HITACHI
Inspire the Next

HA8000-bd シリーズ　内蔵 LAN スイッチモジュール
ソフトウェアマニュアル

コンフィグレーションガイド Vol.1

HA8000-bd/BD10X3

Ver. 3.6.0.B 対応

■対象製品

このマニュアルは HA8000-bd シリーズ内蔵 LAN スイッチモジュールを対象に記載しています。また，内蔵 LAN スイッチモジュールのソフトウェア Ver.3.6.0.B の機能について記載しています。ソフトウェア機能は，ソフトウェア OS-L2BS-A によってサポートする機能について記載します。

■輸出時の注意

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

■商標一覧

Ethernet は，富士ゼロックス株式会社の登録商標です。
Microsoft は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
Windows は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
RSA，SecurID については RSA Security Inc. の米国およびその他の国における商標もしくは登録商標です。
sFlow は，米国およびその他の国における米国 InMon Corp. の登録商標です。
イーサネットは，富士ゼロックス株式会社の登録商標です。
Wake on LAN は，IBM Corp. の登録商標です。
MagicPacket は，Advanced Micro Devices,Inc. の登録商標です。
そのほかの記載の会社名，製品名は，それぞれの会社の商標もしくは登録商標です。

■マニュアルはよく読み，保管してください。

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

■ご注意

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

■発行

２０１４年　１０月 （初版）

■著作権

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 HA8000-bd シリーズ内蔵 LAN スイッチモジュールを対象に記載しています。また，内蔵 LAN スイッチモジュールのソフトウェア Ver.3.6.0.B の機能について記載しています。ソフトウェア機能は，ソフトウェア OS-L2BS-A によってサポートする機能について記載します。

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

■このマニュアルの訂正について

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

■対象読者

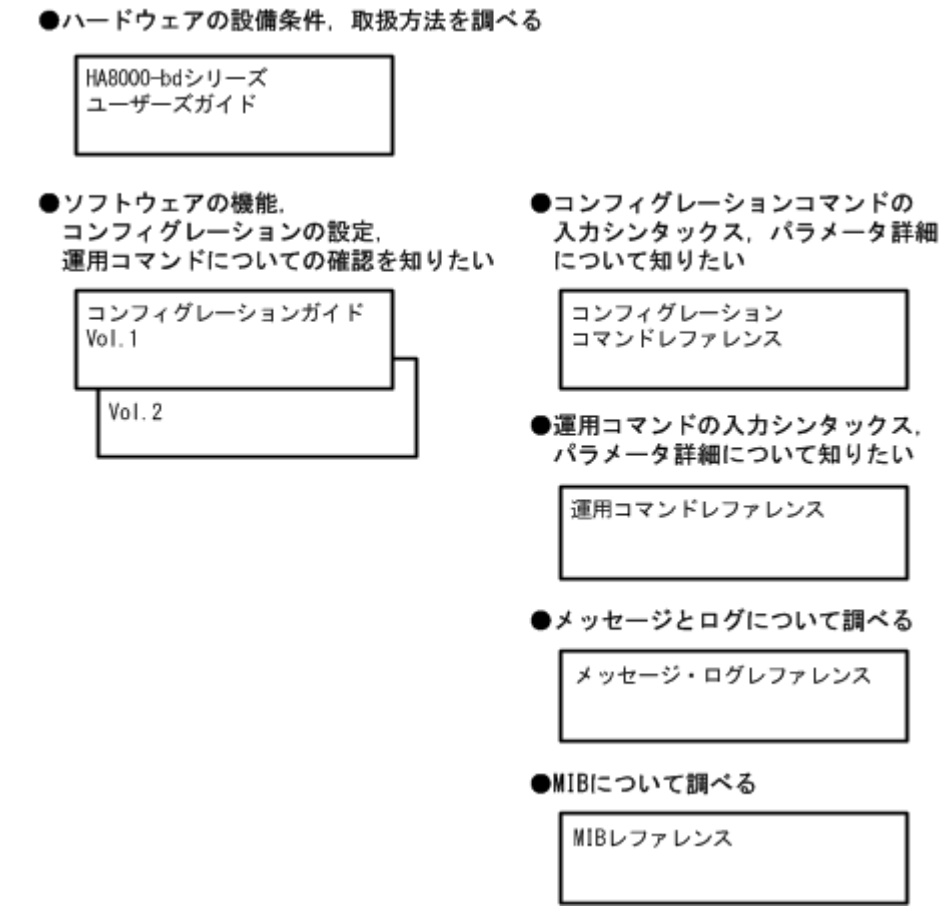
本装置を利用したネットワークシステムを構築し，運用するシステム管理者の方を対象としています。

また，次に示す知識を理解していることを前提としています。

- ネットワークシステム管理の基礎的な知識

■マニュアルの読書手順

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



■このマニュアルでの表記

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

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

SNMP	Simple Network Management Protocol
SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SPF	Shortest Path First
SSAP	Source Service Access Point
STP	Spanning Tree Protocol
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
TLV	Type, Length, and Value
TOS	Type Of Service
TPID	Tag Protocol Identifier
TTL	Time To Live
UDLD	Uni-Directional Link Detection
UDP	User Datagram Protocol
ULR	Uplink Redundant
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
VAA	VLAN Access Agent
VLAN	Virtual LAN
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

■ kB(バイト) などの単位表記について

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

目次

第 1 編　本装置の概要と収容条件

第 2 編　運用管理

第 4 編 レイヤ 2 スイッチ

第 5 編　IP インタフェース

1 本装置の概要

この章では，本装置の特長について説明します。

1.1　本装置の特長

（1） 高速通信

● サーバブレード間，サーバブレードと外部接続機器間を高速通信で接続

- 外部機器とは 1000BASE-T/10GBASE-T ※を 2 ポート（ポート 0/1 ～ 0/2）サポート，10BASE-T/100BASE-TX/1000BASE-T を 2 ポート（ポート 0/3 ～ 0/4）で接続

注※

100BASE-TX は未サポートです。

- サーバブレードとは 1Gbit/s 全二重で通信（ポート 0/5 ～ 0/24）

● サーバブレードと冗長構成の構築が可能

- 本装置を介した通信経路の冗長化が可能
  本装置を HA8000-bd シリーズに 4 台搭載して，サーバブレードのチーミング機能などを使用することで，冗長構成を構築することができます。

（2） ミッションクリティカル対応のネットワークを実現する高信頼性

● 高い装置品質

- 厳選した部品と厳しい設計・検査基準による装置の高い信頼性

● 多様な冗長ネットワーク構築

- 標準機能：リンクアグリゲーション (IEEE802.3ad)，高速スパニングツリー (IEEE802.1w, IEEE802.1s)
- 独自機能：GSRP aware，Autonomous Extensible Ring Protocol ※（以降，Ring Protocol と呼びます。）

注※

Ring Protocol の詳細については，「19　Ring Protocol の解説」を参照してください。

● L2 ループ回避

- UDLD 機能により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などを未然に防ぐことが可能
- L2 ループ検知機能により，ネットワーク上の装置の誤接続を検知し，ループの発生を防ぐことが可能

（3） 強固なセキュリティ

● 高性能できめ細かなパケットフィルタが可能

- ハードウェアによる高性能なフィルタ処理
- レイヤ 2 ／レイヤ 3 ／レイヤ 4 ヘッダの指定が可能
- 多条件指定可能なスケーラビリティ

● 各種 VLAN サポート（Tag-VLAN，ポート VLAN，MAC VLAN，プロトコル VLAN）

● VLAN トンネリングによる L2-VPN の実現

● RADIUS による装置へのログイン・パスワード認証が可能

（4） ハードウェアによる強力な QoS をイーサネット上で実現

● ハードウェアによる高性能な QoS 処理を実現

● きめ細かなパラメータ（レイヤ２／レイヤ３／レイヤ４ヘッダの一部）指定が可能

● 高い精度の QoS 制御が可能

● 多様な QoS 制御機能

L2-QoS(IEEE 802.1p，帯域制御，優先制御など)，IP-QoS（Diff-Serv※，優先制御など）

注※

マーカー機能だけサポートしています。

● 音声・データ統合ネットワークでさまざまなシェーパ機能

- VoIP パケットを優先し，クリアな音声を提供

（5） コンパクトな筐体

● シャーシ内蔵のコンパクトな筐体

（6） 操作しやすいユーザインタフェース（コンフィグレーションコマンド）

● 業界標準のコマンドラインインタフェース

- 入力コマンドとコンフィグレーション情報の形式を同様にし，操作性を向上
- コンフィグレーション情報のコピーアンドペースト機能をサポート

（7） 優れたネットワーク管理，保守・運用

● IPv4/v6 デュアルスタックや IPv6 環境に対応したネットワーク管理（SNMP over IPv6）など充実した機能

● 基本的な MIB-II に加え，IPv6 対応の新 ip MIB(RFC4293)，RMON などの豊富な MIB をサポート

● ミラーポート機能によって，トラフィックを監視，解析することが可能（受信側と送信側ポートの両方可）

● sFlow や sFlow-MIB によるトラフィック特性の分析が可能

● SD メモリカード※採用

- コンフィグレーションのバックアップや障害情報採取が容易に実行可能
- 保守作業の簡略化が可能

注※

本シリーズのマニュアルでは，SD メモリカードの操作および表示説明で「MC」と表記しています。

（8） 優れたコストパフォーマンス

- エンタープライズ向けネットワークに十分なスイッチング容量を優れたパフォーマンスで提供
- アーキテクチャ設計・部品選択の段階で低消費電力を志向。導入後の TCO（Total Cost of Ownership）の削減に寄与

1.2　本装置のモデル

本装置は，10Gbit/sLAN のモジュール型ギガビット・イーサネットスイッチです。

本装置は，外部装置との接続用に 1000BASE-T/10GBASE-T※ポートを 2 ポート，10BASE-T/100BASE-TX/1000BASE-T ポートを 2 ポート，サーバブレード接続専用ポート（SERDES）として 1Gbit/s を 20 ポート装備しています。

注※ 100BASE-TX は未サポートです。

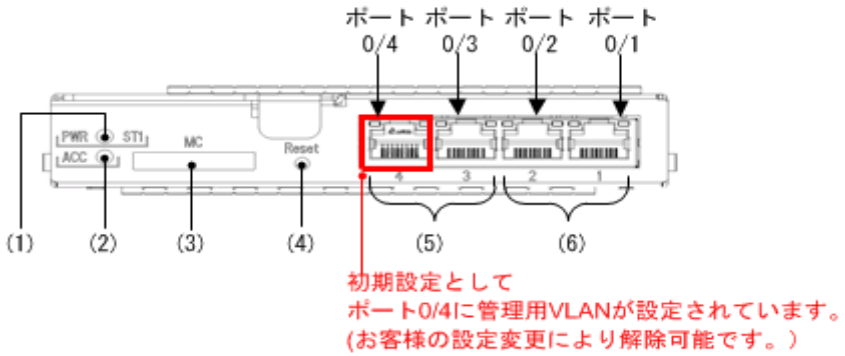
機能として，リンクアグリゲーション，VLAN，スパニングツリー，IGMP/MLD snooping，レイヤ 2 認証機能を備えています。また，高度なフィルタ／QoS 機能をサポートし，ワイヤレート／ノンブロッキングのスイッチングに対応します。

最大ポート数ごとの対応モデルを次の表に示します。

1.2.1　装置の外観

装置外観図を次の図に示します。

図 1-1　装置外観図



(1) 電源/ステータス1ランプ（PWR/ST1）
(2) アクセスランプ（ACC）
(3) メモリカードスロット（MC）
(4) リセットスイッチ（Reset）
(5) 1Gbit/s LANインタフェースコネクタ３～４
(6) 10Gbit/s LANインタフェースコネクタ１～２

2 収容条件

この章では，収容条件について説明します。

2.1 搭載条件

2.1.1 収容回線数

本装置の最大収容可能回線数を以下に示します。

表 2-1 最大収容可能回線数

モデル	イーサネット種別		
	1000BASE-T/10GBASE-T※1	10BASE-T/100BASE-TX/ 1000BASE-T	サーバ接続ポート（SERDES）※2
GR-BEX310GL	2	2	20

注※1 100BASE-TX は未サポートです。

注※2 サーバ接続ポートは 1Gbit/s 固定です。

2.1.2 搭載メモリ量

メインボード搭載メモリ量，および使用可能な MC 容量を次の表に示します。本装置ではメモリの増設はできません。

表 2-2 メインボード搭載メモリ量と内蔵フラッシュメモリ・MC 容量

項目	本装置
メインボード搭載メモリ量(RAMDISK 含む)	512MB （内，RAMDISK は 30MB）
内蔵フラッシュメモリ容量	64MB

（1） RAMDISK について

RAMDISK は，本装置から MC へコピー，または MC から本装置へファイルを登録するときの一時保存エリアとして使用します。

例えば，下記の操作の前に，該当ファイルを一時的に RAMDISK にコピーする操作を行います。

- 例１：コンフィグレーションファイルを本装置から MC へコピーする
- 例２：PC などで作成した Web 認証画面入れ替えファイルを本装置へ登録する

MC へコピー，または本装置に登録したあとは，RAMDISK 上のファイルは不要です。運用コマンドで RAMDISK 上のファイルを削除してください。

なお，本装置を再起動すると，RAMDISK 上のファイルは削除されます。

2.2　収容条件

2.2.1　ログインセキュリティと RADIUS

リモート運用端末から本装置への最大ログイン数と，RADIUS サーバ情報登録数を次の表に示します。

表 2-3　リモート運用端末から本装置への最大ログイン数

項目	最大ログイン数
telnet	16
ftp	1

表 2-4　RADIUS サーバ情報登録数

RADIUS サーバ情報 種別	登録 可能数	RADIUS サーバ グループ情報への 引用可否	登録可能 グループ数	RADIUS サーバ グループ内 登録サーバ数
汎用 RADIUS サーバ情報	20	引用可能	4／装置	4／グループ
IEEE802.1X 認証専用 RADIUS サーバ情報	4	引用不可	－	－
Web 認証専用 RADIUS サーバ情報	4	引用不可	－	－
MAC 認証専用 RADIUS サーバ情報	4	引用不可	－	－

（凡例）－：未サポート

2.2.2　リンクアグリゲーション

コンフィグレーションによって設定できるリンクアグリゲーションの収容条件を次の表に示します。

表 2-5　リンクアグリゲーションの収容条件

項目	最大数
チャネルグループ当たりの最大ポート数	8
装置当たりの最大チャネルグループ	64※

注※

ただし，物理ポートの重複設定はできません。また，装置の動作として 51 グループまでの設定を推奨します。

2.2.3　レイヤ 2 スイッチ機能

（1）MAC アドレステーブル

L2 スイッチ機能では，接続されたホストの MAC アドレスをダイナミックに学習して MAC アドレステーブルへ登録します。また，スタティックに MAC アドレステーブルへ登録することもできます。

MAC アドレステーブルに登録できる MAC アドレスのエントリの最大数を次の表に示します。

表 2-6 MAC アドレステーブルに登録できる MAC アドレスのエントリ数

項目		装置当たり
MAC アドレステーブル	最大エントリ数	16384※
	スタティックエントリ数	256

注※
ハードウェアの制限によって収容条件の最大数まで登録できない場合があります。

MAC アドレスが収容条件を超えた場合，学習済みエントリがエージングされるまで新たな MAC アドレス学習は行われません。従って，未学習の MAC アドレス宛てのフレームは該当する VLAN ドメイン内でフラッディングされます。

また，本装置では，MAC アドレステーブルのエントリの数をコンフィグレーションによって変更することはできません。

（2） VLAN

コンフィグレーションによって設定できる VLAN の数を次の表に示します。

表 2-7 VLAN のサポート数

項目	最大数
ポート当たり VLAN	4094
装置当たり VLAN	4094
ポートごと VLAN 数の装置での合計	24576

注
推奨する VLAN 数は 1024 以下です。
ポートごと VLAN 数の装置での合計は，ポートに設定している VLAN の数を，装置の全ポートで合計した値です。例えば，24 ポートの装置で，ポート 1 からポート 10 では設定している VLAN 数が 200，ポート 11 からポート 24 では設定している VLAN 数が 1 の場合，ポートごと VLAN 数の装置での合計は 2014 となります。ポートごと VLAN 数の装置での合計が収容条件を超えた場合，CPU の利用率が高くなり，コンフィグレーションコマンドや運用コマンドのレスポンスが遅くなったり，実行できなくなったりすることがあります。

本装置で設定できる最大 VLAN 数は 4094 ですが，そのうち IP アドレスを設定できる VLAN（VLAN インタフェース）数は最大 128 です。

(a) プロトコル VLAN

プロトコル VLAN では，イーサネットフレーム内の Ethernet-Type，LLC SAP，および SNAP type フィールドの値を基にプロトコルの識別を行います。コンフィグレーションによって設定できるプロトコルの種類数を次の表に示します。

表 2-8 プロトコル VLAN のプロトコルの種類数と VLAN 数

項目	ポート当たり	装置当たり
プロトコル VLAN のプロトコルの種類数	16	16
プロトコル VLAN 数	48※	48

注※
トランクポートに設定できるプロトコル VLAN 数です。プロトコルポートに設定できるプロトコル VLAN 数は 16

です。

（b） MAC VLAN

MAC VLAN の収容条件を次の表に示します。

表 2-9　MAC VLAN の登録 MAC アドレス数

項目	最大数
コンフィグレーションによる最大登録 MAC アドレス数	64
L2 認証機能による最大登録 MAC アドレス数	1000
同時登録最大 MAC アドレス数	1000 ※

注※

コンフィグレーショにより登録される MAC アドレス数は，レイヤ 2 認証機能により登録される最大 MAC アドレス数に含まれます。

（c） VLAN トンネリング

VLAN トンネリングを設定したスイッチにおいてトランクポートに設定できる VLAN の数を次の表に示します。

表 2-10　VLAN トンネリングの数

項目	装置当たり
VLAN トンネリングの数	4094

（d） Tag 変換

コンフィグレーションによって設定できる Tag 変換情報エントリ数を次の表に示します。

表 2-11　Tag 変換情報エントリ数

項目	装置当たり
Tag 変換情報エントリ数	768 ※

注※

ハードウェアの制限によって収容条件の最大数まで登録できない場合があります。

（3） スパニングツリー

スパニングツリーの収容条件を種類ごとに次の表に示します。

表 2-12　PVST+ の収容条件

Ring Protocol 共存有無	対象 VLAN 数	VLAN ポート数※1
共存なし	250	256 ※2
共存あり	128	200 ※2

注※ 1

スパニングツリー対象となる各 VLAN に設定するポート数の合計（VLAN 数とポート数の積）。

例えば，100 個の VLAN を設定し，それぞれの VLAN に 2 回線が所属している場合，ポート数は 100 × 2 ＝ 200

となります。

注※2

PortFast 機能を設定したポート数は含めません。

表 2-13 シングルスパニングツリーの収容条件

Ring Protocol 共存有無	対象 VLAN 数	VLAN ポート数※1	VLAN ポート数※1 (PVST+ 併用時※2)
共存なし	256※3	1024	256
共存あり	256※3	768	200

注※1

スパニングツリー対象となる各 VLAN に設定するポート数の合計（VLAN 数とポート数の積）。

例えば，100 個の VLAN を設定し，それぞれの VLAN に 2 回線が所属している場合，ポート数は 100 × 2 ＝ 200 となります。

注※2

PVST+ の対象ポートを含む合計の最大値が 256 となります。

注※3

PVST+ 同時動作時は PVST+ 対象 VLAN 数を引いた値となります。

表 2-14 マルチプルスパニングツリーの収容条件

Ring Protocol 共存有無	対象 VLAN 数	VLAN ポート数※1	MST インスタンス数	MST インスタンスごとの対象 VLAN 数※2
共存なし	256	1024	16	200
共存あり	256	768	16	200

注※1

スパニングツリー対象となる各 VLAN に設定するポート数の合計（VLAN 数とポート数の積）。

例えば，100 個の VLAN を設定し，それぞれの VLAN に 2 回線が所属している場合，ポート数は 100 × 2 ＝ 200 となります。

注※2

MST インスタンス 0 は除きます。MST インスタンス 0 の対象 VLAN 数は 256 となります。

（4） Ring Protocol

（a） Ring Protool

Ring Protocol の収容条件を次の表に示します。

表 2-15 Ring Protocol の収容条件

項目	リング当たり	装置当たり
リング数	－	51※1
VLAN マッピング数	－	128
VLAN グループ数	2	102※2
VLAN グループの VLAN 数	1023※3※4	1023※3※4
リングポート数※5	2	52

（凡例）－：該当なし

注※ 1

Ring Protocol とスパニングツリーの併用，または多重障害監視機能を使用する場合は，8 となります。

注※ 2

Ring Protocol とスパニングツリーの併用，または多重障害監視機能を使用する場合は，16 となります。

注※ 3

装置として推奨する VLAN の最大数です。
本装置の推奨 VLAN 数は最大 1024 ですが，リング当たりに制御 VLAN 用として VLAN を一つ消費するため，VLAN グループに使用できる VLAN の最大数は 1023 となります。ただし，リング数が増加するに従い，VLAN グループに使用できる VLAN の最大数は減少します。

注※ 4

多重障害監視機能は，多重障害監視 VLAN 用としてリング当たり VLAN を一つ消費するため，VLAN グループに使用できる VLAN の最大数は減少します。

注※ 5

チャネルグループの場合は，チャネルグループ単位で 1 ポートと数えます。

(b) 仮想リンク

仮想リンクの収容条件を次の表に示します。

表 2-16 仮想リンクの収容条件

項目	最大数
装置当たりの仮想リンク ID 数	1
仮想リンク当たりの VLAN 数	1
拠点当たりのリングノード数	2
ネットワーク全体での仮想リンクの拠点数	250

(c) 多重障害監視機能

多重障害監視機能の収容条件を次の表に示します。

表 2-17 多重障害監視機能の収容条件

項目	最大数
装置当たりの多重障害監視可能リング数	4
リング当たりの多重障害監視 VLAN 数	1
装置当たりの多重障害監視 VLAN 数	4

(5) IGMP snooping ／ MLD snooping

IGMP/MLD snooping の収容条件を次の表に示します。IGMP/MLD snooping で学習したマルチキャスト MAC アドレスは MAC アドレステーブルに登録します。登録可能なマルチキャスト MAC アドレス数を次の表に示します。

表 2-18 IGMP snooping の収容条件

項目	最大数
設定 VLAN 数	32

項目	最大数
VLAN ポート数※1	512
登録エントリ数※2※3	1000

注※1
IGMP snooping が動作するポート数（IGMP snooping を設定した VLAN に収容されるポートの総和）です。例えば，各々 10 ポート収容している 16 個の VLAN で IGMP snooping を動作させる場合，IGMP snooping 動作ポート数は 160 となります。
注※2
各 VLAN で学習したマルチキャスト MAC アドレスの総和です。
注※3
登録エントリ数は，IGMP snooping/MLD snooping で使用するエントリの総和となります。

表 2-19　MLD snooping の収容条件

項目	最大数
設定 VLAN 数	32
VLAN ポート数※1	512
登録エントリ数※2※3	1000

注※1
MLD snooping が動作するポート数（MLD snooping を設定した VLAN に収容されるポートの総和）です。例えば，各々 10 ポート収容している 16 個の VLAN で MLD snooping を動作させる場合，MLD snooping 動作ポート数は 160 となります。
注※2
各 VLAN で学習したマルチキャスト MAC アドレスの総和です。
注※3
登録エントリ数は，IGMP snooping/MLD snooping で使用するエントリの総和となります。

2.2.4　IP インタフェース

本装置では VLAN に対して IP アドレスを設定します。ここでは，IP アドレスを設定できる VLAN インタフェースの最大数，設定できる IP アドレスの最大数，通信できる相手装置の最大数などについて説明します。また，ダイナミックエントリとスタティックエントリ数，DHCP サーバの収容条件についても説明します。

（1）IP アドレスを設定できる最大インタフェース数

本装置でサポートする最大インタフェース数を次の表に示します。ここで示す値は，IPv4 と IPv6 の合計の値です。なお，IPv4 と IPv6 を同一のインタフェースに設定することも，個別に設定することもできます。

表 2-20　IP アドレスを設定できる最大インタフェース数

項目	装置当たり
IP アドレスを設定できる最大インタフェース数	128

（2） VLAN ごとの受信制御ができる最大インタフェース数

VLAN ごとの受信制御ができる最大インタフェース数を次の表に示します。IP アドレスを設定したインタフェース数がここで示す値以下の場合は，IP アドレス未設定の VLAN で，本装置の MAC アドレスを宛先とするパケットを中継することができます。

表 2-21　VLAN ごとの受信制御ができる最大インタフェース数

項目	装置当たり
VLAN ごとの受信制御ができる最大インタフェース数	32

（3） マルチホームの最大サブネット数

LAN のマルチホーム接続では一つのインタフェースに対して，複数の IPv4 アドレス，または IPv6 アドレスを設定します。

（a） IPv4 アドレス

IPv4 でのマルチホームの最大サブネット数を次の表に示します。

表 2-22　マルチホームの最大サブネット数（IPv4 の場合）

項目	インタフェース当たり
マルチホームの最大サブネット数（IPv4）	128

（b） IPv6 アドレス

IPv6 でのマルチホームの最大サブネット数を次の表に示します。なお，ここで示す値にはインタフェースのデフォルトリンクローカルアドレスおよび RA 受信によって自動生成される IPv6 アドレスを含みません。

表 2-23　マルチホームの最大サブネット数（IPv6 の場合）

項目	インタフェース当たり
マルチホームの最大サブネット数（IPv6）	7

（4） IP アドレス最大設定数

（a） IPv4 アドレス

装置当たりのコンフィグレーションで設定できる IPv4 アドレスの最大数を次の表に示します。

表 2-24　コンフィグレーションで装置に設定できる IPv4 アドレス最大数

項目	装置当たり
コンフィグレーションで設定可能な IPv4 アドレス最大数	128

（b） IPv6 アドレス

コンフィグレーションで設定できる装置当たりの IPv6 アドレスの最大数を次の表に示します。なお，ここで示す値は通信用のインタフェースに設定できる最大数です。インタフェースのデフォルトリンクローカルアドレスおよび RA 受信によって自動生成される IPv6 アドレスを含みません。

表 2-25 コンフィグレーションで装置に設定できる IPv6 アドレス最大数

項目	装置当たり
コンフィグレーションで設定可能な IPv6 アドレス最大数	128

(5) RA 受信による自動生成数

IPv6 での RA 受信による IPv6 アドレスと IPv6 デフォルトゲートウェイの自動生成数を次の表に示します。

表 2-26 RA 受信による自動生成数

項目		最大数
IPv6 プレフィクス	インタフェース当たり	2
IPv6 デフォルトゲートウェイ	装置当たり	2

(6) 最大相手装置数

本装置が接続する LAN を介して通信できる最大相手装置数を示します。この場合の相手装置はルータに限らず，端末も含みます。

(a) ARP エントリ数

IPv4 の場合，LAN では ARP によって，送信しようとするフレームの宛先アドレスに対応するハードウェアアドレスを決定します。従って，これらのメディアでは ARP エントリ数によって最大相手装置数が決まります。本装置でサポートする ARP エントリの最大数を次の表に示します。

表 2-27 ARP エントリの最大数

項目	インタフェース当たり	装置当たり
ARP エントリ数	2048	2048

注

スタティック ARP は 128 個です。

(b) NDP エントリ数

IPv6 の場合，LAN では NDP でのアドレス解決によって，送信しようとするパケットの宛先アドレスに対応するハードウェアアドレスを決定します。したがって，NDP エントリ数によって最大相手装置数が決まります。本装置でサポートする NDP エントリの最大数を次の表に示します。

表 2-28 NDP エントリの最大数

項目	インタフェース当たり	装置当たり
NDP エントリ数	256	256

注

スタティック NDP は 128 個です。

(7) ダイナミックエントリ，スタティックエントリの最大エントリ数

ダイナミックエントリとスタティックエントリの最大エントリ数を次の表に示します。

本装置では，スタティックルーティングだけが利用でき，RIP/RIPng，OSPF/OSPFv3 などのルーティングプロトコルはサポートしていません。

表 2-29 ダイナミックエントリとスタティックエントリの最大エントリ数

分類	項 目	装置当たりの最大エントリ数	最大ダイナミックエントリ数	最大スタティックエントリ数
IPv4	ユニキャスト経路エントリ	128※	－	128※
IPv6	ユニキャスト経路エントリ	1※	－	1※

（凡例）－：未サポート
注※ ダイレクト経路は含みません。

（8） DHCP サーバ

DHCP サーバで設定できるインタフェース数および配布可能 IP アドレス数などを次の表に示します。

表 2-30 DHCP サーバの収容条件

項 目	最大数
DHCP サーバインタフェース数	64
DHCP サーバ管理サブネット数	64
配布可能 IP アドレス数	1024※
配布可能固定 IP アドレス数	80
配布除外アドレス数	1024

注※
配布可能固定 IP アドレス数を含みます。

2.2.5 フィルタ・QoS

フィルタ・QoS の検出条件はコンフィグレーション（access-list，qos-flow-list）で設定します。ここでは，設定したリストを装置内部で使用する形式（エントリ）に変換したエントリ数の上限をフィルタ・QoS の収容条件として示します。

フィルタ・QoS の検出条件によるリソース配分を決定するために，フィルタおよび QoS 共通モードであるフロー検出モードを選択します。フロー検出モードは，受信側および送信側について，それぞれ対応する次のコンフィグレーションコマンドで設定します。選択するモードによって，エントリ数の上限値を決定する条件が異なります。インタフェース種別ごとにインタフェース当たりの上限値，および装置当たりの上限値がありますので，その範囲内で設定してください。

- コンフィグレーションコマンド flow detection mode：受信側フロー検出モードの設定
- コンフィグレーションコマンド flow detection out mode：送信側フロー検出モードの設定

なお，受信側のエントリ数については「(1) 受信側フィルタエントリ数」「(2) 受信側 QoS エントリ数」を，送信側のエントリ数については「(3) 送信側フィルタエントリ数」を参照してください。受信側はフィルタ・QoS 機能を，送信側はフィルタ機能をサポートしています。

（1） 受信側フィルタエントリ数

受信側フロー検出モード layer2-1，layer2-2，または layer2-3 のいずれかを選択した場合に設定できる受

信側フィルタ最大エントリ数を次の表に示します。フロー検出条件は選択するモードによって決まり，layer2-1 の場合は MAC 条件を，layer2-2 の場合は IPv4 条件，layer2-3 の場合は IPv4 条件および IPv6 条件を使用できます。

表 2-31　受信側フィルタ最大エントリ数

受信側フロー検出モード	インタフェース種別	受信側フィルタ最大エントリ数※					
		インタフェース当たり			装置当たり		
		MAC 条件	IPv4 条件	IPv6 条件	MAC 条件	IPv4 条件	IPv6 条件
layer2-1	イーサネット	256	－	－	256	－	－
	VLAN	256	－	－	256	－	－
layer2-2	イーサネット	－	256	－	－	256	－
	VLAN	－	256	－	－	256	－
layer2-3	イーサネット	－	256	128	－	256	128
	VLAN						

（凡例）－：該当なし

注※

フィルタエントリ追加時，当該イーサネットインタフェースまたは VLAN インタフェースに対してフロー未検出時に動作するエントリ（廃棄動作）を 自動的に付与します。このため，フィルタ最大エントリ数のすべてを使用することはできません。フィルタエントリの数え方の例を次に示します。

（例 1）

エントリ条件 ：イーサネットインタフェース 0/1 に 1 エントリ設定
エントリ数　：設定エントリ (1) とイーサネットインタフェース 0/1 の廃棄エントリ (1) の合計 2 エントリを使用する
残エントリ数：受信側フィルタ最大エントリ数－エントリ数

（例 2）

エントリ条件：イーサネットインタフェース 0/1 に 2 エントリ，イーサネットインタフェース 0/2 に 3 エントリ設定
エントリ数　：設定エントリ (5) とイーサネットインタフェース 0/1 の廃棄エントリ (1) およびイーサネットインタフェース 0/2 の廃棄エントリ (1) の合計 7 エントリを使用する
残エントリ数：受信側フィルタ最大エントリ数－エントリ数

（2） 受信側 QoS エントリ数

受信側フロー検出モード layer2-1，layer2-2，または layer2-3 のいずれかを選択した場合に設定できる受信側 QoS 最大エントリ数を次の表に示します。フロー検出条件は選択するモードによって決まり，layer2-1 の場合は MAC 条件を，layer2-2 の場合は IPv4 条件を，layer2-3 の場合は IPv4 条件および IPv6 条件を使用できます。

表 2-32 受信側 QoS 最大エントリ数

受信側フロー検出モード	インタフェース種別	受信側 QoS 最大エントリ数					
		インタフェース当たり			装置当たり		
		MAC 条件	IPv4 条件	IPv6 条件	MAC 条件	IPv4 条件	IPv6 条件
layer2-1	イーサネット	128	－	－	128	－	－
	VLAN	128	－	－	128	－	－
layer2-2	イーサネット	－	128	－	－	128	－
	VLAN	－	128	－	－	128	－
layer2-3	イーサネット	－	128	64	－	128	64
	VLAN						

（凡例）－：該当なし

（3） 送信側フィルタエントリ数

送信側フロー検出モード layer2-1-out，layer2-2-out，または layer2-3-out のいずれかを選択した場合に設定できる送信側フィルタ最大エントリ数を次の表に示します。フロー検出条件は選択するモードによって決まり，layer2-1-out の場合は MAC 条件を，layer2-2-out の場合は IPv4 条件を，layer2-3-out の場合は MAC 条件，IPv4 条件および IPv6 条件を使用できます。

表 2-33 送信側フィルタ最大エントリ数

送信側フロー検出モード	インタフェース種別	送信側フィルタ最大エントリ数					
		インタフェース当たり			装置当たり		
		MAC 条件	IPv4 条件	IPv6 条件	MAC 条件	IPv4 条件	IPv6 条件
layer2-1-out	イーサネット	128	－	－	128	－	－
	VLAN	128	－	－	128	－	－
layer2-2-out	イーサネット	－	128	－	－	128	－
	VLAN	－	128	－	－	128	－
layer2-3-out	イーサネット	128	128	128	128	128	128
	VLAN						

（凡例）－：該当なし

（4） TCP/UDP ポート番号検出パターン数

フィルタ・QoS のフロー検出条件での TCP/UDP ポート番号検出パターンの収容条件を次の表に示します。TCP/UDP ポート番号検出パターンは，フロー検出条件のポート番号指定で使用されるハードウェアリソースです。

表 2-34　TCP/UDP ポート番号検出パターン収容条件

受信側フロー検出モード	装置当たりの最大数
layer2-1	－
layer2-2	16
layer2-3	16

（凡例）
－：TCP/UDP ポート番号検出パターンを使用しない受信側フロー検出モードです。

次の表に示すフロー検出条件の指定で，TCP/UDP ポート番号検出パターンを使用します。なお，アクセスリスト（access-list）および QoS フローリスト（qos-flow-list）の作成だけでは TCP/UDP ポート番号検出パターンを使用しません。作成したアクセスリストおよび QoS フローリストを次に示すコンフィグレーションでインタフェースに適用したときに TCP/UDP ポート番号検出パターンを使用します。

- ip access-group
- ipv6 traffic-filter
- ip qos-flow-group
- ipv6 qos-flow-group

表 2-35　TCP/UDP ポート番号検出パターンを使用するフロー検出条件パラメータ

フロー検出条件のパラメータ	指定方法	受信側フロー検出モード		送信側フロー検出モード	
		layer2-1	layer2-2 layer2-3	layer2-1-out	layer2-2-out layer2-3-out
送信元ポート番号	単一指定（eq）	指定不可	－	指定不可	－
	範囲指定（range）	指定不可	○	指定不可	指定不可
宛先ポート番号	単一指定（eq）	指定不可	－	指定不可	－
	範囲指定（range）	指定不可	○	指定不可	指定不可

（凡例）
○：TCP/UDP ポート番号検出パターンを使用する
－：TCP/UDP ポート番号検出パターンを使用しない

本装置では，TCP/UDP ポート番号検出パターンを共有して使用します。

1. 複数のフィルタエントリと複数の QoS エントリで共有します。
2. フロー検出条件の TCP と UDP で共有します。
3. フロー検出条件の送信元ポート番号と宛先ポート番号では共有しません。
4. フロー検出条件の IPv4 条件と IPv6 条件で共有します。

次の表に TCP/UDP ポート番号検出パターンを使用する例を示します。受信側フロー検出モードが layer2-2 のときの例です。

表 2-36 TCP/UDP ポート番号検出パターンの使用例

パターンの使用例※	使用するパターン数
フィルタエントリで • 送信元ポート番号の範囲指定 (10 ～ 30) フィルタエントリで • 送信元ポート番号の範囲指定 (10 ～ 40)	二つのエントリでは指定している範囲が異なるため， • 送信元ポート番号の範囲指定 (10 ～ 30) • 送信元ポート番号の範囲指定 (10 ～ 40) の 2 パターンを使用します。
フィルタエントリで • 送信元ポート番号の指定なし • 宛先ポート番号の範囲指定 (10 ～ 20) フィルタエントリで • 送信元ポート番号の指定なし • 宛先ポート番号の範囲指定 (10 ～ 20) QoS エントリで • 送信元ポート番号の指定なし • 宛先ポート番号の範囲指定 (10 ～ 20)	上記 1 の共有する場合の例です。 三つのエントリがありますが，どれも宛先ポート番号の範囲指定 (10 ～ 20) で同じ範囲を指定しているのでパターンを共有します。 • 宛先ポート番号の範囲指定 (10 ～ 20) の 1 パターンを使用します。
QoS エントリで • TCP を指定 • 送信元ポート番号の範囲指定 (10 ～ 30) • 宛先ポート番号の指定なし QoS エントリで • UDP を指定 • 送信元ポート番号の範囲指定 (10 ～ 30) • 宛先ポート番号の指定なし	上記 2 の共有する場合の例です 二つのエントリがありますが，どちらも送信元ポート番号の範囲指定 (10 ～ 30) で同じ値を指定しているのでパターンを共有します。 • 送信元ポート番号の範囲指定 (10 ～ 30) の 1 パターンを使用します。
QoS エントリで • 送信元ポート番号の範囲指定 (10 ～ 20) • 宛先ポート番号の範囲指定 (10 ～ 20)	上記 3 の共有しない場合の例です。 指定した範囲が同じでも送信元と宛先ではパターンを共有しません。 • 送信元ポート番号の範囲指定 (10 ～ 20) • 宛先ポート番号の範囲指定 (10 ～ 20) の 2 パターンを使用します。

（凡例）

() 内は単一指定したときの値，または範囲指定したときの範囲です。

2.2.6 レイヤ 2 認証機能

（1） レイヤ 2 認証共通

装置全体の認証端末数を次の表に示します。

表 2-37 装置全体の認証端末数

認証モード	認証機能	認証機能ごとの端末数	装置全体の端末数	認証数制限の最大設定数	
				ポート単位	装置単位
固定 VLAN モード	IEEE802.1X	1024	1024	1024※2	1024※3
	Web 認証	1024			
	MAC 認証	1024			
ダイナミック VLAN モード	IEEE802.1X	1000	1000※1		
	Web 認証	1000			
	MAC 認証	1000			
装置全体での全認証機能 / 認証モードの合計最大端末数			1024		

注※ 1
認証数制限を 1000 以上に設定した場合でも，ダイナミック VLAN モードの最大認証数は 1000 までとなります。

注※ 2
設定した当該ポートで全認証機能（IEEE802.1X/Web 認証 /MAC 認証）の固定 VLAN モードおよびダイナミック VLAN モード合計の認証数を制限します。

注※ 3
装置全体で全認証機能（IEEE802.1X/Web 認証 /MAC 認証）の固定 VLAN モードおよびダイナミック VLAN モード合計の認証数を制限します。

表 2-38 その他のレイヤ 2 認証共通機能収容条件

項目	最大数
汎用 RADIUS サーバ登録数	20※1
認証専用 IPv4 アクセスリストで指定できるアクセスリスト名	1
認証専用 IPv4 アクセスリストに指定できるフィルタ条件数	250※2
認証失敗端末最大登録可能数	256※3

注※ 1
ログインセキュリティ機能を含む装置全体での登録数です。

注※ 2
収容条件以上のフィルタエントリ数を設定した場合，収容条件以内のエントリだけが適用されます。

注※ 3
認証失敗端末数が最大数を超えたときは，更新時期が古い端末から削除して，新規失敗端末を登録します。

（2） IEEE802.1X

IEEE802.1X の収容条件を次の表に示します。

表 2-39 IEEE802.1X の最大認証端末数※

認証モード		ポート単位	装置全体
ポート単位認証	(静的)	1024	1024
	(動的)	1000	1000
IEEE802.1X 認証全体での最大端末数		1024	1024

注※
認証数制限設定は，レイヤ 2 認証共通です。「表 2-37 装置全体の認証端末数」も参照してください。

表 2-40 IEEE802.1X の収容条件

項目		最大数
認証方式グループ登録数	装置デフォルト	1
	認証方式リスト	4
IEEE802.1X 認証専用 RADIUS サーバ登録数※1		4
最大 IEEE802.1X 設定可能物理ポート数	全モデル共通	装置の最大物理ポート数
認証除外端末オプションの最大除外端末数	MAC アドレステーブルスタティック登録	256／装置※2
	MAC VLAN へ MAC アドレススタティック登録	64／装置※3

注※ 1
RADIUS アカウント機能のサーバは，認証用 RADIUS サーバ（IEEE802.1X 認証専用 RADIUS サーバまたは汎用 RADIUS サーバ）の設定に従います。

注※ 2
MAC アドレステーブルのスタティックエントリ数です。

注※ 3
MAC VLAN 収容条件のコンフィグレーションによる最大登録 MAC アドレス数です。

(3) Web 認証

Web 認証の収容条件を次の表に示します。

表 2-41 Web 認証の最大認証ユーザ数※

認証モード	ポート単位	装置全体
固定 VLAN モード	1024	1024
ダイナミック VLAN モード	1000	1000
Web 認証全体での最大認証ユーザ数	1024	1024

注※
認証数制限設定は，レイヤ 2 認証共通です。「表 2-37 装置全体の認証端末数」も参照してください。

表 2-42 Web 認証の収容条件

項目		最大数
認証方式グループ登録数	装置デフォルト	1
	認証方式リスト	4

項目		最大数
Web 認証専用 RADIUS サーバ登録数※1		4
内蔵 Web 認証 DB 登録ユーザ数		300※2
Web 認証画面入れ替えで指定できるファイルの合計サイズ		1024kB ／装置※3
	Web 認証画面のカスタムファイルセット※4 登録数	5 ／装置 内訳 • 基本 Web 認証画面：1 • 個別 Web 認証画面：4
	1 ファイルセットあたりのファイル数	100

注※ 1

RADIUS アカウント機能のサーバは，認証用 RADIUS サーバ（Web 認証専用 RADIUS サーバまたは汎用 RADIUS サーバ）の設定に従います。

注※ 2

内蔵 Web 認証 DB に登録したユーザ ID を複数の端末で使用すると，最大認証ユーザ数まで端末を認証できます。ただし，認証対象となるユーザ ID の数が内蔵 Web 認証 DB の最大登録ユーザ数より多い場合は，RADIUS サーバを用いた RADIUS 認証方式を使用してください。

注※ 3

基本 Web 認証画面および個別 Web 認証画面すべての合計です。なお，ファイル領域には管理領域も含んでいますので，実動上は 1024kB よりも少ない値となります。

注※ 4

カスタムファイルセットについては，「コンフィグレーションガイド Vol.2 8 Web 認証の解説」を参照してください。

（4） MAC 認証

MAC 認証の収容条件を次の表に示します。

表 2-43 MAC 認証の最大認証端末数※

認証モード	ポート単位	装置全体
固定 VLAN モード	1024	1024
ダイナミック VLAN モード	1000	1000
MAC 認証全体での最大端末数	1024	1024

注※

認証数制限設定は，レイヤ 2 認証共通です。「表 2-37 装置全体の認証端末数」も参照してください。

表 2-44 MAC 認証の収容条件

項目		最大数
認証方式グループ登録数	装置デフォルト	1
	認証方式リスト	4
MAC 認証専用 RADIUS サーバ登録数※		4
内蔵 MAC 認証 DB 登録 MAC アドレス数		1024

注※

RADIUS アカウント機能のサーバは，認証用 RADIUS サーバ（MAC 認証専用 RADIUS サーバまたは汎用

RADIUS サーバ）の設定に従います。

2.2.7 ネットワークの障害検出による高信頼化機能

（1） IEEE802.3ah/UDLD

IEEE802.3ah/UDLD の収容条件を次の表に示します。

表 2-45 IEEE802.3ah/UDLD の収容条件

項目	最大数
リンク監視情報数	装置の最大物理ポート数

（2） L2 ループ検知

L2 ループ検知フレーム送信レートを次の表に示します。

表 2-46 L2 ループ検知フレーム送信レート

項目	装置当たり
L2 ループ検知フレーム送信レート	20（packet/ 秒）※1

L2 ループ検知フレームを送信可能なポート数および VLAN 数の算出式

L2 ループ検知フレーム送信対象の総和※2 ÷ L2 ループ検知フレームの送信レート（packet/ 秒）≦送信間隔（秒）

注※ 1

20（packet/ 秒）を超えるフレームは送信しません。送信できなかったフレームに該当するポートや VLAN ではループ障害を検知できなくなります。

注※ 2

L2 ループ検知フレーム送信ポート数× L2 ループ検知フレーム送信 VLAN 数

2.2.8 隣接装置情報（LLDP）

隣接装置情報（LLDP）の収容条件を次の表に示します。

表 2-47 隣接装置情報（LLDP）の収容条件

項目	最大収容数
LLDP 隣接装置情報	装置の最大物理ポート数

3 装置へのログイン

この章では，装置の起動と停止，およびログイン・ログアウト，運用管理の概要，運用端末とその接続形態について説明します。

3.1 運用端末による管理

本装置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 RS-232C 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。また，本装置は 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。コンソールやリモート運用端末といった本装置の管理を行う端末を運用端末といいます。

3.1.1 運用端末

本装置の運用端末の条件を次の表に示します。

表 3-1 運用端末の条件

端末種別	接続形態	必要機能
コンソール	シリアル接続 (RS-232C)	RS-232C(回線速度：19200，9600，4800，2400，1200)
リモート運用端末	通信用ポート接続	TCP/IP telnet ftp

! 注意事項

本装置は，改行コードとして [CR] を認識します。一部の端末では，改行コードとして [CR] および [LF] を送信します。これらの端末から本装置に接続すると，端末に空行を表示するなどの現象がおこります。このような場合は，各端末の設定を確認してください。

(1) コンソール

(a) コンソールの接続

コントロールボックスモジュールの内蔵 LAN スイッチ設定用ポート（SER SW）と PC クライアントを RS-232C クロスケーブルで接続します。詳細は「ユーザーズガイド」を参照してください。

(b) 端末の通信ソフトウェアの設定

コンソールは RS-232C に接続する端末で，一般的な通信端末，通信ソフトウェアが使用できます。コンソールが本装置と通信できるように，次の標準 VT100 設定値（本装置のデフォルト設定値）が通信ソフトウェアに設定されていることを確認してください。

- 通信速度：9600bit/s
- データ長：8 ビット
- パリティビット：なし
- ストップビット：1 ビット
- フロー制御：なし

なお，通信速度を 9600 bit/s 以外（1200 ／ 2400 ／ 4800 ／ 19200 bit/s）で設定して使用したい場合は，コンフィグレーションコマンド speed で本装置側の通信速度設定を変更してください。その後，端末ソフトウェアの速度を本装置の速度と同じとなるよう変更してください。

図 3-1 コンソールの通信速度の設定例

```
(config)# line console 0
(config-line)# speed 19200
(config-line)# exit
```

! 注意事項

コンソールを使用する場合は次の点に注意してください。

- 本装置ではコンソール端末からログインする際に，自動的に VT100 の制御文字を使用して画面サイズを取得・設定します。VT100 に対応していないコンソール端末では，不正な文字列を表示したり，最初の CLI プロンプトをずれて表示したりして，画面サイズを取得・設定できません。コンソール端末は，端末運用モード：VT100 でご使用ください。
  また，ログインと同時にキー入力した場合，VT100 の制御文字の表示結果が正常に取得できないため同様の現象となりますのでご注意ください。この場合は，再度ログインし直してください。
- 通信速度の設定が反映されるのは，ログアウトしたあとになります。コンソールからいったんログアウトしたあとで，使用している通信端末や通信ソフトウェアの通信速度の設定を変更してください。変更するまでは文字列が不正な表示になります（「login」プロンプトなど）。
- 通信速度を 9600bit/s 以外に設定して運用している場合，装置を起動（再起動）するとコンフィグレーションが装置に反映されるまでの間，不正な文字列が表示されます。

(2) リモート運用端末

(a) リモート運用端末の接続

内蔵 LAN スイッチモジュールの LAN インタフェースコネクタ（line 4）と PC クライアントを LAN ケーブルで接続します。詳細は「ユーザーズガイド」を参照してください。本装置には，初期導入時，以下のコンフィグレーションが設定（工場出荷設定）されています。

- ポート 0/4 は管理用として専用 VLAN と IP アドレスが設定
  VLAN4094，IP アドレス：192.168.0.254（サブネットマスク 255.255.255.0）
- リモート運用端末からのログイン許可を設定（line vty）

本装置に IP ネットワーク経由で接続してコマンド操作を行う端末が，リモート運用端末です。telnet プロトコルのクライアント機能がある端末はすべてリモート運用端末として使用できます。

! 注意事項

設定変更や接続ポートのリンクダウンなどにより端末側で telnet が切断された場合，約 10 分間は再接続できなくなる場合があります。

(3) 運用端末ごとの特長

運用端末ごとの特長をを次の表に示します。

表 3-2 運用端末ごとの特長

運用端末	コンソール	リモート運用端末
遠隔からのログイン	不可	可
本装置から運用端末へのログイン	不可	可
アクセス制御	なし	あり
コマンド入力	可	可
ファイル転送方式	なし	ftp

運用端末	コンソール	リモート運用端末
IP 通信	不可	IPv4 および IPv6
SNMP マネージャ接続	不可	可
コンフィグレーション設定	不要	必要

3.1.2 運用管理機能の概要

本装置はセットアップ作業が終了し，装置の電源 ON で運用に入ります。本装置と接続した運用端末では，運用コマンドやコンフィグレーションコマンドを実行し，装置の状態を調べたり，接続ネットワークの変更に伴うコンフィグレーションの変更を実施したりできます。本装置で実施する運用管理の種類を次の表に示します。

表 3-3 運用管理の種類

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	Telnet ログインによるリモート操作をサポートします。
ログ・統計情報	過去に発生した障害情報およびパケットカウンタ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 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を行います。
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などのコマンドを持ちます。
MC 保守機能	MC のフォーマットなどを行います。

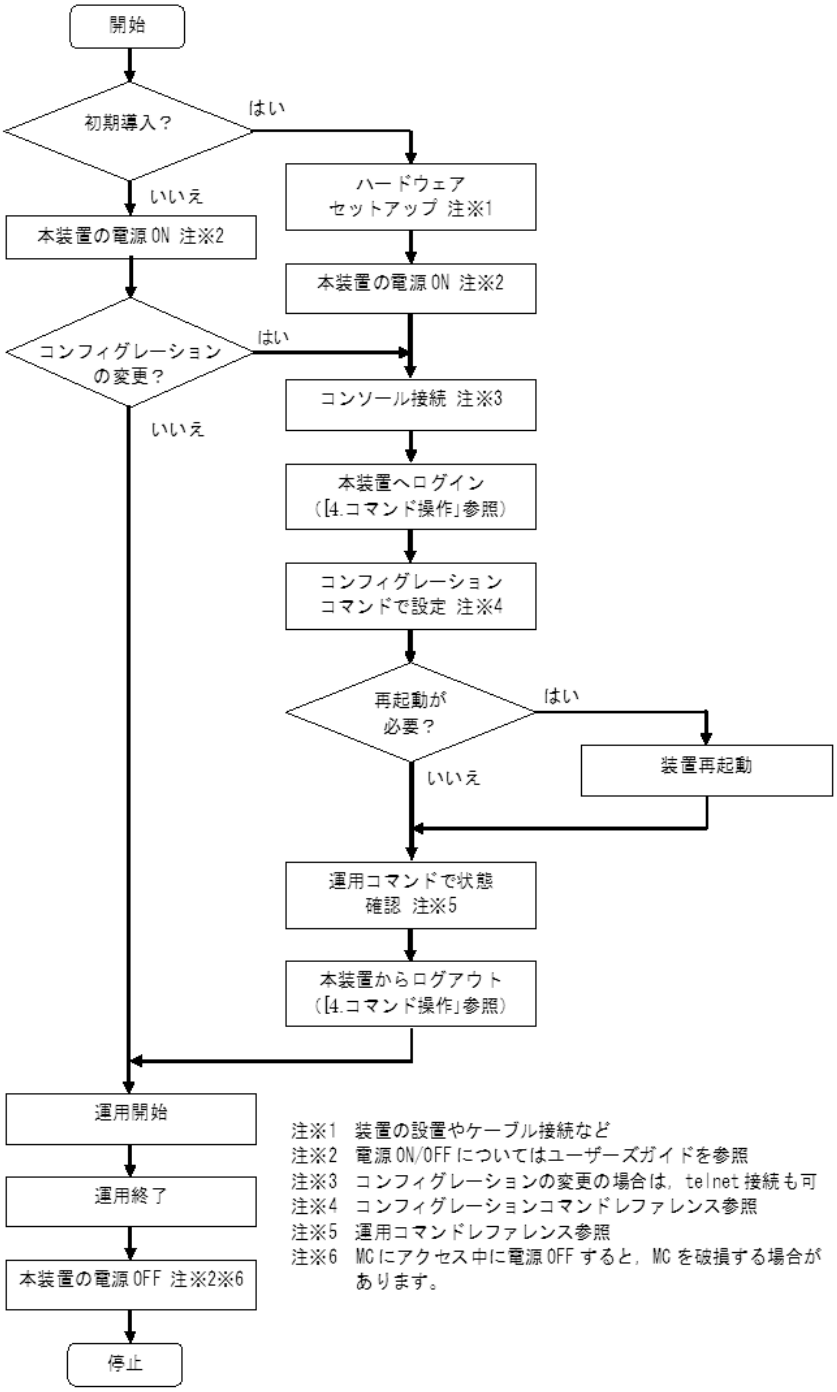
3.2　装置起動

この節では，装置の起動と停止について説明します。

3.2.1　本装置の起動から停止までの概略

本装置の起動から停止までの概略フローを次の図に示します。ハードウェアセットアップの内容については「ユーザーズガイド」を参照してください。

図 3-2　本装置の起動から停止までの概略フロー



3.2.2 装置の起動

本装置の起動，再起動の方法を次の表に示します。

表 3-4 起動，再起動の方法

起動の種類	内容	操作方法
電源 ON による起動	HA8000-bd に電源が入ると，連動して本装置が電源 OFF から立ち上がります。	HA8000-bd の電源モジュールに電源ケーブルを接続します。
リセットによる再起動	障害発生などにより，本装置をリセットしたい場合に行います。	本体のリセットスイッチを押します。
コマンドによる再起動	障害発生などにより，本装置をリセットしたい場合に行います。	運用コマンド reload を実行します。

HA8000-bd の電源モジュールに電源ケーブルを接続することで HA8000-bd に電源が入り，連動して本装置が起動します。詳細は「ユーザーズガイド」を参照してください。本装置を起動，再起動したときに PWR/ST1 LED が赤点灯となった場合は，致命的障害が発生していることを示しますので，お買い求め先にご連絡いただくか，保守員をお呼びください。また，LED 表示内容の詳細は，「ユーザーズガイド」を参照してください。

ソフトウェアイメージを k.img という名称で書き込んだ MC をスロットに挿入して，本装置を起動すると MC から起動できます。

3.2.3 装置の停止

本装置の電源を OFF にする場合は，HA8000-bd の電源モジュールから，電源ケーブルを外すことで本装置の電源も OFF となります。詳細は「ユーザーズガイド」を参照してください。アクセス中のファイルが壊れるおそれがあるので，本装置にログインしているユーザがいない状態で行ってください。

3.3　ログイン・ログアウト

この節では，ログインとログアウトについて説明します。

（1） ログイン

装置が起動すると，ログイン画面を表示します。この画面でユーザ ID とパスワードを入力してください。正しく認証された場合は，コマンドプロンプトを表示します。また，認証に失敗した場合は”Login incorrect”のメッセージを表示し，ログインできません。ログイン画面を次の図に示します。

なお，初期導入時には，ユーザ ID”operator” でパスワードなしでログインができます。

図 3-3　ログイン画面

```
login: operator
Password:                                                    …1

Copyright (c) 2010-2014 ALAXALA Networks Corporation. All rights reserved.

>                                                            …2
```

1. パスワードが設定されていない場合は，「Password:」を表示しません。
   パスワードが設定されている場合は，入力したパスワードの文字を表示しません。
2. コマンドプロンプトを表示します。

（2） ログアウト

CLI での操作を終了してログアウトしたい場合は logout コマンドまたは exit コマンドを実行してください。ログアウト画面を次の図に示します。

図 3-4　ログアウト画面

```
> logout

login:
```

（3） 自動ログアウト

一定時間（デフォルト：60 分）内にキーの入力がなかった場合，自動的にログアウトします。なお，自動ログアウト時間は運用コマンド set exec-timeout で変更できます。

4 コマンド操作

この章では，本装置でのコマンドの指定方法について説明します。

4.1 コマンド入力モード

4.1.1 運用コマンド一覧

コマンド入力モードの切り換えに関する運用コマンド一覧を次の表に示します。

表 4-1 運用コマンド一覧

コマンド名	説明
enable	コマンド入力モードを一般ユーザモードから装置管理者モードに変更します。
disable	コマンド入力モードを装置管理者モードから一般ユーザモードに変更します。
exit	現在のコマンド入力モードを終了します。
logout	装置からログアウトします。
configure(configure terminal)	コマンド入力モードを装置管理者モードからコンフィグレーションコマンドモードに変更して，コンフィグレーションの編集を開始します。
end	コンフィグレーションコマンドモードを終了して装置管理者モードに戻ります。

4.1.2 コマンド入力モード

本装置でコンフィグレーションの変更を実施したり，または装置の状態を参照したりする場合，適切なコマンド入力モードに遷移し，コンフィグレーションコマンドや運用コマンドを入力する必要があります。また，CLI プロンプトでコマンド入力モードを識別できます。

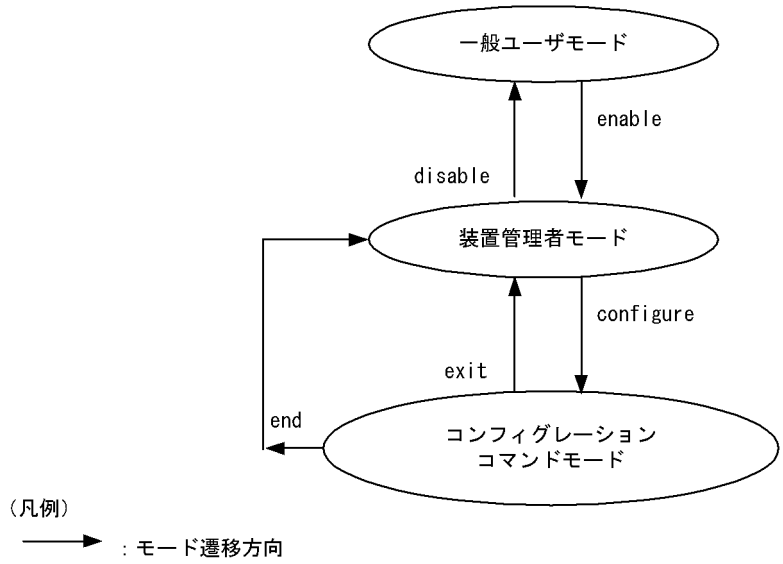
コマンド入力モードとプロンプトの対応を次の表に示します。

表 4-2 コマンド入力モードとプロンプトの対応

コマンド入力モード	実行可能なコマンド	プロンプト
一般ユーザモード	運用コマンド（configure コマンドなど，一部のコマンドは装置管理者モードでだけ実行可能です。）	>
装置管理者モード		#
コンフィグレーションコマンドモード	コンフィグレーションコマンド	(config)#

モード遷移の概要を次の図に示します。

図 4-1 モード遷移の概要



また，CLI プロンプトとして，次に示す場合でも，その状態を意味する文字をプロンプトの先頭に表示します。

1. コンフィグレーションコマンド hostname で本装置の識別名称を設定している場合，識別名称の先頭から 20 文字目までがプロンプトに反映されます。
2. ランニングコンフィグレーションを編集し，その内容をスタートアップコンフィグレーションファイルに保存していない場合，プロンプトの先頭に「！」が付きます。

1. ～ 2. のプロンプト表示例を次の図に示します。

図 4-2 プロンプト表示例

```
> enable
# configure
(config)# hostname "OFFICE1"
!OFFICE1(config)# end
!OFFICE1# copy running-config startup-config
Do you wish to copy from running-config to startup-config? (y/n): y
OFFICE1#
```

コンフィグレーションの編集・保存後，装置の再起動が必要な場合はプロンプトの先頭に「@」が付きます。この場合は，運用コマンド reload を入力し装置を再起動してください。

図 4-3 プロンプト表示例（@を表示する例）

```
OFFICE1# configure
OFFICE1(config)# limit-queue-length 728
Please execute the reload command after save,
because this command becomes effective after reboot.
!OFFICE1(config)# end
!OFFICE1# copy running-config startup-config
Do you wish to copy from running-config to startup-config? (y/n): y
@OFFICE1# reload
Restart OK? (y/n): y
```

