TCP コネクションを終了 (TCP FIN or RST) してから最大無通信時間経過した場合
- 設定したエントリ数を超えたフローが到着した場合 (drop モード以外)

- 最大無通信時間を経過した場合 (未設定時 15 秒)
- 最大通信時間を経過した場合 (未設定時 30 分)

注

最大無通信時間 (timeout-inactive) や最大通信時間 (timeout-active) は NetFlow 統計のコンフィグレーションで変更可能です。

表 10-19 NetFlow バージョンごとの特徴と推奨ネットワーク

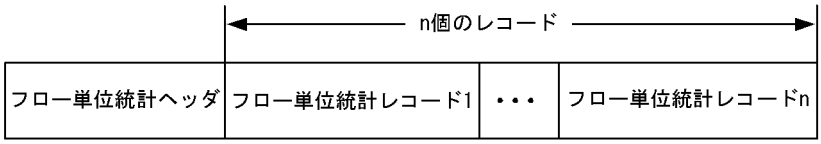
NetFlow バージョン	利用ネットワーク	特徴	備考
Version 5	IPv4 ネットワーク	[収集情報] IPv4 パケットのレイヤ 3，4 の情報を収集 [利点] • Version 8 より情報量が多いため，複数の観点で統計情報の分析が可能 • 対応コレクタ装置が多い [利用例] IPv4 ネットワークの負荷状況の監視 特定フロー (ウィルスやアタックなど) の分析	Version 8 と同時動作可能だが推奨しない
Version 8	IPv4 ネットワーク	[収集情報] IPv4 パケットのレイヤ 3，4 の情報を収集 (ただし，Version 5 より収集情報量は少ない) [利点] CP-CPU 負荷が Version5 より少なくて済む [利用例] Version 5 と同等 (ただし，集約種別によるため，違う観点で見直すことは困難) コレクタ装置への回線速度が遅い環境	Version 5 と同時動作可能だが推奨しない
Version 9	IPv4 ネットワーク ＋ IPv6 ネットワーク	[収集情報] IPv4/IPv6 パケットのレイヤ 3，4 の情報を収集 [利点] IPv6 パケットを対象にできる 先進的な機能のサポートが期待できる RFC3954 で規定されているため，仕様変更に影響されない [利用例] IPv6 ネットワークの負荷状況の監視 特定フロー (ウィルスやアタックなど) の分析	OP-ADV ライセンスが必要

10.2.3 フロー単位統計 (NetFlow Version 5)

フロー単位統計は，本装置に入ってくるパケットをサンプリングし，7 つのフィールド (発信元 IP アドレス，宛先 IP アドレス，発信元ポート番号，宛先ポート番号，プロトコルタイプ，TOS，受信インタフェース) がすべて同じものを一つのまとまり (フロー単位統計レコード) としてコレクタ装置へ通知します。フロー単位統計機能を使うためにはフロー単位統計エントリ (entries) とサンプル間隔 (sample) の設定が必要です。

以下にフロー単位統計パケットのフォーマットを示します。

図 10-10　フロー単位統計パケットフォーマット



(1) フロー単位統計ヘッダ

フロー単位統計ヘッダへ設定される内容を次の表に示します。

表 10-20　フロー単位統計ヘッダ

収集項目	説明	サポート
Version	NetFlow パケットのバージョン番号 (=5)	○
Count	この NetFlow パケットに含まれるフローレコードの数 (最大 30)	○
SysUptime	この NetFlow パケットの生成時刻 (装置起動後からのミリ秒)	○
UnixSecs	この NetFlow パケットの生成時刻 (1970 年を 0000 とする)[秒]	○
UnixNsecs	この NetFlow パケットの生成時刻 (1970 年を 0000 とする)[ナノ秒]	○
FlowSequence	フロー単位統計レコードの生成ごとに増加するシーケンス番号 (“収集項目：Count” の累計数に相当)	○
EngineType	フロー中継エンジンの種別	0 固定
EngineId	フロー中継エンジンの ID 番号	0 固定
SamplingInterval	サンプリングモードおよびサンプリング間隔	○

(凡例)　○：サポートする

(2) フロー単位統計レコード

フロー単位統計のレコードに設定される内容を次の表に示します。

表 10-21　フロー単位統計レコード

収集項目	説明	サポート
SourceIPaddr	送信元 IPv4 アドレス	○
DestinationIPaddr	宛先 IPv4 アドレス	○
NextHop	次の転送先ルータの IPv4 アドレス※ 1	○
Input	受信インタフェースの SNMP Interface Index※ 2	○
Output	送信インタフェースの SNMP Interface Index※ 3※ 4	○
Packets	フローのパケットの総数	○
Bytes	フローのパケットの総バイト数	○
First	フロー開始パケット受信時の SysUptime[秒]	○
Last	フロー最終パケット受信時の SysUptime[秒]	○
SrcPort	TCP/UDP 送信元ポート番号	○
DstPort	TCP/UDP 宛先ポート番号	○
Flags	TCP フラグの累積	○
Protocol	IP プロトコルタイプ ((例) 6=TCP, 17=UDP)	○

収集項目	説明	サポート
TOS	IP のタイプオブサービス	○
SrcAs	送信元もしくは送信元側隣接ピアの AS 番号※1	○
DstAs	宛先もしくは宛先側隣接ピアの AS 番号※1	○
SrcMaskBits	送信元 IPv4 アドレスのプレフィックスマスクビット数※1	○
DstMaskBits	宛先 IPv4 アドレスのプレフィックスマスクビット数※1	○

(凡例) ○：サポートする

注※ 1
レイヤ 2 中継の場合 0 が入ります。

注※ 2
物理ポートの SNMP Index 値を設定。

注※ 3
優先順位は物理ポートの SNMP Index 値より論理ポートの SNMP Index 値 (VLAN> リンクアグリゲーション) の方が高くなります。

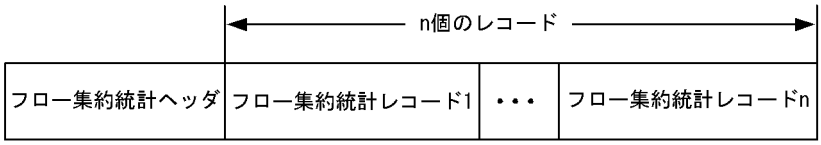
注※ 4
エントリ作成時点 (1 個目のパケットが到着した時点) の送信インタフェースが設定されます。もし，タイムアウト (Active/InActive) 経過前に変更になった場合は正しく通知されない可能性があります。

10.2.4 フロー集約統計 (NetFlow Version 8)

フロー集約統計は，フロー単位統計として収集したデータを更に特定の条件 (集約種別) で一つにまとめて (フロー集約統計レコード) からコレクタ装置へ通知します。フロー集約統計機能を使うためにはフロー単位統計エントリ (entries) とフロー集約統計エントリ (aggregation-entries) とサンプル間隔 (sample) の設定が必要です。

フロー集約統計パケットのフォーマットを次に示します。

図 10-11 フロー集約統計パケットフォーマット



(1) フロー集約統計ヘッダ

フロー集約統計ヘッダに設定される内容を次の表に示します。なお，レイヤ 2 中継パケットはフロー集約統計の対象にはなりません。

表 10-22 フロー集約統計ヘッダ

収集項目	説明	サポート
Version	NetFlow パケットのバージョン番号 (=8)	○
Count	この NetFlow パケットに含まれるフローレコードの数 (最大 51)	○
SysUptime	この NetFlow パケットの生成時刻 (装置起動後からのミリ秒)	○
UnixSecs	この NetFlow パケットの生成時刻 (1970 年を 0000 とする)[秒部分]	○

収集項目	説明	サポート
UnixNsecs	この NetFlow パケットの生成時刻 (1970 年を 0000 とする)[ナノ秒部分]	○
FlowSequence	フロー集約統計レコードの生成ごとに増加するシーケンス番号 (“収集項目：Count” の累計数に相当)	○
EngineType	フロー中継エンジンの種別	0 固定
EngineId	フロー中継エンジンの ID 番号	0 固定
Aggregationtype	フロー集約統計の種別 1: AS Aggregation 2: Protocol-Port Aggregation 3: Source Prefix Aggregation 4: Destination-Prefix Aggregation 5: Prefix Aggregation 9: AS-ToS Aggregation 10: Protocol-Port-ToS Aggregation 11: Source Prefix-ToS Aggregation 12: Destination-Prefix-ToS Aggregation 13: Prefix-ToS Aggregation 14: Prefix-Port Aggregation	○
AggregationVersion	Aggregation のバージョン番号 (=2)	○
SamplingInterval	サンプリングモードおよびサンプリング間隔	○

(凡例)　○：サポートする

(2) フロー集約統計レコード

フロー集約統計レコードへ設定される内容を「表 10-23　AS Aggregation レコード (Aggregationtype=1)」～「表 10-33　Prefix-Port Aggregation レコード (Aggregationtype=14)」に示します。

表 10-23　AS Aggregation レコード (Aggregationtype=1)

収集項目	説明	サポート
Flows	集約したフロー数	○
Packets	集約したフローに含まれる総パケット数	○
Bytes	集約したフローに含まれるパケットの総バイト数	○
First	フロー開始パケット受信時の SysUptime[秒]	○
Last	フロー最終パケット受信時の SysUptime[秒]	○
SrcAs	送信元もしくは送信元側隣接ピアの AS 番号	○
DstAs	宛先もしくは宛先側隣接ピアの AS 番号	○
Input	受信インタフェースの SNMP Interface Index	○
Output	送信インタフェースの SNMP Interface Index	○

(凡例)　○：サポートする

表 10-24　Protocol-Port Aggregation レコード (Aggregationtype=2)

収集項目	説明	サポート
Flows	集約したフロー数	○
Packets	集約したフローに含まれる総パケット数	○
Bytes	集約したフローに含まれるパケットの総バイト数	○

収集項目	説明	サポート
First	フロー開始パケット受信時の SysUptime [秒]	○
Last	フロー最終パケット受信時の SysUptime [秒]	○
Protocol	IP プロトコルタイプ ((例) 6=TCP, 17=UDP)	○
SrcPort	TCP/UDP 送信元ポート	○
DstPort	TCP/UDP 宛先ポート	○

(凡例) ○ : サポートする

表 10-25 Source Prefix Aggregation レコード (Aggregationtype=3)

収集項目	説明	サポート
Flows	集約したフロー数	○
Packets	集約したフローに含まれる総パケット数	○
Bytes	集約したフローに含まれるパケットの総バイト数	○
First	フロー開始パケット受信時の SysUptime [秒]	○
Last	フロー最終パケット受信時の SysUptime [秒]	○
SrcPrefix	集約した送信元 IPv4 アドレスのプレフィックス	○
SrcMaskBits	集約した送信元 IPv4 アドレスのプレフィックスビット数	○
SrcAs	送信元もしくは送信元側隣接ピアの AS 番号	○
Input	受信インタフェースの SNMP Interface Index	○

(凡例) ○ : サポートする

表 10-26 Destination-Prefix Aggregation レコード (Aggregationtype=4)

収集項目	説明	サポート
Flows	集約したフロー数	○
Packets	集約したフローに含まれる総パケット数	○
Bytes	集約したフローに含まれるパケットの総バイト数	○
First	フロー開始パケット受信時の SysUptime [秒]	○
Last	フロー最終パケット受信時の SysUptime [秒]	○
DstPrefix	集約した宛先 IPv4 アドレスのプレフィックス	○
DstMaskBits	集約した宛先 IPv4 アドレスのプレフィックスビット数	○
DstAs	宛先もしくは宛先側隣接ピアの AS 番号	○
Output	送信インタフェースの SNMP Interface Index	○

(凡例) ○ : サポートする

表 10-27 Prefix Aggregation レコード (Aggregationtype=5)

収集項目	説明	サポート
Flows	集約したフロー数	○
Packets	集約したフローに含まれる総パケット数	○
Bytes	集約したフローに含まれるパケットの総バイト数	○

収集項目	説明	サポート
First	フロー開始パケット受信時の SysUptime [秒]	○
Last	フロー最終パケット受信時の SysUptime [秒]	○
SrcPrefix	集約した送信元 IPv4 アドレスのプレフィックス	○
DstPrefix	集約した宛先 IPv4 アドレスのプレフィックス	○
DstMaskBits	集約した宛先 IPv4 アドレスのプレフィックスビット数	○
SrcMaskBits	集約した送信元 IPv4 アドレスのプレフィックスビット数	○
SrcAs	送信元もしくは送信元側隣接ピアの AS 番号	○
DstAs	宛先もしくは宛先側隣接ピアの AS 番号	○
Input	受信インタフェースの SNMP Interface Index	○
Output	送信インタフェースの SNMP Interface Index	○

(凡例)　○ : サポートする

表 10-28　AS-ToS Aggregation レコード (Aggregationtype=9)

収集項目	説明	サポート
Flows	集約したフロー数	○
Packets	集約したフローに含まれる総パケット数	○
Bytes	集約したフローに含まれるパケットの総バイト数	○
First	フロー開始パケット受信時の SysUptime [秒]	○
Last	フロー最終パケット受信時の SysUptime [秒]	○
SrcAs	送信元もしくは送信元側隣接ピアの AS 番号	○
DstAs	宛先もしくは宛先側隣接ピアの AS 番号	○
Input	受信インタフェースの SNMP Interface Index	○
Output	送信インタフェースの SNMP Interface Index	○
TOS	IP のタイプオブサービス	○

(凡例)　○ : サポートする

表 10-29　Protocol-Port-ToS Aggregation レコード (Aggregationtype=10)

収集項目	説明	サポート
Flows	集約したフロー数	○
Packets	集約したフローに含まれる総パケット数	○
Bytes	集約したフローに含まれるパケットの総バイト数	○
First	フロー開始パケット受信時の SysUptime [秒]	○
Last	フロー最終パケット受信時の SysUptime [秒]	○
Protocol	IP プロトコルタイプ ((例) 6=TCP，17=UDP)	○
TOS	IP のタイプオブサービス	○
SrcPort	TCP/UDP 送信元ポート	○
DstPort	TCP/UDP 宛先ポート	○
Input	受信インタフェースの SNMP Interface Index	○

収集項目	説明	サポート
Output	送信インタフェースの SNMP Interface Index	○

(凡例) ○：サポートする

表 10-30 Source Prefix-ToS Aggregation レコード (Aggregationtype=11)

収集項目	説明	サポート
Flows	集約したフロー数	○
Packets	集約したフローに含まれる総パケット数	○
Bytes	集約したフローに含まれるパケットの総バイト数	○
First	フロー開始パケット受信時の SysUptime [秒]	○
Last	フロー最終パケット受信時の SysUptime [秒]	○
SrcPrefix	集約した送信元 IPv4 アドレスのプレフィックス	○
SrcMaskBits	集約した送信元 IPv4 アドレスのプレフィックスビット数	○
TOS	IP のタイプオブサービス	○
SrcAs	送信元もしくは送信元側隣接ピアの AS 番号	○
Input	受信インタフェースの SNMP Interface Index	○

(凡例) ○：サポートする

表 10-31 Destination-Prefix-ToS Aggregation レコード (Aggregationtype=12)

収集項目	説明	サポート
Flows	集約したフロー数	○
Packets	集約したフローに含まれる総パケット数	○
Bytes	集約したフローに含まれるパケットの総バイト数	○
First	フロー開始パケット受信時の SysUptime [秒]	○
Last	フロー最終パケット受信時の SysUptime [秒]	○
DstPrefix	集約した宛先 IPv4 アドレスのプレフィックス	○
DstMaskBits	集約した宛先 IPv4 アドレスのプレフィックスビット数	○
TOS	IP のタイプオブサービス	○
DstAs	宛先もしくは宛先側隣接ピアの AS 番号	○
Output	送信インタフェースの SNMP Interface Index	○

(凡例) ○：サポートする

表 10-32 Prefix-ToS Aggregation レコード (Aggregationtype=13)

収集項目	説明	サポート
Flows	集約したフロー数	○
Packets	集約したフローに含まれる総パケット数	○
Bytes	集約したフローに含まれるパケットの総バイト数	○
First	フロー開始パケット受信時の SysUptime [秒]	○
Last	フロー最終パケット受信時の SysUptime [秒]	○

収集項目	説明	サポート
SrcPrefix	集約した送信元 IPv4 アドレスのプレフィックス	○
DstPrefix	集約した宛先 IPv4 アドレスのプレフィックス	○
DstMaskBits	集約した宛先 IPv4 アドレスのプレフィックスビット数	○
SrcMaskBits	集約した送信元 IPv4 アドレスのプレフィックスビット数	○
TOS	IP のタイプオブサービス	○
SrcAs	送信元もしくは送信元側隣接ピアの AS 番号	○
DstAs	宛先もしくは宛先側隣接ピアの AS 番号	○
Input	受信インタフェースの SNMP Interface Index	○
Output	送信インタフェースの SNMP Interface Index	○

(凡例)　○：サポートする

表 10-33　Prefix-Port Aggregation レコード (Aggregationtype=14)

収集項目	説明	サポート
Flows	集約したフロー数	○
Packets	集約したフローに含まれる総パケット数	○
Bytes	集約したフローに含まれるパケットの総バイト数	○
First	フロー開始パケット受信時の SysUptime [秒]	○
Last	フロー最終パケット受信時の SysUptime [秒]	○
SrcPrefix	集約した送信元 IPv4 アドレスのプレフィックス	○
DstPrefix	集約した宛先 IPv4 アドレスのプレフィックス	○
DstMaskBits	集約した宛先 IPv4 アドレスのプレフィックスビット数	○
SrcMaskBits	集約した送信元 IPv4 アドレスのプレフィックスビット数	○
TOS	IP のタイプオブサービス	○
Protocol	IP プロトコルタイプ ((例) 6=TCP, 17=UDP)	○
SrcPort	TCP/UDP 送信元ポート	○
DstPort	TCP/UDP 宛先ポート	○
Input	受信インタフェースの SNMP Interface Index	○
Output	送信インタフェースの SNMP Interface Index	○

(凡例)　○：サポートする

10.2.5　フロー統計 (NetFlow Version 9)【OP-ADV】

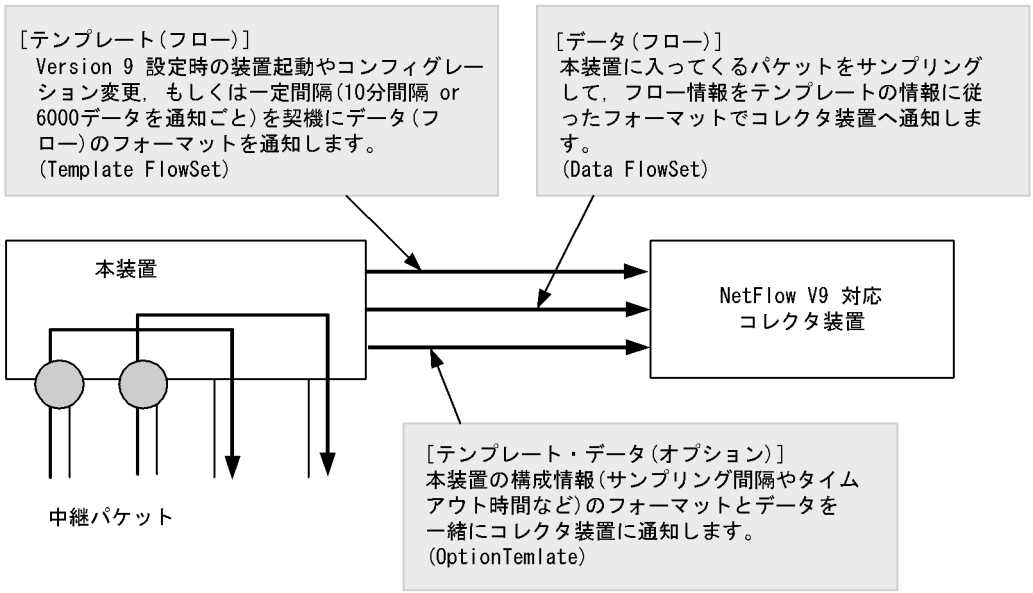
NetFlow Version 9 は，従来の Version 5 や Version 8 のように固定のフォーマット形式でエージェントからコレクタ装置に統計情報を通知するのではなく，テンプレートレコード (以下テンプレート) とデータレコード (以下データ) という二つの情報の組み合わせでコレクタ装置に統計情報を通知します。テンプレートは後続の通知パケットに含まれるデータのフォーマットを指定するために用いられます。データはパケットを受信したデバイスに流れる IP フローの情報を提供します。データの各グループは，それ以前に送信されたテンプレート ID を含んでおり，レコード内のデータを関連付けるために使用します。

NetFlow コンフィグレーションのフロー単位統計のバージョン (flow-export-version) を”9”に設定する

ことで開始します。特徴として統計対象に IPv6 パケットがサポートされました。

NetFlow Version 9 やテンプレートとデータの関係の詳細については RFC3954(Cisco Systems NetFlow Services Export Version 9) をご参照してください。

図 10-12 テンプレートとデータ



以下に本装置で NetFlow Version 9 パケットとして使われるフォーマットを示します。

図 10-13 Template FlowSet パケットフォーマット

NetFlow Version 9 ヘッダ	Template FlowSet 情報 1	•••	Template FlowSet 情報 m

図 10-14 Data FlowSet パケットフォーマット

NetFlow Version 9 ヘッダ	Data FlowSet 情報 1	•••	Data FlowSet 情報 n

図 10-15 OptionTemplate パケットフォーマット

NetFlow Version 9 ヘッダ	OptionTemplate 情報	Option Data 情報

(1) NetFlow Version 9 ヘッダ

NetFlow Version 9 ヘッダの内容を次の表に示します。

表 10-34 NetFlow Version 9 ヘッダフォーマット

収集項目	説明	サポート
Version	NetFlow パケットのバージョン番号 (=9)	○
Count	この NetFlow パケットに含まれる Template もしくは Data FlowSet の数	○

収集項目	説明	サポート
SysUptime	この NetFlow パケットの生成時刻 (装置起動後からのミリ秒)	○
UnixSecs	この NetFlow パケットの生成時刻 (1970 年を 0000 とする)[秒部分]	○
Package Sequence	NetFlow パケットの生成ごとに増加するシーケンス番号	○
SourceId	フロー中継エンジンの種別および ID 番号。 1 ～ 2 バイト目：Reserved。 3 バイト目：フロー中継エンジンの種別。 4 バイト目：フロー中継エンジンの ID 番号。	0 固定

(凡例)　○：サポートする

（2） Template FlowSet 情報

フロー単位統計やフロー集約統計を NetFlow Version9 形式でコレクタ装置に通知するために使います。

図 10-16　Template FlowSet パケットフォーマット

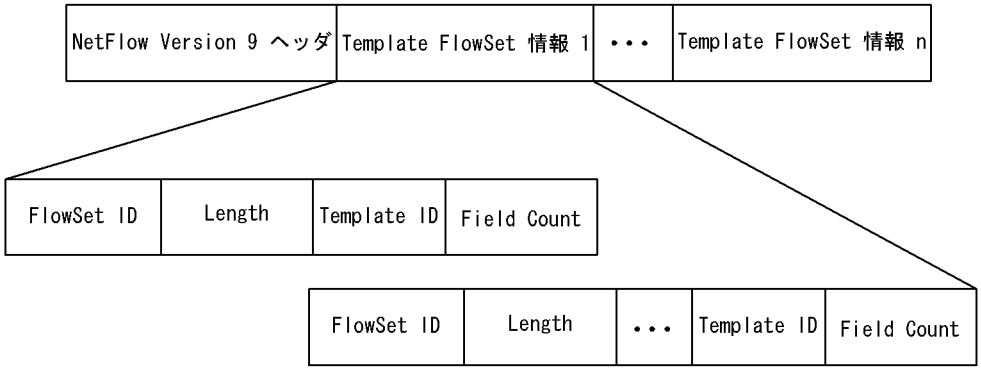


表 10-35　Template FlowSet 情報フォーマット

収集項目	説明	サポート
FlowSet ID	Template，DataFlowSet を識別するための番号。 (Template FlowSet の場合 =0)	○
Length	Template FlowSet の長さ (FlowSet ID および Length も含む)	○

収集項目	説明	サポート
Template ID	コレクタ装置に通知するフォーマットを識別するための番号が記述されます。同時に複数のテンプレートをコレクタ装置に通知することも可能です。詳細については「表 10-37　Version 5 相当情報 {IPv4} (Template ID =256)」～「表 10-62　BGP-Nexthop-Tos Aggregation Record 相当情報 {IPv6} (Template ID =281)」を参照してください。 [Template ID とフォーマットの関係] 256 : Version 5 相当情報 {IPv4} （「表 10-37　Version 5 相当情報 {IPv4} (Template ID =256)」） 257 : Version 5 相当情報 {IPv6} （「表 10-38　Version 5 相当情報 {IPv6} (Template ID =257)」） 258 : AS Aggregation Record 相当情報 {IPv4} （「表 10-39　AS Aggregation Record 相当情報 {IPv4}(Template ID =258)」） 259 : AS Aggregation Record 相当情報 {IPv6} （「表 10-40　AS Aggregation Record 相当情報 {IPv6}(Template ID =259)」） 260 : Protocol-Port Aggregation Record 相当情報 {IPv4} （「表 10-41　Protocol-Port Aggregation Record 相当情報 {IPv4}(Template ID =260)」） 261 : Protocol-Port Aggregation Record 相当情報 {IPv6} （「表 10-42　Protocol-Port Aggregation Record 相当情報 {IPv6} (Template ID =261)」） 262 : Source Prefix Aggregation Record 相当情報 {IPv4} （「表 10-43　Source Prefix Aggregation Record 相当情報 {IPv4}(Template ID =262)」） 263 : Source Prefix Aggregation Record 相当情報 {IPv6} （「表 10-44　Source Prefix Aggregation Record 相当情報 {IPv6} (Template ID =263)」） 264 : Destination-Prefix Aggregation Record 相当情報 {IPv4} （「表 10-45　Destination Prefix Aggregation Record 相当情報 {IPv4}(Template ID =264)」） 265 : Destination-Prefix Aggregation Record 相当情報 {IPv6} （「表 10-46　Destination Prefix Aggregation Record 相当情報 {IPv6} (Template ID =265)」） 266 : Prefix Aggregation Record 相当情報 {IPv4} （「表 10-47　Prefix Aggregation Record 相当情報 {IPv4}(Template ID =266)」） 267 : Prefix Aggregation Record 相当情報 {IPv6} （「表 10-48　Prefix Aggregation Record 相当情報 {IPv6} (Template ID =267)」） 268 : AS-ToS Aggregation Record 相当情報 {IPv4} （「表 10-49　AS-ToS Aggregation Record 相当情報 {IPv4}(Template ID =268)」） 269 : AS-ToS Aggregation Record 相当情報 {IPv6} （「表 10-50　AS-ToS Aggregation Record 相当情報 {IPv6} (Template ID =269)」） 270 : Protocol-Port-ToS Aggregation Record 相当情報 {IPv4} （「表 10-51　Protocol-Port-ToS Aggregation Record 相当情報 {IPv4}(Template ID =270)」）	○

収集項目	説明	サポート
	271：Protocol-Port-ToS Aggregation Record 相当情報 {IPv6} （「表 10-52　Protocol-Port-ToS Aggregation Record 相当情報 {IPv6} (Template ID =271)」） 272：Source Prefix-ToS Aggregation Record 相当情報 {IPv4} （「表 10-53　Source Prefix-ToS Aggregation Record 相当情報 {IPv4}(Template ID =272)」） 273：Source Prefix-ToS Aggregation Record 相当情報 {IPv6} （「表 10-54　Source Prefix-ToS Aggregation Record 相当情報 {IPv6} (Template ID =273)」） 274：Destination-Prefix-ToS Aggregation Record 相当情報 {IPv4} （「表 10-55　Destination Prefix-ToS Aggregation Record 相当情報 {IPv4}(Template ID =274)」） 275：Destination-Prefix-ToS Aggregation Record 相当情報 {IPv6} （「表 10-56　Destination-Prefix-ToS Aggregation Record 相当情報 {IPv6} (Template ID =275)」） 276：Prefix-ToS Aggregation Record 相当情報 {IPv4} （「表 10-57　Prefix-ToS Aggregation Record 相当情報 {IPv4}(Template ID =276)」） 277：Prefix-ToS Aggregation Record 相当情報 {IPv6} （「表 10-58　Prefix-ToS Aggregation Record 相当情報 {IPv6} (Template ID =277)」） 278：Prefix-Port Aggregation Record 相当情報 {IPv4} （「表 10-59　Prefix-Port Aggregation Record 相当情報 {IPv4}(Template ID =278)」） 279：Prefix-Port Aggregation Record 相当情報 {IPv6} （「表 10-60　Prefix-Port Aggregation Record 相当情報 {IPv6} (Template ID =279)」） 280：BGP-Nexthop-Tos Aggregation Record 相当情報 {IPv4} （「表 10-61　BGP-Nexthop-Tos Aggregation Record 相当情報 {IPv4}(Template ID =280)」） 281：BGP-Nexthop-Tos Aggregation Record 相当情報 {IPv6} （「表 10-62　BGP-Nexthop-Tos Aggregation Record 相当情報 {IPv6} (Template ID =281)」）	
Field Count	Template に格納するフィールド数	○
Field Type	Template のフィールドのタイプ。 (FieldType の一覧は「表 10-36　NetFlow Version 9 FieldType 一覧」を参照してください)	○
Field Length	Template のフィールドの長さ。 (本装置で扱う長さは「表 10-36　NetFlow Version 9 FieldType 一覧」を参照してください)	○
PAD	Length が 4 の倍数になるように設定する。 (値は 0)	○

(凡例)　○：サポートする

表 10-36　NetFlow Version 9 FieldType 一覧

フィールド名	タイプ	サイズ (バイト)	説明	サポート
IN_BYTES	1	n <4>	パケット受信時のフローの L3 パケット総バイト数。	○
IN_PKTS	2	n <4>	パケット受信時のフローの L3 パケット総数。	○

フィールド名	タイプ	サイズ（バイト）	説明	サポート
FLOWS	3	n <4>	集約したフロー数。	○
PROTOCOL	4	1	上位プロトコル。（例）6=TCP, 17=UDP	○
SRC_TOS	5	1	パケット受信時の IP TOS。	○
TCP_FLAGS	6	1	TCP フラグの累積。	○
L4_SRC_PORT	7	2	TCP/UDP 送信元ポート。	○
IPV4_SRC_ADDR	8	4	送信元 IPv4 アドレス。	○
SRC_MASK	9	1	送信元 IPv4 アドレスのプレフィックスマスクビット数。（例：/24）	○
INPUT_SNMP	10	n <2>	受信インタフェースの SNMP Interface Index。	○※2
L4_DST_PORT	11	2	TCP/UDP 宛先ポート。	○
IPV4_DST_ADDR	12	4	宛先 IPv4 アドレス。	○
DST_MASK	13	1	宛先 IPv4 アドレスのプレフィックスマスクビット数。（例：/24）	○
OUTPUT_SNMP	14	n <2>	送信インタフェースの SNMP Interface Index。	○※3 ※4
IPV4_NEXT_HOP	15	4	次の転送先ルータの IPv4 アドレス	○※1
SRC_AS	16	n <2>	送信元／送信元側隣接ピア何れかの AS 番号。	○※1
DST_AS	17	n <2>	宛先／宛先側隣接ピア何れかの AS 番号。	○※1
BGP_IPV4_NEXT_HOP	18	4	次 BGP ドメイン内ルータの IPv4 アドレス	○※1
MUL_DST_PKTS	19	n	IP マルチキャストパケット送信時のフローの L3 パケット総数。	×
MUL_DST_BYTES	20	n	IP マルチキャストパケット送信時のフローの L3 パケット総バイト数。	×
LAST_SWITCHED	21	4	フロー最終パケット受信時の SysUptime[秒]。	○
FIRST_SWITCHED	22	4	フロー開始パケット受信時の SysUptime[秒]。	○
(reserved)	23	-	-	-
OUT_PKTS	24	n	パケット送信時のフローの L3 パケット総数。	×
OUT_BYTES	25	n	パケット送信時のフローの L3 パケット総バイト数。	×
(reserved)	26	-	-	-
IPV6_SRC_ADDR	27	16	送信元 IPv6 アドレス。	○
IPV6_DST_ADDR	28	16	宛先 IPv6 アドレス。	○
IPV6_SRC_MASK	29	1	送信元 IPv6 アドレスのプレフィックスマスクビット数。（例：/64）	○

フィールド名	タイプ	サイズ (バイト)	説明	サポート
IPV6_DST_MASK	30	1	宛先 IPv6 アドレスのプレフィックスマスクビット数。(例 : /64)	○
IPV6_FLOW_LABEL	31	3	IPv6 フローラベル (RFC 2460)。	○
ICMP_TYPE	32	2	ICMP パケットタイプ ((ICMP Type* 256) + ICMP code)。	×
MUL_IGMP_TYPE	33	1	IGMP パケットタイプ。	×
SAMPLING_INTERVAL	34	4	サンプリング間隔。	○
SAMPLING_ALGORITHM	35	1	サンプリングアルゴリズム。 0x01 : パケット間隔方式 0x02 : 閾値乱数方式	○
FLOW_ACTIVE_TIMEOUT	36	2	Active 状態継続中のフローを定期的に Expire するインターバル時間 [秒]。	○
FLOW_INACTIVE_TIMEOUT	37	2	Active 状態でなくなったと判断するための，当該フローの無通信状態時間 [秒]。	○
ENGINE_TYPE	38	1	フロー中継エンジンの種別。	0 固定
ENGINE_ID	39	1	フロー中継エンジンの ID 番号。	0 固定
TOTAL_BYTES_EXP	40	n	送信した datagram の総バイト数。	×
TOTAL_EXP_PKTS_SENT	41	n	送信した datagram の総パケット数。	×
TOTAL_FLOWS_EXP	42	n	送信した datagram の総フロー数。	×
(reserved)	43	-	-	-
IPV4_SRC_PREFIX	44	4	集約した送信元 IPv4 アドレスのプレフィックス	○
IPV4_DST_PREFIX	45	4	集約した宛先 IPv4 アドレスのプレフィックス	○
MPLS_TOP_LABEL_TYPE	46	1	先頭 MPLS ラベルのタイプ。	×
MPLS_TOP_LABEL_IP_ADDR	47	4	MPLSTopLabel に対応する IPv4 アドレス。	×
FLOW_SAMPLER_ID	48	1	flow-sampler の ID。	×
FLOW_SAMPLER_MODE	49	1	サンプリングアルゴリズム (0x02: random sampling)。	×
FLOW_SAMPLER_RANDOM_INTERVAL	50	4	パケットサンプリング間隔。	×
(reserved)	51 ～ 54	-	-	-
DST_TOS	55	1	パケット送信時の IP TOS。	×
IN_SRC_MAC	56	6	受信時の送信元 MAC アドレス	×
OUT_DST_MAC	57	6	送信時の宛先 MAC アドレス	×
SRC_VLAN	58	2	送信元 VLAN-ID	×
DST_VLAN	59	2	宛先 VLAN-ID	×
IP_PROTOCOL_VERSION	60	1	IP バージョン。 (IPv4=4，IPv6=6)	○
DIRECTION	61	1	フローの方向。 (受信フロー =0，送信フロー =1)	×

フィールド名	タイプ	サイズ (バイト)	説明	サポート
IPV6_NEXT_HOP	62	16	次の転送先ルータの IPv6 アドレス	○※1
BPG_IPV6_NEXT_HOP	63	16	次 BGP ドメイン内ルータの IPv6 アドレス	○※1
IPV6_OPTION_HEADERS	64	4	フローに含まれる IPv6 拡張ヘッダを示すビットマップ。	×
(reserved)	65 ～ 69	-	-	-
MPLS LABEL 1	70	3	1 番目の MPLS ラベル。	×
MPLS LABEL 2	71	3	2 番目の MPLS ラベル。	×
MPLS LABEL 3	72	3	3 番目の MPLS ラベル。	×
MPLS LABEL 4	73	3	4 番目の MPLS ラベル。	×
MPLS LABEL 5	74	3	5 番目の MPLS ラベル。	×
MPLS LABEL 6	75	3	6 番目の MPLS ラベル。	×
MPLS LABEL 7	76	3	7 番目の MPLS ラベル。	×
MPLS LABEL 8	77	3	8 番目の MPLS ラベル。	×
MPLS LABEL 9	78	3	9 番目の MPLS ラベル。	×
MPLS LABEL 10	79	3	10 番目の MPLS ラベル。	×

(凡例) ○：サポートする。 ×：サポートしない。

注 1

< > 内は本装置で扱う FiledType の実装バイト長。

注 2

レイヤ 2 中継パケットはフロー集約統計の対象にはなりません。

注※ 1

レイヤ 2 中継の場合，Data FlowSet の内容としては 0 が入ります。

注※ 2

物理ポートの SNMP Index 値を設定。

注※ 3

優先順位は物理ポートの SNMP Index 値より論理ポートの SNMP Index 値 (VLAN> リンクアグリゲーション) の方が高くなります。

注※ 4

エントリ作成時点の送信インタフェースが設定されます。もし，タイムアウト (Active/InActive) 経過前に変更になった場合は正しく通知されない可能性があります。

表 10-37 Version 5 相当情報 {IPv4} (Template ID =256)

収集項目	説明	サポート
Template ID	Template の ID 番号 (IPv4 パケット用 Version 5 相当情報 {IPv4} =0x0100)	○
Field Count	この Template に格納するフィールド数	○
IPV4_SRC_ADDR	送信元 IPv4 アドレス	○
IPV4_DST_ADDR	宛先 IPv4 アドレス	○
IPV4_NEXT_HOP	次の転送先ルータの IPv4 アドレス	○

収集項目	説明	サポート
INPUT_SNMP	受信インタフェースの SNMP Interface Index	○
OUTPUT_SNMP	送信インタフェースの SNMP Interface Index	○
IN_PKTS	フローのパケットの総数	○
IN_BYTES	フローのパケットの総バイト数	○
FIRST_SWITCHED	フロー開始パケット受信時の SysUptime[秒]	○
LAST_SWITCHED	フロー最終パケット受信時の SysUptime[秒]	○
L4_SRC_PORT	TCP/UDP 送信元ポート番号	○
L4_DST_PORT	TCP/UDP 宛先ポート番号	○
SRC_AS	送信元もしくは送信元側隣接ピアの AS 番号	○
DST_AS	宛先もしくは宛先側隣接ピアの AS 番号	○
SRC_MASK	送信元 IPv4 アドレスのプレフィックスマスクビット数	○
DST_MASK	宛先 IPv4 アドレスのプレフィックスマスクビット数	○
TCP_FLAGS	TCP フラグの累積	○
PROTOCOL	IP プロトコルタイプ	○
SRC_TOS	IP のタイプオブサービス	○

(凡例)　○：サポートする

表 10-38　Version 5 相当情報 {IPv6} (Template ID =257)

収集項目	説明	サポート
Template ID	Template の ID 番号 (IPv6 パケット用 Version 5 相当情報 {IPv6} =0x0101)	○
Field Count	この Template に格納するフィールド数 (0x0013)	○
IPV6_SRC_ADDR	送信元 IPv6 アドレス	○
IPV6_DST_ADDR	宛先 IPv6 アドレス	○
IPV6_NEXT_HOP	次の転送先ルータの IPv6 アドレス	○
INPUT_SNMP	受信インタフェースの SNMP Interface Index	○
OUTPUT_SNMP	送信インタフェースの SNMP Interface Index	○
IN_PKTS	フローのパケットの総数	○
IN_BYTES	フローのパケットの総バイト数	○
FIRST_SWITCHED	フロー開始パケット受信時の SysUptime[秒]	○
LAST_SWITCHED	フロー最終パケット受信時の SysUptime[秒]	○
L4_SRC_PORT	TCP/UDP 送信元ポート番号	○
L4_DST_PORT	TCP/UDP 宛先ポート番号	○
SRC_AS	送信元もしくは送信元側隣接ピアの AS 番号	○
DST_AS	宛先もしくは宛先側隣接ピアの AS 番号	○
IPv6_SRC_MASK	送信元 IPv6 アドレスのプレフィックスマスクビット数	○
IPv6_DST_MASK	宛先 IPv6 アドレスのプレフィックスマスクビット数	○
TCP_FLAGS	TCP フラグの累積	○

収集項目	説明	サポート
PROTOCOL	IP プロトコルタイプ	○
SRC_TOS	IP のタイプオブサービス	○
IP_PROTOCOL_VERSION	プロトコルバージョン	○

(凡例) ○：サポートする

表 10-39 AS Aggregation Record 相当情報 {IPv4}(Template ID =258)