4.2 CLI での操作

4.2.1 補完機能

コマンドライン上で［Tab］を入力することで，コマンド入力時のコマンド名称やファイル名の入力を少なくすることができ，コマンド入力が簡単になります。補完機能を使用したコマンド入力の簡略化を次の図に示します。

図 4-4 補完機能を使用したコマンド入力の簡略化

```
(config)# in[Tab]
(config)# interface
```

[Tab]押下で使用できるコマンドやパラメータの一覧を表示します。

```
(config)# interface [Tab]
gigabitethernet     port-channel        range               vlan
(config)# interface
```

注意

入力できない選択肢を表示する場合があります。「コンフィグレーションコマンドレファレンス」および「運用コマンドレファレンス」の各コマンドの入力形式と入力範囲をご確認ください。

4.2.2 ヘルプ機能

コマンドライン上で［?］を入力することで，指定できるコマンドまたはパラメータを検索できます。また，コマンドやパラメータの意味を知ることができます。次の図に［?］入力時の表示例を示します。

図 4-5 ［?］入力時の表示例

```
> show vlan ?
 <VLAN ID list>          - [1-4094] ex. "5", "10-20" or "30,40"
 <Display option>        - {detail | list | summary}
 channel-group-number    - Display the VLAN information specified by channel-gro
                           up-number
 id                      - A part of VLAN ID
 mac-vlan                - Display the MAC VLAN information
 port                    - Display the VLAN information specified by port number

 <cr>
> show vlan
```

注意

1. ＜＞のないパラメータ名を表示する場合があります。
2. 入力できない選択肢を表示する場合があります。「コンフィグレーションコマンドレファレンス」および「運用コマンドレファレンス」の各コマンドの入力形式と入力範囲をご確認ください。

なお，パラメータの入力途中でスペース文字を入れないで［?］を入力した場合は，補完機能が実行されます。

4.2.3 入力エラー指摘機能

コマンドまたはパラメータを不正に入力した際，次行にエラーメッセージ（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　35　コンフィグレーション編集時のエラーメッセージ」を参照）を表示します。［Tab］入力時と［?］入力時も同様となります。

エラーメッセージの説明によって，コマンドまたはパラメータを見直して再度入力してください。入力エラー指摘の表示例を「図 4-6　入力エラーをしたときの表示例 (gigabitethernet のスペルミス)」および

「図 4-7　パラメータ入力途中の表示例 (duplex のパラメータ指定なし)」に示します。

図 4-6　入力エラーをしたときの表示例 (gigabitethernet のスペルミス)

```
(config)# interface gigabtiethernet 0/3 [Enter]
                    ^
Error: Invalid parameter.
(config)#
```

図 4-7　パラメータ入力途中の表示例 (duplex のパラメータ指定なし)

```
(config)# interface gigabitethernet 0/3
(config-if)# duplex  [Enter]
                   ^
Error: Missing parameter.
(config-if)#
```

4.2.4　コマンド短縮実行

コマンドまたはパラメータを短縮して入力し，入力された文字が一意のコマンドまたはパラメータとして認識できる場合，コマンドを実行します。短縮入力のコマンド実行例を次の図に示します。

図 4-8　短縮入力のコマンド実行例（show ip arp の短縮入力）

```
> sh ip ar [Enter]

Date 20XX/06/14 20:04:23 UTC
Total: 2
IP Address      Linklayer Address  Interface  Expire     Type
10.0.0.55       0013.20ad.0155     VLAN2048   20min      arpa
10.0.0.56       0013.20ad.0156     VLAN2048   20min      arpa

>
```

4.2.5　ヒストリ機能

ヒストリ機能を使用すると，過去に入力したコマンドを簡単な操作で再実行したり，過去に入力したコマンドの一部を変更して再実行したりできます。ヒストリ機能を使用した例を次の図に示します。

図 4-9　ヒストリ機能を使用したコマンド入力の簡略化

```
> ping 192.168.100.2 interval 2 count 1 packetsize 120      …1
PING 192.168.100.2 (192.168.100.2): 120 data bytes
128 bytes from 192.168.100.2: icmp_seq=0 ttl=128 time=0 ms

----192.168.100.2 PING Statistics----
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max = 0/0/0 ms
>                                                           …2
> ping 192.168.100.2 interval 2 count 1 packetsize 120      …3
PING 192.168.100.2 (192.168.100.2): 120 data bytes
128 bytes from 192.168.100.2: icmp_seq=0 ttl=128 time=0 ms

----192.168.100.2 PING Statistics----
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max = 0/0/0 ms
>                                                           …4
> ping 192.168.100.3 interval 2 count 1 packetsize 120      …5
PING 192.168.100.3 (192.168.100.3): 120 data bytes
128 bytes from 192.168.100.3: icmp_seq=0 ttl=128 time=0 ms

----192.168.100.3 PING Statistics----
1 packets transmitted, 0 packets received, 100.0% packet loss
>
```

1. 192.168.100.2 に対して ping コマンドを実行します。
2. ［↑］キーを入力することで前に入力したコマンドを呼び出せます。
   この例の場合，［↑］キーを 1 回押すと「ping 192.168.100.2 interval 2 count 1 packetsize 120」を表示しますので，［Enter］キーの入力だけで同じコマンドを再度実行できます。
3. 192.168.100.2 に対して ping コマンドを実行します。
4. ［↑］キーを入力することで前に入力したコマンドを呼び出し，［←］キーおよび［Backspace］キーを使ってコマンド文字列を編集できます。
   この例の場合，［↑］キーを 1 回押すと「ping 192.168.100.2 interval 2 count 1 packetsize 120」を表示しますので，IP アドレスの「2」の部分を「3」に変更して［Enter］キーを入力しています。
5. 192.168.100.3 に対して ping コマンドを実行します。

注意

通信ソフトウェアによっては方向キー（[↑], [↓], [←], [→]）を入力してもコマンドが呼び出されない場合があります。その場合は，通信ソフトウェアのマニュアルなどで設定を確認してください。

4.2.6 ページング

コマンドの実行により出力される結果について，表示すべき情報が一画面にすべて表示しきれない場合は，ユーザのキー入力を契機に一画面ごとに区切って表示します。なお，ページングは運用コマンド set terminal pager でその機能を有効にしたり無効にしたりできます。

4.2.7 キーボードコマンド機能

端末アプリケーションおよび端末の設定により，使用可能なキーが異なります。本装置では，VT100 で仕様が明確になっているキーを使用した下表の組み合わせでの操作を推奨します。

表 4-3 推奨キーボードコマンド

キーボード	本装置の動作
Backspace	カーソルの左の 1 文字を削除します。（ただし行の先頭まで）
Ctrl ＋ A	コマンド行の先頭へ移動します。
Ctrl ＋ B	1 文字戻ります。（ただし行の先頭まで）
Ctrl ＋ C	コマンドを中断します。
Ctrl ＋ D	1 文字削除します。
Ctrl ＋ E	コマンド行の行末へ移動します。
Ctrl ＋ F	1 文字進みます。（ただし行の終わりまで）
Ctrl ＋ L	コンソール画面をリフレッシュし，画面上のコマンド入力行以外は表示を消去します。
Ctrl ＋ N	カレントコマンドまで次のヒストリを表示します。
Ctrl ＋ P	一つ前のヒストリを表示します。
Ctrl ＋ U	カーソル行のテキストを削除します。
Ctrl ＋ W	1 語のカーソルまでを削除します。 例） !> show sysversion 　　~ 上記入力状態で，カーソルを”v”へ移動し，Ctrl ＋ W を押下すると，下記のようにカーソルの前までの文字（sys）が消えます。 !> show version
Ctrl ＋ Z	コンフィグレーションコマンドモードを終了して装置管理者モードに戻ります。

キーボード	本装置の動作
Ctrl ＋ K	カーソルの後ろのテキストを削除します。
Ctrl ＋ T	カレントの文字と前の文字を交換します。
ESC ＋ B	１語戻ります。
ESC ＋ F	１語進みます
ESC ＋ D	語のカーソルから後ろを削除します。

4.2.8 CLI 設定のカスタマイズ

自動ログアウト機能や CLI 機能の一部は，CLI 環境情報としてユーザごとに動作をカスタマイズできます。カスタマイズ可能な CLI 機能と CLI 環境情報を次の表に示します。

表 4-4 カスタマイズ可能な CLI 機能と CLI 環境情報

機能	カスタマイズ内容と初期導入時のデフォルト設定
自動ログアウト	自動ログアウトするまでの時間を設定できます。 初期導入時のデフォルト設定は，60 分です。
ページング	ページングするかどうかを設定できます。 初期導入時のデフォルト設定は，ページングをします。

これらの CLI 環境情報は，次に示す運用コマンドで設定できます。

- set exec-timeout
- set terminal pager

設定内容は，コマンドが実行されたセッションでは実行直後から動作に反映されます。同一ユーザでも別セッションの場合は，次回ログイン時に反映されます。また，設定内容は，運用コマンド show users で確認してください。

なお，運用コマンド adduser で no-flash パラメータを指定して追加したアカウントのユーザは，装置を再起動したときに，CLI 環境情報が初期導入時のデフォルト設定に戻ります。

4.3 CLIの注意事項

(1) ログイン後の制限

ログイン後に運用端末がダウンした場合，本装置内ではログインしたままの状態になっていることがあります。この場合，自動ログアウトを待ってください。

(2) 補完機能，ヘルプ機能の表示制限

一部のコマンドにはパラメータの補完，ヘルプ表示に制限があります。

コンフィグレーションコマンドレファレンス，運用コマンドレファレンスに従い，該当コマンドを入力し直してください。

本項ではパラメータの説明として，下記の表記を使用します。

- 可変値パラメータ：任意の数字や文字列を入力するパラメータ
- 固定文字列キーワード：決まった文字列で入力するパラメータ

(a) 可変値パラメータの後ろに固定文字列キーワードがある場合

入力形式：コマンド ＜可変値＞ 固定文字列キーワード

＜可変値＞を入力後，入力不可能な固定文字列キーワードが入力可能となる場合があります（補完も可能です）。ただし，入力形式としては不当なため，[Enter] を押下した場合エラーとなります。

図 4-10 入力後に，入力不可能な固定文字列キーワードを表示する例

```
(config)# spanning-tree mst 5 [?]
configuration           - Configure the common information used by each MST ins
                          tance of multiple spanning tree, and enter MST config
                          uration mode
forward-time            - Specify the time which state changes take to a bridge
                          interface
hello-time              - Specify a BPDU transmitting interval
max-age                 - Specify the maximum time holding the received protoco
                          l information
max-hops                - Specify the maximum number of hop about BPDU
root                    - Specify a root
transmission-limit      - Specify the maximum number of BPDU which can be trans
                          mitted for one second
(config)# spanning-tree mst 5
```

"spanning-tree mst 5" まで入力後，[？] を入力すると入力可能な固定文字列キーワードやパラメータを表示します。しかし，上記の図に示すように入力不可能な固定文字列キーワード（太字下線付きで表記した部分）も表示します。この場合，"spanning-tree mst 5 configuration" と入力すると，入力形式としては不当なため，[Enter] を押下した場合エラーとなります。

(b) 固定文字列キーワードなしのパラメータが複数ある場合

入力形式：コマンド [＜可変値＞] [＜可変値＞] ・・・

[ ] で囲まれた固定文字列キーワードを付けないパラメータが複数あると，ヘルプ表示や [Tab] による一覧表示で，入力不可能でもパラメータを表示する場合があります。

図 4-11 [ ] で囲まれた固定文字列キーワードを付けないパラメータが複数ある例

```
(dhcp-config)# lease 360 [？]
 <Time hour>              - [0-23]
 <Time min>               - [0-59]
 <Time sec>               - [0-59]
 <cr>
(dhcp-config)# lease 360 [Tab]
<cr>                <Time hour>          <Time min>           <Time sec>
```

上記の例では "lease 360"（days まで指定）を入力した [？] を入力すると，入力可能なパラメータを表示します。しかし，上記の図に示すように入力不可能なパラメータ（太字下線付きで表記した部分）も表示します。

(c) 可変値パラメータと固定文字列キーワードが同じ入力順にある場合

可変値パラメータと固定文字列キーワードが同じ入力順にある場合，固定文字列キーワードを優先します。このため，可変値パラメータの文字列が固定文字列キーワードの先頭から完全一致すると，固定文字列キーワードとして認識します（補完機能が動作します)。

下記に固定文字列キーワードと認識する例と，可変値パラメータと認識する例を示します。

図 4-12 可変値パラメータを固定文字列キーワードとして補完する例

```
(config)# aaa authentication mac-authentication
 <List name>            - Specify the RADIUS server list name 1 to 32 character
                          s
 default                - Specify default mac authentication mechanism
(config)# aaa authentication mac-authentication de  ⇒固定文字列キーワードとして認識
 group                  - Specify mac authentication mechanism using RADIUS pro
                          tocol
 local                  - Specify mac authentication mechanism using local pass
                          word
```

上記の例では，可変値パラメータ <List name> として "de" を入力します。しかし，<List name> と同じ入力順にある固定文字列キーワード "default" の先頭から完全一致しているため "default" と認識し，"default" の次に入力できるキーワードのヘルプを表示します。

図 4-13 可変値パラメータとして認識する例

```
(config)# aaa authentication mac-authentication device  ⇒可変値パラメータとして認識
 group                  - group <Group name>: Specify mac authentication mechan
                          ism using RADIUS protocol
(config)# aaa authentication mac-authentication device
```

上記の例では，可変値パラメータ <List name> として "device" を入力します。この場合は，<List name> と同じ入力順にある固定文字列キーワード "default" の先頭から完全一致しないため "device" と認識し，<List name> の次に入力できるヘルプを表示します。

(d) ヘルプのコマンドやパラメータの表示文字数制限

コマンドやパラメータの文字数が 24 文字以上の場合，ヘルプ表示時に 24 文字目以降を表示しません。

図 4-14 ヘルプの表示文字数が制限された例

```
(config)# switchport-backup
 startup-active-port-sel - Specify the mode of active port selection pattern at
                           startup
(config)#
```

上記の例では，switchport-backup のヘルプ "startup-active-port-selection" が 24 文字以上のため，"startup-active-port-sel" まで表示し，以降を表示しません。

(e) 選択式の固定文字列キーワードに特定パラメータがある場合

選択式の固定文字列キーワードが列挙される入力形式で，特定の固定文字列キーワードだけにパラメータが存在する場合，入力不可能な時点でもヘルプやコマンド一覧に表示します。ただし入力形式としては不当なため，[Enter] を押下した場合エラーとなります。

図 4-15　選択式の固定文字列キーワードの一部にパラメータも表示する例

```
(config)# snmp-server host 10.0.0.1 traps ABC
 version                 - version {1 | 2c | 3}: Specifies SNMP trap version
 security level          - {noauth | auth | priv}: Specify SNMP Security Level
 snmp                    - SNMP traps send
 rmon                    - RMON traps send
 login                   - Login traps send
 temperature             - Temperature trap sends
 storm-control           - Storm-control trap sends
 efmoam                  - IEEE802.3ah/UDLD trap sends
 dot1x                   - 802.1X traps send
 web-authentication      - Web authentication traps send
 mac-authentication      - MAC authentication traps send
 loop-detection          - L2 loop detection trap sends
  <cr>
```

"snmp-server host 10.10.0.1 traps ABC" まで入力後，[？] を入力すると入力可能な固定文字列キーワードやパラメータを表示します。しかし，上記の図に示すように入力不可能なパラメータ（太字下線付きで表記した部分）も表示します。（下線部の security level は，version 3 を選択したときに指定するパラメータです。）

この場合，"snmp-server host 10.10.0.1 traps ABC auth" と入力すると，入力形式としては不当なため，[Enter] を押下した場合エラーとなります。

(f) コンフィグレーションコマンド deny / permit / qos のヘルプ表示や補完機能の制限

コンフィグレーションコマンドの deny / permit（ip access-list standard 以外），および qos のヘルプ表示や補完機能には，下記に示す制限があります。

- ヘルプ表示にコマンドの入力形式を表示
  パラメータ <source ipv4> や <source ipv6>，または <source mac> を指定すると，以降のパラメータのヘルプ表示はすべて次の図に示すように該当コマンドの入力形式を表示します。

図 4-16　ヘルプ表示に入力形式を表示する例（ip access-list extended の例）

```
(config-ext-nacl)# permit
 <protocol>              - 0-255,ah,esp,gre,icmp,igmp,ip,ipinip,ospf,pcp,pim,sct
                           p,tcp,tunnel,udp,vrrp
(config-ext-nacl)# permit ip
 <PARAMs:input format>   - permit <protocol> {<source ipv4> <source ipv4 wildcar
                           d> | host <source ipv4> | any} [*1] {<destination ipv
                           4> <destination ipv4 wildcard> | host <destination ip
                           v4> | any} [*2][*3][*4] {[tos <tos>] [precedence <pre
                           cedence>] | dscp <dscp>} [vlan <vlan id>] [user-prior
                           ity <priority>]   NOTE: *1:(TCP/UDP)- {eq <source por
                           t> | range <source port start> <source port end>}  *2
                           :(TCP/UDP)- {eq <destination port> | range <destinati
                           on port start> <destination port end>}  *3:(ICMP)- [{
                           <icmp type> [<icmp code>] | <icmp message>}]  *4:(TCP
                           )- [ack][fin][psh][rst][syn][urg]
```

- ヘルプ表示で <cr> を表示する場合
  通常ヘルプ表示では，入力を終了してもよい場合に <cr> を表示しますが，コンフィグレーションコマンド deny/permit/qos では，入力が不完全な状態でも <cr> を表示する場合があります。入力途中で <cr> 表示に従い [Enter] を押下すると，入力形式として不当な場合はエラーとなります。コンフィグレーションコマンドレファレンス，運用コマンドレファンレスに従い，該当コマンドを入力し直してください。

図 4-17　コマンド不完全で <cr> が表示される例（ip access-list extended の例）

```
config-ext-nacl)# permit ip any host
 <PARAMs:input format>   - permit <protocol> {<source ipv4> <source ipv4 wildcar
                           d> | host <source ipv4> | any} [*1] {<destination ipv
                           4> <destination ipv4 wildcard> | host <destination ip
                           v4> | any} [*2][*3][*4] {[tos <tos>] [precedence <pre
                           cedence>] | dscp <dscp>} [vlan <vlan id>] [user-prior
                           ity <priority>]   NOTE: *1:(TCP/UDP)- {eq <source por
                           t> | range <source port start> <source port end>}  *2
                           :(TCP/UDP)- {eq <destination port> | range <destinati
                           on port start> <destination port end>}  *3:(ICMP)- [{
                           <icmp type> [<icmp code>] | <icmp message>}]  *4:(TCP
                           )- [ack][fin][psh][rst][syn][urg]
 <cr>
```

- 補完機能の制限
  パラメータ <source ipv4> や <source ipv6>，および <source mac> 以降は補完できません。

図 4-18　補完不可の例（ip access-list extended の例）

```
(config-ext-nacl)# permit i
icmp                igmp                ip                  ipinip

(config-ext-nacl)# permit ip a  ⇒"any"補完不可
```

（g）コマンドの入力形式に <interface id list> が複数ある場合

入力形式　monitor session <session no.> source interface <interface id list> [{rx | tx | both}] destination interface <interface id list>

上記コマンドのように入力形式に <interface id list> の入力箇所が複数ある場合，２箇所目以降では区切り文字（コンマ）入力の有無に関わらず，続けて <interface id list> を入力したり省略が可能となる場合があります。

図 4-19　期待するヘルプ表示および動作【1 箇所目の <interface id list> の入力時】

```
(config)# monitor session 1 source interface gigabitethernet 0/3
 <monitor frames>       - {rx | tx | both}: Set monitor of receiving frames / mon
                          itor of transmitting frames / monitor of receiving and
                            transmitting frames
 destination            - Specify a mirrored port

(config)# monitor session 1 source interface gigabitethernet 0/3,
 gigabitethernet        - gigabitethernet <interface no. list> : The type of a
                          port is specified in 10BASE-T/100BASE-TX/1
                          000BASE-T line ex."0/3","0/3-4"
 tengigabitethernet     - tengigabitethernet <interface no. list> : The type of
                           a port is specified in 10GBASE-T line ex."0/1-2","0/1"
```

上記の例では，ポート番号に区切り文字（コンマ）無のときは次の入力パラメータをヘルプに表示しています。ポート番号に区切り文字（コンマ）有のときは，続けて入力可能なインタフェース種別

（gigabitethernet/tengigabitethernet）をヘルプに表示します。

図 4-20　期待しないヘルプ表示および動作【2 箇所目の <interface id list> の入力時】（ポート番号にコンマ無）

```
(config)# monitor session 1 source interface gigabitethernet 0/3, gigabitethernet
0/4 rx destination interface gigabitethernet 0/11
 gigabitethernet      - The type of a port is specified in 10BASE-T/100BASE-TX/
                        1000BASE-T line
 tengigabitethernet   - The type of a port is specified in 10GBASE-T line
 <cr>
```

図 4-21　期待しないヘルプ表示および動作【2 箇所目の <interface id list> の入力時】（ポート番号にコンマ有）

```
(config)# monitor session 1 source interface gigabitethernet 0/3, gigabitethernet
0/4 rx destination interface gigabitethernet 0/11,
 gigabitethernet      - The type of a port is specified in 10BASE-T/100BASE-TX/
                        1000BASE-T line
 tengigabitethernet   - The type of a port is specified in 10GBASE-T line
 <cr>
```

上記の 2 箇所目の <interface id list> を入力時，ポート番号に区切り文字（コンマ）無の場合，期待するヘルプ表示は入力終了の <cr> ですが，図内太字下線部のように続けて入力可能なインタフェース種別（gigabitethernet/tengigabitethernet）をヘルプに表示します。

逆にポート番号に区切り文字（コンマ）有の場合，期待するヘルプ表示は入力終了の <cr> の表示無ですが，図内太字下線部のように <cr> をヘルプに表示します。

このような場合，コマンド入力後の show では下記のように表示します。

図 4-22　2 箇所目の <interface id list> でコンマ有で入力後の show 表示

```
(config)# monitor session 1 source interface gigabitethernet 0/3, gigabitethernet
0/10 rx destination interface gigabitethernet 0/4,
(config)# show
monitor session 1 source interface gigabitethernet 0/3, gigabitethernet 0/10 rx
destination interface gigabitethernet 0/4     ⇒コンマ無で表示
```

図 4-23　2 箇所目の <interface id list> でコンマ無で入力後の show 表示

```
(config)# monitor session 1 source interface gigabitethernet 0/3, gigabitethernet
0/10 rx destination interface gigabitethernet 0/4 interface tengigabitethernet
0/1
(config)# show
monitor session 1 source interface gigabitethernet 0/3, gigabitethernet 0/10 rx
destination interface gigabitethernet 0/4, interface tengigabitethernet 0/1  ⇒
コンマ有で表示
```

(h) コンフィグレーションの削除で省略可能パラメータを指定した場合の制限

入力形式　コマンド < パラメータ > [省略可能パラメータ]

コンフィグレーションの削除コマンドで省略可能パラメータを指定した場合，省略可能パラメータに範囲外の値を指定すると，ヘルプ表示や [Tab] によるコマンド一覧にその時点で入力不可能なパラメータを表示します。

図 4-24　入力不可能なパラメータを表示する例

```
(config)# no ip dhcp excluded-address 192.168.0.1 127.0.0.1⇒範囲外の値
 <High address>          - Last address of an excluded range⇒入力不可能なパラメータ
 <cr>
```

この状態で [Enter] を押下すると，省略可能パラメータを無視して削除を実行します。

上記の例では，"no ip dhcp excluded-address 192.168.0.1" として実行するため，"ip dhcp excluded-address 192.168.0.1" が設定されている場合は削除されます。

(i) no の補完，ヘルプについて

設定の削除などに入力する "no" は，[？] によるヘルプおよび [Tab] によるコマンド一覧で表示しません。また，[Tab] で補完しません。

(3) コンフィグレーションモードでの入力について

コンフィグレーションモード（第二階層）で，グローバルコンフィグレーションモード（第一階層）のコマンドは入力できません。exit コマンドを入力してグローバルコンフィグレーションモードに戻ってから入力してください。

(4) コンソール (RS-232C) の設定について

コンソール端末は，端末運用モード：VT100，画面サイズ（ターミナルサイズ）：80 桁× 24 行でご使用ください。

5 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設定しておく必要があります。この章では，コンフィグレーションを設定するのに必要なことについて説明します。

5.1 コンフィグレーション

運用開始時または運用中，ネットワークの運用環境に合わせて，本装置に接続するネットワークの構成および動作条件などのコンフィグレーションを設定する必要があります。ただし，初期導入時，以下のコンフィグレーションが設定（工場出荷設定）されています。

- ポート 0/4 は管理用として専用 VLAN が設定
  VLAN4094，IP アドレス：192.168.0.254（サブネットマスク 255.255.255.0）
- ポート 0/5 ～ 0/24 のサーバ接続ポートをエッジポート設定（spanning-tree portfast trunk）
- ポート 0/5 ～ 0/24 の伝送速度は，speed：auto
  上記以外の伝送速度に変更されると，サーバとの通信障害となるケースがありますので，サーバ接続ポートの伝送速度はデフォルト設定のままご使用ください。また，サーバ接続ポートで duplex の変更は未サポートです（全二重で動作します）。
- リモート運用端末からのログイン許可を設定（line vty）

工場出荷設定に関しては，HA8000-bd シリーズのマニュアル「ユーザーズガイド」を参照してください。

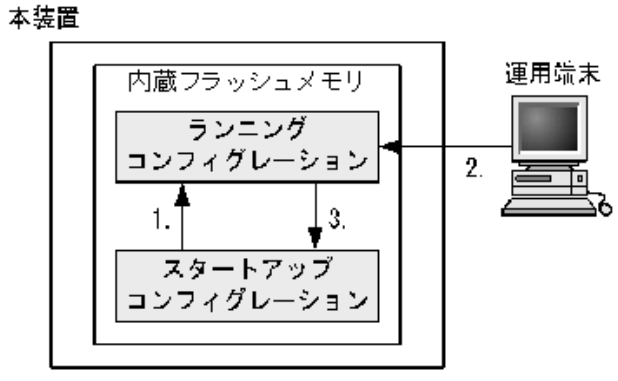
デフォルト設定の構成定義に VLAN や IP アドレスなどを追加設定する場合は，ポート 0/4 を介してリモート端末からログインするか，またはコンソールからログインして，コンフィグレーションを設定してください。（コンソールからのログインについては，「3　装置へのログイン」を参照してください。）

5.1.1 起動時のコンフィグレーション

本装置の電源を入れると，内蔵フラッシュメモリ上のスタートアップコンフィグレーションファイルが読み出され，設定されたコンフィグレーションに従って運用を開始します。運用に使用されているコンフィグレーションをランニングコンフィグレーションと呼びます。

なお，スタートアップコンフィグレーションファイルは，直接編集できません。ランニングコンフィグレーションを編集したあとに，コンフィグレーションコマンド save(write) または運用コマンド copy を使用することで，スタートアップコンフィグレーションファイルが更新されます。起動時，および運用中のコンフィグレーションの概要を次の図に示します。

図 5-1　起動時，および運用中のコンフィグレーションの概要



1. 本装置を起動すると，内蔵フラッシュメモリのスタートアップコンフィグレーションファイルが読み出され，運用を開始します。
2. コンフィグレーションを変更した場合は，ランニングコンフィグレーションに反映されます。
3. 変更されたランニングコンフィグレーションをスタートアップコンフィグレーションファイルに保存します。

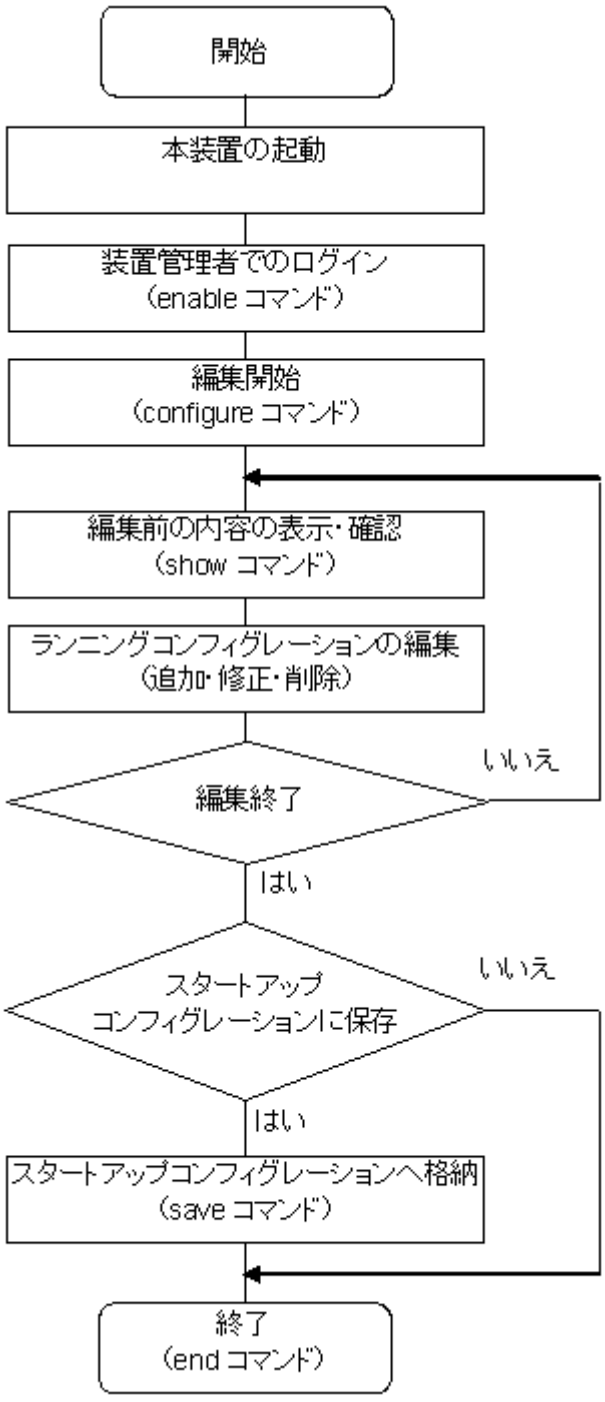
5.1.2 運用中のコンフィグレーション

運用中にコンフィグレーションを編集すると，編集した内容はランニングコンフィグレーションとしてすぐに運用に反映されます。コンフィグレーションコマンド save(write) または運用コマンド copy を使用することで，ランニングコンフィグレーションが内蔵フラッシュメモリにあるスタートアップコンフィグレーションファイルに保存されます。編集した内容を保存しないで装置を再起動すると，編集した内容が失われるので注意してください。

5.2　ランニングコンフィグレーションの編集概要

初期導入時やネットワーク構成を変更する場合は，ランニングコンフィグレーションを編集します。なお，初期導入時のランニングコンフィグレーションの編集はコンソールから行う必要があります。ランニングコンフィグレーションの編集の流れを次の図に示します。詳細については，「5.4　コンフィグレーションの編集方法」を参照してください。

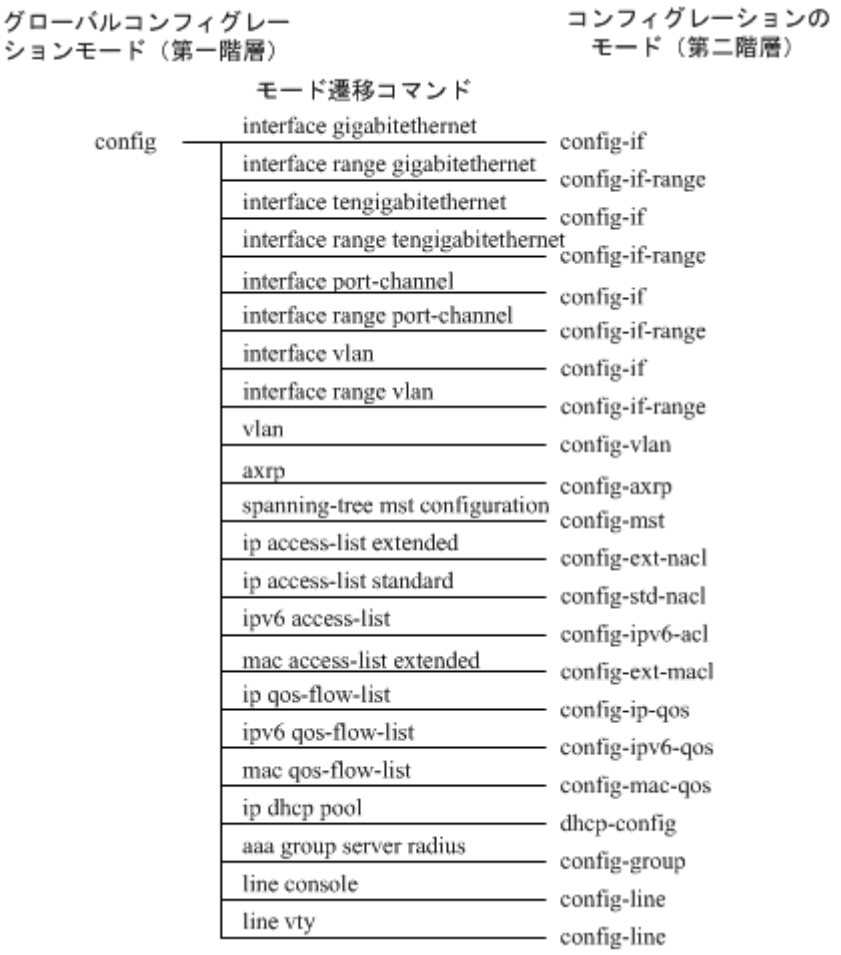
図 5-2　ランニングコンフィグレーションの編集の流れ



5.3 コンフィグレーションコマンド入力におけるモード遷移

コンフィグレーションは，実行可能なコンフィグレーションモードで編集します。第二階層のコンフィグレーションを編集する場合は，グローバルコンフィグレーションモードで第二階層のコンフィグレーションモードに移行するためのコマンドを実行してモードを移行した上で，コンフィグレーションコマンドを実行する必要があります。コンフィグレーションのモード遷移の概要を次の図に示します。

図 5-3 コンフィグレーションのモード遷移の概要



5.4 コンフィグレーションの編集方法

5.4.1 コンフィグレーション・運用コマンド一覧

コンフィグレーションの編集および操作に関するコンフィグレーションコマンド一覧を次の表に示します。

表 5-1 コンフィグレーションコマンド一覧

コマンド名	説明
end	コンフィグレーションコマンドモードを終了して装置管理者モードに戻ります。
exit	モードを一つ戻ります。グローバルコンフィグレーションモードで編集中の場合は，コンフィグレーションコマンドモードを終了して装置管理者モードに戻ります。
save(write)	編集したコンフィグレーションをスタートアップコンフィグレーションファイルに保存します。
show	編集中のコンフィグレーションを表示します。
top	コンフィグレーションコマンドモード移行後は，本コマンド入力でグローバルコンフィグレーションモード（第一階層）に戻ります。

コンフィグレーションの表示およびファイル操作に関する運用コマンド一覧を次の表に示します。

表 5-2 運用コマンド一覧

コマンド名	説明
show running-config	ランニングコンフィグレーションを表示します。
show startup-config	スタートアップコンフィグレーションファイルを表示します。
copy	指定したファイルまたはディレクトリをコピーします。
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内容を削除します。
rename	ファイル名の変更をします。
del	指定したファイルを削除します。
mkdir	新しいディレクトリを作成します。
rmdir	指定したディレクトリを削除します。

5.4.2 configure（configure terminal）コマンド

コンフィグレーションを編集する場合は，enable コマンドを実行して装置管理者モードに移行してください。装置管理者モードで，configure コマンドまたは configure terminal コマンドを入力すると，プロンプトが「(config)#」になり，ランニングコンフィグレーションの編集が可能となります。ランニングコンフィグレーションの編集開始例を次の図に示します。

図 5-4 ランニングコンフィグレーションの編集開始例

```
> enable                  …1
# configure               …2
(config)#
```

1. enable コマンドで装置管理者モードに移行します。
2. ランニングコンフィグレーションの編集を開始します。

5.4.3 コンフィグレーションの表示・確認（show コマンド）

（1）スタートアップコンフィグレーションファイル，ランニングコンフィグレーションの表示・確認

装置管理者モードで運用コマンド show running-config ／ show startup-config を使用することで，ランニングコンフィグレーションおよびスタートアップコンフィグレーションファイルを表示・確認できます。ランニングコンフィグレーションの表示例を次の図に示します。

図 5-5　ランニングコンフィグレーションの表示例

```
# show running-config                    …1
#configuration list for XXXXXX-XXX
!
vlan 1
  name "VLAN0001"
!
vlan 100
  state active
!
vlan 200
  state active
!
vlan 4094
  name "BS_MANAGEMENT"
!
spanning-tree mode pvst
!
interface tengigabitethernet 0/1
  switchport mode access
  switchport access vlan 100
!
interface tengigabitethernet 0/2
  switchport mode access
  switchport access vlan 200
!
       :
       :
#
```

1. ランニングコンフィグレーションを表示します。

（2）コンフィグレーションの表示・確認

コンフィグレーションモードで show コマンドを使用することで，編集前，編集後のコンフィグレーションを表示・確認できます。コンフィグレーションを表示した例を「図 5-6　コンフィグレーションの内容をすべて表示」～「図 5-9　インタフェースモードで指定のインタフェース情報を表示」に示します。

［注意事項］

1. グローバルコンフィグレーションモードでは，コンフィグレーションモード（第二階層）へ遷移するコマンドに対してだけパラメータを指定できます。補完機能・ヘルプ機能・短縮実行なども使用可能です。
2. コンフィグレーションモード（第二階層）では，グローバルコンフィグレーションモードと同様にモードを遷移するコマンドに対してだけパラメータを指定できますが，補完機能・ヘルプ機能などは使用できません。

図 5-6　コンフィグレーションの内容をすべて表示

```
(config)# show                                  …1
#configuration list for XXXXXX-XXX
!
vlan 1
  name "VLAN0001"
!
vlan 100
  state active
!
vlan 200
  state active
!
vlan 4094
  name "BS_MANAGEMENT"
!
spanning-tree mode pvst
!
interface tengigabitethernet 0/1
  switchport mode access
  switchport access vlan 100
!
interface tengigabitethernet 0/2
  switchport mode access
  switchport access vlan 200
!
        :
        :
(config)#
```

1. パラメータを指定しない場合はランニングコンフィグレーションを表示します。

図 5-7　gigabitethernet インタフェース情報を表示

```
(config)# show interface gigabitethernet        …1
interface gigabitethernet 0/3
  switchport mode access
  switchport access vlan 100
!
interface gigabitethernet 0/4
  switchport mode access
  switchport access vlan 4094
  spanning-tree portfast trunk
!
        :
        :
(config)#
```

1. ランニングコンフィグレーションのうち，gigabitethernet インタフェース情報をすべて表示します。

図 5-8　指定のインタフェース情報を表示

```
(config)# show interface gigabitethernet 0/3      …1
interface gigabitethernet 0/3
  switchport mode access
  switchport access vlan 100
!
(config)#
```

1. ランニングコンフィグレーションのうち，インタフェース 0/3 を表示します。

図 5-9 インタフェースモードで指定のインタフェース情報を表示

```
(config)# interface gigabitethernet 0/3 …1
(config-if)# show
interface gigabitethernet 0/3
  switchport mode access
  switchport access vlan 100
!
(config-if)#
```

1. ランニングコンフィグレーションのうち，インタフェース 0/3 を表示します。

5.4.4 コンフィグレーションの追加・変更・削除

(1) コンフィグレーションコマンドの入力

コンフィグレーションコマンドを使用して，コンフィグレーションを編集します。また，コンフィグレーションのコマンド単位での削除は，コンフィグレーションコマンドの先頭に「no」を指定することで実現できます。

ただし，機能の抑止を設定するコマンドでは，コンフィグレーションコマンドの先頭に「no」を指定して設定し，機能の抑止を解除する場合は「no」を外したコンフィグレーションコマンドを入力します。

コンフィグレーションの編集例を「図 5-10 コンフィグレーションの編集例」に，機能の抑止および解除の編集例を「図 5-11 機能の抑止および解除の編集例」に示します。

図 5-10 コンフィグレーションの編集例

```
(config)# vlan 100                                  …1
!(config-vlan)# state active                        …2
!(config-vlan)# exit
!(config)# interface gigabitethernet 0/3            …3
!(config-if)# switchport mode access                …4
!(config-if)# switchport access vlan 100            …5
!(config-if)# exit
!(config)# vlan 100                                 …6
!(config-vlan)# state suspend                       …7
!(config-vlan)# exit
!(config)# interface gigabitethernet 0/3            …8
!(config-if)# no switchport access vlan             …9
!(config-if)# exit
!(config)#
```

1. VLAN 100 をポート VLAN として設定します。
2. VLAN 100 を有効にします。
3. イーサネットインタフェース 0/3 にモードを遷移します。
4. イーサネットインタフェース 0/3 にアクセスモードを設定します。
5. アクセス VLAN に 100 を設定します。
6. VLAN 100 にモードを遷移します。
7. VLAN 100 を有効から無効に変更します。
8. イーサネットインタフェース 0/3 にモードを遷移します。
9. 設定されているアクセス VLAN の VLAN ID 100 を削除します。

図 5-11　機能の抑止および解除の編集例

```
(config)# interface gigabitethernet 0/3
!(config-if)# shutdown                                  …1
!(config-if)# speed 100                                 …2
!(config-if)# duplex full                               …3
!(config-if)# no shutdown                               …4
!(config-if)#
```

1. インタフェースを無効にします。
2. 伝送速度を 100Mbit/s に設定します。
3. duplex を full（全二重）に設定します。
4. インタフェースを有効にします。

（2） 入力コマンドのチェック

コンフィグレーションコマンドを入力すると，入力されたコンフィグレーションに誤りがないかすぐにチェックされます。エラーがない場合は「図 5-12　正常入力時の出力」に示すようにプロンプトを表示して，コマンドの入力待ちになります。ランニングコンフィグレーションの編集中の場合は，変更した内容がすぐに運用に使用されます。

エラーがある場合は「図 5-13　異常入力時のエラーメッセージ出力」に示すように，入力したコマンドの行の下にエラーの内容を示したエラーメッセージを表示します。この場合，入力したコンフィグレーションは反映されないので，入力の誤りを修正してから再度入力してください。

図 5-12　正常入力時の出力

```
(config)# interface gigabitethernet 0/3
!(config-if)# description TokyoOsaka
!(config-if)#
```

図 5-13　異常入力時のエラーメッセージ出力

```
(config)# interface gigabitethernet 0/3
!(config-if)# description
                           ^
Error: Missing parameter.
!(config-if)#
```

5.4.5　コンフィグレーションのファイルへの保存

コンフィグレーションコマンド save(write) または運用コマンド copy を使用することで，編集したランニングコンフィグレーションをスタートアップコンフィグレーションファイルに保存できます。コンフィグレーションの保存例を次の図に示します。

図 5-14　コンフィグレーションの保存例（save コマンド）

```
# configure                 …1
(config)#
        :
        :                   …2
        :
!(config)# save             …3
(config)#
```

1. ランニングコンフィグレーションの編集を開始します。
2. コンフィグレーションを変更します。
3. スタートアップコンフィグレーションファイルに保存します。

図 5-15 コンフィグレーションの保存例（copy コマンド）

```
# configure                                  …1
(config)#
        :
        :                                    …2
        :
!(config)# end                               …3
!# copy running-config startup-config …4
Do you wish to copy from running-config to startup-config? (y/n) :y
#
```

1. ランニングコンフィグレーションの編集を開始します。
2. コンフィグレーションを変更します。
3. end コマンドで装置管理者モードまで戻ります。
4. スタートアップコンフィグレーションファイルに保存します。

5.4.6 コンフィグレーションの編集終了（exit コマンド）

ランニングコンフィグレーションの編集を終了する場合は，グローバルコンフィグレーションモードで exit コマンドを実行します。

5.4.7 コンフィグレーションの編集時の注意事項

（1） 設定できるコンフィグレーションのコマンド数に関する注意事項

制限を超えるようなコンフィグレーションを編集した場合は，「Maximum number of entries are already defined .」などのメッセージを表示します。このような場合，むだなコンフィグレーションが設定されていないか確認してください。

（2） コンフィグレーションをコピー＆ペーストで入力する際の注意事項

コンフィグレーションをコピー&ペーストで入力する場合，一度に 1000 文字（スペース，改行含む）以内でご使用ください。

1000 文字を超えるコンフィグレーションを設定する場合は，1000 文字以内で複数回にわけてコピー&ペーストを行ってください。

5.5 コンフィグレーションの操作

この節では，コンフィグレーションのバックアップ，ファイル転送などの操作について説明します。

5.5.1 ftp を使用したファイル転送

リモート運用端末との間でファイル転送をするときは ftp プロトコルを使用します。

(1) バックアップコンフィグレーションファイルを本装置に転送する場合

PC に保存してあるバックアップコンフィグレーションファイルを，ftp で本装置に転送後，運用コマンド copy を使用してスタートアップコンフィグレーションファイルにコピーします。

PC でコマンドプロンプト画面を開きます。(Windows 標準の場合，PC で「スタート」⇒「すべてのプログラム」⇒「アクセサリ」⇒「コマンドプロンプト」の順に開きます。)

バックアップコンフィグレーションファイルを格納したディレクトリにディレクトリチェンジし，ftp で本装置にログインします。ASCII モードで本装置の RAMDISK に転送します。

ftp で接続するポートに VLAN と IP アドレスを設定してください。

C:\TEMP に backup.cnf ファイルを保存した状態での操作例を下記に示します。

図 5-16 コマンドプロンプト画面での操作：バックアップコンフィグレーションファイルの本装置へのファイル転送例

```
C:\TEMP>ftp 192.168.0.1
Connected to 192.168.0.1
220 GR-BEX310GL FTP server ready
User (192.168.0.1:(none)): operator
331 Password required
Password:
230 User logged in
ftp> asc
200 Type set to A, ASCII mode
ftp>
ftp> put backup.cnf
200 Port set okay
150 Opening ASCII mode data connection
226 Transfer complete
ftp:xxxxxx bytes sent in xx.x Seconds (xx.xx Kbytes/sec)
ftp> bye
221 Bye…see you later
C:\TEMP>
```

コンソールログインし，運用コマンド copy で RAMDISK に転送した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にコピーします。

図 5-17 コンソール画面での操作：転送したファイルを本装置へ反映（copy コマンド）

```
> enable
# copy ramdisk backup.cnf startup-config
Do you wish to copy from RAMDISK to startup-config? (y/n):y
#
```

(2) バックアップコンフィグレーションファイルをリモート運用端末へ転送する場合

本装置の RAMDISK に格納したバックアップコンフィグレーションファイルをリモート運用端末へ転送する例を次の図に示します。

コンソールにログインし，運用コマンド copy でスタートアップコンフィグレーションファイルを

RAMDISK にコピーします。

図 5-18 コンソール画面での操作：スタートアップコンフィグレーションファイルを RAMDISK へコピー（copy コマンド）

```
> enable
# copy startup-config ramdisk backup.cnf
#
```

PC でコマンドプロンプト画面を開きます。

バックアップコンフィグレーションファイルを格納するディレクトリにディレクトリチェンジし，ftp で本装置にログインします。ASCII モードで本装置の RAMDISK からファイルを PC に転送します。

図 5-19 コマンドプロンプト画面での操作：バックアップコンフィグレーションファイルの本装置へのファイル転送例

```
C:\TEMP>ftp 192.168.0.1
Connected to 192.168.0.1
220 GR-BEX310GL FTP server ready
User (192.168.0.1:(none)): operator
331 Password required
Password:
230 User logged in
ftp> asc
200 Type set to A, ASCII mode
ftp>
ftp> get backup.cnf
200 Port set okay
150 Opening ASCII mode data connection
226 Transfer complete
ftp:xxxxxx bytes sent in xx.x Seconds (xx.xx Kbytes/sec)
ftp> bye
221 Bye…see you later
C:\TEMP>
```

5.5.2 MC を使用したファイル転送

MC にファイル転送をするときは運用コマンド copy を使用します。

（1）バックアップコンフィグレーションファイルを本装置に転送する場合

バックアップコンフィグレーションファイルを格納した MC をスロットに挿入します。運用コマンド copy を使用して，MC 内のバックアップコンフィグレーションファイルを本装置の RAMDISK にコピーします。運用コマンド copy を使用して，RAMDISK の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にコピーします。操作例を次の図に示します。

図 5-20 バックアップコンフィグレーションファイルの MC から本装置へのファイル転送例（copy コマンド）

```
> enable
# copy mc backup.cnf ramdisk backup.cnf          …1
# copy ramdisk backup.cnf startup-config         …2
Do you wish to copy from RAMDISK to startup-config? (y/n): y
#
```

1. バックアップコンフィグレーションファイルを MC から RAMDISK にコピーします。
2. RAMDISK の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にコピーします。

（2）バックアップコンフィグレーションファイルを MC に転送する場合

バックアップコンフィグレーションファイルを運用コマンド copy を使用して，MC に保存します。

運用コマンド copy を使用してスタートアップコンフィグレーションファイルを RAMDISK にコピーします。運用コマンド copy を使用して RAMDISK のバックアップコンフィグレーションファイルを MC 内にコピーします。操作例を次の図に示します。

図 5-21　バックアップコンフィグレーションファイルを本装置から MC へコピー（copy コマンド）

```
> enable
# copy startup-config ramdisk backup.cnf                    …1
# copy ramdisk backup.cnf mc backup.cnf                     …2
#
```

1. スタートアップコンフィグレーションファイルを RAMDISK へコピーします。
2. バックアップコンフィグレーションファイルを RAMDISK から MC にコピーします。

5.5.3　バックアップコンフィグレーションファイル反映時の注意事項

運用コマンド copy を使用して，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にコピーした場合，そのままではランニングコンフィグレーションに反映されません。運用コマンド reload，またはリセットスイッチにより，装置の再起動が必要となりますので，リモートからログインしている場合は注意してください。

バックアップコンフィグレーションファイルの内容が本装置の構成と一致していない場合は，バックアップコンフィグレーションファイルの内容を変更してから運用コマンド copy を使用してください。

6 リモート運用端末から本装置へのログイン

この章では，リモート運用端末から本装置へのリモートアクセスについて説明します。

6.1　解説

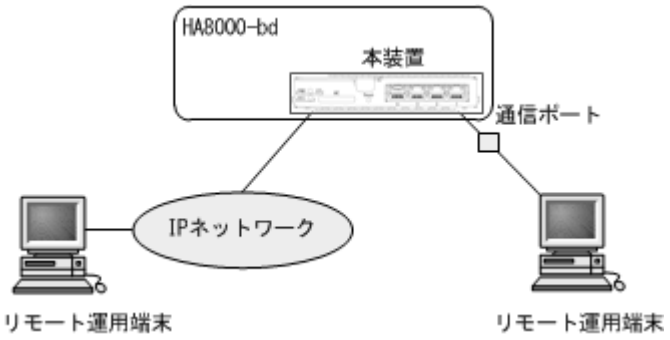
通信用ポートを介して，リモート運用端末から本装置へログインするには，本装置で VLAN や IP アドレスなどの設定が必要です。ただし，初期導入時，以下のコンフィグレーションが設定（工場出荷設定）されています。

- ポート 0/4 は管理用として専用 VLAN が設定
  VLAN4094，IP アドレス：192.168.0.254（サブネットマスク 255.255.255.0）
- ポート 0/5 ～ 0/24 のサーバ接続ポートをエッジポート設定（spanning-tree portfast trunk）
- ポート 0/5 ～ 0/24 の伝送速度は，speed：auto
  上記以外の伝送速度に変更されると，サーバとの通信障害となるケースがありますので，サーバ接続ポートの伝送速度はデフォルト設定のままご使用ください。また，サーバ接続ポートで duplex の変更は未サポートです（全二重で動作します）。
- リモート運用端末からのログイン許可を設定（line vty）

工場出荷設定に関しては，HA8000-bd シリーズのマニュアル「ユーザーズガイド」を参照してください。

デフォルト設定の構成定義に VLAN や IP アドレスなどを追加設定する場合は，ポート 0/4 を介してリモート端末からログインするか，またはコンソールからログインして，コンフィグレーションを設定してください。（コンソールからのログインについては，「3　装置へのログイン」を参照してください。）

図 6-1　リモート運用端末からの本装置へのログイン



6.2　コンフィグレーション

6.2.1　コンフィグレーションコマンド一覧

運用端末の接続とリモート操作に関するコンフィグレーションコマンド一覧を次の表に示します。

表 6-1　コンフィグレーションコマンド一覧

コマンド名	説明
ftp-server	リモート運用端末から ftp プロトコルを使用したアクセスを許可します。
line console	コンソール（RS-232C）のパラメータを設定します。
line vty	装置への telnet リモートアクセスを許可します。
speed	コンソール（RS-232C）の通信速度を設定します。
transport input	リモート運用端末から各種プロトコルを使用したアクセスを規制します。

VLAN の設定，および IPv4/IPv6 インタフェースの設定に関するコンフィグレーションコマンドについては，「16　VLAN」，「24　IPv4 インタフェース」または「25　IPv6 インタフェース」を参照してください。

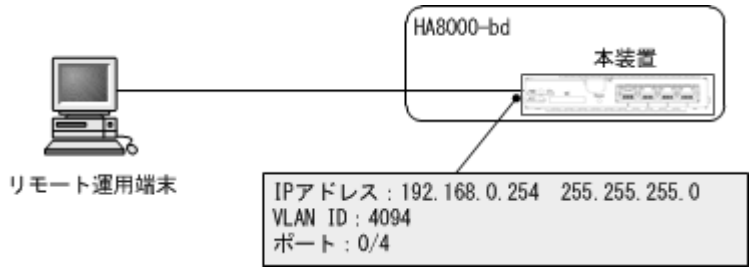
6.2.2　本装置への IP アドレスの設定

リモート運用端末から本装置へアクセスするためには，工場出荷設定の管理用インタフェース（IP アドレス・マスクは「6.1　解説」参照）を使用するか，または新規に接続するインタフェースに対して IP アドレスを設定する必要があります。

（1）工場出荷設定を使用した接続

工場出荷設定の場合は，ポート 0/4 に VLAN と IP アドレスが設定されていますので，ポート 0/4 にリモート運用端末を接続すればアクセスできます。

図 6-2　工場出荷設定を使用したリモート運用端末との接続例

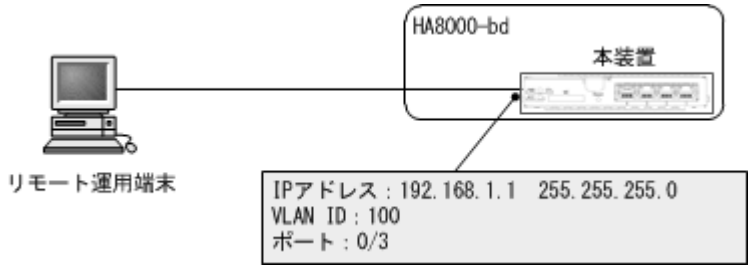


（2）新規に IP アドレスを設定して接続

［設定のポイント］

新規に接続するインタフェースに，あらかじめ VLAN と IP アドレスを設定します。

図 6-3 新規に IP アドレスを設定したリモート運用端末との接続例



［コマンドによる設定］

1. **(config)# vlan 100**
   (config-vlan)# exit
   VLAN ID 100 のポート VLAN を作成します。

2. **(config)# interface gigabitethernet 0/3**
   (config-if)# switchport mode access
   (config-if)# switchport access vlan 100
   (config-if)# exit
   ポート 0/3 のイーサネットインタフェースコンフィグレーションモードに移行します。ポート 0/3 を VLAN 100 のアクセスポートに設定します。

3. **(config)# interface vlan 100**
   (config-if)# ip address 192.168.1.1 255.255.255.0
   (config-if)# exit
   (config)#
   VLAN ID 100 のインタフェースコンフィグレーションモードに移行します。VLAN ID 100 に IPv4 アドレス 192.168.1.1，サブネットマスク 255.255.255.0 を設定します。

6.2.3 telnet によるログインを許可する

［設定のポイント］

あらかじめ，IP アドレスを設定しておく必要があります。
リモート運用端末から本装置に telnet プロトコルによるリモートログインを許可するコンフィグレーションを実施します。
このコンフィグレーションが設定されていない場合，コンソールからだけ本装置にログインできます。

［コマンドによる設定］

1. **(config)# line vty 0 15**
   (config-line)# exit
   リモート運用端末から本装置への telnet プロトコルによるリモートアクセスを許可します。本装置に同時にリモートログインできるユーザ数を最大 16 に設定します。

6.2.4 ftp によるログインを許可する

［設定のポイント］

あらかじめ，IP アドレスを設定しておく必要があります。

リモート運用端末から本装置に ftp プロトコルによるリモートアクセスを許可するコンフィグレーションを実施します。
このコンフィグレーションを実施していない場合，ftp プロトコルを用いた本装置へのアクセスはできません。

［コマンドによる設定］

1. **(config)# ftp-server**
   リモート運用端末から本装置への ftp プロトコルによるリモートアクセスを許可します。

6.3　オペレーション

6.3.1　運用コマンド一覧

運用端末の接続とリモート操作に関する運用コマンド一覧を次の表に示します。

表 6-2　運用コマンド一覧

コマンド名	説明
set exec-timeout	自動ログアウトが実行されるまでの時間を設定します。
set terminal pager	ページングの実施／未実施を設定します。
telnet	指定された IP アドレスのリモートホストへ telnet で接続します。
ftp	本装置と TCP ／ IP で接続されているリモート運用端末との間でファイル転送をします。
tftp	本装置と接続されているリモート運用端末との間で UDP でファイル転送をします。

6.3.2　リモート運用端末と本装置との通信の確認

本装置とリモート運用端末との通信は，運用コマンド ping などを用いて確認できます。詳細は，「24 IPv4 インタフェース」または「25　IPv6 インタフェース」を参照してください。

7 ログインセキュリティと RADIUS

この章では，本装置のログイン制御，ログインセキュリティおよび RADIUS について説明します。

7.1 ログインセキュリティの設定

7.1.1 コンフィグレーション・運用コマンド一覧

ログインセキュリティに関するコンフィグレーションコマンド一覧を次の表に示します。

表 7-1 コンフィグレーションコマンド一覧

コマンド名	説明
aaa authentication login	リモートログイン時に使用する認証方式を指定します。
aaa authentication login end-by-reject	ログイン時の認証で，否認された場合に認証を終了します。通信不可（RADIUS サーバ無応答など）による認証失敗時は，コンフィグレーションコマンド aaa authentication login で次に指定されている認証方式で認証します。
ip access-group	本装置へリモートログインを許可または拒否するリモート運用端末の IPv4 アドレスを指定したアクセスリストを設定します。
ipv6 access-class	本装置へリモートログインを許可または拒否するリモート運用端末の IPv6 アドレスを指定したアクセスリストを設定します。

ログインセキュリティに関する運用コマンド一覧を次の表に示します。

表 7-2 運用コマンド一覧

コマンド名	説明
adduser	新規ログインユーザ用のアカウントを追加します。
rmuser	adduser コマンドで登録されているログインユーザのアカウントを削除します。
password	ログインユーザのパスワードを指定します。
clear password	ログインユーザのパスワードを削除します。
show users	本装置に設定した有効なユーザ情報を表示します。
show sessions(who)	本装置にログインしているユーザを表示します。

7.1.2 ログイン制御の概要

本装置にはローカルログイン（シリアル接続）と IPv4 および IPv6 ネットワーク経由のリモートログイン機能（telnet）があります。

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. ログイン時に不正アクセスを防止するため，ユーザ ID とパスワードによるチェックを設けています。
2. ローカルとリモートの運用端末から同時にログインできます。
3. 本装置にログインできるリモートユーザ数は最大 16 ユーザです。なお，コンフィグレーションコマンド line vty でログインできるユーザ数を制限できます。
4. 本装置にアクセスできる IPv4 アドレスおよび IPv6 アドレスをコンフィグレーションコマンド ip access-list standard，ipv6 access-list，ip access-group，ipv6 access-class で制限できます。
5. 本装置にアクセスできるプロトコル（telnet，ftp）をコンフィグレーションコマンド transport input や ftp-server で制限できます。
6. 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。（この場合の運用端末には，コンソール，telnet，ftp を含みます。）

7. 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。運用ログは運用コマンド show logging で参照できます。
8. 一定時間（デフォルト：60 分）内にキーの入力がなかった場合，自動的にログアウトします。なお，自動ログアウト時間は運用コマンド set exec-timeout で変更できます。

7.1.3　ログインユーザの作成と削除

運用コマンド adduser を用いて本装置にログインできるユーザを作成してください。ログインユーザの作成例を次の図に示します。

図 7-1　newuser を作成

```
> enable
# adduser newuser
User(empty password) add done. Please setting password.

Changing local password for newuser.
New password:********                                    … 1
Retype new password:********                             … 2
# exit
>
```

1. パスワードを入力します（実際には入力文字は表示されません）。
2. 確認のため再度パスワードを入力します（実際には入力文字は表示されません）。

また，使用しなくなったユーザは rmuser コマンドを用いて削除できます。

特に，初期導入時に設定されているログインユーザ "operator" を運用中のログインユーザとして使用しない場合，セキュリティの低下を防ぐため，新しいログインユーザを作成したあとに rmuser コマンドで削除することをお勧めします。また，コンフィグレーションコマンド aaa authentication login で，RADIUS を使用したログイン認証ができます。コンフィグレーションの設定例については，「7.3.2　ログイン認証方式の設定」を参照してください。