収集項目	説明	サポート
Template ID	Template の ID 番号。 (AS Aggregation Record 相当情報 {IPv4} =0x0102)	○
Field Count	この Template に格納するフィールド数 (0x0009)	○
FLOWS	集約したフロー数	○
IN_PKTS	集約したフローに含まれる総パケット数	○
IN_BYTES	集約したフローに含まれるパケットの総バイト数	○
FIRST_SWITCHED	フロー開始パケット受信時の SysUptime[秒]	○
LAST_SWITCHED	フロー最終パケット受信時の SysUptime[秒]	○
INPUT_SNMP	受信インタフェースの SNMP Interface Index	○
OUTPUT_SNMP	送信インタフェースの SNMP Interface Index	○
SRC_AS	送信元もしくは送信元側隣接ピアの AS 番号	○
DST_AS	宛先もしくは宛先側隣接ピアの AS 番号	○

(凡例) ○：サポートする

表 10-40 AS Aggregation Record 相当情報 {IPv6}(Template ID =259)

収集項目	説明	サポート
Template ID	Template の ID 番号。 (AS Aggregation Record 相当情報 {IPv6} =0x0103)	○
Field Count	この Template に格納するフィールド数 (0x000a)	○
FLOWS	集約したフロー数	○
IN_PKTS	集約したフローに含まれる総パケット数	○
IN_BYTES	集約したフローに含まれるパケットの総バイト数	○
FIRST_SWITCHED	フロー開始パケット受信時の SysUptime[秒]	○
LAST_SWITCHED	フロー最終パケット受信時の SysUptime[秒]	○
INPUT_SNMP	受信インタフェースの SNMP Interface Index	○
OUTPUT_SNMP	送信インタフェースの SNMP Interface Index	○
SRC_AS	送信元もしくは送信元側隣接ピアの AS 番号	○
DST_AS	宛先もしくは宛先側隣接ピアの AS 番号	○
IP_PROTOCOL_VERSION	プロトコルバージョン	○

(凡例) ○：サポートする

表 10-41　Protocol-Port Aggregation Record 相当情報 {IPv4}(Template ID =260)

収集項目	説明	サポート
Template ID	Template の ID 番号 (Protocol-Port Aggregation Record 相当情報 {IPv4} =0x0104)	○
Field Count	この Template に格納するフィールド数 (0x0008)	○
FLOWS	集約したフロー数	○
IN_PKTS	集約したフローに含まれる総パケット数	○
IN_BYTES	集約したフローに含まれるパケットの総バイト数	○
FIRST_SWITCHED	フロー開始パケット受信時の SysUptime[秒]	○
LAST_SWITCHED	フロー最終パケット受信時の SysUptime[秒]	○
L4_SRC_PORT	TCP/UDP 送信元ポート番号	○
L4_DST_PORT	TCP/UDP 宛先ポート番号	○
PROTOCOL	IP プロトコルタイプ	○

(凡例)　○ : サポートする

表 10-42　Protocol-Port Aggregation Record 相当情報 {IPv6} (Template ID =261)

収集項目	説明	サポート
Template ID	Template の ID 番号 (Protocol-Port Aggregation Record 相当情報 {IPv6} =0x0105)	○
Field Count	この Template に格納するフィールド数 (0x0009)	○
FLOWS	集約したフロー数	○
IN_PKTS	集約したフローに含まれる総パケット数	○
IN_BYTES	集約したフローに含まれるパケットの総バイト数	○
FIRST_SWITCHED	フロー開始パケット受信時の SysUptime[秒]	○
LAST_SWITCHED	フロー最終パケット受信時の SysUptime[秒]	○
L4_SRC_PORT	TCP/UDP 送信元ポート番号	○
L4_DST_PORT	TCP/UDP 宛先ポート番号	○
PROTOCOL	IP プロトコルタイプ	○
IP_PROTOCOL_VERSION	プロトコルバージョン	○

(凡例)　○ : サポートする

表 10-43　Source Prefix Aggregation Record 相当情報 {IPv4}(Template ID =262)

収集項目	説明	サポート
Template ID	Template の ID 番号 (Source Prefix Aggregation Record 相当情報 {IPv4} =0x0106)	○
Field Count	この Template に格納するフィールド数 (0x0008)	○
FLOWS	集約したフロー数	○
IN_PKTS	集約したフローに含まれる総パケット数	○
IN_BYTES	集約したフローに含まれるパケットの総バイト数	○
FIRST_SWITCHED	フロー開始パケット受信時の SysUptime[秒]	○

収集項目	説明	サポート
LAST_SWITCHED	フロー最終パケット受信時の SysUptime[秒]	○
IPV4_SRC_PREFIX	集約した送信元 IPv4 アドレスのプレフィックス	○
INPUT_SNMP	受信インタフェースの SNMP Interface Index	○
SRC_AS	送信元もしくは送信元側隣接ピアの AS 番号	○
SRC_MASK	集約した送信元 IPv4 アドレスのプレフィックスビット数	○

(凡例) ○ : サポートする

表 10-44 Source Prefix Aggregation Record 相当情報 {IPv6} (Template ID =263)

収集項目	説明	サポート
Template ID	Template の ID 番号 (Source Prefix Aggregation Record 相当情報 {IPv6} =0x0107)	○
Field Count	この Template に格納するフィールド数 (0x0009)	○
FLOWS	集約したフロー数	○
IN_PKTS	集約したフローに含まれる総パケット数	○
IN_BYTES	集約したフローに含まれるパケットの総バイト数	○
FIRST_SWITCHED	フロー開始パケット受信時の SysUptime[秒]	○
LAST_SWITCHED	フロー最終パケット受信時の SysUptime[秒]	○
IPV6_SRC_ADDR	集約した送信元 IPv6 アドレスのプレフィックス	○
INPUT_SNMP	受信インタフェースの SNMP Interface Index	○
SRC_AS	送信元もしくは送信元側隣接ピアの AS 番号	○
IPv6_SRC_MASK	集約した送信元 IPv6 アドレスのプレフィックスビット数	○
IP_PROTOCOL_VERSION	プロトコルバージョン	○

(凡例) ○ : サポートする

表 10-45 Destination Prefix Aggregation Record 相当情報 {IPv4}(Template ID =264)

収集項目	説明	サポート
Template ID	Template の ID 番号 (Destination Prefix Aggregation Record 相当情報 {IPv4} =0x0108)	○
Field Count	この Template に格納するフィールド数 (0x0009)	○
FLOWS	集約したフロー数	○
IN_PKTS	集約したフローに含まれる総パケット数	○
IN_BYTES	集約したフローに含まれるパケットの総バイト数	○
FIRST_SWITCHED	フロー開始パケット受信時の SysUptime[秒]	○
LAST_SWITCHED	フロー最終パケット受信時の SysUptime[秒]	○
IPV4_DST_PREFIX	集約した宛先 IPv4 アドレスのプレフィックス	○
OUTPUT_SNMP	送信インタフェースの SNMP Interface Index	○
DST_AS	宛先もしくは宛先側隣接ピアの AS 番号	○
DST_MASK	集約した宛先 IPv4 アドレスのプレフィックスビット数	○

(凡例)　○：サポートする

表 10-46　Destination Prefix Aggregation Record 相当情報 {IPv6} (Template ID =265)

収集項目	説明	サポート
Template ID	Template の ID 番号 (Destination Prefix Aggregation Record 相当情報 {IPv6} =0x0109)	○
Field Count	この Template に格納するフィールド数 (0x000a)	○
FLOWS	集約したフロー数	○
IN_PKTS	集約したフローに含まれる総パケット数	○
IN_BYTES	集約したフローに含まれるパケットの総バイト数	○
FIRST_SWITCHED	フロー開始パケット受信時の SysUptime[秒]	○
LAST_SWITCHED	フロー最終パケット受信時の SysUptime[秒]	○
IPV6_DST_ADDR	集約した宛先 IPv6 アドレスのプレフィックス	○
OUTPUT_SNMP	送信インタフェースの SNMP Interface Index	○
DST_AS	宛先もしくは宛先側隣接ピアの AS 番号	○
IPv6_DST_MASK	集約した宛先 IPv6 アドレスのプレフィックスビット数	○
IP_PROTOCOL_VERSION	プロトコルバージョン	○

(凡例)　○：サポートする

表 10-47　Prefix Aggregation Record 相当情報 {IPv4}(Template ID =266)

収集項目	説明	サポート
Template ID	Template の ID 番号 (Prefix Aggregation Record 相当情報 {IPv4} =0x010a)	○
Field Count	この Template に格納するフィールド数 (0x000d)	○
FLOWS	集約したフロー数	○
IN_PKTS	集約したフローに含まれる総パケット数	○
IN_BYTES	集約したフローに含まれるパケットの総バイト数	○
FIRST_SWITCHED	フロー開始パケット受信時の SysUptime[秒]	○
LAST_SWITCHED	フロー最終パケット受信時の SysUptime[秒]	○
IPV4_SRC_PREFIX	集約した送信元 IPv4 アドレスのプレフィックス	○
IPV4_DST_PREFIX	集約した宛先 IPv4 アドレスのプレフィックス	○
INPUT_SNMP	受信インタフェースの SNMP Interface Index	○
OUTPUT_SNMP	送信インタフェースの SNMP Interface Index	○
SRC_AS	送信元もしくは送信元側隣接ピアの AS 番号	○
DST_AS	宛先もしくは宛先側隣接ピアの AS 番号	○
SRC_MASK	送信元 IPv4 アドレスのプレフィックスマスクビット数	○
DST_MASK	宛先 IPv4 アドレスのプレフィックスマスクビット数	○

(凡例)　○：サポートする

表 10-48 Prefix Aggregation Record 相当情報 {IPv6} (Template ID =267)

収集項目	説明	サポート
Template ID	Template の ID 番号 (Prefix Aggregation Record 相当情報 {IPv6} =0x010b)	○
Field Count	この Template に格納するフィールド数 (0x000e)	○
FLOWS	集約したフロー数	○
IN_PKTS	集約したフローに含まれる総パケット数	○
IN_BYTES	集約したフローに含まれるパケットの総バイト数	○
FIRST_SWITCHED	フロー開始パケット受信時の SysUptime[秒]	○
LAST_SWITCHED	フロー最終パケット受信時の SysUptime[秒]	○
IPV6_SRC_ADDR	集約した送信元 IPv6 アドレスのプレフィックス	○
IPV6_DST_ADDR	集約した宛先 IPv6 アドレスのプレフィックス	○
INPUT_SNMP	受信インタフェースの SNMP Interface Index	○
OUTPUT_SNMP	送信インタフェースの SNMP Interface Index	○
SRC_AS	送信元もしくは送信元側隣接ピアの AS 番号	○
DST_AS	宛先もしくは宛先側隣接ピアの AS 番号	○
IPv6_SRC_MASK	送信元 IPv6 アドレスのプレフィックスマスクビット数	○
IPv6_DST_MASK	宛先 IPv6 アドレスのプレフィックスマスクビット数	○
IP_PROTOCOL_VERSION	プロトコルバージョン	○

(凡例) ○ : サポートする

表 10-49 AS-ToS Aggregation Record 相当情報 {IPv4}(Template ID =268)

収集項目	説明	サポート
Template ID	Template の ID 番号 (AS-ToS Aggregation Record 相当情報 {IPv4} =0x010c)	○
Field Count	この Template に格納するフィールド数 (0x000a)	○
FLOWS	集約したフロー数	○
IN_PKTS	集約したフローに含まれる総パケット数	○
IN_BYTES	集約したフローに含まれるパケットの総バイト数	○
FIRST_SWITCHED	フロー開始パケット受信時の SysUptime[秒]	○
LAST_SWITCHED	フロー最終パケット受信時の SysUptime[秒]	○
INPUT_SNMP	受信インタフェースの SNMP Interface Index	○
OUTPUT_SNMP	送信インタフェースの SNMP Interface Index	○
SRC_AS	送信元もしくは送信元側隣接ピアの AS 番号	○
DST_AS	宛先もしくは宛先側隣接ピアの AS 番号	○
SRC_TOS	IP のタイプオブサービス	○

(凡例) ○ : サポートする

表 10-50　AS-ToS Aggregation Record 相当情報 {IPv6} (Template ID =269)

収集項目	説明	サポート
Template ID	Template の ID 番号 (AS-ToS Aggregation Record 相当情報 {IPv6} =0x010d)	○
Field Count	この Template に格納するフィールド数 (0x000b)	○
FLOWS	集約したフロー数	○
IN_PKTS	集約したフローに含まれる総パケット数	○
IN_BYTES	集約したフローに含まれるパケットの総バイト数	○
FIRST_SWITCHED	フロー開始パケット受信時の SysUptime[秒]	○
LAST_SWITCHED	フロー最終パケット受信時の SysUptime[秒]	○
INPUT_SNMP	受信インタフェースの SNMP Interface Index	○
OUTPUT_SNMP	送信インタフェースの SNMP Interface Index	○
SRC_AS	送信元もしくは送信元側隣接ピアの AS 番号	○
DST_AS	宛先もしくは宛先側隣接ピアの AS 番号	○
SRC_TOS	IP のタイプオブサービス	○
IP_PROTOCOL_VERSION	プロトコルバージョン	○

(凡例)　○ : サポートする

表 10-51　Protocol-Port-ToS Aggregation Record 相当情報 {IPv4}(Template ID =270)

収集項目	説明	サポート
Template ID	Template の ID 番号 (Protocol-Port-ToS Aggregation Record 相当情報 {IPv4} =0x010e)	○
Field Count	この Template に格納するフィールド数 (0x000b)	○
FLOWS	集約したフロー数	○
IN_PKTS	集約したフローに含まれる総パケット数	○
IN_BYTES	集約したフローに含まれるパケットの総バイト数	○
FIRST_SWITCHED	フロー開始パケット受信時の SysUptime[秒]	○
LAST_SWITCHED	フロー最終パケット受信時の SysUptime[秒]	○
INPUT_SNMP	受信インタフェースの SNMP Interface Index	○
OUTPUT_SNMP	送信インタフェースの SNMP Interface Index	○
L4_SRC_PORT	TCP/UDP 送信元ポート番号	○
L4_DST_PORT	TCP/UDP 宛先ポート番号	○
PROTOCOL	IP プロトコルタイプ	○
SRC_TOS	IP のタイプオブサービス	○

(凡例)　○ : サポートする

表 10-52 Protocol-Port-ToS Aggregation Record 相当情報 {IPv6} (Template ID =271)

収集項目	説明	サポート
Template ID	Template の ID 番号 (Protocol-Port-ToS Aggregation Record 相当情報 {IPv6} =0x010f)	○
Field Count	この Template に格納するフィールド数 (0x000c)	○
FLOWS	集約したフロー数	○
IN_PKTS	集約したフローに含まれる総パケット数	○
IN_BYTES	集約したフローに含まれるパケットの総バイト数	○
FIRST_SWITCHED	フロー開始パケット受信時の SysUptime[秒]	○
LAST_SWITCHED	フロー最終パケット受信時の SysUptime[秒]	○
INPUT_SNMP	受信インタフェースの SNMP Interface Index	○
OUTPUT_SNMP	送信インタフェースの SNMP Interface Index	○
L4_SRC_PORT	TCP/UDP 送信元ポート番号	○
L4_DST_PORT	TCP/UDP 宛先ポート番号	○
PROTOCOL	IP プロトコルタイプ	○
SRC_TOS	IP のタイプオブサービス	○
IP_PROTOCOL_VERSION	プロトコルバージョン	○

(凡例) ○：サポートする

表 10-53 Source Prefix-ToS Aggregation Record 相当情報 {IPv4}(Template ID =272)

収集項目	説明	サポート
Template ID	Template の ID 番号 (Source Prefix-ToS Aggregation Record 相当情報 {IPv4} =0x0110)	○
Field Count	この Template に格納するフィールド数 (0x000a)	○
FLOWS	集約したフロー数	○
IN_PKTS	集約したフローに含まれる総パケット数	○
IN_BYTES	集約したフローに含まれるパケットの総バイト数	○
FIRST_SWITCHED	フロー開始パケット受信時の SysUptime[秒]	○
LAST_SWITCHED	フロー最終パケット受信時の SysUptime[秒]	○
IPV4_SRC_PREFIX	集約した送信元 IPv4 アドレスのプレフィックス	○
INPUT_SNMP	受信インタフェースの SNMP Interface Index	○
SRC_AS	送信元もしくは送信元側隣接ピアの AS 番号	○
SRC_MASK	送信元 IPv4 アドレスのプレフィックスマスクビット数	○
SRC_TOS	IP のタイプオブサービス	○

(凡例) ○：サポートする

表 10-54　Source Prefix-ToS Aggregation Record 相当情報 {IPv6} (Template ID =273)

収集項目	説明	サポート
Template ID	Template の ID 番号 (Source Prefix-ToS Aggregation Record 相当情報 {IPv6} =0x0111)	○
Field Count	この Template に格納するフィールド数 (0x000b)	○
FLOWS	集約したフロー数	○
IN_PKTS	集約したフローに含まれる総パケット数	○
IN_BYTES	集約したフローに含まれるパケットの総バイト数	○
FIRST_SWITCHED	フロー開始パケット受信時の SysUptime[秒]	○
LAST_SWITCHED	フロー最終パケット受信時の SysUptime[秒]	○
IPV6_SRC_ADDR	集約した送信元 IPv6 アドレスのプレフィックス	○
INPUT_SNMP	受信インタフェースの SNMP Interface Index	○
SRC_AS	送信元もしくは送信元側隣接ピアの AS 番号	○
IPV6_SRC_MASK	送信元 IPv6 アドレスのプレフィックスマスクビット数	○
SRC_TOS	IP のタイプオブサービス	○
IP_PROTOCOL_VERSION	プロトコルバージョン	○

(凡例)　○ : サポートする

表 10-55　Destination Prefix-ToS Aggregation Record 相当情報 {IPv4}(Template ID =274)

収集項目	説明	サポート
Template ID	Template の ID 番号 (Destination Prefix-ToS Aggregation Record 相当情報 {IPv4} =0x0112)	○
Field Count	この Template に格納するフィールド数 (0x000a)	○
FLOWS	集約したフロー数	○
IN_PKTS	集約したフローに含まれる総パケット数	○
IN_BYTES	集約したフローに含まれるパケットの総バイト数	○
FIRST_SWITCHED	フロー開始パケット受信時の SysUptime[秒]	○
LAST_SWITCHED	フロー最終パケット受信時の SysUptime[秒]	○
IPV4_DST_PREFIX	集約した宛先 IPv4 アドレスのプレフィックス	○
OUTPUT_SNMP	送信インタフェースの SNMP Interface Index	○
DST_AS	宛先もしくは宛先側隣接ピアの AS 番号	○
DST_MASK	宛先 IPv4 アドレスのプレフィックスマスクビット数	○
SRC_TOS	IP のタイプオブサービス	○

(凡例)　○ : サポートする

表 10-56 Destination-Prefix-ToS Aggregation Record 相当情報 {IPv6} (Template ID =275)

収集項目	説明	サポート
Template ID	Template の ID 番号 (Destination-Prefix-ToS Aggregation Record 相当情報 {IPv6} =0x0113)	○
Field Count	この Template に格納するフィールド数 (0x000b)	○
FLOWS	集約したフロー数	○
IN_PKTS	集約したフローに含まれる総パケット数	○
IN_BYTES	集約したフローに含まれるパケットの総バイト数	○
FIRST_SWITCHED	フロー開始パケット受信時の SysUptime[秒]	○
LAST_SWITCHED	フロー最終パケット受信時の SysUptime[秒]	○
IPV6_DST_ADDR	集約した宛先 IPv6 アドレスのプレフィックス	○
OUTPUT_SNMP	送信インタフェースの SNMP Interface Index	○
DST_AS	宛先もしくは宛先側隣接ピアの AS 番号	○
IPV6_DST_MASK	宛先 IPv6 アドレスのプレフィックスマスクビット数	○
SRC_TOS	IP のタイプオブサービス	○
IP_PROTOCOL_VERSION	プロトコルバージョン	○

(凡例) ○ : サポートする

表 10-57 Prefix-ToS Aggregation Record 相当情報 {IPv4}(Template ID =276)

収集項目	説明	サポート
Template ID	Template の ID 番号 (Prefix-ToS Aggregation Record 相当情報 {IPv4} =0x0114)	○
Field Count	この Template に格納するフィールド数 (0x000e)	○
FLOWS	集約したフロー数	○
IN_PKTS	集約したフローに含まれる総パケット数	○
IN_BYTES	集約したフローに含まれるパケットの総バイト数	○
FIRST_SWITCHED	フロー開始パケット受信時の SysUptime[秒]	○
LAST_SWITCHED	フロー最終パケット受信時の SysUptime[秒]	○
IPV4_SRC_PREFIX	集約した送信元 IPv4 アドレスのプレフィックス	○
IPV4_DST_PREFIX	集約した宛先 IPv4 アドレスのプレフィックス	○
INPUT_SNMP	受信インタフェースの SNMP Interface Index	○
OUTPUT_SNMP	送信インタフェースの SNMP Interface Index	○
SRC_AS	送信元もしくは送信元側隣接ピアの AS 番号	○
DST_AS	宛先もしくは宛先側隣接ピアの AS 番号	○
SRC_MASK	送信元 IPv4 アドレスのプレフィックスマスクビット数	○
DST_MASK	宛先 IPv4 アドレスのプレフィックスマスクビット数	○
SRC_TOS	IP のタイプオブサービス	○

(凡例) ○ : サポートする

表 10-58　Prefix-ToS Aggregation Record 相当情報 {IPv6} (Template ID =277)

収集項目	説明	サポート
Template ID	Template の ID 番号 (Prefix-ToS Aggregation Record 相当情報 {IPv6} =0x0115)	○
Field Count	この Template に格納するフィールド数 (0x000f)	○
FLOWS	集約したフロー数	○
IN_PKTS	集約したフローに含まれる総パケット数	○
IN_BYTES	集約したフローに含まれるパケットの総バイト数	○
FIRST_SWITCHED	フロー開始パケット受信時の SysUptime[秒]	○
LAST_SWITCHED	フロー最終パケット受信時の SysUptime[秒]	○
IPV6_SRC_ADDR	集約した送信元 IPv6 アドレスのプレフィックス	○
IPV6_DST_ADDR	集約した宛先 IPv6 アドレスのプレフィックス	○
INPUT_SNMP	受信インタフェースの SNMP Interface Index	○
OUTPUT_SNMP	送信インタフェースの SNMP Interface Index	○
SRC_AS	送信元もしくは送信元側隣接ピアの AS 番号	○
DST_AS	宛先もしくは宛先側隣接ピアの AS 番号	○
SRC_TOS	IP のタイプオブサービス	○
IPV6_SRC_MASK	送信元 IPv6 アドレスのプレフィックスマスクビット数	○
IPV6_DST_MASK	宛先 IPv6 アドレスのプレフィックスマスクビット数	○
IP_PROTOCOL_VERSION	プロトコルバージョン	○

(凡例)　○：サポートする

表 10-59　Prefix-Port Aggregation Record 相当情報 {IPv4}(Template ID =278)

収集項目	説明	サポート
Template ID	Template の ID 番号 (Prefix-Port Aggregation Record 相当情報 {IPv4} =0x0116)	○
Field Count	この Template に格納するフィールド数 (0x000f)	○
FLOWS	集約したフロー数	○
IN_PKTS	集約したフローに含まれる総パケット数	○
IN_BYTES	集約したフローに含まれるパケットの総バイト数	○
FIRST_SWITCHED	フロー開始パケット受信時の SysUptime[秒]	○
LAST_SWITCHED	フロー最終パケット受信時の SysUptime[秒]	○
IPV4_SRC_PREFIX	集約した送信元 IPv4 アドレスのプレフィックス	○
IPV4_DST_PREFIX	集約した宛先 IPv4 アドレスのプレフィックス	○
INPUT_SNMP	受信インタフェースの SNMP Interface Index	○
OUTPUT_SNMP	送信インタフェースの SNMP Interface Index	○
L4_SRC_PORT	TCP/UDP 送信元ポート番号	○
L4_DST_PORT	TCP/UDP 宛先ポート番号	○
PROTOCOL	IP プロトコルタイプ	○
SRC_MASK	送信元 IPv4 アドレスのプレフィックスマスクビット数	○

収集項目	説明	サポート
DST_MASK	宛先 IPv4 アドレスのプレフィックスマスクビット数	○
SRC_TOS	IP のタイプオブサービス	○

(凡例) ○：サポートする

表 10-60 Prefix-Port Aggregation Record 相当情報 {IPv6} (Template ID =279)

収集項目	説明	サポート
Template ID	Template の ID 番号 (Prefix-Port Aggregation Record 相当情報 {IPv6} =0x0117)	○
Field Count	この Template に格納するフィールド数 (0x0010)	○
FLOWS	集約したフロー数	○
IN_PKTS	集約したフローに含まれる総パケット数	○
IN_BYTES	集約したフローに含まれるパケットの総バイト数	○
FIRST_SWITCHED	フロー開始パケット受信時の SysUptime[秒]	○
LAST_SWITCHED	フロー最終パケット受信時の SysUptime[秒]	○
IPV6_SRC_ADDR	集約した送信元 IPv6 アドレスのプレフィックス	○
IPV6_DST_ADDR	集約した宛先 IPv6 アドレスのプレフィックス	○
INPUT_SNMP	受信インタフェースの SNMP Interface Index	○
OUTPUT_SNMP	送信インタフェースの SNMP Interface Index	○
L4_SRC_PORT	TCP/UDP 送信元ポート番号	○
L4_DST_PORT	TCP/UDP 宛先ポート番号	○
SRC_TOS	IP のタイプオブサービス	○
PROTOCOL	IP プロトコルタイプ	○
IPV6_SRC_MASK	送信元 IPv6 アドレスのプレフィックスマスクビット数	○
IPV6_DST_MASK	宛先 IPv6 アドレスのプレフィックスマスクビット数	○
IP_PROTOCOL_VERSION	プロトコルバージョン	○

(凡例) ○：サポートする

表 10-61 BGP-Nexthop-Tos Aggregation Record 相当情報 {IPv4}(Template ID =280)

収集項目	説明	サポート
Template ID	Template の ID 番号 (BGP-Nexthop-Tos Aggregation Record 相当情報 {IPv4} =0x0118)	○
Field Count	この Template に格納するフィールド数 (0x000b)	○
FLOWS	集約したフロー数	○
IN_PKTS	集約したフローに含まれる総パケット数	○
IN_BYTES	集約したフローに含まれるパケットの総バイト数	○
FIRST_SWITCHED	フロー開始パケット受信時の SysUptime[秒]	○
LAST_SWITCHED	フロー最終パケット受信時の SysUptime[秒]	○
INPUT_SNMP	受信インタフェースの SNMP Interface Index	○

収集項目	説明	サポート
OUTPUT_SNMP	送信インタフェースの SNMP Interface Index	○
SRC_AS	送信元もしくは送信元側隣接ピアの AS 番号	○
DST_AS	宛先もしくは宛先側隣接ピアの AS 番号	○
BGP_IPV4_NEXT_HOP	次 BGP ドメイン内ルータの IPv4 アドレス	○
SRC_TOS	IP のタイプオブサービス	○

(凡例)　○：サポートする

表 10-62　BGP-Nexthop-Tos Aggregation Record 相当情報 {IPv6} (Template ID =281)

収集項目	説明	サポート
Template ID	Template の ID 番号 (BGP-Nexthop-Tos Aggregation Record 相当情報 {IPv6} =0x0119)	○
Field Count	この Template に格納するフィールド数 (0x000c)	○
FLOWS	集約したフロー数	○
IN_PKTS	集約したフローに含まれる総パケット数	○
IN_BYTES	集約したフローに含まれるパケットの総バイト数	○
FIRST_SWITCHED	フロー開始パケット受信時の SysUptime[秒]	○
LAST_SWITCHED	フロー最終パケット受信時の SysUptime[秒]	○
INPUT_SNMP	受信インタフェースの SNMP Interface Index	○
OUTPUT_SNMP	送信インタフェースの SNMP Interface Index	○
SRC_AS	送信元もしくは送信元側隣接ピアの AS 番号	○
DST_AS	宛先もしくは宛先側隣接ピアの AS 番号	○
BGP_IPV6_NEXT_HOP	次 BGP ドメイン内ルータの IPv6 アドレス	○
SRC_TOS	IP のタイプオブサービス	○
IP_PROTOCOL_VERSION	プロトコルバージョン	○

(凡例)　○：サポートする

(3) Data FlowSet 情報

Template FlowSet 情報で規定したフォーマットに従い，フロー単位統計やフロー集約統計の情報をコレクタ装置に通知します。

表 10-63　Data FlowSet 情報フォーマット

収集項目	説明	サポート
FlowSet ID (Template ID)	Template，DataFlowSet を識別するための番号。「表 10-37 Version 5 相当情報 {IPv4} (Template ID =256)」～「表 10-62 BGP-Nexthop-Tos Aggregation Record 相当情報 {IPv6} (Template ID =281)」で示している Template ID が設定されます。 (DataFlowSet の範囲は 256 ～ 65535)	○
Length	Data FlowSet の長さ (FlowSet ID および Length,PAD も含む)	○

収集項目	説明	サポート
Data FlowSet	Template FlowSet 情報で記述された内容でコレクタ装置に統計情報が通知されます。詳細については「表 10-37 Version 5 相当情報 {IPv4} (Template ID =256)」～「表 10-62 BGP-Nexthop-Tos Aggregation Record 相当情報 {IPv6} (Template ID =281)」を参照してください。	○
PAD	Length が 4 の倍数になるように設定する。 (値は 0)	○

(凡例) ○ : サポートする

（4） OptionTemplate 情報

本装置の NetFlow 統計に関係する情報を報告するフォーマットをコレクタ装置に通知するために使います。

表 10-64 OptionTemplate 情報

収集項目	説明	サポート
FlowSet ID	Template, DataFlowSet を識別するための番号。 (OptionTemplate の場合 =1)	○
Length	OptionTemplate の長さ (FlowSet ID および Length,PAD も含む)	○
Template ID	Template の ID 番号 (OptionTemplate 情報 =0x0200)	○
Option Scope Length	この OptionTemplate に格納する Scope フィールドの長さ (0x0002)	○
Options Length	この OptionTemplate に格納する Options フィールドの長さ (0x0010)	○
Scope Field Type	この OptionTemplate の値が有効となる範囲。 (装置単位 =0x0001)	○
Scope Field Length	Scope Field の有効範囲の長さ (0x0000)	○
FLOW_ACTIVE_TIMEOUT	フロー単位統計のアクティブタイムアウト時間	○※
FLOW_INACTIVE_TIMEOUT	フロー単位統計のインアクティブタイムアウト時間	○※
SAMPLING_INTERVAL	サンプリング間隔	○
SAMPLING_ALGORITHM	サンプリングのアルゴリズム	○
PAD	Length が 4 の倍数になるように設定する。 (値は 0)	○

(凡例) ○ : サポートする
注※ 装置単位で通知しているためフロー単位統計だけ送る。

（5） OptionData 情報

OptionData 情報に記述された形式で装置固有な情報をコレクタ装置に通知します。

OptionData 情報を次の表に示します。

表 10-65　OptionData 情報 (Template ID =512)

収集項目	説明	サポート
FlowSet ID (Template ID)	Template，DataFlowSet を識別するための番号。 (OptionData の場合 =512)	○
Length	OptionData の長さ (FlowSet ID および Length，PAD も含む)	○
OptionData	OptionTemplate 情報で記述された内容でコレクタ装置に統計情報が通知されます。詳細については「表 10-64 OptionTemplate 情報」を参照してください。	○
PAD	Length が 4 の倍数になるように設定する。 (値は 0)	○

(凡例)　○：サポートする

10.2.6　フロー統計エントリ

(1) フロー統計エントリとは

本装置の NetFlow エージェントはフロー単位統計情報やフロー集約統計情報を収集するために，QoS エントリを利用しています。この機能を利用する前に QoS エントリが十分空いていること※を確認してください。以降，フロー単位統計機能として使用する QoS エントリをフロー単位統計エントリと呼び，フロー集約統計で使用している集約用のエントリエリアをフロー集約統計エントリと呼びます。両エントリともを意味する場合はフロー統計エントリと呼びます。以降に各エントリの実装位置を「図 10-17　フロー統計エントリの実装位置【SB-7800S】」「図 10-18　フロー統計エントリの実装位置【SB-5400S】」，状態遷移とその動作条件を「図 10-19　フロー統計エントリの状態遷移図」に示します。

注※

目安となるエントリ数は「(2) フロー統計エントリとコンフィグレーションの関係」を参照してください。

図 10-17　フロー統計エントリの実装位置【SB-7800S】

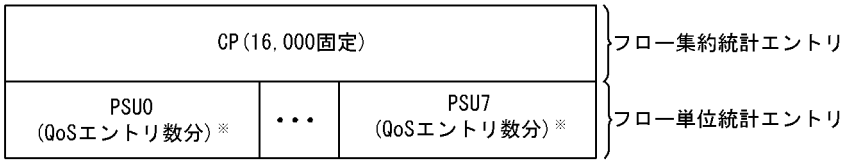
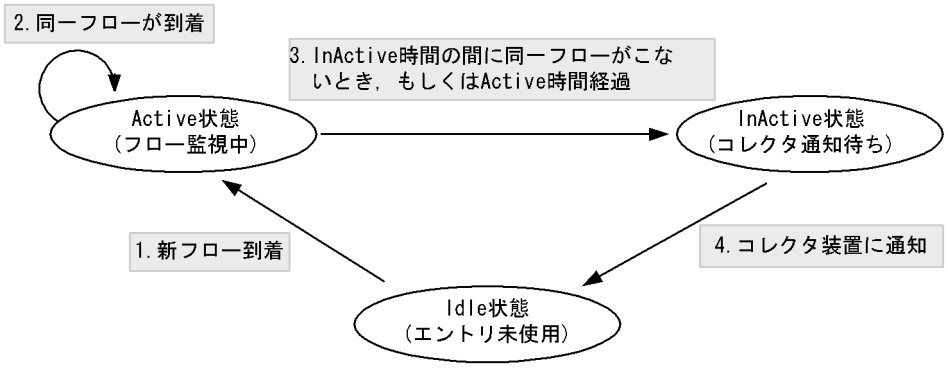


図 10-18　フロー統計エントリの実装位置【SB-5400S】

注※

最大 QoS エントリ数は装置モデルによります。詳細は，SB-7800S の場合「解説書 Vol.1　3.2.1(19) フィルタリング・QoS」，SB-5400S の場合「解説書 Vol.1　3.2.2(18) フィルタリング・QoS」を参照してください。

図 10-19　フロー統計エントリの状態遷移図



〔図の説明〕

1. フロー統計エントリに空きがある状態で新規フローが到着した時，Idle 状態のエントリを一つ確保し，フロー情報を登録して Active 状態にします。
2. もし，同じフローが到着した場合は登録されているエントリにパケット数とバイト数を加算します。
3. その後，InActive 時間の間に同一フローが来ない場合，もしくはエントリが作成されてから Active 時間が経過した場合はコレクタ通知待ち状態に移行します。
4. コレクタ通知待ちのエントリをコレクタ装置に通知します。

(2) フロー統計エントリとコンフィグレーションの関係

フロー単位統計エントリおよびフロー集約統計エントリとして必要なエントリ数は，「サンプリング間隔 (sample)」「無通信最大時間 (timeout-inactive)」「通信最大時間 (timeout-active)」の値によって，変化します。コンフィグレーションコマンドによって，「PSU 単位 (SB-5400S では BSU 単位) のエントリ数 (entries)」「集約種別ごとのエントリ数 (aggregation-entries)」を設定してください。以下に平均的に利用するフロー統計エントリ数およびコンフィグレーションの関係式とその計算例を示します。

フロー単位統計エントリ平均利用数　＝
1 秒間に流れる平均パケット数 ÷ サンプリング間隔 × 最大無通信時間 (秒)

注
ただし，「1 秒間に流れるフロー数」が小さい場合，エントリ利用数は少なくなります。

【目安値の計算】

- 回線負荷　　＝ 1 秒間に流れるパケット数が 200,000 個
- サンプリング間隔＝ 1,000 パケットに 1 個サンプリング
- 最大無通信時間　＝ 15 秒間に同一フローが到着しなければコレクタ装置へ通知

200,000[パケット数／秒] ÷ 1,000[サンプリング間隔] × 15[最大無通信時間 (秒)]
＝ 3,000 個のフロー単位統計エントリが最低必要※1※2

フロー集約統計エントリ数 (aggregation-entries) については，次の関係式を目安としてください。

フロー集約統計エントリ平均利用数＝
1 秒間に流れる平均パケット数 ÷ サンプリング間隔 × 集約の最大無通信時間 (秒)

注
ただし，「1 秒間に流れる集約後のフロー数」が小さい場合，エントリ利用数は少なくなります。

【目安値の計算】

- 回線負荷　　＝ 1 秒間に流れるパケット数が 500,000 個。
  集約後のフローパターン数を 2,000 とします。
- サンプリング間隔＝ 1,000 パケットに 1 個サンプリング
- 集約ごとの最大無通信時間
  ＝ 15 秒間に同一フローが到着しなければコレクタ装置へ通知

500,000[パケット数／秒] ÷ 1,000[サンプリング間隔] × 15[最大無通信時間 (秒)]

＝ 7,500 個のフロー集約統計エントリが最低必要※1※2

ただし，前提条件によって集約後のフローパターン数が 2,000 であることから，このパターンでは 2,000 個のフロー集約統計エントリがあれば十分です。

注※ 1

この値は平均的に利用するフロー統計エントリ数です。環境によって増加しますのでこの値より大きな値を設定してください。

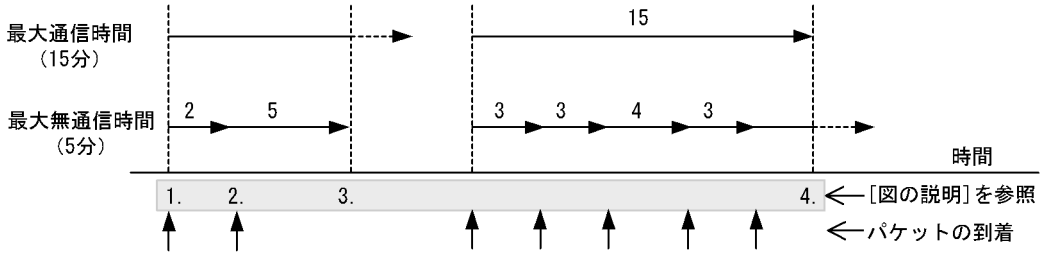
注※ 2

エントリ数が少なくても，show netflow コマンドの「Dropped Flows」が増えない限り正常に収集できています。ただし，少ない場合 CP-CPU への負荷が高くなります。

(3) 最大通信時間および最大無通信時間によるコレクタ装置への通知タイミング

フロー単位統計およびフロー集約統計で設定する「最大通信時間 (timeout-active)」と「最大無通信時間 (timeout-inactive)」の値によって，フロー統計エントリの情報をコレクタ装置に通知するタイミングが変わります。最大通信時間および最大無通信時間によるコレクタ装置への通知タイミングを次の図に示します。

図 10-20　最大通信時間および最大無通信時間によるコレクタ装置への通知タイミング



〔図の説明〕

1. 新規フローが到着したとき，最大通信時間 (例では 15 分) および最大無通信時間 (例では 5 分) のタイマを起動します。
2. 同じフローが到着したとき，古い最大無通信時間タイマを停止して，再度最大無通信時間タイマを起動します。
3. もし，最後にパケットが到着してから最大無通信時間経過した場合は，その時点でフロー統計エントリの情報をコレクタ装置に通知して，該当フロー統計エントリの削除 (タイマの停止) を行います。
4. もし，常に同じフローのパケットが最大無通信時間以内に到着し続け，最大通信時間が経過した場合は，その時点でフロー統計エントリ情報をコレクタ装置に通知して，該当フロー統計エントリの削除 (タイマの停止) を行います。

10.2.7　本装置での NetFlow 統計の動作について

（1） NetFlow 統計収集の対象パケットに関する注意点

- 本装置での NetFlow 統計は，受信時に他装置へ転送または自宛てと判定されるパケットを対象パケットとして扱います。
- 受信時に廃棄と判定されるパケット (Filter 機能で廃棄判定されるパケットなど) は，NetFlow 統計収集の対象外パケットとして扱います。ただし，QoS 機能の廃棄制御に従ってキューイング時に廃棄されるパケットは NetFlow 統計収集の対象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

- 本装置での NetFlow 統計は，受信側でフロー情報を収集しコレクタ装置に通知します。この性質上，送信インタフェース側に Filter 機能や QoS 機能を設定してパケットを廃棄する条件でも，コレクタ装置には中継しているように通知してしまいます。Filter 機能や QoS 機能と併用する場合は，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 NetFlow 統計収集条件を次の表に示します。