作成したユーザ ID は忘れないようにしてください。

7.1.4　装置管理者モード移行のパスワードの設定

コンフィグレーションコマンドを実行するためには enable コマンドで装置管理者モードに移行する必要があります。初期導入時に enable コマンドを実行した場合，パスワードは設定されていませんので認証なしで装置管理者モードに移行します。ただし，通常運用中にすべてのユーザがパスワード認証なしで装置管理者モードに移行できるのはセキュリティ上危険ですので，初期導入時にパスワードを設定しておいてください。パスワード設定の実行例を次の図に示します。

図 7-2　初期導入直後の装置管理者モード移行のパスワード設定

```
> enable
# password enable-mode
Changing local password for admin.
New password:
Retype new password:
#
```

7.1.5　リモート運用端末からのログインの許可

コンフィグレーションコマンド line vty を設定することで，リモート運用端末から本装置へログインでき

るようになります。このコンフィグレーションが設定されていない場合，コンソールからだけ本装置にログインできます。リモート運用端末からのログインを許可する設定例を次の図に示します。

図 7-3 リモート運用端末からのログインを許可する設定例

```
(config)# line vty 0 1
(config-line)# exit
```

また，リモート運用端末から ftp プロトコルを用いて，本装置にアクセスする場合には，コンフィグレーションコマンド ftp-server を設定する必要があります。本設定を実施しない場合，ftp プロトコルを用いた本装置へのアクセスはできません。

図 7-4 ftp プロトコルによるアクセス許可の設定例

```
(config)# ftp-server
(config)#
```

7.1.6 同時にログインできるユーザ数の設定

コンフィグレーションコマンド line vty を設定することで，リモート運用端末から本装置へログインできるようになります。コンフィグレーションコマンド line vty の <End allocation> パラメータで，リモートログインできるユーザ数が制限されます。なお，この設定にかかわらず，コンソールからは常にログインできます。最大 16 人まで同時にログインを許可する設定例を次の図に示します。

図 7-5 同時にログインできるユーザ数の設定例

```
(config)# line vty 0 15
(config-line)# exit
```

同時ログインに関する動作概要を次に示します。

- 複数ユーザが同時にログインすると，ログインしているユーザ数が制限数以下でもログインできない場合があります。
- 同時にログインできるユーザ数を変更しても，すでにログインしているユーザのセッションが切れることはありません。

7.1.7 リモート運用端末からのログインを許可する IP アドレスの設定

リモート運用端末から本装置へのログインについて，次に示す設定でログインを制限できます。なお，設定後はリモート運用端末から本装置へのログインの可否を確認してください。

［設定のポイント］

特定のリモート運用端末からだけ，本装置へのアクセスを許可する場合は，コンフィグレーションコマンド ip access-list standard，ipv6 access-list，ip access-group，ipv6 access-class であらかじめアクセスを許可する端末の IP アドレスを登録しておく必要があります。アクセスを許可する IPv4 アドレスとサブネットマスク，または IPv6 アドレスとプレフィックスは，合わせて最大 128 リストの登録ができます。このコンフィグレーションを実施していない場合，すべてのリモート運用端末から本装置へのアクセスが可能となります。

［コマンドによる設定］（IPv4 の場合）

1. **(config)# ip access-list standard REMOTE**
   (config-std-nacl)# deny host 192.168.0.254

```
(config-std-nacl)# permit 192.168.0.0 0.0.0.255
(config-std-nacl)# exit
```

ネットワーク（192.168.0.0/24）からだけログインを許可し，そのうち 192.168.0.254 の IPv4 アドレスからのログインを拒否する，アクセスリスト情報 REMOTE を設定します。

2.
```
(config)# line vty 0 1
(config-line)# ip access-group REMOTE in
(config-line)# exit
```

line モードに遷移し，アクセスリスト情報 REMOTE を適用し，ネットワーク（192.168.0.0/24）にあるリモート運用端末からだけログインを許可します。

［コマンドによる設定］（IPv6 の場合）

1.
```
(config)# ipv6 access-list REMOTE6
(config-ipv6-nacl)# deny ipv6 host 3ffe:501:811:ff01::0001
(config-ipv6-nacl)# permit ipv6 3ffe:501:811:ff01::/64 any
(config-ipv6-nacl)# exit
```

ネットワーク（3ffe:501:811:ff01::/64）からだけログインを許可し，そのうち 3ffe:501:811:ff01::0001 の IPv6 アドレスからのログインを拒否する，アクセスリスト情報 REMOTE6 を設定します。

2.
```
(config)# line vty 0 1
(config-line)# ipv6 access-class REMOTE6 in
(config-line)# exit
```

line モードに遷移し，アクセスリスト情報 REMOTE6 を適用し，ネットワーク（3ffe:501:811:ff01::/64）にあるリモート運用端末からだけログインを許可します。

［注意事項］

- 本機能で使用するアクセスリストは，フロー検出モードの設定に依存しません。
- permit 条件に一致した IP アドレスは，リモートログイン許可の対象となります。
  deny 条件に一致した IP アドレスは，リモートログイン拒否の対象となります。
- ip access-group および ipv6 access-class の最終リストには，全 IP アドレスを対象とした暗黙の deny 条件が存在します。登録されているすべてのグループに一致しなかった場合は，暗黙の deny 条件に一致したものとみなし，リモートログインを拒否します。
- ip access-group および ipv6 access-class にアクセスリストが登録されていない場合は，permit と同様の処理となります。

7.2　RADIUS の解説

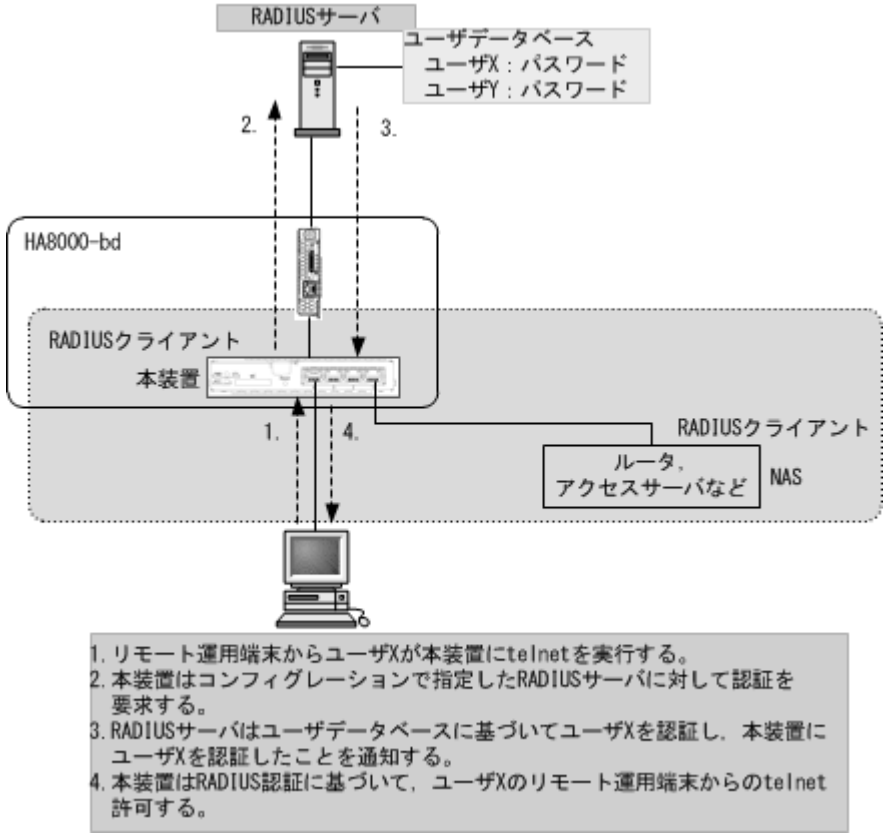
7.2.1　RADIUS の概要

RADIUS （Remote Authentication Dial In User Service）とは，NAS（Network Access Server）に対して認証やアカウンティングを提供するプロトコルです。NAS は RADIUS サーバ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 サーバに対してユーザ認証やアカウンティングなどのサービスを要求します。RADIUS 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。本装置は NAS の機能をサポートします。

RADIUS を使用すると 1 台の RADIUS 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やアカウンティング情報を一元管理できるようになります。本装置では，RADIUS サーバに対してユーザ認証やアカウンティングを要求できます。

RADIUS 認証の流れを次の図に示します。

図 7-6　RADIUS 認証の流れ



7.2.2　RADIUS 認証の適用機能および範囲

本装置で RADIUS 認証を適用する機能を次に示します。

- リモート運用端末からログイン時のユーザ認証（以下，ログイン認証）
  RADIUS 認証

- レイヤ 2 認証機能（IEEE802.1X，Web 認証，MAC 認証）
  RADIUS 認証，RADIUS アカウンティング

レイヤ 2 認証機能については，コンフィグレーションガイド Vol.2 を参照してください。

本項では，ログイン認証について，RADIUS 認証のサポート範囲を記述します。

（1） RADIUS 認証の適用範囲

RADIUS 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 ftp（IPv4/IPv6）

次に示す操作は RADIUS 認証を適用できません。

- コンソール（RS-232C）からのログイン

（2） RADIUS サーバのサポート範囲

RADIUS サーバに対して，本装置がサポートする NAS 機能を次の表に示します。

表 7-3　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	ログイン認証で使用する次のタイプ • Access-Request (送信) • Access-Accept (受信) • Access-Reject (受信) • Access-Challenge(受信)
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-IPv6-Address • Reply-Message • State • NAS-Identifier

（a） 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。

- Access-Request パケット
  本装置が送信するパケットには，この表で示す以外の属性は添付しません。
- Access-Accept，Access-Reject，Access-Challenge パケット
  この表で示す以外の属性が添付されていた場合，本装置ではそれらの属性を無視します。

表 7-4　使用する RADIUS 属性の内容

属性名	属性値	パケットタイプ	内容
User-Name	1	Access-Request	認証するユーザの名前。
User-Password	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。

属性名	属性値	パケットタイプ	内容
Service-Type	6	Access-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	4	Access-Request	本装置の IPv4 アドレス。 IPv4 アドレスが登録されている VLAN インタフェースのうち，最も小さい VLAN ID の IPv4 アドレスを使用します。
Reply-Message	18	Access-Challenge Access-Accept ※ 1 Access-Reject ※ 1	テキスト文字列。
State	24	Access-Challenge Access-Request	テキスト文字列。 Access-Challenge に対応する Access-Request のときに，本装置で保持していた State 情報を付加します。
NAS-Identifier	32	Access-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。
NAS-IPv6-Address	95	Access-Request	本装置の IPv6 アドレス。 IPv6 アドレスが登録されている VLAN インタフェースのうち，最も小さい VLAN ID の IPv6 アドレスを使用します。

注※ 1

Access-Accept と Access-Reject は，Reply-Message を無視します。

7.2.3 RADIUS を使用した認証

本項ではログイン認証で使用する RADIUS 認証について説明します。

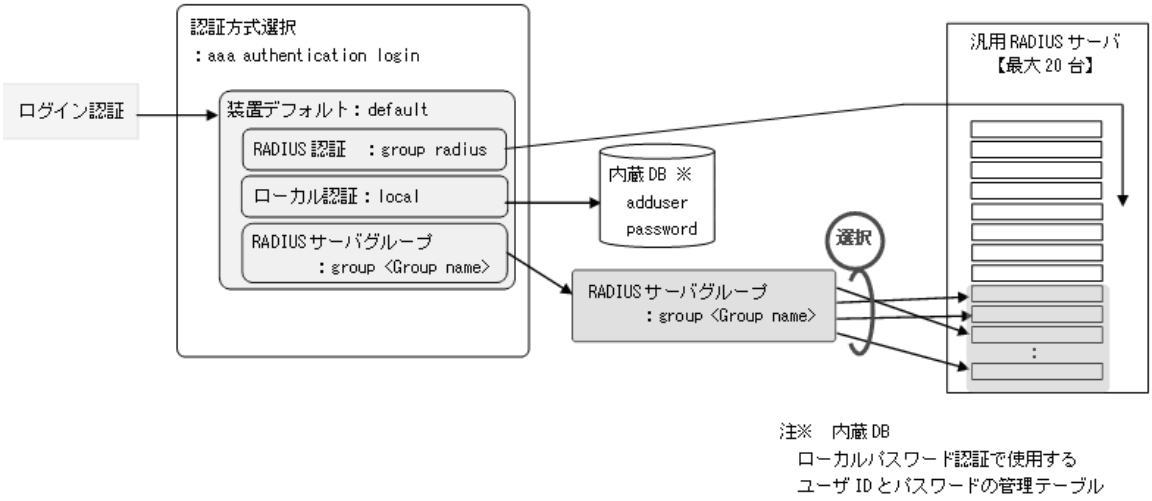
なお，後述の RADIUS サーバの選択や自動復旧機能は，レイヤ 2 認証でも同様に使用します。詳細は，「コンフィグレーションガイド Vol.2 5 レイヤ 2 認証機能の概説」を参照してください。

(1) ログイン認証サービスの選択

ログイン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 認証（汎用 RADIUS サーバ認証，または RADIUS サーバグループ認証）および adduser/password コマンドによる本装置単体でのローカルパスワード認証機能です。

認証方式設定の相関図を次の図に示します。

図 7-7　認証方式設定の相関図



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。また，同時に指定された場合に先に指定された方式で認証に失敗したときの認証サービスの選択動作を，コンフィグレーションコマンド aaa authentication login end-by-reject で変更できます。

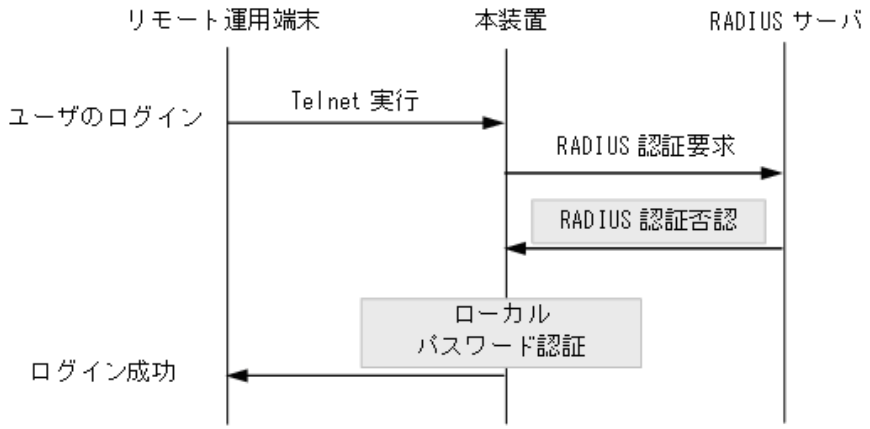
なお，上図の group radius（汎用 RADIUS サーバ認証）と group <Group name>（RADIUS サーバグループ認証）は，どちらも RADIUS 認証サービスとして扱いますので，両方を同時に指定できません。どちらか一つとローカルパスワード認証を組み合わせてご使用ください。

（a） end-by-reject 未設定時

end-by-reject 未設定時の認証サービスの選択について説明します。end-by-reject 未設定時は，先に指定された方式で認証に失敗した場合に，その失敗の理由に関係なく，次に指定された方式で認証できます。

例として，コンフィグレーション認証方式に RADIUS 認証，単体でのローカルパスワード認証の順番で指定し，それぞれの認証結果が RADIUS サーバ認証否認，ローカルパスワード認証成功となる場合の認証方式シーケンスを次の図に示します。

図 7-8　認証方式シーケンス (end-by-reject 未設定時)



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 サーバとの認証否認によって RADIUS サーバでの認証に失敗すると，次に本

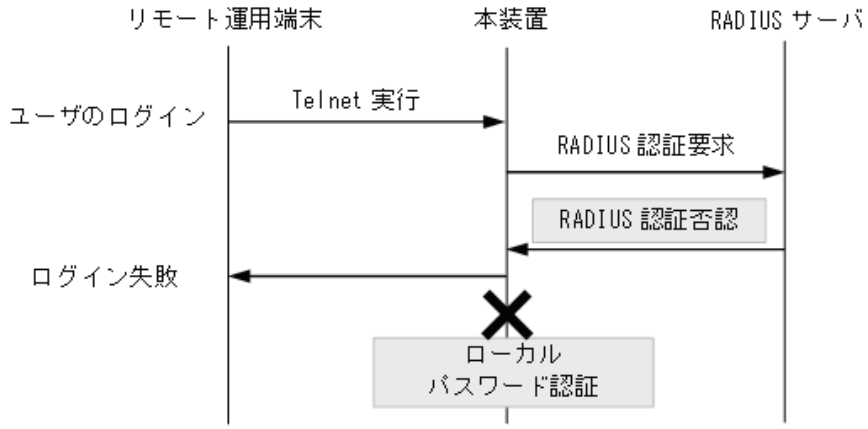
装置のローカルパスワード認証での認証を実行します。ここで認証に成功し，ユーザは本装置へのログインに成功します。

（b） end-by-reject 設定時

end-by-reject 設定時の認証サービスの選択について説明します。end-by-reject 設定時は，先に指定された方式で認証否認された場合に，次に指定された方式で認証を行いません。否認された時点で認証を終了し，一連の認証が失敗となります。通信不可（RADIUS サーバ無応答など）によって認証が失敗した場合だけ，次に指定された方式で認証できます。

例として，認証方式に RADIUS 認証，単体でのローカルパスワード認証の順番で指定し，認証結果が RADIUS サーバ認証否認となる場合の認証方式シーケンスを次の図に示します。

図 7-9　認証方式シーケンス (end-by-reject 設定時)



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 サーバでの認証否認によって RADIUS サーバでの認証に失敗すると，この時点で一連の認証が失敗となり，認証を終了します。次に指定されている本装置のローカルパスワード認証は行いません。その結果，ユーザは本装置へのログインに失敗します。

（2） RADIUS サーバの選択と自動復旧（dead-interval）機能

リモートログインの RADIUS 認証で使用する汎用 RADIUS サーバは最大 20 台まで指定できます。一つのサーバと通信できず，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への接続を試行します。

- RADIUS サーバの選択（通信不可を判断するまでの最大時間）
  RADIUS サーバと通信不可を判断する応答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 3 回です。このため，ログイン方式として RADIUS サーバが使用できないと判断するまでの最大時間は，応答タイムアウト時間×（最初の 1 回＋再送回数）× RADIUS サーバ設定数になります。
- 自動復旧（dead-interval）機能
  本装置の RADIUS 認証では，認証対象端末からのフレーム受信による RADIUS 認証要求を契機に有効な RADIUS サーバを検出し，以降の端末は常に有効な RADIUS サーバを使用します。この方式では，認証されるまでの時間は軽減されますが，RADIUS サーバを負荷分散構成などで使用時，RADIUS サーバに障害が発生すると負荷分散状態に自動的に復旧できません。本装置では，最初の有効な RADIUS サーバ（プライマリ RADIUS サーバ）への自動復旧手段として，監視タイマによる自動復旧（dead-interval）機能をサポートしています。監視タイマのデフォルトは 10 分です。

（3） RADIUS サーバへの登録情報

RADIUS サーバにユーザ ID およびパスワードを登録します。RADIUS サーバへ登録するユーザ ID には次に示す 2 種類があります。

- 運用コマンド adduser を使用して本装置に登録済みのユーザ ID
  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 ID
  初期状態のユーザ ID"operator" でログイン処理を行います。

ユーザ ID とパスワードは，下記の範囲で RADIUS サーバへ登録してください。

- ユーザ ID：英数字で 1 ～ 16 文字（1 文字目は英字，2 文字目以降は英数字）
- パスワード：英数字で 6 ～ 128 文字

7.2.4 RADIUS サーバとの接続

（1） RADIUS サーバでの本装置の識別

RADIUS サーバでは RADIUS クライアントを識別するキーとして，要求パケットの送信元 IP アドレスを使用します。本装置では，送信元 VLAN インタフェースの IP アドレスを使用します。

（2） 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 1645 のポート番号を使用している場合があります。このときはコンフィグレーションコマンド radius-server host の auth-port パラメータで 1645 を指定してください。なお，auth-port パラメータでは 1 ～ 65535 の任意の値が指定できますので，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。

（3） 本装置で設定する RADIUS サーバ情報

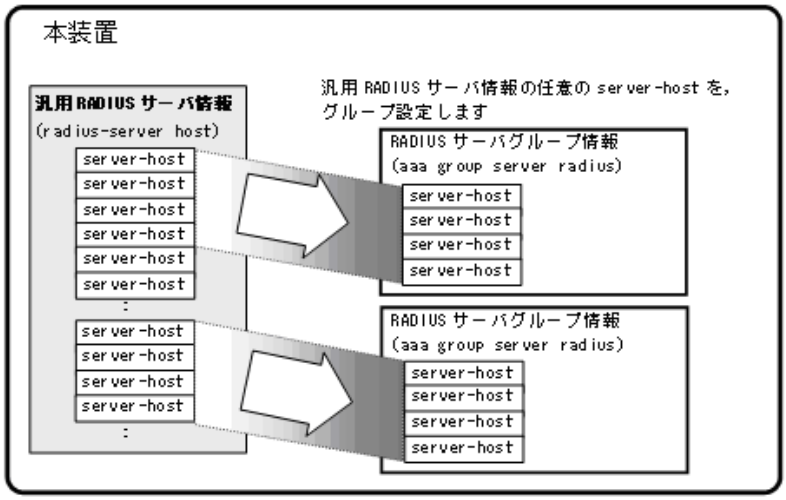
本装置では，以下の RADIUS サーバ情報を設定できます。

- 汎用 RADIUS サーバ情報
  ログイン認証とレイヤ 2 認証機能の両方で使用します。
- 認証専用 RADIUS サーバ情報（IEEE802.1X，Web 認証，MAC 認証）
  各レイヤ 2 認証機能だけで使用します。
- RADIUS サーバグループ情報
  汎用 RADIUS サーバをグループ化し，ログイン認証とレイヤ 2 認証機能の両方で使用します。

レイヤ 2 認証機能と各 RADIUS サーバ情報の設定や運用については，「コンフィグレーションガイド Vol.2 5 レイヤ 2 認証機能の概説」を参照してください。

RADIUS サーバグループ情報は，設定した汎用 RADIUS サーバ情報から割り当てます。RADIUS サーバグループと汎用 RADIUS サーバの関係を次の図に示します。

図 7-10　RADIUS サーバグループ情報と汎用 RADIUS サーバ情報の関係



RADIUS サーバグループで設定する IP アドレス，認証用ポート番号，アカウンティング用ポート番号は，汎用 RADIUS サーバ情報（コンフィグレーションコマンド radius-server host）と同値を設定します。

なお，RADIUS サーバグループ内の RADIUS サーバ選択動作は，その他の RADIUS サーバと同様ですが，自動復旧時間はコンフィグレーションコマンド radius-server dead-interval の設定に従います。

RADIUS サーバグループの収容条件については，「2.2　収容条件」を参照してください。

RADIUS サーバグループは，レイヤ 2 認証機能のポート別認証方式や Web 認証のユーザ ID 別認証方式でも運用します。詳細は「コンフィグレーションガイド Vol.2　5　レイヤ 2 認証機能の概説」を参照してください。

7.3 RADIUS のコンフィグレーション

7.3.1 コンフィグレーションコマンド一覧

RADIUS に関するコンフィグレーションコマンド一覧を次の表に示します。

表 7-5 コンフィグレーションコマンド一覧（RADIUS）

コマンド名	説明
aaa group server radius	RADIUS サーバグループを設定します。
server	RADIUS サーバグループの RADIUS サーバホストを設定します。
radius-server dead-interval	プライマリ RADIUS サーバへ自動復旧するまでの監視タイマを設定します。
radius-server host	認証に使用する汎用 RADIUS サーバ情報を設定します。
radius-server key	認証に使用する RADIUS サーバ鍵を設定します。
radius-server retransmit	認証に使用する RADIUS サーバへの再送回数を設定します。
radius-server timeout	認証に使用する RADIUS サーバの応答タイムアウト値を設定します。
radius-server attribute station-id capitalize	RADIUS サーバへ送信時に使用する RADIUS 属性の MAC アドレスを大文字で送信します。（レイヤ 2 認証機能で使用※）

注※

レイヤ 2 認証機能で本コマンドが適用される RADIUS 属性については，「コンフィグレーションガイド Vol.2」の各認証機能解説編を参照してください。

7.3.2 ログイン認証方式の設定

ログイン認証方式として，下記の設定例を示します。

- 汎用 RADIUS サーバ認証とローカルパスワード認証の組み合わせ
- RADIUS サーバグループ認証とローカルパスワード認証の組み合わせ

（1） 汎用 RADIUS サーバ認証とローカルパスワード認証の設定

［設定のポイント］

本例では，認証方式に RADIUS 認証とローカルパスワード認証を設定します。通信不可（RADIUS サーバ無応答など）により RADIUS 認証に失敗した場合は，本装置によるローカルパスワード認証を行うように設定します。

なお，RADIUS 認証否認によって認証に失敗した場合には，その時点で認証を終了し，ローカルパスワード認証を行いません。

また，RADIUS 認証で使用する汎用 RADIUS サーバ情報を設定します。

あらかじめ，通常のリモートアクセスに必要な設定を行っておく必要があります。

［コマンドによる設定］

1. **(config)# aaa authentication login default group radius local**
   使用するログイン認証方式を RADIUS 認証，ローカルパスワード認証の順に設定します。

2. **(config)# aaa authentication login end-by-reject**
   RADIUS 認証で否認された場合には，その時点で認証を終了し，ローカルパスワード認証を行わない

ように設定します。

3. **(config)# radius-server host 192.168.10.1 key "AAAA1234"**
RADIUS 認証に使用する汎用 RADIUS サーバ 192.168.10.1 の IP アドレスと共有鍵を設定します。

4. **(config)# radius-server host 192.168.10.2 key "BBBB1234"**
RADIUS 認証に使用する汎用 RADIUS サーバ 192.168.10.2 の IP アドレスと共有鍵を設定します。

[注意事項]

1. "group radius" と "group < グループ名 >" はどちらも RADIUS 認証のため，同一 <Method> として扱いますので，認証方式には一緒に設定できません。複数指定の場合は，どちらか一方と "local" を組み合わせてください。

(2) RADIUS サーバグループ認証とローカルパスワード認証の設定

[設定のポイント]

本例では，認証方式に RADIUS サーバグループ認証とローカルパスワード認証を設定します。通信不可（RADIUS サーバ無応答など）により RADIUS サーバグループ認証に失敗した場合は，本装置によるローカルパスワード認証を行うように設定します。
なお，RADIUS 認証否認によって認証に失敗した場合には，その時点で認証を終了し，ローカルパスワード認証を行いません。
また，RADIUS サーバグループ認証で使用する RADIUS サーバグループ情報については，「7.3.3 RADIUS サーバグループの設定」を参照してください。
あらかじめ，通常のリモートアクセスに必要な設定を行っておく必要があります。

[コマンドによる設定]

1. **(config)# aaa authentication login default group LOGIN-SEC local**
RADIUS サーバグループ名，ローカルパスワード認証の順番に設定します。

2. **(config)# aaa authentication login end-by-reject**
RADIUS サーバグループ認証で否認された場合には，その時点で認証を終了し，ローカルパスワード認証を行わないように設定します。

[注意事項]

1. "group radius" と "group < グループ名 >" はどちらも RADIUS 認証のため，同一 <Method> として扱いますので，認証方式には一緒に設定できません。複数指定の場合は，どちらか一方と "local" を組み合わせてください。

7.3.3 RADIUS サーバグループの設定

[設定のポイント]

認証で使用する RADIUS サーバグループを設定します。
RADIUS サーバグループには，コンフィグレーションコマンド radius-server host（汎用 RADIUS サーバ）で設定した RADIUS サーバから，グループ使用するアドレスを設定します。
1 グループには最大 4 つの RADIUS サーバ情報を設定できます。

[コマンドによる設定]（IPv4 の場合）

1. **(config)# radius-server host 192.168.10.1 key "AAAA1234"**
(config)# radius-server host 192.168.10.2 key "BBBB1234"

```
(config)# radius-server host 192.168.10.3 key "CCCC1234"
(config)# radius-server host 192.168.10.4 key "DDDD1234"
(config)# radius-server host 192.168.10.5 key "EEEE1234"
(config)# radius-server host 192.168.10.6 key "FFFF1234"
(config)# radius-server host 192.168.10.7 key "GGGG1234"
(config)# radius-server host 192.168.10.8 key "HHHH1234"
```

汎用 RADIUS サーバの IPv4 アドレスと共有鍵を設定します。

2. **(config)# aaa group server radius LOGIN-SEC**
   RADIUS サーバグループ名を設定し，RADIUS サーバグループコンフィグレーションモードへ移行します。

3. **(config-group)# server 192.168.10.1**
   (config-group)# server 192.168.10.2
   (config-group)# server 192.168.10.7
   (config-group)# server 192.168.10.8
   (config-group)# exit
   コンフィグレーションコマンド radius-server host で設定した汎用 RADIUS サーバのなかから，グループで使用するサーバのアドレスを設定します。
   本例では，認証用ポート番号とアカウンティング用ポート番号を省略しているので，認証用ポート番号は 1812，アカウンティング用ポート番号は 1813 で動作します。

［コマンドによる設定］（IPv6 の場合）

1. **(config)# radius-server host 3ffe:501:811:ff03::c7c0 key "AAAA1234"**
   (config)# radius-server host 3ffe:501:811:ff03::c7c1 key "BBBB1234"
   (config)# radius-server host 3ffe:501:811:ff03::c7d0 key "CCCC1234"
   (config)# radius-server host 3ffe:501:811:ff03::c7d1 key "DDDD1234"
   (config)# radius-server host 3ffe:501:811:ff03::c7e0 key "EEEE1234"
   (config)# radius-server host 3ffe:501:811:ff03::c7e1 key "FFFF1234"
   (config)# radius-server host 3ffe:501:811:ff03::c7f0 key "GGGG1234"
   (config)# radius-server host 3ffe:501:811:ff03::c7f1 key "HHHH1234"
   汎用 RADIUS サーバの IPv6 アドレスと共有鍵を設定します。

2. **(config)# aaa group server radius LOGIN-SEC-IPv6**
   RADIUS サーバグループ名を設定し，RADIUS サーバグループコンフィグレーションモードへ移行します。

3. **(config-group)# server 3ffe:501:811:ff03::c7c1**
   (config-group)# server 3ffe:501:811:ff03::c7d1
   (config-group)# server 3ffe:501:811:ff03::c7e1
   (config-group)# server 3ffe:501:811:ff03::c7f1
   (config-group)# exit
   コンフィグレーションコマンド radius-server host で設定した汎用 RADIUS サーバのなかから，グループで使用するサーバのアドレスを設定します。
   本例では，認証用ポート番号とアカウンティング用ポート番号を省略しているので，認証用ポート番号は 1812，アカウンティング用ポート番号は 1813 で動作します。

［注意事項］

1. コンフィグレーションコマンド aaa group server radius で設定するグループ名は，先頭を大文字で設定することを推奨します。
2. コンフィグレーションコマンド server の設定は，下記条件をすべて満たしているときに有効です。
   - コンフィグレーションコマンド radius-server host と同値であること（IP アドレス，認証用ポート番号，アカウンティング用ポート番号）
   - server コマンドと同値の radius-server host の設定が有効であること（key パラメータ指定有，または radius-server key 設定有）

7.4 RADIUS のオペレーション

7.4.1 運用コマンド一覧

RADIUS に関する運用コマンド一覧を次の表に示します。

表 7-6 運用コマンド一覧

コマンド名	説明
show radius-server	本装置に設定した有効な RADIUS サーバ情報を表示します。
clear radius-server	認証要求先 RADIUS サーバを，最初に設定した RADIUS サーバにします。
show radius-server statistics	本装置に設定した有効な RADIUS サーバの統計情報を表示します。
clear radius-server statistics	本装置に設定した有効な RADIUS サーバの統計情報をクリアします。

7.4.2 有効 RADIUS サーバ情報の表示

(1) 有効 RADIUS サーバの表示

運用コマンド show radius-server で，本装置に設定されている RADIUS サーバ情報を表示します。全 RADIUS サーバ使用不可のときは「* hold down」を表示します。

図 7-11 show radius-server の実行結果（有効 RADIUS サーバで動作中）

```
> show radius-server

Date 20XX/06/01 09:45:52 UTC
 <common>
   [Authentication]
    * IP address: 192.168.100.254
         Port:  1812  Timeout:  5  Retry:  3  Remain:    -
      IP address: 2001::fe
         Port:  1812  Timeout:  5  Retry:  3  Remain:    -
   [Accounting]
    * IP address: 192.168.100.254
         Port:  1813  Timeout:  5  Retry:  3  Remain:    -
      IP address: 2001::fe
         Port:  1813  Timeout:  5  Retry:  3  Remain:    -
 <dot1x>
   [Authentication]
    * IP address: 2001::fe
         Port:  1812  Timeout:  5  Retry:  3  Remain:    -
      IP address: 192.168.100.254
         Port:  1812  Timeout:  5  Retry:  3  Remain:    -
   [Accounting]
    * IP address: 2001::fe
         Port:  1813  Timeout:  5  Retry:  3  Remain:    -
      IP address: 192.168.100.254
         Port:  1813  Timeout:  5  Retry:  3  Remain:    -
 <mac-auth>
   [Authentication]
      IP address: 192.168.101.254
         Port:  1812  Timeout:  5  Retry:  3  Remain:    -
      IP address: 2000::fe
         Port:  1812  Timeout:  5  Retry:  3  Remain:    -
    * hold down                                        591
   [Accounting]
    * IP address: 192.168.101.254
         Port:  1813  Timeout:  5  Retry:  3  Remain:    -
      IP address: 2000::fe
         Port:  1813  Timeout:  5  Retry:  3  Remain:    -
 <web-auth>
```

```
   [Authentication]
    * IP address: 192.168.100.254
         Port:  1812  Timeout:  5  Retry:  3  Remain:    -
      IP address: 2001::fe
         Port:  1812  Timeout:  5  Retry:  3  Remain:    -
   [Accounting]
    * IP address: 192.168.100.254
         Port:  1813  Timeout:  5  Retry:  3  Remain:    -
      IP address: 2001::fe
         Port:  1813  Timeout:  5  Retry:  3  Remain:    -
 <Group1>
   [Authentication]
    * IP address: 192.168.100.254
         Port:  1812  Timeout:  5  Retry:  3  Remain:    -
      IP address: 2001::fe
         Port:  1812  Timeout:  5  Retry:  3  Remain:    -

>
```

「*」は現在使用中の RADIUS サーバの IP アドレスを示します。

（2） 有効 RADIUS サーバの統計情報表示

本装置に設定されている有効 RADIUS サーバの統計情報を表示します。

- 運用コマンド show radius-server statistics summary でサマリ情報を表示します。
- 運用コマンド show radius-server statistics で統計情報を表示します。

図 7-12　show radius-server statistics summary の実行結果

```
> show radius-server statistics summary

Date 20XX/06/01 09:46:02 UTC
192.168.100.254 [Tx]Timeout: 0 [Rx]Accept/Reject: 1/1
192.168.101.254 [Tx]Timeout: 4 [Rx]Accept/Reject: 0/0
2000::fe [Tx]Timeout: 4 [Rx]Accept/Reject: 0/0
2001::fe [Tx]Timeout: 0 [Rx]Accept/Reject: 1/0

>
```

図 7-13　show radius-server statistics の実行結果

```
> show radius-server statistics

Date 20XX/06/01 09:45:57 UTC
  IP address: 192.168.100.254
   [Authentication]     Current Request:          0
    [Tx] Request  :           2  Error  :          0
         Retry    :           0  Timeout:          0
    [Rx] Accept   :           1  Reject :          1  Challenge  :          0
         Malformed:           0  BadAuth:          0  UnknownType:          0
   [Accounting]         Current Request:          0
    [Tx] Request  :           0  Error  :          0
         Retry    :           0  Timeout:          0
    [Rx] Responses:           0
         Malformed:           0  BadAuth:          0  UnknownType:          0
  IP address: 192.168.101.254
   [Authentication]     Current Request:          0
    [Tx] Request  :           1  Error  :          0
         Retry    :           3  Timeout:          4
    [Rx] Accept   :           0  Reject :          0  Challenge  :          0
         Malformed:           0  BadAuth:          0  UnknownType:          0
   [Accounting]         Current Request:          0
    [Tx] Request  :           0  Error  :          0
         Retry    :           0  Timeout:          0
    [Rx] Responses:           0
         Malformed:           0  BadAuth:          0  UnknownType:          0
  IP address: 2000::fe
   [Authentication]     Current Request:          0
    [Tx] Request  :           1  Error  :          0
         Retry    :           3  Timeout:          4
```

```
    [Rx] Accept   :          0  Reject :          0  Challenge  :          0
         Malformed:          0  BadAuth:          0  UnknownType:          0
   [Accounting]         Current Request:          0
    [Tx] Request  :          0  Error  :          0
         Retry    :          0  Timeout:          0
    [Rx] Responses:          0
         Malformed:          0  BadAuth:          0  UnknownType:          0
  IP address: 2001::fe
   [Authentication]     Current Request:          0
    [Tx] Request  :          2  Error  :          0
         Retry    :          0  Timeout:          0
    [Rx] Accept   :          1  Reject :          0  Challenge  :          1
         Malformed:          0  BadAuth:          0  UnknownType:          0
   [Accounting]         Current Request:          0
    [Tx] Request  :          0  Error  :          0
         Retry    :          0  Timeout:          0
    [Rx] Responses:          0
         Malformed:          0  BadAuth:          0  UnknownType:          0

>
```

8 時刻の設定と NTP

この章では，時刻の設定と NTP について説明します。

8.1 時刻の設定と確認

8.1.1 サポート仕様

時刻は，本装置の初期導入時に設定してください。時刻は，本装置のログ情報や各種ファイルの作成時刻などに付与される情報です。運用開始時には正確な時刻を本装置に設定してください。運用コマンド set clock で時刻を設定できます。

また，このほかに，NTP プロトコルを使用して，ネットワーク上の NTP サーバと時刻の同期を行えます。

本装置でサポートしている NTP クライアント機能は下記のとおりです。

表 8-1 本装置でサポートする NTP クライアント機能

機能	内容
Unicast モード	本装置から NTP サーバに対して，定期的に時刻を取得するモード
Multicast モード	未サポート
Broadcast モード	NTP サーバから Broadcast で送付される時刻を取得するモード
手動時刻取得機能	運用コマンド set clock ntp により NTP サーバから時刻を取得（Unicast モード）
配信元制限機能	未サポート
ホスト名指定（DNS 使用）機能	未サポート
認証機能	未サポート
時刻補正機能	未サポート

定期時刻取得設定が有効な場合（コンフィグレーションで設定している場合），装置起動時に NTP サーバへの時刻取得を実施します。

各モードは同時設定可能ですが，有効となるモードは１つだけです。また，手動時刻取得は，下記に関係なく実施可能です。

表 8-2 同時設定時の有効モード（○：設定あり，×：設定なし）

Unicast	Broadcast	有効モード
○	×	Unicast
○	○	Unicast
×	○	Broadcast

（1） 指定した NTP サーバから定期時刻取得（Unicast モード）

時刻情報を要求する NTP サーバアドレスを設定することにより，NTP サーバに対して定期的に時刻情報を要求し，本装置内部の時計を更新します。（NTP サーバアドレス要求発行間隔は，コンフィグレーションで設定できます。）

NTP サーバアドレスは最大２個登録でき，最初に登録されたアドレスをプライマリ，後から登録されたアドレスをセカンダリと呼びます。プライマリの NTP サーバアドレスに対して時刻取得に失敗した場合は，セカンダリの NTP サーバアドレスに対して時刻情報を要求します。

図 8-1 Unicast モードによる時刻情報取得図（プライマリ設定時）

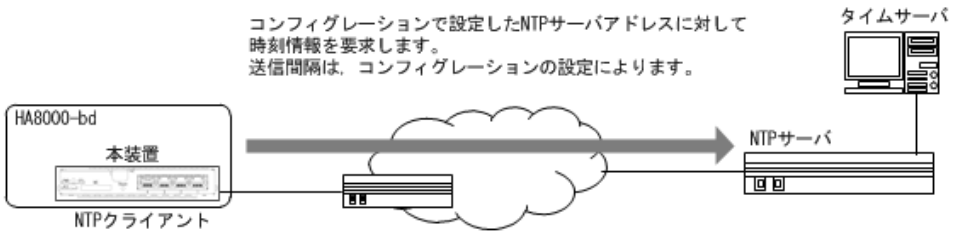
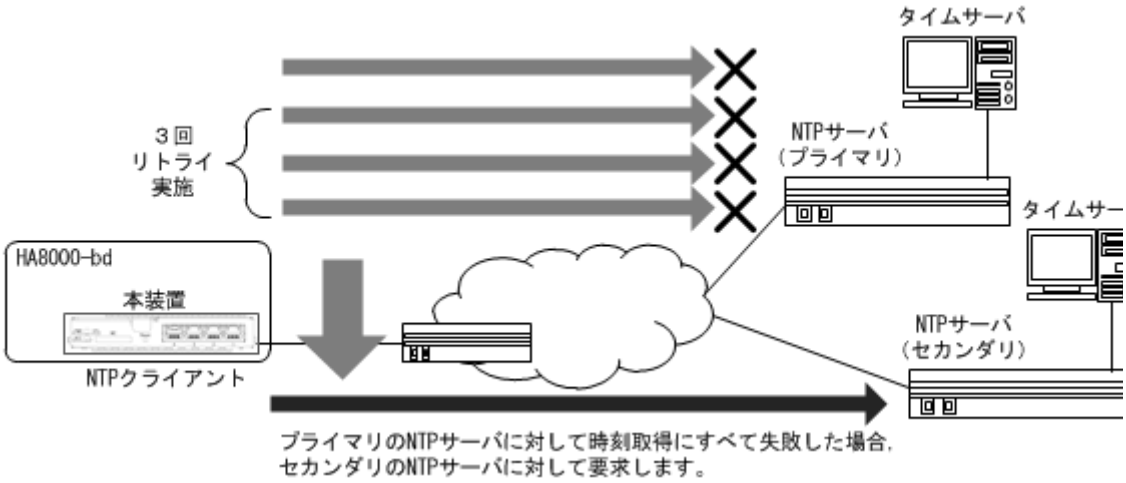


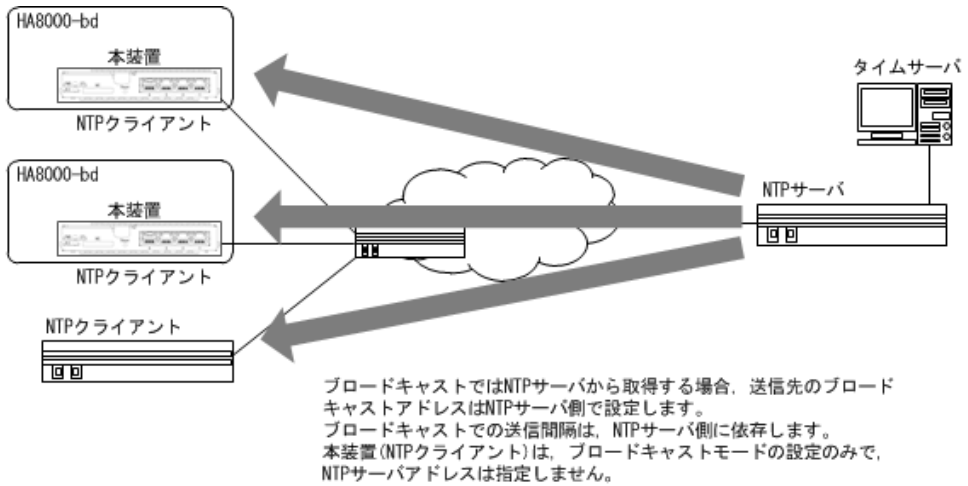
図 8-2 Unicast モードによる時刻情報取得図（プライマリ／セカンダリ設定時）



（2） ブロードキャストで取得（Broadcast モード）

ブロードキャストモードにより，NTP サーバからのブロードキャスト時刻配信を受信し，本装置内部の時計を更新します。

図 8-3 Broadcast モードによる時刻情報取得図



（3） 手動取得

運用コマンドで NTP サーバアドレスを指定して NTP サーバに対して時刻情報を要求し，本装置内部の時計を更新します。また，NTP サーバアドレスの指定を省略した場合は，コンフィグレーションで設定されている定期時刻更新の NTP サーバアドレス情報を使用します。

8.1.2　時刻変更に関する注意事項

本装置で収集している統計情報の CPU 使用率は，下記操作で 0 クリアされます。

- 装置の再起動時
- コンフィグレーションコマンド clock timezone でタイムゾーンを変更した時
- 運用コマンド set clock，または NTP クライアントで時刻を変更した時（秒単位表示データだけクリア）

8.2 コンフィグレーション

8.2.1 コンフィグレーションコマンド

時刻設定および NTP に関するコンフィグレーションコマンド一覧を次の表に示します。

表 8-3 コンフィグレーションコマンド一覧

コマンド名	説明
clock timezone	タイムゾーンを設定します。
ntp broadcast client	NTP サーバからブロードキャストで送信される時刻情報を受け付ける設定を行います。
ntp interval	NTP サーバから定期的に時刻情報を取得する実行間隔を設定します。
ntp server	時刻情報を取得する NTP サーバアドレスを設定します。

8.2.2 システムクロックの設定

［設定のポイント］

日本時間として時刻を設定する場合は，あらかじめコンフィグレーションコマンド clock timezone でタイムゾーンに JST，UTC からのオフセットを +9 に設定する必要があります。

［コマンドによる設定］

1. **(config)# clock timezone JST +9**
   日本時間として，タイムゾーンに JST，UTC からのオフセットを +9 に設定します。
2. **(config)# exit**
   # copy running-config startup-config
   Do you wish to copy from running-config to startup-config? (y/n): y
   コンフィグレーションモードから装置管理者モードに移行し，保存します。
3. **# set clock** 1406021530
   Mon Jun 02 15:30:17 JST 2014
   #
   2014 年 6 月 2 日 15 時 30 分に時刻を設定します。

8.2.3 NTP サーバから定期的に時刻情報を取得する

NTP クライアント機能を用いて，NTP サーバから定期的に時刻情報を取得します。

［設定のポイント］

時刻情報を要求する NTP サーバアドレスを設定します。要求実行間隔は，コンフィグレーションコマンド ntp interval で設定してください。

［コマンドによる設定］

1. **(config)# ntp server 192.168.1.100**
   時刻情報を要求する NTP サーバアドレスを設定します。
2. **(config)# ntp interval 7200**
   NTP サーバへ時刻情報を要求する実行間隔を秒単位で設定します。（コンフィグレーションコマンド ntp interval 未設定の場合は，デフォルト 3600 秒（1 時間）ごとに要求を実行します。）

8.3 オペレーション

8.3.1 運用コマンド一覧

時刻設定および NTP に関する運用コマンド一覧を次の表に示します。

表 8-4 運用コマンド一覧

コマンド名	説明
set clock	日付，時刻を表示，設定します。
set clock ntp	NTP サーバから手動で時刻情報を取得します。
show clock	現在設定されている日付，時刻を表示します。
show ntp-client	NTP クライアント情報を表示します。

8.3.2 時刻の確認

本装置に設定されている時刻情報は，運用コマンド show clock で確認できます。次の図に例を示します。

図 8-4 時刻の確認

```
> show clock
Mon Jun 02 15:30:24 JST 2014
>
```

8.3.3 NTP クライアント情報の表示

NTP サーバから時刻情報を取得している場合は，運用コマンド show ntp-client で NTP クライアント情報を表示できます。次の図に例を示します。

図 8-5 NTP クライアント情報の表示

```
> show ntp-client

Date 20XX/06/03 19:52:48 UTC
 Last NTP Status
  NTP-Server : 192.1.0.254, Source-Address : ---
  Mode : Unicast, Lapsed time : 104(s), Offset : 1(s)

 Activate NTP Client
  NTP-Server : 192.1.0.254, Source-Address : ---
  Mode : Unicast, Interval : 120(s)

 NTP Execute History(Max 10 entry)
  NTP-Server      Source-Address  Mode      Set-NTP-Time          Status
  192.1.0.254     ---             Unicast   20XX/06/03 19:51:05        1
  192.1.0.254     ---             Unicast   20XX/06/03 19:49:05        1
  192.1.0.254     ---             Unicast   20XX/06/03 19:47:05        1
  192.1.0.254     ---             Unicast   20XX/06/03 19:45:05        1
  192.1.0.254     ---             Unicast   20XX/06/03 19:43:05        1
  192.1.0.254     ---             Unicast   20XX/06/03 19:41:05        1
  192.1.0.254     ---             Unicast   20XX/06/03 19:39:05        1
  192.1.0.254     ---             Command   20XX/06/03 19:38:27       -2
  192.2.0.254     ---             Unicast   20XX/06/03 19:37:30  Timeout
  192.1.0.254     ---             Unicast   20XX/06/03 19:37:18  Timeout

>
```

9 ホスト名と DNS

この章では，ホスト名と DNS の解説と操作方法について説明します。

9.1 解説

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設定できます。設定したホスト名情報は，運用コマンド telnet，ftp，tftp などでネットワーク上のほかの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設定できます。

- コンフィグレーションコマンド ip host ／ ipv6 host で個別に指定する方法
- DNS リゾルバ機能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 ip host ／ ipv6 host を使用して設定する場合は，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設定する必要があります。DNS リゾルバを使用する場合は，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 アドレスを設定する必要がなくなります。

コンフィグレーションコマンド ip host ／ ipv6 host と DNS リゾルバ機能の両方が設定されている場合，ip host ／ ipv6 host で設定されているホスト名が優先されます。コンフィグレーションコマンド ip host ／ ipv6 host または DNS リゾルバ機能を使用して，IPv4 と IPv6 で同一のホスト名を設定している場合，IPv4 が優先されます。

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。

9.2 コンフィグレーション

9.2.1 コンフィグレーションコマンド

ホスト名・DNS に関するコンフィグレーションコマンド一覧を次の表に示します。

表 9-1 コンフィグレーションコマンド一覧

コマンド名	説明
ip domain lookup	no ip domain lookup 設定時，DNS リゾルバ機能が無効になります。
ip domain name	DNS リゾルバで使用するドメイン名を設定します。
ip domain reverse-lookup	no ip domain reverse-lookup 設定時，DNS リゾルバ機能の逆引き機能が無効になります。
ip host	IPv4 アドレスに付与するホスト名情報を設定します。
ip name-server	DNS リゾルバが参照するネームサーバを設定します。
ipv6 host	IPv6 アドレスに付与するホスト名情報を設定します。

9.2.2 ホスト名の設定

（1） IPv4 アドレスに付与するホスト名の設定

［設定のポイント］

IPv4 アドレスに付与するホスト名を設定します。

［コマンドによる設定］

1. **(config)# ip host WORKPC1 192.168.0.1**
   IPv4 アドレス 192.168.0.1 の装置にホスト名 WORKPC1 を設定します。

（2） IPv6 アドレスに付与するホスト名の設定

［設定のポイント］

IPv6 アドレスに付与するホスト名を設定します。

［コマンドによる設定］

1. **(config)# ipv6 host WORKPC2 3ffe:501:811:ff45::87ff:fec0:3890**
   IPv6 アドレス 3ffe:501:811:ff45::87ff:fec0:3890 の装置にホスト名 WORKPC2 を設定します。

9.2.3 DNS の設定

（1） DNS リゾルバの設定

［設定のポイント］

DNS リゾルバで使用するドメイン名および DNS リゾルバが参照するネームサーバを設定します。
DNS リゾルバ機能はデフォルトで有効なため，ネームサーバが設定された時点から機能します。

［コマンドによる設定］

1. **(config)# ip domain name domainserver.example.com**
   ドメイン名を domainserver.example.com に設定します。

2. **(config)# ip name-server 192.168.0.1**
   ネームサーバを 192.168.0.1 に設定します。

(2) DNS リゾルバ機能の無効化

[設定のポイント]
DNS リゾルバ機能を無効にします。

[コマンドによる設定]

1. **(config)# no ip domain lookup**
   DNS リゾルバ機能を無効にします。

10 装置の管理

この章では，本装置を導入した際，および本装置を管理する上で必要な作業について説明します。

10.1 装置の状態確認，および運用形態に関する設定

10.1.1 コンフィグレーション・運用コマンド一覧

装置を管理する上で必要なコンフィグレーションコマンドおよび運用コマンド一覧を次の表に示します。

表 10-1 コンフィグレーションコマンド一覧

コマンド名	説明
system l2-table mode	レイヤ 2 ハードウェアテーブルの検索方式を設定します。
system memory-soft-error	Switch processor 内メモリのソフトエラー発生時にログメッセージの出力を設定します。
system recovery	no system recovery コマンドを設定すると，装置の障害が発生したときに，本装置を再起動しないで障害状態のままにします。

表 10-2 運用コマンド一覧（ソフトウェアバージョンと装置状態の確認）

コマンド名	説明
show version	本装置に組み込まれているソフトウェアや実装されているボードの情報を表示します。
show system	本装置の運用状態を表示します。
show environment	装置の温度の状態と累積稼働時間を表示します。
reload	装置を再起動します。
show tech-support	テクニカルサポートで必要となるハードウェアおよびソフトウェアの状態を示す情報を採取します。

表 10-3 運用コマンド一覧（MC および RAMDISK の確認）

コマンド名	説明
show mc	MC の形式と使用状態を表示します。
show mc-file	MC 内のファイル名およびファイルサイズを表示します。
show ramdisk	RAMDISK の形式と使用状態を表示します。
show ramdisk-file	RAMDISK 内のファイル名およびファイルサイズを表示します。
format flash	内蔵フラッシュメモリのファイルシステムを初期化します。
format mc	MC を本装置用のフォーマットで初期化します。

表 10-4 運用コマンド一覧（ログ情報の確認）

コマンド名	説明
show logging	本装置で収集しているログを表示します。
clear logging	本装置で収集しているログを消去します。
show logging console	set logging console コマンドで設定された内容を表示します。
set logging console	システムメッセージの画面表示をイベントレベル単位で制御します。
show critical-logging	装置障害ログの詳細情報をログレコード単位で表示します。
show critical-logging summary	装置障害ログをリファレンスコードで一覧表示します。
clear critical-logging	本装置で収集している装置障害ログをクリアします。

表 10-5 運用コマンド一覧（リソース情報の確認）

コマンド名	説明
show cpu	CPU 使用率を表示します。
show memory summary	装置の物理メモリの実装量・使用量・空き容量を表示します。

10.1.2 ソフトウェアバージョンの確認

運用コマンド show version で本装置に組み込まれているソフトウェアの情報を確認できます。次の図に例を示します。

図 10-1 ソフトウェア情報の確認

```
> show version

Date 20XX/06/06 17:38:02 UTC
Model: GR-BEX310GL
S/W: OS-L2BS-A Ver. x.x (Build:yy)
H/W: GR-BEX310GL [SSSSSSSSSSSSSSSSSSSSS:R]

>
```

10.1.3 装置の状態確認

運用コマンド show system で装置の動作状態や搭載メモリ量などを確認できます。次の図に例を示します。

図 10-2 装置の状態確認

```
> show system

Date 20XX/06/08 03:06:44 UTC
System: GR-BEX310GL Ver. x.x (Build:yy)
    Name            : -
    Contact         : -
    Locate          : -
    Machine ID      : 0000.8762.3f8e
    Boot Date       : 20XXX/06/08 02:58:12
    Elapsed time    : 0 days 00:08:32
    LED
    PWR/ST1 LED     : Green

Environment
    Temperature  : normal
    Accumulated running time
       total     : 69 days and 6 hours
       critical  : 0 days and 0 hours

File System
    < RAMDISK information >
       used       168,960 byte
       free    31,288,320 byte
       total   31,457,280 byte
    < RAMDISK files >
    File Date               Size Name
    20XX/06/08 03:06       1,024 Config_File/
    20XX/06/08 03:02       4,648 Test_Config.txt
    20XX/06/08 03:06       6,196 Config_File/12Floor_Config.txt
    20XX/06/08 03:02      14,964 Config_File/11Floor_Config.txt
    < MC information >
    MC : enable
    Manufacture ID : 00000003
       used      9,108,992 byte
       free    116,801,536 byte
       total   125,910,528 byte
    < MC files >
```

```
    File Date               Size Name
    20XX/06/06 18:12   8,990,720 K.IMG
    20XX/06/08 03:05      16,384 Config_File/
    20XX/05/20 12:08       4,648 Test_Config.txt
    20XX/05/04 10:30       6,196 Config_File/12Floor_Config.txt
    20XX/06/05 20:17      14,964 Config_File/11Floor_Config.txt

Device Resources
    IPv4 Routing Entry(static)    :     5(max entry=128)
    IPv4 Routing Entry(connected) :    22(max entry=128)
    IP Interface Entry            :     4(max entry=128)
    IPv4 ARP Entry                :    11(max entry=2048)
    IPv6 NDP Entry                :     7(max entry=256)
    MAC-address Table Entry       :    35(max entry=32768)

    System Layer2 Table Mode  : 1
    Flow detection mode : layer2-2
      Used resources for filter(Used/Max)
                                  MAC      IPv4
        Port 0/1-24         :       -     2/256
        VLAN                :       -     2/256
      Used resources for QoS(Used/Max)
                                  MAC      IPv4
        Port 0/1-24         :       -     1/128
        VLAN                :       -     1/128
      Used resources for TCP/UDP port detection pattern
        Resources(Used/Max):  0/16
    Flow detection out mode: layer2-2-out
      Used resources for filter outbound(Used/Max)
                                  MAC      IPv4
        Port 0/1-24         :       -     2/128
        VLAN                :       -     2/128

>
```

運用コマンド show environment で温度の状態，累積稼働時間を確認できます。

図 10-3　装置の環境状態の確認

```
> show environment

Date 20XX/06/07 18:12:36 UTC
Temperature environment
    Main          : Sensor(1) = 30  degrees C
                    Sensor(2) = 45  degrees C
    Warning level : Sensor(1) = normal
                    Sensor(2) = normal

    Accumulated running time
       total     : 69 days and 21 hours
       critical  : 0 days and 0 hours

>
```

10.1.4　運用メッセージの出力抑止と確認

装置の状態が変化した場合，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コンソールやリモート運用端末に表示します。例えば，通信可能状態になった場合は通信可能状態になった運用メッセージを，通信停止状態になった場合は通信停止状態になった運用メッセージを表示します。

運用端末に出力される運用メッセージは，運用コマンド set logging console を使用することでイベントレベル単位で出力を抑止できます。また，その抑止内容については，運用コマンド show logging console で確認できます。イベントレベルが E5 以下の運用メッセージの運用端末への出力抑止の設定例を次に示します。

図 10-4　運用メッセージの出力抑止の設定例

```
> set logging console disable E5
> show logging console
  System message mode : E5
>
```

注意

多数の運用メッセージが連続して発生した際，コンソールやリモート運用端末上に「WARNING!! There are too many messages to output.」メッセージを表示する場合があります。これは表示できなかった運用メッセージがあることを示していますので，運用コマンド show logging で確認してください。

10.1.5　運用ログ情報の確認

運用メッセージは運用端末に出力するほか，運用ログとして装置内に保存します。この情報で装置の運用状態や障害の発生を管理できます。

運用ログは装置運用中に発生した事象（イベント）を発生順に記録したログ情報で，運用メッセージと同様の内容が格納されます。運用ログとして格納する情報には次に示すものがあります。

- ユーザのコマンド操作と応答メッセージ
- 運用メッセージ

種別ログは装置内で発生した障害や警告についての運用ログ情報をメッセージ ID ごとに分類した上で，同事象が最初に発生した日時および最後に発生した日時と累積回数をまとめた情報です。

これらのログは装置内にテキスト形式で格納されており，運用コマンド show logging で確認できます。

10.2 装置情報のバックアップ・リストア

装置障害または交換時は，装置情報のバックアップファイルからリストアにより復旧します。

次に示す「10.2.2 バックアップおよびリストア実行時の対象情報」を実施してください。すべてを手作業で復旧することもできますが，取り扱う情報が複数にわたるため管理が複雑になり，また完全に復旧できないため，お勧めしません。

10.2.1 運用コマンド一覧

バックアップ・リストアに使用する運用コマンド一覧を次の表に示します。

表 10-6 運用コマンド一覧

コマンド名	説明
backup	稼働中のソフトウェアおよび装置の情報を MC，RAMDISK，またはリモートの ftp サーバに保存します。
restore	MC，RAMDISK，およびリモートの ftp サーバに保存している装置情報を本装置に復元します。

10.2.2 バックアップおよびリストア実行時の対象情報

(1) 情報のバックアップ

装置が正常に稼働しているときに，運用コマンド backup を用いてバックアップファイルを作成しておきます。運用コマンド backup は，装置の稼働に必要な次の情報を一つのファイルにまとめて MC，RAMDISK，またはリモートの ftp サーバに保存します。

これらの情報を更新したときは，バックアップファイルの作成をお勧めします。

表 10-7 バックアップファイルに保存される装置情報

装置情報種別	備考
稼働中のソフトウェア	
スタートアップコンフィグレーションファイル	
ログイン認証ユーザ ID ／ログイン認証パスワード	運用コマンド adduser 運用コマンド rmuser 運用コマンド password
CLI 環境情報	運用コマンド set exec-timeout 運用コマンド set terminal pager
装置管理者モードパスワード	運用コマンド password enable-mode
Web 認証データベース	内蔵 Web 認証 DB
Web 認証用に登録された認証画面ファイル （登録された認証画面カスタムファイルセット）	基本 Web 認証画面カスタムファイルセット 個別 Web 認証画面カスタムファイルセット
Web 認証証明書ファイル	
MAC 認証データベース	内蔵 MAC 認証 DB