表 10-66　他機能と併用時の NetFlow 統計収集条件

機能	IN 側に設定	OUT 側に設定
Filter 機能	廃棄対象は収集されない	収集される
QoS 機能	帯域・優先度で制限される場合は収集されない	収集される

（3） entries(QoS エントリ) 利用上の注意点

- NetFlow 統計を利用する場合，NetFlow コンフィグレーションの entries の指定が必要です。集約用エントリ (aggregation-entries) はそのままフロー数分の監視が可能です。
- 本エントリ数は，QoS 機能とエントリを共用します。したがって，本値と QoS 機能で使用しているエントリ数の合計が，最大エントリ数を超えて設定することはできません。現在利用しているエントリ数を確認する場合は，コンフィグレーションコマンド show flow used_resources を使用してください。コマンドの詳細については，「コンフィグレーションコマンドレファレンス Vol.2　1. フロー情報」の各コンフィグレーションを参照してください。
- SB-7800S での最大エントリ数については，「解説書 Vol.1　3.2.1(19)(d) NetFlow 統計のエントリ数」および「解説書 Vol.1　3.2.1(13) 基本制御モジュール (BCU) のメモリ量と収容経路エントリ数」の表の QoS エントリ数を参照してください。
- SB-5400S での最大エントリ数については，「解説書 Vol.1　3.2.2(18)(d) NetFlow 統計のエントリ数」および「解説書 Vol.1　3.2.2(12) 基本制御モジュール (BCU) のメモリ量と収容経路エントリ数」の表の QoS エントリ数を参照してください。

10.2.8　NetFlow 機能に関する制限事項【SB-7800S】

（1） ハードに依存する制限事項

PSU-1，PSU-2 では，IP アドレスを定義していないインタフェースで受信したパケットを廃棄する場合，当該パケットをフロー登録およびフロー統計収集の対象パケットとして扱います。上記以外の PSU では非対象パケットとして扱います。

PSU-1，PSU-2 では，マルチキャストの定義を設定していないインタフェースで受信した IP アドレスがマルチキャストであるパケットを廃棄する場合，当該パケットをフロー登録およびフロー統計収集の対象

パケットとして扱います。上記以外の PSU では非対象パケットとして扱います。ただし，IPv4 アドレスが 224.0.0.0/24，あるいは IPv6 アドレスが FF00::/12 のパケットは，フロー登録およびフロー統計収集の対象パケットとして扱います。

PSU-1，PSU-2 では，NetFlow 統計機能を停止する際は，まず当該ポートを収容している PSU を close してください。その後，NetFlow 統計を停止してください。行わない場合，PSU が hardware failure でダウンする可能性があります。

PSU-1，PSU-2 では，NetFlow 統計のフロー最終パケット受信時刻値が当該フローの最終サンプルパケット受信時刻でなく，当該フローの最終パケット受信時刻［非サンプル］になります。

同一 PSU に NIF を 2 枚搭載して，NetFlow が有効なポートを収容している NIF から，中継されるパケットと廃棄されるパケットを混在して受信した場合，廃棄されたパケットの NetFlow 統計を収集する場合があります。

BCU-SH8MS/BCU-SM8MS/BCU-SL8MS の場合に NetFlow 統計機能で取り扱える IPv6 経路数は 16,384（16k）経路までです。

（2）ハードに依存しない制限事項

IP オプションパケットは，NetFlow 統計収集の対象外パケットとして扱います。

IPv6 拡張ヘッダ付きパケットは，フラグメントヘッダ付きパケットを除き，NetFlow 統計収集の対象外パケットとして扱います。

Null インタフェースで廃棄されるパケットは NetFlow 統計収集の対象外パケットとして扱います。

dot1x(IEEE 802.1X 機能情報) 構成情報を有効にしているポートに対して，NetFlow 統計情報を有効にした場合，該当ポートで 802.1X として廃棄している自宛パケットが，NetFlow 統計の対象パケットとして誤って採取する場合があります。

10.2.9　NetFlow 機能に関する制限事項【SB-5400S】

（1）ハードに依存する制限事項

BSU-C1，BSU-S1 では，IP アドレスを定義していないインタフェースで受信したパケットを廃棄する場合，当該パケットをフロー登録およびフロー統計収集の対象パケットとして扱います。この場合，あらかじめ設定されたサンプリングレートに従いフロー登録およびフロー統計収集を行うか否かを判定し，処理を行うと判定した場合だけ，当該パケットのフロー登録処理およびフロー統計収集処理を行います。

BSU-C1，BSU-S1 では，マルチキャストの定義を設定していないインタフェースで受信した IP アドレスがマルチキャストであるパケットを廃棄する場合，当該パケットをフロー登録およびフロー統計収集の対象パケットとして扱います。上記以外の BSU では非対象パケットとして扱います。ただし，IPv4 アドレスが 224.0.0.0/24，あるいは IPv6 アドレスが FF00::/12 のパケットは，フロー登録およびフロー統計収集の対象パケットとして扱います。

SB-5404S で NIF を 2 枚以上※搭載して，NetFlow が有効なポートを収容している NIF から，中継されるパケットと廃棄されるパケットを混在して受信した場合，廃棄されたパケットの NetFlow 統計を収集する場合があります。

注※

2 枚搭載の場合は，実装位置が NIF 番号 0 または 1 に 1 枚実装，NIF 番号 2 または 3 に 1 枚実装される場合にだけ上記現象が発生します。

（2） ハードに依存しない制限事項

IP オプションパケットは，NetFlow 統計収集の対象外パケットとして扱います。

IPv6 拡張ヘッダ付きパケットは，フラグメントヘッダ付きパケットを除き，NetFlow 統計収集の対象外パケットとして扱います。

Null インタフェースで廃棄されるパケットは NetFlow 統計収集の対象外パケットとして扱います。

dot1x(IEEE 802.1X 機能情報) 構成情報を有効にしているポートに対して，NetFlow 統計情報を有効にした場合，該当ポートで 802.1X として廃棄している自宛パケットが，NetFlow 統計の対象パケットとして誤って採取する場合があります。

11 隣接装置情報の管理

この章では本装置の隣接装置情報の管理についてサポート仕様を中心に説明します。

11.1　LLDP 機能

11.1.1　概要

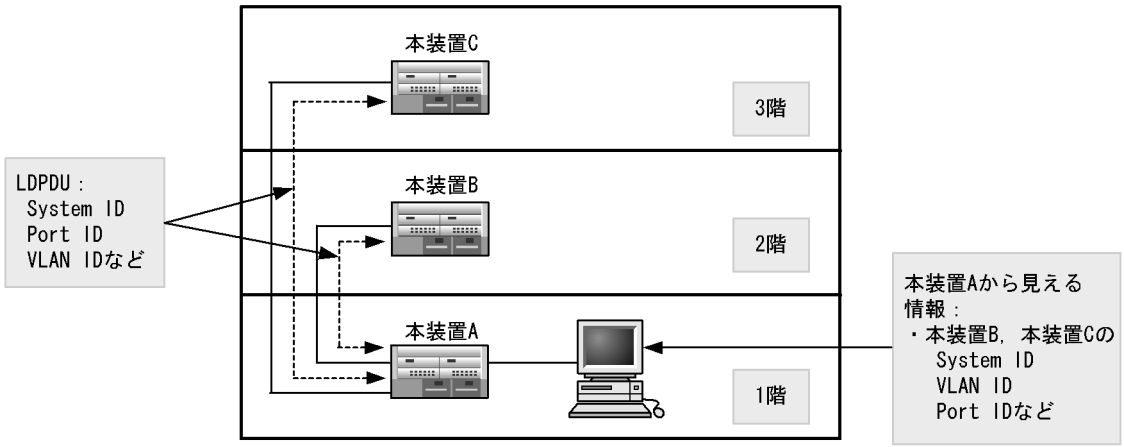
LLDP（Link Layer Discovery Protocol）は隣接する装置情報を収集するプロトコルです。収集した情報を運用コマンドで表示することで，運用・保守時に接続装置の情報を簡単に調査できることを目的とした機能です。

（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 から把握することが可能となります。

図 11-1　LLDP の適用例



11.1.2　サポート機能

この機能を用いて隣接装置に配布する情報は，IEEE Std 802.1AB D6 をベースに拡張機能として弊社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 11-1　LLDP でサポートする情報

項番		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・組織が独自に定めた TLV
	a	VLAN ID	定義されている VLAN ID

項番		名称	説明
	b	VLAN Address	VLAN に関連付けられた 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することが可能ですが，初期状態で使用することを推奨します。コンフィグレーションの詳細は，マニュアル「コンフィグレーションコマンドレファレンス Vol.2」を参照してください。

(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。次の表に subtype と送信内容を示します。

表 11-2 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
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以下のとおりです。

- 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 について受信可能です。
- 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。次の表に subtype と送信内容を示します。

表 11-3 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

subtype	種別	送信内容
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以下のとおりです。

- 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 について受信可能です。
- 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以下のとおりです。

- 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以下のとおりです。

- 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以下のとおりです。

- 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

弊社独自に以下の情報をサポートしています。

（a） VLAN ID

この情報は該当ポートが Tag-VLAN 連携を使用している場合に，Tag-VLAN 連携として所属している VLAN ID の番号を示します。

（b） VLAN Address

この情報は，該当ポートで定義されている VLAN のうち，IP アドレスが定義されている最も小さい VLAN ID とその IP アドレスを示します。

11.1.3 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

下記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することができるので，直接接続されている装置間の情報と区別がつかなくなります。
- ルータを経由して接続した場合には，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することはできません。

(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：CDP(Cisco Discovery Protocol)
Extreme：EDP(Extreme Discovery Protocol)
Foundry：FDP(Foundry Discovery Protocol)

(3) 隣接装置の最大数について

装置当たり最大 384 の隣接装置情報を収容可能です。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。

(4) 二重化切り替えについて【SB-7800S】

BCU の切り替えが起こった際には，切り替え動作時に装置 MAC アドレスが変更されます。その場合，切り替えが起こる前の配布情報が保持時間のタイムアウトで削除されるまで，二つの装置が接続されているように show lldp コマンドで表示されます。

この状態を回避するためには，コンフィグレーションコマンド local-mac-address で装置 MAC アドレスを変更しないようにする必要があります。

11.1.4 OADP との共存

本装置に，PSU-1，PSU-2，BSU-C1，BSU-S1 が 1 枚でも存在すると，LLDP が優先的に動作して，OADP と LLDP を同時に動作させることができません (コンフィグレーションに混在させることは可能です)。

11.2　OADP 機能

11.2.1　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することができます。

また，CDP(Cisco Discovery Protocol) を解釈することができるため，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 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。

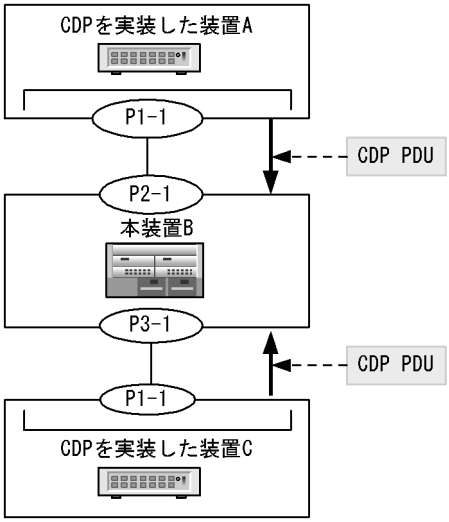
この機能では，隣接装置の装置情報やポート情報を表示することで隣接装置との接続状況を容易に把握できることから，隣接装置にログインしたりネットワーク構成図を参照したりしなくても，装置間の接続の状況を確認できます。また，この機能によって表示される接続状況とネットワーク構成図を比較することによって，装置間が正しく接続されているか確認することができます。

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。

本装置と CDP を実装した装置を接続した時の動作を以下に示します。

- この例では，CDP を実装した装置同士がお互いを認識できなくなる可能性があることを説明しています。
  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 PDU を受信するように設定 (cdp-listener コマンドを実行) 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-listener コマンドを実行しなければ，本装置 B は CDP PDU を受信せずに透過するので，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)。

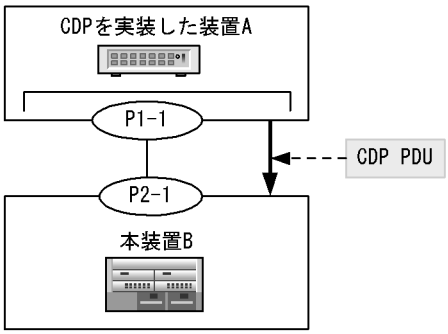
図 11-2　実装装置が隣接関係を認識できない例



- この例では，隣接関係が非対称になることを説明しています。
  CDP を実装した装置と本装置を接続し，本装置で CDP PDU を受信するように設定した場合，本装置では CDP PDU を送信しないので，CDP を実装した装置では本装置を認識できませんが，本装置では

CDP を実装した装置を認識できるので，隣接関係が非対称になります。

図 11-3 隣接関係が非対称になる例

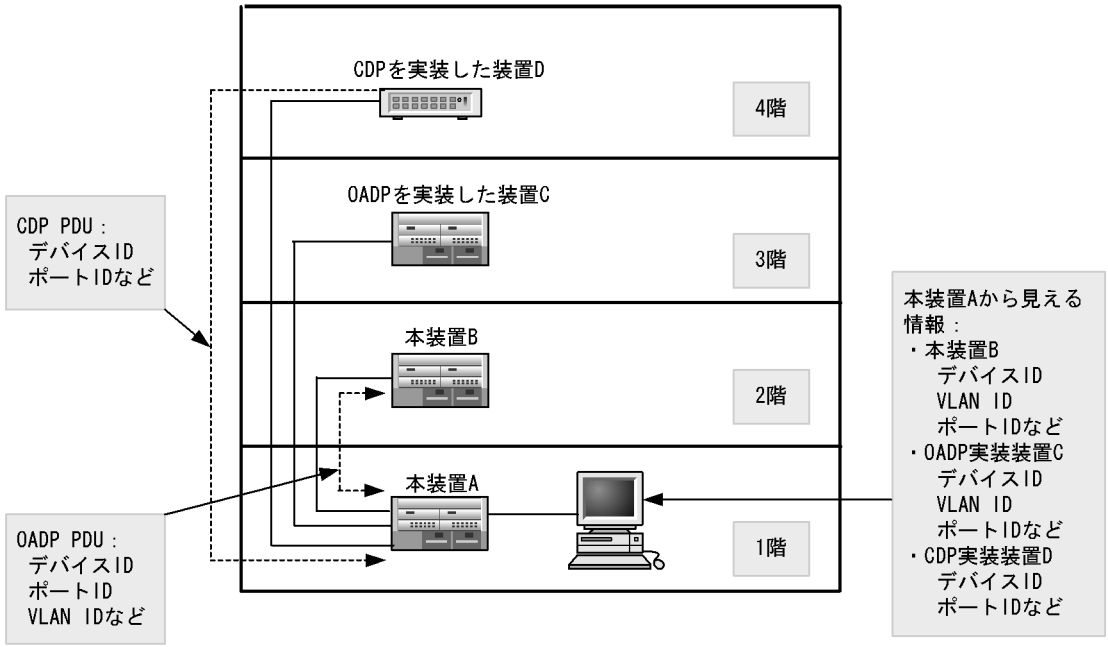


（1） OADP の適用例

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によって，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 11-4 OADP の適用例



11.2.2 サポート機能

OADP PDU で使用する情報を次の表に示します。

表 11-4 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 を送信するポートに関連するアドレス
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 11-5 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

11.2.3 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 11-6 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

(凡例) ○：サポート　×：未サポート

11.2.4　LLDP との共存

本装置に PSU-1，PSU-2，BSU-C1，BSU-S1 が 1 枚でも存在すると，LLDP が優先的に動作し，OADP と LLDP を同時に動作させることができません (コンフィグレーションに混在させることは可能です)。

それ以外の種類だけであれば，同時に動作させることができます。

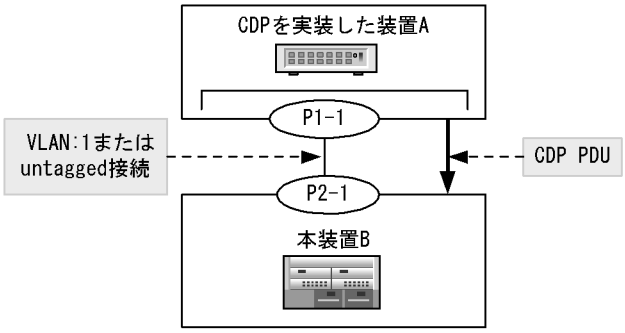
11.2.5　CDP を実装した装置と接続したときの注意事項

CDP を実装した装置と接続したとき，本装置で CDP を受信 (または，転送) できない場合があります。Tag-VLAN 連携機能を使用している場合は，そのポートに VLAN ID=1 の設定を行ってください。レイヤ 2 スイッチの VLAN 機能を使用して VLAN-Tag を用いる場合は，Default VLAN を enable 状態にしてください。それ以外の場合は，本装置で廃棄されます (転送もされません)。

もしくは，CDP を受信するポートでは Tag を使わないように設定してください。

Tag-VLAN 連携機能の注意事項については，「解説書 Vol.1　10.2(4) Tag-VLAN 連携使用時の注意事項」を参照してください。

図 11-5　CDP を実装した装置との接続



12 ポートミラーリング

ポートミラーリングの機能とサポート仕様について説明します。

12.1 ポートミラーリング概説

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ナライザなどで受信することによって，トラフィックの監視や解析を行うことができます。

受信フレーム，および送信フレームに対するミラーリングのそれぞれの動作を次の図に示します。

図 12-1 受信フレームのミラーリング

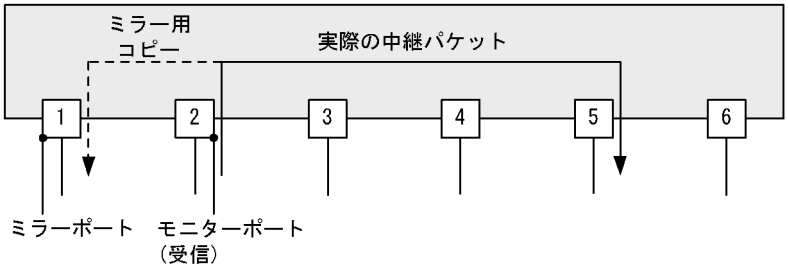
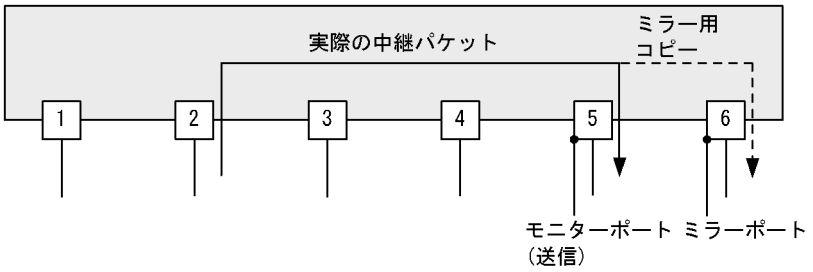


図 12-2 送信フレームのミラーリング



これらの図で示すとおり，トラフィックを監視する物理ポートを**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。

通常，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。コンフィグレーションの設定によって，ミラーポートでも通常フレーム（ミラーリングによってコピーされたミラーフレーム以外のフレーム）の受信および送信ができます。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，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。

なお，本節での自発フレームとは，ARP など本装置から送信する中継フレーム以外のフレームを指します。具体的には，次に示すフレームです。

- 送信元 MAC アドレスが自装置の MAC アドレスで，かつ送信元 IP アドレスが自装置の IP アドレスである IP フレーム
- 送信元 MAC アドレスが自装置の MAC アドレスである非 IP フレーム

また，自宛フレームとは，次に示すフレームを指します。

- 宛先 MAC アドレスが自装置の MAC アドレスで，かつ宛先 IP アドレスが自装置の IP アドレスである IP フレーム
- 宛先 MAC アドレスがブロードキャストまたはマルチキャストのフレーム

- 宛先 MAC アドレスが自装置の MAC アドレスである非 IP フレーム

12.2 フィルタ /QoS 制御機能併用時の動作

モニターポートに対してフィルタ /QoS 制御を設定することができます。ポートミラーリング機能とフィルタ /QoS 制御機能の併用を次の図に示します。図に示す (a) ～ (d) の各ポイントについて，ポートミラーリング機能とフィルタ /QoS 制御機能の併用時の動作を「表 12-1　ポートミラーリング機能とフィルタ /QoS 制御機能の併用時の動作」に示します。

図 12-3　ポートミラーリング機能とフィルタ /QoS 制御機能の併用

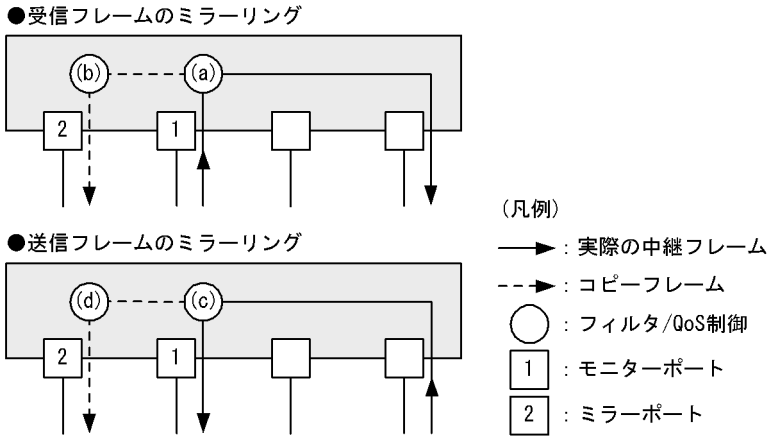


表 12-1　ポートミラーリング機能とフィルタ /QoS 制御機能の併用時の動作

フィルタ /QoS 制御 ポイント	フィルタ /QoS 制御 動作可否	フィルタ /QoS 制御の動作仕様
(a)	○	モニターポートの入力側で，受信するフレームに対してフィルタ /QoS 制御を行います。フィルタによって実際のフレームを廃棄しても，該当フレームはミラーリングされます。また IP ヘッダの書き換えを行うと，コピーしたフレームの IP ヘッダも書き換わります。ただし，レイヤ 2 ヘッダの書き換え (ユーザ優先度の書き換えなど) を行っても，コピーしたフレームのレイヤ 2 ヘッダは書き換わりません。
(b)	○	ミラーポートの出力側で，コピーしたフレームに対するフィルタ /QoS 制御は <Portlist> に指定の場合にだけ動作します。インタフェース名指定の場合は動作しません。※
(c)	○	モニターポートの出力側で，送信するフレームに対してフィルタ /QoS 制御を行います。(a) と同様，制限なし。フィルタによる廃棄を指定した場合，送信フレームが廃棄されるため，フレームをミラーリングすることはありません。回線に出力するフレームだけがミラーリングされます。
(d)	-	ミラーポートの出力側で，コピーしたフレームに対するフィルタ /QoS 制御は動作しません。

(凡例)　○ : フィルタ /QoS 制御できる　- : フィルタ /QoS 制御できない
注※　ミラーポートでは，DSCP を書き換える動作はできません。

なお，ミラーポートでの通常通信に対するフィルタ /QoS 制御は，制限なく動作します。

12.3　サポート仕様

この節ではポートミラーリングのサポート仕様を示します。まず，モニターポートとミラーポートの最大数を次の表に示します。

表 12-2　モニターポートとミラーポートの最大数【SB-7800S】

項目	仕様
モニターポート数 / 装置	64
ミラーポート数 / 装置	64

表 12-3　モニターポートとミラーポートの最大数【SB-5400S】

項目	仕様
モニターポート数 / 装置	64
ミラーポート数 / 装置	64

次に，SB-7800S と SB-5400S のポートミラーリングの設定可否をそれぞれ次の表に示します。

表 12-4　ポートミラーリングの設定可否【SB-7800S】

NIF 種別	モニターポート (受信)	モニターポート (送信)	ミラーポート
NE1G-12TA NE1G-6GA NE1G-12SA NEMX-12	○	○※1	○
NE1G-48T	○	○※1	○
NE10G-1ER NE10G-1EW NE10G-1LW NE10G-1RX S22-10G4RX S33-10G4RX	○	-	○
NE1GSHP-4S	-	-	-
NE1GSHP-8S	○	○※1※2	○※2※3
NP192-1S4 NP48-4S NP192-1S	-	-	-
S12-1G48T S12-1G48S	○	○※4	○

(凡例) ○ : 設定できる　- : 設定できない

注※ 1

モニターポートとミラーポートが同一 NIF 内でなければなりません。

注※ 2

送信フレームをモニターする場合，モニターポートのコンフィグレーションの階層化シェーパ情報のアグリゲートキューの設定と同じ設定をミラーポートに設定してください。

注※ 3

受信フレームのモニターポートが NE1GSHP-8S 以外の場合，コンフィグレーションの階層化シェーパ情報でデ

フォルトアグリゲートキューをミラーポートに設定してください。

注※ 4

モニターポートとミラーポートが同一 NIF 内の 12 ポート単位のグループ (0 ～ 11，12 ～ 23，24 ～ 35，36 ～ 47) 内でなければなりません。モニターポートとミラーポートの組み合わせを次の表に示します。

表 12-5　モニターポートとミラーポートの組み合わせ

項目		ミラーポート番号			
		0 ～ 11	12 ～ 23	24 ～ 35	36 ～ 47
送信モニターポート番号	0 ～ 11	○	-	-	-
	12 ～ 23	-	○	-	-
	24 ～ 35	-	-	○	-
	36 ～ 47	-	-	-	○

(凡例) ○：ミラーリング可能　-：ミラーリング不可能

表 12-6　ポートミラーリングの設定可否【SB-5400S】

NIF 種別	モニターポート (受信)	モニターポート (送信)	ミラーポート
NF1G-6G NF100-48TA	○	○※ 1	○
NF1G-48T NF1G-32S NFMX-44	○	○※ 1	○
NFMX-34	○	○※ 1※ 2	○

(凡例) ○：設定できる

注※ 1

モニターポートとミラーポートが同一 NIF 内でなければなりません。

注※ 2

モニターポート（送信）が 0 ～ 31 ポート，ミラーポートが 32 または 33 ポートの組み合わせは使用できません。モニターポートとミラーポートの組み合わせを次の表に示します。

表 12-7　モニターポートとミラーポートの組み合わせ【SB-5400S】

項目		ミラーポート番号				
		0 ～ 7	8 ～ 15	16 ～ 23	24 ～ 31	32, 33
送信モニターポート番号	0 ～ 7	○	○	○	○	-
	8 ～ 15	○	○	○	○	-
	16 ～ 23	○	○	○	○	-
	24 ～ 31	○	○	○	○	-
	32, 33	○	○	○	○	○

(凡例) ○：ミラーリング可能　-：ミラーリング不可能

次に，ポートミラーリング使用時の帯域制限について，回線種別ごとに仕様を説明します。

表 12-8 ポートミラーリングの帯域制限

回線種別	ポート種別に対する帯域の上限		
	モニターポート (受信)	モニターポート (送信)	ミラーポート
10GBASE-R 10GBASE-W	6Gbit/s まで受信できます。※	-	回線帯域まで送信できます。
1000BASE-X 1000BASE-T	(ミラーリングが動作しないポートの受信帯域) ＋ (ミラーリングが動作する受信帯域× 2) が約 12Gbit/s までです。※	回線帯域まで送信できます。	
100BASE-TX 10BASE-T	回線帯域まで送信できます。		

(凡例) - : 未サポート

注※ 帯域を超えたフレームは廃棄されます。

12.4 ポートミラーリング使用時の注意事項

1. 次に示すフレームは送信フレームのミラーリング対象外です。
   - FCS が不正な場合
   - ソフトウェア中継フレーム
   - 自発フレーム（ARP など）
   - ミラーリングされたフレーム
2. 次に示すフレームは受信フレームのミラーリング対象外です。
   - FCS が不正な場合
   - IEEE802.3 形式フレームで MAC ヘッダの LENGTH 値が，受信フレームの LLC ヘッダと SNAP ヘッダおよび DATA 領域の合計長と一致しない受信フレーム（ただし，LENGTH 値が 0 ～ 0x2D のときはパッドを付加するため合計長は 46 バイトとなり LENGTH 長と不一致となりますが，この場合についてはミラーリングします。）
3. 送信のミラーリングによりコピーされたフレームは，該当するミラーポートのコンフィグレーションに従って Tag Protocol IDentifier（TPID）が決まります。
4. ミラーポートで通常フレームを送信抑止した状態（コンフィグレーションのポートミラーリング情報で outpkts_disable パラメータを設定）でも自発フレームは送信します。
5. 廃棄制御で廃棄されたフレームは回線から出力されませんが，該当フレームのコピーはミラーポートから出力されます。
6. フロー検出条件オプションが定義されていない PSU または BSU のミラーポートでは，フレームを受信抑止した状態（コンフィグレーションのポートミラーリング情報で inpkts_disable パラメータを設定）でも，自宛フレームを受信します。

13 RADIUS/TACACS+

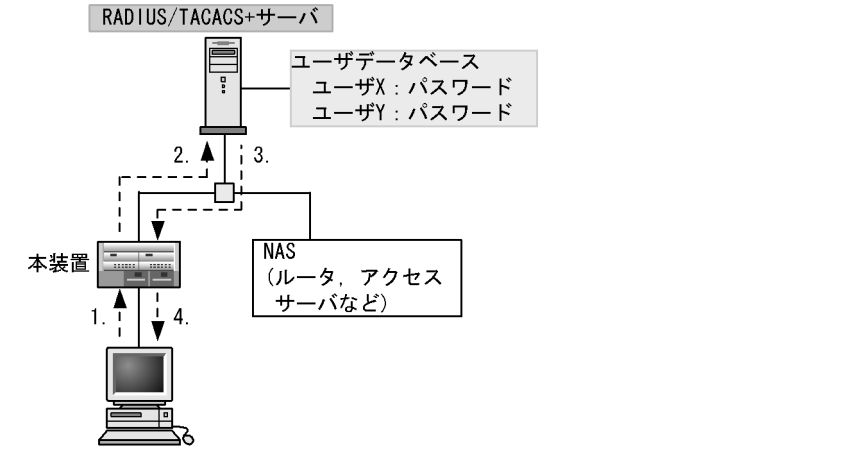
この章では RADIUS/TACACS+ サーバに対して本装置が要求する認証・承認・アカウンティング機能について説明します。

13.1 RADIUS/TACACS+ 概説

RADIUS (Remote Authentication Dial In User Service)，TACACS+(Terminal Access Controller Access Control System Plus) とは，NAS(Network Access Server) に対して認証・承認・アカウンティング機能を提供するプロトコルです。NAS は RADIUS/TACACS+ のクライアントとして動作するリモートアクセスサーバ，ルータなどの装置のことです。NAS は構築されている RADIUS/TACACS+ サーバに対してユーザ認証，コマンド承認，アカウンティングなどのサービスを要求します。RADIUS/TACACS+ サーバはその要求に対して，サーバ上に構築された管理情報データベースに基づいて要求に対する応答を返します。

RADIUS/TACACS+ を使用すると一つの RADIUS/TACACS+ サーバだけで，複数 NAS でのユーザパスワードなどの認証情報，コマンド承認情報やアカウンティング情報を一元管理することができるようになります。本装置では，RADIUS/TACACS+ サーバに対してユーザ認証・コマンド承認・アカウンティングを要求できます。また，RADIUS サーバに対して IEEE802.1X の端末認証を要求できます (IEEE802.1X での RADIUS 認証については「3　IEEE 802.1X」を参照してください)。RADIUS/TACACS+ 認証の流れを次の図に示します。

図 13-1　RADIUS/TACACS+ 認証の流れ



1. リモート運用端末からユーザXが本装置にtelnetを実行する。
2. 本装置はコンフィグレーションで指定したRADIUS/TACACS+サーバに対して認証を要求する。
3. RADIUS/TACACS+サーバはユーザデータベースに基づいてユーザXを認証し，本装置にユーザXを認証したことを通知する。
4. 本装置はRADIUS/TACACS+認証に基づいて，ユーザXのリモート運用端末からのtelnetを許可する。
5. 本装置はコンフィグレーションでコマンド承認を設定した場合，RADIUS/TACACS+サーバに設定してあるコマンドリストに従って，ユーザが投入する運用コマンドを許可／制限する。

13.2 RADIUS/TACACS+ の適用機能および範囲

本装置では，RADIUS/TACACS+ をリモート運用端末からのログイン時のユーザ認証，コマンド承認，アカウンティングに使用します。また，RADIUS を IEEE802.1X の端末認証に使用します (IEEE802.1X での RADIUS 認証の適用機能および範囲については「3 IEEE 802.1X」を参照してください)。RADIUS/TACACS+ 機能のサポート範囲を次に示します。ログインについては，「14.3 ログイン制御」も参照してください。

(1) RADIUS/TACACS+ の適用範囲

RADIUS/TACACS+ 認証を適用できる操作を次に示します。

- 本装置への telnet(IPv4/IPv6)
- 本装置への rlogin(IPv4/IPv6)
- 本装置への ftp(IPv4/IPv6)

次に示す操作は RADIUS/TACACS+ 認証を適用できません。

- RS232C からのログイン

RADIUS/TACACS+ コマンド承認を適用できる操作を次に示します。

- 本装置への telnet(IPv4/IPv6)
- 本装置への rlogin(IPv4/IPv6)

RADIUS/TACACS+ アカウンティングを適用できる操作を次に示します。

- 本装置への telnet(IPv4/IPv6) によるログイン・ログアウト
- 本装置への rlogin(IPv4/IPv6) によるログイン・ログアウト
- 本装置への ftp(IPv4/IPv6) によるログイン・ログアウト
- RS232C からのログイン・ログアウト
- CLI でのコマンド入力 (TACACS+ だけサポート)
- システム操作パネルでのコマンド入力 (TACACS+ だけサポート)

(2) RADIUS のサポート範囲

RADIUS のサポート範囲を次の表に示します。

表 13-1 RADIUS のサポート範囲

分類	内容
文書全体	NAS に関する記述だけを対象にします。
パケットタイプ	ログイン認証／コマンド承認で使用する次のタイプ • Access-Request (送信) • Access-Accept (受信) • Access-Reject (受信) • アカウンティングで使用する次のタイプ • Accounting-Request (送信) • Accounting-Response (受信)

分類	内容
属性	ログイン認証で使用する次の属性 • User-Name • User-Password • Service-Type • NAS-IP-Address • NAS-Identifier • Reply-Message コマンド承認で使用する次の属性 • Class • Vendor-Specific(Vender-ID=21839) アカウンティングで使用する次の属性 • User-Name • NAS-IP-Address • NAS-Port • NAS-Port-Type • Service-Type • Calling-Station-Id • Acct-Status-Type • Acct-Delay-Time • Acct-Session-Id • Acct-Authentic • Acct-Session-Time

(3) 使用する RADIUS 属性の内容

使用する RADIUS 属性の内容を次の表に示します。

表 13-2 使用する RADIUS 属性の内容

属性名	パケットタイプ	内容
User-Name (属性値 =1)	Access-Request Accounting-Request	認証するユーザの名前。
User-Password (属性値 =2)	Access-Request	認証ユーザのパスワード。 送信時には暗号化されます。
Service-Type (属性値 =6)	Access-Request Accounting-Request	Login(値 =1)。 Access-Accept および Access-Reject に添付された場合は無視します。
NAS-IP-Address (属性値 =4)	Access-Request Accounting-Request	本装置の IP アドレス。 ローカルアドレスが設定されている場合はローカルアドレス，ローカルアドレスが設定されていない場合は，送信インタフェースの IP アドレスになります。
NAS-Identifier (属性値 =32)	Access-Request Accounting-Request	本装置の装置名。 装置名が設定されていない場合は添付されません。
Reply-Message (属性値 =18)	Access-Accept Access-Reject Accounting-Response	サーバからのメッセージ。 添付されている場合は，運用ログとして出力されます (アカウンティングの場合はトレース情報として格納します。)。
Class (属性値 =25)	Access-Accept	ログインクラス。 コマンド承認で適用します。 詳細は注 3 を参照してください。
Vendor-Specific (属性値 =26)	Access-Accept	ログインリスト。 コマンド承認で適用します。 詳細は注 3 を参照してください。

属性名	パケットタイプ	内容
NAS-Port (属性値 =5)	Accounting-Request	ユーザが接続されている NAS のポート番号を指します。 本装置では，tty ポート番号を格納します。ただし，ftp の場合は 100 を格納します。
NAS-Port-Type (属性値 =61)	Accounting-Request	NAS に接続した方法を指します。 本装置では，telnet/rlogin/ftp は Virtual(5)，コンソール /AUX 時には Async(0) を格納します。
Calling-Station-Id (属性値 =31)	Accounting-Request	利用者の識別 ID を指します。 本装置では，telnet/rlogin/ftp はクライアントの IPv4/IPv6 アドレス，コンソールは「console」，AUX ポートは「aux」を格納します。
Acct-Status-Type (属性値 =40)	Accounting-Request	Accounting-Request がどのタイミングで送信されたかを指します。 本装置では，ユーザのログイン時に Start(1)，ログアウト時に Stop(2) を格納します。
Acct-Delay-Time (属性値 =41)	Accounting-Request	送信すべきイベント発生から Accountig-Request を送信するまでに要した時間 (秒) を格納します。
Acct-Session-Id (属性値 =44)	Accounting-Request	セッションを識別するための文字列を指します。 本装置では，セッションのプロセス ID を格納します。
Acct-Authentic (属性値 =45)	Accounting-Request	ユーザがどのように認証されたかを指します。 本装置では，RADIUS(1)，Local(2)，Remote(3) の 3 種類を格納します。
Acct-Session-Time (属性値 =46)	Accounting-Request (Acct-Status-Type が Stop の場合だけ)	ユーザがサービスを利用した時間 (秒) を指します。 本装置では，ユーザがログイン後，ログアウトするまでの時間 (秒) を格納します。

注 1

この表で示す以外の属性については，本装置が送信する Access-Request タイプパケットには添付しません。

注 2

RADIUS サーバから送信される Access-Accept，Access-Reject，および Accounting-Response タイプパケットにこの表で示す以外の属性が添付されている場合，本装置ではそれらを無視します。

注 3

RADIUS サーバを利用してコマンド制限する場合は，認証時に次の表に示すような属性値を返すように RADIUS サーバ側で設定します。RADIUS サーバでは，下記のベンダー固有属性をサポートしていない場合があります。その場合は，サーバにベンダー固有属性を登録 (dictionary ファイルなどに設定) してください。

表 13-3　コマンド承認で使用する RADIUS 属性の内容

属性名		内容
Class		ログインクラス 次のどれかの文字列を指定します。 root, allcommand, noconfig, nomanage, noenable
Vendor-Specific (Vendor-Id=21839)	Vendor type 101 ALAXALA-Allow-Commands	許可コマンドリスト 許可するコマンドの前方一致文字列を”,”で区切って指定します。空白も区別します。 例：ALAXALA-Allow-Commands=”show, ping, telnet”
	Vendor type 102 ALAXALA-Deny-Commands	制限コマンドリスト 制限するコマンドの前方一致文字列を”,”で区切って指定します。空白も区別します。 例：ALAXALA-Deny-Commands=”enable, reload, close”

(4) TACACS+ のサポート範囲

TACACS+ のサポート範囲を次の表に示します。

表 13-4 TACACS+ のサポート範囲

分類		内容
文書全体		NAS に関する記述だけを対象にします。
パケットタイプ		ログイン認証で使用する次のタイプ • Authentication Start (送信) • Authentication Reply(受信) • Authentication Continue (送信) コマンド承認で使用する次のタイプ • Authorization Request (送信) • Authorization Response (受信) アカウンティングで使用する次のタイプ • Accounting Request (送信) • Accounting Reply (受信)
ログイン認証		• User • Password
コマンド承認	Service	• grlogin
	属性	• class • allow-commands • deny-commands
アカウンティング	flag	• TAC_PLUS_ACCT_FLAG_START • TAC_PLUS_ACCT_FLAG_STOP
	属性	• task_id • start_time • stop_time • elapsed_time • timezone • service • priv-lvl • cmd

(5) 使用する TACACS+ 属性の内容

コマンド承認時に使用する TACACS+ 属性 (Attribute-Value) の内容を次の表に示します。

表 13-5 TACACS+ 設定 Attribute-Value 一覧

Service	Attribute	Value
grlogin	class	ログインクラス 次のどれかの文字列を指定 root, allcommand, noconfig, nomanage, noenable 例 : class=” noenable”
	allow-commands	許可コマンドリスト 許可するコマンドの前方一致文字列を”,”で区切って指定します。空白も区別します。 例 : allow-commands=” show ,ping ,telnet”
	deny-commands	制限コマンドリスト 制限するコマンドの前方一致文字列を”,”で区切って指定します。空白も区別します。 例 : deny-commands=” enable,reload,close”