運用コマンド backup では次に示す情報は保存されないので注意してください。

- 運用コマンド show logging で表示される運用ログなど

（2） 情報のリストア

運用コマンド backup で作成したバックアップファイルから情報を復旧する場合，運用コマンド restore を用います。

運用コマンド restore を実行すると，バックアップファイル内に保存されているソフトウェアアップデート用ファイルを用いて装置のソフトウェアをアップデートします。このアップデート作業後，装置は自動的に再起動します。再起動後，復旧された環境になります。

なお，運用コマンド restore を実行するときは，次の点に注意してください。

1. 運用コマンド restore で情報を復旧する場合は，リストア対象の装置と同じモデル名称の装置で作成したバックアップファイルを使用してください。
   装置のモデル名称は，運用コマンド show version で表示される Model で確認してください。
2. バックアップファイル作成時のソフトウェアバージョンが，リストア対象の装置に適していることを確認してください。

10.3　障害時の復旧

10.3.1　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 10-8　障害部位と復旧内容

障害部位	装置の対応	復旧内容	影響範囲
メインボード	自動復旧を 6 回／ 1 時間行います。6 回目の復旧後から 1 時間未満で 7 回目の障害が発生すると停止します。 1 時間以上運用すると，自動復旧回数を初期化します。	装置を再起動します。※	装置内の全ポートを介する通信が中断されます。
SW チップ	内蔵メモリのパリティエラー発生時，自動復旧を実施します。復旧後，障害が継続する場合，装置再起動による復旧を実施します。	発生箇所を正常状態に設定します。※	通信に影響があります。
ポート障害	自動復旧を無限回行ないます。	該当ポートの再設定，再初期化を行ないます。	該当するポートを介する通信に影響する場合があります。

（凡例）
　○：自動復旧あり
　－：自動復旧なし

注※
　コンフィグレーションコマンド no system recovery で復旧処理を行わない設定をしている場合には，重度障害（E9 レベルの障害ログ採取時）でも，自動復旧を行いません。

（1） 自動復旧停止状態について

システムリカバリー無効時（no system recovery）は自動復旧は停止状態となり，重度障害（E9 レベルの障害）が発生しても，障害ログ採取後は本装置を再起動しません。この場合は PWR/ST1 LED が赤点灯し，全ポートがリンクダウンして通信停止状態となります。

(a) 自動復旧停止状態中の装置状態情報の採取

自動復旧停止状態となった場合は，コンソール端末から運用コマンド show tech-support で装置状態情報を採取し，本装置を復旧してください。

自動復旧停止状態中の運用コマンド show tech-support の実行では，コンソール画面への表示だけが許可されます。従って，本コマンドの実行では "ramdisk" や "page" オプションを指定しないでください。また，本コマンドの実行でコンソール画面に表示される情報は，端末のキャプチャ機能などを利用して，採取してください。

なお，本装置が自動復旧停止状態中は，下記に注意してください。

- 自動復旧停止状態で，ソフトウェアのアップデートを実施しないでください。本装置を復旧してから，アップデートを実施してください。
- 自動復旧停止状態では，各種コマンドを正常に実行できない場合があります。

(b) 本装置の復旧

本装置の自動復旧停止状態は，下記により復旧します。

- RESET スイッチで，本装置を再起動してください。
- 自動復旧停止状態でソフトウェアがハングアップする状態に陥った場合は，ハードウェアで強制リセットを行い，本装置を再起動します。

11 ソフトウェアの管理

この章では，ソフトウェアのアップデートについて説明します。実際のアップデート手順については，「ソフトウェアアップデートガイド」を参照してください。

11.1　運用コマンド一覧

ソフトウェア管理に関する運用コマンド一覧を次の表に示します。

表 11-1　運用コマンド一覧

コマンド名	説明
ppupdate	MC から RAMDISK にコピーした新しいソフトウェア，または ftp，tftp などでダウンロードした新しいソフトウェアにアップデートします。

11.2　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とは，旧バージョンのソフトウェアから新バージョンのソフトウェアにバージョンアップすることを指します。ソフトウェアのアップデートは，MC から本装置の RAMDISK にアップデートファイルをコピーして運用コマンド ppupdate を実行するか，または PC などのリモート運用端末からアップデートファイルを本装置に転送し運用コマンド ppupdate を実行することで実現します。
アップデート時，装置管理のコンフィグレーションおよびユーザ情報（ログインアカウント，パスワードなど）はそのまま引き継がれます。詳細については，「ソフトウェアアップデートガイド」を参照してください。

ソフトウェアのアップデートの概要を次の図に示します。

図 11-1　ソフトウェアのアップデートの概要 (MC)

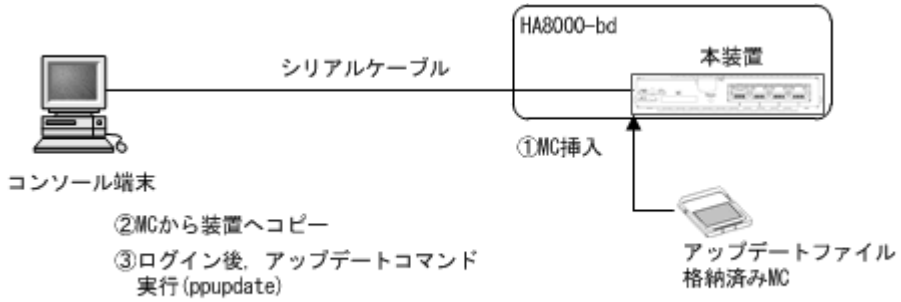
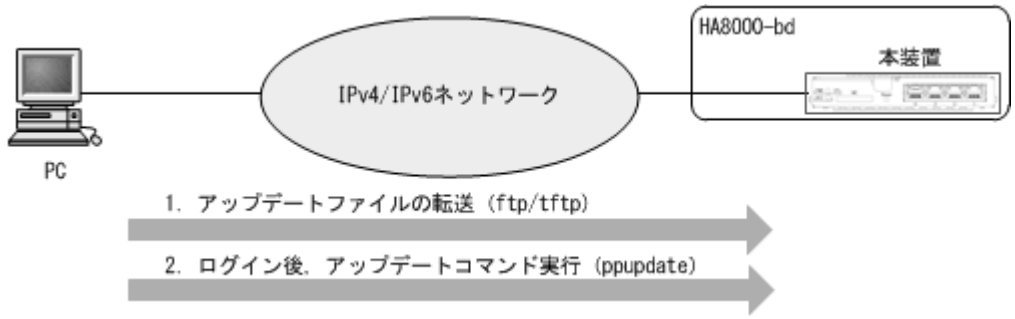


図 11-2　ソフトウェアのアップデートの概要 (ftp/tftp)



12 イーサネット

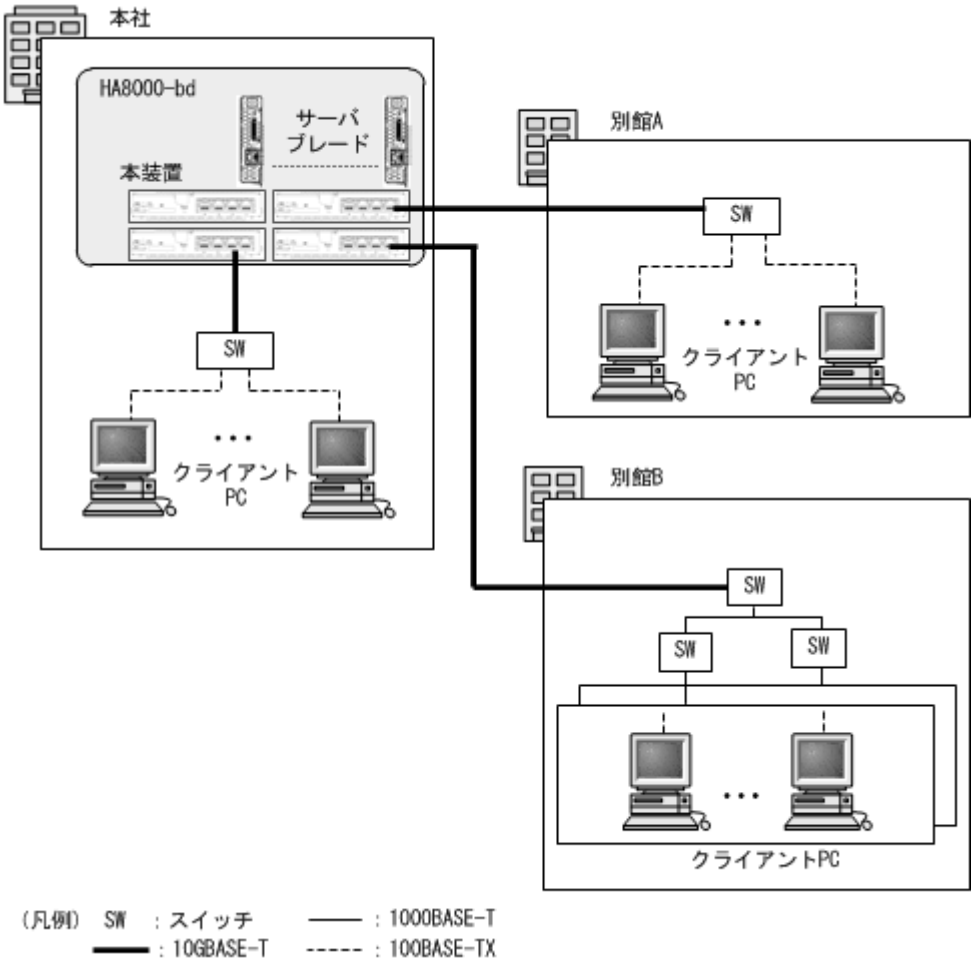
この章では，本装置のイーサネットについて説明します。

12.1　イーサネット共通の解説

12.1.1　ネットワーク構成例

本装置を使用したイーサネット構成例を次の図に示します。

図 12-1　イーサネットの構成例



12.1.2　物理インタフェース

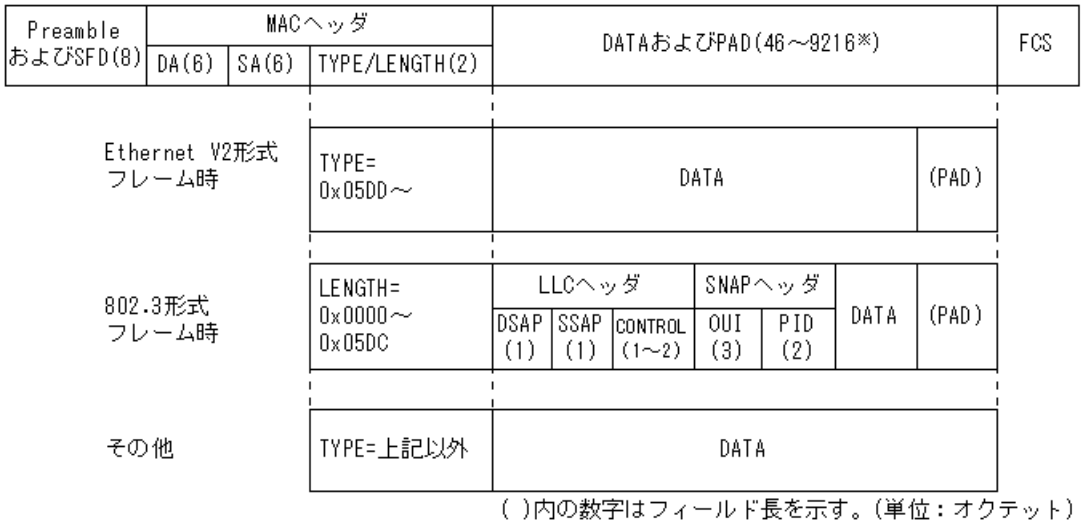
イーサネットには次の 2 種類があります。

- IEEE802.3 に準拠した 10BASE-T ／ 100BASE-TX ／ 1000BASE-T のツイストペアケーブルを使用したインタフェース
- IEEE802.3 に準拠した 1000BASE-T ／ 10GBASE-T ※のツイストペアケーブルを使用したインタフェース
  注※　100BASE-TX は未サポートです。

12.1.3　MAC および LLC 副層制御

フレームフォーマットを次の図に示します。

図 12-2 フレームフォーマット



注※ DATAおよびPADの最大長はEthernetV2形式フレーム時だけ9216。
802.3形式フレームおよびその他の形式のフレームは1500。

(1) MAC 副層フレームフォーマット

(a) Preamble および SFD

64 ビット長の 2 進数で「1010...1011(最初の 62 ビットは '10' を繰り返し，最後の 2 ビットは '11')」のデータです。送信時にフレームの先頭に付加します。この 64 ビットパターンのないフレームは受信できません。

(b) DA および SA

48 ビット形式をサポートします。16 ビット形式およびローカルアドレスはサポートしていません。

(c) TYPE ／ LENGTH

TYPE ／ LENGTH フィールドの扱いを次の表に示します。

表 12-1 TYPE ／ LENGTH フィールドの扱い

TYPE ／ LENGTH 値	本装置での扱い
0x0000 ～ 0x05DC	IEEE802.3 CSMA/CD のフレーム長
0x05DD ～	Ethernet V2.0 のフレームタイプ

(d) FCS

32 ビットの CRC 演算を使用します。

(2) LLC 副層フレームフォーマット

IEEE802.2 の LLC タイプ 1(UI フレームのみ) をサポートしています。Ethernet V2 では LLC 副層はありません。

(a) DSAP

LLC 情報部の宛先のサービスアクセス点を示します。

（b） SSAP

LLC 情報部を発信した特定のサービスアクセス点を示します。

（c） CONTROL

情報転送形式，監視形式，非番号制御形式の三つの形式を示します。

（d） OUI

SNAP 情報部を発信した組織コードフィールドを示します。

（e） PID

SNAP 情報部を発信したイーサネット・タイプ・フィールドを示します。

（3） 受信フレームの廃棄条件

次に示すどれかの条件によって受信したフレームを廃棄します。

- フレーム長がオクテットの整数倍でない
- 受信フレーム長（DA ～ FCS）が 64 オクテット未満，または 1523 オクテット以上
  ただし，ジャンボフレーム選択時は，指定したフレームサイズを超えた場合
- FCS エラー
- 接続インタフェースが半二重の場合は，受信中に衝突が発生したフレーム

（4） パッドの扱い

送信フレーム長が 64 オクテット未満の場合，MAC 副層で FCS の直前にパッドを付加します。パッドの値は不定です。

12.1.4 本装置の MAC アドレス

（1） 装置 MAC アドレス

本装置は，装置を識別するための MAC アドレスを一つ持ちます。この MAC アドレスのことを装置 MAC アドレスと呼びます。装置 MAC アドレスは，スパニングツリーなどのプロトコルの装置識別子として使用します。

（2） 装置 MAC アドレスを使用する機能

装置 MAC アドレスを使用する機能を次の表に示します。

表 12-2 装置 MAC アドレスを使用する機能

機能	用途
VLAN	VLAN インタフェースの MAC アドレス
リンクアグリゲーションの LACP	装置識別子
スパニングツリー	装置識別子
Ring Protocol	装置識別子
LLDP	装置識別子
IEEE802.3ah/UDLD	装置識別子
L2 ループ検知	装置識別子

12.1.5 イーサネットフレームの順序について

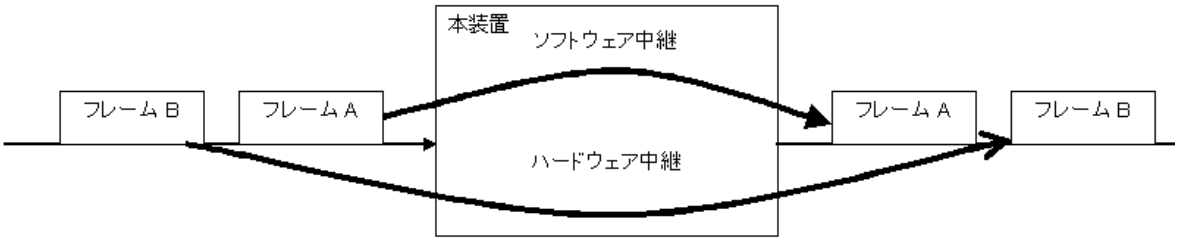
本装置では一部のフレームをソフトウェアで中継しています。そのため中継したフレームの順番が入れ替わる場合があります。また，CoS 値※による優先制御機能が動作した場合も，フレームの順番が入れ替わる場合があります。

注※
CoS 値は，本装置内におけるフレームの優先度を表すインデックス値です。

(1) ソフトウェア中継による中継フレームの順番の入れ替わりについて

本装置でのソフトウェア中継対象フレームは IGMP ／ MLD snooping の一部のフレーム（query 等）が該当します。

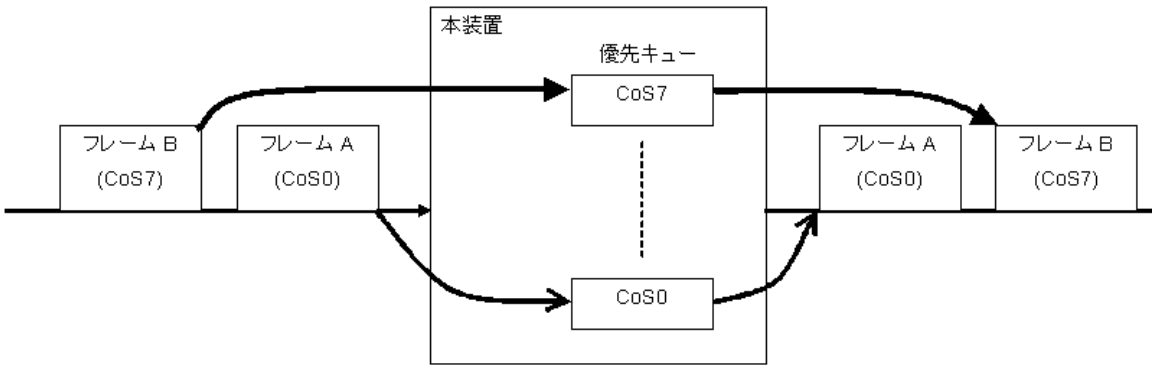
図 12-3 ソフトウェア中継によるフレームの入れ替わり



(2) 優先制御によるフレーム順番の入れ替わりについて

本装置では CoS 値による優先制御がデフォルトで有効となっています。従って CoS 値の異なるフレームを受信すると，フレームの入れ替わりが発生する場合があります。

図 12-4 優先制御によるフレームの入れ替わり



12.2 イーサネット共通のコンフィグレーション

12.2.1 コンフィグレーションコマンド一覧

イーサネット共通のコンフィグレーションコマンド一覧を次の表に示します。

表 12-3 コンフィグレーションコマンド一覧

コマンド名	説明
bandwidth	ポートの帯域幅を設定します。
description	ポートの補足説明を設定します。
duplex	ポートの duplex を設定します。
flowcontrol	ポートのフローコントロールを設定します。
interface gigabitethernet	回線速度が最大 1000Mbit/s の外部装置接続用ポート，およびサーバ接続ポートに関する項目を設定します。
interface tengigabitethernet	最大回線速度が 10Gbit/s の外部装置接続用ポートに関する項目を設定します。
link debounce	リンクダウン検出時間を設定します。
link up-debounce	リンクアップ検出時間を設定します。
mdix auto	ポートの自動 MDIX 機能を設定します。
mtu	ポートの MTU を設定します。
shutdown	ポートをシャットダウンします。
speed	ポートの速度を設定します。
system mtu	全ポート共通の MTU を設定します。

12.2.2 イーサネットインタフェースのポートの設定

［設定のポイント］

イーサネットのコンフィグレーションでは，インタフェースのポート番号を指定し，config-if モードに遷移して情報を設定します。

［コマンドによる設定］

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

   10 ギガビットイーサネットインタフェースのポート 0/1 への設定を指定します。

12.2.3 複数ポートの一括設定

［設定のポイント］

イーサネットのコンフィグレーションでは，複数のポートに同じ情報を設定することがあります。このような場合，複数のポートを range 指定することで，情報を一括して設定できます。

［コマンドによる設定］

1. **(config)# interface range tengigabitethernet 0/1, gigabitethernet 0/5-24**

   10 ギガビットイーサネットインタフェースのポート 0/1，1 ギガビットインタフェース 0/5 から 0/24 への設定を指定します。

2. **(config-if-range)# ＊＊＊＊＊**
   (config-if-range)# exit
   複数のポートに同じコンフィグレーションを一括して設定します。

12.2.4 イーサネットのシャットダウン

［設定のポイント］

イーサネットのコンフィグレーションでは，複数のコマンドでコンフィグレーションを設定することがあります。そのとき，コンフィグレーションの設定が完了していない状態でポートがリンクアップ状態になると期待した通信ができません。従って，最初にポートをシャットダウンしてから，コンフィグレーションの設定が完了したあとにポートのシャットダウンを解除することを推奨します。なお，使用しないポートはシャットダウンしておいてください。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/3**
   ポート 0/3 の設定を指定します。

2. **(config-if)# shutdown**
   ポートをシャットダウンします。

3. **(config-if)# ＊＊＊＊＊**
   ポートに対するコンフィグレーションを設定します。

4. **(config-if)# no shutdown**
   (config-if)# exit
   ポートのシャットダウンを解除します。

［関連事項］

運用コマンド inactivate でポートの運用を停止することもできます。ただし，運用コマンド inactivate で inactive 状態とした場合は，装置を再起動するとポートが active 状態になります。ポートをシャットダウンした場合は，装置を再起動してもポートは disable 状態のままとなり，active 状態にするためにはコンフィグレーションコマンドで no shutdown を設定してシャットダウンを解除する必要があります。（コンフィグレーション設定後は，save コマンドで保存しておいてください。）

12.2.5 ジャンボフレームの設定

イーサネットインタフェースの MTU は規格上 1500 オクテットです。本装置は，ジャンボフレームを使用して MTU を拡張し，一度に転送するデータ量を大きくすることでスループットを向上できます。

ジャンボフレームで使用するポートでは MTU を設定します。本装置は，設定された MTU に VLAN Tag が一つ付いているフレームを送受信できるようになります。

ポートの MTU の設定値は，ネットワークおよび相手装置と合わせて決定します。

VLAN トンネリングなどで，VLAN Tag が二つ付く場合は，そのフレームを送受信できるように，MTU の値に 4 を加えた値を設定します。

(1) ポートの MTU の設定

[設定のポイント]

ポート 0/3 の MTU を 8192 オクテットに設定します。この設定によって，VLAN Tag の付かないフレームであれば 8206 オクテット，VLAN Tag の付いたフレームであれば 8210 オクテットまでのジャンボフレームを送受信できるようになります。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/3**
   (config-if)# shutdown
   (config-if)# mtu 8192
   ポート 0/3 の MTU を 8192 オクテットに設定します。

2. **(config-if)# no shutdown**
   (config-if)# exit

[注意事項]

コンフィグレーションでポートの MTU を設定していても，10BASE-T または 100BASE-TX 半二重で接続する場合（オートネゴシエーションの結果が 10BASE-T または 100BASE-TX 半二重になった場合も含みます）は，ポートの MTU は 1500 オクテットになります。

(2) 全ポート共通の MTU の設定

[設定のポイント]

本装置の全ポートで MTU を 4096 オクテットに設定します。この設定によって，VLAN Tag の付かないフレームであれば 4110 オクテット，VLAN Tag の付いたフレームであれば 4114 オクテットまでのジャンボフレームを送受信できるようになります。

[コマンドによる設定]

1. **(config)# system mtu 4096**
   装置の全ポートの MTU を 4096 オクテットに設定します。

[注意事項]

コンフィグレーションでポートの MTU を設定していても，10BASE-T または 100BASE-TX 半二重で接続する場合（オートネゴシエーションの結果が 10BASE-T または 100BASE-TX 半二重になった場合も含みます）は，ポートの MTU は 1500 オクテットになります。

12.2.6 リンクダウン検出タイマの設定

リンク障害を検出してからリンクダウンするまでのリンクダウン検出時間が短い場合，相手装置によってはリンクが不安定になることがあります。このような場合，リンクダウン検出タイマを設定することで，リンクが不安定になることを防ぐことができます。

［設定のポイント］

リンクダウン検出時間は，リンクが不安定とならない範囲でできるだけ短い値にします。リンクダウン検出時間を設定しなくてもリンクが不安定とならない場合は，リンクダウン検出時間を設定しないでください。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/3**
   ポート 0/3 の設定を指定します。

2. **(config-if)# link debounce time 5000**
   (config-if)# exit
   リンクダウン検出タイマを 5000 ミリ秒に設定します。

［注意事項］

リンクダウン検出時間を設定すると，リンクが不安定になることを防ぐことができますが，障害が発生した場合にリンクダウンするまでの時間が長くなります。リンク障害を検出してからリンクダウンするまでの時間を短くしたい場合は，リンクダウン検出タイマを設定しないでください。

12.2.7 リンクアップ検出タイマの設定

リンク障害回復を検出してからリンクアップするまでのリンクアップ検出時間が短い場合，相手装置によってはネットワーク状態が不安定になることがあります。このような場合，リンクアップ検出タイマを設定することで，ネットワーク状態が不安定になることを防ぐことができます。

［設定のポイント］

リンクアップ検出時間は，ネットワーク状態が不安定とならない範囲でできるだけ短い値にします。リンクアップ検出時間を設定しなくてもネットワーク状態が不安定とならない場合は，リンクアップ検出時間を設定しないでください。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/3**
   ポート 0/3 の設定を指定します。

2. **(config-if)# link up-debounce time 5000**
   (config-if)# exit
   リンクアップ検出タイマを 5000 ミリ秒に設定します。

［注意事項］

リンクアップ検出タイマを長く設定すると，リンク障害回復から通信できるまでの時間が長くなります。リンク障害回復から通信できるまでの時間を短くしたい場合は，リンクアップ検出タイマを設定しないでください。

12.2.8 フローコントロールの設定

本装置内の受信バッファが枯渇して受信フレームを廃棄することがないようにするためには，ポーズパケットを送信して相手装置に送信規制を要求します。相手装置はポーズパケットを受信して送信規制できる必要があります。

相手装置からのポーズパケットを受信したとき，本装置が送信規制するかどうかは設定に従います。本装置では，オートネゴシエーション時に相手装置とポーズパケットを送受信するかどうかを折衝できます。

［設定のポイント］

フローコントロールの設定内容は，相手装置と矛盾しないように決定してください。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/3**
   (config-if)# shutdown
   (config-if)# flowcontrol send off
   (config-if)# flowcontrol receive off
   相手装置とのポーズパケット送受信を停止します。

2. **(config-if)# no shutdown**
   (config-if)# exit

12.3　イーサネット共通のオペレーション

12.3.1　運用コマンド一覧

イーサネット共通の運用コマンド一覧を次の表に示します。

表 12-4　運用コマンド一覧

コマンド名	説明
show interfaces	イーサネットの情報を表示します。
show port	イーサネットの情報を一覧で表示します。
clear counters	イーサネットの統計情報カウンタをクリアします。
inactivate	active 状態のイーサネットを inactive 状態にします。
activate	inactive 状態のイーサネットを active 状態にします。
test interfaces	回線テストを実行します。
no test interfaces	回線テストを停止し，結果を表示します。

12.3.2　イーサネットの動作状態を確認する

（1）全イーサネットの動作状態を確認する

運用コマンド show port で，本装置に実装している全イーサネットの状態を確認できます。使用するイーサネットの Status の表示が up になっていることを確認します。

運用コマンド show port の実行結果を次の図に示します。

図 12-5 「本装置に実装している全イーサネットの状態」の表示例

```
> show port

DDate 20XX/06/19 15:21:43 UTC
Port Counts: 28
Port  Name           Status  Speed           Duplex     FCtl FrLen  ChGr/Status
 0/1  tengeth0/1     up      10GBASE-T       full(auto) off   9234  -/-
 0/2  tengeth0/2     up      10GBASE-T       full(auto) off   9234  -/-
 0/3  geth0/3        up      1000BASE-T      full(auto) off   9234  -/-
 0/4  geth0/4        up      1000BASE-T      full(auto) off   9234  -/-
 0/5  geth0/5        down    SERDES             -          -        -  -/-
 0/6  geth0/6        down    SERDES             -          -        -  -/-
 0/7  geth0/7        down    SERDES             -          -        -  -/-
  :
  :

>
```

12.4 10BASE-T/100BASE-TX/1000BASE-T の解説

10BASE-T ／ 100BASE-TX ／ 1000BASE-T のツイストペアケーブルを使用したインタフェースについて説明します。

なお，本装置の 10BASE-T ／ 100BASE-TX ／ 1000BASE-T のインタフェースは，ポート 0/3 ～ 0/4 の 2 ポートです。

12.4.1 機能一覧

(1) 接続インタフェース

(a) 10BASE-T ／ 100BASE-TX ／ 1000BASE-T 自動認識（オートネゴシエーション）

10BASE-T ／ 100BASE-TX ／ 1000BASE-T では自動認識機能（オートネゴシエーション）と固定接続機能をサポートしています。

- 自動認識…10BASE-T，100BASE-TX，1000BASE-T（全二重）
- 固定接続…10BASE-T，100BASE-TX

コンフィグレーションでは次のモードを指定できます。接続するネットワークに合わせて設定してください。本装置のデフォルト値は，オートネゴシエーションとなります。

- オートネゴシエーション
- 100BASE-TX 全二重固定
- 100BASE-TX 半二重固定
- 10BASE-T 全二重固定
- 10BASE-T 半二重固定

(b) 10BASE-T ／ 100BASE-TX ／ 1000BASE-T 接続仕様

本装置のコンフィグレーションでの指定値と相手装置の伝送速度および，全二重／半二重モードの接続仕様を次の表に示します。

10BASE-T および 100BASE-TX は，相手装置によってオートネゴシエーションでは接続できない場合がありますので，できるだけ相手装置のインタフェースに合わせた固定設定にしてください。

1000BASE-T は，全二重のオートネゴシエーションだけの接続となります。

表 12-5 伝送速度，全二重／半二重モードごとの接続仕様

接続装置		本装置の設定				
設定	インタフェース	固定				オートネゴシエーション
		10BASE-T 半二重	10BASE-T 全二重	100BASE-TX 半二重	100BASE-TX 全二重	
固定	10BASE-T 半二重	10BASE-T 半二重	×	×	×	10BASE-T 半二重
	10BASE-T 全二重	×	10BASE-T 全二重	×	×	×
	100BASE-TX 半二重	×	×	100BASE-TX 半二重	×	100BASE-TX 半二重
	100BASE-TX 全二重	×	×	×	100BASE-TX 全二重	×
	1000BASE-T 半二重	×	×	×	×	×
	1000BASE-T 全二重	×	×	×	×	×
オートネゴシエーション	10BASE-T 半二重	10BASE-T 半二重	×	×	×	10BASE-T 半二重
	10BASE-T 全二重	×	×	×	×	10BASE-T 全二重
	10BASE-T 全二重および半二重	10BASE-T 半二重	×	×	×	10BASE-T 全二重
	100BASE-TX 半二重	×	×	100BASE-TX 半二重	×	100BASE-TX 半二重
	100BASE-TX 全二重	×	×	×	×	100BASE-TX 全二重
	100BASE-TX 全二重および半二重	×	×	100BASE-TX 半二重	×	100BASE-TX 全二重
	10/100BASE-TX 全二重および半二重	10BASE-T 半二重	×	100BASE-TX 半二重	×	100BASE-TX 全二重
	1000BASE-T 半二重	×	×	×	×	×
	1000BASE-T 全二重	×	×	×	×	1000BASE-T 全二重
	1000BASE-T 全二重および半二重	×	×	×	×	1000BASE-T 全二重
	10/100/1000 BASE-T 全二重および半二重	10BASE-T 半二重	×	100BASE-TX 半二重	×	1000BASE-T 全二重

（凡例） ×：接続できない

（2）オートネゴシエーション

オートネゴシエーションは，伝送速度，全二重／半二重モード認識およびフローコントロールについて，

対向装置間でやりとりを行い，接続動作を決定する機能です。

本装置での接続仕様を，「表 12-5　伝送速度，全二重／半二重モードごとの接続仕様」に示します。また，本装置では，ネゴシエーションで解決できなかった場合，リンク接続されるまで接続動作を繰り返します。（本動作については，「12.4.1　機能一覧（6）ダウンシフト機能」を参照してください。）

（3） フローコントロール

フローコントロールは，装置内の受信バッファ枯渇でフレームを廃棄しないように，相手装置にフレームの送信をポーズパケットによって，一時的に停止指示する機能です。自装置がポーズパケット受信時は，送信規制を行います。この機能は全二重だけサポートします。

本装置では，受信バッファの使用状況を監視し，相手装置の送信規制を行う場合，ポーズパケットを送信します。本装置がポーズパケット受信時は，送信規制を行います。フローコントロールのコンフィグレーションは，送信と受信でそれぞれ設定でき，有効または無効および，ネゴシエーション結果により決定したモードを選択できます。本装置と相手装置の設定を送信と受信が一致するように合わせてください。例えば，本装置のポーズパケット送信を on に設定した場合，相手装置のポーズパケット受信は有効に設定してください。本装置と相手装置の設定内容と実行動作モードを「表 12-6　フローコントロールの送信動作」，「表 12-7　フローコントロールの受信動作」および「表 12-8　オートネゴシエーション時のフローコントロール動作」に示します。

表 12-6　フローコントロールの送信動作

本装置のポーズパケット送信	相手装置のポーズパケット受信	フローコントロール動作
on	有効	相手装置が送信規制を行う
off	無効	相手装置が送信規制を行わない
desired	desired	相手装置が送信規制を行う

（凡例）

on：有効。

off：無効。desired と組み合わせた設定の場合，ネゴシエーション結果によって動作します。フローコントロール動作は「表 12-8　オートネゴシエーション時のフローコントロール動作」を参照してください。

desired：有効。オートネゴシエーション選択時は，ネゴシエーション結果によって動作します。フローコントロール動作は「表 12-8　オートネゴシエーション時のフローコントロール動作」を参照してください。

表 12-7　フローコントロールの受信動作

本装置のポーズパケット受信	相手装置のポーズパケット送信	フローコントロール動作
on	有効	本装置が送信規制を行う
off	無効	本装置が送信規制を行わない
desired	desired	本装置が送信規制を行う

（凡例）

on：有効。

off：無効。desired と組み合わせた設定の場合，ネゴシエーション結果によって動作します。フローコントロール動作は「表 12-8　オートネゴシエーション時のフローコントロール動作」を参照してください。

desired：有効。オートネゴシエーション選択時は，ネゴシエーション結果によって動作します。フローコントロール動作は「表 12-8　オートネゴシエーション時のフローコントロール動作」を参照してください。

表 12-8 オートネゴシエーション時のフローコントロール動作

本装置		相手装置		本装置のオートネゴシエーション結果		フローコントロール動作	
ポーズパケット送信	ポーズパケット受信	ポーズパケット送信	ポーズパケット受信	ポーズパケット送信	ポーズパケット受信	本装置の送信規制	相手装置の送信規制
on	desired	有効	有効	on	on	行う	行う
			無効	on	off	行わない	行わない
			desired	on	on	行う	行う
		無効	有効	on	on	行わない	行う
			無効	on	off	行わない	行わない
			desired	on	on	行う	行う
		desired	有効	on	on	行う	行う
			無効	on	off	行わない	行わない
			desired	on	on	行う	行う
off		有効	有効	on	on	行う	行う
			無効	off	on	行う	行わない
			desired	on	on	行う	行う
		無効	有効	on	on	行わない	行う
			無効	off	off	行わない	行わない
			desired	on	on	行う	行う
		desired	有効	on	on	行う	行う
			無効	off	on	行う	行わない
			desired	on	on	行う	行う
desired	on	有効	有効	on	on	行う	行う
			無効	off	on	行う	行わない
			desired	on	on	行う	行う
		無効	有効	on	on	行わない	行う
			無効	off	on	行わない	行わない
			desired	on	on	行う	行う
		desired	有効	on	on	行う	行う
			無効	off	on	行わない	行わない
			desired	on	on	行う	行う
	off	有効	有効	off	off	行わない	行わない
			無効	off	off	行わない	行わない
			desired	off	off	行わない	行わない
		無効	有効	on	off	行わない	行う
			無効	off	off	行わない	行わない
			desired	on	off	行わない	行う
		desired	有効	off	off	行わない	行わない
			無効	off	off	行わない	行わない
			desired	off	off	行わない	行わない

本装置		相手装置		本装置のオートネゴシエーション結果		フローコントロール動作	
ポーズパケット送信	ポーズパケット受信	ポーズパケット送信	ポーズパケット受信	ポーズパケット送信	ポーズパケット受信	本装置の送信規制	相手装置の送信規制
	desired	有効	有効	on	on	行う	行う
			無効	off	off	行わない	行わない
			desired	on	on	行う	行う
		無効	有効	on	on	行わない	行う
			無効	off	off	行わない	行わない
			desired	on	on	行う	行う
		desired	有効	on	on	行う	行う
			無効	off	off	行わない	行わない
			desired	on	on	行う	行う

(4) 自動 MDIX 機能

自動 MDIX 機能は，MDI と MDI-X を自動的に切り替える機能です。これによって，クロスケーブルまたはストレートケーブルどちらでも通信できるようになります。オートネゴシエーション時だけサポートします。半二重および全二重固定時は MDI-X となります。MDI ／ MDI-X のピンマッピングを次の表に示します。

表 12-9　MDI ／ MDI-X のピンマッピング

RJ45	MDI			MDI-X		
Pin No.	1000BASE-T	100BASE-TX	10BASE-T	1000BASE-T	100BASE-TX	10BASE-T
1	BI_DA ＋	TD ＋	TD ＋	BI_DB ＋	RD ＋	RD ＋
2	BI_DA －	TD －	TD －	BI_DB －	RD －	RD －
3	BI_DB ＋	RD ＋	RD ＋	BI_DA ＋	TD ＋	TD ＋
4	BI_DC ＋	Unused	Unused	BI_DD ＋	Unused	Unused
5	BI_DC －	Unused	Unused	BI_DD －	Unused	Unused
6	BI_DB －	RD －	RD －	BI_DA －	TD －	TD －
7	BI_DD ＋	Unused	Unused	BI_DC ＋	Unused	Unused
8	BI_DD －	Unused	Unused	BI_DC －	Unused	Unused

注 1

10BASE-T と 100BASE-TX では，送信（TD）と受信（RD）信号は別々の信号線を使用しています。

注 2

1000BASE-T では，8 ピンすべてを送信と受信が同時双方向（bi-direction）通信するため，信号名表記が異なります。（BI_Dx：双方向データ信号）

(5) ジャンボフレーム

ジャンボフレームは，MAC ヘッダの DA ～データが 1518 オクテットを超えるフレームを中継するための機能です。

フレームについては，「12.1.3　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。Tag 付きフレームについては，「16.1.5　VLAN Tag」の Tag 付きフレームのフォーマットを参照してください。また，物理インタフェースは，100BASE-TX（全二重），1000BASE-T（全二重）だけサポートします。ジャンボフレームのサポート機能を次の表に示します。

表 12-10　ジャンボフレームサポート機能

項目	フレーム形式		内容
	EthernetV2※	IEEE802.3※	
フレーム長（オクテット）	Tag 無 :1519 ～ 9234 Tag 付 :1523 ～ 9238	×	MAC ヘッダの DA ～データの長さ。FCS は含みます。
受信機能	○	×	IEEE802.3 フレームは，LENGTH フィールド値が 0x05DD（1501 オクテット）以上の場合に廃棄します。
送信機能	○	×	IEEE802.3 フレームは送信しません。

（凡例）
　○：サポート　×：未サポート

注※
「12.1.3　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。

（6） ダウンシフト機能

ダウンシフト機能はオートネゴシエーション設定時に機能し，オートネゴシエーションによるリンク接続失敗時に，オートネゴシエーション広告の最も速い速度をディセーブルに設定し，次に速い速度でリンク接続を試みる機能です。（ダウンシフト機能を OFF にする操作はありません。）

（a） 適用回線

本機能は 1000BASE-T でサポートします。

（b） 回線速度変更順序

オートネゴシエーション完了後にリンク接続不可の場合，オートネゴシエーション広告の回線速度を，フェーズ１⇒フェーズ２・・・の順に落としていきます。回線速度が最低となってもリンク接続不可の場合は，フェーズ１に戻り再度ダウンシフトを繰り返します。

表 12-11　回線速度変更順序

項番	ダウンシフト機能	フェーズ	構成定義（speed パラメータ設定内容） ※ 1				備考
			auto	auto 10 100 1000	auto 10 100	auto 1000 or auto 100 or auto 10	
1	On	1	10 100 1000	10 100 1000	10 100	－	
2		2	10 100	10 100	10	－	
3		3	10	10	－	－	

－：ダウンシフト動作しません。通常のオートネゴシエーション動作となります。
注※ 1　数字は回線速度を示します。

（7） 10BASE-T ／ 100BASE-TX ／ 1000BASE-T 接続時の注意事項

1. 伝送速度，全二重／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運用コマンド inactivate および activate を実行してください。
2. 使用するケーブルについては，マニュアル「ユーザーズガイド」を参照してください。
3. 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，相手接続インタフェース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。
4. 1000BASE-T を使用する場合は全二重オートネゴシエーションだけとなります。なお，コンフィグレーションコマンド speed 1000，duplex half 設定の場合は，リンクアップしませんので注意してください。

12.5　10BASE-T/100BASE-TX/1000BASE-T のコンフィグレーション

12.5.1　ポートの設定

（1） 速度と duplex の設定

本装置と相手装置の伝送速度と duplex を設定できます。デフォルトでは相手装置とオートネゴシエーションで，伝送速度と duplex を決定します。

（a） オートネゴシエーションに対応していない相手装置と接続する場合

［設定のポイント］

10BASE-T および 100BASE-TX では，相手装置によってはオートネゴシエーションで接続できない場合があります。その場合は，相手装置に合わせて回線速度と duplex を指定し，固定設定で接続します。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/3**
   (config-if)# shutdown
   (config-if)# speed 100
   (config-if)# duplex half
   相手装置と 100BASE-TX 半二重で接続する設定をします。

2. **(config-if)# no shutdown**
   (config-if)# exit

［注意事項］

speed 10 または 100 を設定する場合は，duplex half または full を設定してください。
なお，speed 1000，duplex half を設定した場合は，リンクアップしません。

（b） オートネゴシエーションでも特定の速度を使用したい場合

［設定のポイント］

本装置は，オートネゴシエーションで接続する場合でも，回線速度を設定できます。オートネゴシエーションに加えて回線速度を設定した場合，相手装置とオートネゴシエーションで接続しても，設定された回線速度にならないときはリンクがアップしません。そのため，意図しない回線速度で接続されることを防止できます。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/3**
   (config-if)# shutdown
   (config-if)# speed auto 1000
   相手装置とオートネゴシエーションで接続しても，1000BASE-T だけで接続するようにします。

2. **(config-if)# no shutdown**
   (config-if)# exit

［注意事項］

回線速度と duplex は正しい組み合わせで設定してください。オートネゴシエーションの場合は，回線速度と duplex の両方ともにオートネゴシエーションを設定する必要があります。固定設定の場合は，回線速度と duplex の両方を固定設定にする必要があります。正しい組み合わせが設定されていない場合は，オートネゴシエーションで相手装置と接続します。

12.5.2 フローコントロールの設定

「12.2.8 フローコントロールの設定」を参照してください。

12.5.3 自動 MDIX の設定

本装置の 10BASE-T/100BASE-TX/1000BASE-T ポートは，自動 MDIX 機能をサポートしています。そのため，オートネゴシエーション時に，ケーブルのストレートまたはクロスに合わせて自動的に MDI 設定が切り替わり通信できます。また，本装置は MDI の固定機能を持っており，MDI 固定時は MDI-X（HUB 仕様）となります。

（1） 固定 MDI の設定

［設定のポイント］

AUTO-MDI を MDI-X に固定する場合に，固定したいポートに設定します。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/3**
   ポート 0/3 の設定を指定します。

2. **(config-if)# no mdix auto**
   (config-if)# exit
   自動 MDIX 機能を無効にし，MDI-X 固定にします。

12.6 1000BASE-T/10GBASE-T の解説

1000BASE-T ／ 10GBASE-T※のツイストペアケーブルを使用したインタフェースについて説明します。

注※ 100BASE-TX は未サポートです。

本装置の 1000BASE-T ／ 10GBASE-T のインタフェースは，ポート 0/1 ～ 0/2 の 2 ポートです。

12.6.1 機能一覧

(1) 接続インタフェース

(a) 1000BASE-T ／ 10GBASE-T 自動認識（オートネゴシエーション）

1000BASE-T ／ 10GBASE-T では自動認識機能（オートネゴシエーション）をサポートしています。

100BASE-TX，および固定接続は未サポートです。

(b) 1000BASE-T ／ 10GBASE-T 接続仕様

本装置のコンフィグレーションでの指定値と相手装置の伝送速度および，全二重／半二重モードの接続仕様を次の表に示します。

表 12-12 伝送速度，全二重／半二重モードごとの接続仕様

接続装置		本装置の設定
設定	インタフェース	オート ネゴシエーション
固定	100BASE-TX 半二重	×
	100BASE-TX 全二重	×
	1000BASE-T 半二重	×
	1000BASE-T 全二重	×
	10GBASE-T 全二重	×
オート ネゴシエーション	100BASE-TX 半二重	×
	100BASE-TX 全二重	×
	1000BASE-T 半二重	×
	1000BASE-T 全二重	1000BASE-T 全二重
	100/1000BASE-T 半二重	×
	100/1000BASE-T 全二重	1000BASE-T 全二重

接続装置		本装置の設定
設定	インタフェース	オート ネゴシエーション
	10GBASE-T 全二重	10GBASE-T 全二重
	100/1000/10GBASE-T 半二重	×
	100/1000/10GBASE-T 全二重	10GBASE-T 全二重

（凡例） ×：接続できない

（2） オートネゴシエーション

オートネゴシエーションは，伝送速度，全二重／半二重モード認識およびフローコントロールについて，対向装置間でやりとりを行い，接続動作を決定する機能です。

本装置での接続仕様を，「表 12-12　伝送速度，全二重／半二重モードごとの接続仕様」に示します。また，本装置では，ネゴシエーションで解決できなかった場合，リンク接続されるまで接続動作を繰り返します。（本動作については，「12.6.1　機能一覧（6）ダウンシフト機能」を参照してください。）

（3） フローコントロール

「12.4.1　機能一覧　（3）フローコントロール」を参照してください。

（4） 自動 MDIX 機能

自動 MDIX 機能は，MDI と MDI-X を自動的に切り替える機能です。これによって，クロスケーブルまたはストレートケーブルどちらでも通信できるようになります。オートネゴシエーション時だけサポートします。半二重および全二重固定時は MDI-X となります。MDI ／ MDI-X のピンマッピングを次の表に示します。

表 12-13　MDI ／ MDI-X のピンマッピング

RJ45	MDI			MDI-X		
Pin No.	10GBASE-T	1000BASE-T	100BASE-TX	10GBASE-T	1000BASE-T	100BASE-TX
1	BI_DA ＋	BI_DA ＋	未サポート	BI_DB ＋	BI_DB ＋	未サポート
2	BI_DA －	BI_DA －		BI_DB －	BI_DB －	
3	BI_DB ＋	BI_DB ＋		BI_DA ＋	BI_DA ＋	
4	BI_DC ＋	BI_DC ＋		BI_DD ＋	BI_DD ＋	
5	BI_DC －	BI_DC －		BI_DD －	BI_DD －	
6	BI_DB －	BI_DB －		BI_DA －	BI_DA －	
7	BI_DD ＋	BI_DD ＋		BI_DC ＋	BI_DC ＋	
8	BI_DD －	BI_DD －		BI_DC －	BI_DC －	

注 1

1000BASE-T では，8 ピンすべてを送信と受信が同時双方向（bi-direction）通信するため，信号名表記が異なります。（BI_Dx：双方向データ信号）

(5) ジャンボフレーム

「12.4.1 機能一覧 (5) ジャンボフレーム」を参照してください。

(6) ダウンシフト機能

ダウンシフト機能はオートネゴシエーション設定時に機能し，オートネゴシエーションによるリンク接続失敗時に，オートネゴシエーション広告の最も速い速度をディセーブルに設定し，次に速い速度でリンク接続を試みる機能です。(ダウンシフト機能を OFF にする操作はありません。)

(a) 適用回線

本機能は 10GBASE-T でサポートします。

(b) 回線速度変更順序

オートネゴシエーション完了後にリンク接続不可の場合，オートネゴシエーション広告の回線速度を，フェーズ１⇒フェーズ２・・・の順に落としていきます。回線速度が最低となってもリンク接続不可の場合は，フェーズ１に戻り再度ダウンシフトを繰り返します。

表 12-14 回線速度変更順序

項番	ダウンシフト機能	フェーズ	構成定義（speed パラメータ設定内容） ※１				備考
			auto	auto 100 1000 10000	auto 100 1000	auto 10000 or auto 1000 or auto 100	
1	On	1	100 1000 10000	100 1000 10000	100 1000	－	
2		2	100 1000	100 1000	100	－	
3		3	100	100	－	－	

－：ダウンシフト動作しません。通常のオートネゴシエーション動作となります。
注※１ 数字は回線速度を示します。

(7) 1000BASE-T/10GBASE-T 接続時の注意事項

1. 使用するケーブルについては，マニュアル「ユーザーズガイド」を参照してください。
2. 1000BASE-T/10GBASE-T ポートは全二重のオートネゴシエーションだけです。オートネゴシエーションに完了後にリンク接続不可の場合，前述のとおりダウンシフト機能が動作しますが，回線速度が低くなっても接続できない場合があります。この場合，ダウンシフト機能を OFF にする設定はありませんので，コンフィグレーションコマンド speed で auto 1000，または auto 10000 を設定してご使用ください。duplex は全二重固定のため設定変更はできません。
3. 100BASE-TX は未サポートです。

12.7 1000BASE-T/10GBASE-T のコンフィグレーション

12.7.1 ポートの設定

(1) 速度の設定

本装置と相手装置の伝送速度を設定できます。デフォルトでは相手装置とオートネゴシエーションで，伝送速度を決定します。デフォルトは auto（auto 100 1000 10000 と同じ）ですが，100BASE-TX は未サポートですので，auto 1000 または auto 10000 を設定してご使用ください。

なお，duplex は全二重固定です。

[設定のポイント]

本装置は，オートネゴシエーションで接続する場合でも，回線速度を設定できます。オートネゴシエーションに加えて回線速度を設定した場合，相手装置とオートネゴシエーションで接続しても，設定された回線速度にならないときはリンクがアップしません。そのため，意図しない回線速度で接続されることを防止できます。

[コマンドによる設定]

1. **(config)# interface tengigabitethernet 0/1**
   (config-if)# shutdown
   (config-if)# speed auto 10000
   相手装置とオートネゴシエーションで接続しても，10GBASE-T だけで接続するようにします。

2. **(config-if)# no shutdown**
   (config-if)# exit

12.7.2 フローコントロールの設定

「12.2.8 フローコントロールの設定」を参照してください。

12.7.3 自動 MDIX の設定

本装置の 1000BASE-T/10GBASE-T ポートは，自動 MDIX 機能をサポートしています。そのため，オートネゴシエーション時に，ケーブルのストレートまたはクロスに合わせて自動的に MDI 設定が切り替わり通信できます。また，本装置は MDI の固定機能を持っており，MDI 固定時は MDI-X（HUB 仕様）となります。

(1) 固定 MDI の設定

[設定のポイント]

AUTO-MDI を MDI-X に固定する場合に，固定したいポートに設定します。

[コマンドによる設定]

1. **(config)# interface tengigabitethernet 0/1**
   ポート 0/1 の設定を指定します。

2. **(config-if)# no mdix auto**
   (config-if)# exit
   自動 MDIX 機能を無効にし，MDI-X 固定にします。

12.7.4 ジャンボフレームの設定

「12.2.5 ジャンボフレームの設定」を参照してください。

12.8　サーバ接続ポートの解説

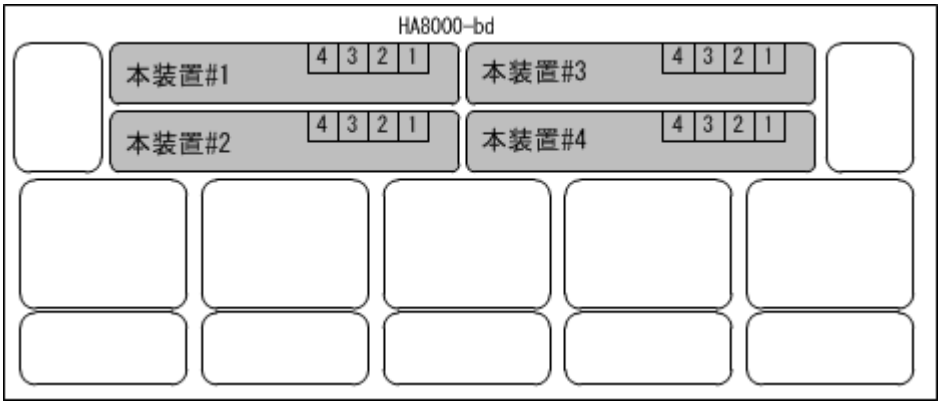
12.8.1　機能一覧

本装置のポート 0/5 からポート 0/24 は，HA8000-bd シリーズに搭載しているサーバブレードと接続する専用のポートです。ここではサーバ接続ポートについて記述します。

（1） サーバ接続ポートとサーバブレードとの接続

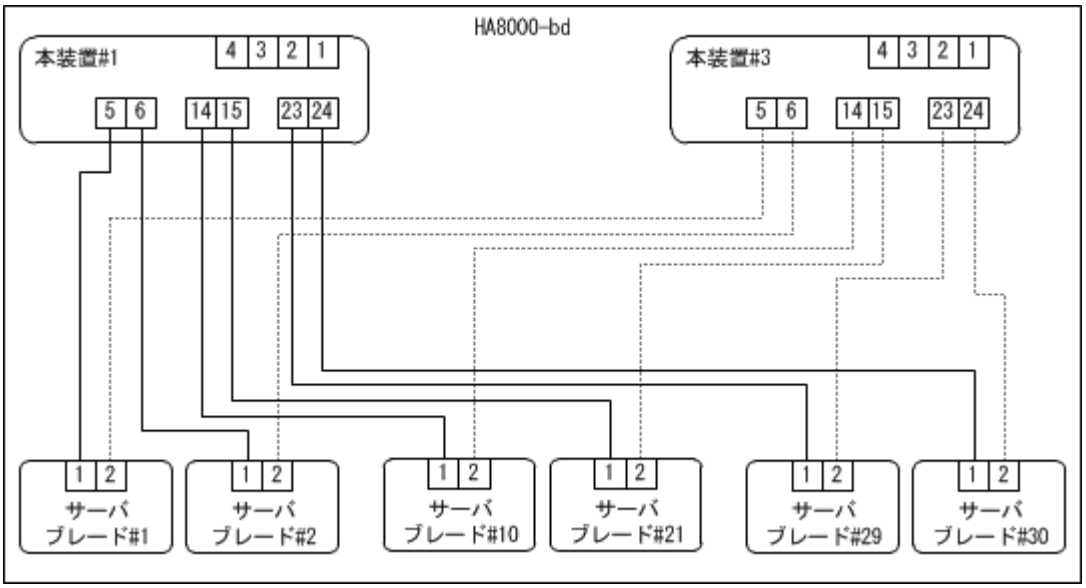
本装置は次の図に示すように HA8000-bd シリーズの背面に 4 台搭載しています。

図 12-6　本装置の搭載図



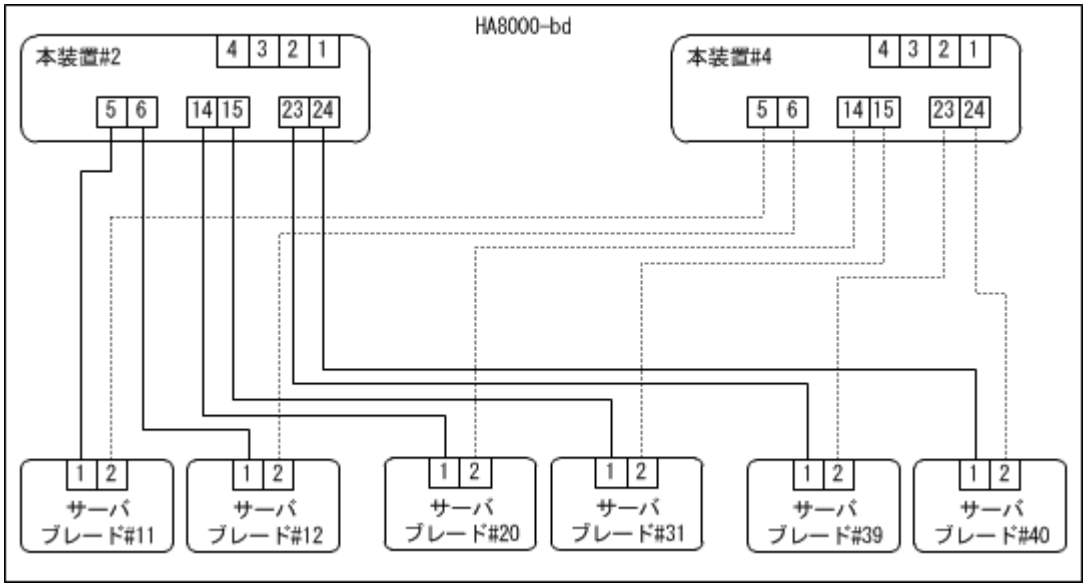
本装置のサーバ接続ポートとサーバブレードは，HA8000-bd シリーズ内で以下のように接続しています。

図 12-7　サーバ接続ポートとサーバブレードの接続（スイッチ #1 および #3 の接続）



スイッチ #1 とスイッチ #3 は，サーバブレード #1 ～ #10，#21 ～ #30 と接続しています。

図 12-8　サーバ接続ポートとサーバブレードの接続（スイッチ #2 および #4 の接続）



スイッチ #2 とスイッチ #4 は，サーバブレード #11 ～ #20，#31 ～ #40 と接続しています。

（2） サーバ接続ポートの仕様

サーバ接続ポートの仕様を「表 1 12　サーバ接続ポート仕様」に示します。

表 12-15　サーバ接続ポート仕様

項目	内容	備考
伝送速度	1000Mbit/s（固定）	伝送速度の変更不可※
全二重／半二重モード	全二重（固定）	半二重への変更不可※
オートネゴシエーション	あり	
フローコントロール	あり	
使用ポート	0/5 ～ 0/24	サーバブレード以外との接続不可

注※
　伝送速度および全二重／半二重モードは，1000Mbit/s 全二重固定であるため，変更できません。

（3） オートネゴシエーション

オートネゴシエーションは，全二重モード選択およびフローコントロールについて，対向装置間でやりとりを行い，接続動作を決定する機能です。

また，本装置では，ネゴシエーションで解決できなかった場合，リンク接続されるまで接続動作を繰り返します。

（4） フローコントロール

「12.4.1　機能一覧　(3) フローコントロール」を参照してください。

（5） ジャンボフレーム

「12.4.1　機能一覧　(5) ジャンボフレーム」を参照してください。

12.9　サーバ接続ポートのコンフィグレーション

12.9.1　サーバ接続ポートの設定

（1） 速度の設定

本装置のサーバ接続ポートの伝送速度は，工場出荷時の初期値で以下が設定されています。初期値のため，運用コマンド show running-config で表示されません。また，サーバ接続ポートで duplex の変更は未サポートです（全二重で動作します）。

- サーバ接続ポート 0/5 ～ 0/24　伝送速度：Auto

［注意事項］

サーバ接続ポートの伝送速度は初期値のままご使用ください。変更した場合はサーバブレードとの通信障害となる場合があります。

12.9.2　フローコントロールの設定

「12.2.8　フローコントロールの設定」を参照してください。

12.9.3　ジャンボフレームの設定

「12.2.5　ジャンボフレームの設定」を参照してください。

13 リンクアグリゲーション

この章では，リンクアグリゲーションの解説と操作方法について説明します。

13.1 リンクアグリゲーション基本機能の解説

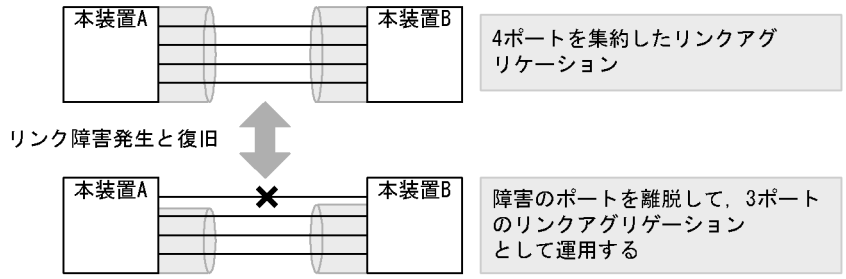
13.1.1 概要

リンクアグリゲーションは，隣接装置との間を複数のイーサネットポートで接続し，それらを束ねて一つの仮想リンクとして扱う機能です。この仮想リンクをチャネルグループと呼びます。リンクアグリゲーションによって接続装置間の帯域の拡大や冗長性を確保できます。

13.1.2 リンクアグリゲーションの構成

リンクアグリゲーションの構成例を次の図に示します。この例では四つのポートを集約しています。集約しているポートのうちの 1 本が障害となった場合には，チャネルグループから離脱し，残りのポートでチャネルグループとして通信を継続します。

図 13-1 リンクアグリゲーションの構成例



13.1.3 サポート仕様

(1) リンクアグリゲーションのモード

本装置のリンクアグリゲーションは，モードとして LACP およびスタティックの 2 種類をサポートします。

- LACP リンクアグリゲーション
  IEEE802.3ad 準拠の LACP を利用したリンクアグリゲーションです。LACP によるネゴシエーションが成功した場合にチャネルグループとしての運用を開始します。LACP によって，隣接装置との整合性確認やリンクの正常性確認ができます。
- スタティックリンクアグリゲーション
  コンフィグレーションによるスタティックなリンクアグリゲーションです。LACP は動作させません。チャネルグループとして設定したポートがリンクアップした時点で運用を開始します。

リンクアグリゲーションのサポート仕様を次の表に示します。

表 13-1 リンクアグリゲーションのサポート仕様

項目	サポート仕様	備考
装置当たりのチャネルグループ数	64	－
1 グループ当たりの最大ポート数	8	－
リンクアグリゲーションのモード	• LACP • スタティック	－

項目	サポート仕様	備考
ポート速度	同一速度だけを使用します。	遅い回線※は離脱します。
Duplex モード	全二重だけ	－

（凡例）
－：該当しない

注※
その時点でリンクアップしている最高速度よりも遅い回線です。

13.1.4 チャネルグループの MAC アドレス

スパニングツリーなどのプロトコルを運用する際に，チャネルグループの MAC アドレスを使用します。本装置は，チャネルグループの MAC アドレスとして，グループに所属するポートのうちどれかの MAC アドレスを使用します。

チャネルグループに所属するポートから MAC アドレスを使用しているポートを削除するとグループの MAC アドレスが変更になります。

13.1.5 フレーム送信時のポート振り分け

リンクアグリゲーションへフレームを送信するとき，送信するフレームごとにポートを選択しトラフィックを各ポートへ分散させることで複数のポートを効率的に利用します。ポートの振り分けは，送信するフレーム内の情報を基にポートを選択して振り分けます。

ポートの振り分けに使用する情報を次の表に示します。

表 13-2 フレーム送信時のポート振り分け

中継	フレームの種類	振り分けに使用する情報
レイヤ 2 中継	MAC アドレス未学習フレーム（ブロードキャスト，マルチキャスト含む）	宛先 MAC アドレス 送信元 MAC アドレス 受信ポート番号または受信チャネルグループ番号
	MAC アドレス学習済の IP フレーム	宛先 IP アドレス 送信元 IP アドレス 宛先 TCP/UDP ポート番号 送信元 TCP/UDP ポート番号
	MAC アドレス学習済の非 IP フレーム	宛先 MAC アドレス 送信元 MAC アドレス 受信 VLAN イーサタイプ

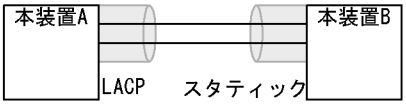
13.1.6 リンクアグリゲーション使用時の注意事項

（1） リンクアグリゲーションが不可能な構成

リンクアグリゲーション構成時には，装置間での設定が一致している必要があります。リンクアグリゲーションが不可能な構成例を次に示します。

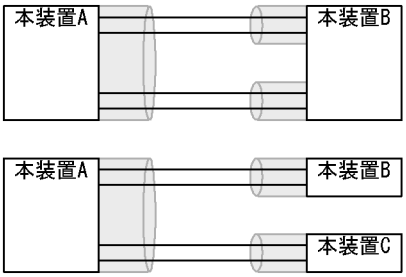
図 13-2 リンクアグリゲーションが不可能な構成例

●装置間でモードが異なる場合



この構成を実施したときの動作
・LACPのネゴシエーションが成立しないで通信断状態になる。

●装置間でチャネルグループがポイントーマルチポイントになっている場合



この構成を実施したときの動作
・本装置Aから送信したフレームが本装置Bを経由して戻るなど，
ループ構成となって正常に動作しない。

(2) リンクアグリゲーションの設定手順

リンクアグリゲーション構成時には，装置間での設定が一致している必要があります。一致していない状態で通信を開始しようとするとループ構成となるおそれがあります。設定はリンクダウン状態で行い，「(1) リンクアグリゲーションが不可能な構成」のような構成になっていないことを確認したあとで，ポートをリンクアップさせることをお勧めします。

(3) CPU 過負荷時

LACP リンクアグリゲーションモード使用時に CPU が過負荷な状態になった場合，本装置が送受信する LACPDU の廃棄または処理遅延が発生して，一時的な通信断になることがあります。一時的な通信断が頻発する場合は，CPU が過負荷状態となっている可能性があるため，LACPDU の送信間隔を長くするか，スタティックリンクアグリゲーションを使用してください。

13.2　リンクアグリゲーション基本機能のコンフィグレーション

13.2.1　コンフィグレーションコマンド一覧

リンクアグリゲーション基本機能のコンフィグレーションコマンド一覧を次の表に示します。

表 13-3　コンフィグレーションコマンド一覧

コマンド名	説明
channel-group lacp system-priority	チャネルグループごとに LACP システム優先度を設定します。
channel-group mode	ポートをチャネルグループに追加し，また，リンクアグリゲーションのモードを設定します。
channel-group periodic-timer	LACPDU の送信間隔を設定します。
description	チャネルグループの補足説明を設定します。
interface port-channel	ポートチャネルインタフェースに関する項目を設定します。
lacp port-priority	LACP のポート優先度を設定します。
lacp system-priority	channel-group lacp system-priority コマンドの設定がないチャネルグループの LACP システム優先度を設定します。
shutdown	チャネルグループに登録したポートを shutdown にして通信を停止します。

13.2.2　スタティックリンクアグリゲーションの設定

［設定のポイント］

スタティックリンクアグリゲーションは，イーサネットインタフェースコンフィグレーションモードで，コンフィグレーションコマンド channel-group mode を使用してチャネルグループ番号と「on」のモードを設定します。スタティックリンクアグリゲーションは，コンフィグレーションコマンド channel-group mode を設定することによって動作を開始します。

［コマンドによる設定］

1. **(config)# interface range gigabitethernet 0/3-4**
   ポート 0/3，0/4 のイーサネットインタフェースモードに移行します。

2. **(config-if-range)# channel-group 3 mode on**
   (config-if-range)# exit
   ポート 0/3，0/4 を，スタティックモードのチャネルグループ 3 に登録します。

13.2.3　LACP リンクアグリゲーションの設定

（1）チャネルグループの設定

［設定のポイント］

LACP リンクアグリゲーションは，イーサネットインタフェースコンフィグレーションモードで，コンフィグレーションコマンド channel-group mode を使用して，チャネルグループ番号と「active」または「passive」のモードを設定します。

［コマンドによる設定］

1. **(config)# interface range gigabitethernet 0/3-4**
   ポート 0/3，0/4 のイーサネットインタフェースモードに移行します。

2. **(config-if-range)# channel-group 3 mode active**
   (config-if-range)# exit
   ポート 0/3，0/4 を LACP モードのチャネルグループ 3 に登録します。LACP は active モードとして対向装置に関係なく LACPDU の送信を開始します。passive を指定した場合は，対向装置からの LACPDU を受信したときだけ LACPDU の送信を開始します。

（2） システム優先度の設定

LACP のシステム優先度を設定します。通常，本パラメータを変更する必要はありません。

［設定のポイント］
LACP システム優先度は値が小さいほど高い優先度となります。

［コマンドによる設定］

1. **(config)# lacp system-priority 100**
   本装置の LACP システム優先度を 100 に設定します。

2. **(config)# interface port-channel 3**
   (config-if)# channel-group lacp system-priority 50
   (config-if)# exit
   チャネルグループ 3 の LACP システム優先度を 50 に設定します。本設定を行わない場合は装置のシステム優先度である 100 を使用します。

（3） ポート優先度の設定

LACP のポート優先度を設定します。本装置では，ポート優先度は拡張機能のスタンバイリンク機能で使用します。通常，本パラメータを変更する必要はありません。

［設定のポイント］
LACP ポート優先度は値が小さいほど高い優先度となります。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/3**
   (config-if)# lacp port-priority 100
   (config-if)# exit
   ポート 0/3 の LACP ポート優先度を 100 に設定します。

（4） LACPDU 送信間隔の設定

［設定のポイント］
対向装置が本装置に向けて送信する LACPDU の間隔を設定します。本装置は本パラメータで設定した間隔で LACPDU を受信します。
LACPDU の送信間隔は long（30 秒），short（1 秒）のどちらかを選択します。デフォルトは long

（30 秒）で動作します。送信間隔を short（1 秒）に変更した場合，リンクの障害によるタイムアウトを検知しやすくなり，障害時に通信が途絶える時間を短く抑えることができます。

［コマンドによる設定］

1. **(config)# interface port-channel 3**
   (config-if)# channel-group periodic-timer short
   (config-if)# exit
   チャネルグループ 3 の LACPDU 送信間隔を short（1 秒）に設定します。

［注意事項］

LACPDU 送信間隔を short（1 秒）に設定すると，障害を検知しやすくなる一方で，LACPDU トラフィックが増加することによってリンクアグリゲーションプログラムの負荷が増加します。本パラメータを short（1 秒）にすることでタイムアウトのメッセージや一時的な通信断が頻発する場合は，デフォルトの long（30 秒）に戻すかスタティックモードを使用してください。

13.2.4 ポートチャネルインタフェースの設定

ポートチャネルインタフェースでは，チャネルグループ上で動作する機能を設定します。

ポートチャネルインタフェースは，コンフィグレーションコマンドで設定するか，イーサネットインタフェースコンフィグレーションモードで，コンフィグレーションコマンド channel-group mode を設定することによって自動的に生成されます。

（1） ポートチャネルインタフェースとイーサネットインタフェースの関係

ポートチャネルインタフェースは，チャネルグループ上で動作するものを設定します。それらはイーサネットインタフェースコンフィグレーションモードでも設定することができます。このような機能を設定するコマンドはポートチャネルインタフェースとイーサネットインタフェースで関連性があり，設定する際に次のように動作します。

- ポートチャネルインタフェースとイーサネットインタフェースで関連コマンドの設定が一致している必要があります。
- ポートチャネルインタフェースを未設定の状態で，イーサネットインタフェースにコンフィグレーションコマンド channel-group mode を設定すると，自動的にポートチャネルインタフェースを生成します。このとき，コンフィグレーションコマンド channel-group mode を設定するイーサネットインタフェースに，関連コマンドが設定されていてはいけません。
- ポートチャネルインタフェースがすでに設定済みの状態で，イーサネットインタフェースにコンフィグレーションコマンド channel-group mode を設定する場合，関連コマンドが一致している必要があります。
- ポートチャネルインタフェースで関連コマンドを設定すると，コンフィグレーションコマンド channel-group mode で登録されているイーサネットインタフェースの設定にも，同じ設定が反映されます。

ポートチャネル関連コマンドを次の表に示します。

表 13-4 ポートチャネルインタフェースの関連コマンド

機能	コマンド
VLAN	switchport mode
	switchport access

機能	コマンド
	switchport protocol
	switchport trunk
	switchport mac
	switchport mac auto-vlan
	switchport vlan mapping
	switchport vlan mapping enable
スパニングツリー	spanning-tree portfast
	spanning-tree bpdufilter
	spanning-tree bpduguard
	spanning-tree guard
	spanning-tree link-type
	spanning-tree port-priority
	spanning-tree cost
	spanning-tree vlan port-priority
	spanning-tree vlan cost
	spanning-tree single port-priority
	spanning-tree single cost
	spanning-tree mst port-priority
	spanning-tree mst cost
レイヤ２認証共通	authentication arp-relay
	authentication ip access-group
	authentication force-authorized vlan
	authentication logout linkdown
	authentication max-user(interface)
IEEE802.1X	dot1x authentication
	dot1x ignore-eapol-start
	dot1x max-req
	dot1x multiple-authentication
	dot1x port-control
	dot1x reauthentication
	dot1x supplicant-detection
	dot1x timeout reauth-period
	dot1x timeout tx-period
	dot1x timeout supp-timeout
	dot1x timeout server-timeout
	dot1x timeout keep-unauth
	dot1x timeout quiet-period
Web 認証	web-authentication authentication
	web-authentication html-fileset
	web-authentication port

機能	コマンド
MAC 認証	mac-authentication authentication
	mac-authentication port
L2 ループ検知	loop-detection

(2) チャネルグループ上で動作する機能の設定

[設定のポイント]

ポートチャネルインタフェースでは，VLAN やスパニングツリーなど，チャネルグループ上で動作する機能を設定します。ここでは，トランクポートを設定する例を示します。

[コマンドによる設定]

1. **(config)# interface range gigabitethernet 0/3-4**
   (config-if-range)# channel-group 3 mode on
   (config-if-range)# exit
   ポート 0/3，0/4 をスタティックモードのチャネルグループ 3 に登録します。また，チャネルグループ 3 のポートチャネルインタフェースが自動生成されます。

2. **(config)# interface port-channel 3**
   チャネルグループ 3 のポートチャネルインタフェースコンフィグレーションモードに移行します。

3. **(config-if)# switchport mode trunk**
   (config-if)# exit
   チャネルグループ 3 をトランクポートに設定します。

(3) ポートチャネルインタフェースの shutdown

[設定のポイント]

ポートチャネルインタフェースを shutdown に設定すると，チャネルグループに登録されているすべてのポートの通信を停止します。リンクアップしているポートはアップ状態のまま通信停止状態になります。

[コマンドによる設定]

1. **(config)# interface range gigabitethernet 0/3-4**
   (config-if-range)# channel-group 3 mode on
   (config-if-range)# exit
   ポート 0/3，0/4 をスタティックモードのチャネルグループ 3 として登録します。

2. **(config)# interface port-channel 3**
   (config-if)# shutdown
   (config-if)# exit
   ポートチャネルインタフェースモードに移行して shutdown を設定します。ポート 0/3，0/4 の通信が停止し，チャネルグループ 3 は停止状態になります。

13.2.5 チャネルグループの削除

チャネルグループのポートやチャネルグループ全体を削除する場合は，削除する対象のポートをあらかじめイーサネットインタフェースコンフィグレーションモードで shutdown に設定してください。
shutdown に設定することで，削除する際にループが発生することを防ぎます。

（1） チャネルグループ内のポートの削除

［設定のポイント］

ポートをチャネルグループから削除します。削除したポートはチャネルグループとは別のポートとして動作するため，削除時のループを回避するために事前に shutdown に設定します。
削除したポートには，削除前に interface port-channel で設定した関連コマンド（表 13-4　ポートチャネルインタフェースの関連コマンド）は残るため，別の用途に使用する際には注意してください。
チャネルグループ内のすべてのポートを削除しても，interface port-channel の設定は自動的には削除されません。チャネルグループ全体の削除は「(2) チャネルグループ全体の削除」を参照してください。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/3**
   (config-if)# shutdown
   ポート 0/3 をチャネルグループから削除するために，事前に shutdown にしてリンクダウンさせます。

2. **(config-if)# no channel-group**
   (config-if)# exit
   ポート 0/3 からチャネルグループの設定を削除します。

（2） チャネルグループ全体の削除

［設定のポイント］

チャネルグループ全体を削除します。削除したチャネルグループに登録していたポートはそれぞれ個別のポートとして動作するため，削除時のループを回避するために事前に shutdown に設定します。
チャネルグループは interface port-channel を削除することによって，全体が削除されます。この削除によって，登録していた各ポートからコンフィグレーションコマンド channel-group mode が自動的に削除されます。ただし，各ポートには削除前に interface port-channel で設定した関連コマンド（表 13-4　ポートチャネルインタフェースの関連コマンド）は残るため，別の用途に使用する際には注意してください。

［コマンドによる設定］

1. **(config)# interface range gigabitethernet 0/3-4**
   (config-if-range)# shutdown
   (config-if-range)# exit
   チャネルグループ全体を削除するために，削除したいチャネルグループに登録されているポートをすべて shutdown に設定しリンクダウンさせます。

2. **(config)# no interface port-channel 3**
   チャネルグループ 3 を削除します。ポート 0/3，0/4 に設定されているコンフィグレーションコマンド channel-group mode も自動的に削除されます。

13.3　リンクアグリゲーション拡張機能の解説

13.3.1　スタンバイリンク機能

（1）解説

チャネルグループ内にあらかじめ待機用のポートを用意しておき，運用中のポートで障害が発生したときに待機用のポートに切り替えることによって，グループとして運用するポート数を維持する機能です。この機能を使用すると，障害時に帯域の減少を防ぐことができます。

この機能は，スタティックリンクアグリゲーションで使用してください。

（2）スタンバイリンクの選択方法

コンフィグレーションでチャネルグループとして運用する最大ポート数を設定します。グループに属するポート数が指定された最大ポート数を超えた分のポートが待機用ポートになります。

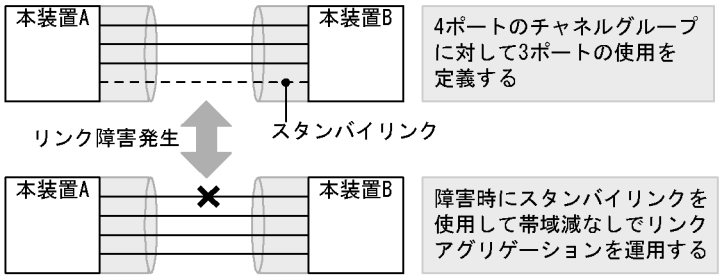
待機用ポートは，コンフィグレーションで設定するポート優先度，ポート番号から選択されます。待機用ポートは，次の表に示すように選択優先度の高い順に決定します。

表 13-5　待機用ポートの選択方法

選択優先度	パラメータ	備考
高 ↑	ポート優先度	優先度の低いポートから待機用ポートとして選択
↓ 低	ポート番号	ポート番号の大きい順に待機用ポートとして選択

スタンバイリンク機能の例を次の図に示します。この例では，グループに属するポート数を 4，運用する最大ポート数を 3 としています。

図 13-3　スタンバイリンク機能の構成例



本装置では，チャネルグループで運用するポートを以下に従って決定します。

- 全二重でリンクアップしていないポートを除外します。
- 当該時点でリンクアップしている最高速度のポート（同じチャネルグループに属するものに限る）と異なる速度のポートを除外します。
- 残るポートのうちから，ポート優先度の高い順（優先度の設定値の小さい順，優先度の設定値が同じ場合はポート番号の小さい順）に，本コマンドで設定した最大数に達するまで確保したポートを運用ポートとします。

no-link-down が指定されていない状態で，最大数の運用ポートが存在する場合（最大数の運用ポートを確

保した場合）は，最も低いポート優先度の運用ポートよりも低いポート優先度のポートをシャットダウンします。ポート優先度のコンフィグレーションがない場合，ポート番号の小さい低速ポートが先にリンクアップすると，ポート番号の大きい高速ポートがシャットダウンされます。

(3) スタンバイリンクのモード

スタンバイリンク機能には，次に示す二つのモードがあります。

- リンクダウンモード
  スタンバイリンク（待機用ポート）をリンクダウン状態にします。スタンバイリンク機能をサポートしていない対向装置も待機用ポートにすることができます。
- 非リンクダウンモード
  スタンバイリンク（待機用ポート）をリンクダウン状態にしないで，送信だけを停止します。リンクアップ状態のため，待機中のポートでも障害を監視できます。また，スタティックリンクアグリゲーションの場合は，待機中のポートは送信だけを停止して，受信は行います。スタンバイリンク機能をサポートしていない対向装置は，リンクダウンが伝わらないためスタンバイリンク上で送信を継続しますが，そのような対向装置とも接続できます。
  なお，チャネルグループ内の全ポートが半二重でリンクアップした場合はチャネルはアップしませんが，その場合でも一部のパケットは受信可能です。

リンクダウンモードを使用している場合，運用中のポートが一つのとき，そのポートで障害が発生すると，待機用のポートに切り替わる際にチャネルグループがいったんダウンします。非リンクダウンモードの場合，ダウンせずに待機用ポートを使用します。

運用中のポートが一つの状態とは，以下の状態を示します。

- コンフィグレーションコマンド max-active-port で 1 を設定している状態。

13.4　リンクアグリゲーション拡張機能のコンフィグレーション

13.4.1　コンフィグレーションコマンド一覧

リンクアグリゲーション拡張機能のコンフィグレーションコマンド一覧を次の表に示します。

表 13-6　コンフィグレーションコマンド一覧

コマンド名	説明
channel-group lacp system-priority	システム優先度をチャネルグループごとに設定します。
channel-group max-active-port	スタンバイリンク機能を設定し，最大ポート数を指定します。
lacp port-priority	ポート優先度を設定します。スタンバイリンクを選択するために使用します。
lacp system-priority	channel-group lacp system-priority コマンドの設定がないチャネルグループの LACP システム優先度を設定します。

13.4.2　スタンバイリンク機能のコンフィグレーション

［設定のポイント］

チャネルグループにスタンバイリンク機能を設定して，同時に最大ポート数を設定します。また，リンクダウンモード，非リンクダウンモードのどちらかを設定します。スタンバイリンク機能は，スタティックリンクアグリゲーションだけで使用できます。

待機用ポートはポート優先度によって設定し，優先度が低いポートからスタンバイリンクに選択します。ポート優先度は値が小さいほど高い優先度になります。

［コマンドによる設定］

1. **(config)# interface port-channel 3**

   チャネルグループ 3 のポートチャネルインタフェースコンフィグレーションモードに移行します。

2. **(config-if)# channel-group max-active-port 3**

   チャネルグループ 3 にスタンバイリンク機能を設定して，最大ポート数を 3 に設定します。チャネルグループ 3 はリンクダウンモードで動作します。

3. **(config-if)# exit**

   グローバルコンフィグレーションモードに戻ります。

4. **(config)# interface port-channel 5**
   (config-if)# channel-group max-active-port 1 no-link-down
   (config-if)# exit

   チャネルグループ 5 のポートチャネルインタフェースコンフィグレーションモードに移行して，スタンバイリンク機能を設定します。最大ポート数を 1 とし，非リンクダウンモードを設定します。

5. **(config)# interface gigabitethernet 0/3**
   (config-if)# channel-group 5 mode on
   (config-if)# lacp port-priority 300
   (config-if)# exit

   チャネルグループ 5 にポート 0/3 を登録して，ポート優先度を 300 に設定します。ポート優先度は値が小さいほど優先度が高く，ポート優先度のデフォルト値の 128 よりもスタンバイリンクに選択されやすくなります。

13.5 リンクアグリゲーションのオペレーション

13.5.1 運用コマンド一覧

リンクアグリゲーションの運用コマンド一覧を次の表に示します。

表 13-7 運用コマンド一覧

コマンド名	説明
show channel-group	リンクアグリゲーションの情報を表示します。
show channel-group statistics	リンクアグリゲーションのデータパケット送受信統計情報を表示します。
show channel-group statistics lacp	LACPDU の送受信統計情報を表示します。
clear channel-group statistics lacp	LACPDU の送受信統計情報をクリアします。

13.5.2 リンクアグリゲーションの状態の確認

(1) リンクアグリゲーションの接続状態の確認

リンクアグリゲーションの情報を運用コマンド show channel-group で表示します。CH Status でチャネルグループの接続状態を確認できます。また，設定が正しいことを各項目で確認してください。

運用コマンド show channel-group の実行結果を次の図に示します。

図 13-4 show channel-group の実行結果

```
> show channel-group

Date 20XX/06/06 18:20:48 UTC
ChGr: 31  Mode: LACP
  CH Status       : Down    Elapsed Time: -
  Max Active Port: 8
  MAC address     : -               VLAN ID: 4093
  Actor System    : Priority: 128    MAC: 0000.87a4.fe51  Key: 31
  Partner System : -
  Port Information
    0/3   Down  State: Detached
    0/4   Down  State: Detached
ChGr: 32  Mode: LACP
  CH Status       : Up      Elapsed Time: 00:15:16
  Max Active Port: 8
  Description     : lab network
  MAC address     : 0000.8754.ba14  VLAN ID: 4093
  Periodic Timer : Long
  Actor System    : Priority: 128    MAC: 0000.87a4.fe51  Key: 32
  Partner System : Priority: 128    MAC: 0000.87a8.85a2  Key: 32
  Port Information
    0/20  Up    State: Distributing
ChGr: 33  Mode: LACP
  CH Status       : Down    Elapsed Time: -
  Max Active Port: 8
  MAC address     : -               VLAN ID: 4093
  Actor System    : Priority: 128    MAC: 0000.87a4.fe51  Key: 33
  Partner System : -
  Port Information
    0/21  Up    State: Detached
ChGr: 64  Mode: Static
  CH Status       : Up      Elapsed Time: 00:15:21
  Max Active Port: 8
  MAC address     : 0000.8754.ba12  VLAN ID: 4093
  Port Information
```

```
    0/24  Up    State: Distributing

>
```

（2） 各ポートの運用状態の確認

運用コマンド show channel-group detail で各ポートの詳細な状態を表示します。ポートの通信状態を Status で確認してください。

運用コマンド show channel-group detail の実行結果を次の図に示します。

図 13-5　show channel-group detail の実行結果

```
> show channel-group detail

Date 20XX/06/06 18:22:36 UTC
ChGr: 31  Mode: LACP
  CH Status      : Down    Elapsed Time: -
  Max Active Port: 8
  MAC address    : -               VLAN ID: 4093
  Actor System   : Priority: 128    MAC: 0000.87a4.fe51  Key: 31
  Partner System : -
  Port Information
  Port: 0/3  Down
    State: Detached      Speed: -      Duplex: -
    Actor   Port  : Priority: 128
  Port: 0/4  Down
    State: Detached      Speed: -      Duplex: -
    Actor   Port  : Priority: 128
ChGr: 32  Mode: LACP
  CH Status      : Up      Elapsed Time: 00:17:04
  Max Active Port: 8
  Description    : lab network
  MAC address    : 0000.8754.ba14  VLAN ID: 4093
  Periodic Timer : Long
  Actor System   : Priority: 128    MAC: 0000.87a4.fe51  Key: 32
  Partner System : Priority: 128    MAC: 0000.87a8.85a2  Key: 32
  Port Information
  Port: 0/20  Up
    State: Distributing  Speed: 1G     Duplex: Full
    Actor   Port  : Priority: 128
    Partner System: Priority: 128    MAC: 0000.87a8.85a2  Key: 32
    Partner Port  : Priority: 128    Number: 23
ChGr: 33  Mode: LACP
  CH Status      : Down    Elapsed Time: -
  Max Active Port: 8
  MAC address    : -               VLAN ID: 4093
  Actor System   : Priority: 128    MAC: 0000.87a4.fe51  Key: 33
  Partner System : -
  Port Information
  Port: 0/21  Up
    State: Detached      Speed: 1G     Duplex: Full
    Actor   Port  : Priority: 128
ChGr: 64  Mode: Static
  CH Status      : Up      Elapsed Time: 00:17:11
  Max Active Port: 8
  MAC address    : 0000.8754.ba12  VLAN ID: 4093
  Port Information
  Port: 0/24  Up
    State: Distributing  Speed: 1G     Duplex: Full

>
```

14 レイヤ 2 スイッチ概説

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

14.1　概要

14.1.1　MAC アドレス学習

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

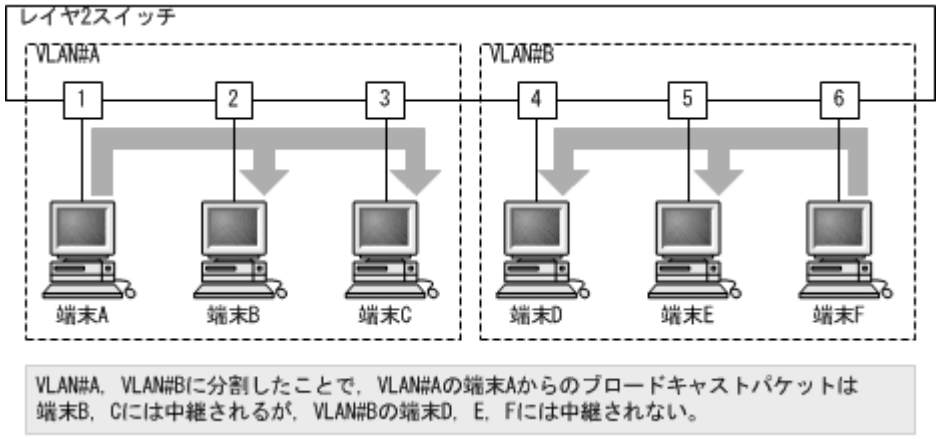
レイヤ 2 スイッチは，MAC アドレステーブルのエントリに従ってフレームを中継します。フレームの宛先 MAC アドレスに一致するエントリがあると，そのエントリのポートに中継します（エントリのポートが受信したポートである場合は中継しません）。一致するエントリがない場合，受信したポート以外のすべてのポートにフレームを中継します。この中継をフラッディングと呼びます。

14.1.2　VLAN

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

VLAN の概要を次の図に示します。VLAN#A と VLAN#B の間ではブロードキャストドメインが分割されるため，フレームが届くことはありません。

図 14-1　VLAN の概要



14.2 サポート機能

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

これらの機能は，組み合わせて利用できる機能とできない機能があります。機能の組み合わせ制限については，次項で説明します。

表 14-1 レイヤ 2 スイッチサポート機能

サポート機能		機能概要
MAC アドレス学習		MAC アドレステーブルに登録する MAC アドレスの学習機能
VLAN	ポート VLAN	ポート単位にスイッチ内を仮想的なグループに分ける機能
	プロトコル VLAN	プロトコル単位にスイッチ内を仮想的なグループに分ける機能
	MAC VLAN	送信元の MAC アドレス単位にスイッチ内を仮想的なグループに分ける機能
	デフォルト VLAN	コンフィグレーションが未設定のときにデフォルトで所属する VLAN
	ネイティブ VLAN	トランクポート，プロトコルポート，MAC ポートでの Untagged フレームを扱うポート VLAN の呼称
	VLAN トンネリング	複数ユーザの VLAN をほかの VLAN に集約して「トンネル」する機能
	Tag 変換	VLAN Tag を変換して別の VLAN に中継する機能
	L2 プロトコルフレーム透過機能	レイヤ 2 のプロトコルのフレームを中継する機能 スパニングツリー (BPDU)，IEEE802.1X(EAP) を透過します。
スパニングツリー	PVST+	VLAN 単位のスイッチ間のループ防止機能
	シングルスパニングツリー	装置単位のスイッチ間のループ防止機能
	マルチプルスパニングツリー	MST インスタンス単位のスイッチ間のループ防止機能
Ring Protocol		リングトポロジーでのレイヤ 2 ネットワークの冗長化機能
IGMP snooping/MLD snooping		レイヤ 2 スイッチで VLAN 内のマルチキャストトラフィック制御機能
ポート間中継遮断機能		指定したポート間ですべての通信を遮断する機能

14.3 レイヤ 2 スイッチ機能と他機能の共存について

レイヤ 2 スイッチ機能と併用する際，共存不可または制限事項がある機能があります。機能間の共存についての制限事項を次の表に示します。

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

表 14-2 VLAN での制限事項

使用したい機能		制限のある機能	制限の内容
VLAN 種別	ポート VLAN	VLAN トンネリング	一部制限あり※1
		レイヤ 2 認証	一部制限あり※2
		ポートミラーリング (ミラーポート)	共存不可
	プロトコル VLAN	デフォルト VLAN	共存不可
		VLAN トンネリング	
		PVST+	
		レイヤ 2 認証	一部制限あり※2
		ポートミラーリング (ミラーポート)	共存不可
	MAC VLAN	デフォルト VLAN	共存不可
		VLAN トンネリング	
		PVST+	
		レイヤ 2 認証	一部制限あり※2
		ポートミラーリング (ミラーポート)	共存不可
デフォルト VLAN		プロトコル VLAN	共存不可
		MAC VLAN	
		IGMP snooping	
		MLD snooping	
		レイヤ 2 認証	一部制限あり※2
		ポートミラーリング (ミラーポート)	共存不可
VLAN Tag の TPID 変更		Tag 変換	一部制限あり※3
VLAN 拡張機能	Tag 変換	VLAN Tag の TPID 変更	一部制限あり※3
		PVST+	共存不可
		IGMP snooping	一部制限あり※4
		MLD snooping	
		VLAN インタフェースの送信フィルタ	
		VLAN 条件を含む送信フィルタ	

使用したい機能		制限のある機能	制限の内容
	VLAN トンネリング	プロトコル VLAN	共存不可
		MAC VLAN	
		PVST+	
		シングルスパニングツリー	
		マルチプルスパニングツリー	
		IGMP snooping	
		MLD snooping	
		レイヤ 2 認証	
		VLAN インタフェースの送信フィルタ	
		VLAN 条件を含む送信フィルタ	
		sFlow 統計機能	一部制限あり※5
	L2 プロトコルフレーム透過機能 (BPDU)	PVST+	共存不可
		シングルスパニングツリー	
		マルチプルスパニングツリー	
	L2 プロトコルフレーム透過機能 (EAP)	レイヤ 2 認証	一部制限あり※2
	ポート間中継遮断機能	スパニングツリー	一部制限あり※6
		IGMP snooping	
		MLD snooping	
		GSRP aware	

注※ 1

VLAN トンネリングを使用する場合は，トランクポートでネイティブ VLAN を使用しないでください。

注※ 2

「コンフィグレーションガイド Vol.2　5　レイヤ 2 認証機能の概説」を参照してください。

注※ 3

当該機能が有効なポートでは，TPID の設定および変更はできません。

注※ 4

当該機能が有効なポートでは，Tag 変換を使用できません。

注※ 5

- 2 段以上の VLAN Tag があるフレームは，フロー統計収集の対象外フレームとして扱います。
- VLAN トンネリング機能と sFlow 統計機能を併用したとき，トンネリングポートの VLAN Tag があるフレーム（トランクポートで 2 段以上の VLAN Tag があるフレーム）は，フロー統計収集の対象フレームにならない場合があります。

注※ 6

「17.7.2　ポート間中継遮断機能使用時の注意事項」を参照してください。

表 14-3 スパニングツリーでの制限事項

使用したい機能	制限のある機能	制限の内容
PVST+	プロトコル VLAN	共存不可
	MAC VLAN	
	VLAN トンネリング	
	Tag 変換	
	L2 プロトコルフレーム透過機能（BPDU）	
	マルチプルスパニングツリー	
	レイヤ 2 認証	一部制限あり※1
シングルスパニングツリー	VLAN トンネリング	共存不可
	L2 プロトコルフレーム透過機能（BPDU）	
	マルチプルスパニングツリー	
	レイヤ 2 認証	一部制限あり※1
マルチプルスパニングツリー	VLAN トンネリング	共存不可
	L2 プロトコルフレーム透過機能（BPDU）	
	シングルスパニングツリー	
	PVST+	
	ループガード	
	レイヤ 2 認証	一部制限あり※1

注※ 1

「コンフィグレーションガイド Vol.2 5 レイヤ 2 認証機能の概説」を参照してください。

表 14-4 Ring Protocol での制限事項

使用したい機能	制限のある機能	制限の内容
Ring Protocol	レイヤ 2 認証	一部制限あり※1

注※ 1

認証を行うポートは，リングポート以外を設定してください。

表 14-5 IGMP/MLD snooping での制限事項

使用したい機能	制限のある機能	制限の内容
IGMP snooping	デフォルト VLAN	共存不可
	VLAN トンネリング	
	Tag 変換	一部制限あり※1
	レイヤ 2 認証	一部制限あり※2
MLD snooping	デフォルト VLAN	共存不可
	VLAN トンネリング	
	Tag 変換	一部制限あり※1
	レイヤ 2 認証	一部制限あり※2

注※ 1

IGMP snooping/MLD snooping を行うポートでは，Tag 変換を使用できません。

注※ 2

「コンフィグレーションガイド Vol.2　5　レイヤ 2 認証機能の概説」を参照してください。

15 MAC アドレス学習

この章では，MAC アドレス学習機能の解説と操作方法について説明します。

15.1 MAC アドレス学習の解説

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

MAC アドレス学習では，チャネルグループを一つのポートとして扱います。

15.1.1 送信元 MAC アドレス学習

すべての受信フレームを MAC アドレス学習の対象とし，送信元 MAC アドレスを学習して MAC アドレステーブルに登録します。登録した MAC アドレスは，エージング処理で削除されるまで保持します。学習は VLAN 単位に行い，MAC アドレステーブルは MAC アドレスと VLAN のペアによって管理します。同一の MAC アドレスでも VLAN が異なる場合は登録します。

15.1.2 MAC アドレス学習の移動検出

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

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

15.1.3 学習 MAC アドレスのエージング

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

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

学習したエントリを削除するまでに最大でエージング時間の 2 倍掛かることがあります。

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

15.1.4 MAC アドレスによるレイヤ 2 スイッチング

MAC アドレス学習の結果に基づいてレイヤ 2 スイッチングを行います。宛先 MAC アドレスに対応するエントリを保持している場合，学習したポートだけに中継します。

レイヤ 2 スイッチングの動作仕様を次の表に示します。

表 15-1 レイヤ 2 スイッチングの動作仕様

宛先 MAC アドレスの種類	動作概要
学習済みのユニキャスト	学習したポートへ中継します。
未学習のユニキャスト	受信した VLAN に所属する全ポートへ中継します。
ブロードキャスト	受信した VLAN に所属する全ポートへ中継します。
マルチキャスト	受信した VLAN に所属する全ポートへ中継します。ただし，IGMP snooping，MLD snooping 動作時は snooping 機能の学習結果に従って中継します。

15.1.5 スタティックエントリの登録

受信フレームによるダイナミックな学習のほかに，ユーザ指定によってスタティックに MAC アドレスを登録できます。ユニキャスト MAC アドレスに対して一つのポートまたはチャネルグループを指定できます。

ユニキャスト MAC アドレスに対してスタティックに登録を行うと，そのアドレスについてダイナミックな学習は行いません。すでに学習済みのエントリは MAC アドレステーブルから削除してスタティックエントリを登録します。また，指定された MAC アドレスが送信元のフレームをポートまたはチャネルグループ以外から受信した場合は，そのフレームを廃棄します。スタティックエントリの指定パラメータを次の表に示します。

表 15-2 スタティックエントリの指定パラメータ

項番	指定パラメータ	説明
1	MAC アドレス	ユニキャスト MAC アドレスを指定できます。
2	VLAN	このエントリを登録する VLAN を指定します。
3	送信先ポート指定	一つのポートまたはチャネルグループを指定できます。

15.1.6 MAC アドレステーブルのクリア

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

表 15-3 MAC アドレステーブルをクリアする契機

契機	説明
ポートダウン※1	該当ポートから学習したエントリを削除します。
チャネルグループダウン※2	該当チャネルグループから学習したエントリを削除します。
運用コマンド clear mac-address-table の実行	MAC アドレステーブルをクリアします。
スパニングツリーのトポロジー変更	[本装置でスパニングツリーを構成] トポロジー変更を検出した時に MAC アドレステーブルをクリアします。
	[スパニングツリーと Ring Protocol を併用しているネットワーク構成で本装置がリングノードとして動作] Ring Protocol と併用している装置がトポロジー変更を検出した時に送信するフラッシュ制御フレームを受信した場合，MAC アドレステーブルをクリアします。

契機	説明
GSRP のマスタ／バックアップ切り替え	［本装置が GSRP aware として動作］ GSRP スイッチがマスタ状態になった時に送信される GSRP Flush request フレームを受信した場合，MAC アドレステーブルをクリアします。
	［GSRP と Ring Protocol を併用しているネットワーク構成で本装置がリングノードとして動作］ Ring Protocol と併用している装置がマスタ状態になった時に送信するフラッシュ制御フレームを受信した場合，MAC アドレステーブルをクリアします。
Ring Protocol による経路の切り替え	［本装置がマスタノードとして動作］ 経路切り替え時に MAC アドレステーブルをクリアします。
	［本装置がトランジットノードとして動作］ 経路切り替え時にマスタノードから送信されるフラッシュ制御フレームを受信した場合，MAC アドレステーブルをクリアします。 フラッシュ制御フレーム受信待ち保護時間のタイムアウト時に MAC アドレステーブルをクリアします。
	多重障害監視機能適用時，バックアップリングの切り替え／切り戻しに伴い共有ノードから送信されるフラッシュ制御フレームを受信した場合，MAC アドレステーブルをクリアします。
	経路切り替え時にマスタノードから送信される隣接リング用フラッシュ制御フレームを受信した場合，MAC アドレステーブルをクリアします。
他装置のアップリンク・リダンダント機能によるプライマリポートとセカンダリポートの切り替え	プライマリポートからセカンダリポートへの切り替え時，およびセカンダリポートからプライマリポートへの切り戻し時に他装置から送信されるフラッシュ制御フレームを受信した場合，MAC アドレステーブルをクリアします。

注※ 1

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

注※ 2

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

15.1.7 注意事項

（1） レイヤ 2 認証機能を使用時のエージング時間について

学習したエントリのエージング時間はコンフィグレーションで設定可能ですが，レイヤ 2 認証機能を使用時は，下記のエージング時間で動作します。

表 15-4　レイヤ 2 認証機能使用時のエージング時間

レイヤ 2 認証機能 設定状態	MAC アドレステーブル エージング時間設定状態	エージング動作	
		動作	エージング時間
下記認証機能のいずれかが動作中 1. IEEE802.1X •認証モード ポート単位認証（静的）または ポート単位認証（動的） •無通信監視機能有効 2. Web 認証 •認証モード 固定 VLAN モードまたは ダイナミック VLAN モード •無通信監視機能有効 3. MAC 認証 •認証モード 固定 VLAN モードまたは ダイナミック VLAN モード •無通信監視機能有効	エージング時間を 0 秒で設定	×	－
	エージング時間を 10 ～ 300 秒の範囲内で設定	○	300 秒
	エージング時間を 301 ～ 1000000 秒の範囲内で設定	○	設定時間
	未設定	○	300 秒
上記以外	エージング時間を 0 秒で設定	×	－
	エージング時間を 10 ～ 300 秒の範囲内で設定	○	設定時間
	エージング時間を 301 ～ 1000000 秒の範囲内で設定	○	設定時間
	未設定	○	300 秒

（凡例）
○：エージングする
×：エージングしない
－：該当なし

15.2 MAC アドレス学習のコンフィグレーション

15.2.1 コンフィグレーションコマンド一覧

MAC アドレス学習のコンフィグレーションコマンド一覧を次の表に示します。

表 15-5 コンフィグレーションコマンド一覧

コマンド名	説明
mac-address-table aging-time	MAC アドレス学習のエージング時間を設定します。
mac-address-table static	スタティックエントリを設定します。

15.2.2 エージング時間の設定

[設定のポイント]

MAC アドレス学習のエージング時間を変更できます。設定は装置単位です。設定しない場合，エージング時間は 300 秒です。

[コマンドによる設定]

1. **(config)# mac-address-table aging-time 100**
   エージング時間を 100 秒に設定します。

[注意事項]

レイヤ 2 認証機能を併用しているときに，本コマンドで設定した 10 ～ 300 秒の範囲のエージング時間は 300 秒となります。詳細は，「15.1.7 注意事項 (1) レイヤ 2 認証機能を使用時のエージング時間について」を参照してください。

15.2.3 スタティックエントリの設定

スタティックエントリを登録すると，指定した MAC アドレスについて MAC アドレス学習をしないで，常に登録したエントリに従ってフレームを中継するため，MAC アドレスのエージングによるフラッディングを回避できます。本装置に直接接続したサーバなどのように，ポートの移動がなく，かつトラフィック量の多い端末などに有効な機能です。

スタティックエントリには，MAC アドレス，VLAN および出力先を指定します。出力先はポート，チャネルグループのどちらかを指定します。

(1) 出力先にポートを指定するスタティックエントリ

[設定のポイント]

出力先にポートを指定した例を示します。

[コマンドによる設定]

1. **(config)# mac-address-table static 0000.8700.1122 vlan 10 interface gigabitethernet 0/4**
   VLAN 10 で，宛先 MAC アドレス 0000.8700.1122 のフレームの出力先をポート 0/4 に設定します。

［注意事項］

1. VLAN 10 で，送信元 MAC アドレス 0000.8700.1122 のフレームをポート 0/4 以外から受信した場合は廃棄します。
2. 指定 VLAN が，レイヤ 2 認証機能でポートに自動割り当てされた VLAN と一致したときは，設定できません。

（2） 出力先にリンクアグリゲーションを指定するスタティックエントリ

［設定のポイント］

出力先にリンクアグリゲーションを指定した例を示します。

［コマンドによる設定］

1. **(config)# mac-address-table static 0000.8700.1122 vlan 10 interface port-channel 5**

   VLAN 10 で，宛先 MAC アドレス 0000.8700.1122 のフレームの出力先をチャネルグループ 5 に設定します。

［注意事項］

VLAN 10 で，送信元 MAC アドレス 0000.8700.1122 のフレームをチャネルグループ 5 以外から受信した場合は廃棄します。

15.3 MAC アドレス学習のオペレーション

15.3.1 運用コマンド一覧

MAC アドレス学習の運用コマンド一覧を次の表に示します。

表 15-6 運用コマンド一覧

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

15.3.2 MAC アドレス学習の状態の確認

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

運用コマンド show mac-address-table では，MAC アドレス学習によって登録したエントリ，スタティックエントリ，レイヤ 2 認証機能，IGMP snooping および MLD snooping によって登録したエントリを表示します。

図 15-1 show mac-address-table の実行結果

```
> show mac-address-table

Date 20XX/06/09 21:30:08 UTC
Aging time : 300
MAC address         VLAN    Type      Port-list
0000.87cf.fd5d         1    Dot1x     0/1
0000.8703.0110         1    Dynamic   0/1
0000.8703.0132         1    Dynamic   0/2
0000.8700.00fb         1    Snoop     0/3
       :
       :

>
```

15.3.3 MAC アドレス学習数の確認

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

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

図 15-2 show mac-address-table（learning-counter パラメータ指定）の実行結果

```
> show mac-address-table learning-counter

Date 20XX/06/09 21:47:47 UTC
 Port          Count
 0/1               0
 0/2           13961
 0/3              12
 0/4               2
       :
       :
       :
 ChGr:8            0
 ChGr:62          13
 ChGr:63           1
 ChGr:64          34

>
```

16 VLAN

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

16.1 VLAN 基本機能の解説

この節では，VLAN の概要を説明します。

16.1.1 VLAN の種類

本装置がサポートする VLAN の種類を次の表に示します。

表 16-1 サポートする VLAN の種類

項目	概要
ポート VLAN	ポート単位に VLAN のグループを分けます。
プロトコル VLAN	プロトコル単位に VLAN のグループを分けます。
MAC VLAN	送信元の MAC アドレス単位に VLAN のグループを分けます。

16.1.2 ポートの種類

(1) 解説

本装置は，ポートの設定によって使用できる VLAN が異なります。使用したい VLAN の種類に応じて各ポートの種類を設定する必要があります。ポートの種類を次の表に示します。

表 16-2 ポートの種類

ポートの種類	概要	使用する VLAN
アクセスポート	ポート VLAN として Untagged フレームを扱います。 このポートでは，すべての Untagged フレームを一つのポート VLAN で扱います。	ポート VLAN MAC VLAN
プロトコルポート	プロトコル VLAN として Untagged フレームを扱います。 このポートでは，フレームのプロトコルによって VLAN を決定します。 Tagged フレームを受信したときは廃棄します。	プロトコル VLAN ポート VLAN
MAC ポート	MAC VLAN として Untagged フレームを扱います。 このポートでは，フレームの送信元 MAC アドレスによって VLAN を決定します。 Tagged フレームを受信したときは，コンフィグレーションの設定に従います。詳細は「16.7.4 MAC ポートのオプション機能」を参照してください。	MAC VLAN ポート VLAN
トランクポート	すべての種類の VLAN で Tagged フレームを扱います。 このポートでは，VLAN Tag によって VLAN を決定します。 Untagged フレームを受信したときは，ネイティブ VLAN で扱います。	ポート VLAN プロトコル VLAN MAC VLAN
トンネリングポート	VLAN トンネリングのポート VLAN として，フレームの Untagged と Tagged を区別しないで扱います。このポートでは，すべてのフレームを一つのポート VLAN で扱います。	ポート VLAN

ポートの種類ごとの，使用できる VLAN の種類を次の表に示します。VLAN Tag を扱うトランクポートはすべての VLAN で同じポートを使用できます。

表 16-3 ポート上で使用できる VLAN

ポートの種類	VLAN の種類		
	ポート VLAN	プロトコル VLAN	MAC VLAN
アクセスポート	○	×	○
プロトコルポート	○	○	×
MAC ポート	○	×	○
トランクポート	○	○	○
トンネリングポート	○	×	×

（凡例） ○：使用できる ×：使用できない

（2） ポートのネイティブ VLAN

アクセスポート，トンネリングポート以外のポート（プロトコルポート，MAC ポート，トランクポート）では，それぞれの設定と一致しないフレームを受信する場合があります。例えば，プロトコルポートで IPv4 プロトコルだけ設定していたときに IPv6 のフレームを受信した場合です。アクセスポート，トンネリングポート以外ではこのようなフレームを扱うためにポート VLAN を一つ設定することができます。この VLAN のことを，各ポートでのネイティブ VLAN と呼びます。

アクセスポート，トンネリングポート以外の各ポートでは，ポートごとに作成済みのポート VLAN をネイティブ VLAN に設定できます。コンフィグレーションで指定がないポートは，VLAN 1（デフォルト VLAN）がネイティブ VLAN になります。

16.1.3 デフォルト VLAN

（1） 概要

本装置では，コンフィグレーションが未設定の状態であっても，装置の起動後すぐにレイヤ 2 中継ができます。このとき，すべてのポートはアクセスポートとなり，デフォルト VLAN と呼ぶ VLAN ID 1 の VLAN に属します。デフォルト VLAN は常に存在し，VLAN ID「1」は変更できません。

（2） デフォルト VLAN から除外するポート

アクセスポートは，コンフィグレーションが未設定の場合は VLAN 1（デフォルト VLAN）に属します。しかし，コンフィグレーションによってデフォルト VLAN の自動的な所属から除外する場合があります。次に示すポートはデフォルト VLAN に自動的に所属しなくなります。

- アクセスポートで VLAN 1 以外を指定したポート
- VLAN トンネリング機能を設定した場合の全ポート
- ミラーポート

アクセスポート以外のポート（プロトコルポート，MAC ポート，トランクポート，トンネリングポート）は自動的に VLAN に所属することはありません。

16.1.4 VLAN の優先順位

（1） フレーム受信時の VLAN 判定の優先順位

フレームを受信したとき，受信したフレームの VLAN を判定します。VLAN 判定の優先順位を次の表に

示します。

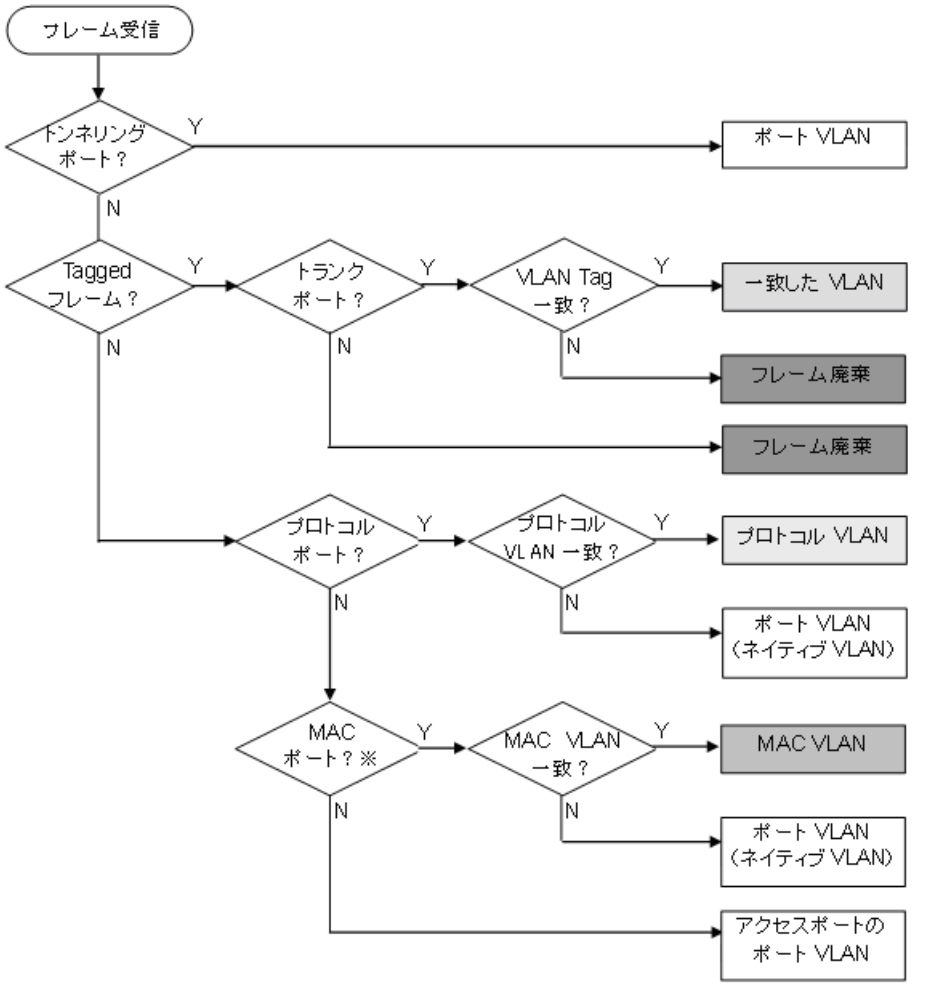
表 16-4　VLAN 判定の優先順位

ポートの種類	VLAN 判定の優先順位
アクセスポート	ポート VLAN
プロトコルポート	プロトコル VLAN ＞ポート VLAN（ネイティブ VLAN）
MAC ポート	VLAN Tag※＞ MAC VLAN ＞ポート VLAN（ネイティブ VLAN）
トランクポート	VLAN Tag ＞ポート VLAN（ネイティブ VLAN）
トンネリングポート	ポート VLAN

注※
コンフィグレーションにより Tagged フレームも扱えます。詳細は「16.7.4　MAC ポートのオプション機能」を参照してください。

VLAN 判定のアルゴリズムを次の図に示します。

図 16-1　VLAN 判定のアルゴリズム



注※
コンフィグレーション設定により Tagged フレームも扱えます。

16.1.5 VLAN Tag

（1） 概要

IEEE 802.1Q 規定による VLAN Tag（イーサネットフレーム中に Tag と呼ばれる識別子を挿入する方法）を使用して，一つのポートに複数の VLAN を構築できます。

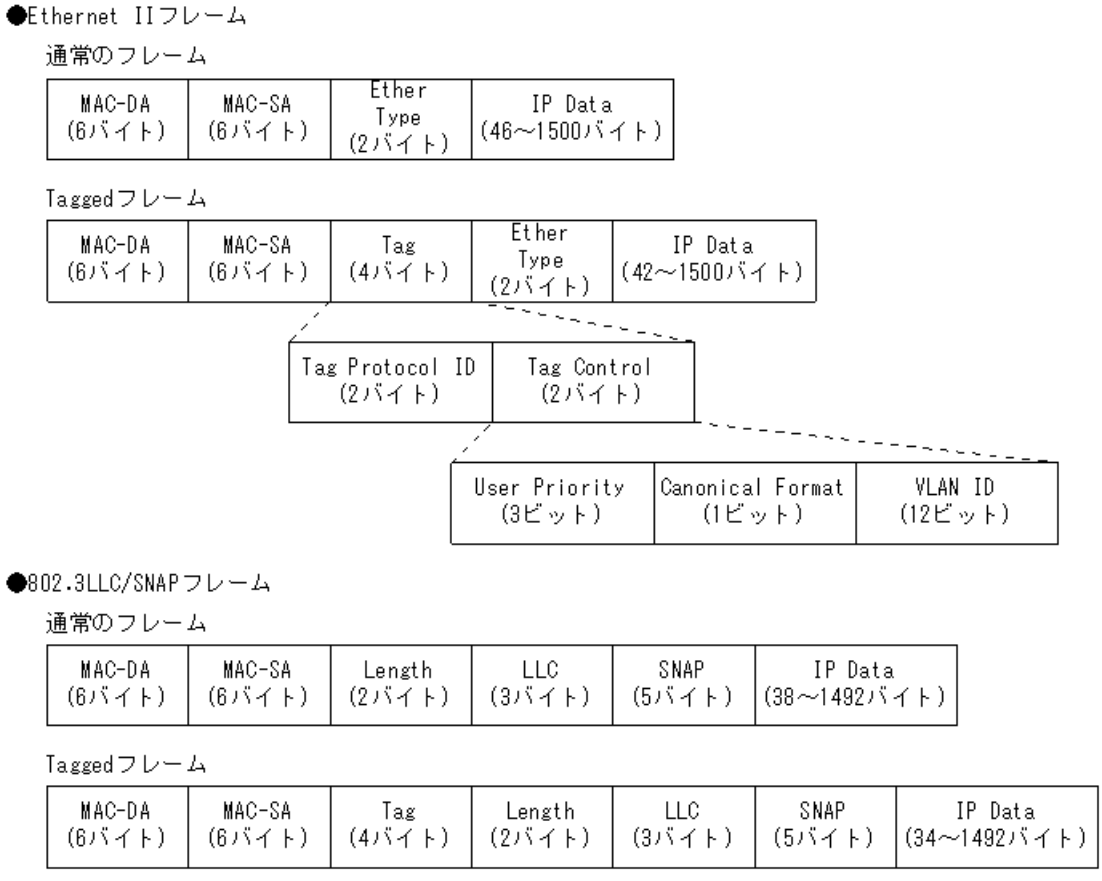
VLAN Tag はトランクポート，MAC ポートで使用します。トランクポート，MAC ポートはその対向装置も VLAN Tag を認識できなければなりません。

（2） プロトコル仕様

VLAN Tag は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（=VLAN ID）を離れたセグメントへと伝えることができます。

Tagged フレームのフォーマットを次の図に示します。VLAN Tag を挿入するイーサネットフレームのフォーマットは，Ethernet V2 フォーマットと 802.3 フォーマットの 2 種類があります。

図 16-2 Tagged フレームのフォーマット



VLAN Tag のフィールドの説明を次の表に示します。

表 16-5 VLAN Tag のフィールド

フィールド	説明	本装置の条件
TPID (Tag Protocol ID)	IEEE802.1Q VLAN Tag が続くことを示す Ether Type 値を示します。	ポートごとに任意の値を設定できます。
User Priority	IEEE802.1D のプライオリティを示します。	コンフィグレーションで 8 段階のプライオリティレベルを選択できます。
CF (Canonical Format)	MAC ヘッダ内の MAC アドレスが標準フォーマットに従っているかどうかを示します。	本装置では標準 (0) だけをサポートします。
VLAN ID	VLAN ID を示します。※	ユーザが使用できる VLAN ID は 1 ～ 4094 です。

注※

Tag 変換を使用している場合，Tag 変換で設定した VLAN ID を使用します。詳細は「17.3 Tag 変換の解説」を参照してください。VLAN ID=0 を受信した場合は，Untagged フレームと同様の扱いになります。VLAN ID=0 を送信することはありません。

本装置が中継するフレームの User Priority は，受信したフレームの User Priority と同じです。また，User Priority のデフォルト値は下記のとおりです。

- 受信したフレームが中継フレームの場合：User Priority のデフォルト値は 3
- 自発送信フレームの場合：User Priority のデフォルト値は 7

なお，送信するフレームの User Priority はコンフィグレーションで変更することができます。User Priority の変更については，下記を参照してください。

- 中継フレーム：「コンフィグレーションガイド Vol.2 3.4 マーカー解説」
- 自発送信フレーム：「コンフィグレーションガイド Vol.2 3.10 自発フレームのユーザ優先度の解説」

16.1.6 VLAN 使用時の注意事項

(1) 他機能との共存

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

16.2 VLAN 基本機能のコンフィグレーション

16.2.1 コンフィグレーションコマンド一覧

VLAN 基本機能のコンフィグレーションコマンド一覧を次の表に示します。

表 16-6 コンフィグレーションコマンド一覧

コマンド名	説明
name	VLAN の名称を設定します。
state	VLAN の状態 (停止 / 開始) を設定します。
switchport access	アクセスポートの VLAN を設定します。
switchport dot1q ethertype	ポートごとに VLAN Tag の TPID を設定します。
switchport mac	MAC VLAN ポートの情報を設定します。
switchport mode	ポートの種類（アクセス，プロトコル，MAC，トランク，トンネリング）を設定します。
switchport protocol	プロトコルポートの VLAN を設定します。
switchport trunk	トランクポートの VLAN を設定します。
vlan	VLAN を作成します。また，VLAN コンフィグレーションモードで VLAN に関する項目を設定します。
vlan-dot1q-ethertype	VLAN Tag の TPID のデフォルト値を設定します。

16.2.2 VLAN の設定

［設定のポイント］

VLAN を作成します。新規に VLAN を作成するためには，VLAN ID と VLAN の種類を指定します。VLAN の種類を省略した場合はポート VLAN を作成します。VLAN ID リストによって複数の VLAN を一括して設定することもできます。

コンフィグレーションコマンド vlan によって，VLAN コンフィグレーションモードに移行します。作成済みの VLAN を指定した場合は，モードの移行だけとなります。VLAN コンフィグレーションモードでは VLAN のパラメータを設定できます。

なお，ここでは VLAN の種類によらない共通した設定について説明します。ポート VLAN，プロトコル VLAN，MAC VLAN のそれぞれについては次節以降を参照してください。

［コマンドによる設定］

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

   VLAN ID 10 のポート VLAN を作成し，VLAN 10 の VLAN コンフィグレーションモードに移行します。

2. **(config-vlan)# name "PORT BASED VLAN 10"**
   (config-vlan)# exit

   作成したポート VLAN 10 の名称を”PORT BASED VLAN 10”に設定します。

3. **(config)# vlan 100-200**

   VLAN ID 100 ～ 200 のポート VLAN を一括して作成します。また，VLAN 100 ～ 200 の VLAN コン

フィグレーションモードに移行します。

4. **(config-vlan)# state suspend**
   (config-vlan)# exit
   作成した VLAN ID 100 ～ 200 のポート VLAN を一括して停止状態にします。