アカウンティング時に使用する TACACS+ flag を次の表に示します。

表 13-6 TACACS+ アカウンティング flag 一覧

flag	内容
TAC_PLUS_ACCT_FLAG_START	アカウンティング START パケットを示します。 ただし，コンフィグレーションで送信契機に stop-only を指定している場合は，アカウンティング START パケットは送信しません。
TAC_PLUS_ACCT_FLAG_STOP	アカウンティング STOP パケットを示します。 ただし，コンフィグレーションで送信契機に stop-only を指定している場合は，このアカウンティング STOP パケットだけを送信します。

アカウンティング時に使用する TACACS+ 属性 (Attribute-Value) の内容を次の表に示します。

表 13-7 TACACS+ アカウンティング Attribute-Value 一覧

Attribute	Value
task_id	イベントごとに割り当てられる ID です。 本装置ではアカウンティングイベントのプロセス ID を格納します。
start_time	イベントを開始した時刻です。 本装置ではアカウンティングイベントが開始された時刻を格納します。この属性は以下のイベントで格納されます。 • 送信契機 start-stop 指定時のログイン時，コマンド実行前 • 送信契機 stop-only 指定時のコマンド実行前
stop_time	イベントを終了した時刻です。 本装置ではアカウンティングイベントが終了した時刻を格納します。この属性は以下のイベントで格納されます。 • 送信契機 start-stop 指定時のログアウト時，コマンド実行後 • 送信契機 stop-only 指定時のログアウト時
elapsed_time	イベント開始からの経過時間 (秒) です。 本装置ではアカウンティングイベントの開始から終了までの時間 (秒) を格納します。この属性は以下のイベントで格納されます。 • 送信契機 start-stop 指定時のログアウト時，コマンド実行後 • 送信契機 stop-only 指定時のログアウト時
timezone	タイムゾーン文字列を格納します。
service	文字列「shell」を格納します。
priv-lvl	コマンドアカウンティング設定時に指定されたコマンドが運用コマンドの場合は 1，コンフィグレーションコマンドの場合は 15 を格納します。
cmd	コマンドアカウンティング設定時に指定されたコマンド文字列 (最大 250 文字) を格納します。

13.3 RADIUS/TACACS+ を使用した認証

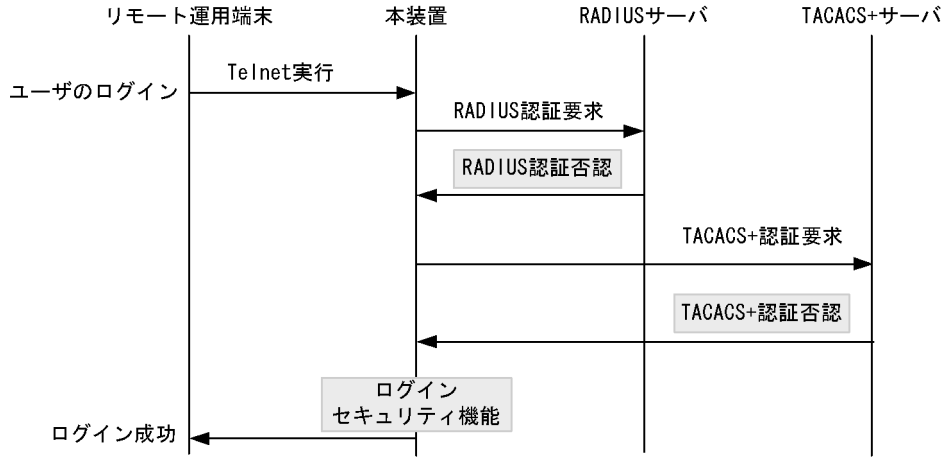
RADIUS/TACACS+ を使用した認証方法について説明します。

(1) ログイン認証方式の指定

リモートログインの認証に使用するサービスは複数指定できます。指定できるサービスは RADIUS，TACACS+ および password コマンドによる本装置単体でのログインセキュリティ機能です。これらの認証方式は単独でも同時でも指定でき，同時に指定された場合は先に指定された方式で認証に失敗した場合に，次に指定された方式で認証できます。

認証方式として RADIUS，TACACS+，単体でのログインセキュリティの順番で指定した場合の認証方式シーケンスを次の図に示します。

図 13-2 認証方式シーケンス



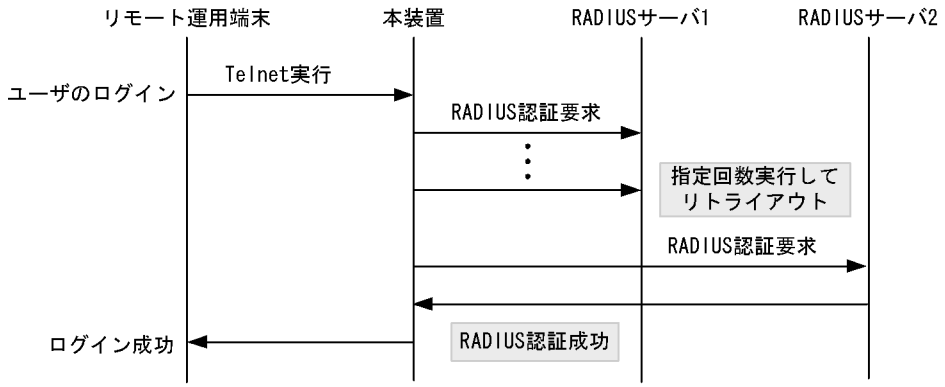
この図で端末からユーザが本装置に telnet を実行すると，RADIUS サーバに対し本装置から RADIUS 認証を要求します。RADIUS サーバと通信不可または RADIUS サーバでの認証に失敗すると，次に TACACS+ サーバに対し本装置から TACACS+ 認証を要求します。TACACS+ サーバと通信不可または TACACS+ サーバでの認証に失敗すると，次に本装置のログインセキュリティ機能での認証を実行します。ここで認証に成功し，ユーザは本装置へのログインに成功します。

(2) RADIUS/TACACS+ サーバの選択

RADIUS サーバ，TACACS+ サーバはそれぞれ最大四つまで指定できます。一つのサーバと通信できないで認証サービスが受けられない場合は，順次これらのサーバに接続を試行します。

RADIUS/TACACS+ サーバと通信不可を判断するタイムアウト時間を設定できます。デフォルト値は 5 秒です。また，各 RADIUS サーバでタイムアウトした場合は，再接続を試行します。この再試行回数も設定でき，デフォルト値は 2 回です。このため，ログイン方式として RADIUS が使用できないと判断するまでの最大時間は，タイムアウト時間×リトライ回数× RADIUS サーバ設定数になります。なお，各 TACACS+ サーバでタイムアウトした場合は，再接続を試行しません。このため，ログイン方式として TACACS+ が使用できないと判断するまでの最大時間は，タイムアウト時間× TACACS+ サーバ設定数になります。RADIUS サーバ選択のシーケンスを次の図に示します。

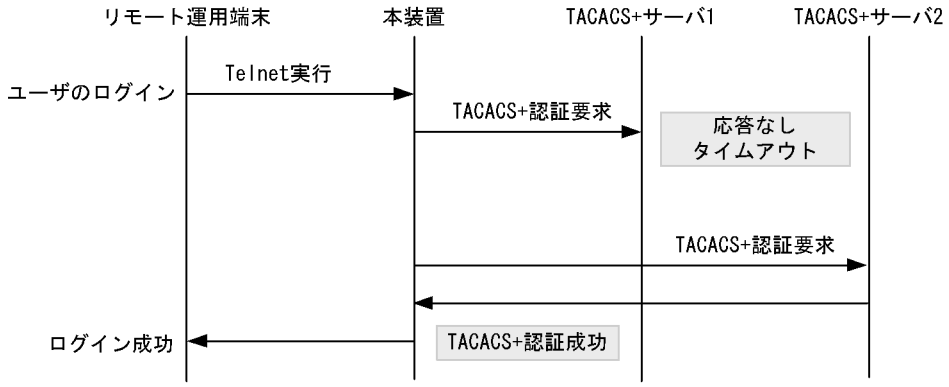
図 13-3 RADIUS サーバ選択のシーケンス



この図でリモート運用端末からユーザが本装置に telnet を実行すると，RADIUS サーバ 1 に対し本装置から RADIUS 認証を要求します。RADIUS サーバ 1 と通信できなかった場合は，続いて RADIUS サーバ 2 に対して RADIUS 認証を実行します。ここで認証に成功し，ユーザは本装置へのログインに成功します。

TACACS+ サーバ選択のシーケンスを次の図に示します。

図 13-4 TACACS+ サーバ選択のシーケンス



この図でリモート運用端末からユーザが本装置に telnet を実行すると，TACACS+ サーバ 1 に対し本装置から TACACS+ 認証を要求します。TACACS+ サーバ 1 と通信できなかった場合は，続いて TACACS+ サーバ 2 に対して TACACS+ 認証を実行します。ここで認証に成功し，ユーザは本装置へのログインに成功します。

13.4 RADIUS/TACACS+/ ローカル（コンフィグレーション）を使用したコマンド承認

RADIUS/TACACS+/ ローカル（コンフィグレーション）を使用したコマンド承認方法について説明します。

（1） コマンド承認の指定

本装置の RADIUS/TACACS+ およびログインコンフィグレーションでコマンド承認を設定すると，RADIUS/TACACS+ を設定したときは，ログイン認証と同時に，サーバからコマンドクラスおよびコマンドリストを取得します。ログインコンフィグレーションでローカルコマンド承認を設定したときは，ログイン認証と同時に，コンフィグレーションで設定されているコマンドクラスおよびコマンドリストを使用します。本装置ではこのコマンドクラスおよびコマンドリストに従ってログイン後の運用コマンドを許可／制限します。RADIUS/TACACS+ サーバやコンフィグレーションの設定については，「運用ガイド 5.2.6 CLI コマンドを制限する」および「コンフィグレーションガイド　21.3 ログイン情報」を参照してください。

図 13-5　RADIUS/TACACS+ サーバによるコマンド承認のシーケンス

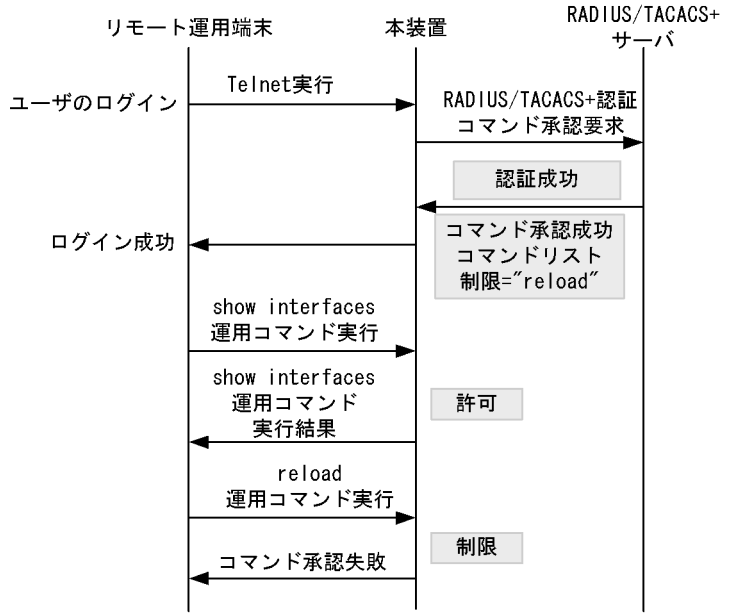
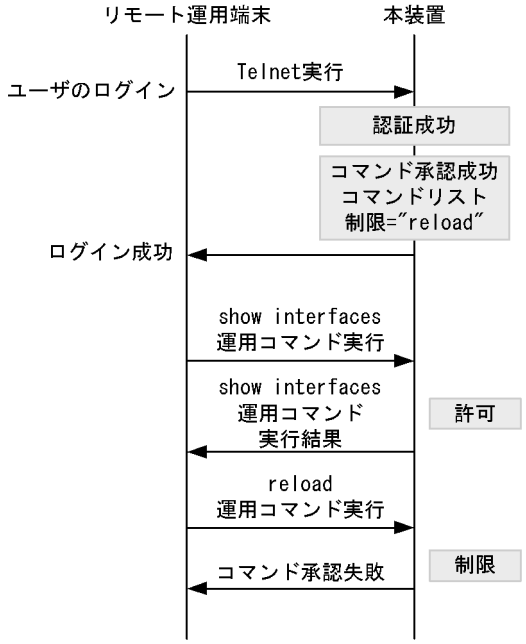


図 13-6 ローカルコマンド承認のシーケンス



「図 13-5 RADIUS/TACACS+ サーバによるコマンド承認のシーケンス」で端末からユーザが本装置に telnet を実行すると，RADIUS/TACACS+ サーバに対し本装置から認証，コマンド承認を要求します。認証成功時に RADIUS/TACACS+ サーバからコマンドリストを取得し，ユーザは本装置にログインします。

「図 13-6 ローカルコマンド承認のシーケンス」で端末からユーザが本装置に telnet を実行すると，ローカル認証を行います。認証成功時にコンフィグレーションからコマンドリストを取得し，ユーザは本装置にログインします。

ユーザは本装置で show interfaces 運用コマンドなどを実行できますが，reload 運用コマンドはコマンドリストによって制限されているために実行できません。

! 注意事項

RADIUS/TACACS+ サーバのコマンドクラスおよびコマンドリストの設定を変更した場合，またはコンフィグレーションのコマンドクラスおよびコマンドリストの設定を変更した場合は，次回のログイン認証後から反映されます。

13.5 RADIUS/TACACS+ 認証でのログインユーザの扱い

RADIUS/TACACS+ 認証機能を使用するには，RADIUS/TACACS+ サーバにユーザ名およびパスワードを登録します。RADIUS/TACACS+ サーバへ登録するユーザ名には次に示す 2 種類があります。

- 本装置に adduser コマンドを使用して登録済みのユーザ名
  本装置に登録されたユーザ情報を使用してログイン処理を行います。
- 本装置に未登録のユーザ名
  次に示す共通のユーザ情報でログイン処理を行います。
  - ホームディレクトリ：/usr/home/share/remote_user

本装置に未登録のユーザでログインした場合の注意点を示します。

- ファイルの管理
  ファイルを作成した場合，すべて remote_user 管理となって，別のユーザでも，作成したファイルの読み込みおよび書き込みができます。重要なファイルは ftp などで外部に保管するなど，ファイルの管理に注意してください。

13.6　RADIUS/TACACS+ を使用したアカウンティング

RADIUS/TACACS+ を使用したアカウンティング方法について説明します。

（1） アカウンティングの指定

本装置の RADIUS/TACACS+ コンフィグレーションと system コンフィグレーションのアカウンティングを設定すると，運用端末から本装置へのログイン・ログアウト時に RADIUS または TACACS+ サーバへアカウンティング情報を送信します。また，本装置へのコマンド入力時に，TACACS+ サーバへアカウンティング情報を送信します。

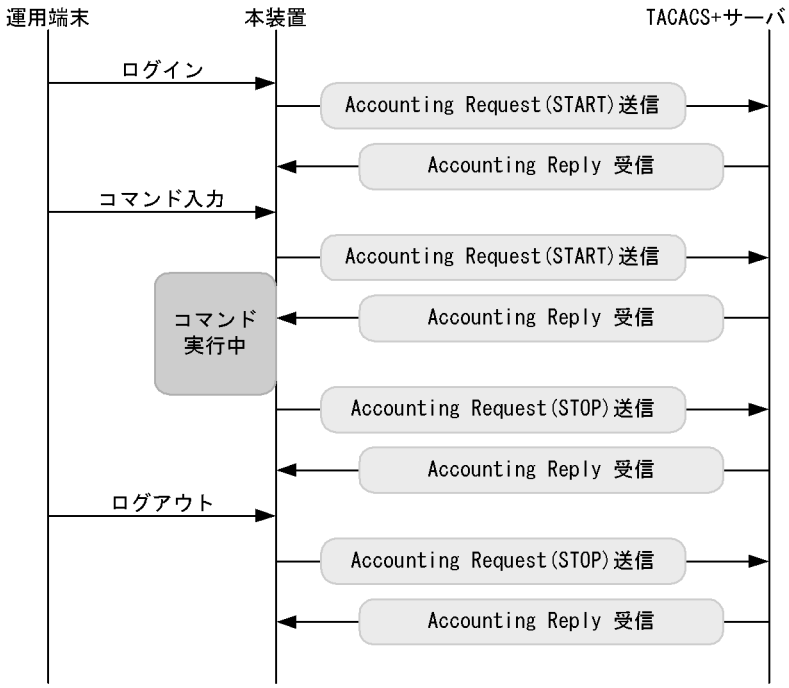
アカウンティングの設定は，ログインとログアウトのイベントを送信するログインアカウンティング指定と，コマンド入力のイベントを送信するコマンドアカウンティング指定があります。コマンドアカウンティングは TACACS+ だけでサポートしています。

それぞれのアカウンティングに対して，アカウンティング START と STOP を両方送信するモード（start-stop）と STOP だけを送信するモード（stop-only）を選択できます。さらに，コマンドアカウンティングに対しては，入力したコマンドをすべて送信するモードとコンフィグレーションコマンドだけを送信するモードとを選択できます。また，設定された各 RADIUS/TACACS+ サーバに対して，通常は，どこかのサーバでアカウンティングが成功するまで順に送信しますが，成功したかどうかにかかわらずすべてのサーバへ順に送信するモード（broadcast）も選択できます。

（2） アカウンティングの流れ

ログインアカウンティングとコマンドアカウンティングの両方を START-STOP 送信モードで TACACS+ サーバへ送信する設定をした場合のシーケンスを次の図に示します。

図 13-7　TACACS+ アカウンティングのシーケンス (ログイン・コマンドアカウンティングの START-STOP 送信モード時)

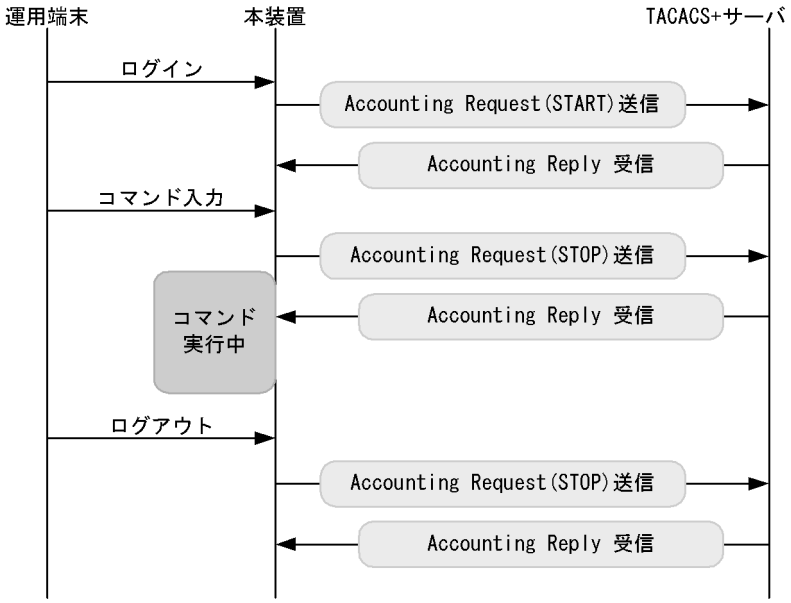


この図で運用端末から本装置にログイン成功すると，本装置から TACACS+ サーバに対しユーザ情報や時

刻などのアカウンティング情報を送信します。また，コマンド入力前後にも本装置から TACACS+ サーバに対し入力コマンド情報などのアカウンティング情報を送信します。最後に，ログアウト時には，ログインしていた時間などの情報を送信します。

ログインアカウンティングは START-STOP 送信モードのままで，コマンドアカウンティングだけを STOP-ONLY 送信モードにして TACACS+ サーバへ送信する設定をした場合のシーケンスを次の図に示します。

図 13-8　TACACS+ アカウンティングのシーケンス (ログインアカウンティング START-STOP，コマンドアカウンティング STOP-ONLY 送信モード時)



「図 13-7　TACACS+ アカウンティングのシーケンス (ログイン・コマンドアカウンティングの START-STOP 送信モード時)」の例と比べ，ログイン・ログアウトでのアカウンティング動作は同じですが，コマンドアカウンティングで STOP-ONLY を指定している場合，コマンド入力前にだけ本装置から TACACS+ サーバに対し入力コマンド情報などのアカウンティング情報を送信します。

(3) アカウンティングの注意事項

RADIUS/TACACS+ コンフィグレーション，system コンフィグレーションのアカウンティングの設定や IPv4 装置アドレスを変更した場合は，送受信途中や未送信のアカウンティングイベントと統計情報はクリアされ，新しい設定で動作します。

多数のユーザが，コマンドを連続して入力したり，ログイン・ログアウトを繰り返したりした場合，アカウンティングイベントが大量発生するため，一部のイベントでアカウンティングできないことがあります。

アカウンティングイベントの大量発生による本装置・サーバ・ネットワークへの負担を避けるためにも，コマンドアカウンティングは STOP-ONLY で設定することをお勧めします。また，正常に通信できない RADIUS/TACACS+ サーバは指定しないでください。

運用コマンド clear accounting でアカウンティング統計情報をクリアする場合，clear accounting コマンドの入力時点で各サーバへの送受信途中のアカウンティングイベントがあるときは，そのイベントの送受信終了後に，各サーバへの送受信統計のカウントを開始します。

14 運用機能

この章は，本装置の管理対象の考え方，管理情報および運用に使用する機能の概要について説明します。なお，リモート運用端末から本装置の運用管理を行うためにはIPネットワークへ接続されていることが必要です。

14.1 運用管理

本装置はセットアップ作業が終了すると，コンソールまたはリモート運用端末を使用して運用管理します。運用管理の種類を次の表に示します。

表 14-1 運用管理

運用機能	概要
コマンド入力機能	コマンドラインによる入力を受け付けます。
ログイン制御機能	不正アクセス防止，パスワードチェックを行います。
コンフィグレーション編集機能	運用のためのコンフィグレーションを設定します。設定された情報はすぐ運用に反映されます。
ネットワークコマンド機能	IP，IPv6 情報表示，リモート操作コマンドなどをサポートします。
ログ・統計情報	過去に発生した障害情報および回線使用率などの統計情報を表示します。
LED および障害部位の表示	LED およびシステム操作パネルによって本装置の状態を表示します。
MIB 情報収集	SNMP マネージャによるネットワーク管理が行います。
装置保守機能	装置を保守するための状態表示，装置とネットワークの障害を切り分けるための回線診断，およびボードの取り替えなどのコマンドを持ちます。
MC 保守機能	MC のコピー，フォーマットなどを行います。

14.1.1 運用端末

本装置は運用端末として初期導入時にコンソールが必要です。そのあとの運用にはコンソールまたはリモート運用端末が必要です。コンソールは RS232C に接続する端末，リモート運用端末は IP ネットワーク経由で接続する端末です。運用端末は telnet や rlogin でログイン接続します。運用端末は IP ネットワーク経由で SNMP マネージャによるネットワーク管理にも対応しています。運用端末の接続形態を「図 14-1 運用端末の接続形態」に，RM イーサネットポート (SB-5400S ではリモートマネージメントポート) と運用端末の条件を「表 14-2 運用端末の条件【SB-7800S】」，「表 14-3 運用端末の条件【SB-5400S】」に示します。

図 14-1　運用端末の接続形態

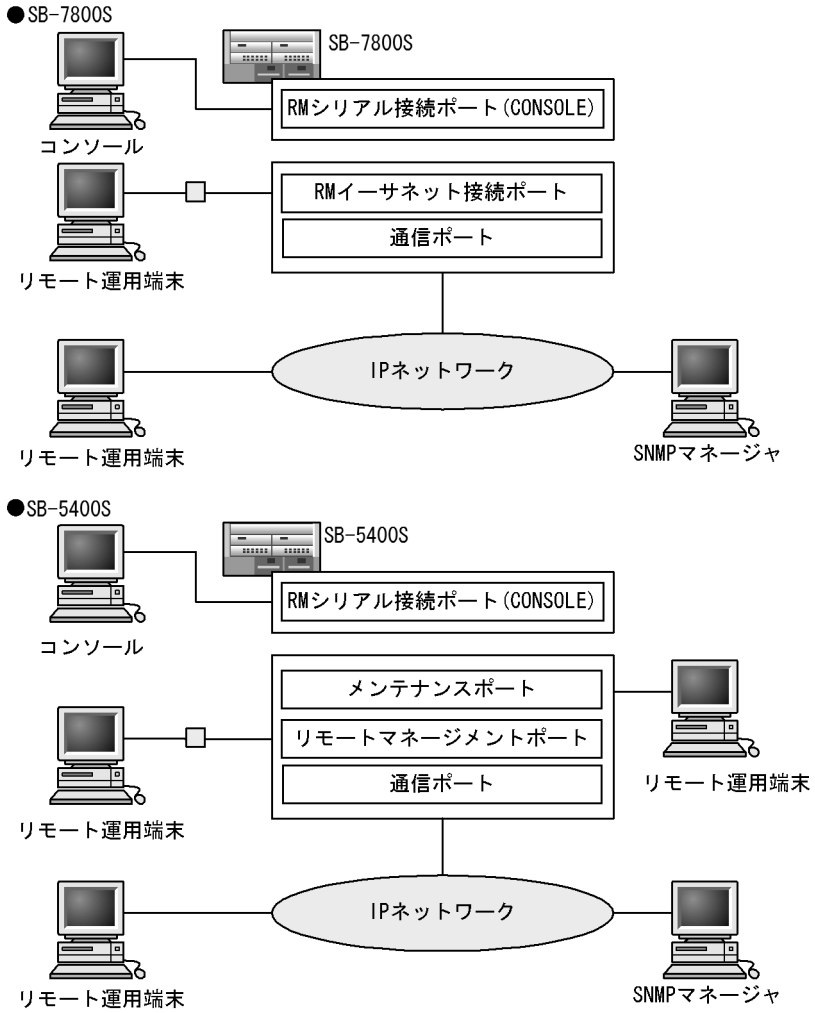


表 14-2　運用端末の条件【SB-7800S】

端末種別	接続形態	必要機能
コンソール	RM シリアル接続 (RS232C)	RS232C(回線速度：19200，9600，4800，2400，1200) ZMODEM 手順 CD-ROM(ISO-9660) ※
	RM シリアル接続 (モデム)	RS232C(回線速度：9600)
	ダイアルアップ IP 接続	RS232C(回線速度：9600)
リモート運用端末	RM イーサネットポート接続	TCP/IP telnet または rlogin ftp CD-ROM(ISO-9660) ※
	通信用ポート接続 (NIF 接続)	

注※　本端末を使用してソフトウェアの入れ替えを行う場合に必要です。

表 14-3 運用端末の条件【SB-5400S】

端末種別	接続形態	必要機能
コンソール	RM シリアル接続 (RS232C)	RS232C(回線速度：19200，9600，4800，2400，1200) ZMODEM 手順 CD-ROM(ISO-9660) ※
リモート運用端末	リモートマネージメントポート接続	TCP/IP telnet または rlogin ftp CD-ROM(ISO-9660) ※
	メンテナンスポート接続	
	通信用ポート接続 (NIF 接続)	

注※ 本端末を使用してソフトウェアの入れ替えを行う場合に必要です。

(1) コンソール

コンソールは RM シリアル接続 (RS232C) と RM シリアル接続 (モデム) があります。RM シリアル接続 (RS232C) の本装置のシリアルインタフェースは D-Sub9 ピンです。コンソールと接続する場合にはクロスケーブルを使用してください。例えば，AT 互換機と本装置を接続する場合には，AT 互換機同士をシリアルで接続するための D-Sub9 ピンクロスケーブルを使用してください。クロスケーブルの結線仕様を次の図に示します。

図 14-2 クロスケーブルの結線仕様

本装置側9ピン(メス)		接続	セットアップ端末側9ピン(メス)	
ピン番号	信号名		ピン番号	信号名
5	SG		5	GND
3	SD		2	RX
2	RD		3	TX
7	RS		1	DCD
8	CS		8	CTS
1	CD		7	RTS
6	DR		4	DTR
4	ER		6	DSR

RM シリアル接続 (モデム) およびダイアルアップ IP 接続のコンソールを本装置の RM シリアルインタフェースにモデムを接続する場合には，AT 互換機とモデムを接続するためのストレートケーブルを使用してください。また，本装置に接続するモデムは自動着信に設定してください。本装置ではモデムを設定できないので，PC などに接続して設定してください。

ダイアルアップ IP 接続のコンソールのダイアルアップ IP 接続手順は「運用ガイド 5.8 ダイアルアップ IP 接続を設定する」を参照してください。

ダイアルアップ IP 接続は，AUX ポートにモデムを接続して行います。ダイアルアップ IP 接続は，回線接続後にリモート運用端末として機能します。

(2) リモート運用端末

リモート運用端末は，本装置と運用端末を直接イーサネット接続する場合にはクロスケーブルを使用しま

す。RM イーサネットポート (SB-5400S ではリモートマネージメントポート) およびメンテナンスポート (SB-5400S だけ) は 10BASE-T および 100BASE-TX をサポートしています。

14.1.2 運用形態

運用端末の接続形態による特徴を次の表に示します。

表 14-4 運用端末接続形態ごとの特徴

運用機能	RM シリアル	通信用ポート	RM イーサネット (SB-5400S ではリモートマネージメントポート)	メンテナンスポート【SB-5400S】
接続運用端末	コンソール	リモート運用端末	リモート運用端末	リモート運用端末
遠隔からのログイン	不可	可	可	不可
待機系へのログイン	可	不可	不可	可
本装置から運用端末へのログイン	不可	可	可	不可
アクセス制御	なし	あり	あり	なし
コマンド入力	可	可	可	可
ROM コマンド入力	可	不可	不可	不可
ファイル転送方式	zmodem 手順	ftp	ftp	ftp
IP 通信	不可※	IPv4 および IPv6	IPv4 だけ	IPv4 だけ
SNMP マネージャ接続	不可	可	可	不可
コンフィグレーション設定	不要	必要	必要	不要

注※ SB-7800S では，AUX ポートでダイアルアップ IP 接続が可能です。

(1) RM シリアル接続ポート

RM シリアル接続ポートには運用端末としてコンソールを接続します。コンフィグレーションの設定なしに本ポートを介してログインすることができますので，初期導入時には本ポートからログインし，初期設定を行うことができます。また，ROM プロンプトでのコマンド入力は本ポートでだけ使用可能ですので，BCU パッケージ交換時のハードウェア設定時にはこのポートを使用して設定を行います。

このポートにモデムまたは RS-232C の無手順通信に対応した回線を接続することで，遠隔からログイン可能ですが，基本的には遠隔からのログインを行うことはできません。

(2) 通信用ポート

NIF 通信用ポートを介して，遠隔のリモート運用端末からの本装置に対するログイン，SNMP マネージャによるネットワーク管理を行うことができます。このポートを介して telnet や ftp による本装置へログインするためには，本装置のコンフィグレーションで IP アドレスおよびリモートアクセスの設定を行う必要があります。このポートを介して，待機系 BCU へのログインはできません。

(3) RM イーサネット (SB-5400S ではリモートマネージメントポート)

通信用ポートと同様な運用が可能ですが，IPv6 による通信を行うことができません。

(4) メンテナンスポート【SB-5400S】

メンテナンスポートではリモート運用端末を接続して，コンフィグレーションの設定なしに本装置の運用系 BCU および待機系 BCU へログインすることができます。BCU0 のメンテナンスポートには 192.168.0.1/24，BCU1 のメンテナンスポートには 192.168.0.2/24 の IP アドレスを自動で割り付けます。メンテナンスポートに割り付けられる IP アドレスはほかの通信ポートとは装置内で別管理となりますので，ほかのインタフェースにメンテナンスポートと同一のネットワークアドレスや IP アドレスを割り当てても問題ありません。ただし，経路情報の設定は行うことができませんので，ルータ越えを伴う別サブネットワークに属する遠隔のリモート運用端末から，このポートを介してログインすることはできません。また，このポートからほかの通信ポートへ IP 中継も行いません。

このポートでは IP アドレスによるアクセス制限を行いません。そのため，セキュリティ上，常時ネットワークに接続して運用するのではなく，本装置へのログイン時にリモート運用端末をクロスケーブルで直結して接続し，ログアウト後にはケーブルを抜くような運用を推奨いたします。メンテナンスポートでのサポート機能を次の表に示します。

表 14-5 メンテナンスポートのサポート機能

機能	解説
telnet によるログイン	リモート運用端末から本装置へ telnet でログインするこができます（ただし，本装置からリモート運用端末へ telnet でログインすることはできません)。
ftp によるログイン	リモート運用端末から本装置へ ftp でログインするこができます（ただし，本装置からリモート運用端末へ ftp でログインすることはできません)。
ping 応答	リモート運用端末から実行した ping コマンドに対して本装置が応答することができます（ただし，本装置から ping コマンドを実行することはできません)。
ARP	運用コマンドで，このポートで学習した ARP エントリの表示および削除を行うことができます（ただし，スタティック ARP を設定することはできません)。
IP アドレス設定	自動的に以下の IP アドレスを割り付けます。 BCU0: 192.168.0.1/24 BCU1: 192.168.0.2/24 この IP アドレスはコンフィグレーションにて変更可能です。
保守機能	以下の保守機能があります。 • 運用状態を show ip interface コマンドで確認できます。 • tcpdump コマンドでパケットのモニタができます。 • 回線テストを行うことができます。

14.1.3 ホスト名情報

本装置ではネットワーク上の装置を識別するためにホスト名情報を定義できます。定義したホスト名情報は本装置のログ情報，NTP 情報などのコンフィグレーションを行うときにネットワーク上の他装置を指定する名称として使用できます。

本装置で使用するホスト名情報は次に示す方法で定義できます。

- コンフィグレーションコマンド hosts で個別に指定する方法
- DNS リゾルバ機能 (コンフィグレーションコマンド dns-resolver) を使用してネットワーク上の DNS サーバに問い合わせる方法

コンフィグレーションコマンド hosts を使用して定義する場合には使用するホスト名ごとに IP アドレスとの対応を明示的に定義する必要があります。

DNS リゾルバを使用する場合にはネットワーク上の DNS サーバで管理されている名称を問い合わせて参

照するため，本装置で参照するホスト名ごとに IP アドレスを定義する必要がなくなります。

本装置の DNS リゾルバ機能は RFC1034 および RFC1035 に準拠しています。

14.2 立ち上げ

本章は本装置の立ち上げについての仕様および使用する上での注意点を中心に説明します。

14.2.1 立ち上げおよび再起動

(1) 立ち上げ【SB-7800S】

本装置は，まず MC から BCU 用ソフトウェアをローディングして BCU の運用を開始したあとで，PSU の運用を開始します。2 枚の MC がスロットに実装されている場合は，一方のスロット (通常はスロット 0) で立ち上げを行いますが，起動に失敗したときには自動的に他方 (通常はスロット 1) での立ち上げに切り替わります。また，PSU の運用開始には PSU 初期導入と定常運用の 2 種類の立ち上げ処理があり，それぞれで動作が異なります。

(a) PSU 初期導入

本装置では PSU 導入時に PSU のフラッシュメモリにソフトウェアが書き込まれていない場合，または現在の運用バージョンと異なるバージョンのソフトウェアが書き込まれている場合は，自動的に PSU 用ソフトウェアを同 PSU に書き込みます。書き込まれたソフトウェアは通常 PSU の障害が発生しないかぎり消えることはありません。この書き込み処理のために PSU のフラッシュメモリ上のソフトウェアで起動する定常運用時よりも初期化時間が長くかかります。装置として初期化にかかる時間は PSU の実装枚数に依存します。

(b) 定常運用

定常運用状態での立ち上げは，PSU 初期導入時に行う PSU へのソフトウェアの書き込み処理がないため，個々の PSU は独立して初期化処理を行います。初期化にかかる時間は PSU の実装枚数にほとんど影響を受けません。

(2) 立ち上げ【SB-5400S】

本装置は，まず MC から BCU 用ソフトウェアをローディングして BCU の運用を開始したあとで，BSU の運用を開始します。2 枚の MC がスロットに実装されている場合は，一方のスロット (通常はスロット 0) で立ち上げを行いますが，起動に失敗したときには自動的に他方 (通常はスロット 1) での立ち上げに切り替わります。また，BSU の運用開始には BSU 初期導入と，BSU のフラッシュメモリ上のソフトウェアで起動する定常運用の 2 種類の立ち上げ処理があり，それぞれで動作が異なります。

(a) BSU 初期導入

本装置では BSU 導入時に BSU のフラッシュメモリにソフトウェアが書き込まれていない場合，または現在の運用バージョンと異なるバージョンのソフトウェアが書き込まれている場合は，自動的に BSU 用ソフトウェアを同 BSU に書き込みます。書き込まれたソフトウェアは通常 BSU の障害が発生しないかぎり消えることはありません。この書き込み処理のために，定常運用時よりも初期化時間が長くかかります。

(b) 定常運用

定常運用状態での立ち上げは，BSU 初期導入時に行う BSU へのソフトウェアの書き込み処理がありません。

(3) 再起動

本装置の再起動には管理者が手動で行う再起動と装置が自立して行う自動再起動があります。

(a) マニュアル再起動

管理者はコマンドを使用するか，装置上のリセットスイッチを操作することで本装置の再起動を行えます。

(b) 障害回復による再起動

本装置に重度の障害が発生した場合は，装置は自動的に障害復旧のために再起動を行います。詳細は「14.10　障害時の復旧および情報収集」を参照してください。

14.2.2　自己診断テスト

本装置では立ち上げ時に，BCU と PSU または BSU で自己診断テスト(ハードウェアの診断)をします。ハードウェアに異常が発見された場合は，種別ログを採取します。BCU または BSU で障害を検出した場合，冗長構成の時は系切替をします。また，PSU で障害を検出した場合，障害検出した PSU 以外は立ち上がります。

14.3 ログイン制御

本装置にはローカルログイン (RM シリアル接続) と IP および IPv6 ネットワーク経由のリモートログイン機能が (rlogin または telnet) あります。

14.3.1 ログイン制御

本装置ではログイン時およびログイン中に次に示す制御を行っています。

1. 複数の運用端末から同時にログインできます。
2. コマンド実行結果はログインした端末だけに表示します。運用メッセージはログインしているすべての運用端末に表示されます。
3. キー入力が最大 60 分間ない場合は自動的にログアウトします。
4. killuser コマンドを使用してユーザを強制ログアウトできます。
5. ログイン時に不正アクセスを防止するためパスワードによるチェックやユーザ ID によるコマンドの使用範囲の制限を設けています。
6. 入力したコマンドとその応答メッセージおよび運用メッセージを運用ログとして収集します。運用ログは show logging コマンドで参照できます。
7. ログインできるリモートユーザ数は 10 ユーザです。ただし，コンソールや AUX ポートからのログインユーザ数はこの数に含みません。
8. コンフィグレーションでログインできるリモートユーザ数を制限できます。ただし，コンソールや AUX ポートからのログインはユーザ数制限の対象としません。
9. 本装置にアクセスできるプロトコル (telnet，rlogin，ftp) をコンフィグレーションで制限できます。

14.3.2 ログインセキュリティ制御

(1) ユーザ ID 管理

ユーザ ID を adduser コマンドで作成できます。また，rmuser コマンドで削除できます。

システムが二重化運用されている場合，待機系の現用 MC に自動的にアカウントの同期を行います。また，運用系および待機系に予備 MC が実装されている場合，確認後アカウントの同期を行います。

(2) パスワード管理

本装置ログイン時のコマンドレベルの制御およびセキュリティレベル機能としてパスワードによるアクセス権制御機能を持ちます。パスワードは運用端末から本装置を操作する場合のアクセス制限と認証に使用します。パスワードは password コマンドによって変更できるので，セキュリティのために，定期的に変更されることをお勧めします。

システムが冗長構成で運用されている場合，待機系の現用 MC に自動的にパスワードの同期を行います。また，運用系および待機系に予備 MC が実装されている場合，確認後パスワードの同期を行います。

(3) アクセスできる端末の制限

リモート運用端末から本装置へアクセス制限を行います。アクセスを許可するリモート運用端末の IP アドレスおよびサブネットマスク，または IPv6 アドレスおよびプレフィックスをコンフィグレーションに登録し，登録外の端末からの使用を防止します。なお，サブネットマスクおよびプレフィックスは省略できます。アクセス許可するアドレスは IP と IPv6 を合計して最大 128 個登録できます。なお，初期導入時にはリモート運用端末からのアクセスができない設定になっています。