16.2.3 ポートの設定

［設定のポイント］

イーサネットインタフェースコンフィグレーションモード，ポートチャネルインタフェースコンフィグレーションモードでポートの種類を設定します。ポートの種類は使用したい VLAN の種類に合わせて設定します。

なお，ポート VLAN，プロトコル VLAN，MAC VLAN それぞれの詳細な設定方法については次節以降を参照してください。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/3**
   ポート 0/3 のイーサネットインタフェースコンフィグレーションモードに移行します。

2. **(config-if)# switchport mode access**
   (config-if)# exit
   ポート 0/3 をアクセスポートに設定します。ポート 0/3 はポート VLAN で Untagged フレームを扱うポートになります。

3. **(config)# interface port-channel 3**
   チャネルグループ 3 のポートチャネルインタフェースコンフィグレーションモードに移行します。

4. **(config-if)# switchport mode trunk**
   (config-if)# exit
   チャネルグループ 3 をトランクポートに設定します。ポートチャネル 3 は Tagged フレームを扱うポートになります。

16.2.4 トランクポートの設定

［設定のポイント］

トランクポートは VLAN の種類に関係なく，すべての VLAN で使用でき，Tagged フレームを扱います。また，イーサネットインタフェースおよびポートチャネルインタフェースで使用できます。

トランクポートは，コンフィグレーションコマンド switchport mode を設定しただけではどの VLAN にも所属していません。このポートで扱う VLAN はコンフィグレーションコマンド switchport trunk allowed vlan によって設定します。

VLAN の追加と削除は，コンフィグレーションコマンド switchport trunk vlan add および switchport trunk vlan remove によって行います。すでにコンフィグレーションコマンド switchport trunk allowed vlan を設定した状態でもう一度コンフィグレーションコマンド switchport trunk allowed vlan を実行すると，指定した VLAN ID リストに置き換わります。

［コマンドによる設定］

1. **(config)# vlan 10-20,100,200-300**

```
(config-vlan)# exit
(config)# interface gigabitethernet 0/3
(config-if)# switchport mode trunk
```

VLAN 10 ～ 20，100，200 ～ 300 を作成します。また，ポート 0/3 のイーサネットインタフェースコンフィグレーションモードに移行し，トランクポートに設定します。この状態では，ポート 0/1 はどの VLAN にも所属していません。

2. **(config-if)# switchport trunk allowed vlan 10-20**
   ポート 0/3 に VLAN 10 ～ 20 を設定します。ポート 0/3 は VLAN 10 ～ 20 の Tagged フレームを扱います。

3. **(config-if)# switchport trunk allowed vlan add 100**
   ポート 0/3 で扱う VLAN に VLAN 100 を追加します。

4. **(config-if)# switchport trunk allowed vlan remove 15,16**
   ポート 0/3 で扱う VLAN から VLAN 15 および VLAN 16 を削除します。この状態で，ポート 0/3 は VLAN 10 ～ 14，17 ～ 20，VLAN 100 の Tagged フレームを扱います。

5. **(config-if)# switchport trunk allowed vlan 200-300**
   (config-if)# exit
   ポート 0/3 で扱う VLAN を VLAN 200 ～ 300 に設定します。以前の設定はすべて上書きされ，VLAN 200 ～ 300 の Tagged フレームを扱います。

［注意事項］

トランクポートで Untagged フレームを扱うためには，ネイティブ VLAN を設定します。詳しくは，「16.4.3　トランクポートのネイティブ VLAN の設定」を参照してください。

16.2.5　VLAN Tag の TPID の設定

［設定のポイント］

本装置は，VLAN Tag の TPID を任意の値に設定することができます。コンフィグレーションコマンド vlan-dot1q-ethertype で装置のデフォルト値を，コンフィグレーションコマンド switchport dot1q ethertype でポートごとの値を設定します。ポートごとの値を設定していないポートは装置のデフォルト値で動作します。

ポートごとの TPID の設定は，イーサネットインタフェースコンフィグレーションモードで設定します。

［コマンドによる設定］

1. **(config)# vlan-dot1q-ethertype 9100**
   装置のデフォルト値を 0x9100 に設定します。すべてのポートにおいて VLAN Tag を TPID 0x9100 として動作します。

2. **(config)# interface gigabitethernet 0/3**
   ポート 0/3 のイーサネットインタフェースコンフィグレーションモードに移行します。

3. **(config-if)# switchport dot1q ethertype 8100**
   (config-if)# exit
   ポート 0/3 の TPID を 0x8100 に設定します。ポート 0/3 は VLAN Tag を TPID 0x8100 として動作します。そのほかのポートは装置のデフォルト値である 0x9100 で動作します。

［注意事項］

TPID は，フレーム上では Untagged フレームの EtherType と同じ位置を使用します。そのため，IPv4 の EtherType である 0x0800 など，EtherType として使用している値を設定するとネットワークが正しく構築できないおそれがあります。EtherType 値として未使用の値を設定してください。

16.3 ポート VLAN の解説

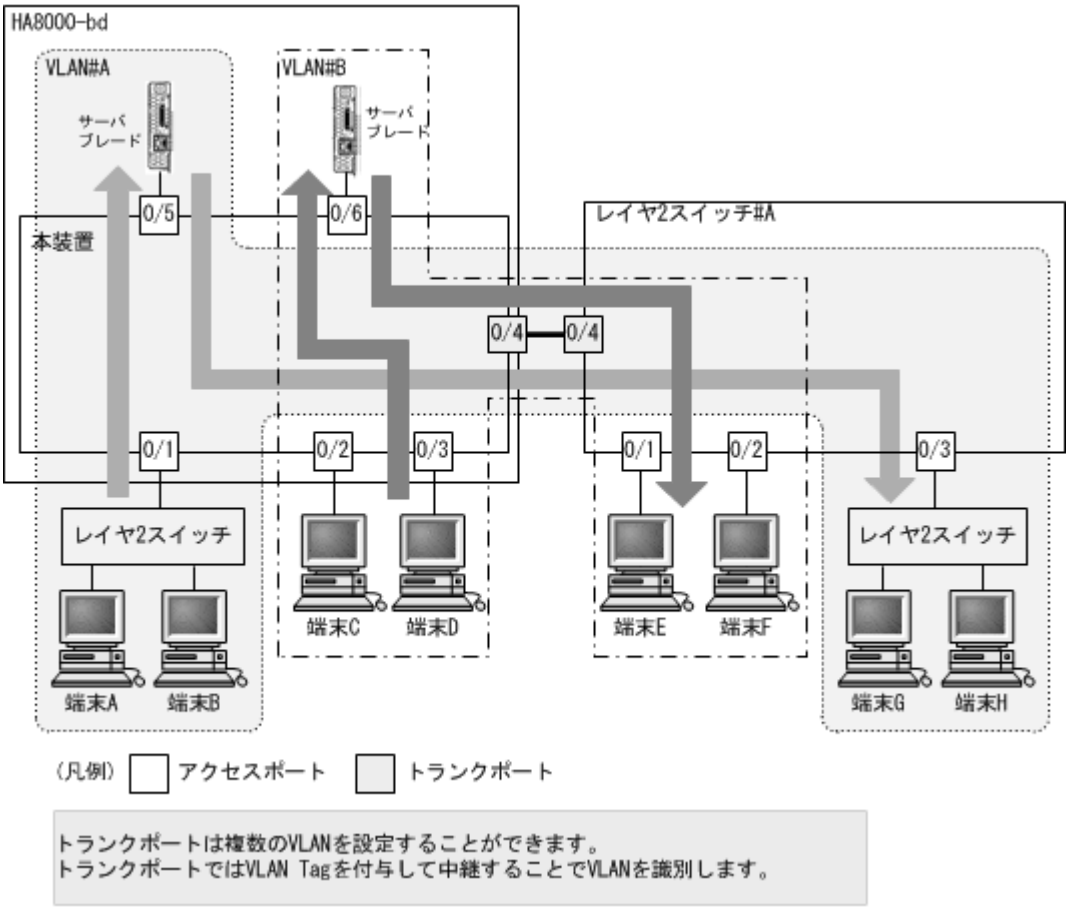
ポート単位に VLAN のグループ分けを行います。

16.3.1 アクセスポートとトランクポート

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

ポート VLAN の構成例を次の図に示します。ポート 0/1 ～ 0/3，0/5 ～ 0/6 はアクセスポートとしてポート VLAN を設定します。本装置のポート 0/4 とレイヤ 2 スイッチ #A の間はトランクポートで接続します。そのとき，VLAN Tag を使います。

図 16-3 ポート VLAN の構成例



16.3.2 ネイティブ VLAN

プロトコルポート，MAC ポート，トランクポートにはコンフィグレーションに一致しないフレームを扱うネイティブ VLAN があります。各ポートのネイティブ VLAN はコンフィグレーションで指定しない場合は VLAN 1（デフォルト VLAN）です。また，ほかのポート VLAN にコンフィグレーションで変更することもできます。

例えば，「図 16-3　ポート VLAN の構成例」のトランクポートにおいて VLAN#B をネイティブ VLAN に設定すると，VLAN#B はトランクポートでも Untagged フレームで中継します。

16.3.3　ポート VLAN 使用時の注意事項

（1） アクセスポートでの Tagged フレームに関する注意事項

アクセスポートは Untagged フレームを扱うポートです。Tagged フレームを受信した場合は廃棄します。また，送信することもできません。なお，VLAN Tag 値が VLAN の ID と一致する場合および 0 の場合は，受信時に Untagged フレームと同じ扱いになります。これらのフレームを送信することはありません。

16.4 ポート VLAN のコンフィグレーション

16.4.1 コンフィグレーションコマンド一覧

ポート VLAN のコンフィグレーションコマンド一覧を次の表に示します。

表 16-7 コンフィグレーションコマンド一覧

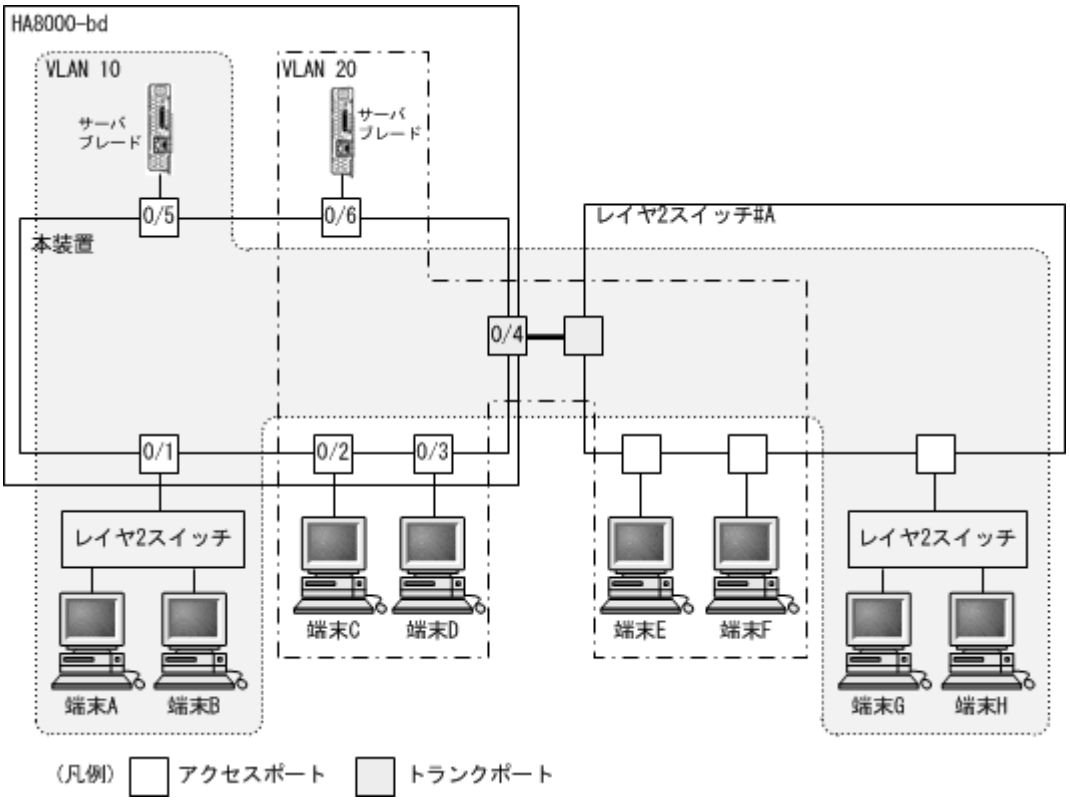
コマンド名	説明
switchport access	アクセスポートの VLAN を設定します。
switchport mode	ポートの種類（アクセス，トランク）を設定します。
switchport trunk	トランクポートの VLAN を設定します。
vlan	ポート VLAN を作成します。また，VLAN コンフィグレーションモードで VLAN に関する項目を設定します。

16.4.2 ポート VLAN の設定

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

ポート 0/1，0/5 はポート VLAN 10 を設定します。ポート 0/2，0/3，0/6 はポート VLAN 20 を設定します。ポート 0/4 はトランクポートでありすべての VLAN を設定します。

図 16-4 ポート VLAN の設定例



（1） ポート VLAN の作成

［設定のポイント］

ポート VLAN を作成します。VLAN を作成する際に VLAN ID だけを指定して VLAN の種類を指定しないで作成するとポート VLAN となります。

［コマンドによる設定］

1. **(config)# vlan 10,20**
   (config-vlan)# exit
   VLAN ID 10，VLAN ID 20 をポート VLAN として作成します。

(2) アクセスポートの設定

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

［設定のポイント］

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

［コマンドによる設定］

1. **(config)#** interface range tengigabitethernet 0/1, gigabitethernet 0/5
   ポート 0/1，0/5 のイーサネットインタフェースコンフィグレーションモードに移行します。

2. **(config-if-range)# switchport mode access**
   (config-if-range)# switchport access vlan 10
   (config-if-range)# exit
   ポート 0/1，0/5 をアクセスポートに設定します。また，VLAN 10 を設定します。

3. **(config)# i**nterface range tengigabitethernet 0/2, gigabitethernet 0/3, gigabitethernet 0/6
   ポート 0/2，0/3，0/6 のイーサネットインタフェースコンフィグレーションモードに移行します。ポート 0/2，0/3，0/6 は同じコンフィグレーションとなるため，一括して設定します。

4. **(config-if-range)# switchport mode access**
   (config-if-range)# switchport access vlan 20
   (config-if-range)# exit
   ポート 0/2，0/3，0/6 をアクセスポートに設定します。また，VLAN 20 を設定します。

(3) トランクポートの設定

［設定のポイント］

Tagged フレームを扱うポートはトランクポートとして設定し，そのトランクポートに VLAN を設定します。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/4**
   ポート 0/4 のイーサネットインタフェースコンフィグレーションモードに移行します。

2. **(config-if)# switchport mode trunk**
   (config-if)# switchport trunk allowed vlan 10,20

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

ポート 0/4 をトランクポートに設定します。また，VLAN 10，20 を設定します。

16.4.3 トランクポートのネイティブ VLAN の設定

［設定のポイント］

トランクポートで Untagged フレームを扱いたい場合，ネイティブ VLAN を設定します。ネイティブ VLAN はポート VLAN または MAC VLAN を設定できます。
ネイティブ VLAN の VLAN ID をコンフィグレーションコマンド switchport trunk allowed vlan で指定すると，トランクポートで Untagged フレームを扱う VLAN となります。ネイティブ VLAN は，コンフィグレーションで明示して指定しない場合は VLAN 1（デフォルト VLAN）です。
トランクポート上で，デフォルト VLAN で Tagged フレーム（VLAN ID 1 の VLAN Tag）を扱いたい場合は，ネイティブ VLAN をほかの VLAN に変更してください。

［コマンドによる設定］

1. **(config)# vlan 10,20**
   (config-vlan)# exit
   VLAN ID 10，VLAN ID 20 をポート VLAN として作成します。

2. **(config)# vlan 300 mac-based**
   (config-vlan)# exit
   VLAN ID 300 を MAC VLAN として作成します。

3. **(config)# interface gigabitethernet 0/4**
   (config-if)# switchport mode trunk
   ポート 0/4 のイーサネットインタフェースコンフィグレーションモードに移行します。また，トランクポートとして設定します。この状態で，トランクポート 0/4 のネイティブ VLAN はデフォルト VLAN です。

4. **(config-if)# switchport trunk allowed vlan 1,10,20,300**
   (config-if)# switchport trunk native vlan 300
   (config-if)# exit
   トランクポート 0/4 に allowed vlan に VLAN1，10，20，300 を設定します。また，ネイティブ VLAN に VLAN 300 を設定します。VLAN 1（デフォルト VLAN），VLAN 10，20 は Tagged フレームを扱い，ネイティブ VLAN である VLAN300 は Untagged フレームを扱います。

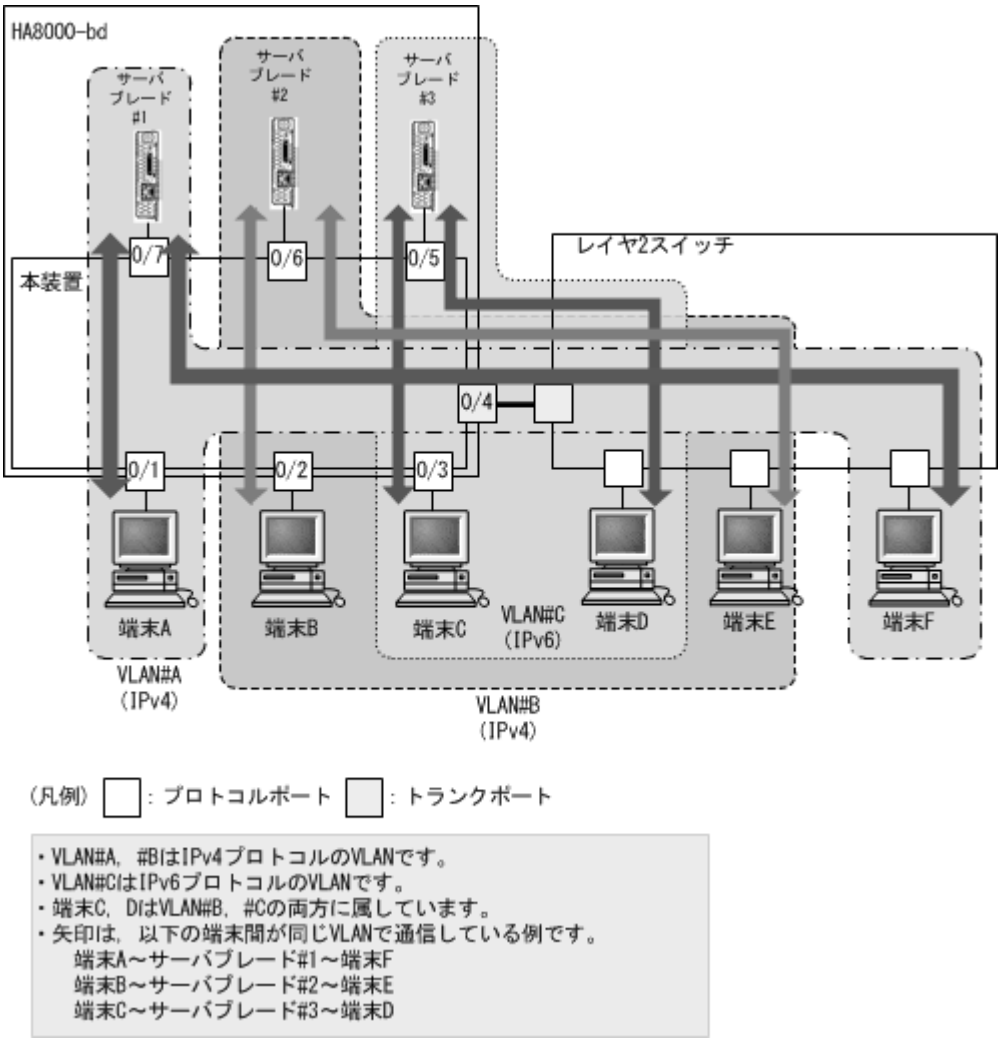
16.5 プロトコル VLAN の解説

16.5.1 概要

プロトコル単位で VLAN のグループ分けを行います。IPv4 や IPv6 といったプロトコルごとに異なる VLAN を構成できます。複数のプロトコルを同一のプロトコル VLAN に設定することもできます。

プロトコル VLAN の構成例を次の図に示します。VLAN#A，#B を IPv4 プロトコルで構成し，VLAN#C を IPv6 プロトコルで構成した例を示しています。

図 16-5 プロトコル VLAN の構成例



16.5.2 プロトコルの識別

プロトコルの識別には次の 3 種類の値を使用します。

表 16-8 プロトコルを識別する値

識別する値	概要
EtherType 値	EthernetV2 形式フレームの EtherType 値によってプロトコルを識別します。

識別する値	概要
LLC 値	802.3 形式フレームの LLC 値 (DSAP,SSAP) によってプロトコルを識別します。
SNAP EtherType 値	802.3 形式フレームの EtherType 値によってプロトコルを識別します。フレームの LLC 値が AA AA 03 であるフレームだけが対象となります。

プロトコルは，コンフィグレーションによってプロトコルを作成し VLAN に対応付けます。一つのプロトコル VLAN に複数のプロトコルを対応付けることもできます。

16.5.3 プロトコルポートとトランクポート

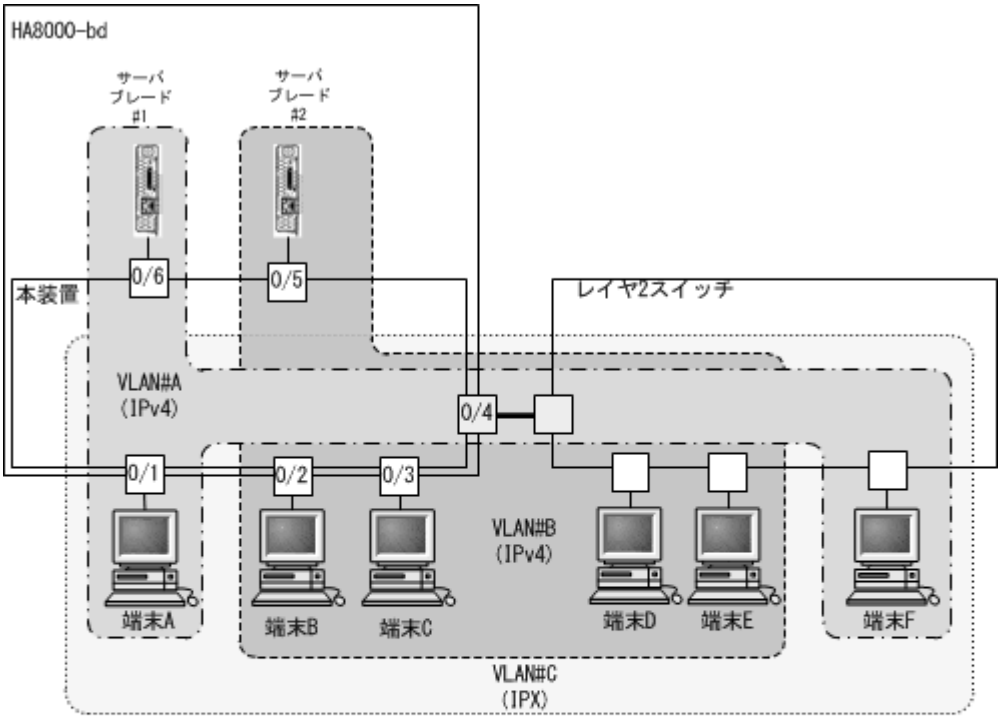
プロトコルポートは Untagged フレームのプロトコルを識別します。プロトコル VLAN として使用するポートはプロトコルポートを設定します。プロトコルポートには複数のプロトコルで異なる VLAN を割り当てることもできます。複数のプロトコル VLAN をほかの LAN スイッチなどに接続するためにはトランクポートを使用します。なお，トランクポートは VLAN Tag によって VLAN を識別するため，プロトコルによる識別は行いません。

16.5.4 プロトコルポートのネイティブ VLAN

プロトコルポートでコンフィグレーションに一致しないプロトコルのフレームを受信した場合はネイティブ VLAN で扱います。ネイティブ VLAN は，コンフィグレーションで指定しない場合は VLAN 1（デフォルト VLAN）です。また，ほかのポート VLAN にコンフィグレーションで変更することもできます。

次の図に，プロトコルポートでネイティブ VLAN を使用する構成例を示します。図の構成は，IPX プロトコルをネットワーク全体で一つの VLAN とし，そのほか（IPv4 など）のプロトコルについてはポート VLAN で VLAN を分ける例です。VLAN#A，VLAN#B を各ポートのネイティブ VLAN として設定します。なお，この構成例では，VLAN#A，VLAN#B も IPv4 のプロトコル VLAN として設定することもできます。

図 16-6　プロトコルポートでネイティブ VLAN を使用する構成例



（凡例）□：プロトコルポート　□：トランクポート

・VLAN#A, #Bはポート VLANでネイティブVLANとして設定します。
・VLAN#Cは IPXプロトコルのVLANです。
・すべての端末(A～F)は IPXプロトコルVLANに属しています。
・以下の端末およびサーバブレードは異なるポート VLANに属しています。
　端末A, サーバブレード#1, 端末F
　端末B, C, サーバブレード#2, 端末D, E

16.6 プロトコル VLAN のコンフィグレーション

16.6.1 コンフィグレーションコマンド一覧

プロトコル VLAN のコンフィグレーションコマンド一覧を次の表に示します。

表 16-9 コンフィグレーションコマンド一覧

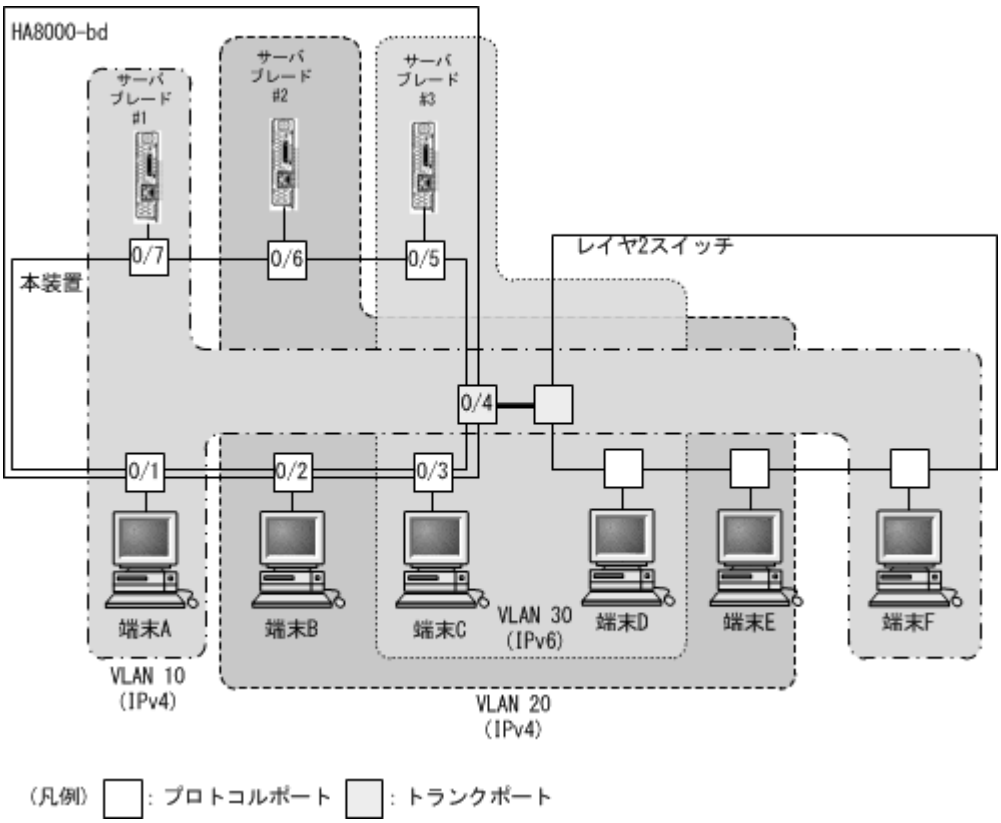
コマンド名	説明
protocol	プロトコル VLAN で VLAN を識別するプロトコルを設定します。
switchport mode	ポートの種類（プロトコル，トランク）を設定します。
switchport protocol	プロトコルポートの VLAN を設定します。
switchport trunk	トランクポートの VLAN を設定します。
vlan-protocol	プロトコル VLAN 用のプロトコル名称とプロトコル値を設定します。
vlan protocol-based	プロトコル VLAN を作成します。また，VLAN コンフィグレーションモードで VLAN に関する項目を設定します。

16.6.2 プロトコル VLAN の作成

プロトコル VLAN を設定する手順を以下に示します。ここでは，次の図に示す本装置 #1 の設定例を示します。

ポート 0/1，0/7 は IPv4 プロトコル VLAN 10 を設定します。ポート 0/2，0/6 は IPv4 プロトコル VLAN 20 を設定します。ポート 0/3 は VLAN 20 と同時に IPv6 プロトコル VLAN 30 にも所属します。ポート 0/4 はトランクポートであり，すべての VLAN を設定します。

図 16-7　プロトコル VLAN の設定例



(1) VLAN を識別するプロトコルの作成

[設定のポイント]

プロトコル VLAN は，VLAN を作成する前に識別するプロトコルを vlan-protocol コマンドで設定します。プロトコルは，プロトコル名称とプロトコル値を設定します。一つの名称に複数のプロトコル値を関連づけることもできます。

IPv4 プロトコルは，IPv4 の EtherType 値と同時に ARP の EtherType 値も指定する必要があるため，IPv4 には二つのプロトコル値を関連づけます。

[コマンドによる設定]

1. **(config)# vlan-protocol IPV4 ethertype 0800,0806**

   名称 IPV4 のプロトコルを作成します。プロトコル値として，IPv4 の EtherType 値 0800 と ARP の EtherType 値 0806 を関連づけます。

   なお，この設定でのプロトコル判定は EthernetV2 形式のフレームだけとなります。

2. **(config)# vlan-protocol IPV6 ethertype 86dd**

   名称 IPV6 のプロトコルを作成します。プロトコル値として IPv6 の EtherType 値 86DD を関連づけます。

[注意事項]

EtherType 値は，05FF 以下の値の場合，0000 で動作します。

(2) プロトコル VLAN の作成

[設定のポイント]

プロトコル VLAN を作成します。VLAN を作成する際に VLAN ID と protocol-based パラメータを指定します。また，VLAN を識別するプロトコルとして，作成したプロトコルを指定します。

［コマンドによる設定］

1. **(config)# vlan 10,20 protocol-based**
   VLAN 10，20 をプロトコル VLAN として作成します。VLAN 10，20 は同じ IPv4 プロトコル VLAN とするため一括して設定します。本コマンドで VLAN コンフィグレーションモードに移行します。

2. **(config-vlan)# protocol IPV4**
   (config-vlan)# exit
   VLAN 10，20 を識別するプロトコルとして，作成した IPv4 プロトコルを設定します。

3. **(config)# vlan 30 protocol-based**
   (config-vlan)# protocol IPV6
   (config-vlan)# exit
   VLAN 30 をプロトコル VLAN として作成します。また，VLAN 30 を識別するプロトコルとして，作成した IPv6 プロトコルを設定します。

(3) プロトコルポートの設定

［設定のポイント］
プロトコル VLAN でプロトコルによって VLAN を識別するポートは，プロトコルポートを設定します。このポートでは Untagged フレームを扱います。

［コマンドによる設定］

1. **(config)# interface tengigabitethernet 0/1**
   ポート 0/1 のイーサネットインタフェースコンフィグレーションモードに移行します。

2. **(config-if)# switchport mode protocol-vlan**
   (config-if)# switchport protocol vlan 10
   (config-if)# exit
   ポート 0/1 をプロトコルポートに設定します。また，VLAN 10 を設定します。

3. **(config)# interface range** tengigabitethernet 0/2, gigabitethernet 0/3
   (config-if-range)# switchport mode protocol-vlan
   (config-if-range)# switchport protocol vlan 20
   (config-if-range)# exit
   ポート 0/2，0/3 をプロトコルポートに設定します。また，VLAN 20 を設定します。

4. **(config)# interface gigabitethernet 0/3**
   (config-if)# switchport protocol vlan add 30
   (config-if)# exit
   ポート 0/3 に VLAN 30 を追加します。ポート 0/3 は IPv4，IPv6 の 2 種類のプロトコル VLAN を設定しています。

［注意事項］

switchport protocol vlan コマンドは，それ以前のコンフィグレーションに追加するコマンドではなく指定した <VLAN ID list> に設定を置き換えます。すでにプロトコル VLAN を運用中のポートで VLAN の追加や削除を行う場合は，switchport protocol vlan add コマンドおよび switchport protocol vlan remove コマンドを使用してください。

（4） トランクポートの設定

［設定のポイント］

プロトコル VLAN においても，Tagged フレームを扱うポートはトランクポートとして設定し，そのトランクポートに VLAN を設定します。

［コマンドによる設定］

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

   ポート 0/4 のイーサネットインタフェースコンフィグレーションモードに移行します。

2. **(config-if)# switchport mode trunk**
   (config-if)# switchport trunk allowed vlan 10,20,30
   (config-if)# exit

   ポート 0/4 をトランクポートに設定します。また，VLAN 10，20，30 を設定します。

16.6.3 プロトコルポートのネイティブ VLAN の設定

［設定のポイント］

プロトコルポートで設定したプロトコルに一致しない Untagged フレームを扱いたい場合，そのフレームを扱う VLAN としてネイティブ VLAN を設定します。ネイティブ VLAN はポート VLAN だけが設定できます。

ネイティブ VLAN の VLAN ID を switchport protocol native vlan コマンドで設定すると，プロトコルポート上で設定したプロトコルに一致しない Untagged フレームを扱う VLAN となります。ネイティブ VLAN は，コンフィグレーションで明示して設定しない場合は VLAN 1（デフォルト VLAN）です。

ネイティブ VLAN に status suspend が設定されている場合は，設定したプロトコルと一致しないフレームが中継されません。

［コマンドによる設定］

1. **(config)# vlan 10,20 protocol-based**
   (config-vlan)# exit
   (config)# vlan 30
   (config-vlan)# exit

   VLAN 10，20 をプロトコル VLAN として作成します。また，VLAN 30 をポート VLAN として作成します。

2. **(config)# interface gigabitethernet 0/3**
   (config-if)# switchport mode protocol-vlan

   ポート 0/3 のイーサネットインタフェースコンフィグレーションモードに移行します。また，プロトコルポートとして設定します。

3. **(config-if)# switchport protocol native vlan 30**

```
(config-if)# switchport protocol vlan 10,20
(config-if)# exit
```

プロトコルポート 0/3 のネイティブ VLAN をポート VLAN 30 に設定し，設定したプロトコルに一致しない Untagged フレームを扱う VLAN とします。また，プロトコル VLAN 10，20 を設定します。

16.7 MAC VLAN の解説

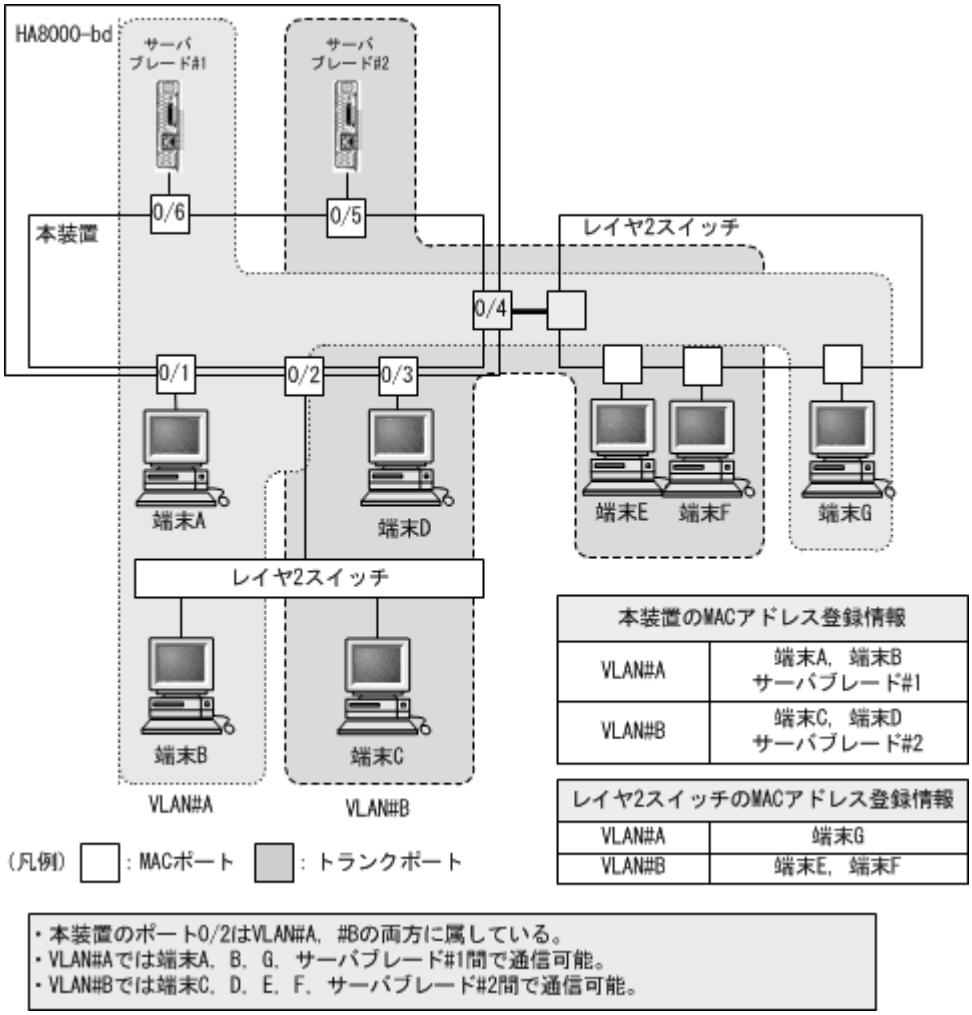
16.7.1 概要

送信元の MAC アドレス単位に VLAN のグループ分けを行います。VLAN への MAC アドレスの登録は，コンフィグレーションによる登録と，レイヤ 2 認証機能による動的な登録ができます。

MAC VLAN は，許可した端末の MAC アドレスをコンフィグレーションで登録するか，レイヤ 2 認証機能で認証された MAC アドレスを登録することによって，接続を許可された端末とだけ通信できるように設定できます。

MAC VLAN の構成例を次の図に示します。VLAN を構成する装置間にトランクポートを設定している場合は，送信元 MAC アドレスに関係なく VLAN Tag によって VLAN を決定します。そのため，すべての装置に同じ MAC アドレスの設定をする必要はありません。装置ごとに MAC ポートに接続した端末の MAC アドレスを設定します。

図 16-8　MAC VLAN の構成例



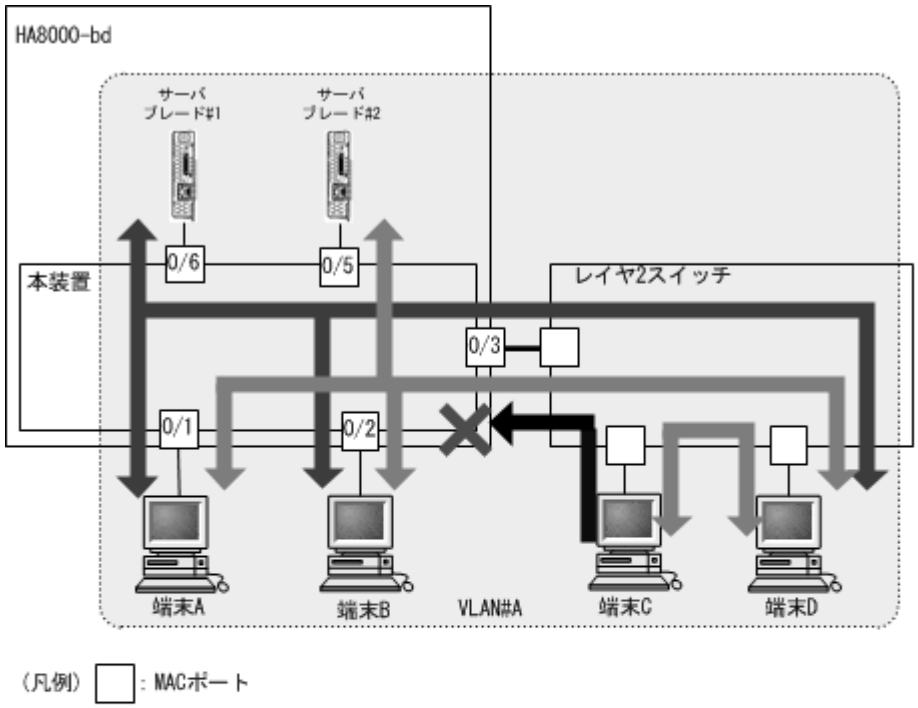
16.7.2 装置間の接続と MAC アドレス設定

複数の装置で MAC VLAN を構成する場合，装置間の接続はトランクポートをお勧めします。トランクポートで受信したフレームの VLAN 判定は VLAN Tag で行います。そのため，送信元 MAC アドレスが VLAN に設定されていなくても，MAC VLAN で通信できます。トランクポートで装置間を接続した場合については，「図 16-8　MAC VLAN の構成例」を参照してください。

MAC ポートで装置間を接続する場合は，その VLAN に属するすべての MAC アドレスをすべての装置に設定する必要があります。ルータが存在する場合は，ルータの MAC アドレスも登録してください。また，VRRP を使用している場合は，仮想ルータ MAC アドレスを登録してください。

MAC ポートで装置間を接続した場合の図を次に示します。

図 16-9　装置間を MAC ポートで接続した場合



本装置のMACアドレス登録情報	
VLAN#A	端末A，端末B，端末D， サーバブレード#1，#2

レイヤ2スイッチのMACアドレス登録情報	
VLAN#A	端末A，端末B， 端末C，端末D， サーバブレード#1，#2

- 端末A，端末B：本装置，レイヤ2スイッチの両方に設定があるため，端末Dと通信可能。
- 端末C：本装置に設定がないため，端末A，端末B，サーバブレード#，#2と通信不可。
- 端末D：本装置，レイヤ2スイッチの両方に設定があるため，端末A，端末B，サーバブレード#1，サーバブレード#2と通信可能。

16.7.3 レイヤ 2 認証機能との連携について

（1） MAC VLAN に MAC アドレスを動的登録

MAC VLAN は，レイヤ 2 認証機能と連携して，VLAN への MAC アドレスを動的に登録できます。連携するレイヤ 2 認証機能を次に示します。

- IEEE802.1X：ポート単位認証（動的）
- Web 認証：ダイナミック VLAN モード
- MAC 認証：ダイナミック VLAN モード

コンフィグレーションとレイヤ 2 認証機能で同じ MAC アドレスを設定した場合，コンフィグレーションの MAC アドレスを MAC VLAN に登録します。

プリンタやサーバなどの Untagged フレームの装置を，レイヤ 2 認証させずに MAC ポートで意図した VLAN に収容したい場合は，コンフィグレーションコマンド mac-address で対象装置の MAC アドレスを MAC VLAN に登録します。

IEEE802.1X ポート単位認証（動的），Web 認証 /MAC 認証のダイナミック VLAN モードの場合は，コンフィグレーションコマンド mac-address-table static で MAC アドレステーブルにも対象装置の MAC アドレスを登録してください。

また，MAC ポートではコンフィグレーションコマンド switchport mac dot1q vlan を指定した VLAN で，Tagged フレームを中継することが可能です。この機能とレイヤ 2 認証機能については後述の「16.7.4 MAC ポートのオプション機能」を参照してください。

レイヤ 2 認証機能については，「コンフィグレーションガイド Vol.2　5　レイヤ 2 認証機能の概説」および各認証機能の解説編を参照してください。

（2） MAC ポートに対する自動 VLAN 割当

MAC ポートに VLAN を設定するときは，コンフィグレーションコマンド swithcport mac vlan で設定，またはレイヤ 2 認証機能による自動割当が可能です。

自動 VLAN 割当が動作するレイヤ 2 認証機能を次に示します。

- IEEE802.1X：ポート単位認証（動的）
- Web 認証：ダイナミック VLAN モード
- MAC 認証：ダイナミック VLAN モード

コンフィグレーションコマンド switchport mac vlan で，自動で割り当てた VLAN と同じ VLAN をポートに設定したときは，自動で割り当てた VLAN は解除します。ただし，認証済みの端末は設定したコンフィグレーションに従いますので，認証は解除しません。

なお，MAC ポートに対する自動 VLAN 割当を抑止する場合は，コンフィグレーションコマンド no switchport mac auto-vlan を設定してください。

レイヤ 2 認証機能の自動 VLAN 割当については，「コンフィグレーションガイド Vol.2　5.4　レイヤ 2 認証の共通機能」を参照してください。

16.7.4　MAC ポートのオプション機能

MAC ポートのオプション機能として，MAC ポートで任意の VLAN ID の Tagged フレームを中継させることができます。

本オプションは，コンフィグレーションコマンド switchport mac dot1q vlan を設定します。コンフィグレーションコマンド switchport mac dot1q vlan で指定できる VLAN は，ポート VLAN または MAC VLAN です。

本オプションの VLAN に収容する Tagged フレームの装置は，フレーム内の VLAN Tag によって収容さ

れるため，コンフィグレーションで MAC アドレスを登録する必要はありません。

(1) 受信フレームの動作

コンフィグレーションコマンド switchport mac dot1q vlan で設定した VLAN ID を持つ Tagged フレームは，当該 VLAN に中継されます。なお，本コマンドを設定した場合，「表 16-11　コンフィグレーションコマンドと VLAN 種別」で設定した VLAN ID を持つ Tagged フレームを中継します。

(2) 送信フレームの動作

コンフィグレーションコマンド switchport mac dot1q vlan で設定した VLAN の Tagged フレームの中継先により Tag の有無が異なります。

表 16-10　中継先と Tagged フレームの処理

中継先	Tagged フレームの処理
アクセスポート	Tag を外して Untagged フレームを送信
トランクポートのネイティブ VLAN	Tag を外して Untagged フレームを送信
トランクポートのネイティブ VLAN 以外	Tagged フレームを送信
プロトコルポートのネイティブ VLAN	Tag を外して Untagged フレームを送信
MAC ポートの MAC VLAN	Tag を外して Untagged フレームを送信
MAC ポートの dot1q vlan で指定した VLAN	Tagged フレームを送信

(3) オプション機能使用時の注意事項

(a) VLAN の排他について

下記のコンフィグレーションコマンドで指定する VLAN は，すべて排他設定となります。いずれかに設定した VLAN ID を，その他のコマンドで設定することはできません。

表 16-11　コンフィグレーションコマンドと VLAN 種別

コンフィグレーションコマンド	指定可能な VLAN 種別
switchport mac dot1q vlan	ポート VLAN，MAC VLAN
switchport mac vlan	MAC VLAN
switchport mac native vlan	ポート VLAN

(b) コンフィグレーションコマンド switchport mac dot1q vlan について

本コマンドは，コンフィグレーションコマンド switchport mode mac-vlan 設定時に有効となります。

(c) レイヤ２認証機能との併用について

MAC ポートでコンフィグレーションコマンド switchport mac dot1q vlan を設定した場合，当該 VLAN での Untagged フレームおよび Tagged フレームとレイヤ２認証は下記の動作となります。

- Untagged フレームとレイヤ２認証
  「16.7.3　レイヤ 2 認証機能との連携について」と同様に使用可能です。
- Tagged フレームとレイヤ２認証
  当該 VLAN を収容したインタフェースポートに，Web 認証 /MAC 認証の固定 VLAN モードが設定され

ている場合，「表 16-11　コンフィグレーションコマンドと VLAN 種別」で設定した VLAN ID を持つ Tagged フレームは固定 VLAN モードの認証対象となります。
固定 VLAN モードで認証させない場合は，コンフィグレーションコマンド mac-address-table static で対象 MAC アドレスと VLAN ID※を登録します。

注※：コンフィグレーションコマンド switchport mac dot1q vlan で設定した VLAN ID を指定してください。

16.8 MAC VLAN のコンフィグレーション

16.8.1 コンフィグレーションコマンド一覧

MAC VLAN のコンフィグレーションコマンド一覧を次の表に示します。

表 16-12 コンフィグレーションコマンド一覧

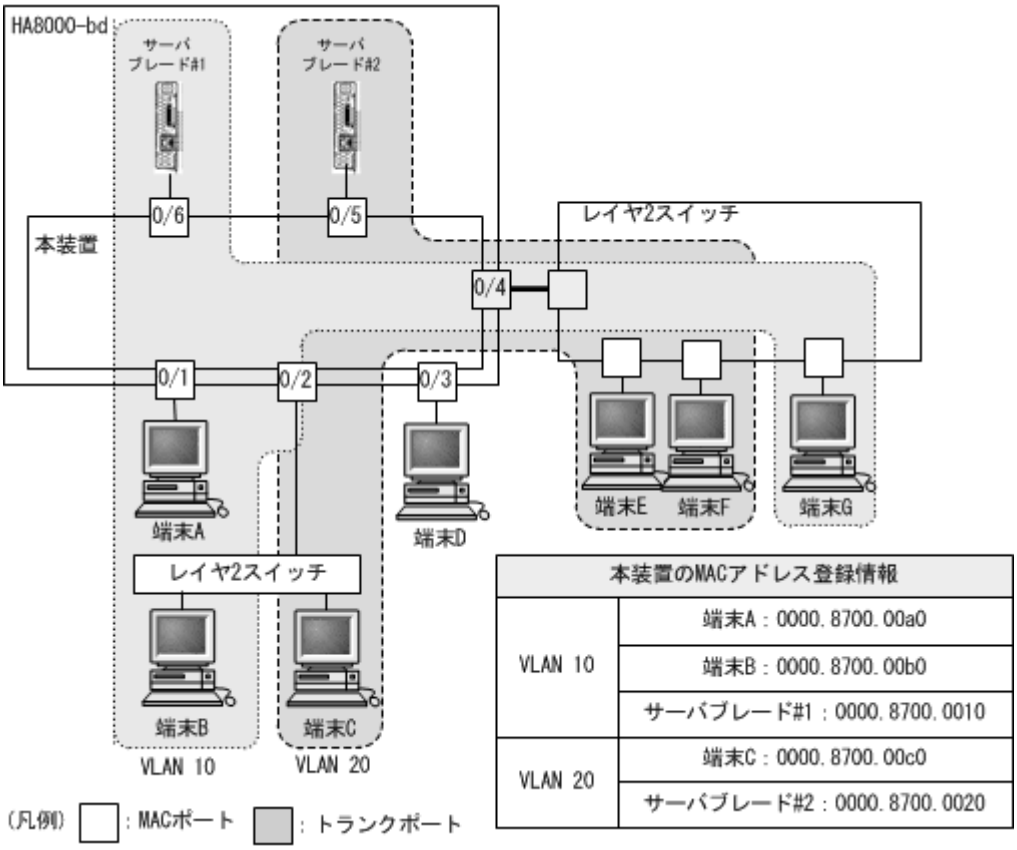
コマンド名	説明
mac-address	MAC VLAN で VLAN に所属する端末の MAC アドレスをコンフィグレーションによって設定します。
switchport mac vlan	MAC ポートの VLAN を設定します。
switchport mac auto-vlan	no switchport mac auto-vlan 設定時，認証機能による認証後 VLAN が switchport mac vlan で指定された VLAN と一致するときだけ通信できます。（MAC VLAN の自動 VLAN 割当を抑止）
switchport mode	ポートの種類（MAC，トランク）を設定します。
switchport trunk	トランクポートの VLAN を設定します。
vlan mac-based	MAC VLAN を作成します。また，VLAN コンフィグレーションモードで VLAN に関する項目を設定します。

16.8.2 MAC VLAN の設定

MAC VLAN を設定する手順を以下に示します。ここでは，MAC VLAN と VLAN に所属する MAC アドレスをコンフィグレーションで設定する場合の例を示します。レイヤ 2 認証機能との連携については，マニュアル「コンフィグレーションガイド Vol.2」の各認証機能の「設定と運用」を参照してください。

次の図に示す本装置 #1 の設定例を示します。ポート 0/1 は MAC VLAN 10 を設定します。ポート 0/2 は MAC VLAN 10 および 20，0/3 は MAC VLAN 20 を設定します。ただし，ポート 0/3 には MAC アドレスを登録していない端末 D を接続しています。

図 16-10　MAC VLAN の設定例



(1) MAC VLAN の作成と MAC アドレスの登録

[設定のポイント]

MAC VLAN を作成します。VLAN を作成する際に VLAN ID と mac-based パラメータを指定します。

また，VLAN に所属する MAC アドレスを設定します。構成例の端末 A ～ C，サーバブレード #1, #2 をそれぞれの VLAN に登録します。端末 D は MAC VLAN での通信を許可しないので登録しません。

[コマンドによる設定]

1. **(config)# vlan 10 mac-based**

   VLAN 10 を MAC VLAN として作成します。本コマンドで VLAN コンフィグレーションモードに移行します。

2. **(config-vlan)# mac-address 0000.8700.00a0**
   (config-vlan)# mac-address 0000.8700.00b0
   (config-vlan)# mac-address 0000.8700.0010
   (config-vlan)# exit

   端末 A（0000.8700.00a0），端末 B（0000.8700.00b0），サーバブレード #1（0000.8700.0010）を MAC VLAN 10 に登録します。

3. **(config)# vlan 20 mac-based**
   (config-vlan)# mac-address 0000.8700.00c0

```
(config-vlan)# mac-address 0000.8700.0020
(config-vlan)# exit
```

VLAN 20 を MAC VLAN として作成し，端末 C（0000.8700.00c0），サーバブレード #2（0000.8700.0020）を MAC VLAN 20 に登録します。

［注意事項］

MAC VLAN に登録する MAC アドレスでは，同じ MAC アドレスを複数の VLAN に登録できません。

（2） MAC ポートの設定

［設定のポイント］

MAC VLAN で送信元 MAC アドレスによって VLAN を識別するポートは，MAC ポートを設定します。このポートでは Untagged フレームを扱います。

［コマンドによる設定］

1. **(config)# interface range tengigabitethernet 0/1-2, gigabitethernet 0/6**

   ポート 0/1，0/2，0/6 のイーサネットインタフェースコンフィグレーションモードに移行します。ポート 0/1，0/2，0/6 に MAC VLAN 10 を設定するため一括して指定します。

2.
```
(config-if-range)# switchport mode mac-vlan
(config-if-range)# switchport mac vlan 10
(config-if-range)# exit
```

   ポート 0/1，0/2，0/6 を MAC ポートに設定します。また，VLAN 10 を設定します。

3.
```
(config)# interface range tengigabitethernet 0/2, gigabitethernet 0/3,
gigabitethernet 0/5
(config-if-range)# switchport mode mac-vlan
(config-if-range)# switchport mac vlan add 20
(config-if-range)# exit
```

   ポート 0/2，0/3，0/5 を MAC ポートに設定します。また，VLAN 20 を設定します。ポート 0/2 にはすでに VLAN 10 を設定しているため，switchport mac vlan add コマンドで追加します。ポート 0/3，0/5 は新規の設定と同じ意味になります。

［注意事項］

コンフィグレーションコマンド switchport mac vlan は，それ以前のコンフィグレーションに追加するコマンドではなく指定した <VLAN ID list> に設定を置き換えます。すでに MAC VLAN を運用中のポートで VLAN の追加や削除を行う場合は，コンフィグレーションコマンド switchport mac vlan add および switchport mac vlan remove を使用してください。

（3） トランクポートの設定

［設定のポイント］

MAC VLAN においても，Tagged フレームを扱うポートはトランクポートとして設定し，そのトランクポートに VLAN を設定します。

［コマンドによる設定］

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

   ポート 0/4 のイーサネットインタフェースコンフィグレーションモードに移行します。

2. **(config-if)# switchport mode trunk**
   (config-if)# switchport trunk allowed vlan 10,20
   (config-if)# exit
   ポート 0/4 をトランクポートに設定します。また，VLAN 10，20 を設定します。

16.8.3 MAC ポートのネイティブ VLAN の設定

［設定のポイント］

MAC ポートで MAC VLAN に登録した MAC アドレスに一致しない Untagged フレームを扱いたい場合，そのフレームを扱う VLAN としてネイティブ VLAN を設定します。ネイティブ VLAN はポート VLAN だけが設定できます。

ネイティブ VLAN の VLAN ID をコンフィグレーションコマンド switchport mac native vlan で指定すると，MAC ポート上で登録した MAC アドレスに一致しない Untagged フレームを扱う VLAN となります。ネイティブ VLAN は，コンフィグレーションで明示して指定しない場合は VLAN 1（デフォルト VLAN）です。

ネイティブ VLAN に status suspend が設定されていた場合は，登録した MAC アドレスに一致しないフレームが中継されません。

［コマンドによる設定］

1. **(config)# vlan 10,20 mac-based**
   (config-vlan)# exit
   (config)# vlan 30
   (config-vlan)# exit
   VLAN 10,20 を MAC VLAN として作成します。また，VLAN 30 をポート VLAN として作成します。

2. **(config)# interface tengigabitethernet 0/1**
   (config-if)# switchport mode mac-vlan
   ポート 0/1 のイーサネットインタフェースコンフィグレーションモードに移行します。また，MAC ポートとして設定します。

3. **(config-if)# switchport mac vlan 10,20**
   ポート 0/1 に MAC VLAN 10，20 を設定します。
   この状態で，ポート 0/1 は MAC VLAN 10，20 だけ通信を許可するポートとなります。登録されていない MAC アドレスは通信することはできません。登録されていない MAC アドレスから通信するためには，ネイティブ VLAN が通信可能となるように設定します。

4. **(config-if)# switchport mac native vlan 30**
   (config-if)# exit
   ポート 0/1 にポート VLAN30 をネイティブ VLAN として設定します。VLAN 30 はポート 0/1 で登録されていない MAC アドレスからの Untagged フレームを扱う VLAN となります。

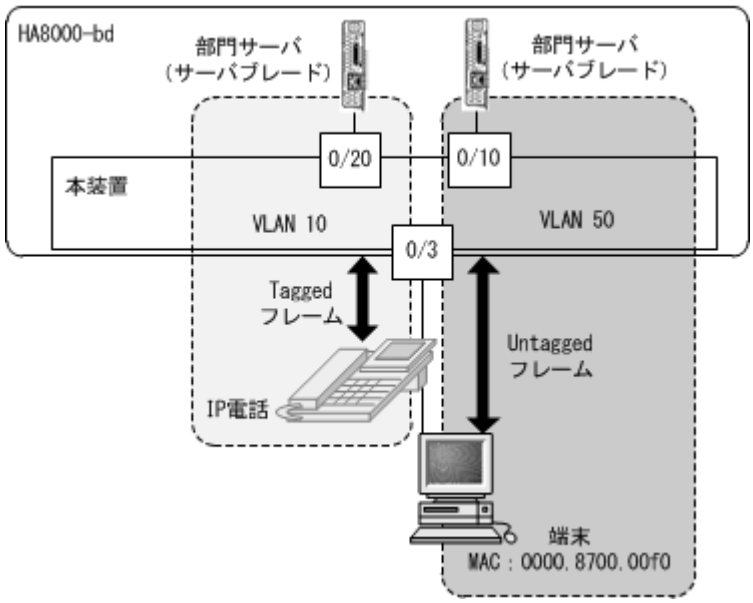
16.8.4 MAC ポートでの Tagged フレーム中継の設定

下記構成図のように，同一ポートで IP 電話機からは Tagged フレーム，IP 電話機配下の端末からは Untagged フレームを受信して通信する場合は，MAC ポートのオプション機能を使用します。

オプション機能は，コンフィグレーションコマンド switchport mac dot1q vlan で，Tagged フレーム中継用の VLAN ID を指定することにより，同一 MAC ポートで Tagged フレーム／ Untagged フレームの中継が可能となります。

IP 電話機および端末をレイヤ 2 認証機能で認証する設定については，マニュアル「コンフィグレーションガイド Vol.2」を参照してください。

図 16-11　MAC ポートでの Tagged フレーム中継の設定例



［設定のポイント］

MAC ポートを設定し，同一 MAC ポートで Tagged フレームと Untagged フレームを扱うポートとして設定します。また，MAC VLAN には端末の MAC アドレスを設定します。

- VLAN 10：ポート VLAN で Tagged フレームを扱います。
- VLAN 50：MAC VLAN で Untagged フレームを扱います。

［コマンドによる設定］

1. **(config)# vlan 10**
   (config-vlan)# exit
   VLAN 10 をポート VLAN として作成します。

2. **(config)# vlan 50 mac-based**
   (config-vlan)# mac-address 0000.8700.00f0
   (config-vlan)# exit
   VLAN 50 を MAC VLAN として作成し，VLAN 50 に所属する端末の MAC アドレス（0000.8700.00f0）を設定します。

3. **(config)# interface gigabitethernet 0/3**
   ポート 0/3 のイーサネットインタフェースコンフィグレーションモードに移行します。

4. **(config-if)# switchport mode mac-vlan**
   ポート 0/3 を MAC ポートとして設定します。

5. **(config-if)# switchport mac dot1q vlan 10**
   MAC ポートで Tagged フレームを扱う VLAN として，VLAN 10 を設定します。

6. **(config-if)# switchport mac vlan 50**
   (config-if)# exit
   MAC ポートで Untagged フレームを扱う VLAN として，VLAN50 を設定します。