14.4 コンフィグレーション

本装置にはネットワークの運用環境に合わせて，構成および動作条件などのコンフィグレーションを定義しておく必要があります。初期導入時はコンフィグレーションを定義していません。

14.4.1 コンフィグレーションの内容

コンフィグレーションファイルに定義できるコンフィグレーションの一覧を次の表に示します。

表 14-6 コンフィグレーション一覧

情報グループ名	内容
装置管理情報	装置名，設置場所などの管理情報 リモート運用端末の IP アドレス，IPv6 アドレス定義
SNMP 情報	コミュニティ名，SNMP マネージャアドレスなどの SNMP セッションに関する定義 SNMP エンジン ID，SNMP セキュリティユーザ，SNMP ビュー，SNMP グループなどの SNMPv3 に関する定義 リアルタイムモニタに関する定義
回線 (Line) 情報	回線の種別，回線速度などのレイヤ 1 の定義 リンクアグリゲーション機能の定義 Tag-VLAN 連携機能の定義
リンクレイヤプロトコル情報 **【SB-7800S】**	PPP プロトコルの各種パラメータ定義（レイヤ 2 の情報）
トンネル情報	トンネルインタフェースに関する定義
レイヤ 2 スイッチ情報	VLAN 機能の定義 FDB 機能の定義 スパニングツリー機能の定義 GSRP 機能の定義
IP インタフェース情報	IPv4 アドレスやスタティック ARP の定義 IPv6 アドレスやスタティック NDP，RA の定義 IP パケットフィルタリングに関する定義 アドレス変換機能に関する定義
IP ルーティングプロトコル情報	RIP，OSPF，BGP，RIPng，OSPFv3，BGP4+，IS-IS のプロトコルに関する定義 スタティックルーティングに関する定義
IP マルチキャストルーティングプロトコル情報	PIM-DM，PIM-SM，DVMRP，IGMP のプロトコルに関する定義
フロー情報	フロー制御に関する定義
QoS 情報	最低帯域保証などのサービス品質保証 (QoS) に関する定義
デフォルト情報	コンフィグレーション※での初期値に関する定義
VRRP 情報	VRRP に関する定義
RA 情報	RA に関する定義
ホスト名情報	ホスト名称に関する定義
ログ情報	ログの運用方法に関する定義
NTP 情報	NTP に関する定義
Disable 情報	H ／ W ボードの閉塞に関する定義

注※ 装置管理情報，SNMP 情報，回線 (Line) 情報，リンクレイヤプロトコル情報**【SB-7800S】**，トンネル情報，レ

イヤ 2 スイッチ情報，IP インタフェース情報，IP ルーティングプロトコル情報，IP マルチキャストルーティングプロトコル情報，フロー情報の各コンフィグレーションを示します。

14.4.2 コンフィグレーションファイルの種類

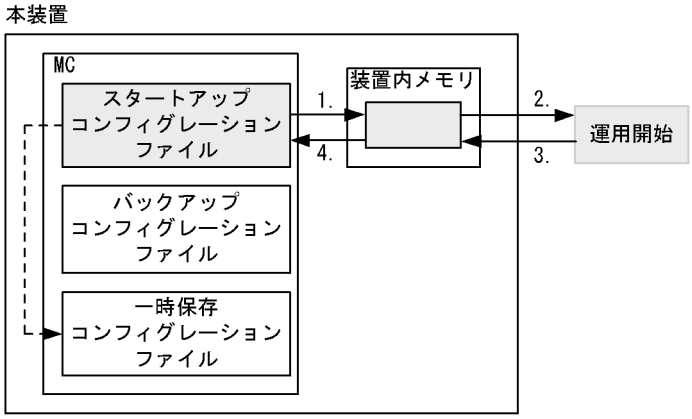
本装置はインタフェース中継機能の動作条件などをコンフィグレーションとしてテキストファイル形式で MC に記憶します。コンフィグレーションには次に示すファイルの種類があります。

- **スタートアップコンフィグレーションファイル**
  本装置の立ち上げ時に使用し，そのコンフィグレーションに従って運用されます。
- **バックアップコンフィグレーションファイル**
  スタートアップコンフィグレーションファイルのコピーまたは将来のネットワークの変更に備えた編集用コンフィグレーションとして利用します。
- **一時保存コンフィグレーションファイル**
  運用中にコンフィグレーションを変更して MC に格納した場合に，編集前のスタートアップコンフィグレーションファイルを一時保存したファイルです。
  本装置の電源投入時，スタートアップコンフィグレーションファイルが正しく読み出せない場合は，一時保存コンフィグレーションファイルで運用を開始します。

14.4.3 コンフィグレーションの運用方法

コンフィグレーションの運用方法を次の図に示します。

図 14-3 コンフィグレーションの運用方法



1. 本装置を起動すると，MC内のスタートアップコンフィグレーションファイルの内容が装置内メモリにロードされる。
2. 装置内メモリの内容で運用を開始する。
3. コンフィグレーションが変更された場合は，装置内メモリのコンフィグレーションを編集する。
4. 変更されたコンフィグレーションをMCに格納する。
   このとき，編集前のスタートアップコンフィグレーションファイルの内容を一時保存コンフィグレーションファイルとして保存する。

MC 故障に備えてリモート運用端末にコンフィグレーションファイルのバックアップを取ることをお勧めします。本装置は MC1 枚でも運用できますが，運用中に MC が故障した場合には，リモート装置にアクセスするためのコンフィグレーションの設定，バックアップコンフィグレーションファイルの転送などに時間がかかり，迅速に復旧できません。迅速に復旧させるために MC は 2 枚で運用することをお勧めします。

MC を 2 枚で運用した場合，コンフィグレーションを編集したあとに必ず運用コマンドの copy mc コマン

ドを使用して，現用スロットから予備スロットにコピーすることをお勧めします。これは，本装置は MC 故障時にブートする MC を自動的に切り替えることができますが，現用スロットのコンフィグレーションファイルより予備スロットのコンフィグレーションファイルが古い場合には，故障後に古いコンフィグレーションに従って運用するためです。

14.4.4　コンフィグレーションの表示と編集

（1） 表示

コンフィグレーションコマンドの show コマンドでコンフィグレーションを表示できます。また，MC に格納したコンフィグレーションファイルは運用コマンドの cat コマンドで表示することもできます。

（2） 編集

本装置は導入時および運用中のネットワーク構成変更時に使用するコンフィグレーションの編集機能を持ちます。スタートアップコンフィグレーションおよびバックアップコンフィグレーションは共に同一の操作で編集できます。

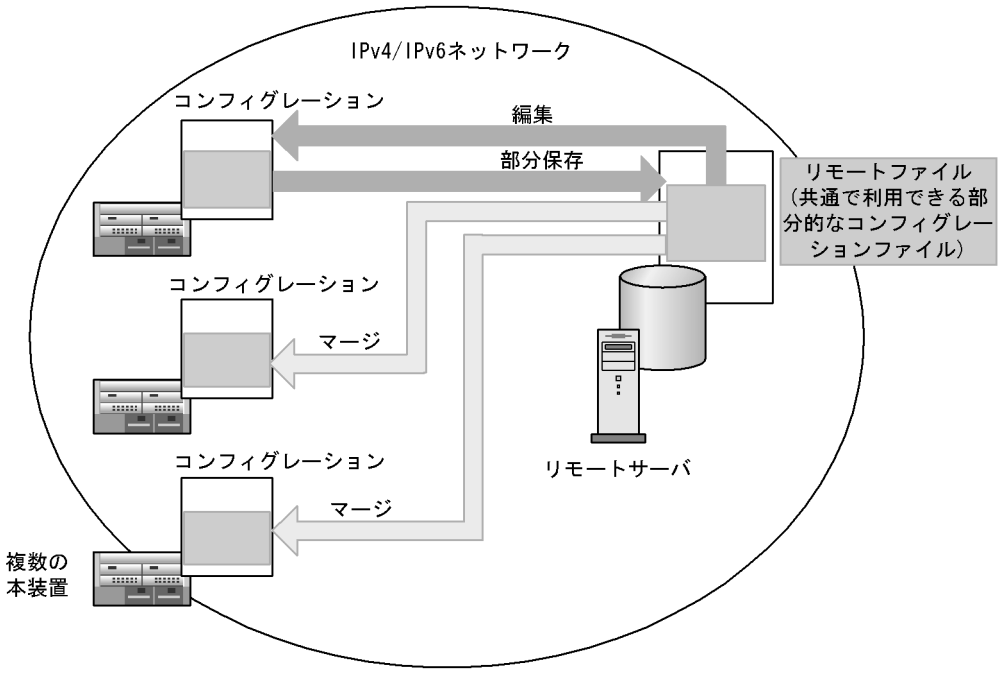
14.4.5　リモートサーバを利用したコンフィグレーションの編集・管理

複数の本装置でコンフィグレーションの編集を行う場合などに，リモートサーバ上に保存されたコンフィグレーションファイルを直接利用して便利に編集できます。以下に例を示します。

（1） コンフィグレーションファイルの共通利用例

あらかじめ，ある本装置で，共通に利用できる部分的なコンフィグレーションファイルを作成し，リモートサーバへ保存しておきます。その後，複数の本装置でコンフィグレーションを編集する際，リモートサーバに保存されたコンフィグレーションファイルを直接読み込み，編集中のコンフィグレーションへマージすることで，共通部分の定義を行うことができます。コンフィグレーションファイルの共通利用例を次の図に示します。

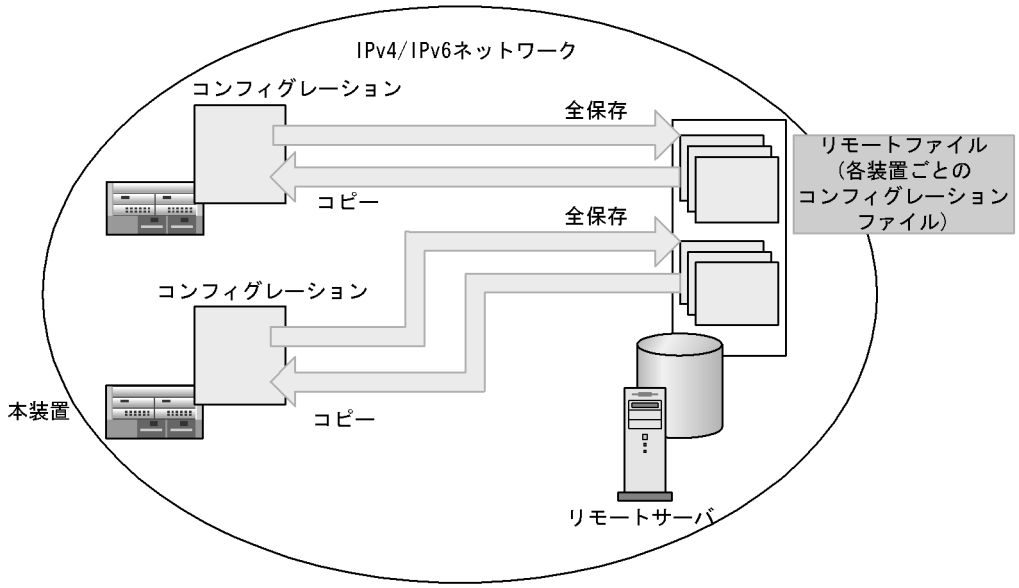
図 14-4　コンフィグレーションファイルの共通利用例



(2) コンフィグレーションの履歴管理例

各本装置で，スタートアップコンフィグレーションを作成した段階で，それをバックアップコンフィグレーションファイルとしてリモートサーバへ直接保存し，リモートサーバでその履歴を管理しておきます。その後，従来のコンフィグレーションへ戻したい場合，リモートサーバに保存されたバックアップコンフィグレーションファイルをスタートアップコンフィグレーションファイルへ直接コピーして反映させることができます。コンフィグレーションの履歴管理例を次の図に示します。

図 14-5 コンフィグレーションの履歴管理例



14.5 運用コマンド

本装置で使用できる運用コマンドとその用途を次の表に示します。各コマンドの詳細は，マニュアル「運用コマンドレファレンス Vol.1」および「運用コマンドレファレンス Vol.2」を参照してください。

表 14-7 運用コマンドとその用途

分 類	コマンド名称	機 能
モード切換	enable	装置管理者モードへのモード変更
	disable	装置管理者モードの終了
	quit(exit)	現在のコマンド入力モードの終了
	logout	装置ログアウト
	configure(configure terminal)	コンフィグレーションモードへのモード変更
	end	コンフィグレーションモードの終了
ログインユーザ管理	adduser	新規ユーザの追加
	rmuser	ユーザの削除
	password	パスワード設定 / 変更
	clear password	パスワード削除
	show sessions	ログインしている全ユーザの表示
	show whoami	ログインしている自ユーザの表示
	killuser	指定ユーザの強制ログアウト
ターミナル	set terminal warning-level	「警告がある旨のメッセージ」出力レベル設定
	set exec-timeout	「自動ログアウト」実行までの時間設定
	set terminal command-literal	CLI 運用コマンドコマンド入力モード変更
	set terminal help	ヘルプメッセージで表示するコマンド一覧の設定
	set terminal pager	ページング処理の有無設定
	show history	コマンド履歴表示
	stty	端末属性表示
リモート操作	telnet	他装置への遠隔ログイン
	rlogin	他装置への遠隔ログイン
	ftp	ファイル転送
ソフトウェア管理	show version	バージョン表示
	ppupdate	S ／ W のバージョンアップ
	ftpbackup	ftp サーバへのソフトウェア保存
	ftprestore	ftp サーバからのソフトウェア回復
	synchronize	MC の内容をコピー
MC 保守	copy mc	MC のコピー
	format mc	MC の初期化
	show mc	MC の情報表示
	set mc disable	MC のアクセス禁止
	set mc enable	MC のアクセス禁止解除
ファイル操作	show running-config(show configuration)	ランニングコンフィグレーションの表示

分 類	コマンド名称	機　能
	show startup-config	スタートアップコンフィグレーションファイルの表示
	copy running-config	ランニングコンフィグレーションのコピー
	copy startup-config	スタートアップコンフィグレーションファイルのコピー
	copy backup-config	バックアップコンフィグレーションファイルのコピー
	copy merge-config	MC のスタートアップコンフィグレーションファイルにマージ
	erase startup-config	スタートアップコンフィグレーションファイルの全削除
	show file	ローカルまたはリモートサーバ上のファイルの内容と行数の表示
	cd	カレントディレクトリ移動
	pwd	カレントディレクトリのパス名の表示
	ls	ディレクトリ内容の表示
	dir	MC ファイルの表示
	cat	ファイルの連結・出力
	cp	ファイルのコピー
	mkdir	ディレクトリの作成
	mv	ファイルの移動，ファイル名の変更
	rm	ファイルの削除
	rmdir	ディレクトリの削除
	delete	回復可能な MC ファイルの削除
	undelete	回復可能な MC 上の削除ファイルの回復
	squeeze	回復可能な MC 上の削除ファイルの消去
	chmod	ファイルの許可モード変更
	zmodem	RS232C でのファイル転送
ユーティリティ	diff	テキストファイル間の行内容の相違表示
	grep	ファイルからのパターン検索
	egrep	ファイルからの拡張パターン検索
	fgrep	ファイルからの固定文字列検索
	more	テキストファイルの表示，ページング
	less	テキストファイルの表示，ページング
	vi	テキストエディタ
	sort	ファイルのソート
	tail	ファイルの最後の部分の表示
	hexdump	ヘキサダンプ表示
装置管理	show system	装置運用状態 / 統計情報表示
	clear counters system	装置に実装されている全 NIF 配下の統計情報カウンタクリア
	clear control-counter	リトライカウンタのクリア
	show power-supply	電圧表示
	show environment【SB-5400S】	シャーシの運用状態表示

分 類	コマンド名称	機　能
	reload	再立ち上げ
	close rmEthernet【SB-7800S】	RM イーサネット閉塞状態指示
	close mgmtPort【SB-5400S】	リモートマネージメントポート閉塞状態指示
	free rmEthernet【SB-7800S】	RM イーサネット閉塞状態解除
	free mgmtPort【SB-5400S】	リモートマネージメントポート閉塞状態解除
	test interfaces rmEthernet【SB-7800S】	RM イーサネット回線テスト開始
	test interfaces mgmtPort【SB-5400S】	リモートマネージメントポート回線テスト開始
	no test interfaces rmEthernet【SB-7800S】	RM イーサネット回線テスト終了
	no test interfaces mgmtPort【SB-5400S】	リモートマネージメントポート回線テスト終了
	close maintenance【SB-5400S】	メンテナンスポートを一時的に運用状態から閉塞状態に設定
	free maintenance【SB-5400S】	一時的に設定したメンテナンスポートの閉塞状態を運用状態に変更
	test interfaces maintenance【SB-5400S】	メンテナンスポートの回線テスト開始
	no test interfaces maintenance【SB-5400S】	メンテナンスポートの回線テスト終了
	show tech-support	本装置の保守情報採取
	show tcpdump (tcpdump)	パケットモニタリングコマンド
	ttcp	2 点間の TCP/UDP レベルでのスループットの計測
	show psu resources【SB-7800S】	PSU の H/W テーブルエントリ数表示
	show bsu resources【SB-5400S】	BSU の H/W テーブルエントリ数表示
PSU/BSU/NIF 管理	close psu【SB-7800S】	PSU を運用状態から閉塞状態に設定
	close bsu【SB-5400S】	BSU を運用状態から閉塞状態に設定
	free psu【SB-7800S】	PSU の閉塞状態を解除
	free bsu【SB-5400S】	BSU の閉塞状態を解除
	show psu information【SB-7800S】	PSU の CAM データリカバリ回数表示
	show bsu information【SB-5400S】	BSU の CAM データリカバリ回数表示
	show nif	NIF 運用情報
	clear counters nif	統計情報カウンタクリア
	show nif(POS)【SB-7800S】	POS の NIF 運用情報
	clear counters nif(POS)【SB-7800S】	POS の NIF 配下の統計情報カウンタクリア
	close nif	NIF を運用状態から閉塞状態に設定
	free nif	NIF の閉塞状態を解除
メッセージ・ログ	show logging	運用ログ表示

分 類	コマンド名称	機　　能
	clear logging	運用ログ消去
	show logging console	システムメッセージレベル表示
	set logging console	システムメッセージレベル設定
	show warning	警告メッセージ表示
アカウンティング情報	show accounting	アカウンティング情報の表示
	clear accounting	アカウンティング統計情報のクリア
	restart accounting	アカウンティングプログラムの再起動
	dump protocols accounting	アカウンティングプログラムで採取している情報のファイル出力
リソース情報	show rm cpu	RM CPU 使用率表示
	show cp cpu	CP CPU 使用率 / バッファ使用率表示
	show cp buffer	CP バッファ統計情報の表示
	clear cp buffer	CP バッファ統計情報カウンタクリア
	show processes	プロセス情報表示
	show memory	メモリ情報表示
	df	ディスクの空き容量表示
	du	ディスクの使用容量表示
CP 保守情報	show trace	CP トレース表示
	debug trace	CP トレース採取開始
	no debug trace	CP トレース採取停止
	clear trace	CP トレース消去
	show trace frame	フレームのトレース表示
	debug trace frame	フレームのトレース採取開始
	no debug trace frame	フレームのトレース採取停止
	clear trace frame	フレームのトレース消去
	show register	CP/PSU(SB-5400S では BSU) レジスタ内容表示
	set register	CP/PSU(SB-5400S では BSU) レジスタ内容設定
	show cp congestion-control	CP の輻輳制御情報の表示
	clear cp congestion-control	CP の輻輳制御情報のクリア
	no cp congestion-control	回線の輻輳制御状態を運用状態に戻す
ダンプ情報	dump cp	CP ダンプ採取
	dump psu【SB-7800S】	PSU ダンプ採取
	dump bsu【SB-5400S】	BSU のメモリダンプ情報採取
	dump nif	NIF ダンプ採取
	set dump	CP/PSU(SB-5400S では BSU) ダンプ採取範囲設定
	show dump status	CP/PSU(SB-5400S では BSU) ダンプ採取範囲表示
	erase dumpfile	ダンプファイル消去
	show dumpfile	ダンプファイル一覧表示
時刻管理	show calendar	日付・時間の表示

分 類	コマンド名称	機　　能
	set calendar	日付・時間の設定
	rdate	日付・時間をリモートホストから設定
	show ntp status	ntp サーバの状態表示
	restart ntp	ntp サーバの再初期化
イーサネット	show interfaces	回線運用状態 / 統計情報表示
	clear counters	回線統計情報カウンタクリア
	show port	装置に実装されたイーサネットポート情報の一覧表示
	show port statistics	装置に実装された回線の送受信パケット数および廃棄パケット数の表示
	show port transceiver	着脱可能トランシーバ対応ポートのトランシーバ実装有無，種別，識別情報の一覧表示
	show vlan	Tag-VLAN 連携回線の統計表示
	show vlans	全 Tag-VLAN 連携回線の統計表示
	clear counters	Tag-VLAN 連携回線の統計情報カウンタクリア
	clear vlan statistics	全 Tag-VLAN 連携回線の統計情報カウンタクリア
	close	閉塞状態指示
	free	閉塞状態解除
	test interfaces	回線テスト開始
	no test interfaces	回線テスト終了
リンクアグリゲーション情報	show link-aggregation	リンクアグリゲーション情報表示
	show link-aggregation statistics	リンクアグリゲーション統計情報表示
	clear link-aggregation statistics lacp	リンクアグリゲーション統計情報クリア
	restart link-aggregation	リンクアグリゲーションプログラム再起動
	dump protocols link-aggregation	リンクアグリゲーションダンプ情報収集
POS	show interfaces(POS) **【SB-7800S】**	POS 回線の運用状態 / 統計情報表示
	clear counters(POS) **【SB-7800S】**	POS 回線の統計情報カウンタクリア
	show port statistics(POS) **【SB-7800S】**	装置に実装された POS 回線の送受信パケット数および廃棄パケット数の表示
	close(POS)**【SB-7800S】**	POS インタフェースの閉塞状態指示
	free(POS)**【SB-7800S】**	POS インタフェースの閉塞状態解除
	show trace ppp**【SB-7800S】**	PPP 制御パケットトレース情報の表示
	clear trace ppp**【SB-7800S】**	PPP 制御パケットトレース情報のクリア
	debug trace ppp**【SB-7800S】**	PPP 制御パケットの採取開始
	no debug trace ppp**【SB-7800S】**	PPP 制御パケットの採取停止
	show trace ppp history **【SB-7800S】**	PPP 制御パケットトレース履歴情報の表示
	test interfaces(POS) **【SB-7800S】**	POS 回線テスト開始

分 類	コマンド名称	機　能
	no test interfaces(POS) **【SB-7800S】**	POS 回線テスト終了
全インタフェース	show interface	全インタフェース運用状態 / 統計情報表示
VLAN 情報	show vlan	VLAN 情報表示
	show vlan mac-vlan **【SB-7800S】**	MAC VLAN に登録されている MAC アドレスの表示
	show vlan private-vlan	プライベート VLAN の対応関係表示
	show vlan traffic	VLAN 統計情報表示
	clear vlan traffic	VLAN 統計情報クリア
	restart vlan	VLAN プログラム再起動
	dump protocols vlan	VLAN ダンプ情報収集
FDB 情報	show fdb	FDB 情報表示
	clear fdb	FDB 情報クリア
スパニングツリープロトコル情報	show spanning-tree	スパニングツリープロトコル情報表示
	show spanning-tree statistics	スパニングツリープロトコル統計情報表示
	clear spanning-tree statistics	スパニングツリープロトコル統計情報クリア
	clear spanning-tree detected-protocol	スパニングツリーの STP 互換モードの強制回復
	show spanning-tree port-count	スパニングツリーの収容数を表示
	restart spanning-tree	スパニングツリープロトコルプログラム再起動
	dump protocols spanning-tree	スパニングツリープロトコルダンプ情報収集
IGMP/MLD snooping 情報	show igmp-snooping	IGMP snooping 情報表示
	clear igmp-snooping	IGMP snooping 情報クリア
	show mld-snooping	MLD snooping 情報表示
	clear mld-snoopingt	MDL snooping 情報クリア
	restart snooping	snooping プログラム再起動
	dump protocols snooping	イベントトレース情報および制御テーブル情報のファイル出力
IPv4 ネットワーク情報	show ip-dual interface(IPv4)	ネットワークインタフェース・パラメータの表示
	show ip interface	IPv4 ネットワークインタフェース・パラメータの表示
	clear counters null-interface(IPv4)	NULL インタフェース廃棄パケット数カウンタクリア
	ping	エコーテスト
	traceroute	ルート表示
	show ip arp	ARP 表示
	clear arp-cache	ARP 削除
	show netstat(netstat)(IPv4)	ネットワークのステータス表示
	clear netstat(IPv4)	ネットワーク統計情報カウンタクリア
	clear tcp(IPv4)	TCP コネクションの切断

分 類	コマンド名称	機　能
	show filter-flow(IPv4)	フローフィルタ統計情報表示
	clear filter-flow(IPv4)	フローフィルタ統計情報カウンタクリア
	show ip-dual policy(IPv4)	指定インタフェース名称のポリシールーティング条件定義済みフィルタリスト番号表示
	show ip-dual local policy(IPv4)	指定インタフェース名称のポリシールーティング条件，出力先情報表示
	show ip-dual cache policy(IPv4)	ポリシーグループ情報の表示
	show ip policy	ポリシールーティング条件定義済みフィルタリスト番号表示
	show ip local policy	ポリシールーティング条件，出力先情報表示
	show ip cache policy	ポリシーグループ情報の表示
	show dhcp traffic	DHCP サーバの統計情報の表示
	clear dhcp traffic	DHCP サーバの統計情報カウンタクリア
	show dhcp giaddr	インタフェースに対する giaddr 情報の表示
	show ip dhcp binding	DHCP サーバ上の結合情報の表示
	clear ip dhcp binding	DHCP サーバのデータベースから自動連結アドレスを削除
	show ip dhcp import	DHCP サーバのコンフィグレーションで設定されたオプション / パラメータ値の表示
	show ip dhcp conflict	DHCP サーバによって検出した矛盾 IP アドレスの表示
	clear ip dhcp conflict	DHCP サーバから矛盾 IP アドレスを削除
	show ip dhcp server statistics	DHCP サーバの統計情報の表示
	clear ip dhcp server statistics	DHCP サーバの統計情報をリセット
	restart dhcp	DHCP サーバデーモンプロセスの再起動
	dump protocols dhcp	DHCP サーバプログラムで採取しているサーバのログおよびパケットの送受信ログのファイル出力
	dhcp server monitor	DHCP サーバで送受信するパケットの送受信ログの採取開始
	no dhcp server monitor	DHCP サーバプログラムでのパケットの送受信ログの採取停止
	show dns-relay	DNS リレーの動作状況表示
	clear counters dns-relay	DNS リレーのエラー統計情報カウンタクリア
IPv6 ネットワーク情報	show ip-dual interface(IPv6)	ネットワークインタフェース・パラメータの表示
	show ipv6 interface	IPv6 ネットワークインタフェース・パラメータの表示
	clear counters null-interface(IPv6)	NULL インタフェース廃棄パケット数カウンタクリア
	show interface	トンネルインタフェース運用状態 / 統計情報表示
	clear counters	トンネルインタフェース統計情報カウンタクリア
	ping ipv6	ICMP6 エコーテスト
	traceroute ipv6	IPv6 経由ルートの表示
	show ipv6 neighbors	NDP 表示

分 類	コマンド名称	機　能
	clear ipv6 neighbors	ダイナミック NDP 情報クリア
	show netstat(netstat)(IPv6)	ネットワークのステータス表示
	clear netstat(IPv6)	ネットワーク統計情報カウンタクリア
	clear tcp(IPv6)	TCP コネクションの切断
	show filter-flow(IPv6)	フローフィルタ統計情報表示
	clear filter-flow(IPv6)	フローフィルタ統計情報カウンタクリア
	show ip-dual policy(IPv6)	指定インタフェース名称のポリシールーティング条件定義済みフィルタリスト番号表示
	show ip-dual local policy(IPv6)	指定インタフェース名称のポリシールーティング条件，出力先情報表示
	show ip-dual cache policy(IPv6)	ポリシーグループ情報の表示
	show ipv6 policy	フィルタリスト番号表示
	show ipv6 local policy	ポリシールーティング条件，出力先情報表示
	show ipv6 cache policy	ポリシーグループ情報の表示
	show ipv6 dhcp binding	IPv6 DHCP サーバの結合情報表示
	clear ipv6 dhcp binding	IPv6 DHCP サーバの結合情報削除
	show ipv6 dhcp server statistics	IPv6 DHCP サーバの統計情報表示
	clear ipv6 dhcp server statistics	IPv6 DHCP サーバの統計情報カウンタクリア
	set ipv6-dhcp server duid	プライマリ MC 上の DHCP サーバ DUID ファイルの設定
	show ipv6-dhcp server duid	プライマリ MC 上の DHCP サーバ DUID ファイルの表示
	erase ipv6-dhcp server duid	プライマリ MC 上の DHCP サーバ DUID ファイルの削除
	restart ipv6-dhcp server	IPv6 DHCP サーバプログラム再起動
	dump protocols ipv6-dhcp server	IPv6 DHCP 情報のダンプ
	ipv6-dhcp server monitor	IPv6 DHCP サーバパケット送受信ログ採取開始
	no ipv6-dhcp server monitor	IPv6 DHCP サーバパケット送受信ログ採取終了
IPv4 ユニキャストルーティングプロトコル情報	show ip route	すべての経路の一覧表示
	show ip route-filter	IPv4 ユニキャスト経路のフィルタ結果の経路情報表示
	clear ip route	経路情報の再インストール，再評価
	show ip entry	特定経路の詳細情報の表示
	show ip rip	RIP プロトコル情報の表示
	clear counters rip ipv4-unicast	RIP プロトコル情報のクリア
	show ip ospf **【OP-OSPF(SB-5400S)】**	OSPF プロトコル情報の表示
	clear ip ospf **【OP-OSPF(SB-5400S)】**	OSPF プロトコル情報のクリア
	show ip bgp **【OP-BGP】**	BGP プロトコル情報の表示

分 類	コマンド名称	機　能
	clear ip bgp【OP-BGP】	BGP プロトコル情報のクリア BGP 経路の再広告／再学習
	show ip static	static 経路情報の表示
	clear ip static-gateway	static 経路情報のクリア
	show ip interface ipv4-unicast	IP ルーティングプログラムが認識するインタフェース情報の表示
	show isis【OP-ISIS】	IS-IS プロトコル情報の表示
	clear isis【OP-ISIS】	IS-IS プロトコル情報のクリア
	debug isis【OP-ISIS】	IS-IS プロトコル送受信パケットの表示
	show graceful-restart unicast(IPv4)【SB-7800S】	ユニキャストルーティングプロトコルの Graceful-Restart のリスタートルータの動作状態の表示
	show processes memory unicast(IPv4)	ユニキャストルーティングプログラムのメモリ使用状況の表示
	show processes cpu unicast(IPv4)	ユニキャストルーティングプログラムの CPU 使用率表示
	show processes task unicast(IPv4)	ユニキャストルーティングプログラムのタスク情報の表示
	show processes timer unicast(IPv4)	ユニキャストルーティングプログラムのタイマ情報の表示
	restart unicast(IPv4)	ユニキャストルーティングプログラムの再起動
	debug protocols unicast(IPv4)	ユニキャストルーティングプログラムのイベントログ情報表示の開始
	no debug protocols unicast(IPv4)	ユニキャストルーティングプログラムのイベントログ情報表示の停止
	debug ip	IP ルーティング・パケットのリアルタイム表示の制御
	dump protocols unicast(IPv4)	ユニキャストルーティングプログラムの制御テーブル情報・イベントトレース情報のダンプ採取
	erase protocol-dump unicast(IPv4)	ユニキャストルーティングプログラムの制御テーブル情報・イベントトレース情報・コア情報のダンプ削除
IPv4 マルチキャストルーティングプロトコル情報	show ip mcache	すべてのマルチキャスト経路の一覧表示
	show ip mstatic	マルチキャストの静的グループ加入情報表示
	show ip pim	PIM 情報の表示
	show ip mroute	PIM-SM マルチキャストルート情報の表示
	clear ip mroute	PIM-SM/SSM のマルチキャスト経路情報の消去
	show ip igmp	IGMP 情報の表示
	show ip dvmrp	DVMRP 情報の表示
	show ip rpf	PIM の RPF 情報の表示
	show ip multicast statistics	IPv4 マルチキャストの統計情報の表示
	clear ip multicast statistics	IPv4 マルチキャストの統計情報のクリア
	restart ipv4-multicast	IP マルチキャストルーティングプログラム（mrp）の再起動

分 類	コマンド名称	機　能
	dump protocols ipv4-multicast	DVMRP のイベントトレース情報および制御テーブル情報のダンプ採取
	erase protocol-dump ipv4-multicast	DVMRP のイベントトレース情報，制御テーブル情報，コアファイルのダンプ削除
IPv6 ユニキャストルーティングプロトコル情報	show ipv6 route	すべての経路の一覧表示
	show ipv6 route-filter	IPv6 ユニキャスト経路のフィルタ結果の経路情報表示
	clear ipv6 route	経路情報の再インストール，再評価
	show ipv6 entry	特定経路の詳細情報の表示
	show ipv6 rip	RIPng プロトコル情報の表示
	clear counters rip ipv6-unicast	RIPng プロトコル情報のクリア
	show ipv6 ospf **【OP-OSPF(SB-5400S)】**	OSPFv3 プロトコル情報の表示
	clear ipv6 ospf **【OP-OSPF(SB-5400S)】**	OSPFv3 プロトコル情報のクリア
	show ipv6 bgp **【OP-BGP】**	BGP4+ プロトコル情報の表示
	clear ipv6 bgp **【OP-BGP】**	BGP4+ プロトコル情報のクリア BGP4+ 経路の再広告／再学習
	show ipv6 static	static 経路情報の表示
	clear ipv6 static-gateway	static 経路情報のクリア
	show ipv6 routers	RA 情報の表示
	show ipv6 interface ipv6-unicast	IPv6 ルーティングプログラムが認識するインタフェース情報の表示
	show graceful-restart unicast(IPv6) **【SB-7800S】**	ユニキャストルーティングプロトコルの Graceful-Restart のリスタートルータの動作状態の表示
	show processes memory unicast(IPv6)	ユニキャストルーティングプログラムのメモリ使用状況の表示
	show processes cpu unicast(IPv6)	ユニキャストルーティングプログラムの CPU 使用率の表示
	show processes task unicast(IPv6)	ユニキャストルーティングプログラムのタスク情報の表示
	show processes timer unicast(IPv6)	ユニキャストルーティングプログラムのタイマ情報の表示
	restart unicast(IPv6)	ユニキャストルーティングプログラムの再起動
	debug protocols unicast(IPv6)	ユニキャストルーティングプログラムのイベントログ情報表示開始
	no debug protocols unicast(IPv6)	ユニキャストルーティングプログラムのイベントログ情報表示終了
	debug ipv6	IPv6 ルーティング・パケットのリアルタイム表示の制御
	dump protocols unicast(IPv6)	ユニキャストルーティングプログラムの制御テーブル情報・イベントトレース情報のダンプ採取
	erase protocol-dump unicast(IPv6)	ユニキャストルーティングプログラムの制御テーブル情報・イベントトレース情報・コア情報のダンプ削除

分 類	コマンド名称	機　能
IPv6 マルチキャストルーティングプロトコル情報	show ipv6 mcache	すべてのマルチキャスト経路の一覧表示
	show ipv6 pim	PIM 情報の表示
	show ipv6 mroute	PIM-SM マルチキャストルート情報の表示
	show ipv6 mld	MLD(IPv6 マルチキャストグループ) 情報の表示
	show ipv6 rpf	PIM の RPF 情報の表示
	show ipv6 multicast statistics	IPv6 マルチキャストの統計情報の表示
	clear ipv6 multicast statistics	IPv6 マルチキャストの統計情報のクリア
	restart ipv6-multicast	IPv6 マルチキャストルーティングプログラムの再起動
	debug protocols ipv6-multicast	IPv6 マルチキャストルーティングプログラムが出力するイベント情報の syslog 出力
	no debug protocols ipv6-multicast	IPv6 マルチキャストルーティングプログラムが出力するイベント情報の syslog 出力停止
	dump protocols ipv6-multicast	IPv6 マルチキャストルーティングプログラムで採取している制御テーブル情報・イベントトレース情報のダンプ採取
	erase protocol-dump ipv6-multicast	IPv6 マルチキャストルーティングプログラムが作成したイベントトレース情報ファイル，制御テーブル情報ファイル，コアファイルのダンプ削除
QoS 情報	show qos ip-flow	フロー QoS 統計情報表示
	clear qos ip-flow	フロー QoS 統計情報カウンタクリア
	show qos flow	特殊 IP フロー統計情報表示
	clear qos flow	特殊 IP フロー統計情報カウンタクリア
	show qos queueing	送受信インタフェースの出力優先度キュー毎の統計情報表示
	clear qos queueing	送受信インタフェースの出力優先度キュー毎の統計情報カウンタクリア
	show shaper【SB-7800S】	イーサネットシェーパ機能を持った送信インタフェースの優先度キュー毎の統計情報表示
	clear shaper【SB-7800S】	イーサネットシェーパ機能を持った送信インタフェースの優先度キュー毎の統計情報カウンタクリア
レイヤ 2 認証情報	show dot1x statistics	802.1X 認証に関わる統計情報の表示
	show dot1x	802.1X 認証に関わる状態情報の表示
	clear dot1x statistics	802.1X 認証に関わる統計情報の 0 クリア
	clear dot1x auth-state	802.1X 認証状態の初期化
	reauthenticate dot1x	802.1X 認証状態の再認証
	restart dot1x	802.1X プログラム再起動
	dump protocols dot1x	802.1X プログラムのダンプ情報収集
	show dot1x logging	802.1X プログラムで採取している動作ログメッセージの表示
	clear dot1x logging	802.1X プログラムで採取している動作ログメッセージのクリア
二重化管理	close standby	待機系 BCU を運用状態から閉塞状態に設定

分 類	コマンド名称	機　能
	free standby	待機系 BCU の閉塞状態を解除
	show mode	運用モード / 装置起動時の優先 MC/ 運用状態の表示
	set mode	運用モード / 装置起動時の優先 MC 設定
	clear mode	運用モード / 装置起動時の優先 MC 設定削除
	swap bcu	二重化 BCU の系切替
GSRP 情報	show gsrp	GSRP 情報表示
	show gsrp aware	GSRP aware 情報表示
	clear gsrp	GSRP 統計情報クリア
	set gsrp master	GSRP マスタ遷移
	clear gsrp port-up-delay	GSRP アクティブポート反映
	restart gsrp	GSRP プログラム再起動
	dump protocols gsrp	GSRP ダンプ情報収集
VRRP 情報	show vrrpstatus(IPv4)	VRRP の運用状態表示
	clear vrrpstatus(IPv4)	VRRP の統計情報カウンタクリア
	swap vrrp(IPv4)	自装置の状態遷移
	show vrrpstatus(IPv6)	VRRP の運用状態表示
	clear vrrpstatus(IPv6)	VRRP の統計情報カウンタクリア
	swap vrrp(IPv6)	自装置の状態遷移
IEEE802.3ah/UDLD	show efmoam	IEEE802.3ah/OAM の設定情報およびポートの状態を表示
	show efmoam statistics	IEEE802.3ah/OAM 統計情報を表示
	clear efmoam statistics	IEEE802.3ah/OAM 統計情報をクリア
	restart efmoam	IEEE802.3ah/OAM を再起動
	dump protocols efmaom	IEEE802.3ah/OAM 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
MIB 情報	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
	snmp get	指定した MIB の値を表示
	snmp getnext	指定した次の MIB の値を表示
	snmp walk	指定した MIB ツリーを表示
	snmp getif	interface グループの MIB 情報を表示
	snmp getroute	ipRouteTable（IP ルーティングテーブル）を表示
	snmp getarp	ipNetToMediaTable（IP アドレス変換テーブル）を表示
	snmp getforward	ipForwardTable（IP フォワーディングテーブル）を表示
	snmp rget	指定したリモート装置の MIB の値を表示
	snmp rgetnext	指定したリモート装置の次の MIB の値を表示
	snmp rwalk	指定したリモート装置の MIB ツリーを表示

分 類	コマンド名称	機　能
	snmp rgetroute	指定したリモート装置の ipRouteTable（IP ルーティングテーブル）を表示
	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
sFlow 統計	show sflow	フロー統計情報表示
	clear sflow statistics	フロー統計情報クリア
	restart sflow	フロー統計プログラム再起動
	dump sflow	フロー統計ダンプ情報収集
NetFlow 統計	show netflow	NetFlow 統計の情報を表示
	show netflow detail	NetFlow 統計の詳細情報を表示
	show netflow export	NetFlow 統計のコレクタ情報を表示
	show netflow sampling	NetFlow 統計のサンプリング情報を表示
	show netflow cache	NetFlow 統計の Active エントリ情報を表示
	clear netflow	NetFlow 統計の情報をクリア
	restart netflow	NetFlow 統計デーモンを再起動
	dump netflow	NetFlow 統計のダンプ情報を収集
LLDP 情報	show lldp	LLDP 情報表示
	show lldp statistics	LLDP 統計情報表示
	clear lldp	LLDP 隣接情報クリア
	clear lldp statistics	LLDP 統計情報クリア
	restart lldp	LLDP プログラム再起動
	dump protocols lldp	LLDP ダンプ情報収集
OADP 情報	show oadp	OADP/CDP の設定情報および隣接装置情報の表示
	show oadp statistics	OADP/CDP 統計情報の表示
	clear oadp	OADP の隣接装置情報クリア
	clear oadp statistics	OADP/CDP 統計情報クリア
	restart oadp	OADP プログラム再起動
	dump protocols oadp	OADP ダンプ情報収集

14.6 MC

本装置では本装置のソフトウェアおよびコンフィグレーションを MC に保持します。装置起動時はこの MC からソフトウェアをローディングし，コンフィグレーションに従って装置を初期化します。

装置起動を行った MC スロットを現用 MC，または起動 MC と呼び，/primaryMC のパスで現用 MC に対してアクセスを行うことができます。また，装置起動を行った MC スロットではないスロット側を予備 MC，またはバックアップ MC と呼び，/secondaryMC のパスで予備 MC に対してアクセスを行うことができます。

現用 MC 上にあるダンプファイルにアクセスする場合の例を，次の図に示します。

図 14-6 現用 MC のダンプファイルの確認

```
>ls -l /primaryMC/var/dump/
total 2536
-rwxr-xr-x 1 root wheel 2596411 Aug 19 16:04 rmdump
```

また，待機系 BCU の現用 MC 上にあるダンプファイルにアクセスする場合の例を，次の図に示します。

図 14-7 待機系現用 MC のダンプファイルの確認

```
>ls -l /standby/primaryMC/var/dump/
total 1496
-rwxr-xr-x 1 root wheel 1516998 Aug 17 13:25 cp00.000
```

MC の名称とパス名の対応を，次の表に示します。

表 14-8 MC の名称とパス名の対応

名称	パス名
MC スロット 1	/mc0
MC スロット 2	/mc1
現用 MC	/primaryMC
予備 MC(バックアップ MC)	/secondaryMC
待機系 BCU の現用 MC	/standby/primaryMC
待機系 BCU の予備 MC(バックアップ MC)	/standby/secondaryMC

14.6.1 バックアップ MC の運用

運用中に MC の故障が発生した場合には，本装置を起動できなくなります。また，MC の故障の状態によってはコンフィグレーションの再入力が必要になる場合があります。本装置では同一内容の 2 枚の MC を用意して BCU のスロット 0，スロット 1 の両方のスロットにそれぞれ MC を挿入して運用することで，一方の MC 障害時には自動的に装置がブートする MC を切り替えることができます。これによって，迅速な運用を再開できます。ただし，この場合に現用 MC と予備 MC のコンフィグレーションが不一致だと運用に支障をきたすので，常に copy mc コマンドでコピーしておくことをお勧めします。この時ログ情報なども copy mc コマンドを実行したときの時点の状態を予備 MC に保存できます。

二つの MC スロットに MC が実装されている場合，BCU の初期状態ではスロット 0 の MC を優先して起動するように設定されています。本装置では set mode コマンドによってこの優先して起動するスロットを変更できます。

14.6.2 優先 MC スロット指定機能

優先 MC スロット指定機能は，装置を起動するための優先 MC スロットを指定する機能です。優先 MC スロットの設定値は基本制御モジュール (BCU) 上に記憶され，電源の ON ／ OFF または MC の入れ替え時にも設定値は保持されます。ただし，基本制御モジュール (BCU) を交換した場合は再設定してください。

優先 MC スロット指定機能は起動する MC スロットの優先度を変更する機能であり，起動する MC スロットを固定する機能ではありません。このため，MC または MC スロットの障害時は，非優先の MC スロットに実装された MC で装置を起動します。

14.6.3 起動 MC スロットの選択機能

起動 MC スロットの選択機能は装置を起動する MC スロットを BCU の自己診断テスト後にコマンド入力によって選択できる機能です。コマンドを入力するためにはコンソールを接続して起動 MC スロットを指定する必要があります。また，確認メッセージ出力から 5 秒経過すると優先 MC スロットで指定された MC スロットで装置を自動的に起動します。起動 MC スロット選択モードの設定値は基本制御モジュール (BCU) 上に記憶され，電源の ON ／ OFF または MC の入れ替え時にも設定値は保持されます。ただし，基本制御モジュール (BCU) を交換した場合は再設定してください。本機能は装置の起動時間が最大 5 秒長くなります。

14.6.4 MC 保守コマンド

次に示すコマンドで MC を保守できます。サポートする保守機能を次に示します。

- MC のコピー　　: copy mc コマンド
- MC の初期化　　: format mc コマンド
- MC の情報表示　　: show mc コマンド
- MC のアクセス禁止　　: set mc disable コマンド
- MC のアクセス禁止解除 : set mc enable コマンド

14.7 管理情報の収集

14.7.1 時計および時刻情報

1. set calendar コマンドで時刻設定，show calendar コマンドで時刻表示ができます。
2. rdate コマンドで現在の時刻の設定をできます。rdate コマンドは遠隔のホストから時刻を得て，その時刻を本装置に設定するコマンドです。
3. NTP プロトコルを使用して，ネットワーク上の NTP サーバと時刻同期を行えます。本装置は RFC1305 NTP バージョン 3 に準拠しています。

14.7.2 装置およびインタフェース状態表示

(1) 管理情報表示コマンド

本装置の管理情報を表示する主な管理情報表示コマンドと表示する管理情報を次の表に示します。各コマンドの詳細についてはマニュアル「運用コマンドレファレンス Vol.1」および「運用コマンドレファレンス Vol.2」を参照してください。

表 14-9 管理情報表示コマンドと表示する管理情報

コマンド名	用途	表示する管理情報
show ip interface show ipv6 interface show ip-dual interface	IP インタフェースの状態および各インタフェースに対応するメディアの情報を表示します。	• インタフェース名 • インタフェースのステータス • IP アドレス • IPv6 アドレス • サブネットマスク • MAC アドレス
show system show nif show interfaces	system，nif，line など，本装置について指定された部位ごとの情報を表示します。	• 装置構成 • 装置 (部位) のステータス 表示項目は指定単位によって異なります。
show version	本装置に実装されているボードとソフトウェアについての情報を表示します。	• 実装されているボードの型名 • インストールされているソフトウェアのバージョン

(2) 装置の状態情報

装置の部位ごとの状態情報を次の表に示します。これらの管理情報は show system コマンド，show interfaces コマンド，および show nif コマンドで確認できます。

表 14-10 装置の部位ごとの状態情報

部位	状態情報	
	ステータス名称	意味
電源	active	運用中
	fault	障害
	disconnect	未実装
RM	active	運用系として運用中
	standby	待機系として運用中
	fault	障害中
	close	コマンド閉塞中

部位	状態情報	
	ステータス名称	意味
	disconnect	未実装
	configuration discord	コンフィグレーション不一致によって運用系と非同期中
	software version discord	ソフトウェアバージョン不一致によって運用系と非同期中
	license key discord	ライセンスキー不一致によって運用系と非同期中
RM イーサネットポート (SB-5400S ではリモートマネージメントポート)	active	運用中
	fault	障害中
	unused	未使用 (コンフィグレーション未設定)
	close	コマンド閉塞中
	locked	コンフィグレーションで運用停止中
	test	回線テスト中
メンテナンスポート **【SB-5400S】**	active	運用中
	unused	未使用
	closed	コマンド閉塞中
	locked	コンフィグレーションで運用停止中
	test	回線テスト中
CP	active	運用中
	initialize	初期化中
	fault	障害中
	close	コマンド閉塞中
	unused	未使用 (コンフィグレーション未設定)
PSU	active	運用中
	initialize	初期化中
	fault	障害中
	close	コマンド閉塞中
	unused	未使用 (コンフィグレーション未設定)
	locked	コンフィグレーションで運用停止中
BSU	active	運用中
	initialize	初期化中
	fault	障害中
	close	コマンド閉塞中
	unused	未使用 (コンフィグレーション未設定)
	locked	コンフィグレーションで運用停止中
NIF	active	運用中
	initialize	初期化中
	fault	障害中
	closed	コマンド閉塞中

部位	状態情報	
	ステータス名称	意味
	unused	未使用 (コンフィグレーション未設定)
	mismatch	コンフィグレーション不一致
	locked	コンフィグレーションで運用停止中
Line	active up	運用中 (正常動作中)
	active down	運用中 (ネットワーク障害発生中)
	initialize	初期化中
	test	回線テスト中
	fault	障害中
	closed	コマンド閉塞中
	unused	未使用 (コンフィグレーション未設定)
	mismatch	コンフィグレーション不一致

14.7.3 統計情報

本装置では運用に必要な情報を統計情報として取得します。統計情報は show rm cpu コマンド，show cp cpu コマンドで本装置の CPU 使用率，show cp buffer コマンドでバッファ使用率などを取得できます。また，show system コマンド，show interfaces コマンドおよび show nif コマンドで各ネットワークインタフェースのトラフィックカウント，エラーカウントなどを参照できます。また，これらの情報は SNMP の MIB 情報として参照することもできます。

14.7.4 運用メッセージおよび運用ログ

本装置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。

種別ログは装置内で発生した障害や警告についての情報をメッセージ 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。

運用ログに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

これらのログは装置内にテキスト形式で格納しています。装置の管理者はこれらの情報を，表示コマンドで参照できます。また，必要に応じて MC に格納したあとにファイルとして扱うこともできます。

14.8 LED および障害部位の表示

本装置には装置の状態を示すために LED ランプ（以降 LED と略す）とシステム操作パネルへの障害表示を使用しています。LED および障害表示の仕様について示します。

14.8.1 LED

LED ランプは装置に実装されているボードのパネル面にあり，障害状態（赤・黄）と，動作状態表示（緑）およびネットワーク障害について表示します。詳細は「ハードウェア取扱説明書」を参照してください。

14.8.2 障害表示

装置内で故障が発生した場合に，故障部位または機能の切り分けを行うためにシステム操作パネルに障害表示を行います。BCU ボード上の ALARM LED が点灯している場合は，装置障害が発生していることを示す障害表示を行います。また，ERROR LED が点灯している場合は，装置の部分障害が発生していることを示す障害表示を行います。

障害表示は，エラーレベル E9，E8，E7，E6，E5 の障害に対して行われ，エラーレベルの高い障害が優先的に表示されます。障害個所が修復されると，障害表示は自動的に消えます。

14.9　ネットワーク障害切り分け機能

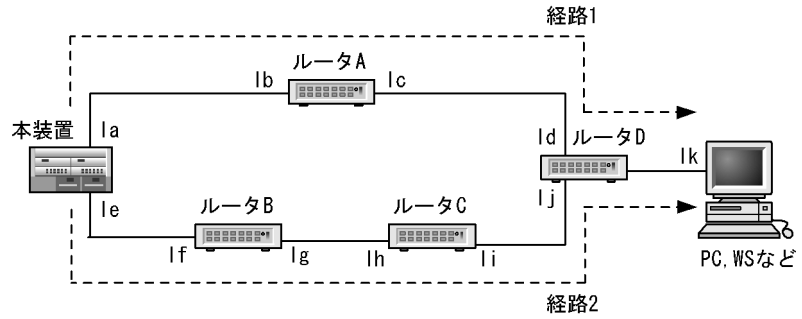
14.9.1　経路確認

経路確認コマンドとして，traceroute と traceroute ipv6 があります。

（1） traceroute コマンド

パケットの宛先の装置までの経路情報を確認するコマンドです。TTL(Time To Live) 値を 1 から順次増加したテスト用 IP パケットを送信して，経路途中のルータからの ICMP エラー応答を受け取ることで，宛先の装置までの経路情報を取得して，運用端末に表示します。このコマンドを使用してパケットの宛先の装置まで疎通確認できます。本装置から宛先の装置までの経路が複数あるような場合に，期待した経路で IP パケットが中継されるかどうかを確認するのに有効です。traceroute コマンドの使用例を次の図に示します。

図 14-8　traceroute コマンドの使用例



経路1でIPパケットが中継された場合：IPアドレスIb，Id，Ikと応答待ち時間を表示する
経路2でIPパケットが中継された場合：IPアドレスIf，Ih，Ij，Ikと応答待ち時間を表示する

（2） traceroute ipv6 コマンド

traceroute コマンドと同様の機能を持ち，IPv6 パケットの宛先の装置までの経路情報を確認するコマンドです。Hop Limit 値を 1 から順次増加したテスト用 IPv6 パケットを送信して，経路途中のルータからの ICMPv6 エラー応答を受け取ることで宛先の装置までの経路情報を取得し，運用端末に表示します。

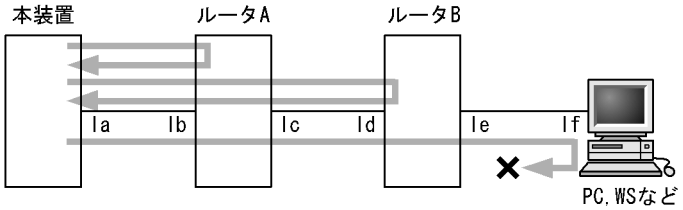
14.9.2　疎通テスト

疎通テスト確認のコマンドとして，ping，ping ipv6 があります。

（1） ping コマンド (ICMP エコー)

IP ネットワークでの障害切り分けに有効なコマンドです。このコマンドは指定した IP アドレスを持つ装置が ICMP エコーを返す機能を利用しています。宛先アドレスまでの経路途中のルータに対して順番に ping コマンドで疎通を確認していくことで，通信ができなくなっている範囲を絞り込むことができます。ping コマンドの使用例を次の図に示します。

図 14-9　ping コマンドの使用例



IPアドレスlb，ld，lfを宛先としてpingコマンドを実行したところ，lfからの応答がなかった。
この場合，ルータBのle，lfを持つ装置，le-lf間のネットワークに要因があると考えられる。

（2） ping ipv6 コマンド (ICMPv6 エコー)

ping コマンドと同様の機能を持ち，IPv6 ネットワークでの障害切り分けに有効なコマンドです。本コマンドは指定した IPv6 アドレスを持つ装置が ICMPv6 エコーを返す機能を利用しています。宛先アドレスまでの経路途中のルータに対して順番に ping ipv6 コマンドで疎通を確認していくことで，通信ができなくなっている範囲を絞り込むことができます。

14.9.3　回線テスト

回線テストには次に示すコマンドを使用します。

- 回線テストの開始　　：test interfaces コマンド
- 回線テストの終了，およびその結果表示：no test interfaces コマンド

（1） test interfaces コマンド，no test interfaces コマンド

回線障害が発生した場合に，障害の要因が本装置にあるか，接続するネットワーク側にあるかを切り分けるコマンドです。ネットワークインタフェースの種別によってサポートするテスト種別が異なるので，詳細はマニュアル「運用コマンドレファレンス Vol.1」の test interfaces コマンド，no test interfaces コマンドを参照してください。

14.10 障害時の復旧および情報収集

本装置では運用中に障害が発生した場合は自動的に復旧処理を行います。障害部位に応じて復旧処理を局所化して行い，復旧処理による影響範囲を狭めることによって，正常運用部分が中断しないようにします。

14.10.1 障害部位と復旧内容

障害発生時，障害の内容によって復旧内容が異なります。障害部位と復旧内容を次の表に示します。

表 14-11 障害部位と復旧内容【SB-7800S】

障害部位	装置の対応	復旧内容	影響範囲
回線障害	自動復旧を無限回行います。	該当する回線の再初期化を行います。	該当する回線を介する通信が中断されます。
ネットワークインタフェースボード障害 (NIF)	自動復旧を 3 回／ 1Hr 行います。 障害継続中は 1 時間経過後に再度復旧処理を実行します。※	該当する NIF の再初期化を行います。	該当する NIF が収容する全回線を介する通信が中断されます。
パケットスイッチングモジュール障害 (PSU)	自動復旧を 3 回／ 1Hr 行います。 復旧処理後も障害継続中の場合，1 時間経過後に再度復旧処理を実行します。 なお，この障害での自動復旧回数は，最初の障害発生から 1 時間経過後に初期化されます。※	該当する PSU の再初期化を行います。	該当する PSU が収容する全 NIF を介する通信が中断されます。
コントロールプロセッサ障害 (CP)	自動復旧を 3 回／ 1Hr 行います。 復旧処理後も障害継続中の場合，1 時間経過後に再度復旧処理を実行します。 なお，この障害での自動復旧回数は，最初の障害発生から 1 時間経過後に初期化されます。	該当する CP の再初期化を行います。 なお，二重化されている場合は系切替による復旧処理を行います。	装置内の全回線を介する通信が中断されます。
基本制御モジュール障害 (BCU) ルーティングマネージャ ソフトウェア 重度障害（RM）	自動復旧を 7 回行い，以降停止します。 1 時間以上運用時，自動復旧回数を初期化します。	該当する BCU の再初期化を行います。 なお，二重化されている場合は系切替による復旧処理を行います。	装置内の全回線を介する通信が中断されます。
シャーシ障害	停止します。	装置の再起動を行います。	装置内の全回線を介する通信が中断されます。
電源ユニット障害 (POW)	停止します。 なお，電源ユニットが冗長化されている場合は停止しません。	装置の再起動を行います。 なお，電源ユニットが冗長化されている場合は停止しません。	装置内全回線を介する通信が中断されます。 なお，電源ユニットが二重化されている場合は通信の中断はありません。

注※ コンフィグレーションコマンドでパッケージの復旧処理を行わない指定を設定している場合には，自動復旧を行いません。

表 14-12 障害部位と復旧内容【SB-5400S】

障害部位	装置の対応	復旧内容	影響範囲
回線障害	自動復旧を無限回行います。	該当する回線の再初期化を行います。	該当する回線を介する通信が中断されます。
ネットワークインタフェースボード障害 (NIF)	自動復旧を 3 回／ 1Hr 行います。 障害継続中は 1 時間経過後に再度復旧処理を実行します。※	該当する NIF の再初期化を行います。	該当する NIF が収容する全回線を介する通信が中断されます。
コントロールプロセッサ障害 (CP)	自動復旧を 3 回／ 1Hr 行います。 復旧処理後も障害継続中の場合，1 時間経過後に再度復旧処理を実行します。 なお，この障害での自動復旧回数は，最初の障害発生から 1 時間経過後に初期化されます。	該当する CP の再初期化を行います。 なお，二重化されている場合は系切替による復旧処理を行います。	装置内の全回線を介する通信が中断されます。
基本スイッチングモジュール障害 (BSU)	自動復旧を 3 回／ 1Hr 行います。 復旧処理後も障害継続中の場合，1 時間経過後に再度復旧処理を実行します。 なお，この障害での自動復旧回数は，最初の障害発生から 1 時間経過後に初期化されます。※	該当する BSU の再初期化を行います。 なお，二重化されている場合は系切替による復旧処理を行います。	装置内の全回線を介する通信が中断されます。
基本制御モジュール障害 (BCU) ルーティングマネージャ ソフトウェア 重度障害（RM）	自動復旧を 7 回行い，以降は停止します。 1 時間以上運用時，自動復旧回数を初期化します。	該当する BCU の再初期化を行います。 なお，二重化されている場合は系切替による復旧処理を行います。	装置内の全回線を介する通信が中断されます。
シャーシ障害	停止します。	装置再起動を行います。	装置内の全回線を介する通信が中断されます。
電源ユニット障害 (PS)	停止します。 なお，電源ユニットが冗長化されている場合は停止しません。	装置再起動を行います。 なお，電源ユニットが冗長化されている場合は停止しません。	装置内全回線を介する通信が中断されます。 なお，電源ユニットが二重化されている場合は通信の中断はありません。

注※ コンフィグレーションコマンドでパッケージの復旧処理を行わない指定を設定している場合には，自動復旧を行いません。

14.10.2 ログ

(1) ログ採取

障害発生時，障害の内容を種別ログへ採取します。これによって，障害の履歴を管理できます。障害の内容を把握すれば，障害に対する対策のほか，予防保守を行うための判断資料として使用します。

(2) ログ syslog 出力

採取した本装置のログを，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。本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可能になります。

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。

14.10.3 オンライン中のボード交換

本機は故障などによって発生するボードの交換をオンライン中に行うことができます。交換できるボードを次に示します。

- BCU(RM，CP および CSW)
- PSU および BSU
- NIF
- PS
- FAN

なお，BCU については待機系のボードに限ります。

! 注意事項

感電する恐れがあります。オンライン中のボードの交換作業は保守員へご依頼ください。

14.10.4 スイッチ

BCU ボード上にはリセットスイッチがあり，同スイッチを押して手動で BCU の再起動を実行できます。通常，このスイッチを押す必要はありません。

14.10.5 メモリダンプ

本装置で RM，CP，PSU(SB-5400S では BSU) および NIF が再起動するなどの重度障害が発生した場合，障害の詳細調査に使用するために RM，CP，PSU(SB-5400S では BSU) および NIF のメモリダンプ情報を MC 上のダンプ専用ディレクトリにファイルとして格納します。

また，本装置で CP 輻輳などのイベントが発生した場合，イベント詳細調査に使用するためにメモリダンプ情報を MC 上のイベントダンプ専用ディレクトリにファイルとして格納します。

14.11 ソフトウェアのアップデート

本装置ではネットワーク接続したリモート運用端末またはコンソールからの操作でMC内蔵のソフトウェアをアップデートできます。この機能はソフトウェアのインストールにも使用できます。

14.11.1 リモート運用端末からのソフトウェアのアップデート

ソフトウェアのアップデート機能を使用するためには前提条件として次のものが必要です。

- リモート運用端末
  TCP/IPネットワーク接続要，CD-ROM要，ftp機能要
- 本装置のソフトウェアCD-ROM

14.11.2 コンソールからのソフトウェアのアップデート

ソフトウェアのアップデート機能を使用するためには前提条件として次のものが必要です。

- コンソール
  PC/AT互換機，RS232Cインタフェース要，CD-ROM要，ZMODEM手順サポートの通信プログラム要
- 本装置のソフトウェアCD-ROM

14.11.3 ソフトウェアアップデート時の注意事項

1. ソフトウェアのアップデートを行ったあと，装置を再起動するため，ネットワークの運用が一時停止します。
2. コンソールからZMODEM手順を使用してソフトウェアのアップデート／インストールを行うには長時間を必要とします。所要時間の詳細についてはソフトウェア添付資料をご参照ください。

14.12 ファイル属性

ファイルはファイルの所有者，所有者グループ，所有者・所有者グループ以外のその他についてそれぞれリード，ライト，実行の属性を持ちます。

これらの属性を使用して，例えば，所有者だけ読み書き可能とし，そのほかの者には読み書き不可にすれば，所有者以外への秘特性や所有者以外がファイルを誤って削除するなどを防止できます。

ファイルの所有者はファイルを作成したユーザとなります。所有者グループはファイルを作成したユーザが属するグループ名となります。ユーザ登録を行ったユーザのグループは user となります。所有者以外のユーザは所有者，所有者グループ以外のユーザを示します。

ファイルの属性は ls コマンドで確認できます。また，属性は chmod コマンドで変更できます。

14.13　システム操作パネル

システム操作パネルは，BCU ボードに搭載されています。装置情報や各種メッセージを表示するための液晶ディスプレイと，ユーザが装置内の動作情報を取り出すために操作する BACK キー（ ◀ ），ENTR キー（■），FWRD キー（ ▶ ）の三つの操作キーから構成されます。BCU ボードの実装位置などの確認は，ハードウェア取扱説明書を参照してください。

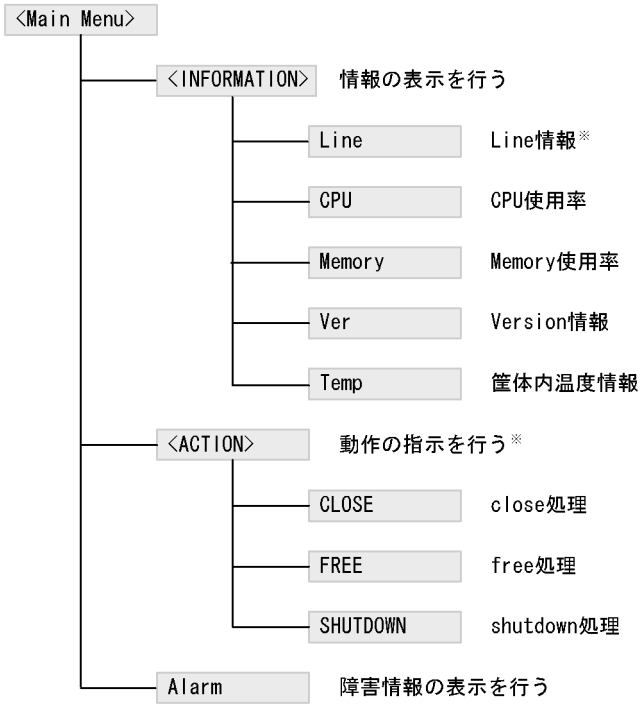
システム操作パネルには，ユーザがメニューから選択して各種情報を表示したり，動作指示を行ったりする機能があります。また，障害発生時には，ERROR/ALARM LED が点灯するとともに，システム操作パネルに障害情報を自動表示する機能があります。

装置起動直後やシステム操作パネルをしばらく操作しない場合には，システム操作パネルに装置型名を表示します。コンフィグレーションコマンドの system name コマンドで <System Name> が設定されている場合には，装置型名の代わりに system name コマンドで設定された文字列を表示します。

メニューを操作していて，現在メニューがどの表示をしているか分からなくなった場合には，ENTR キーを何回か押下することで <Main Menu> に戻ることができます。また，操作キーを操作しないで一定時間が経過しても <Main Menu> に戻ります。

次の図にシステム操作パネルのメニュー構造を示します。<Main Menu> が表示されていない場合には，ENTR キーを何回か押下することで <Main Menu> を表示します。なお待機系の BCU では，表示できない情報があります。各メニューの詳細は，「運用ガイド　4. システム操作パネルの操作」を参照してください。

図 14-10　システム操作パネルのメニュー構造



注※　待機系BCUでは操作できません

14.14 BCU ボードのアップグレード【SB-7800S】

14.14.1 運用中の BCU ボードアップグレード方法

本装置では，冗長構成で運用中に BCU ボードのアップグレードを行うことができます。

BCU ボードのアップグレードは障害が発生したボード交換作業と同じ手順で行うことができます。

ボードの交換作業については，「運用ガイド　9.3 障害が発生した SB-7800S ボードの交換【SB-7800S】」を参照してください。

14.14.2 BCU ボードアップグレード時の注意事項

1. BCU ボードのアップグレードとソフトウェアのバージョンアップを同時に行う場合，ソフトウェアのバージョンアップを完了してから BCU ボードのアップグレードを行うようにしてください。
2. 冗長構成での BCU ボードアップグレードは，運用系および待機系の両方のボードを連続してアップグレードしてください。片側の BCU ボードだけアップグレードしたままで運用の継続を行わないでください。
3. 冗長構成での BCU ボードアップグレード中はコンフィグレーション変更を行わないでください。コンフィグレーション変更は，運用系および待機系の両方の BCU ボードのアップグレード完了後に行ってください。

15 他機種との接続

この章では，システム構築時に検討が必要な他機種との接続について説明します。

15.1　イーサネット

15.1.1　インタフェース種別の設定

本装置と他機種をイーサネットで接続する場合には次の点に注意してください。

（1） 10BASE-T/100BASE-TX/1000BASE-T 接続

- 伝送速度および全二重および半二重モードが相手装置と不一致の場合，接続できないので注意してください。
  不一致の状態で通信を行うと，以降の通信が停止することがあります。この場合，当該ポートに対して close コマンド，free コマンドを実行してください。**【SB-7800S】**
- ポートを 100BASE-TX または 1000BASE-T で使用する場合，接続ケーブルはカテゴリ 5 以上で 8 芯 4 対のツイストペアケーブル (UTP) を使用してください。
- 全二重インタフェースはコリジョン検出とループバック機能を行わないことによって実現しています。このため，10BASE-T または 100BASE-TX を全二重インタフェース設定で使用する場合，相手接続ポートは必ず全二重インタフェースに設定して接続してください。
- 1000BASE-T を使用する場合は全二重のオートネゴシエーションだけとなります。

（2） 1000BASE-X 接続

- 全二重のオートネゴシエーションおよび固定接続だけのサポートとなります。
- 相手装置（スイッチングハブなど）をオートネゴシエーションまたは全二重固定に設定してください。
- 未サポートのトランシーバを使用した場合の動作は保証できません。
  「解説書 Vol.1　4. イーサネット」を参照してください。

（3） 10GBASE-R および 10GBASE-W 接続【SB-7800S】

- 10GBASE-R および 10GBASE-W の半二重およびオートネゴシエーションは IEEE802.3ae 規格にないため，全二重固定接続だけとなります。
- トランシーバが交換可能な NIF の場合，未サポートのトランシーバを使用した場合の動作は保証できません。「解説書 Vol.1　4. イーサネット」を参照してください。

（4） オートネゴシエーション接続 (10BASE-T ／ 100BASE-TX ／ 1000BASE-T, 1000BASE-X)

本装置と相手装置の両方をオートネゴシエーションで使用する場合，接続する相手装置が ISO/IEC8802.3 オートネゴシエーションで接続できるか確認してください。この場合，設定されるモードは本装置および接続相手装置がサポートしている中で最も高速なモードが設定されます。

相手装置が固定設定の場合，本装置はオートネゴシエーションではなく固定設定にしてください。

また，相手装置によってはオートネゴシエーションが正しく完了しないで通信ができない場合があります。この場合，本装置は次に示すシステムメッセージを表示するケース，本装置のリンクがアップしないケース，または相手装置のリンクがアップしないケースなどがあります。このような問題は，本装置の設定を接続する相手装置に合わせた固定設定にすると回避できます。

```
E4 LINELAN NIF:X LINE:X 90111003 1350:XXXXXXXXXXXX Auto negotiation failed.
```

本装置の NIF 種別が NE1GSHP-4S または NE1GSHP-8S の場合，相手装置のリンクがアップしないケースがあります。この場合，本装置，相手装置ともに固定設定にすると回避できます。

(5) フローコントロール

本装置は 10BASE-T（全二重），100BASE-TX（全二重），1000BASE-T 全二重，1000BASE-X 全二重，10GBASE-R**【SB-7800S】**，10GBASE-W**【SB-7800S】**でフローコントロールを行います。

また，装置間でお互いのフローコントロール動作モードの設定内容を一致させてください。例えば，本装置でポーズパケット送信を有効にした場合，相手装置のポーズパケット受信を有効にします。

(6) ジャンボフレーム

本装置は 100BASE-TX（全二重），1000BASE-T 全二重，1000BASE-X 全二重，10GBASE-R**【SB-7800S】**，10GBASE-W**【SB-7800S】**で EthernetV2 フレーム形式のジャンボフレームだけサポートします。EthernetV2 フレーム形式については，「解説書 Vol.1　4.3 MAC および LLC 副層制御」のフレームフォーマットを参照してください。802.3 形式フレームはサポートしていません。

本装置と相手装置の最大フレーム長を合わせた設定値としてください。

(7) クロック【SB-7800S】

本装置は 10GBASE-W で，独立同期および従属同期をサポートしています。

独立同期は WDM(Wavelength Division Multiplexing) 装置および，ルータまたはスイッチと接続する場合に指定します。

従属同期は網同期で接続する場合に指定します。なお，従属同期での接続は以下の入力周波数精度の装置としてください。

- 9.95328Gbit/s ± 20ppm 以下 (Sonet minimum Clock)

本装置のデフォルト値は独立同期です。IEEE802.3ae に準拠しています。

15.2　POS【SB-7800S】

15.2.1　インタフェース種別の設定

本装置と他機種を POS で接続する場合には次の点に注意してください。

（1） POS 接続

- 以下の設定を相手装置と合わせてください。
  - クロック
  - CRC 長
  - スクランブル
  - 動作モード
  - セクショントレースメッセージモード
  - J0
  - RDI モード
  - C2
  - B2SD ビットエラー率の閾値
  - SF ビットエラー率（B2EBER）の閾値
- トランシーバが交換可能な NIF の場合，未サポートのトランシーバを使用した場合の動作は保証できません。「解説書 Vol.1　5. POS（PPP Over SONET/SDH）【SB-7800S】」を参照してください。

（2） クロック

本装置では，独立同期および従属同期をサポートしています。

独立同期は WDM（Wavelength Division Multiplexing）装置および，ルータまたはスイッチと接続する場合に指定します。

従属同期は網同期で接続する場合に指定します。なお，従属同期での接続は以下の入力周波数精度の装置としてください。

- OC-192c/STM-64 POS の場合：9.95328Gbps ± 4.6ppm 以下（Sonet minimum clock）
- OC-48c/STM-16 POS の場合 ：2.48832Gbps ± 20ppm 以下（Sonet minimum clock）

本装置のデフォルト値は独立同期です。

15.3　レイヤ 2 スイッチ

15.3.1　PVST+ でのシングルスパニングツリーとの接続

本装置を PVST+ のシングル接続ポートとして他装置と接続する場合には，次の点に注意してください。

（1） Ver.9.1 以前の装置との接続

Ver.9.1 以前の PVST+ は，シングルスパニングツリー相当で動作している装置と接続することはできません。なお，本装置と Ver.9.1 以前の装置とは互換性があり接続可能です。このとき，本装置で Ver.9.1 以前の装置と接続している PVST+ のポートは，シングルスパニングツリーと接続できない状態になります。対向装置を Ver.9.2 以降にバージョンアップすることで，本装置の PVST+ のポートは，自動的にシングルスパニングツリーと接続可能になります。

（2） 対向する Ver.9.1 以前の装置を他装置に置き換える場合

(1) のように，Ver.9.1 以前の装置と接続していたポートをシングルスパニングツリー相当で運用している装置に置き換える場合は，一度，当該ポートをリンクダウンさせてください。リンクダウンさせない場合，Ver.9.1 以前の装置との互換性を保持し，シングルスパニングツリーと接続できないままになることがあります。

15.3.2　ソフトウェアアップデート時の注意事項

（1） PVST+ スパニングツリーを運用中に Ver.9.1 以前から Ver.9.2 以降にアップデートする際の注意事項

対向の PVST+ スパニングツリーが動作している装置との接続に PVST+ スパニングツリーが動作しない装置を経由している場合，次の点に注意してください。

Ver.9.2 で，シングル接続ポートでは，PVST+ スパニングツリーが送受信する BPDU を PVST+ スパニングツリーからシングルスパニングツリー (IEEE802.1D 規格または IEEE802.1w 規格) に変更しました。

シングル接続ポートで，対向の PVST+ スパニングツリーが動作している装置との接続に PVST+ スパニングツリーが動作しない装置を経由している場合，アップデート前の運用では，経由している装置が PVST+ スパニングツリーの BPDU を中継していると考えられます。しかし，アップデート後は，シングル接続ポートで送受信するシングルスパニングツリーの BPDU(IEEE802.1D 規格または IEEE802.1w 規格) を，経由している装置が中継しない場合があります。このような場合，アップデート後に PVST+ スパニングツリーを正しく運用できないおそれがあります。

そのため，アップデート実行前に，経由している装置がシングルスパニングツリーの BPDU(IEEE802.1D 規格または IEEE802.1w 規格) を中継することを確認してください。中継しない装置の場合，次に示すどれかを実施することで正しく運用を継続できます。

1. 経由する装置が，設定によって BPDU を中継できる装置の場合，中継するように設定してください。
2. 経由する装置がスパニングツリー (IEEE802.1D 規格または IEEE802.1w 規格) をサポートしている場合，経由する装置でスパニングツリーを動作させてください。
3. 1，2 のどちらも実施できない場合，本装置および対向の装置で，シングル接続ポートとして運用しているポートに未使用の VLAN で Tagged ポートを設定してください。この設定によって，シングル接続ポートの条件を満たさなくなり，PVST+ スパニングツリーの BPDU で送受信を継続するため，アップデート前と同じように動作します。なお，未使用の VLAN は disable を設定することで，通信しな

い VLAN として設定できます。

15.4 レイヤ3インタフェース

15.4.1 Tag-VLAN 連携の LAN スイッチ接続

本装置と LAN スイッチを Tag-VLAN 連携で接続する場合の設定について説明します。

(1) VLAN 種別

本装置がサポートする VLAN は，IPv4 および IPv6 パケットに関する通信だけです。本装置を接続する LAN スイッチがそれ以外の VLAN(例えば，IPX などのプロトコル VLAN) をサポートしている場合でも，LAN スイッチに設定する VLAN は，次に示すどちらかにしてください。

- LAN スイッチが中継する IPv4 および IPv6 パケットに関する VLAN
- LAN スイッチの送受信ポートに関する VLAN

(2) Tag-VLAN 連携設定

本装置と，本装置に接続する LAN スイッチの Tag 値の設定は一致させてください。LAN スイッチと Tag 値の設定を一致させるときは，次に示す点に注意してください。

- VLAN 設定をしたインタフェース (vlan オプションで指定) は，Tag 付きパケットだけを送受信でき，Tag なしパケットを受信した場合，そのパケットを廃棄します。ただし，untagged で VLAN を設定すれば tag なしパケットも送受信できます。
- VLAN 設定をしていないインタフェースは，Tag なしパケットだけを送受信できます。Tag 付きパケットを受信した場合，そのパケットを廃棄します。
- TPID(Tag Protocol Identifier) 値は "0x9100" または "0x8100" を選択できます。

(3) 中継できるパケット

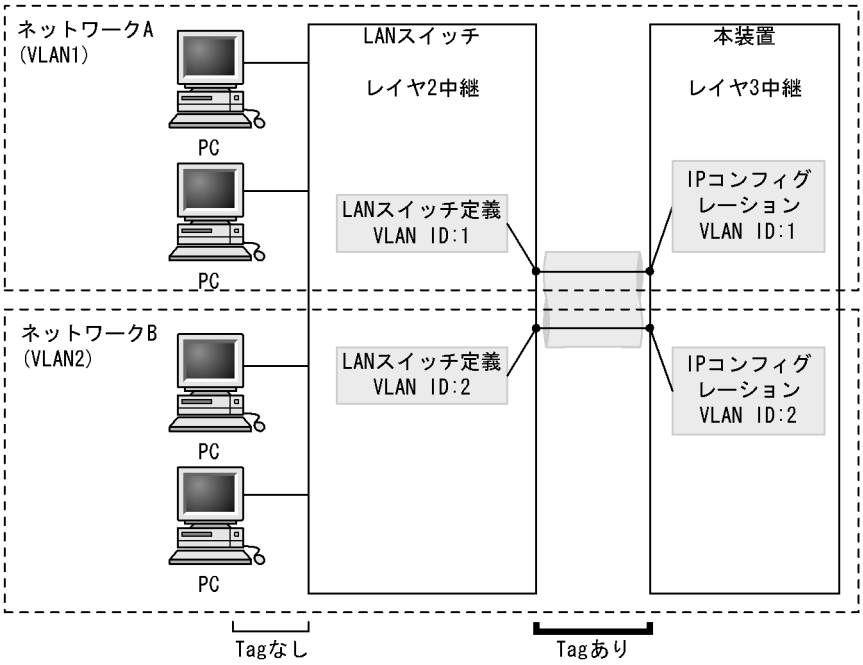
VLAN 設定をしたインタフェース (コンフィグレーションコマンドの vlan オプションで指定) は，IPv4 および IPv6 パケット ARP パケットだけを送受信できます。本装置を接続する LAN スイッチがそれ以外のパケットをサポートしている場合でも，次に示すパケットに関する VLAN は使用しないでください。

- IPX パケット

(4) VLAN ID

VLAN ID は本装置，LAN スイッチから構成される仮想ネットワークの識別子のため，接続する LAN スイッチの VLAN ID と一致させる必要があります。VLAN ID の不一致が発生した場合，パケットの廃棄などが発生して正しい通信が行えません。二つの VLAN を LAN スイッチ経由で本装置に設定する例を次の図に示します。

図 15-1　二つの VLAN を LAN スイッチ経由で本装置に設定する例



- LAN スイッチに設定する VLAN ID(「図 15-1　二つの VLAN を LAN スイッチ経由で本装置に設定する例」の LAN スイッチ定義) と，本装置に設定する IP コンフィグレーションの VLAN ID は同じ値にしてください。