[注意事項]

1. コンフィグレーションコマンド switchport mac dot1q vlan の設定については，下記にご注意ください。
   - 指定可能な VLAN はポート VLAN または MAC VLAN です。コンフィグレーションコマンド switchport mac vlan および switchport mac native vlan で指定した VLAN は指定できません。
   - 本設定は，switchport mode mac-vlan 設定時に有効となります。
2. Tagged フレーム中継を設定したポートには，BPDU を送信する装置を接続しないでください。（接続する場合は，スパニングツリーを Disable に設定してください。）

16.9 VLAN のオペレーション

16.9.1 運用コマンド一覧

VLAN の運用コマンド一覧を次の表に示します。

表 16-13 運用コマンド一覧

コマンド名	説明
show vlan	VLAN の各種情報を表示します。
show vlan mac-vlan	MAC VLAN に登録されている MAC アドレスを表示します。

16.9.2 VLAN の状態の確認

(1) VLAN の設定状態の確認

VLAN の情報は運用コマンド show vlan で確認できます。VLAN ID，Type，IP Address などによって VLAN に関する設定が正しいことを確認してください。また，Untagged はその VLAN で Untagged フレームを扱うポート，Tagged はその VLAN で Tagged フレームを扱うポートになります。VLAN に設定されているポートの設定が正しいことを確認してください。

図 16-12 show vlan の実行結果

```
> show vlan

Date 20XX/06/07 08:57:56 UTC
VLAN counts: 6
VLAN ID: 1     Type: Port based      Status: Up
  Learning: On             Tag-Translation:
  BPDU Forwarding:         EAPOL Forwarding:
  Router Interface Name: VLAN0001
  IP Address:
  Source MAC address: 0000.8762.1fdf(System)
  Description: VLAN0001
  Spanning Tree: None(-)
  AXRP RING ID:        AXRP VLAN group:
  IGMP snooping:       MLD snooping:
  Untagged(43)  : 0/1-9,0/13,0/16-17,0/20-21
  Tagged(0)     :
VLAN ID: 10    Type: Port based      Status: Down
  Learning: On             Tag-Translation:
  BPDU Forwarding:         EAPOL Forwarding:
  Router Interface Name: VLAN0010
  IP Address:
  Source MAC address: 0000.8762.1fdf(System)
  Description: VLAN0010
  Spanning Tree: None(-)
  AXRP RING ID: 200    AXRP VLAN group: Control-VLAN
  IGMP snooping:       MLD snooping:
  Untagged(0)   :
  Tagged(4)     : 0/18-19,0/22,0/24
VLAN ID: 20    Type: Port based      Status: Up
  Learning: On             Tag-Translation:
  BPDU Forwarding:         EAPOL Forwarding:
  Router Interface Name: VLAN0020
  IP Address:
  Source MAC address: 0000.8762.1fdf(System)
  Description: Ring-VL
  Spanning Tree: PVST+(802.1D)
  AXRP RING ID: 200    AXRP VLAN group: 1
  AXRP Virtual-Link-VLAN
  IGMP snooping:       MLD snooping:
```

```
  Untagged(0)    :
  Tagged(4)      : 0/18-19,0/22,0/24
VLAN ID: 30    Type: Protocol based  Status: Up
  Protocol VLAN Information  Name:
  EtherType:  LLC:  Snap-EtherType:
  Learning: On             Tag-Translation:
  BPDU Forwarding:         EAPOL Forwarding:
  Router Interface Name: VLAN0030
  IP Address:
  Source MAC address: 0000.8762.1fdf(System)
  Description: VLAN0030
  Spanning Tree: None(-)
  AXRP RING ID: 200   AXRP VLAN group: 2
  IGMP snooping:      MLD snooping:
  Untagged(2)    : 0/3,0/13
  Tagged(4)      : 0/18-19,0/22,0/24
VLAN ID: 51    Type: MAC based       Status: Up
  Learning: On             Tag-Translation:
  BPDU Forwarding:         EAPOL Forwarding:
  Router Interface Name: VLAN0051
  IP Address: 10.215.196.1/23
              3ffe:501:811:ff08::5/64
              fe80::212:e2ff:fe62:1fdf/64
  Source MAC address: 0000.8762.1fdf(System)
  Description: IPv4/IPv6
  Spanning Tree: None(-)
  AXRP RING ID:       AXRP VLAN group:
  IGMP snooping:      MLD snooping:
  Untagged(3)    : 0/6,0/16,0/20
  Tagged(0)      :
VLAN ID: 4094  Type: Port based      Status: Up
  Learning: On             Tag-Translation: On
  BPDU Forwarding:         EAPOL Forwarding:
  Router Interface Name: VLAN4094
  IP Address:
  Source MAC address: 0000.8762.1fdf(System)
  Description: VLAN4094
  Spanning Tree: None(-)
  AXRP RING ID:       AXRP VLAN group:
  IGMP snooping:      MLD snooping:
  Untagged(0)    :
  Tagged(5)      : 0/10-12,0/14-15
  Tag-Trans(5)   : 0/10-12,0/14-15

>
```

（2）VLAN の通信状態の確認

VLAN の通信状態は運用コマンド show vlan detail で確認できます。Port Information でポートの Up/Down，Forwarding/Blocking を確認してください。Blocking 状態の場合，括弧内に Blocking の要因が示されています。

図 16-13　show vlan detail の実行結果

```
> show vlan 10,4094 detail

Date 20XX/06/07 09:00:00 UTC
VLAN counts: 2
VLAN ID: 10    Type: Port based      Status: Down
  Learning: On             Tag-Translation:
  BPDU Forwarding:         EAPOL Forwarding:
  Router Interface Name: VLAN0010
  IP Address:
  Source MAC address: 0000.8762.1fdf(System)
  Description: VLAN0010
  Spanning Tree: None(-)
  AXRP RING ID: 200   AXRP VLAN group: Control-VLAN
  IGMP snooping:      MLD snooping:
  Port Information
   0/18(ChGr:9)  Down -               Tagged
   0/19(ChGr:9)  Down -               Tagged
```

```
   0/22(ChGr:9)  Down -               Tagged
   0/24          Up   Blocking(AXRP)  Tagged
VLAN ID: 4094  Type: Port based      Status: Up
  Learning: On            Tag-Translation: On
  BPDU Forwarding:        EAPOL Forwarding:
  Router Interface Name: VLAN4094
  IP Address:
  Source MAC address: 0000.8762.1fdf(System)
  Description: VLAN4094
  Spanning Tree: None(-)
  AXRP RING ID:       AXRP VLAN group:
  IGMP snooping:      MLD snooping:
  Port Information
   0/10(ChGr:64) Up   Forwarding      Tagged   Tag-Translation:4093
   0/11(ChGr:64) Up   Forwarding      Tagged   Tag-Translation:4093
   0/12(ChGr:64) Down -               Tagged   Tag-Translation:4093
   0/14(ChGr:64) Up   Forwarding      Tagged   Tag-Translation:4093
   0/15(ChGr:64) Down -               Tagged   Tag-Translation:4093

>
```

（3） VLAN ID 一覧の確認

運用コマンド show vlan summary で，設定した VLAN の種類とその数，VLAN ID を確認できます。

図 16-14　show vlan summary の実行結果

```
> show vlan summary

Date 20XX/06/07 08:59:46 UTC
Total(6)            : 1,10,20,30,51,4094
Port based(4)       : 1,10,20,4094
Protocol based(1)   : 30
MAC based(1)        : 51

>
```

（4） VLAN のリスト表示による確認

運用コマンド show vlan list は VLAN の設定状態の概要を 1 行に表示します。本コマンドによって，VLAN の設定状態やレイヤ 2 冗長機能，IP アドレスの設定状態を一覧で確認できます。また，VLAN，ポートまたはチャネルグループをパラメータとして指定することで，指定したパラメータの VLAN の状態だけを一覧で確認できます。

図 16-15　show vlan list の実行結果

```
> show vlan list

Date 20XX/06/07 09:00:09 UTC
VLAN counts: 6
ID   Status   Fwd/Up /Cfg Name             Type  Protocol         Ext.  IP
   1 Up         3/  3/ 43 VLAN0001         Port  -                - -   -
  10 Down       0/  1/  4 VLAN0010         Port  AXRP (C)         - -   -
  20 Up         1/  1/  4 Ring-VL          Port  -                - -   -
  30 Up         1/  1/  6 VLAN0030         Proto AXRP (-)         - -   -
  51 Up         1/  1/  3 IPv4/IPv6        MAC   -                - -   4/6
4094 Up         3/  3/  5 VLAN4094         Port  -                - T   -
     AXRP (C:Control-VLAN)
     S:IGMP/MLD snooping  T:Tag Translation
     4:IPv4 address configured  6:IPv6 address configured

>
```

（5） MAC VLAN の登録 MAC アドレスの確認

MAC VLAN に登録されている MAC アドレスを，運用コマンド show vlan mac-vlan で確認できます。

括弧内はMACアドレスを登録した機能を示しています。

- 「static」はコンフィグレーションで登録したMACアドレス
- 「dot1x」「web-auth」「mac-auth」はレイヤ2認証機能で登録したMACアドレス

図 16-16　show vlan mac-vlan の実行結果

```
> show vlan mac-vlan

Date 20XX/06/07 06:12:04 UTC
VLAN counts: 1    Total MAC Counts: 3
VLAN ID: 100         MAC Counts: 3
   0000.e22b.ffdd(mac-auth)   000b.972f.e22b(mac-auth)
   0050.daba.4fc8(mac-auth)

>
```

17 VLAN 拡張機能

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

17.1 VLAN トンネリングの解説

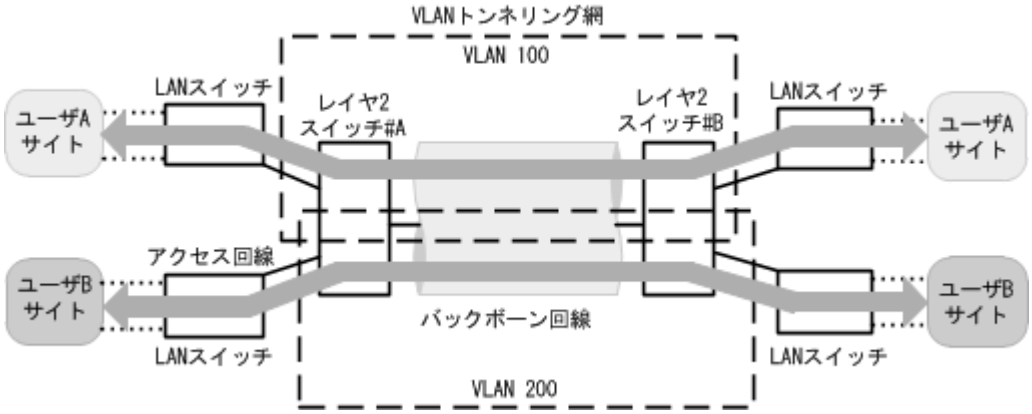
17.1.1 概要

VLAN トンネリング機能とは，複数ユーザの VLAN をほかの VLAN の中に集約して「トンネル」する機能です。IEEE802.1Q VLAN Tag をスタックすることで一つの VLAN 内にほかの VLAN に属するフレームをトランスペアレントに通すことができます。トンネルは 3 か所以上のサイトを接続するマルチポイント接続ができます。

VLAN トンネリング概要（広域イーサネットサービス適用例）を次の図に示します。VLAN トンネリングでは，VLAN Tag をスタックすることで VLAN トンネリング網内の VLAN を識別します。

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

図 17-1 VLAN トンネリング概要（広域イーサネットサービス適用例）



17.1.2 VLAN トンネリングを使用するための必須条件

VLAN トンネリング機能を使用する場合は，次の条件に合わせてネットワークを構築する必要があります。

- ポート VLAN を使用します。
- VLAN トンネリング機能を実現する VLAN では，アクセス回線側はトンネリングポートとし，バックボーン回線側をトランクポートとします。
- VLAN トンネリング網内のバックボーン回線では VLAN Tag をスタックするため，通常より 4 バイト大きいサイズのフレームを扱える必要があります。
- 装置内で，アクセスポートとトンネリングポートは共存できません。一つでもトンネリングポートを設定すると，アクセスポートとして設定していたポートもトンネリングポートとして動作します。

17.1.3 VLAN トンネリング使用時の注意事項

（1） 他機能との共存

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

（2） デフォルト VLAN について

デフォルト VLAN の自動加入を行いません。すべての VLAN を明示的に設定してください。

（3） トランクポートのネイティブ VLAN について

VLAN トンネリングのトランクポートは VLAN Tag をスタックするポートとなりますが，ネイティブ VLAN では VLAN Tag をスタックしません。本装置からフレームを送信するときはアクセスポートと同様に動作して，フレームを受信するときは Untagged フレームだけを扱います。ほかの VLAN と異なる動作となるので，VLAN トンネリング網のバックボーン回線の VLAN としては使用できません。VLAN トンネリングを使用する場合，トランクポートのネイティブ VLAN は suspend 状態とすることをお勧めします。

トランクポートのネイティブ VLAN は，コンフィグレーションコマンド switchport trunk native vlan で設定しない場合デフォルト VLAN です。デフォルト VLAN で VLAN トンネリング機能を使用する場合は，switchport trunk native vlan でネイティブ VLAN にデフォルト VLAN 以外の VLAN を設定してください。

（4） フレームの User Priority について

VLAN トンネリングを使用する場合の User Priority については，「コンフィグレーションガイド Vol.2 3.4 マーカー解説」を参照してください。

17.2 VLAN トンネリングのコンフィグレーション

17.2.1 コンフィグレーションコマンド一覧

VLAN トンネリングのコンフィグレーションコマンド一覧を次の表に示します。

表 17-1 コンフィグレーションコマンド一覧

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

注※
「コンフィグレーションコマンドレファレンス 9. イーサネット」を参照してください。

17.2.2 VLAN トンネリングの設定

(1) アクセス回線，バックボーン回線の設定

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

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/4**
ポート 0/4 のイーサネットインタフェースコンフィグレーションモードに移行します。

2. **(config-if)# switchport mode dot1q-tunnel**
(config-if)# switchport access vlan 10
(config-if)# exit
ポート 0/4 をトンネリングポートに設定します。また，VLAN 10 を設定します。

トランクポートのコンフィグレーションについては，「16.4 ポート VLAN のコンフィグレーション」を参照してください。

(2) バックボーン回線のジャンボフレームの設定

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

[コマンドによる設定]
ジャンボフレームのコンフィグレーションについては，「12.2.5 ジャンボフレームの設定」を参照してください。

17.3　Tag 変換の解説

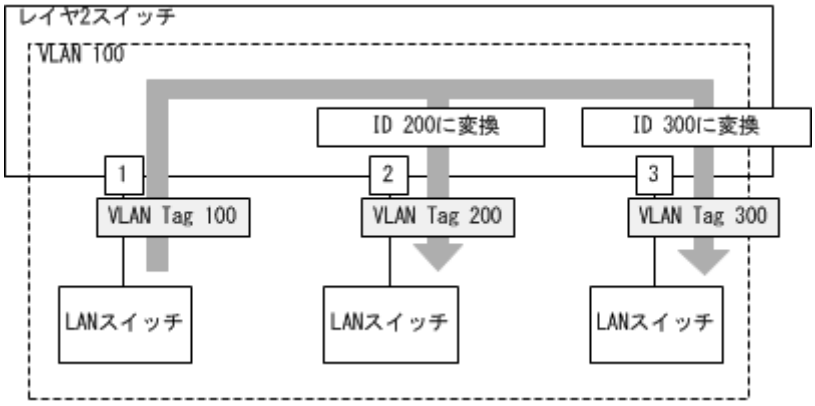
17.3.1　概要

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

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

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

図 17-2　Tag 変換の構成例



17.3.2　Tag 変換使用時の注意事項

（1）他機能との共存

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

（2）Tag 変換を使用しない VLAN について

Tag 変換を使用するポートでは，そのポートで使用するすべての Tag 値で Tag 変換を設定する必要があります。Tag 変換をしない VLAN の場合でも，変換前後で同じ Tag 値になるように明示的に設定する必要があります。

Tag 変換を設定していない Tag 値のフレームを受信すると廃棄します。また，Tag 変換を設定していない VLAN でフレームを送信する場合には，Untagged フレームで送信します。このように動作するため，通信できなくなります。

17.4 Tag 変換のコンフィグレーション

17.4.1 コンフィグレーションコマンド一覧

Tag 変換のコンフィグレーションコマンド一覧を次の表に示します。

表 17-2 コンフィグレーションコマンド一覧

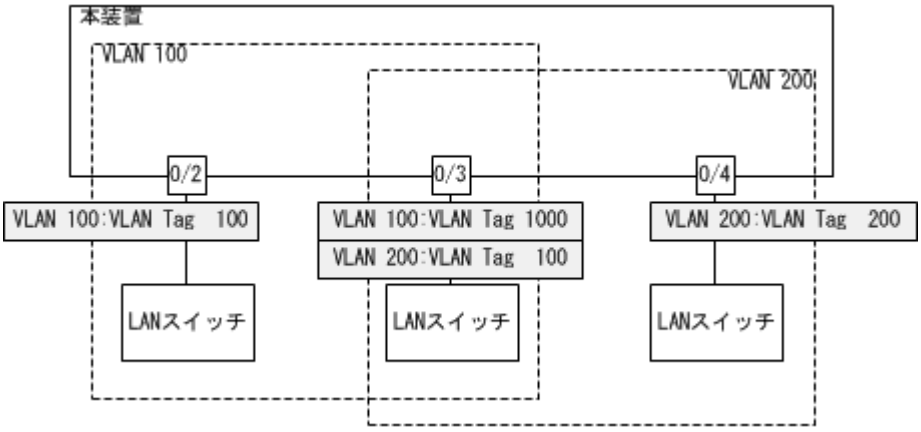
コマンド名	説明
switchport vlan mapping	変換する ID を設定します。
switchport vlan mapping enable	指定したポートで Tag 変換を有効にします。

17.4.2 Tag 変換の設定

Tag 変換を設定する手順を次の図に示します。ここでは，図に示す構成のポート 0/3 の設定例を示します。

構成例では，ポート 0/3 に Tag 変換を適用します。ポート 0/3 では，VLAN 100 のフレームの送受信は VLAN Tag 1000 で行い，VLAN 200 のフレームの送受信は VLAN Tag 100 で行います。このように，VLAN 100 で Tag 変換を行った場合，ほかの VLAN で VLAN Tag 100 を使用することもできます。また，ポート 0/3 では VLAN Tag 200 のフレームを VLAN 200 として扱わないで，未設定の VLAN Tag として廃棄します。

図 17-3 Tag 変換の設定例



［設定のポイント］

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

Tag 変換はコンフィグレーションコマンド switchport vlan mapping で設定します。設定した変換を有効にするためには，コンフィグレーションコマンド switchport vlan mapping enable を設定します。Tag 変換を有効にすると，そのポートで変換を設定していない VLAN はフレームの送受信を停止します。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/3**
   (config-if)# switchport mode trunk
   (config-if)# switchport trunk allowed vlan 100,200

ポート 0/3 をトランクポートに設定して，VLAN 100，200 を設定します。

2. **(config-if)# switchport vlan mapping 1000 100**
   (config-if)# switchport vlan mapping 100 200
   ポート 0/3 で VLAN 100，200 に Tag 変換を設定します。VLAN 100 では VLAN Tag 1000 でフレームを送受信して，VLAN 200 では VLAN Tag 100 でフレームを送受信するように設定します。

3. **(config-if)# switchport vlan mapping enable**
   (config-if)# exit
   ポート 0/3 で Tag 変換を有効にします。本コマンドを設定するまでは Tag 変換は動作しません。

［注意事項］

Tag 変換を使用するポートは，そのポートのすべての VLAN で Tag 変換の設定をする必要があります。変換しない VLAN の場合は，同じ値に変換する設定を行ってください。なお，Tag 変換の収容条件はコンフィグレーションの設定数で 768 で，同じ値に変換する設定も含まれます。

17.5 L2 プロトコルフレーム透過機能の解説

17.5.1 概要

この機能は，レイヤ 2 のプロトコルフレームを中継する機能です。中継するフレームにはスパニングツリーの BPDU，IEEE802.1X の EAPOL があります。通常，これらレイヤ 2 のプロトコルフレームは中継しません。

中継するフレームは本装置では単なるマルチキャストフレームとして扱い，本装置のプロトコルには使用しません。

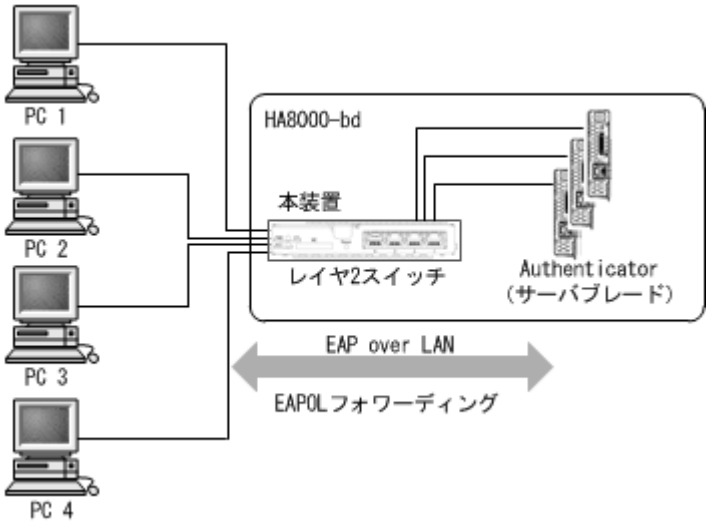
(1) BPDU フォワーディング機能

本装置でスパニングツリーを使用しない場合に BPDU を中継できます。VLAN トンネリングでこの機能を使用すると，ユーザの BPDU を通過させることができます。その際，VLAN トンネリング網のすべてのエッジ装置，コア装置で BPDU フォワーディング機能を設定する必要があります。

(2) EAPOL フォワーディング機能

本装置で IEEE802.1X を使用しない場合に EAPOL を中継できます。本装置を，Authenticator と端末（Supplicant）の間のレイヤ 2 スイッチとして用いるときにこの機能を使用します。

図 17-4 EAPOL フォワーディング機能の適用例



17.5.2 L2 プロトコルフレーム透過機能の注意事項

(1) 他機能との共存

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

17.6 L2 プロトコルフレーム透過機能のコンフィグレーション

17.6.1 コンフィグレーションコマンド一覧

L2 プロトコルフレーム透過機能のコンフィグレーションコマンド一覧を次の表に示します。

表 17-3 コンフィグレーションコマンド一覧

コマンド名	説明
l2protocol-tunnel eap	IEEE802.1X の EAPOL を中継します。
l2protocol-tunnel stp	スパニングツリーの BPDU を中継します。

17.6.2 L2 プロトコルフレーム透過機能の設定

（1） BPDU フォワーディング機能の設定

[設定のポイント]

本機能の設定は装置単位で有効になります。設定すると，BPDU をすべての VLAN で中継します。BPDU フォワーディング機能は，本装置のスパニングツリーを停止してから設定する必要があります。

[コマンドによる設定]

1. **(config)# spanning-tree disable**
   (config)# l2protocol-tunnel stp
   BPDU フォワーディング機能を設定します。事前にスパニングツリーを停止し，BPDU フォワーディング機能を設定します。本装置は BPDU をプロトコルフレームとして扱わないで中継します。

（2） EAPOL フォワーディング機能の設定

[設定のポイント]

本機能の設定は装置単位で有効になります。設定すると，EAPOL をすべての VLAN で中継します。EAPOL フォワーディング機能と IEEE802.1X 機能は同時に使用することはできません。

[コマンドによる設定]

1. **(config)# l2protocol-tunnel eap**
   EAPOL フォワーディング機能を設定します。本装置は EAPOL をプロトコルフレームとして扱わないで中継します。

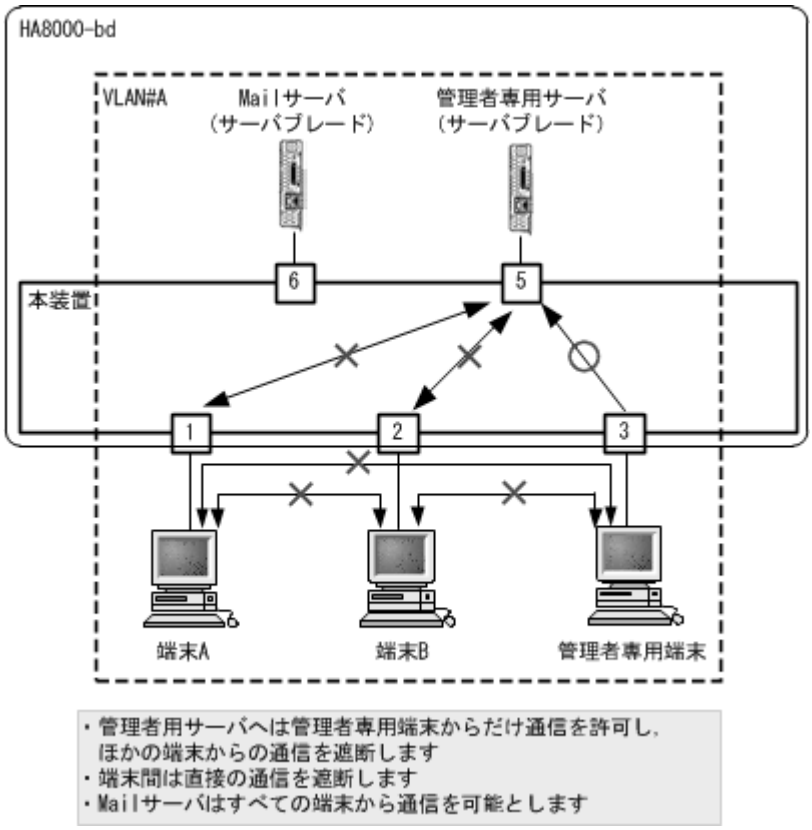
17.7　ポート間中継遮断機能の解説

17.7.1　概要

ポート間中継遮断機能は，指定したポートですべての通信を遮断する機能です。特定のポートからのアクセスだけを許可するサーバの接続や，直接の通信を遮断したい端末の接続などに適用することによってセキュリティを確保できます。

次の図に適用例を示します。この例では，管理者専用サーバは通常の端末からのアクセスを遮断して，管理者専用端末からだけアクセスできます。また，端末間は直接の通信を遮断し，各端末のセキュリティを確保します。

図 17-5　ポート間中継遮断機能の適用例



17.7.2　ポート間中継遮断機能使用時の注意事項

(1) 他機能との共存

ポート間中継遮断機能と下記に示す機能を同時に使用したときの動作を，次の表に示します。

表 17-4　ポート間中継遮断機能と他機能の同時使用について

機能	動作
スパニングツリー	通信を遮断したポートでスパニングツリーを運用すると，トポロジーによって通信できなくなる場合があります。
IGMP snooping	通信を遮断したポートで IGMP snooping を運用すると，IGMP フレームに対してポート間中継遮断機能が無効になり，中継してしまいます。

機能	動作
MLD snooping	通信を遮断したポートで MLD snooping を運用すると，MLD フレームに対してポート間中継遮断機能が無効になり，中継してしまいます。
GSRP aware	通信を遮断したポートで GSRP を運用すると GSRP aware フレームに対してポート間中継遮断機能が無効になり，中継してしまいます。

17.8 ポート間中継遮断機能のコンフィグレーション

17.8.1 コンフィグレーションコマンド一覧

ポート間中継遮断機能のコンフィグレーションコマンド一覧を次の表に示します。

表 17-5 コンフィグレーションコマンド一覧

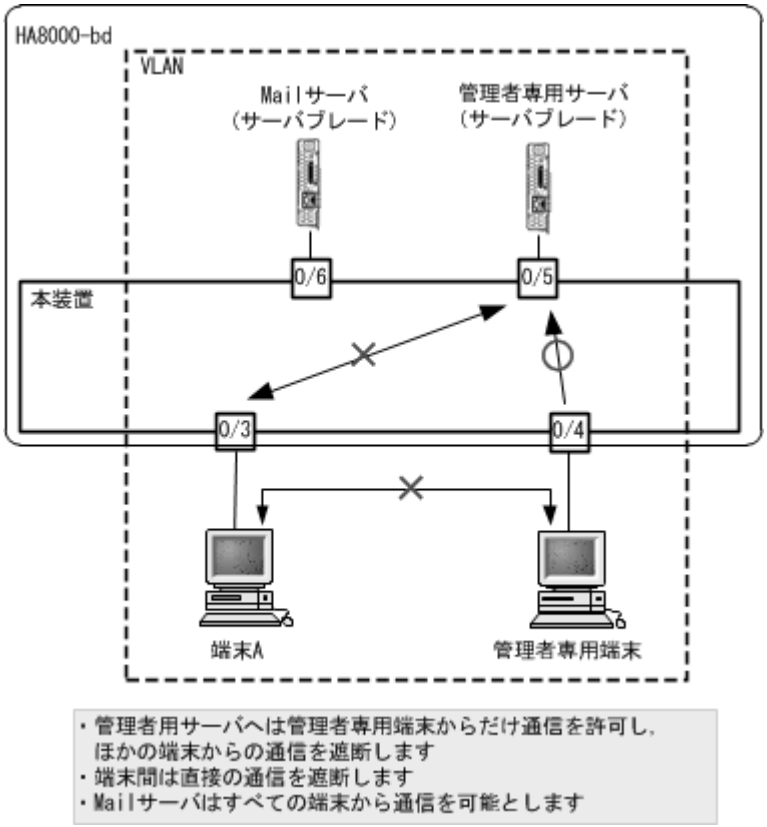
コマンド名	説明
switchport isolation	指定したポートへの中継を遮断します。

17.8.2 ポート間中継遮断機能の設定

ポート間中継遮断機能を設定する手順を次に示します。ここでは，図に示す構成の設定例を示します。

構成例では，ポート 0/1 とポート 0/5 間の通信を遮断します。また，ポート 0/1，0/2 間の通信を遮断します。ポート 0/6 はどのポートとも通信が可能です。

図 17-6 ポート間中継遮断機能の設定例



［設定のポイント］

ポート間中継遮断機能は，イーサネットインタフェースコンフィグレーションモードで，そのポートからの通信を許可しないポートを指定することで設定します。通信を双方向で遮断するためには，遮断したい各ポートで設定する必要があります。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/3**
   ポート 0/3 のイーサネットインタフェースコンフィグレーションモードに移行します。

2. **(config-if)# switchport isolation interface** gigabitethernet 0/4, gigabitethernet 0/5
   (config-if)# exit
   ポート 0/3 でポート 0/4，0/5 からの中継を遮断します。この設定で，ポート 0/3 へ発信する片方向の中継を遮断します。

3. **(config)# interface gigabitethernet 0/4**
   (config-if)# switchport isolation interface gigabitethernet 0/3
   (config-if)# exit
   ポート 0/4 のイーサネットインタフェースコンフィグレーションモードに移行し，ポート 0/4 でポート 0/3 からの中継を遮断します。この設定によって，ポート 0/3，0/4 間は双方向で通信を遮断します。

4. **(config)# interface gigabitethernet 0/5**
   (config-if)# switchport isolation interface gigabitethernet 0/3
   (config-if)# exit
   ポート 0/5 のイーサネットインタフェースコンフィグレーションモードに移行し，ポート 0/5 でポート 0/3 からの中継を遮断します。この設定によって，ポート 0/3，0/5 間は双方向で通信を遮断します。

17.8.3 遮断するポートの変更

［設定のポイント］

コンフィグレーションコマンド switchport isolation add および switchport isolation remove でポート間中継遮断機能で遮断するポートを変更します。すでに設定したポートでコンフィグレーションコマンド switchport isolation interface <interface id list> によって一括して指定した場合，指定した設定に置き換わります。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/4**
   (config-if)# switchport isolation interface gigabitethernet 0/5-10
   ポート 0/4 のイーサネットインタフェースコンフィグレーションモードに移行し，ポート 0/5 ～ 0/10 からポート 0/4 への中継を遮断します。

2. **(config-if)# switchport isolation interface add gigabitethernet 0/11**
   (config-if)# switchport isolation interface remove gigabitethernet 0/5
   ポート 0/11 を追加します。また，ポート 0/5 の設定を解除します。この状態で，0/6 ～ 0/11 からポート 0/4 への通信を遮断します。

3. **(config-if)# switchport isolation interface gigabitethernet 0/6-8**
   (config-if)# exit
   遮断するポートを 0/6 ～ 0/8 に設定します。以前の設定はすべて上書きされ，ポート 0/6 ～ 0/8 からポート 0/4 への中継だけ遮断し，そのほかのポートは通信を可能とします。

17.9 VLAN 拡張機能のオペレーション

17.9.1 運用コマンド一覧

VLAN 拡張機能の運用コマンド一覧を次の表に示します。

表 17-6 運用コマンド一覧

コマンド名	説明
show vlan	VLAN 拡張機能の設定状態を確認します。

17.9.2 VLAN 拡張機能の確認

（1） VLAN の通信状態の確認

VLAN 拡張機能の設定状態を運用コマンド show vlan detail で確認できます。運用コマンド show vlan detail による VLAN 拡張機能の確認方法を次の表に示します。

表 17-7 show vlan detail による VLAN 拡張機能の確認方法

機能	確認方法
VLAN トンネリング	先頭に "VLAN tunneling enabled" を表示します。 （VLAN トンネリングを設定している場合だけ表示します。）
Tag 変換	Port Information で "Tag-Translation" を表示します。
L2 プロトコルフレーム透過機能	BPDU Forwarding，EAPOL Forwarding の欄に表示します。

図 17-7 show vlan detail の実行結果

```
> show vlan 10,4094 detail

Date 20XX/06/06 07:37:32 UTC
VLAN counts: 1                                                    •••1
VLAN ID: 10    Type: Port based      Status: Up
  Learning: On            Tag-Translation: On
  BPDU Forwarding:        EAPOL Forwarding:                       •••3
                :
                :
  Port Information
   0/2(ChGr:64)  Up   Forwarding      Tagged   Tag-Translation:4093   •••2
   0/3(ChGr:64)  Up   Forwarding      Tagged   Tag-Translation:4093
   0/4(ChGr:64)  Down -               Tagged   Tag-Translation:4093

>
```

1. VLAN トンネリングを設定していないので，"VLAN tunneling enabled" を表示していません。
2. このポートに Tag 変換が設定されていることを示します。
3. BPDU フォワーディング機能，および EAPOL フォワーディング機能が設定されていないことを示します。

18 スパニングツリー

この章では，スパニングツリー機能の解説と操作方法について説明します。

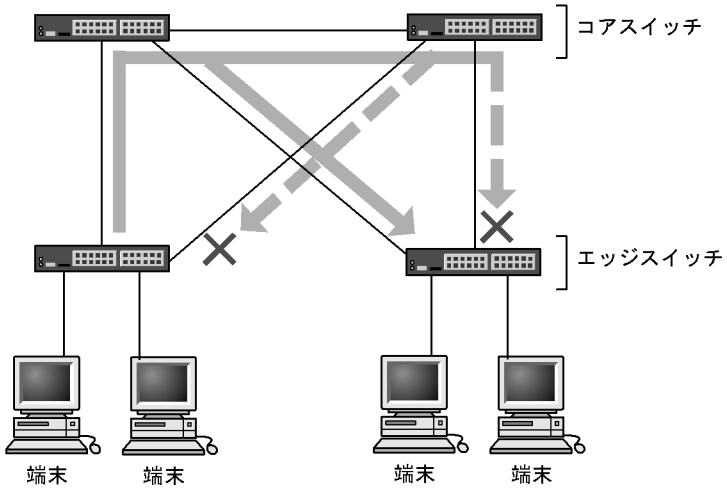
18.1　スパニングツリーの概説

18.1.1　概要

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

スパニングツリーを適用したネットワークの概要を次の図に示します。

図 18-1　スパニングツリーを適用したネットワークの概要



（凡例）×：Blocking状態

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

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

18.1.2　スパニングツリーの種類

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

表 18-1　スパニングツリーの種類

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

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

表 18-2　スパニングツリーの組み合わせと適用範囲

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

注　マルチプルスパニングツリーはほかのツリーと組み合わせて使用できません。

18.1.3　スパニングツリーと高速スパニングツリー

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

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

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

表 18-3 PVST+，STP(シングルスパニングツリー) の状態遷移

状態	状態の概要	次の状態への遷移
Disable	ポートが使用できない状態です。使用可能となるとすぐに Blocking に遷移します。	－
Blocking	通信不可の状態で，MAC アドレス学習も行いません。リンクアップ直後またはトポロジーが安定して Blocking になるポートもこの状態になります。	20 秒 (変更可能) または BPDU を受信
Listening	通信不可の状態で，MAC アドレス学習も行いません。該当ポートが Learning になる前に，トポロジーが安定するまで待つ期間です。	15 秒 (変更可能)
Learning	通信不可の状態です。しかし，MAC アドレス学習は行います。該当ポートが Forwarding になる前に，事前に MAC アドレス学習を行う期間です。	15 秒 (変更可能)
Forwarding	通信可能の状態です。トポロジーが安定した状態です。	－

（凡例）－：該当なし

表 18-4 Rapid PVST+，Rapid STP(シングルスパニングツリー) の状態遷移

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

（凡例）－：該当なし

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

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

- トポロジーの全体を同じプロトコル（Rapid PVST+ または Rapid STP）で構築する（Rapid PVST+ と Rapid STP の相互接続は「18.3.2 アクセスポートの PVST+」を参照してください)。
- スパニングツリーが動作する装置間は Point-to-Point 接続する。
- スパニングツリーが動作する装置を接続しないポートでは PortFast を設定する。

18.1.4 スパニングツリートポロジーの構成要素

スパニングツリーのトポロジーを設計するためには，ブリッジやポートの役割およびそれらの役割を決定するために用いる識別子などのパラメータがあります。これらの構成要素とトポロジー設計における利用方法を以下に示します。

(1) ブリッジの役割

ブリッジの役割を次の表に示します。スパニングツリーのトポロジー設計はルートブリッジを決定するこ

とから始まります。

表 18-5 ブリッジの役割

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

(2) ポートの役割

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

表 18-6 ポートの役割

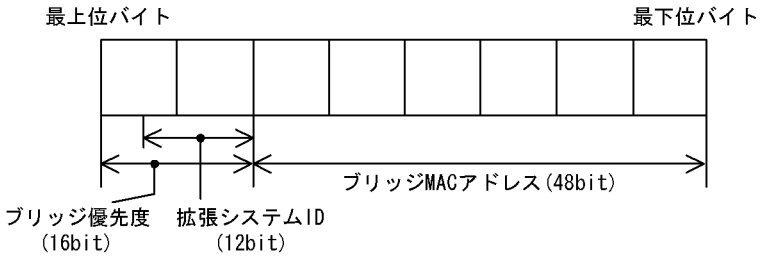
ポートの役割	概要
ルートポート	指定ブリッジからルートブリッジへ向かう通信経路のポートです。通信可能なポートとなります。
指定ポート	ルートポート以外の通信可能なポートです。ルートブリッジからの通信経路でトポロジーの下流へ接続するポートです。
非指定ポート	ルートポート，指定ポート以外のポートで，通信不可の状態のポートです。障害が発生した際に通信可能になり代替経路として使用します。

(3) ブリッジ識別子

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

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

図 18-2 ブリッジ識別子



(4) パスコスト

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

速度が速いポートほどパスコストを低くすることをお勧めしています。パスコストはデフォルト値がポー

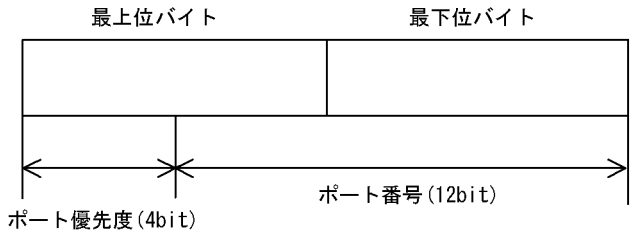
トの速度に応じた値となっていて，コンフィグレーションで変更することもできます。

(5) ポート識別子

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

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

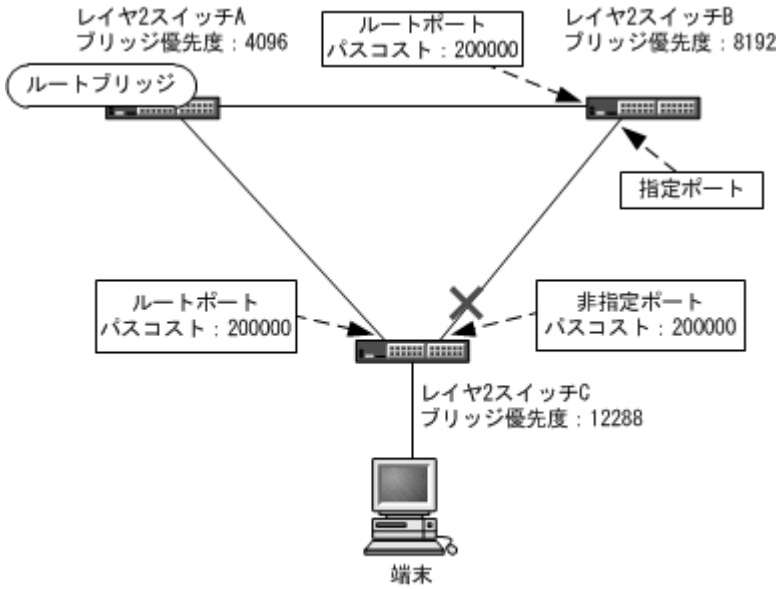
図 18-3 ポート識別子



18.1.5 スパニングツリーのトポロジー設計

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

図 18-4 スパニングツリーのトポロジー設計



（凡例） × ：Blocking状態

(1) ブリッジ識別子によるルートブリッジの選出

ルートブリッジは，ブリッジ識別子の最も小さい装置を選出します。通常，ルートブリッジにしたい装置

のブリッジ優先度を最も小さい値（最高優先度）に設定します。図の例では，レイヤ 2 スイッチ A がルートブリッジになるように設定します。レイヤ 2 スイッチ B，レイヤ 2 スイッチ C は指定ブリッジとなります。

また，ルートブリッジに障害が発生した場合に代替のルートブリッジとして動作するスイッチをレイヤ 2 スイッチ B になるように設定します。レイヤ 2 スイッチ C は最も低い優先度として設定します。

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

（2） 通信経路の設計

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

（a） パスコストによるルートポートの選出

レイヤ 2 スイッチ B，レイヤ 2 スイッチ C では，ルートブリッジに到達するための経路を最も小さいルートパスコスト値になるよう決定します。図の例は，すべてのポートがパスコスト 200000 としています。それぞれ直接接続したポートが最もルートパスコストが小さく，ルートポートとして選出します。

ルートパスコストの計算は，指定ブリッジからルートブリッジへ向かう経路で，各装置がルートブリッジの方向で送信するポートのパスコストの総和で比較します。例えば，レイヤ 2 スイッチ C のレイヤ 2 スイッチ B を経由する経路はパスコストが 400000 となりルートポートには選択されません。

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

（b） 指定ポート，非指定ポートの選出

レイヤ 2 スイッチ B，レイヤ 2 スイッチ C 間の接続はルートポート以外のポートでの接続になります。このようなポートではどれかのポートが非指定ポートとなって Blocking 状態になります。スパニングツリーは，このように片側が Blocking 状態となることでループを防止します。

指定ポート，非指定ポートは次のように選出します。

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

図の例では，ルートパスコストは同一です。ブリッジ優先度によってレイヤ 2 スイッチ B が指定ポート，レイヤ 2 スイッチ C が非指定ポートとなり，レイヤ 2 スイッチ C が Blocking 状態となります。Blocking 状態になるポートをレイヤ 2 スイッチ B にしたい場合は，パスコストを調整してレイヤ 2 スイッチ B のルートパスコストが大きくなるように設定します。

18.1.6 STP 互換モード

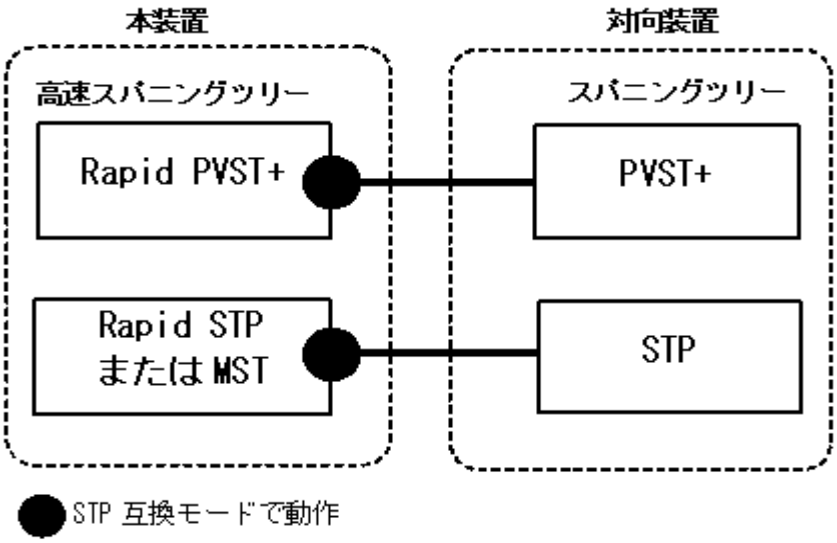
(1) 概要

本装置が高速スパニングツリーで，対向装置がスパニングツリーの場合，本装置の該当するポートは STP 互換モードで動作します。

STP 互換モードで動作中，本装置の該当ポートは対向装置に合わせているため，高速遷移を行いません。

STP 互換モードで動作可能な組み合わせを次の図に示します。

図 18-5 STP 互換モード動作関係図



STP 互換モードで動作していると，該当するポートで高速遷移が行われなくなり，通信復旧に時間が掛かるようになります。

本装置では，高速スパニングツリーへの復旧機能として自動復旧機能と強制復旧機能をサポートしています。

(2) 復旧機能

(a) 自動復旧機能

自動復旧機能は，STP 互換モードで動作中に，対向装置が高速スパニングツリーに変更された場合，STP 互換モードから自動復旧し，再び高速スパニングツリーで動作できるようになります。

- 該当するポートのリンクタイプが point-to-point の場合，STP 互換モード自動復旧機能が動作します。
- 該当するポートが非指定ポート※で STP 互換モードで動作した場合，該当するポートから RST BPDU または MST BPDU を送信することで STP 互換モードを解除します。

  注※
  非指定ポートについては，「18.1.4 スパニングツリートポロジーの構成要素（2）ポートの役割 表 18-6 ポートの役割」を参照してください。
- 該当するポートのリンクタイプが shared の場合，自動復旧モードが正しく動作できないため，自動復旧機能は動作しません。

また，復旧のタイミングによっては，該当するポートと対向装置が STP 互換モードで動作し続ける場合が

あります。

（b） 強制復旧機能

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

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

18.1.7　スパニングツリー共通の注意事項

（1） CPU の過負荷について

CPU が過負荷な状態になった場合，本装置が送受信する BPDU の廃棄が発生して，タイムアウトのメッセージ出力，トポロジー変更，一時的な通信断となることがあります。

（2） VLAN のダウンを伴うコンフィグレーションコマンドの設定について

コンフィグレーションコマンド no spanning-tree disable 設定により，本装置にスパニングツリー機能を適用させると，全 VLAN が一時的にダウンします。

18.2 スパニングツリー動作モードのコンフィグレーション

スパニングツリーの動作モードを設定します。

コンフィグレーションを設定しない状態で本装置を起動すると，動作モードは pvst で動作します。

18.2.1 コンフィグレーションコマンド一覧

スパニングツリー動作モードのコンフィグレーションコマンド一覧を次の表に示します。

表 18-7 コンフィグレーションコマンド一覧

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

18.2.2 動作モードの設定

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

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

表 18-8 スパニングツリー動作モード

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

(1) 動作モード pvst の設定

[設定のポイント]

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

シングルスパニングツリーはデフォルトでは動作しないで，設定することで動作します。その際，デフォルトでは STP で動作し，Rapid STP に変更することもできます。

[コマンドによる設定]

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

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

す。

2. **(config)# spanning-tree vlan 10 mode rapid-pvst**
VLAN 10 の動作モードを Rapid PVST+ に変更します。ほかのポート VLAN は PVST+ で動作し，VLAN 10 は Rapid PVST+ で動作します。

3. **(config)# spanning-tree single**
シングルスパニングツリーを動作させます。PVST+ を使用していない VLAN に適用します。デフォルトでは STP で動作します。

4. **(config)# spanning-tree single mode rapid-stp**
シングルスパニングツリーを Rapid STP に変更します。

（2） 動作モード rapid-pvst の設定

[設定のポイント]

装置の動作モードを rapid-pvst に設定します。ポート VLAN を作成すると，その VLAN で自動的に Rapid PVST+ が動作します。VLAN ごとに PVST+ に変更することもできます。
シングルスパニングツリーはデフォルトでは動作しないで，設定することで動作します。動作モードに rapid-pvst を指定しても，シングルスパニングツリーのデフォルトは STP であることに注意してください。

[コマンドによる設定]

1. **(config)# spanning-tree mode rapid-pvst**
スパニングツリーの動作モードを rapid-pvst に設定します。ポート VLAN で自動的に Rapid PVST+ が動作します。

2. **(config)# spanning-tree vlan 10 mode pvst**
VLAN 10 の動作モードを PVST+ に変更します。ほかのポート VLAN は Rapid PVST+ で動作し，VLAN 10 は PVST+ で動作します。

3. **(config)# spanning-tree single**
シングルスパニングツリーを動作させます。PVST+ を使用していない VLAN に適用します。デフォルトでは STP で動作します。

4. **(config)# spanning-tree single mode rapid-stp**
シングルスパニングツリーを Rapid STP に変更します。

（3） 動作モード mst の設定

[設定のポイント]

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

[コマンドによる設定]

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

マルチプルスパニングツリーを動作させます。

(4) スパニングツリーを停止する設定

[設定のポイント]

スパニングツリーを使用しない場合，disable を設定することで本装置のスパニングツリーをすべて停止します。

[コマンドによる設定]

1. **(config)# spanning-tree disable**
   スパニングツリーの動作を停止します。

18.3　PVST+ 解説

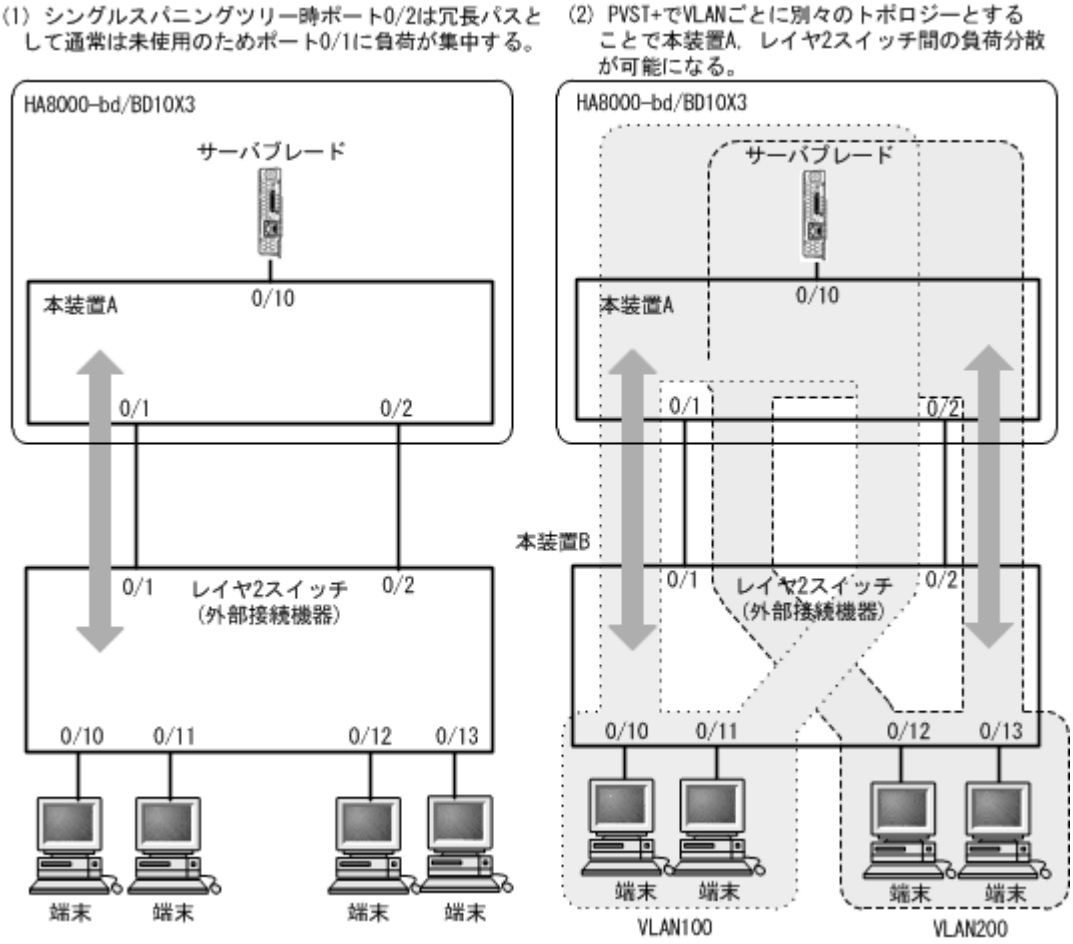
PVST+ は，VLAN 単位にツリーを構築します。VLAN 単位にツリーを構築できるため，ロードバランシングが可能です。また，アクセスポートでは，シングルスパニングツリーで動作しているスイッチと接続できます。

18.3.1　PVST+ によるロードバランシング

次の図に示すような本装置 A，レイヤ 2 スイッチ（外部接続機器）間で冗長パスを組んだネットワークにおいてシングルスパニングツリーを組んだ場合，各端末からサーバへのアクセスは本装置 A，レイヤ 2 スイッチ間のポート 1 に集中します。そこで，複数の VLAN を組み，PVST+ によって VLAN ごとに別々のトポロジーとなるように設定することで冗長パスとして使用できるようになり，さらに負荷分散を図れます。ポート優先度によるロードバランシングの例を次の図に示します。

この例では，VLAN100 に対してはポート 0/1 のポート優先度をポート 0/2 より高く設定し，逆に VLAN200 に対しては 0/2 のポート優先度をポート 0/1 より高く設定することで，各端末からサーバに対するアクセスを VLAN ごとに負荷分散を行っています。

図 18-6　PVST+ によるロードバランシング



18.3.2 アクセスポートの PVST+

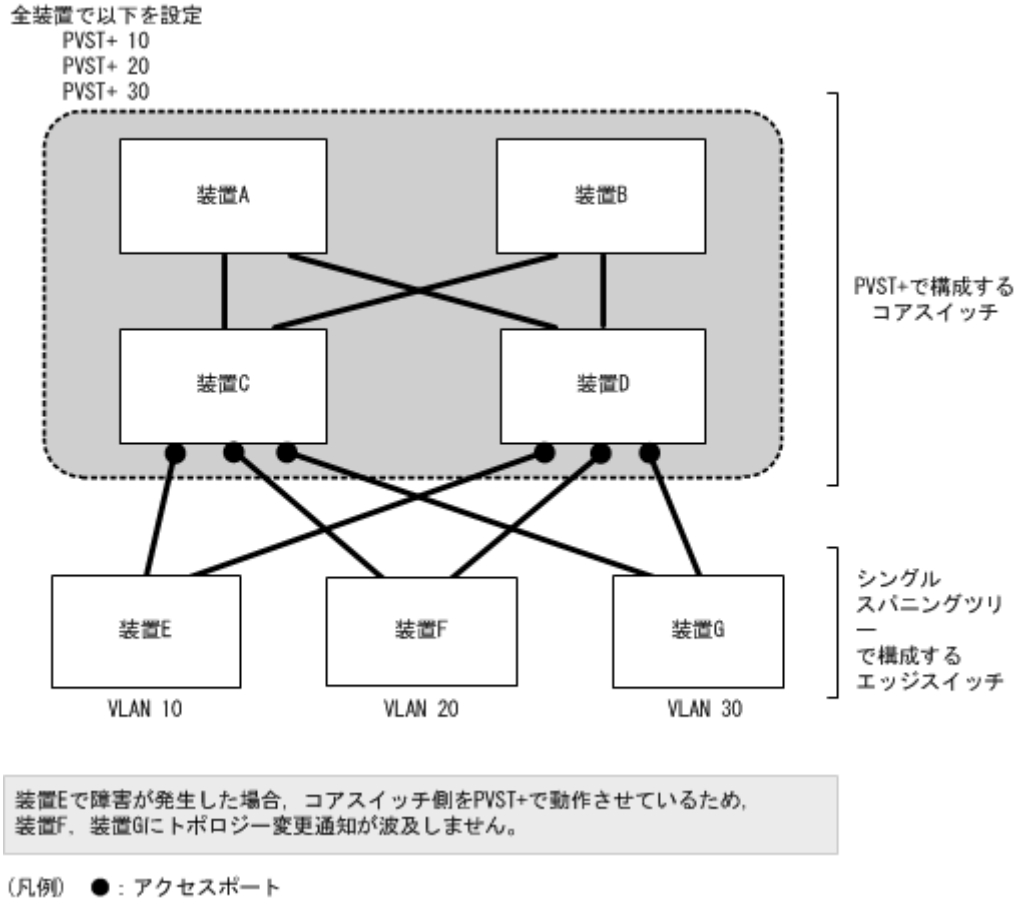
（1） 解説

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

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

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

図 18-7 シングルスパニングツリーとの接続



（2） アクセスポートでシングルスパニングツリーを混在させた場合

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

（3） 構成不一致検出機能

同一 VLAN で接続しているポートについて，本装置でアクセスポート，プロトコルポート，MAC ポートのどれかを設定（Untagged フレームを使用）し，対向装置ではトランクポートを設定（Tagged フレームを使用）した場合，該当 VLAN では通信できないポートとなります。このようなポートを構成不一致として検出します。検出する条件は，本装置がアクセスポートで，対向装置でトランクポートを設定（Tagged フレームを使用）した場合です。この場合，該当するポートを停止状態（Disable）にします。対向装置でトランクポートの設定（Tagged フレームを使用）を削除すれば，hello-time 値× 3 秒（デフォルトは 6 秒）後に，自動的に停止状態を解除します。

18.3.3　PVST+ 使用時の注意事項

（1） 他機能との共存

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

（2） VLAN 1（デフォルト VLAN）の PVST+ とシングルスパニングツリーについて

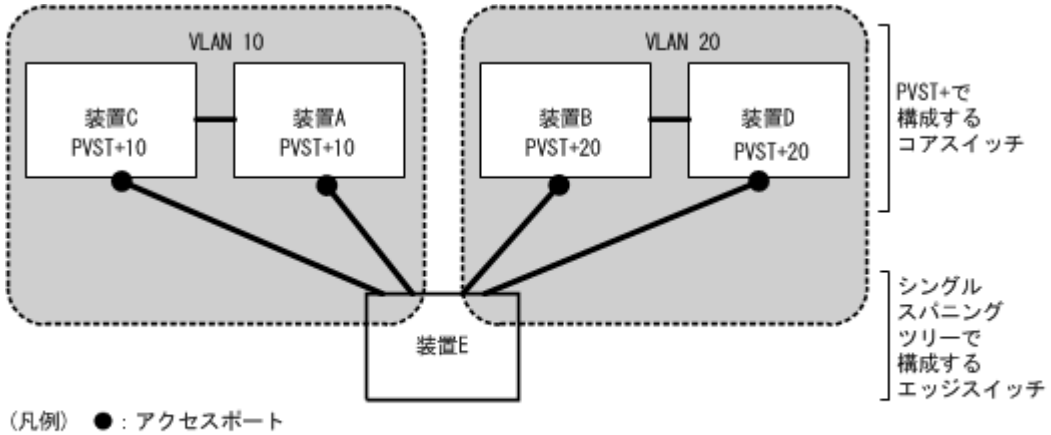
シングルスパニングツリーと VLAN 1 の PVST+ を同時に動作させることはできません。シングルスパニングツリーを動作させると VLAN 1 の PVST+ は停止します。

（3） 禁止構成

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

禁止構成の例を次の図に示します。この例では，装置 E のシングルスパニングツリーが複数の PVST+ スパニングツリーとトポロジーを構成しているため，正しいトポロジーになりません。

図 18-8　シングルスパニングツリーとの禁止構成例



装置Eは単一のスパニングツリーで構成されていないため，正しいトポロジーになりません。

18.4 PVST+ のコンフィグレーション

18.4.1 コンフィグレーションコマンド一覧

PVST+ のコンフィグレーションコマンド一覧を次の表に示します。

表 18-9 コンフィグレーションコマンド一覧

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

18.4.2 PVST+ の設定

[設定のポイント]

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

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

[コマンドによる設定]

1. **(config)# no spanning-tree vlan 20**
   VLAN 20 の PVST+ の動作を停止します。

2. **(config)# spanning-tree vlan 20**
   停止した VLAN 20 の PVST+ を動作させます。

[注意事項]

- PVST+ はコンフィグレーションに表示がないときは自動的に動作しています。コンフィグレーションコマンド no spanning-tree vlan で停止すると，停止状態であることがコンフィグレーションで確認できます。
- PVST+ は最大 250 個のポート VLAN まで動作します。それ以上のポート VLAN を作成しても自動的には動作しません。

18.4.3 PVST+ のトポロジー設定

(1) ブリッジ優先度の設定

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

[設定のポイント]

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

[コマンドによる設定]

1. **(config)# spanning-tree vlan 10 priority 4096**
   VLAN 10 の PVST+ のブリッジ優先度を 4096 に設定します。

(2) パスコストの設定

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

[設定のポイント]