15.4.2　Tag-VLAN 連携の PC 接続

本装置と PC を Tag-VLAN 連携で接続する場合には次の点に注意してください。

- Tag-VLAN のサポート
  Tag-VLAN をサポートしている PC はほとんどありません。本装置と PC を Tag-VLAN として接続する場合は，LAN スイッチ経由で接続してください。
- Layer2 中継
  本装置の Tag-VLAN 連携は IPv4 または IPv6 限定の Layer3 中継だけをサポートします。VLAN ドメイン内の Layer2 中継を PC 間で行う場合は，Tag-VLAN 連携機能を使用しないで，レイヤ 2 中継機能を動作させるか，または LAN スイッチを併用する必要があります。

15.5　IP ルータとの接続

15.5.1　他機種との接続

本装置と他機器を IP ルーティングで接続する場合について説明します。

（1） ポイント - ポイント型回線のインタフェースアドレス

本装置はポイント - ポイント型回線の経路情報 (直結経路) を二つのホスト経路として扱います。したがって，本装置だけで構成されたネットワークでは，ポイント - ポイント型の回線にインタフェースアドレスを割り当てることができます。他機種間では使用しないでください。

ポイント - ポイント型の回線に割り当てられるインタフェースアドレスを次に示します。詳細は「解説書 Vol.1　12.2 ネットワーク設計の考え方」を参照してください。

- 複数のポイント - ポイント型回線に同一のネットワークまたはサブネットワークの IP アドレス
- ポイント - ポイント型回線の両端に異なるネットワークまたはサブネットワークの IP アドレス

! 注意事項

本装置ではポイント - ポイント型回線の経路情報を二つのホスト経路として扱いますが，Cisco 社製ルータでは一つのネットワーク経路として扱います。したがって，ルーティングプロトコルで広告される経路情報に差異が生じるので注意してください。

（2） ポイント - ポイント回線上で RIP-1 を使用する場合の設定

本装置ではポイント - ポイント回線上に RIP パケットを送信する場合，宛先アドレスをユニキャストアドレス (相手装置のインタフェースアドレス) で送信します。また，ポイント - ポイント回線上から RIP パケットを受信する場合，宛先アドレスがユニキャスト・アドレス (自装置のインタフェースアドレス)，または制限付きブロードキャストアドレス (すべて 1 のアドレス) のパケットを受け入れます。

Cisco 社製ルータでは「ip broadcast-address」の設定によって，RIP パケットの宛先アドレスが異なります。本装置と Cisco 社製ルータを接続する場合は，「ip broadcast-address」を設定しないでください。

（3） ポイント - ポイント回線上で OSPF を使用する場合の設定【OP-OSPF(SB-5400S)】

本装置ではポイント - ポイント回線上で OSPF を動作させた場合，HelloInterval のデフォルト値は 10 秒，Routerdeadinterval のデフォルト値は 40 秒となっています。

本装置と他装置をポイント - ポイント回線で接続する場合には，接続する他装置の使用を確認の上，両ルータ間で HelloInterval 値および Routerdeadinterval 値を合わせてください。

（4） OSPF を使用するときの注意事項【OP-OSPF(SB-5400S)】

- HelloInterval のデフォルト値
  本装置の HelloInterval のデフォルト値は 10 秒です。本装置と接続されるルータに設定された HelloInterval を確認して，両ルータ間で HelloInterval 値を合わせてください。
- priority のデフォルト値
  本装置の priority のデフォルト値は 1 です。ただし，NBMA(コンフィグレーションコマンド

interface(ospf backbone/ospf area モード) の nonbroadcast サブコマンドを指定したインタフェース) では 0 です。本装置を指定ルータの選択対象とさせたくない場合は，priority 値を 0 に設定してください。

(5) BGP-4 を使用するときの注意事項【OP-BGP】

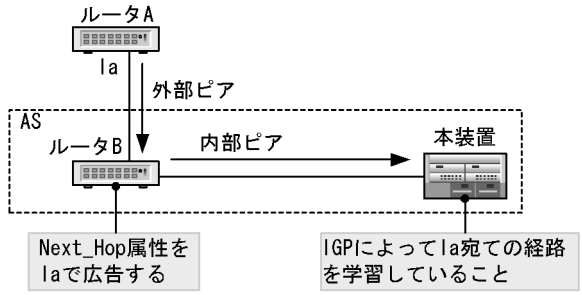
- NextHop 解決

  本装置では同一 AS 内の BGP スピーカへ経路を広告するとき，NEXT_HOP 属性にその BGP スピーカとのピアリングに使用している自側のピアリングアドレスを設定します。また，本装置が受信する経路情報の NEXT_HOP 属性は IGP 経路を基に解決しています。したがって，NEXT_HOP 属性に相手側のピアリングアドレスが設定されている必要はなく，IGP によって NEXT_HOP 属性に対応するアドレス宛ての経路が学習されていれば，Next_Hop 解決は正常に行われます。

  なお，コンフィグレーションコマンド bgp の resolve-nexthop サブコマンドに all を指定すると，Next-Hop 解決に使用する経路情報を IGP 経路および BGP 経路に拡張できます。

  この Next_Hop 解決処理は，すべてのピアタイプ (外部ピア，メンバー AS 間ピア，内部ピア) に適用されます。Next_Hop 解決を次の図に示します。

図 15-2　Next_Hop 解決



(6) RFC1583 に準拠していない装置と OSPF で接続するときの注意事項【OP-OSPF(SB-5400S)】

本装置と本装置以外の装置とで，同じ宛先の AS 外経路またはエリア間経路を，RFC1583 に準拠していない装置に広告するネットワーク構成にしないでください。

これは，OSPF の AS 外経路情報とエリア間経路情報の経路情報識別子 (LSID) フィールドの値は，RFC1247 の規格と RFC1583 以降の規格で異なるためです。

RFC1247 では，宛先アドレスを経路情報識別子として使用します。一方，RFC1583 以降 (本装置が該当) では，宛先アドレス以外の値を経路情報識別子として使用する場合があります (仕様は装置によって異なる)。このため，同一宛先の経路情報でも本装置とそのほかの装置が異なる経路情報識別子を使用することがあります。本装置同士では，同一宛先の経路情報の経路情報識別子は必ず同じ値になります。

RFC1583 に準拠していない装置では，同じ宛先の経路情報を異なる経路情報識別子で学習した場合，最短経路を選択しないか，または経路を学習しません。なお，RFC1583 以降の規格に準拠している装置では，正しく経路を選択します。

15.5.2　他装置との置き換え

次に示す機種は RIP-1 の実装が異なるので，注意が必要です。

- Cisco 社製ルータ

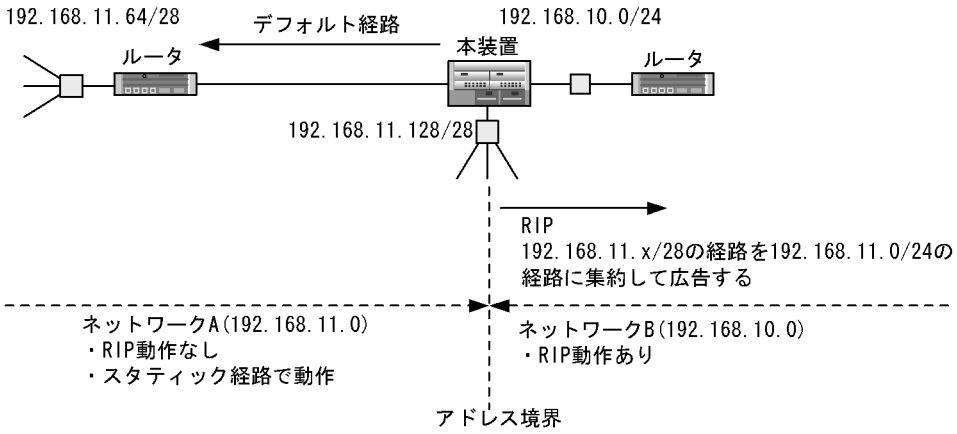
これら以外の装置と本装置を置き換える場合には，旧装置の仕様を確認してください。

本装置では，インタフェースアドレスがサブネット化されている場合，該当するインタフェースに対するネットワーク経路 (ナチュラル・マスク経路) を自動生成しません。ブロードキャスト接続ではサブネット経路を，ポイント - ポイント接続ではホスト経路を生成します。RIP-1 ではアドレス境界をまたがるサブネット経路は広告しないため，コンフィグレーションによって経路集約 (サブネット経路およびホスト経路をネットワーク経路に集約する) 設定が必要になります。詳細は「解説書 Vol.1　12.4.3(3)(a) IP インタフェースが一つの場合の RIP 広告について」を参照してください。

Cisco 社製ルータなど RIP-1 の実装が異なる機種では，サブネット経路を自動的にネットワーク経路に集約し広告する装置もあり，通常該当する集約経路はフォワーディング・テーブルに登録されません。本装置ではサブネット経路をネットワーク経路に集約するためには経路集約の定義が必要です。また，集約経路はアクティブ経路としてフォワーディング・テーブルに登録されます。

集約経路をフォワーディング・テーブルに登録しないような装置と互換性を持って動作させるためには，経路集約の定義経路集約の定義 (コンフィグレーションコマンド aggregate の noinstall サブコマンドの設定) が必要です。noinstall サブコマンドが必要な構成例を次の図に示します。

図 15-3　noinstall サブコマンドが必要な構成例



本装置に集約経路192.168.11.0/24をインストールした場合，192.168.11.64/28宛てのIPパケットは本装置で廃棄される。
(本装置に192.168.11.64/28の経路がなく，デフォルト経路で動作させるような場合)

15.6　IPv6 ルータとの接続

本装置と他機器を IPv6 ルーティングで接続する場合には次の点に注意してください。

15.6.1　他機種との接続

（1） ポイント - ポイント型回線のインタフェースアドレス

本装置はポイント - ポイント型回線の経路情報 (直結経路) を二つのホスト経路として扱います。したがって，本装置だけで構成されたネットワークでは，ポイント - ポイント型の回線に次のインタフェースアドレスを割り当てることができます。他機種間では使用しないでください。詳細は「解説書 Vol.1　12.2 ネットワーク設計の考え方」を参照してください。

- 複数のポイント - ポイント型回線に同一プレフィックスの IPv6 アドレス
- ポイント - ポイント型回線の両端に異なるプレフィックスの IPv6 アドレス

ただし，ポイント - ポイント型回線のインタフェースにこれらのアドレスを割り当てた場合，経路情報の集約設定などが複雑になります。本装置はリンク内だけで有効なリンクローカルアドレスを各インタフェースに割り当てることができるため，ポイント - ポイント型回線のインタフェースにはできるだけリンクローカルアドレスだけを割り当てるようにしてください。

! 注意事項

本装置ではポイント - ポイント型回線の経路情報を二つのホスト経路として扱いますが，Cisco 社製ルータでは一つのネットワーク経路として扱います。したがって，ルーティングプロトコルで広告される経路情報に差異が生じますので注意してください。

（2） ポイント - ポイント型回線による BGP4+ 接続での注意事項【OP-BGP】

本装置では，BGP4+ 接続をリンクローカルアドレスで行うことができます。また，ポイント - ポイント型回線の経路情報を二つのホスト経路として扱います。このため，本装置とポイント - ポイント型回線で接続を行うルータの BGP4+ が次に示す動作条件に該当する場合，本装置は接続先ルータからの経路情報が受信できないことがあります。

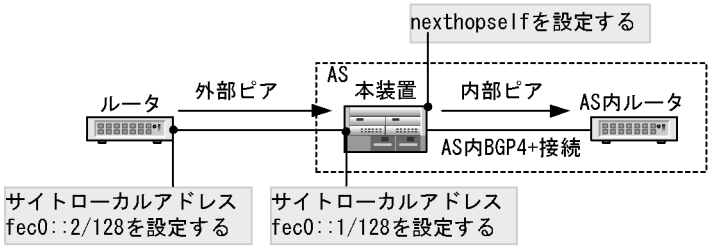
- グローバルアドレスだけで BGP4+ と接続するルータ
- ポイント - ポイント型回線のグローバルアドレスを，ブロードキャストアドレス型回線と同様に一つのネットワーク経路として解釈するルータ

このようなルータとポイント - ポイント型回線で接続し BGP4+ で経路情報の交換を行う場合には，ポイント - ポイント型回線にサイトローカルアドレスを割り当ててください。

Cisco 社ルータと接続する場合は，これらの設定が必要となります。

また，受信した経路情報を本装置で内部 BGP4+ ピアに送信する場合は，該当するピアのコンフィグレーションコマンド peer(bgp4+ externalpeeras/bgp4+ internalpeeras モード) の nexthopself サブコマンドを指定してください。nexthopself サブコマンド指定の例を次の図に示します。

図 15-4　nexthopself サブコマンド指定の例



! 注意事項

割り当てたサイトローカルアドレスは外部へ広告しないようにしてください。

15.7 IEEE802.1X

15.7.1 推奨認証サーバ

本装置では，次に示す認証サーバ（RADIUS サーバ）および認証アルゴリズムで動作確認をしています。これら以外の認証サーバを使用する場合は，十分評価の上，使用してください。

表 15-1 動作確認済み認証サーバおよび認証アルゴリズム

製品名	メーカ	動作確認済み認証アルゴリズム
Windows2003 Server IAS	Microsoft	EAP-MD5 EAP-TLS EAP-PEAP
Windows2000 Server IAS	Microsoft	EAP-MD5
Navis Radius	Lucent Technologies	EAP-MD5

15.7.2 推奨 802.1X 端末

本装置では，次に示す 802.1X 端末および認証アルゴリズムで動作確認をしています。これら以外の端末を使用する場合は，十分評価の上，使用してください。

表 15-2 動作確認済み 802.1X 端末および認証アルゴリズム

製品名	メーカ	動作確認済み認証アルゴリズム
Windows XP Professional Edition	Microsoft	EAP-MD5 EAP-TLS EAP-PEAP
Windows 2000 SP4	Microsoft	EAP-MD5
Odyssey Client ※	Funk Software	EAP-MD5 EAP-TLS

注※

Odyssey Client を端末認証モード（コンフィグレーションコマンド access-control supplicant で指定）で使用する場合，コンフィグレーションコマンド supplicant-detection に shortcut 以外を指定してください。shortcut を指定すると，tx-period のタイミングで通信が一時的に停止することがあります。

15.8　SNMP マネージャとの接続

15.8.1　推奨 SNMP マネージャ

本装置では，次に示す SNMP マネージャで動作確認をしています。これら以外の SNMP マネージャを使用する場合は，十分評価の上，使用してください。

- SNMP マネージャ
  - HP OpenView Network Node Manager Ver4.0x (HP-UX 版)
  - HP OpenView Network Node Manager Ver5.01 (HP-UX 版)
- RMON マネージャ
  - NetScout Systems NetScout Manager Plus Ver5.2
  - 3Com Transcend LANsentry Manager ver3.0

15.8.2　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に対して定期的に MIB の取得処理を行います。この定期的な MIB 取得処理間隔が短いとネットワーク機器やネットワークに負荷をかけることになります。また，装置の状態や回線速度などによって MIB 取得時にマネージャ側でタイムアウトが発生する可能性があります。次に示すことを考慮し，ネットワーク管理を行ってください。

(1) SNMP マネージャ側の応答監視タイマ値の考慮

SNMP マネージャ側で MIB 取得時の応答監視タイマ値を変更できる場合は，5 秒以上に設定してください。なお，本装置が次に示す場合に，マネージャ側で応答タイムアウトが頻発します。応答タイムアウトが頻発する場合は，応答監視タイマ値をさらに延ばす必要があります。

- ネットワークのレスポンスが悪い場合
  例えば，SNMP マネージャと本装置間に多数の接続装置（ブリッジ，ルータなど）がある，または回線速度が低い場合。
- 接続 IP ネットワーク数や接続インタフェース数が多い場合
  例えば，本装置のインタフェース数が多い場合，IP 関連の MIB 情報の検索時間で時間がかかる場合。
- ルーティングテーブルのエントリが多い場合
  例えば，本装置の IP ルーティングエントリ数が多い場合にルーティング関連の MIB 情報の検索時間で時間がかかる。または，経路計算などで MIB 情報の検索する CPU 割当時間の減少による，MIB レスポンス低下が発生する場合。
- ARP 数が多い場合
  例えば，本装置の ARP 数が多い場合，ARP 関連の MIB 情報の検索時間で時間がかかる場合。
- 接続 SNMP マネージャ数が多い場合
  例えば，本装置に接続する SNMP マネージャが多く，一定時間内に MIB 情報の収集が集中する場合。

SNMP マネージャのチューニングパラメータ

- 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

（2） SNMP マネージャによる MIB 情報の収集周期の見直し

本装置は，ネットワークの規模に伴い管理情報 (MIB) 量も増大します。このため，大規模ネットワークに接続する場合，SNMP マネージャからの問い合わせに対する管理情報の収集に長時間を必要とし，一時的に装置が過負荷状態になる場合があります。

過負荷状態が発生した場合，ルーティング情報の取りこぼしや，ルーティング情報を本装置から他装置に配布できなくなり，一時的に IP フレームの中継ができなくなることが発生します。このような場合，SNMP マネージャの各種パラメータのチューニングをお勧めします。

BCU を冗長構成で運用しているとき

SNMP マネージャから MIB を設定すると，待機系 BCU へスタートアップコンフィグレーションファイルの内容を自動的にコピーするため，時間がかかることがあります。このときは，応答監視タイマ値を少なくとも 20 秒以上に設定してください。

15.9 フロー統計コレクタとの接続

15.9.1 推奨 sFlow コレクタ

本装置では，次に示す sFlow コレクタで動作確認をしています。これ以外の sFlow コレクタを使用する場合は，十分評価のうえ，使用してください。本装置でサポートしている sFlow は，sFlow Datagram Format v2 と v4(RFC3176) です。sFlow Datagram Format v2，v4 をサポートしている sFlow コレクタを使用してください。

- InMon Traffic Server Version 4.0.25(RedHat 版)

15.9.2 推奨 NetFlow コレクタ／アナライザ

本装置では，次に示す NetFlow コレクタで動作確認をしています。これら以外の NetFlow コレクタを使用する場合は，十分評価のうえ，使用してください。本装置でサポートしている NetFlow は Cisco NetFlow Version 5，Cisco NetFlow Version 8，Cisco NetFlow Version 9 です。本バージョンをサポートしている NetFlow コレクタを使用してください。

- コレクタ　　：flow-tools Ver0.67(RedHat 版 Free Soft) ※ 2
  ＋アナライザ：FlowScan Release-1.006(RedHat 版 Free Soft) ※ 2
- コレクタ／アナライザ一体：InMon Traffic Server Ver4.0.25(RedHat 版) ※ 1
- コレクタ／アナライザ一体：Cisco CNS NetFlow Collection Engine Ver.5.0.1 ※ 3

注※ 1　Cisco NetFlow Version 5 だけ対応

注※ 2　Cisco NetFlow Version 5，8 に対応

注※ 3　Cisco NetFlow Version 5，8，9 に対応

15.10　RADIUS サーバとの接続

15.10.1　推奨 RADIUS サーバ

本装置では，次に示す RADIUS サーバで動作確認をしています。これら以外の RADIUS サーバを使用する場合は，十分評価の上，使用してください。本装置でサポートしているのは RADIUS を使用したリモートログインのユーザ認証です。

- Lucent Technologies NavisRadius (Windows NT/Solaris 版)

15.10.2　RADIUS サーバの設定

本装置が RADIUS サーバと接続するための注意点を次に示します。

(1) RADIUS サーバでの本装置の識別

RADIUS プロトコルでは NAS を識別するキーとして，要求パケットの発信元 IP アドレスを使用するよう規定されています。本装置では要求パケットの発信元 IP アドレスに次に示すアドレスを使用します。

- コンフィグレーションコマンド local-address によってローカルアドレスが設定されている場合は，ローカルアドレスを発信元 IP アドレスとして使用します。
- ローカルアドレスが設定されていない場合は，送信インタフェースの IP アドレスを使用します。

このため，ローカルアドレスが設定されている場合は，RADIUS サーバに本装置を登録するためにローカルアドレスで指定した IP アドレスを使用する必要があります。これによって，RADIUS サーバと通信するインタフェースが特定できない場合には，ローカルアドレスを設定することで RADIUS サーバを確実に識別できる本装置の情報を登録することができるようになります。

(2) RADIUS サーバのメッセージ

RADIUS サーバは応答に Reply-Message 属性を添付して要求元にメッセージを送付する場合があります。本装置では，RADIUS サーバからの Reply-Message 属性の内容を運用ログに出力します。RADIUS サーバとの認証に失敗する場合は，運用ログを参照してください。

(3) RADIUS サーバのポート番号

RADIUS の認証サービスのポート番号は，RFC2865 で 1812 と規定されています。本装置では特に指定しないかぎり，RADIUS サーバへの要求に 1812 のポート番号を使用します。しかし，一部の RADIUS サーバで 1812 ではなく初期の実装時に使用されていた 1645 のポート番号を使用している場合があります。このときコンフィグレーションの auth_port パラメータで 1645 を指定してください。auth_port パラメータでは 1 ～ 65535 の任意の値が指定できるので，RADIUS サーバが任意のポート番号で待ち受けできる場合にも対応できます。auth_port パラメータについては，「コンフィグレーションコマンドレファレンス Vol.2　14. RADIUS」を参照してください。

15.11　TACACS+ サーバとの接続

15.11.1　推奨 TACACS+ サーバ

本装置では，次に示す RADIUS サーバで動作確認をしています。これら以外の TACACS+ サーバを使用する場合は，十分評価の上，使用してください。本装置でサポートしているのは TACACS+ を使用したリモートログインのユーザ認証，コマンド承認です。

- Cisco Secure ACS v3.1 (Windows 版)

15.11.2　TACACS+ サーバの設定

- 本装置と TACACS+ サーバを接続する場合は，Service と属性名などに注意してください。TACACS+ サーバの設定については，「運用ガイド　5.2.6 CLI コマンドを制限する」を参照してください。
- コンフィグレーションコマンド local-address によってローカルアドレスが設定されている場合は，ローカルアドレスを発信元 IP アドレスとして使用します。

16 網・各種専用線サービスとの接続

この章では，システム構築時に検討が必要な網・各種専用線サービスとの接続について説明します。

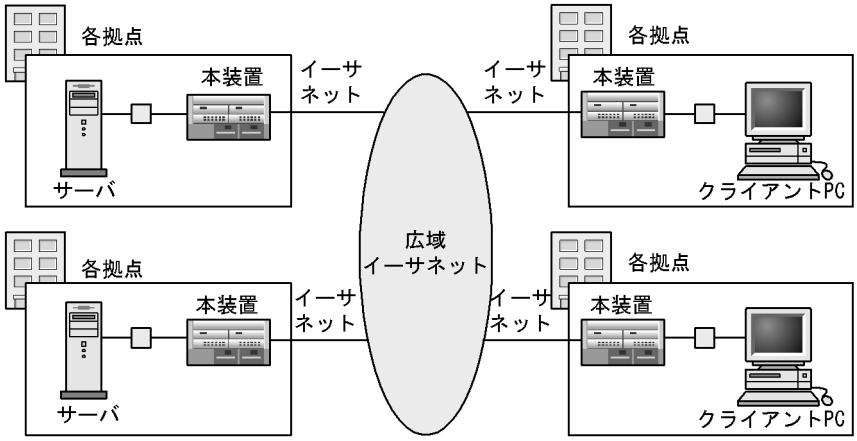
16.1　イーサネット

本装置と各イーサネットサービスの接続について説明します。

16.1.1　広域イーサネット

企業の多くは構内イーサネットを構築しており，複数の拠点や取引先との間でイーサネットを統合して業務を円滑に進めることが必要です。広域イーサネットは複数拠点のイーサネットを一つに統合するサービスです。広域イーサネットは，従来サービスよりも比較的安価で，高速バックボーンの共有によって，動画や画像によるトラフィックの増大にも対応できます。広域イーサネットを使用したネットワーク構成例を次の図に示します。

図 16-1　広域イーサネットを使用したネットワーク構成例



付録

付録 A　準拠規格

付録 A.1　イーサネット

表 A-1　イーサネットインタフェースの準拠規格

種別	規格	名称
10BASE-T, 100BASE-TX, 1000BASE-T, 1000BASE-X, 10GBASE-R **【SB-7800S】**, 10GBASE-W **【SB-7800S】**	ISO/IEC 8802.3 [ANSI/IEEE Std 802.3]	CSMA/CD Access Method and Physical Layer Specifications
	ISO 8802.2 [ANSI/IEEE Std 802.2]	Logical Link Control (LLC)
	IEEE 802.1Q	IEEE Standards for Local and Metropolitan Networks : Virtual Bridged local Area Networks ※
	IEEE Std 802.3x-1997	Specification for 802.3x Full Duplex Operation
	Ethernet V 2.0	The Ethernet-A Local Area Network:Data Link Layer and Physical Layer Specifications
	RFC 894	Standard for the Transmission of IP Datagrams over Ethernet Networks.
	RFC1042	Standard for the Transmission of IP Datagrams over IEEE802 Networks.
	RFC1398	Definitions of Managed Objects for the Ethernet-like Interface Types.
	RFC1757	Remote Network Monitoring Management Information Base.
	RFC2464	Transmission of IPv6 Packets over Ethernet Networks
10GBASE-R **【SB-7800S】**, 10GBASE-W **【SB-7800S】**	IEEE 802.3ae Standard-2002	Media Access Control(MAC) Parameters, Physical Layer, and Management Parameters for 10Gb/s Operation

注　1000BASE-LH の光インタフェースは標準化されていないため本装置の独自仕様です。
注※　GVRP/GMRP はサポートしていません。

表 A-2　リンクアグリゲーションの準拠規格

規格	名称
IEEE802.3ad (IEEE Std 802.3ad-2000)	Aggregation of Multiple Link Segments

付録 A.2　POS【SB-7800S】

表 A-3　POS の準拠規格

種別	規格	名称
OC-192c/STM-64 POS	ITU-T G.691(10/2000)	Optical interfaces for single channel STM-64, STM-256 systems and other SDH systems with optical amplifiers
	Bellcore GR-253-COREIssue 2 Revision 2	Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria
	RFC1332	The PPP Internet Protocol Control Protocol (IPCP)

種別	規格	名称
	RFC1377	The PPP OSI Network Layer Control Protocol (OSINLCP)
	RFC1661	The Point-to-Point Protocol (PPP)
	RFC1662	PPP in HDLC-like Framing
	RFC2472	IP Version 6 over PPP
	RFC2615	PPP over SONET/SDH
OC-48c/STM-16 POS	ITU-T G.957(06/99)	Optical interfaces for equipments and systems relating to the synchronous digital hierarchy
	ITU-T G.958(11/94)	Digital line systems based on the synchronous digital hierarchy for use on optical fiber cables
	Bellcore GR-253-COREIssue 2 Revision 2	Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria
	RFC1332	The PPP Internet Protocol Control Protocol (IPCP)
	RFC1377	The PPP OSI Network Layer Control Protocol (OSINLCP)
	RFC1661	The Point-to-Point Protocol (PPP)
	RFC1662	PPP in HDLC-like Framing
	RFC2472	IP Version 6 over PPP
	RFC2615	PPP over SONET/SDH

付録 A.3　レイヤ 2 スイッチ

表 A-4　VLAN の準拠規格および勧告

規格	名称
IEEE802.1Q (IEEE Std 802.1Q-1998)	Virtual Bridged Local Area Networks
IEEE802.1u (IEEE Std 802.1u-2001)	Virtual Bridged Local Area Networks - Amendment 1: Technical and editorial corrections
IEEE802.1v (IEEE Std 802.1v-2001)	Virtual Bridged Local Area Networks - Amendment 2: VLAN Classification by Protocol and Port

表 A-5　スパニングツリーの準拠規格および勧告

規格	名称
IEEE802.1D (ANSI/IEEE Std 802.1D-1998 Edition)	Media Access Control (MAC) Bridges (The Spanning Tree Algorithm and Protocol)
IEEE802.1t (IEEE Std 802.1t-2001)	Media Access Control (MAC) Bridges - Amendment 1
IEEE802.1w (IEEE Std 802.1w-2001)	Media Access Control (MAC) Bridges - Amendment 2: Rapid Reconfiguration
IEEE802.1s (IEEE Std 802.1s-2002)	Virtual Bridged Local Area Networks - Amendment 3: Multiple Spanning Trees

表 A-6　IGMP snooping/MLD snooping の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC4541(2006 年 5 月)	Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

付録 A.4　IPv4 ネットワーク

表 A-7　IP バージョン 4 の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC791(1981 年 9 月)	Internet Protocol
RFC792(1981 年 9 月)	Internet Control Message Protocol
RFC826(1982 年 11 月)	An Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware
RFC922(1984 年 10 月)	Broadcasting Internet datagrams in the presence of subnets
RFC950(1985 年 8 月)	Internet Standard Subnetting Procedure
RFC1027(1987 年 10 月)	Using ARP to implement transparent subnet gateways
RFC1122(1989 年 10 月)	Requirements for Internet hosts-communication layers
RFC1519(1993 年 9 月)	Classless Inter-Domain Routing (CIDR):an Address Assignment and Aggregation Strategy
RFC1812(1995 年 6 月)	Requirements for IP Version 4 Routers
RFC1933(1996 年 4 月)	Transition Mechanisms for IPv6 Hosts and Routers

表 A-8　DHCP/BOOTP リレーエージェントの準拠規格および勧告

規格番号 (発行年月)	規格名
RFC1542(1993 年 10 月)	Clarifications and Extensions for the Bootstrap Protocol
RFC1812(1995 年 6 月)	Requirements for IP Version 4 Routers
RFC2131(1997 年 3 月)	Dynamic Host Configuration Protocol
RFC3046(2001 年 1 月)	DHCP Relay Agent Information Option

表 A-9　DHCP サーバ機能の準拠規格

規格番号 (発行年月)	規格名
RFC2131(1997 年 3 月)	Dynamic Host Configuration Protocol
RFC2132(1997 年 3 月)	DHCP Options and BOOTP Vendor Extensions
RFC2136(1997 年 4 月)	Dynamic Updates in the Domain Name System (DNS UPDATE)
RFC3679(2004 年 1 月)	Unused Dynamic Host Configuration Protocol (DHCP) Option Codes

表 A-10　DNS リレー機能の準拠規格

規格番号 (発行年月)	規格名
RFC1034(1987 年 3 月)	Domain names - concepts and facilities
RFC1035(1987 年 3 月)	Domain names - implementation and specification

付録 A.5　RIP/OSPF

表 A-11　RIP/OSPF の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC1058(1988 年 6 月)	Routing Information Protocol
RFC2453(1998 年 11 月)	RIP Version 2
RFC2328(1998 年 4 月)	OSPF Version 2
RFC1587(1994 年 3 月)	The OSPF NSSA Option
RFC1519(1993 年 9 月)	Classless Inter-Domain Routing(CIDR): an Address Assignment and Aggregation Strategy
RFC2370(1998 年 7 月)	The OSPF Opaque LSA Option
RFC3623(2003 年 11 月)	Graceful OSPF Restart
RFC3137(2001 年 6 月)	OSPF Stub Router Advertisement

付録 A.6　BGP4【OP-BGP】

表 A-12　BGP4 の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC1771(1995 年 3 月)	A Border Gateway Protocol 4 (BGP-4)
RFC2796(2000 年 4 月)	BGP Route Reflection An alternative to full mesh IBGP
RFC1997(1996 年 8 月)	BGP Communities Attribute
RFC1519(1993 年 9 月)	Classless Inter-Domain Routing(CIDR): an Address Assignment and Aggregation Strategy
RFC1965(1996 年 6 月)	Autonomous System Confederation for BGP
RFC2842(2000 年 5 月)	Capabilities Advertisement with BGP-4
RFC2918(2000 年 9 月)	Route Refresh Capability for BGP-4
RFC2385(1998 年 8 月)	Protection of BGP Sessions via the TCP MD5 Signature Option
draft-ietf-idr-restart-10.txt (2004 年 6 月)	Graceful Restart Mechanism for BGP

付録 A.7　IS-IS【OP-ISIS】

表 A-13　IS-IS の準拠規格および勧告

規格番号	規格名
ISO 9542:1988	Information processing systems - Telecommunications and information exchange between systems - End system to Intermediate system routing exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode network service (ISO 8473)
ISO/IEC 10589:1992	Information technology - Telecommunications and information exchange between system - Intermediate system to Intermediate system intra-domain routing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode Network Service (ISO 8473)
RFC1195(1990 年 12 月)	Use of OSI IS-IS for Routing in TCP/IP and Dual Environments

規格番号	規格名
RFC2763(2000 年 2 月)	Dynamic Hostname Exchange Mechanism for IS-IS
RFC2966(2000 年 10 月)	Domain-wide Prefix Distribution with Two-Level IS-IS
RFC3277(2002 年 4 月)	Intermediate System to Intermediate System (IS-IS) Transient Blackhole Avoidance
RFC3373(2002 年 9 月)	Three-Way Handshake for IS-IS Point-to-Point Adjacencies
RFC3567(2003 年 7 月)	Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication
RFC3784(2004 年 6 月)	Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE)
RFC3847(2004 年 7 月)	Restart Signaling for Intermediate System to Intermediate System (IS-IS)
draft-ietf-isis-ipv6-06.txt (2005 年 10 月)	Routing IPv6 with IS-IS

付録 A.8　IPv4 マルチキャスト【OP-MLT】

表 A-14　IP マルチキャストの準拠規格および勧告

規格番号 (発行年月)	規格名
RFC2236	Internet Group Management Protocol,Version2
draft-ietf-idmr-dvmrp-v3-06.txt (1998 年 3 月)	Distance Vector Multicast Routing Protocol
draft-ietf-pim-v2-03.txt (1999 年 6 月)	Protocol Independent Multicast Version2 Dense Mode Specification
RFC2362	Protocol Independent Multicast-Sparse Mode (PIM-SM) : Specification
draft-ietf-pim-sm-v2-new-05.txt (2002 年 3 月) ※ 1	Protocol Independent Multicast-Sparse Mode (PIM-SM) : Specification (revised)
RFC3376	Internet Group Management Protocol, Version 3
RFC4601(2006 年 8 月) ※ 2	Protocol Independent Multicast-Sparse Mode (PIM-SM) : Specification (revised)
draft-ietf-pim-sm-bsr-07.txt ※ 2	Bootstrap Router (BSR) Mechanism for PIM

注※ 1　この規格は PIM-SSM 関連部だけ準拠しています。

注※ 2　この規格は PIM Hello オプションの Generation ID 関連部だけ準拠しています。

付録 A.9　IPv6 ネットワーク

表 A-15　IPv6 ネットワークの準拠規格および勧告

規格番号 (発行年月)	規格名
RFC2373(1998 年 7 月)	IP Version 6 Addressing Architecture
RFC2460(1998 年 12 月)	Internet Protocol, Version 6 (IPv6) Specification
RFC2461(1998 年 12 月)	Neighbor Discovery for IP Version 6 (IPv6)
RFC2462(1998 年 12 月)	IPv6 Stateless Address Autoconfiguration
RFC2463(1998 年 12 月)	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

規格番号 (発行年月)	規格名
RFC2473(1998 年 12 月)	Generic Packet Tunneling in IPv6 Specification
RFC2710(1999 年 10 月)	Multicast Listener Discovery for IPv6
RFC3056(2001 年 2 月)	Connectioin of IPv6 Domains via IPv4 Clouds
draft-ietf-ipv6-deprecate-rh0-01.txt (2007 年 6 月)	Deprecation of Type 0 Routing Headers in IPv6

表 A-16　IPv6 DHCP サーバ機能の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC3315(2003 年 7 月)	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
RFC3633(2003 年 12 月)	IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6
RFC3646(2003 年 12 月)	DNS Configuration Options for DHCPv6
RFC4075(2005 年 3 月)	Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6
RFC3319(2003 年 7 月)	Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers
RFC3736(2004 年 4 月)	Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6

付録 A.10　RIPng/OSPFv3

表 A-17　RIPng/OSPFv3 の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC2080(1997 年 1 月)	RIPng for IPv6
RFC2740(1999 年 12 月)	OSPF for IPv6
RFC3623(2003 年 11 月)	Graceful OSPF Restart
draft-kompella-ospf-opaquev2-00.txt (2002 年 10 月)	OSPFv2 Opaque LSAs in OSPFv3
RFC3137(2001 年 6 月)	OSPF Stub Router Advertisement

付録 A.11　BGP4+【OP-BGP】

表 A-18　BGP4+ の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC1771(1995 年 3 月)	A Border Gateway Protocol 4 (BGP-4)
RFC2545(1999 年 3 月)	Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing
RFC2858(2000 年 6 月)	Multiprotocol Extensions for BGP-4
RFC2842(2000 年 5 月)	Capabilities Advertisement with BGP-4
RFC2796(2000 年 4 月)	BGP Route Reflection An alternative to full mesh IBGP
RFC1965(1996 年 6 月)	Autonomous System Confederation for BGP
RFC2918(2000 年 9 月)	Route Refresh Capability for BGP-4

規格番号 (発行年月)	規格名
RFC1997(1996 年 8 月)	BGP Communities Attribute
RFC2385(1998 年 8 月)	Protection of BGP Sessions via the TCP MD5 Signature Option
draft-ietf-idr-restart-10.txt (2004 年 6 月)	Graceful Restart Mechanism for BGP

付録 A.12　IPv6 マルチキャスト【OP-MLT】

表 A-19　IPv6 マルチキャストの準拠規格および勧告

規格番号 (発行年月)	規格名
RFC2710(1999 年 10 月)	Multicast Listener Discovery (MLD) for IPv6
RFC2362(1998 年 6 月)	Protocol Independent Multicast-Sparse Mode (PIM-SM): Specification
draft-ietf-pim-sm-v2-new-03.txt (2001 年 7 月) ※ 1	Protocol Independent Multicast-Sparse Mode (PIM-SM): Specification (revised)
draft-ietf-pim-sm-v2-new-05.txt (2002 年 3 月) ※ 2	Protocol Independent Multicast-Sparse Mode (PIM-SM): Specification (revised)
RFC3810(2004 年 6 月)	Multicast Listener Discovery Version 2 (MLDv2) for IPv6
RFC4601(2006 年 8 月) ※ 3	Protocol Independent Multicast-Sparse Mode (PIM-SM): Specification (revised)
draft-ietf-pim-pim-sm-bsr-07.txt ※ 3	Bootstrap Router (BSR) Mechanism for PIM

注※ 1　この規格は IPv6 関連部だけ準拠しています。
注※ 2　この規格は PIM-SSM だけ準拠しています。
注※ 3　この規格は PIM Hello オプションの Generation ID 関連部だけ準拠しています。

付録 A.13　Diff-serv

表 A-20　Diff-serv の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC2474(1998 年 12 月)	Definition of the Differentiated Services Field(DS Field) in the IPv4 and IPv6 Headers
RFC2475(1998 年 12 月)	An Architecture for Differentiated Services
RFC2597(1999 年 6 月)	Assured Forwarding PHB Group
RFC2598(1999 年 6 月)	An Expedited Forwarding PHB

付録 A.14　IEEE802.1X

表 A-21　IEEE802.1X の準拠規格および勧告

規格番号 (発行年月)	規格名
IEEE802.1X(2001 年 6 月)	Port-Based Network Access Control
RFC2284(1998 年 3 月)	PPP Extensible Authentication Protocol (EAP)
RFC2865(2000 年 6 月)	Remote Authentication Dial In User Service (RADIUS)

規格番号 (発行年月)	規格名
RFC2866(2000 年 6 月)	RADIUS Accounting
RFC2869(2000 年 6 月)	RADIUS Extensions
RFC3579(2003 年 9 月)	RADIUS Support For Extensible Authentication Protocol (EAP)
RFC3580(2003 年 9 月)	IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines

付録 A.15　VRRP

表 A-22　VRRP の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC2338(1998 年 4 月)	Virtual Router Redundancy Protocol
draft-ietf-vrrp-ipv6-spec-02.txt (2002 年 2 月)	Virtual Router Redundancy Protocol for IPv6
draft-ietf-vrrp-ipv6-spec-07.txt (2004 年 10 月)	Virtual Router Redundancy Protocol for IPv6
RFC3768(2004 年 4 月)	Virtual Router Redundancy Protocol
draft-ietf-vrrp-unified-mib-04.txt (2006 年 9 月)	Definitions of Managed Objects for the VRRP over IPv4 and IPv6

付録 A.16　IEEE802.3ah/UDLD

表 A-23　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.17　SNMP

表 A-24　SNMP の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC1155(1990 年 5 月)	Structure and Identification of Management Information for TCP/IP-based Internets
RFC1157(1990 年 5 月)	A Simple Network Management Protocol (SNMP)
RFC1213(1991 年 3 月)	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC1354(1992 年 7 月)	IP Forwarding Table MIB
RFC1471(1993 年 6 月)	The Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol
RFC1473(1993 年 6 月)	The Definitions of Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol
RFC1474(1993 年 6 月)	The Definitions of Managed Objects for the Bridge Network Control Protocol of the Point-to-Point Protocol

規格番号 (発行年月)	規格名
RFC1643(1994 年 7 月)	Definitions of Managed Objects for the Ethernet-like Interface Types
RFC1657(1994 年 7 月)	Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2
RFC1659(1994 年 7 月)	Definitions of Managed Objects for RS-232-like Hardware Devices using SMIv2
RFC1757(1995 年 2 月)	Remote Network Monitoring Management Information Base
RFC1850(1995 年 11 月)	OSPF Version2 Management Information Base
RFC1901(1996 年 1 月)	Introduction to Community-based SNMPv2
RFC1902(1996 年 1 月)	Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1903(1996 年 1 月)	Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1904(1996 年 1 月)	Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1905(1996 年 1 月)	Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1906(1996 年 1 月)	Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1907(1996 年 1 月)	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1908(1996 年 1 月)	Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework
RFC2115(1997 年 9 月)	Management Information Base for Frame Relay DTEs Using SMIv2
RFC2233(1997 年 11 月)	The Interfaces Group MIB using SMIv2
RFC2452(1998 年 12 月)	IP Version 6 Management Information Base for the Transmission Control Protocol
RFC2454(1998 年 12 月)	IP Version 6 Management Information Base for the User Datagram Protocol
RFC2465(1998 年 12 月)	Management Information Base for IP Version 6: Textual Conventions and General Group
RFC2466(1998 年 12 月)	Management Information Base for IP Version 6: ICMPv6 Group
RFC2495(1999 年 1 月)	Definitions of Managed Objects for the DS1,E1,DS2 and E2 Interface Types
RFC2496(1999 年 1 月)	Definitions of Managed Objects for the DS3/E3 Interface Type
RFC2578(1999 年 4 月)	Structure of Management Information Version 2 (SMIv2)
RFC2579(1999 年 4 月)	Textual Conventions for SMIv2
RFC2580(1999 年 4 月)	Conformance Statements for SMIv2
RFC2787(2000 年 3 月)	Definitions of Managed Objects for the Virtual Router Redundancy Protocol
RFC2932(2000 年 10 月)	IPv4 Multicast Routing MIB
RFC2933(2000 年 10 月)	Internet Group Management Protocol MIB
RFC2934(2000 年 10 月)	Protocol independent Multicast MIB for IPv4
RFC3410(2002 年 12 月)	Introduction and Applicability Statements for Internet Standard Management Framework

規格番号 (発行年月)	規格名
RFC3411(2002 年 12 月)	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC3412(2002 年 12 月)	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC3413(2002 年 12 月)	Simple Network Management Protocol (SNMP) Applications
RFC3414(2002 年 12 月)	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC3415(2002 年 12 月)	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC3416(2002 年 12 月)	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
RFC3417(2002 年 12 月)	Transport Mappings for the Simple Network Management Protocol (SNMP)
RFC3418(2002 年 12 月)	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
RFC3584(2003 年 8 月)	Coexistence between Version 1, Version 2, and Version 3 of the Internet- standard Network Management Framework

付録 A.18　sFlow

表 A-25　sFlow の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC3176(2001 年 9 月)	InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks

付録 A.19　NetFlow【OP-ADV】

表 A-26　NetFlow の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC3954(2004 年 10 月)	Cisco Systems NetFlow Services Export Version 9

付録 A.20　LLDP

表 A-27　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

付録 A.21　RADIUS/TACACS+

表 A-28　RADIUS/TACACS+ の準拠する規格および勧告

規格番号 (発行年月)	規格名
RFC2865(2000 年 6 月)	Remote Authentication Dial In User Service(RADIUS)

規格番号 (発行年月)	規格名
RFC2866(2000 年 6 月)	RADIUS Accounting
draft-grant-tacacs-02.txt (1997 年 1 月)	The TACACS+ Protocol Version 1.78

付録 A.22　SYSLOG

表 A-29　SYSLOG の準拠する規格および勧告

規格番号 (発行年月)	規格名
RFC3164(2001 年 8 月)	The BSD syslog Protocol

付録 A.23　NTP

表 A-30　NTP の準拠する規格および勧告

規格番号 (発行年月)	規格名
RFC1305(1992 年 3 月)	Network Time Protocol (Version 3)

付録 B　謝辞 (Acknowledgments)

[GateD]

Copyright notice:
(C) 1995, 1996, 1997, 1998 The Regents of the University of Michigan
All rights reserved.
Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators.
GateD Release 9.3.3
Copyright (C) 2003 NextHop Technologies, Inc.
All rights reserved.
Copyright (C) 2001 by NextHop Technologies, Inc. and its licensors.
All rights reserved.
Except as stated herein, none of the software and accompanying documentation "materials") provided by NextHop may be copied, reproduced, distributed, republished, downloaded, displayed, posted or transmitted in any form or by any means, including, but not limited to, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of NextHop. All copyright and other proprietary notices contained within NextHop materials must be retained unless otherwise stated. Permission terminates automatically if any of these terms or conditions is breached. Upon termination, all applicable NextHop materials must be immediately destroyed. Any unauthorized use of any NextHop materials may violate copyright laws, trademark laws, the laws of privacy and publicity, and communications regulations and statutes.
Notice: Acceptance of Terms of Use Use of NextHop material is subject to certain Terms of Use, which constitute a legal agreement between you and NextHop. By using this material, you acknowledge that you have read, understood, and agree to be bound by the Terms of Use. Please review the Terms of Use. A copy of NextHop's Terms of Use is available upon request or on the web at http://www.nexthop.com. If you do not agree to the terms, do not use these materials.
Restricted Rights Legend
This software and any associated documentation are provided with RESTRICTED RIGHTS. The Government's rights to use, modify, reproduce, release, perform, display or disclose are restricted by paragraph (b)(3) of the Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation clause at DFAR 252.227-7014 (Jun 95), and the other restrictions and terms in paragraph (g)(3)(i) of Rights in Data-General clause at FAR 52.227-14, Alternative III (Jun 87) and paragraph (c)(2) of the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19 (Jun 87), contained in the above identified contract. Any reproduction of computer software or portions thereof marked with this legend must also reproduce the markings. Any person, other than the Government, who has been provided access to such software must promptly identify the Contractor. The Contractor/Licensor is NextHop Technologies, Inc. located at 517 West William Street, Ann Arbor, MI 48103.

[SNMP]

****
Copyright 1988-1996 by Carnegie Mellon University
All Rights Reserved

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU not be used in advertising or publicity pertaining to distribution of the

software without specific, written prior permission.

CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.
****

Some of this software has been modified by BBN Corporation and is a derivative of software developed by Carnegie Mellon University. Use of the software remains subject to the original conditions set forth above.
****

Some of this software is Copyright 1989 by TGV, Incorporated but subject to the original conditions set forth above.
****

Some of this software is Copyright (C) 1983,1988 Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of California at Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided "as is" without express or implied warranty.
****

* Primary Author:
Steve Waldbusser

* Additional Contributors:
Erik Schoenfelder (schoenfr@ibr.cs.tu-bs.de): additions, fixes and enhancements for Linux by 1994/1995.
David Waitzman: Reorganization in 1996.

Wes Hardaker <hardaker@ece.ucdavis.edu>: Some bug fixes in his UC
Davis CMU SNMP distribution were adopted by David Waitzman

David Thaler <thalerd@eecs.umich.edu>: Some of the code for making the agent embeddable into another application were adopted by David Waitzman

Many more over the years...

[BSDI Internet Server]

BERKELEY SOFTWARE DESIGN, INC.

Copyright (C) 1992, 1993, 1994, 1995, 1996, 1997 Berkeley Software Design, Inc.
This product includes BSDI Internet Server developed by Berkeley Software Design, Inc.

THE REGENTS OF THE UNIVERSITY OF CALIFORNIA

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

Contributors
Sun Microsystems, Inc.
Keith Muller
Mark Nudelman
Jan-Simon Pendry

AT&T (DAVID M. GAY)

Copyright (C) 1991 by AT&T.

Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.

THIS SOFTWARE IS BEING PROVIDED "AS IS", WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. IN PARTICULAR, NEITHER THE AUTHOR NOR AT&T MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE.

INFO-ZIP GROUP

This product includes Info-ZIP's software which is used for a part of the boot program. Info-ZIP's software (ZIP, UnZip and related utilities) is free and can be obtained as source code or executables from various bulletin board services and anonymous-ftp sites, including CompuServe's IBMPRO forum and ftp.uu.net:/pub/archiving/zip/*.

INTERNET SOFTWARE CONSORTIUM

Copyright (C) 1996 by Internet Software Consortium.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND INTERNET SOFTWARE CONSORTIUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL INTERNET SOFTWARE CONSORTIUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

SIGMASOFT, TH. LOCKERT

Copyright (C) 1994 SigmaSoft, Th. Lockert <tholo@sigmasoft.com>
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

SUN MICROSYSTEMS, INC.

Copyright (C) 1984, 1985, 1986, 1987, 1988, 1993 Sun Microsystems, Inc.

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part. Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

Sun Microsystems, Inc.
2550 Garcia Avenue
Mountain View, California 94043

UNIVERSITY OF TORONTO

Copyright (C) 1986 by University of Toronto.
Written by Henry Spencer. Not derived from licensed software.

Permission is granted to anyone to use this software for any purpose on any computer system, and to redistribute it freely,
subject to the following restrictions:

1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from defects in it.
2. The origin of this software must not be misrepresented, either by explicit claim or by omission.
3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software.

WASHINGTON UNIVERSITY IN SAINT LOUIS

Copyright (C) 1993, 1994 Washington University in Saint Louis
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the Washington University in Saint Louis and its contributors. 4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY WASHINGTON UNIVERSITY AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL WASHINGTON UNIVERSITY OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

WILDBOAR

Portions or all of this file are Copyright (C) 1994,1995,1996
Yoichi Shinoda, Yoshitaka Tokugawa, WIDE Project, Wildboar Project and Foretune. All rights reserved.

This code has been contributed to Berkeley Software Design, Inc. by the Wildboar Project and its contributors.

The Berkeley Software Design Inc. software License Agreement specifies the terms and conditions for redistribution.

THIS SOFTWARE IS PROVIDED BY THE WILDBOAR PROJECT AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR

PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE WILDBOAR PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

MARTIN BIRGMEIER

Copyright (C) 1993 Martin Birgmeier
All rights reserved.

You may redistribute unmodified or modified versions of this source code provided that the above copyright notice and this and the following conditions are retained.

This software is provided "as is", and comes with no warranties of any kind. I shall in no event be liable for anything that happens to anyone/anything when using this software.

CHRISTOPHER G. DEMETRIOU

Copyright (C) 1993, 1994 Christopher G. Demetriou
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by Christopher G. Demetriou.
4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

DAVID HOVEMEYER

Copyright (C) 1995 David Hovemeyer <daveho@infocom.com>

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE DEVELOPERS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE DEVELOPERS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

FRANK VAN DER LINDEN

Copyright (C) 1995 Frank van der Linden
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed for the NetBSD Project by Frank van der Linden
4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THEO DE RAADT

Copyright (C) 1992/3 Theo de Raadt <deraadt@fsa.ca>
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

HENRY SPENCER

Copyright 1992, 1993, 1994 Henry Spencer. All rights reserved.
This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California.

Permission is granted to anyone to use this software for any purpose on any computer system, and to alter it and redistribute it, subject to the following restrictions:

1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from flaws in it.
2. The origin of this software must not be misrepresented, either by explicit claim or by omission. Since few users ever read sources, credits must appear in the documentation.
3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software. Since few users ever read sources, credits must appear in the documentation.
4. This notice may not be removed or altered.

[diff, grep]

Copyright (C) 1988, 1989, 1992, 1993, 1994 Free Software Foundation, Inc.

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

[less]

[tcpd]

[tcpdump]

[libpcap]

License: BSD

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

[traceroute]

Copyright (C) 1988, 1989, 1991, 1994, 1995, 1996

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that: (1) source code distributions retain the above copyright notice and this paragraph in its entirety, (2) distributions including binary code include the above copyright notice and this paragraph in its entirety in the documentation or other materials provided with the distribution, and (3) all advertising materials mentioning features or use of this software display the following acknowledgement: "This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors." Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

[zlib]

Copyright notice:

(C) 1995-1996 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly　　Mark Adler

gzip@prep.ai.mit.edu　madler@alumni.caltech.edu

If you use the zlib library in a product, we would appreciate *not* receiving lengthy legal documents to sign. The sources are provided for free but without warranty of any kind. The library has been entirely written by Jean-loup Gailly and Mark Adler; it does not include third-party code.

If you redistribute modified sources, we would appreciate that you include in the file ChangeLog history information documenting your changes.

[Apache HTTP server]

Copyright (C) 2000 The Apache Software Foundation. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the Apache Software Foundation (http://www.apache.org/)."
Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.
4. The names "Apache" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.
5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.
THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[Xntp Program]

The following copyright notice applies to all files collectively called the Network Time Protocol Version 4 Distribution. Unless specifically declared otherwise in an individual file, this notice applies as if the text was explicitly included in the file.

Copyright (C) David L. Mills 1992, 1993, 1994, 1995, 1996 Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name University of Delaware not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. The University of Delaware makes no representations about the

suitability this software for any purpose. It is provided "as is" without express or implied warranty.

[MD5 Program]

Adapted from the RSA Data Security, Inc.
MD5 Message-Digest Algorithm.

[pimdd]

Permission to use, copy, modify, and distribute this software and its documentation in source and binary forms for lawful purposes and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of Oregon. The name of the University of Oregon may not be used to endorse or promote products derived from this software without specific prior written permission.

THE UNIVERSITY OF OREGON DOES NOT MAKE ANY REPRESENTATIONS ABOUT THE SUITABILITY OF THIS SOFTWARE FOR ANY PURPOSE. THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT.

IN NO EVENT SHALL UO, OR ANY OTHER CONTRIBUTOR BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES, WHETHER IN CONTRACT, TORT, OR OTHER FORM OF ACTION, ARISING OUT OF OR IN CONNECTION WITH, THE USE OR PERFORMANCE OF THIS SOFTWARE.

Other copyrights might apply to parts of this software and are so noted when applicable.

Questions concerning this software should be directed to Kurt Windisch (kurtw@antc.uoregon.edu)

$Id: LICENSE,v 1.2 1998/05/29 21:58:19 kurtw Exp $

Part of this program has been derived from PIM sparse-mode pimd. The pimd program is covered by the license in the accompanying file named "LICENSE.pimd".

The pimd program is COPYRIGHT 1998 by University of Southern California.

Part of this program has been derived from mrouted. The mrouted program is covered by the license in the accompanying file named "LICENSE.mrouted".

The mrouted program is COPYRIGHT 1989 by The Board of Trustees of Leland Stanford Junior University.

[mrouted]

The mrouted program is covered by the following license. Use of the mrouted program represents acceptance of these terms and conditions.

1. STANFORD grants to LICENSEE a nonexclusive and nontransferable license to use, copy and

modify the computer software "mrouted" (hereinafter called the "Program"), upon the terms and conditions hereinafter set out and until Licensee discontinues use of the Licensed Program.

2. LICENSEE acknowledges that the Program is a research tool still in the development state, that it is being supplied "as is," without any accompanying services from STANFORD, and that this license is entered into in order to encourage scientific collaboration aimed at further development and application of the Program.

3. LICENSEE may copy the Program and may sublicense others to use object code copies of the Program or any derivative version of the Program. All copies must contain all copyright and other proprietary notices found
in the Program as provided by STANFORD. Title to copyright to the Program remains with STANFORD.

4. LICENSEE may create derivative versions of the Program. LICENSEE hereby grants STANFORD a royalty-free license to use, copy, modify, distribute and sublicense any such derivative works. At the time LICENSEE provides a copy of a derivative version of the Program to a third party, LICENSEE shall provide STANFORD with one copy of the source code of the derivative version at no charge to STANFORD.

5. STANFORD MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. By way of example, but not limitation, STANFORD MAKES NO REPRESENTATION OR WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE LICENSED PROGRAM WILL NOT INFRINGE ANY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. STANFORD shall not be held liable for any liability nor for any direct, indirect or consequential damages with respect to any claim by LICENSEE or any third party on account of or arising from this Agreement or use of the Program.

6. This agreement shall be construed, interpreted and applied in accordance with the State of California and any legal action arising out of this Agreement or use of the Program shall be filed in a court in the State of California.

7. Nothing in this Agreement shall be construed as conferring rights to use in advertising, publicity or otherwise any trademark or the name of ``Stanford".

The mrouted program is COPYRIGHT 1989 by The Board of Trustees of Leland Stanford Junior University.

[PIM sparse-mode pimd]

Copyright (C) 1998 by the University of Southern California.
All rights reserved.

Permission to use, copy, modify, and distribute this software and its documentation in source and binary forms for lawful purposes and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of Southern California and/or Information Sciences Institute. The name of the University of Southern California may not be used to endorse or promote products derived from this software without specific prior written permission.

THE UNIVERSITY OF SOUTHERN CALIFORNIA DOES NOT MAKE ANY REPRESENTATIONS ABOUT THE SUITABILITY OF THIS SOFTWARE FOR ANY PURPOSE. THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT.

IN NO EVENT SHALL USC, OR ANY OTHER CONTRIBUTOR BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES, WHETHER IN CONTRACT, TORT, OR OTHER FORM OF ACTION, ARISING OUT OF OR IN CONNECTION WITH, THE USE OR PERFORMANCE OF THIS SOFTWARE.

Other copyrights might apply to parts of this software and are so noted when applicable.

Questions concerning this software should be directed to Pavlin Ivanov Radoslavov (pavlin@catarina.usc.edu)

$Id: LICENSE.pimd,v 1.1 1998/05/29 21:58:20 kurtw Exp $

Part of this program has been derived from mrouted.
The mrouted program is covered by the license in the accompanying file named "LICENSE.mrouted".

The mrouted program is COPYRIGHT 1989 by The Board of Trustees of Leland Stanford Junior University.

[LTCS (Label Traffic Control System)]

Copyright (C) 1999 Harris and Jefferies Inc. All rights reserved.
Copyright (C) 2000 NetPlane Systems Inc. All rights reserved.

[KAME IPv6 STACK]

Copyright (C) 1995, 1996, 1997, 1998, 1999 and 2000 WIDE Project.All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)

HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[CRUNCH]

[RADIUS]

[totd]

WIDE

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
This product includes software developed by WIDE Project and and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

University of Tromso

Copyright (C) 1999,2000,2001,2002 University of Tromso, Norway. All rights reserved.

Author: Feike W. Dillema, The Pasta Lab, Institutt for Informatikk University of Tromso, Norway

Permission to use, copy, modify and distribute this software and its documentation is hereby granted, provided that both the copyright notice and this permission notice appear in all copies of the software, derivative works or modified versions, and any portions thereof, and that both notices appear in supporting documentation.
THE UNIVERSITY OF TROMSO ALLOWS FREE USE OF THIS SOFTWARE IN ITS "AS IS" CONDITION. THE UNIVERSITY OF TROMSO DISCLAIMS ANY LIABILITY OF ANY KIND FOR ANY DAMAGES WHATSOEVER RESULTING FROM THE USE OF THIS SOFTWARE.
The author requests users of this software to send back any improvements or extensions that they make and grant him and/or the University the rights to redistribute these changes without restrictions.

Invenia Innovation A.S.

Copyright (C) Invenia Innovation A.S., Norway. All rights reserved.

Author: Feike W. Dillema, Invenia Innovation A.S., Norway.

Permission to use, copy, modify and distribute this software and its documentation is hereby granted, provided that both the copyright notice and this permission notice appear in all copies of the software, derivative works or modified versions, and any portions thereof, and that both notices appear in supporting documentation.
INVENIA INNOVATION A.S. ALLOWS FREE USE OF THIS SOFTWARE IN ITS "AS IS" CONDITION. INVENIA INNOVATION A.S. DISCLAIMS ANY LIABILITY OF ANY KIND FOR ANY DAMAGES WHATSOEVER RESULTING FROM THE USE OF THIS SOFTWARE.
The author requests users of this software to send back any improvements or extensions that they make and grant him and/or the Invenia Innovation the rights to redistribute these changes without restrictions.

Todd C. Miller

Copyright (C) 1998 Todd C. Miller <Todd.Miller@courtesan.com> All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES,INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[libtacplus]

Copyright (C) 1998, 2001, 2002, Juniper Networks, Inc.
All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[tftp]

Copyright (C) 1983, 1993
The Regents of the University of California. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and

[libfetch]

[iides]

[Net-SNMP]

CMU/UCD

Networks Associates Technology, Inc

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Cambridge Broadband Ltd.

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.
All rights reserved.

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Sun Microsystems, Inc.

Copyright (c) 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara,
California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Sparta, Inc

Copyright (c) 2003-2004, Sparta, Inc
All rights reserved.

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,

PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Cisco/BUPTNIC

Copyright (c) 2004, Cisco, Inc and Information Network
Center of Beijing University of Posts and Telecommunications.
All rights reserved.

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

付録 C　用語解説

（英字）

ARP（Address Resolution Protocol）

IPv4 ネットワークで使用する通信プロトコルです。

AS（Autonomous System）

単一の管理権限で運用している独立したネットワークシステムのことを指します。

AS 境界ルータ

OSPF を使用して，AS 外経路を OSPF 内に導入するルータです。

BGP4（Border Gateway Protocol - version 4）

IPv4 ネットワークで使用する経路制御プロトコルです。

BGP4+（Multiprotocol Extensions for Border Gateway Protocol - version 4）

IPv6 ネットワークで使用する経路制御プロトコルです。

BGP4+ スピーカ

BGP4+ が動作するルータのことです。

BGP スピーカ

BGP が動作するルータのことです。

BPDU（Bridge Protocol Data Unit）

ブリッジ間でやり取りされるフレームです。

BSU（Basic packet Switching module）

ルーティング・QoS テーブル検索エンジンおよびパケット送信エンジンを持ち，ハードウェアでルーティングテーブル，フィルタリング・テーブルおよび QoS テーブルを検索し，パケットの送受信を行います。これによって高速な処理を実現しています。

CP 輻輳制御

BCU 内の CP で行う輻輳制御方式のことです。
自装置宛のフレームの輻輳を検知すると，その要因のフレームの受信を止めます。この制御の繰り返しによって，正常に動作している VLAN を収容しているポートの自宛通信への影響を抑えられます。

DHCP（Dynamic Host Configuration Protocol）

ネットワーク接続時に IP アドレスを自動設定するプロトコルです。リレーエージェント機能，サーバ機能およびクライアント機能があります。

DHCP/BOOTP リレーエージェント機能

DHCP/BOOTP サーバと DHCP/BOOTP クライアントが異なるサブネットにあるとき，コンフィグレーションで設定したサーバの IP アドレスを DHCP/BOOTP パケットの宛先 IP アドレスに設定して，パケットをサブネット間中継する機能です。

DHCP サーバ機能

IPv4 DHCP クライアントに対して，IP アドレスなどの環境情報（構成情報）を動的に割り当てるための機能です。

Diff-serv（Differentiated services）機能

IP パケットのヘッダ情報から優先度を決定して，その優先度に従ってルータが処理する機能です。

DNS リレー

DNS(Domain Name System) システムの異なるサブネットワークに存在するサーバとクライアント間で，クライアントからのパケットをドメインネームサーバのアドレスに中継する機能です。

DSCP（Differentiated Services Code Point）

IP フローの IP ヘッダ内 DS Field の上位 6 ビットです。

DS ドメイン

Diff-serv 機能を提供するネットワークです。

DVMRP（Distance Vector Multicast Routing Protocol）

IPv4 マルチキャストで使用する距離ベクトル型の経路制御プロトコルです。

EAP（Extensible Authentication Protocol）

拡張可能な認証プロトコル。具体的なセキュリティー機能を持たないため，EAP の中で使用される各種の認証プロトコルが実際のセキュリティー機能を提供します。

EAPOL（EAP Over LAN）

LAN 上で動作する拡張可能な認証プロトコル。IEEE802.1X に規定されている EAP のメッセージを LAN 上で伝送するための仕組みです。

EFM（Ethernet in the First Mile）

IEEE802.3ah 規格のことです。

FDB（Filtering Data Base）

トランスペアレント・ブリッジで使用されるテーブルです。FDB にはフレームの送信元 MAC アドレス，フレームを受信したポートおよび監視時刻が記録されます。

GSRP（Gigabit Switch Redundancy Protocol）

GSRP はレイヤ 2 のネットワークで，スイッチに障害が発生した場合でも，同一ネットワーク上の別スイッチを経由して通信経路を確保することを目的としたレイヤ 2 での装置の冗長化を実現する機能です。

ICMP（Internet Control Message Protocol）

IPv4 ネットワークで使用する通信プロトコルです。

ICMPv6（Internet Control Message Protocol version 6）

IPv6 ネットワークで使用する通信プロトコルです。

IGMP（Internet Group Management Protocol）

IPv4 ネットワークで使用するホスト - ルータ間のマルチキャストグループ管理プロトコルです。

IPv4（Internet Protocol version 4）

32 ビットの IP アドレスを持つインターネットプロトコルです。

IPv4 マルチキャスト

IPv4 マルチキャストは，ネットワーク内で選択されたグループに対して同一の情報を送信します。マルチキャストは送信者が受信者ごとにデータを複製する必要がないため，受信者の数に関係なくネットワークの負荷が軽減します。

IPv6（Internet Protocol version 6）

128 ビットの IP アドレスを持つインターネットプロトコルです。

IPv6 DHCP サーバ機能

IPv6 DHCP クライアントに対して，プレフィックス，DNS サーバアドレスなどの環境情報（構成情報）を動的に割り当てるための機能です。

IPv6 グローバルアドレス

アドレスプレフィックスの上位 3 ビットが 001 で始まるアドレスです。経路情報の集約を目的とした階層形式になっています。IPv6 グローバルアドレスは世界で一意なアドレスで，インターネットを使用した通信に使用されます。

IPv6 サイトローカルアドレス

アドレスプレフィックスの上位 10 ビットが 1111 1110 11 で，64 ビットのインタフェース ID 部を含むアドレスです。同一サイト内だけで有効なアドレスで，インターネットに接続されていないネットワークで自由に IPv6 アドレスを付ける場合に使用されます。

IPv6 マルチキャスト

IPv6 マルチキャストは IPv4 マルチキャストと同様の機能を IPv6 で実現します。

IPv6 リンクローカルアドレス

アドレスプレフィックスの上位 64 ビットが fe80:: で，64 ビットのインタフェース ID 部を含むアドレスです。同一リンク内だけで有効なアドレスで，自動アドレス設定，近隣探索，またはルータがないときに使用されます。

IS-IS

IS-IS は，ルータ間の接続の状態から構成されるトポロジに基づき最短経路を計算するリンクステートプロトコルです。

LLDP（Link Layer Discovery Protocol）

隣接する装置情報を収集するプロトコルです。

MAC VLAN

送信元の MAC アドレス単位にグループ分けを行う VLAN です。

MIB（Management Information Base）

機器についての情報を表現するオブジェクトです。SNMP プロトコルで使用します。

MLD（Multicast Listener Discovery）

ルータ - ホスト間で使用される IPv6 マルチキャストグループ管理プロトコルです。

NAT（Network Address Translation）

ローカルネットワークのプライベートアドレスをインターネットなどで使用するグローバルアドレスに変換する機能です。

NDP（Neighbor Discovery Protocol）

IPv6 ネットワークで使用する通信プロトコルです。

NetFlow 統計

ネットワークを流れるトラフィックをサンプリングしてモニタし，モニタした NetFlow 統計情報を NetFlow コレクタと呼ばれる装置に集めて分析することによって，ネットワークの利用状況を把握する機能です。

NIF（Network Interface board）

接続する各メディアに対応したインタフェースを持つコンポーネントです。物理レイヤを処理します。

OADP（Octpower Auto Discovery Protocol）

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する機能です。

OAM（Operations, Administration, and Maintenance）

ネットワークでの保守運用管理のことです。

OSPF（Open Shortest Path First）

IPv4 ネットワークで使用する経路制御プロトコルです。

OSPFv3

IPv6 ネットワークで使用する経路制御プロトコルです。

OSPF ドメイン

本装置と接続している独立した各 OSPF ネットワークのことです。

OSPF マルチバックボーン

本装置で 1 台のルータ上で複数の OSPF ネットワークと接続して，OSPF ネットワークごとに個別に経路の交換，生成などを行う機能です。

PHB（Per Hop Behavior）

インテリアリードで DSCP に基づいた優先転送動作のことをいいます。

PIM-DM（Protocol Independent Multicast-Dense Mode）

DVMRP のように基盤になっているユニキャスト IPv4 の経路モジュールに依存しないでマルチキャストの経路制御ができるプロトコルです。パケットの送信後，不要な経路を除外します。

PIM-SM（Protocol Independent Multicast-Sparse Mode）

DVMRP のように基盤になっているユニキャスト IPv4 の経路モジュールに依存しないでマルチキャストの経路制御ができるプロトコルです。ランデブーポイントへのパケット送信後，Shortest path で通信します。

PIM-SSM （Protocol Independent Multicast-Source Specific Multicast）

PIM-SM の拡張機能で，ランデブーポイントを使用しないで最短パスで通信する経路制御プロトコルです。

PPP（Point-to-Point Protocol）

シリアル回線用の通信プロトコルです。非同期接続ができます。

PSU（Packet Switching Module）

パケットスイッチングモジュールです。パケット転送エンジンとルーティング・QoS テーブル検索エンジンを持ち，ルーティングテーブル，フィルタリング・テーブル，QoS テーブルを検索して，IP パケットを送受信します。

QoS（Quality of Service）制御

実時間型・帯域保証型トラフィックに対して，通信の遅延やスループットなどの通信品質を制御する機能です。

RADIUS（Remote Authentication Dial In User Service）

NAS(Network Access Server) に対して認証・課金を提供するプロトコルです。

RFC（Request For Comments）

TCP/IP に関する仕様を記述している公開文書です。

RIP（Routing Information Protocol）

IPv4 ネットワークで使用する経路制御プロトコルです。

RIPng（Routing Information Protocol next generation）

IPv6 ネットワークで使用する経路制御プロトコルです。

RM（Routing Manager）

ルーティングマネージャです。装置全体の管理およびルーティングプロトコル処理を行います。また，ルーティングテーブルを作成・更新して PSU(SB-5400S では BSU) に配布します。

RMON（Remote Network Monitoring）

イーサネット統計情報を提供する機能です。

RTT（Round Trip Time）

ラウンド・トリップ・タイム。パケットがネットワークを一往復する時間です。

sFlow 統計

sFlow 統計はエンド - エンドのトラフィック（フロー）特性や隣接するネットワーク単位のトラフィック特性の分析を行うため，ネットワーク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。

SNMP（Simple Network Management Protocol）

ネットワーク管理プロトコルです。

TACACS+（Terminal Access Controller Access Control System Plus）

NAS(Network Access Server) に対して認証・課金を提供するプロトコルです。

Tag-VLAN

IEEE が標準化した VLAN の一つで，イーサネットフレームに Tag と呼ばれる識別子を埋め込むことで VLAN 情報を離れたセグメントに伝えることができる VLAN です。

UDLD（Uni-Directional Link Detection）

片方向リンク障害を検出する機能です。

UDP（User Datagram Protocol）

トランスポート層の通信プロトコルです。

UPC（Usage Parameter Control）

最大帯域制限，最低帯域監視を行う機能です。

VLAN 単位認証（静的）

IEEE802.1X 認証で使用される基本認証モードです。
本モードでは，ポート VLAN に所属する端末に対して IEEE802.1X 認証を行います。

VLAN 単位認証（動的）

IEEE802.1X 認証で使用される基本認証モードです。
本モードで認証に成功した端末は，認証サーバである RADIUS サーバから指定された VLAN ID に該当する MAC VLAN へ動的に所属します。

VRRP（Virtual Router Redundancy Protocol）

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通信経路を確保する，ホットスタンバイ機能です。この機能を使用すると，同一イーサネット上の複数ルータから構成される仮想ルータを定義できます。エンドホスト側はデフォルトとして仮想ルータを設定しておけば，ルータに障害が発生した場合でも別ルータの切り替えを意識する必要がありません。

（ア行）

イコールコストマルチパス

ある 2 点間にコストが同じ経路が複数ある場合に，この複数の経路のことをイコールコストマルチパスといいます。

インターナルピア
同じ AS 内に属し，物理的に直接接続された BGP スピーカ間に形成するピアです。ピアリングに使用する IP アドレスは直接接続されたインタフェースのインタフェースアドレスを使用します。

インタフェース
本装置で IP アドレスを付与する単位です。

インデックス
MIB を限定するための情報です。

インテリアノード
DS ドメインで，DSCP に基づいた転送動作だけを行うノードです。

インポート・フィルタ
指定プロトコルで受信したルーティング・パケットの経路情報をルーティングテーブルに取り込むかどうかをフィルタリング条件に従って制御します。

運用端末
本装置の運用管理に使用するコンソールまたはリモート運用端末のことを運用端末と呼びます。

エキスターナルピア
異なる AS に属する BGP スピーカ間に形成するピアです。ピアリングに使用する IP アドレスは直接接続されたインタフェースのインタフェースアドレスを使用します。

エキスポート・フィルタ
ルータ上で同時に動作しているルーティングプロトコル間での経路情報の再配布を制御します。エキスポート・フィルタでは配布先プロトコルのフィルタリング条件と学習元プロトコルのフィルタリング条件によって，特定の宛先に特定の経路情報を送出します。

エリアボーダルータ
複数のエリアに所属するルータです。所属するすべてのエリアについて，個別に経路選択を行います。

オブジェクト ID
MIB を特定するための識別 ID です。root から各ノードの数値をならべて番号をつけることで，MIB を一意に識別できます。

（カ行）

仮想リンク
仮想の回線のことです。仮想リンクの実際の経路があるエリアのことを仮想リンクの通過エリアといいます。

均等最低帯域保証
送信帯域の均等最低保証を行う機能です。キューごとに割り当てられた帯域分だけを送信します。ただし，回線の帯域が空いていれば，空いている帯域も使用して送信します。

均等保証
出力キューからパケットを送信するときの送信順を，1 キュー当たり 1 パケットにして各キューから順番に送信する機能です。

クラシファイア
TCP/IP ヘッダからフローを識別して，個々のユーザとの契約に基づいて DSCP に分類・集約する機能です。バウンダリノードが持っている機能です。

コンフィグレーションファイル

ネットワークの運用環境に合わせて構成および動作条件を設定するファイルです。このファイルはテキストファイル形式で MC に格納します。コンフィグレーションファイルには次に示す種類があります。

- スタートアップコンフィグレーションファイル
  本装置の立ち上げに使用します。このコンフィグレーションに従って運用されます。
- バックアップコンフィグレーションファイル
  スタートアップコンフィグレーションファイルのコピー，または将来のネットワークの変更に備えた編集用として使用します。
- 一時保存コンフィグレーションファイル
  運用中にコンフィグレーションを変更して MC に格納した場合に，編集前のスタートアップコンフィグレーションファイルを一時保存したものです。

（サ行）

最低帯域保証

送信帯域の最低保証を行う機能です。キューごとに指定された帯域分だけを送信します。ただし，回線の帯域が空いていれば，空いている帯域も使用して送信します。

シェーパ

バウンダリノードで送信帯域を制御する機能です。

重要パケット保護機能

保証帯域内で，重要なパケットは優先的に保証帯域内パケットとして転送し，通常のパケットは重要なパケットが全保証帯域を使用して転送していない場合に保証帯域内パケットとして転送する機能です。

出力優先制御

出力優先度に従って優先パケットの追い越しを行う制御です。出力優先度の高いキューに積まれたパケットをすべて送信したあとで，より低いキューに積まれたパケットを送信します。

スタティックルーティング

ユーザがコンフィグレーションによって経路情報を設定するルーティング方法です。

ステートレスアドレス自動設定機能

IPv6 リンクローカルアドレスを装置内で自動生成する機能，ホストが IPv6 アドレスを自動生成するときに必要な情報を通知する機能です。

スパニングツリー・アルゴリズム

ブリッジによるルーティングで使用されるアルゴリズムで，論理的木構造を形成します。このアルゴリズムによって任意の二つの ES 間で単一の経路を決定でき，フレームのループ周回を防ぐことができます。

スパニングツリー・プロトコル

スパニングツリー・プロトコルは，ループ防止プロトコルです。スパニングツリー・プロトコルを使用することで，スイッチ間でお互いに通信し，ネットワーク上の物理ループを発見することができます。

スループット

コンピュータ間の通信での実質的な通信速度（実行速度）のことです。

（タ行）

帯域制御

物理ポート単位の最大帯域制限，およびキューごとの最低帯域監視，最大帯域制限，余剰帯域分配を行う機能です。

ダイナミックルーティング

ルーティングプロトコルによってネットワーク内の他ルータと経路情報を交換して経路を選択するルーティング方法です。

トラップ

SNMP エージェントから SNMP マネージャに非同期に通知されるイベント通知です。

（ナ行）

認証デフォルト VLAN 機能

IEEE802.1X の VLAN 単位認証（動的）モードで使用される機能です。
IEEE802.1X 未対応端末，認証失敗，認証成功後の MAC VLAN への動的割り当てが失敗した端末は，デフォルト VLAN またはコンフィグレーションで指定されたポート VLAN に所属します。
認証前の端末は，いったんこの認証デフォルト VLAN に所属します。

（ハ行）

ハードウェアキュー長

1 回の送信処理で回線ハードウェアに与える送信データ長。

バウンダリノード

DS ドメインで，フローを識別して DSCP へ集約して DSCP に基づいて転送動作を行うノードです。

標準 MIB

RFC で規定された MIB です。

フィルタリング

受信したある特定の IP パケットを中継または廃棄する機能です。

プライベート MIB

装置の開発ベンダーが独自に提供する MIB です。

ポリシー

どの業務データを優先的に配信するかという方針を指します。

ポリシーインタフェース情報

ポリシールーティングに従ってパケットを転送するときの，コンフィグレーションで定義したインタフェース情報です。
単一または複数のポリシーインタフェース情報をグループ化してポリシーグループ情報を定義します。

ポリシールーティング

ルーティングプロトコルで登録された経路情報に従わないで，ユーザが設定したポリシーをベースにして特定のインタフェースにパケットを転送するルーティング方法です。

（マ行）

マーカー

IP ヘッダの DS フィールドに DSCP 値を書き込む機能です。バウンダリノードが持っている機能です。

マルチキャスト

ネットワーク内で選択されたグループに属している通信先に対して同一の情報を送信する機能です。

マルチキャストグループマネージメント機能

ホスト - ルータ間でのグループメンバーシップ情報の送受信によって，ルータが直接接続したネットワーク上のマルチキャストグループメンバーの存在を学習する機能です。

マルチキャストトンネル機能

二つのマルチキャストルータがユニキャストルータを経由して接続されている場合に，マルチキャストパケットをカプセル化してデータを送受信して，二つのマルチキャストネットワークを接続する機能です。

マルチパス

宛先のネットワークアドレスに対して複数の経路を構築する接続方式です。

未指定アドレス

すべてのビットが 0 のアドレス 0:0:0:0:0:0:0:0(0::0，または ::) は未指定アドレスと定義されます。未指定アドレスはインタフェースにアドレスがないことを表します。

（ヤ行）

優先 MC スロット指定機能

装置を起動するための優先 MC スロットを指定する機能です。

（ラ行）

ルーティングピア

同じ AS 内に属し，物理的に直接接続されない BGP スピーカ間に形成するピアです。ピアリングに使用する IP アドレスはそのルータの装置アドレス，またはルータ内のインタフェースのインタフェースアドレスのどちらかです。

ルート・フラップ・ダンピング

経路情報が頻発してフラップするような場合に，一時的に該当する経路の使用を抑制して，ネットワークの不安定さを最小限にする機能です。

ルート・リフレクション

AS 内でピアを形成する内部ピアの数を減らすための方法です。内部ピアで配布された経路情報をそのほかの内部ピアに再配布して，AS 内の内部ピアの数を減らします。

ルート・リフレッシュ

変化が発生した経路だけを広告する BGP4+ で，すでに広告された経路を強制的に再広告させる機能です。

ループバックアドレス

アドレス 0:0:0:0:0:0:0:1(0::1，または ::1) はループバックアドレスと定義されています。ループバックアドレスは自ノード宛てに通信するときに，パケットの宛先アドレスとして使用されます。ループバックアドレスをインタフェースに割り当てることはできません。

ロードバランス機能

マルチパスを使用して既存回線を集合して高帯域を供給するための機能です。