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

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

パスコスト値には short（16bit 値），long（32bit 値）の 2 種類があり，トポロジーの全体で合わせる必要があります。デフォルトでは short（16bit 値）で動作します。イーサネットインタフェースの速度による自動的な設定は，short（16bit 値）か long（32bit 値）かで設定内容が異なります。パスコストのデフォルト値を次の表に示します。

表 18-10 パスコストのデフォルト値

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

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/4**
   (config-if)# spanning-tree cost 100
   (config-if)# exit

ポート 0/4 のパスコストを 100 に設定します。

2. **(config)# spanning-tree pathcost method long**
   (config)# interface gigabitethernet 0/4
   (config-if)# spanning-tree vlan 10 cost 200000
   (config-if)# exit
   long（32bit 値）のパスコストを使用するように設定した後に，ポート 0/4 の VLAN 10 をコスト値 200000 に変更します。ポート 0/4 では VLAN 10 だけパスコスト 200000 となり，そのほかの VLAN は 100 で動作します。

［注意事項］

リンクアグリゲーションを使用する場合，チャネルグループのパスコストのデフォルト値は，チャネルグループ内の全ポートの合計ではなく一つのポートの速度の値となります。

（3） ポート優先度の設定

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

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

［設定のポイント］

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

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/4**
   (config-if)# spanning-tree port-priority 64
   (config-if)# exit
   ポート 0/4 のポート優先度を 64 に設定します。

2. **(config)# interface gigabitethernet 0/4**
   (config-if)# spanning-tree vlan 10 port-priority 144
   (config-if)# exit
   ポート 0/4 の VLAN 10 をポート優先度 144 に変更します。ポート 0/4 では VLAN 10 だけポート優先度 144 となり，そのほかの VLAN は 64 で動作します。

18.4.4 PVST+ のパラメータ設定

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

（1） BPDU の送信間隔の設定

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

[設定のポイント]

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

[コマンドによる設定]

1. **(config)# spanning-tree vlan 10 hello-time 3**
   VLAN 10 の PVST+ の BPDU 送信間隔を 3 秒に設定します。

[注意事項]

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

（2） 送信する最大 BPDU 数の設定

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

[設定のポイント]

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

[コマンドによる設定]

1. **(config)# spanning-tree vlan 10 transmission-limit 5**
   VLAN 10 の Rapid PVST+ の hello-time 当たりの最大送信 BPDU 数を 5 に設定します。

（3） BPDU の最大有効時間の設定

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

[設定のポイント]

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

[コマンドによる設定]

1. **(config)# spanning-tree vlan 10 max-age 25**
   VLAN 10 の PVST+ の BPDU の最大有効時間を 25 秒に設定します。

（4） 状態遷移時間の設定

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

［設定のポイント］

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

［コマンドによる設定］

1. **(config)# spanning-tree vlan 10 forward-time 10**
   VLAN 10 の PVST+ の状態遷移時間を 10 秒に設定します。

18.5　PVST+ のオペレーション

18.5.1　運用コマンド一覧

PVST+ の運用コマンド一覧を次の表に示します。

表 18-11　運用コマンド一覧

コマンド名	説明
show spanning-tree	スパニングツリー情報を表示します。
show spanning-tree statistics	スパニングツリーの統計情報を表示します。
clear spanning-tree statistics	スパニングツリーの統計情報をクリアします。
clear spanning-tree detected-protocol	スパニングツリーの STP 互換モードを強制回復します。
show spanning-tree port-count	スパニングツリーの収容数を表示します。

18.5.2　PVST+ の状態の確認

PVST+ の情報は運用コマンド show spanning-tree の実行結果で示されます。Mode で PVST+，Rapid PVST+ の動作モードを確認できます。トポロジーが正しく構築されていることを確認するためには，Root Bridge ID の内容が正しいこと，Port Information の Status，Role が正しいことを確認してください。

図 18-9　show spanning-tree の実行結果

```
> show spanning-tree vlan 4094

Date 20XX/06/14 11:22:22 UTC
VLAN 4090  PVST+ Spanning Tree:Enabled   Mode:PVST+
  Bridge ID       Priority: 36862     MAC Address: 0000.8710.0001
    Bridge Status: Designated
  Root Bridge ID  Priority: 36862     MAC Address: 0000.87c4.2772
    Root Cost: 19
    Root Port: 0/4
  Port Information
    0/1       Down Status:Disabled    Role:-            LoopGuard
    0/2       Down Status:Disabled    Role:-            LoopGuard
    0/3       Down Status:Disabled    Role:-            LoopGuard
    0/4       Up   Status:Forwarding  Role:Root        PortFast

>
```

18.6 シングルスパニングツリー解説

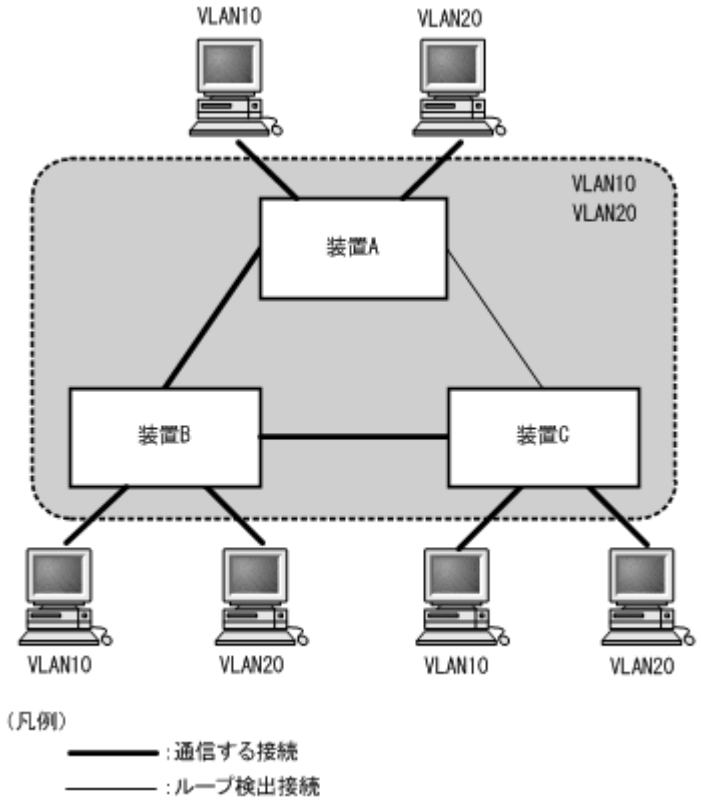
シングルスパニングツリーは装置全体を対象としトポロジーを構築します。

18.6.1 概要

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

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

図 18-10 シングルスパニングツリーによるネットワーク構成



18.6.2 PVST+ との併用

プロトコル VLAN，MAC VLAN では PVST+ を使用できません。また，PVST+ が動作可能な VLAN 数は 250 個であり，それ以上の VLAN で使用することはできません。シングルスパニングツリーを使用することで，PVST+ を使用しながらこれらの VLAN にもスパニングツリーを適用できます。

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

表 18-12　シングルスパニングツリー対象の VLAN

項目	VLAN
PVST+ 対象の VLAN	PVST+ が動作している VLAN。 最大 250 個のポート VLAN は自動的に PVST+ が動作します。
シングルスパニングツリー対象の VLAN	251 個目以上のポート VLAN。
	PVST+ を停止（コンフィグレーションコマンド no spanning-tree vlan で指定）している VLAN。
	デフォルト VLAN（VLAN ID 1 のポート VLAN）。
	プロトコル VLAN。
	MAC VLAN。

18.6.3　シングルスパニングツリー使用時の注意事項

（1）他機能との共存

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

（2）VLAN 1（デフォルト VLAN）の PVST+ とシングルスパニングツリーについて

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

18.7 シングルスパニングツリーのコンフィグレーション

18.7.1 コンフィグレーションコマンド一覧

シングルスパニングツリーのコンフィグレーションコマンド一覧を次の表に示します。

表 18-13 コンフィグレーションコマンド一覧

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

18.7.2 シングルスパニングツリーの設定

［設定のポイント］

シングルスパニングツリーの動作，停止を設定します。シングルスパニングツリーは，動作モード pvst，rapid-pvst を設定しただけでは動作しません。設定することによって動作を開始します。VLAN 1（デフォルト VLAN）とシングルスパニングツリーは同時に使用できません。シングルスパニングツリーを設定すると VLAN 1 の PVST+ は停止します。

［コマンドによる設定］

1. **(config)# spanning-tree single**
   シングルスパニングツリーを動作させます。この設定によって，VLAN 1 の PVST+ が停止し，VLAN 1 はシングルスパニングツリーの対象となります。

2. **(config)# no spanning-tree single**
   シングルスパニングツリーを停止します。VLAN 1 の PVST+ を停止に設定していないで，かつすでに 250 個の PVST+ が動作している状態でない場合，VLAN 1 の PVST+ が自動的に動作を開始します。

18.7.3 シングルスパニングツリーのトポロジー設定

(1) ブリッジ優先度の設定

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

[設定のポイント]

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

[コマンドによる設定]

1. **(config)# spanning-tree single priority 4096**
   シングルスパニングツリーのブリッジ優先度を 4096 に設定します。

(2) パスコストの設定

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

[設定のポイント]

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

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

パスコスト値には short（16bit 値），long（32bit 値）の 2 種類があり，トポロジーの全体で合わせる必要があります。デフォルトでは short（16bit 値）で動作します。イーサネットインタフェースの速度による自動的な設定は，short（16bit 値）か long（32bit 値）かで設定内容が異なります。パスコストのデフォルト値を次の表に示します。

表 18-14 パスコストのデフォルト値

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

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/4**
   (config-if)# spanning-tree cost 100
   (config-if)# exit
   ポート 0/4 のパスコストを 100 に設定します。

2. **(config)# spanning-tree pathcost method long**
   (config)# interface gigabitethernet 0/4
   (config-if)# spanning-tree single cost 200000
   (config-if)# exit
   long（32bit 値）のパスコストを使用するように設定した後に，シングルスパニングツリーのポート 0/4 のパスコストを 200000 に変更します。ポート 0/4 ではシングルスパニングツリーだけパスコスト 200000 となり，同じポートで使用している PVST+ は 100 で動作します。

［注意事項］
リンクアグリゲーションを使用する場合，チャネルグループのパスコストのデフォルト値は，チャネルグループ内の全ポートの合計ではなく一つのポートの速度の値になります。

（3） ポート優先度の設定

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

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

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

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/4**
   (config-if)# spanning-tree port-priority 64
   (config-if)# exit
   ポート 0/4 のポート優先度を 64 に設定します。

2. **(config)# interface gigabitethernet 0/4**
   (config-if)# spanning-tree single port-priority 144
   (config-if)# exit
   シングルスパニングツリーのポート 0/4 のポート優先度を 144 に変更します。ポート 0/4 ではシングルスパニングツリーだけポート優先度 144 となり，同じポートで使用している PVST+ は 64 で動作します。

18.7.4 シングルスパニングツリーのパラメータ設定

各パラメータは「2 × (forward-time − 1) ≧ max-age ≧ 2 × (hello-time + 1)」という関係が成立するように設定する必要があります。パラメータを変える場合はトポロジー全体でパラメータを合わせる必要があります。

（1） BPDU の送信間隔の設定

BPDU の送信間隔は，短くした場合はトポロジー変更を検知しやすくなります。長くした場合はトポロ

ジー変更の検知までに時間が掛かるようになる一方で，BPDU トラフィックや本装置のスパニングツリーの負荷を軽減できます。

[設定のポイント]

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

[コマンドによる設定]

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

[注意事項]

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

（2） 送信する最大 BPDU 数の設定

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

[設定のポイント]

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

[コマンドによる設定]

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

（3） BPDU の最大有効時間

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

[設定のポイント]

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

[コマンドによる設定]

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

（4） 状態遷移時間の設定

STP モードまたは Rapid STP モードでタイマによる動作となる場合，ポートの状態が一定時間ごとに遷

移します。STP モードの場合は Blocking から Listening，Learning，Forwarding と遷移し，Rapid STP モードの場合は Discarding から Learning，Forwarding と遷移します。この状態遷移に必要な時間を設定できます。小さい値を設定すると，より早く Forwarding 状態に遷移できます。

［設定のポイント］

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

［コマンドによる設定］

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

18.8　シングルスパニングツリーのオペレーション

18.8.1　運用コマンド一覧

シングルスパニングツリーの運用コマンド一覧を次の表に示します。

表 18-15　運用コマンド一覧

コマンド名	説明
show spanning-tree	スパニングツリー情報を表示します。
show spanning-tree statistics	スパニングツリーの統計情報を表示します。
clear spanning-tree statistics	スパニングツリーの統計情報をクリアします。
clear spanning-tree detected-protocol	スパニングツリーの STP 互換モードを強制回復します。
show spanning-tree port-count	スパニングツリーの収容数を表示します。

18.8.2　シングルスパニングツリーの状態の確認

シングルスパニングツリーの情報は運用コマンド show spanning-tree で確認してください。Mode で STP，Rapid STP の動作モードを確認できます。トポロジーが正しく構築されていることを確認するためには，Root Bridge ID の内容が正しいこと，Port Information の Status，Role が正しいことを確認してください。

図 18-11　シングルスパニングツリーの情報

```
> show spanning-tree single

Date 20XX/06/14 11:38:40 UTC
Single Spanning Tree:Enabled   Mode:STP
  Bridge ID       Priority: 32768     MAC Address: 0000.8710.0001
    Bridge Status: Root
  Root Bridge ID  Priority: 32768     MAC Address: 0000.8710.0001
    Root Cost: 0
    Root Port: -
  Port Information
    0/1       Down Status:Disabled    Role:-            -
    0/2       Down Status:Disabled    Role:-            RootGuard
    0/3       Down Status:Disabled    Role:-            -
    0/4       Up   Status:Learning    Role:Designated   RootGuard

>
```

18.9　マルチプルスパニングツリー解説

18.9.1　概要

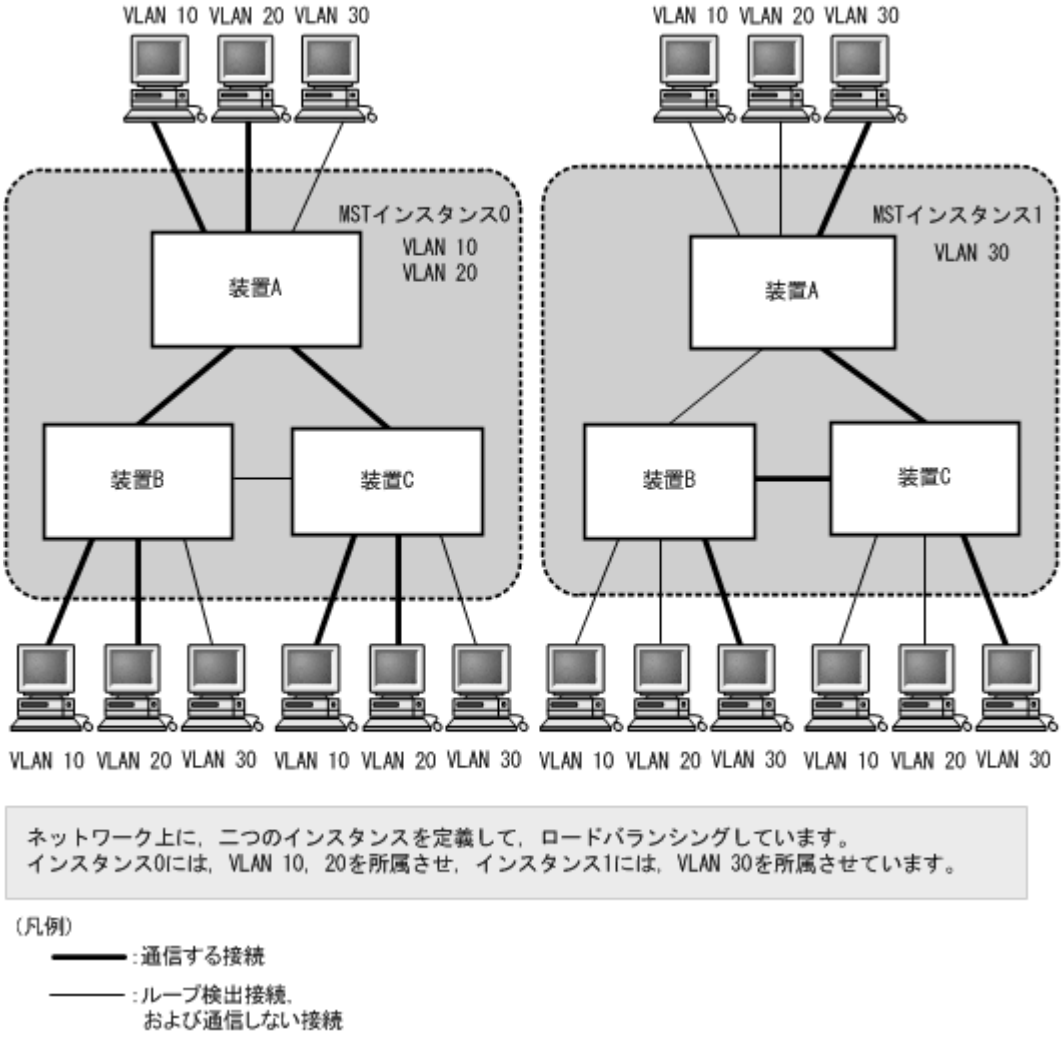
マルチプルスパニングツリーには，次の特長があります。MST インスタンスによってロードバランシングを可能にしています。また，MST リージョンによって，大規模なネットワーク構成を中小構成に分割することでネットワーク設計が容易になります。以降，これらを実現するためのマルチプルスパニングツリーの機能概要を説明します。

（1）MST インスタンス

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

MST インスタンスイメージを次の図に示します。

図 18-12　MST インスタンスイメージ



（2） MST リージョン

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

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

● CST

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

● IST

IST（Internal Spanning Tree）は，MST リージョン外と接続するために，MST リージョン内で Default 動作するトポロジーのことを指し，MST インスタンス ID0 が割り当てられます。MST リージョン外と接続しているポートを境界ポートと呼びます。また，リージョン内，リージョン間で MST

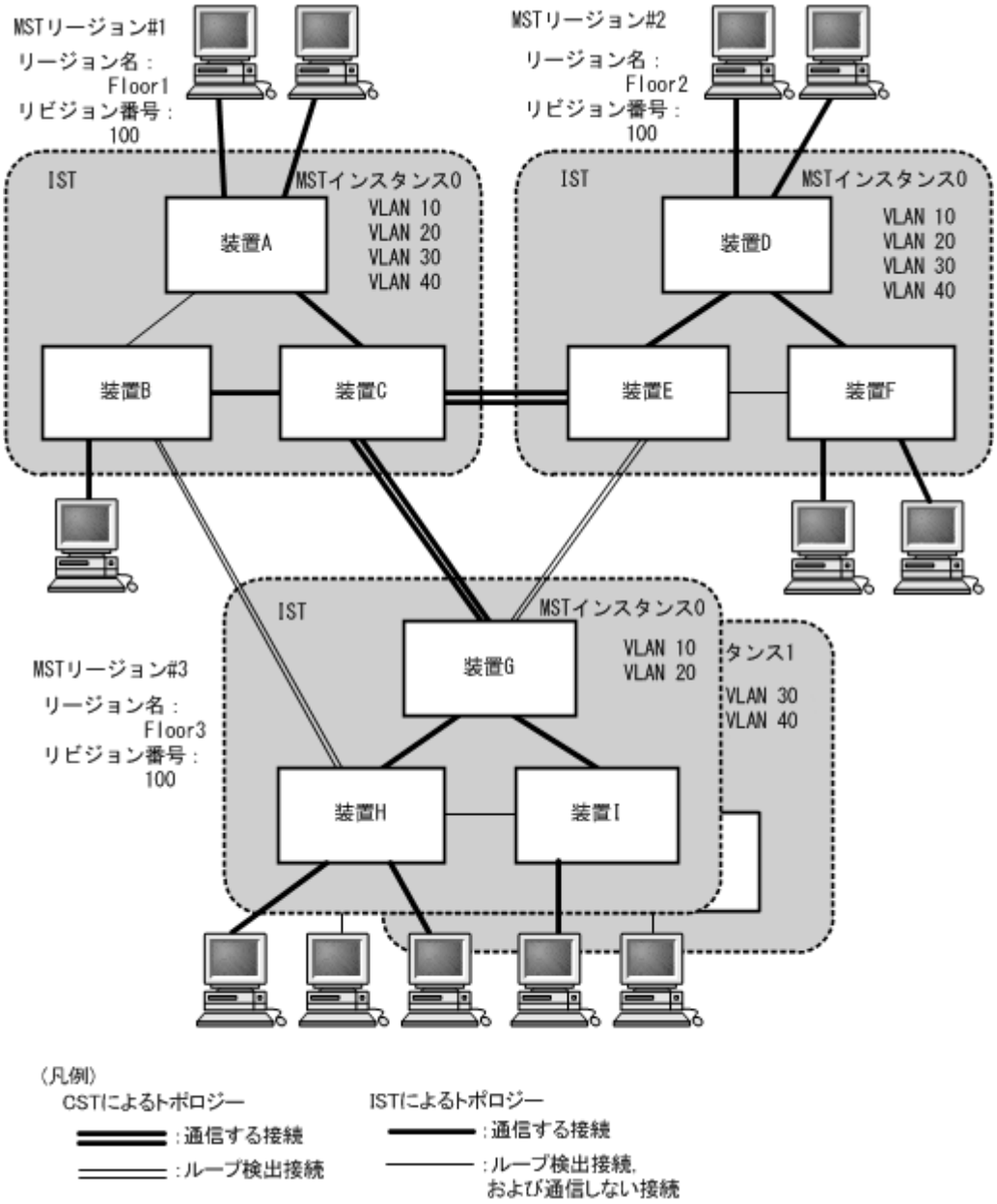
BPDU を送受信する唯一の MST インスタンスとなります。全 MST インスタンスのトポロジー情報は，MST BPDU にカプセル化し通知します。

● CIST

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

マルチプルスパニングツリー概要を次の図に示します。

図 18-13　マルチプルスパニングツリー概要



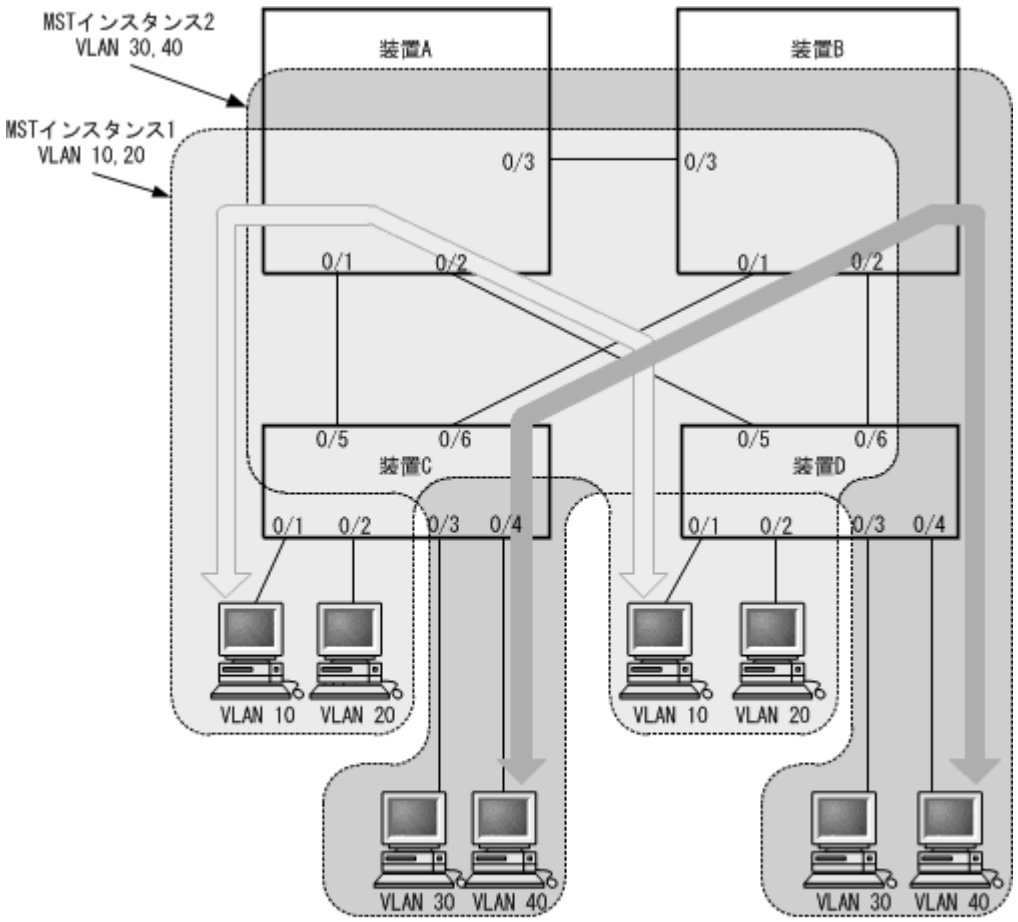
18.9.2　マルチプルスパニングツリーのネットワーク設計

（1）MST インスタンス単位のロードバランシング構成

マルチプルスパニングツリーでは，MST インスタンス単位にロードバランシングができます。ロードバラ

ンシング構成の例を次の図に示します。この例では，VLAN 10，20 を MST インスタンス 1 に，VLAN 30，40 を MST インスタンス 2 に設定して，二つのロードバランシングを行っています。マルチプルスパニングツリーでは，この例のように四つの VLAN であっても二つのツリーだけを管理することでロードバランシングができます。

図 18-14　マルチプルスパニングツリーのロードバランシング構成

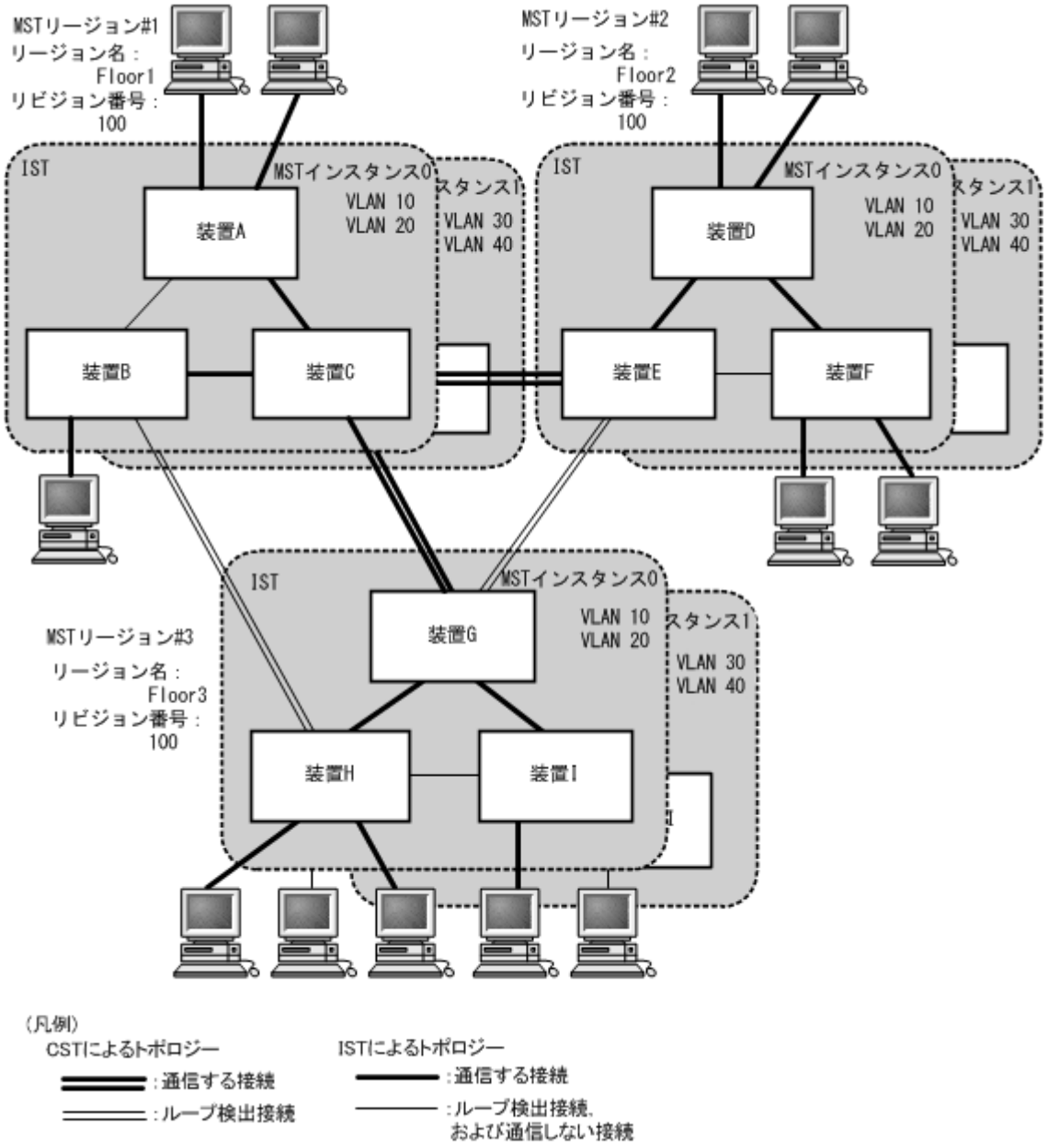


（2） MST リージョンによるネットワーク設計

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

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

図 18-15 MST リージョンによるネットワーク構成



18.9.3 ほかのスパニングツリーとの互換性

（1） シングルスパニングツリーとの互換性

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

（2） PVST+ との互換性

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

18.9.4　マルチプルスパニングツリー使用時の注意事項

（1）他機能との共存

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

（2）MST リージョンについて

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

（3）トポロジーの収束に時間が掛かる場合について

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

表 18-16　ルートブリッジでのイベント発生

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

18.10 マルチプルスパニングツリーのコンフィグレーション

18.10.1 コンフィグレーションコマンド一覧

マルチプルスパニングツリーのコンフィグレーションコマンド一覧を次の表に示します。

表 18-17 コンフィグレーションコマンド一覧

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

18.10.2 マルチプルスパニングツリーの設定

(1) マルチプルスパニングツリーの設定

[設定のポイント]

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

[コマンドによる設定]

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

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

[注意事項]

コンフィグレーションコマンド no spanning-tree mode でマルチプルスパニングツリーの動作モード設定を削除すると，デフォルトの動作モードである pvst になります。その際，ポート VLAN で自動

的に PVST+ が動作を開始します。

(2) リージョン，インスタンスの設定

[設定のポイント]

MST リージョンは，同じリージョンに所属させたい装置はリージョン名，リビジョン番号，MST インスタンスのすべてを同じ設定にする必要があります。
MST インスタンスは，インスタンス番号と所属する VLAN を同時に設定します。リージョンを一致させるために，本装置に未設定の VLAN ID もインスタンスに所属させることができます。インスタンスに所属することを指定しない VLAN は自動的に CIST（インスタンス 0）に所属します。
MST インスタンスは，CIST（インスタンス 0）を含め 16 個まで設定できます。

[コマンドによる設定]

1. **(config)# spanning-tree mst configuration**
   (config-mst)# name "REGION TOKYO"
   (config-mst)# revision 1
   マルチプルスパニングツリーコンフィグレーションモードに移り，name（リージョン名），revision（リビジョン番号）の設定を行います。

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

18.10.3 マルチプルスパニングツリーのトポロジー設定

(1) インスタンスごとのブリッジ優先度の設定

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

[設定のポイント]

ブリッジ優先度は値が小さいほど高い優先度になり，最も小さい値を設定した装置がルートブリッジになります。ルートブリッジはブリッジ優先度と装置の MAC アドレスから成るブリッジ識別子で判定するため，本パラメータを設定しない場合は装置の MAC アドレスが最も小さい装置がルートブリッジになります。
マルチプルスパニングツリーのブリッジ優先度はインスタンスごとに設定します。インスタンスごとに値を変えた場合，インスタンスごとのロードバランシング（異なるトポロジーの構築）ができます。

[コマンドによる設定]

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

設定します。

(2) インスタンスごとのパスコストの設定

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

[設定のポイント]

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

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

パスコストのデフォルト値を次の表に示します。

表 18-18 パスコストのデフォルト値

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

[コマンドによる設定]

1. **(config)# spanning-tree mst configuration**
   (config-mst)# instance 10 vlans 100-150
   (config-mst)# instance 20 vlans 200-250
   (config-mst)# instance 30 vlans 300-350
   (config-mst)# exit
   (config)# interface gigabitethernet 0/4
   (config-if)# spanning-tree cost 2000
   MST インスタンス 10，20，30 を設定し，ポート 0/4 のパスコストを 2000 に設定します。CIST（インスタンス 0），MST インスタンス 10，20，30 のポート 0/4 のパスコストは 2000 になります。

2. **(config-if)# spanning-tree mst 20 cost 500**
   (config-if)# exit
   MST インスタンス 20 のポート 0/4 のパスコストを 500 に変更します。インスタンス 20 以外は 2000 で動作します。

[注意事項]

リンクアグリゲーションを使用する場合，チャネルグループのパスコストのデフォルト値は，チャネルグループ内の全ポートの合計ではなく，一つのポートの速度の値となります。

(3) インスタンスごとのポート優先度の設定

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

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

[設定のポイント]

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

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/4**
   (config-if)# spanning-tree port-priority 64
   (config-if)# exit
   ポート 0/4 のポート優先度を 64 に設定します。

2. **(config)# interface gigabitethernet 0/4**
   (config-if)# spanning-tree mst 20 port-priority 144
   (config-if)# exit
   インスタンス 20 のポート 0/4 にポート優先度 144 を設定します。ポート 0/4 ではインスタンス 20 だけポート優先度 144 となり，そのほかのインスタンスは 64 で動作します。

18.10.4 マルチプルスパニングツリーのパラメータ設定

各パラメータは「2 × (forward-time − 1) ≧ max-age ≧ 2 × (hello-time + 1)」という関係が成立するように設定する必要があります。パラメータを変える場合はトポロジー全体でパラメータを合わせる必要があります。

(1) BPDU の送信間隔の設定

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

[設定のポイント]

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

[コマンドによる設定]

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

[注意事項]

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

（2） 送信する最大 BPDU 数の設定

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

［設定のポイント］

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

［コマンドによる設定］

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

（3） 最大ホップ数の設定

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

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

［設定のポイント］

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

［コマンドによる設定］

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

（4） BPDU の最大有効時間の設定

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

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

［設定のポイント］

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

［コマンドによる設定］

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

(5) 状態遷移時間の設定

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

[設定のポイント]

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

[コマンドによる設定]

1. **(config)# spanning-tree mst forward-time 10**
   マルチプルスパニングツリーの BPDU の状態遷移時間を 10 秒に設定します。

18.11 マルチプルスパニングツリーのオペレーション

18.11.1 運用コマンド一覧

マルチプルスパニングツリーの運用コマンド一覧を次の表に示します。

表 18-19 運用コマンド一覧

コマンド名	説明
show spanning-tree	スパニングツリー情報を表示します。
show spanning-tree statistics	スパニングツリーの統計情報を表示します。
clear spanning-tree statistics	スパニングツリーの統計情報をクリアします。
clear spanning-tree detected-protocol	スパニングツリーの STP 互換モードを強制回復します。
show spanning-tree port-count	スパニングツリーの収容数を表示します。

18.11.2 マルチプルスパニングツリーの状態の確認

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

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

show spanning-tree の実行結果を次の図に示します。

図 18-16 show spanning-tree の実行結果

```
> show spanning-tree mst instance 4095

Date 20XX/06/14 13:04:05 UTC
Multiple Spanning Tree: Enabled
Revision Level: 0      Configuration Name:
MST Instance 4095
  VLAN Mapped: 4094
  Regional Root  Priority: 36863       MAC      : 0000.8710.0001
  Internal Root Cost     : 0           Root Port: -
  Bridge ID      Priority: 36863       MAC      : 0000.8710.0001
  Regional Bridge Status : Root
  Port Information
    0/1       Down Status:Disabled    Role:-            -
    0/2       Down Status:Disabled    Role:-            -
    0/3       Down Status:Disabled    Role:-            -
    0/4       Up   Status:Forwarding  Role:Designated   PortFast

>
```

1. インスタンスマッピング VLAN（VLAN Mapped）の表示について
   本装置は 1 ～ 4094 の VLAN ID をサポートしていますが，リージョンの設定に用いる VLAN ID は規格に従い 1 ～ 4095 としています。表示は規格がサポートする VLAN ID1 ～ 4095 がどのインスタンスに所属しているか確認できるようにするため 1 ～ 4095 を明示します。

18.12　スパニングツリー共通機能解説

18.12.1　PortFast

（1） 概要

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

PortFast 機能は，PortFast の設定とポートの種類に従って動作します。PortFast 機能の動作条件を次の表に示します。

表 18-20　PortFast 機能の動作条件

コンフィグレーションの設定		ポートの種類	
ポート単位の設定 (spanning-tree portfast)	装置単位の設定 (spanning-tree portfast default)	アクセスポート プロトコルポート MAC ポート	トランクポート
PortFast 設定（trunk）	（ポート単位の設定を優先）	○	○
PortFast 無効（disable）		×	×
パラメータ省略時		○	×
コマンド未設定	コマンド設定	○	×
	コマンド未設定	×	×

（凡例）
　○：動作可，×：動作不可

（2） PortFast 適用時の BPDU 受信

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

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

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

（3） PortFast 適用時の BPDU 送信

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

ただし，PortFast を設定したポート同士を誤って接続した状態を検出するために，PortFast 機能によって即時に通信可状態になった時点から 10 フレームだけ BPDU の送信を行います。

（4） BPDU ガード

PortFast に適用する機能として，BPDU ガード機能があります。BPDU ガード機能を適用したポートで

は，BPDU 受信時に，スパニングツリー対象のポートとして動作するのではなくポートを inactive 状態にします。

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

18.12.2 BPDU フィルタ

（1） 概要

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

（2） BPDU フィルタに関する注意事項

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

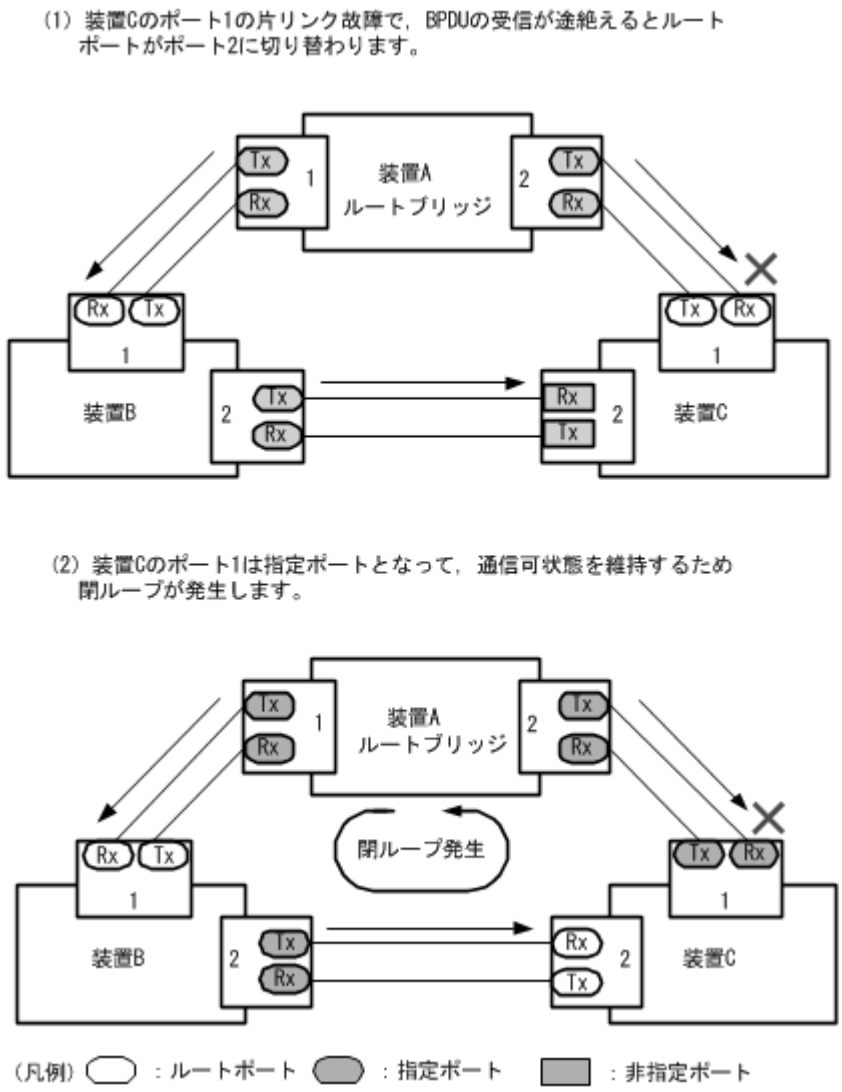
18.12.3　ループガード

（1） 概要

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

次の図に単一方向のリンク障害時の問題点を示します。

図 18-17　単一方向のリンク障害時の問題点



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

ループガード機能は，装置またはポート単位で PortFast 機能を設定している場合，またはルートガード機能を設定したポートでは動作しません。

ループガードの動作条件を次の表に示します。

表 18-21 ループガードの動作条件

PortFast 機能	コンフィグレーションの設定		ループガードの動作
	ポート単位の設定 (spanning-tree guard)	装置単位の設定 (spanning-tree loopguard default)	
有効	ループガード設定（loop）	（ポート単位の設定を優先）	×
	ガード無効設定（none）		×
	ルートガード設定（root）		×
	コマンド未設定	コマンド設定	×
		コマンド未設定	×
無効	ループガード設定（loop）	（ポート単位の設定を優先）	○
	ガード無効設定（none）		×
	ルートガード設定（root）		×
	コマンド未設定	コマンド設定	○
		コマンド未設定	×

（凡例）
○：動作可，×：動作不可

（2） ループガードに関する注意事項

ループガードはマルチプルスパニングツリーでは使用できません。

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

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

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

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

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

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

18.12.4　ルートガード

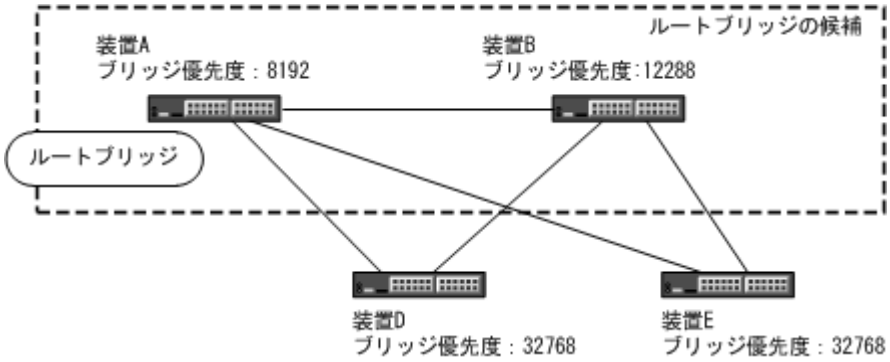
（1）概要

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

誤って装置が接続されたときの問題点を次の図に示します。

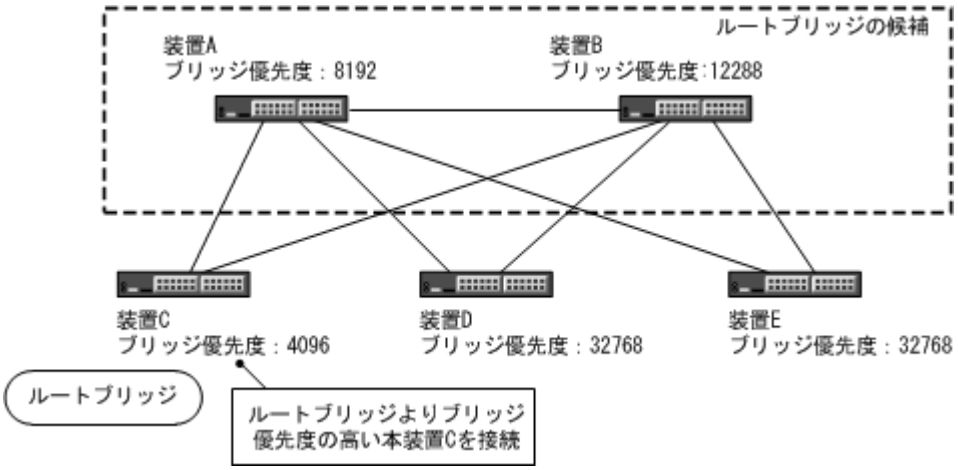
● 装置 A，装置 B をルートブリッジの候補として運用

図 18-18　装置 A，装置 B をルートブリッジの候補として運用



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

図 18-19　装置 A，装置 B よりブリッジ優先度の高い装置 C を接続



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

ルートガードの動作条件を次の表に示します。

表 18-22 ルートガードの動作条件

コンフィグレーションの設定		ルートガードの動作
ポート単位の設定 (spanning-tree guard)	装置単位の設定 (spanning-tree loopguard default)	
ループガード設定（loop）	（ポート単位の設定を優先）	×
ガード無効設定（none）		×
ルートガード設定（root）		○
コマンド未設定	コマンド設定	×
	コマンド未設定	×

（凡例）
○：動作可，×：動作不可

18.13　スパニングツリー共通機能のコンフィグレーション

18.13.1　コンフィグレーションコマンド一覧

スパニングツリー共通機能のコンフィグレーションコマンド一覧を次の表に示します。

表 18-23　コンフィグレーションコマンド一覧

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

18.13.2　PortFast の設定

（1） PortFast の設定

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

［設定のポイント］

コンフィグレーションコマンド spanning-tree portfast default を設定すると，アクセスポート，プロトコルポート，MAC ポートにデフォルトで PortFast 機能を適用します。デフォルトで適用してポートごとに無効にしたい場合は，コンフィグレーションコマンド spanning-tree portfast disable を設定します。

トランクポートでは，ポートごとの指定で適用できます。

［コマンドによる設定］

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

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

2. **(config)# interface gigabitethernet 0/3**
   (config-if)# switchport mode access
   (config-if)# spanning-tree portfast disable
   (config-if)# exit

   ポート 0/3（アクセスポート）で PortFast 機能を使用しないように設定します。

3. **(config)# interface gigabitethernet 0/4**
   (config-if)# switchport mode trunk

```
(config-if)# spanning-tree portfast trunk
(config-if)# exit
```

ポート 0/4 をトランクポートに指定し，PortFast 機能を適用します。トランクポートはデフォルトでは適用されません。ポートごとに指定するためには trunk パラメータを指定する必要があります。

（2） BPDU ガードの設定

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

［設定のポイント］

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

［コマンドによる設定］

1.
```
(config)# spanning-tree portfast default
(config)# spanning-tree portfast bpduguard default
```

すべてのアクセスポート，プロトコルポート，MAC ポートに対して PortFast 機能を設定します。また，PortFast 機能を適用したすべてのポートに対し BPDU ガード機能を設定します。

2.
```
(config)# interface gigabitethernet 0/3
(config-if)# spanning-tree bpduguard disable
(config-if)# exit
```

ポート 0/3(アクセスポート）で BPDU ガード機能を使用しないように設定します。ポート 0/3 は通常の PortFast 機能を適用します。

3.
```
(config)# interface gigabitethernet 0/4
(config-if)# switchport mode trunk
(config-if)# spanning-tree portfast trunk
(config-if)# exit
```

ポート 0/4（トランクポート）に PortFast 機能を設定します。また，BPDU ガード機能を設定します。トランクポートはデフォルトでは PortFast 機能を適用しないためポートごとに設定します。デフォルトで BPDU ガード機能を設定している場合は，PortFast 機能を設定すると自動的に BPDU ガードも適用します。デフォルトで設定していない場合は，コンフィグレーションコマンド spanning-tree bpduguard enable で設定します。

18.13.3 BPDU フィルタの設定

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

［設定のポイント］

インタフェース単位に BPDU フィルタ機能を設定できます。

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/4**
   (config-if)# spanning-tree bpdufilter enable
   (config-if)# exit
   ポート 0/4 で BPDU フィルタ機能を設定します。

18.13.4 ループガードの設定

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

［設定のポイント］

ループガードは，PortFast 機能を設定していないポートで動作します。

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

［コマンドによる設定］

1. **(config)# spanning-tree loopguard default**
   PortFast を設定したポート以外のすべてのポートに対してループガード機能を適用するように設定します。

2. **(config)# interface gigabitethernet 0/3**
   (config-if)# spanning-tree guard none
   (config-if)# exit
   デフォルトでループガードを適用するように設定した状態で，ポート 0/3 はループガードを無効にするように設定します。

3. **(config)# no spanning-tree loopguard default**
   (config)# interface gigabitethernet 0/4
   (config-if)# spanning-tree guard loop
   (config-if)# exit
   デフォルトでループガードを適用する設定を削除します。また，ポート 0/4 に対してポートごとの設定でループガードを適用します。

18.13.5 ルートガードの設定

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

［設定のポイント］

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

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

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/4**
   (config-if)# spanning-tree guard root
   (config-if)# exit
   ポート 0/4 でルートガード機能を設定します。

18.13.6 リンクタイプの設定

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

［設定のポイント］

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

［コマンドによる設定］

1. **(config)# interface gigabitethernet 0/4**
   (config-if)# spanning-tree link-type point-to-point
   (config-if)# exit
   ポート 0/4 を point-to-point 接続とみなして動作させます。

［注意事項］

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

18.14　スパニングツリー共通機能のオペレーション

18.14.1　運用コマンド一覧

スパニングツリー共通機能の運用コマンド一覧を次の表に示します。

表 18-24　運用コマンド一覧

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

18.14.2　スパニングツリー共通機能の状態の確認

スパニングツリーの情報は運用コマンド show spanning-tree detail で確認してください。VLAN 4094 の PVST+ の例を次の図に示します。

- PortFast はポート 0/20 に設定していることを PortFast の項目で確認できます。
- ループガードはポート 0/17 に設定していることを Loop Guard の項目で確認できます。
- ルートガードは RootGuard，BPDU フィルタは BPDUFilter の項目で確認できます。（本例では，どちらも OFF を表示しているので未設定を示しています。）
- リンクタイプは各ポートの Link Type の項目で確認できます。（本例は，PVST+ のため " － " を表示します。）

図 18-20　スパニングツリーの情報

```
> show spanning-tree vlan 4094 detail

Date 20XX/06/14 11:26:46 UTC
VLAN 4094  PVST+ Spanning Tree:Enabled   Mode:PVST+
  Bridge ID
    Priority:36862                 MAC Address:0000.8710.0001
    Bridge Status:Designated       Path Cost Method:Short
    Max Age:20                     Hello Time:2
    Forward Delay:15
  Root Bridge ID
    Priority:36862                 MAC Address:0000.87c4.2772
    Root Cost:19
    Root Port:0/4
    Max Age:20                     Hello Time:2
    Forward Delay:15
  Port Information
  Port:0/3 Down
    Status:Disabled                Role:-
    Priority:128                   Cost:-
    Link Type:-                    Compatible Mode:-
    Loop Guard:ON(Blocking)        PortFast:OFF
    BPDUFilter:OFF                 RootGuard:OFF
  Port:0/4 Up
    Status:Forwarding              Role:Root
    Priority:128                   Cost:19
    Link Type:-                    Compatible Mode:-
    Loop Guard:OFF                 PortFast:ON(BPDU received)
    BPDUFilter:OFF                 RootGuard:OFF
    BPDU Parameters(20XX/06/14 11:26:47):
      Designated Root
        Priority:36862             MAC address:0000.87c4.2772
      Designated Bridge
        Priority:36862             MAC address:0000.87c4.2772
        Root Cost:0
      Port ID
        Priority:128               Number:20
```

```
        Message Age Timer:2(0)/20
    >
```

19 Ring Protocol の解説

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

19.1　Ring Protocol の概要

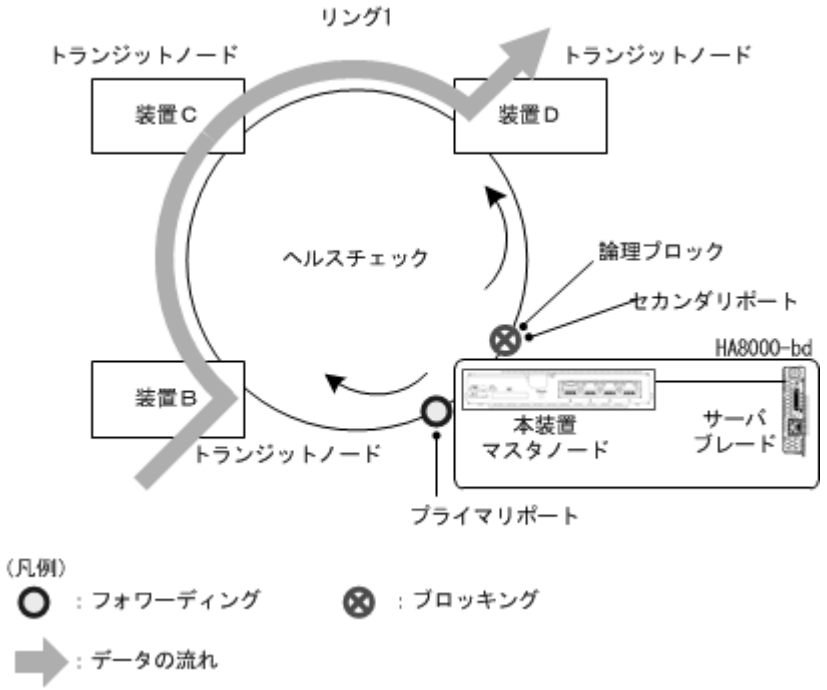
19.1.1　概要

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

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

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

図 19-1　Ring Protocol の概要



リングを構成するノードのうち一つをマスタノードとして，ほかのリング構成ノードをトランジットノードとします。各ノード間を接続する二つのポートをリングポートと呼び，マスタノードのリングポートにはプライマリポートとセカンダリポートがあります。マスタノードはセカンダリポートを論理ブロックすることでリング構成を分断します。これによって，データフレームのループを防止しています。マスタノードはリング内の状態監視を目的とした制御フレーム（ヘルスチェックフレーム）を定期的に送信します。マスタノードは，巡回したヘルスチェックフレームの受信，未受信によって，リング内で障害が発生していないかどうかを判断します。障害または障害復旧を検出したマスタノードは，セカンダリポートの論理ブロックを設定または解除することで経路を切り替え，通信を復旧させます。

19.1.2　特長

（1）イーサネットベースのリングネットワーク

Ring Protocol はイーサネットベースのネットワーク冗長化プロトコルです。従来のリングネットワークで

は FDDI のように二重リンクの光ファイバを用いたネットワークが主流でしたが，Ring Protocol を用いることでイーサネットを用いたリングネットワークが構築できます。

Ring Protocol の適用例を次の図に示します。

図 19-2　Ring Protocol の適用例（その 1）

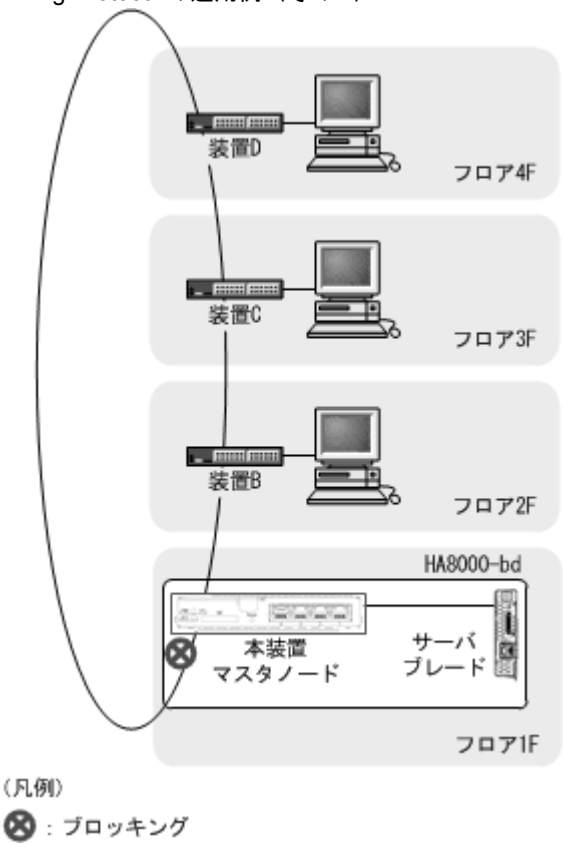
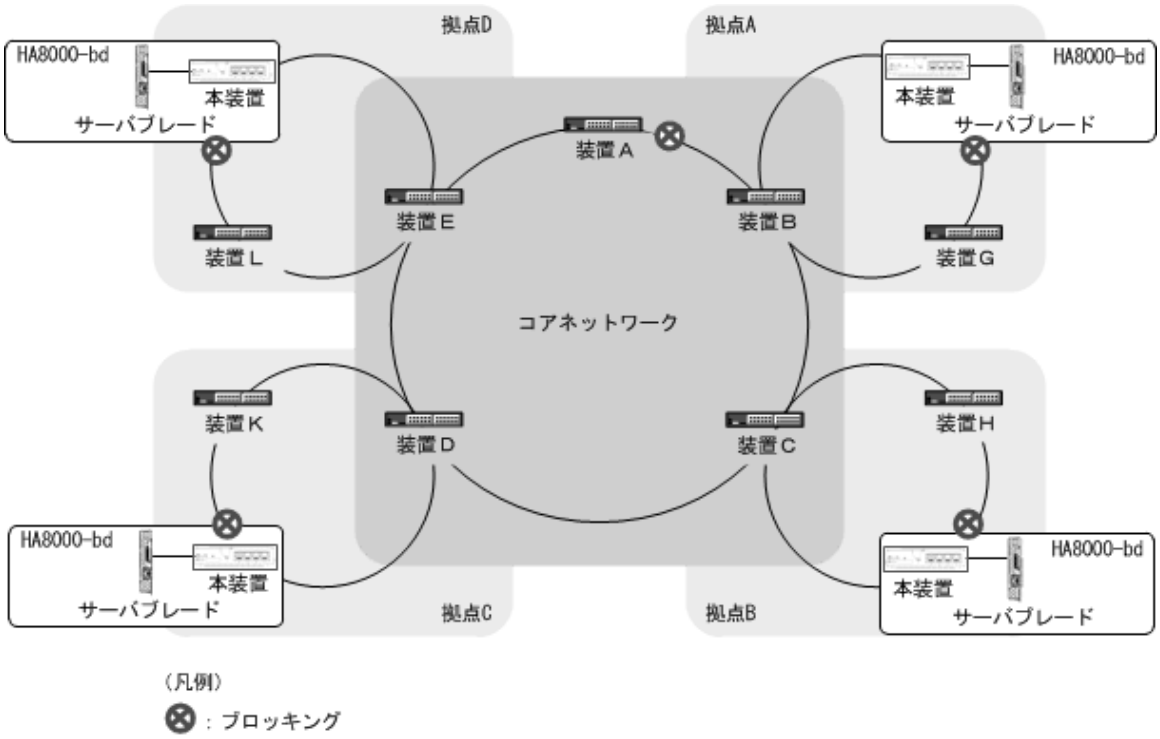


図 19-3　Ring Protocol の適用例（その 2）



（2） シンプルな動作方式

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

（3） 制御フレーム

Ring Protocol では，本プロトコル独自の制御フレームを使用します。制御フレームは，マスタノードによるリング状態の監視やマスタノードからトランジットノードへの経路の切り替え指示に使われます。制御フレームの送受信は，専用の VLAN 上で行われるため，通常のスパニングツリーのようにデータフレームと制御フレームが同じ VLAN 内に流れることはありません。また，制御フレームは優先的に処理されるため，データトラフィックが増大しても制御フレームに影響を与えません。

（4） 負荷分散方式

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

19.1.3　サポート仕様

Ring Protocol でサポートする項目と仕様を次の表に示します。

表 19-1　Ring Protocol でサポートする項目・仕様

項目		内容
適用レイヤ	レイヤ 2	○

項目		内容
	レイヤ 3	×
リング構成	シングルリング	○
	マルチリング	○（共有リンクありマルチリング構成含む）
ノード	マスタノード	○
	トランジットノード	○
	共有ノード	○
装置当たりのリング ID 最大数		51 ただし，Ring Protocol とスパニングツリーの併用，または多重障害監視機能を使用する場合は，8 とする。
リングポート（1 リング ID 当たりのポート数）		2（物理ポートまたはリンクアグリゲーション）
VLAN 数	1 リング ID 当たりの制御 VLAN 数	1（デフォルト VLAN の設定は不可）
	1 リング ID 当たりのデータ転送用 VLAN グループ最大数	2
	1 データ転送用 VLAN グループ当たりの VLAN マッピング最大数	128
	1VLAN マッピング当たりの VLAN 最大数	1023
ヘルスチェックフレーム送信間隔		200 ～ 60000 ミリ秒の範囲で 50 ミリ秒単位
障害監視時間		500 ～ 300000 ミリ秒の範囲で 50 ミリ秒単位
負荷分散方式		二つのデータ転送用 VLAN グループを使用することで可能
多重障害監視機能	装置当たりの多重障害監視可能リング数	4
	1 リング ID 当たりの多重障害監視 VLAN 数	1（デフォルト VLAN の設定は不可）
	多重障害監視フレーム送信間隔	500 ～ 60000 ミリ秒の範囲で 50 ミリ秒単位
	多重障害監視時間	1000 ～ 300000 ミリ秒の範囲で 50 ミリ秒単位

（凡例） ○：サポート ×：未サポート

19.2　Ring Protocol の基本原理

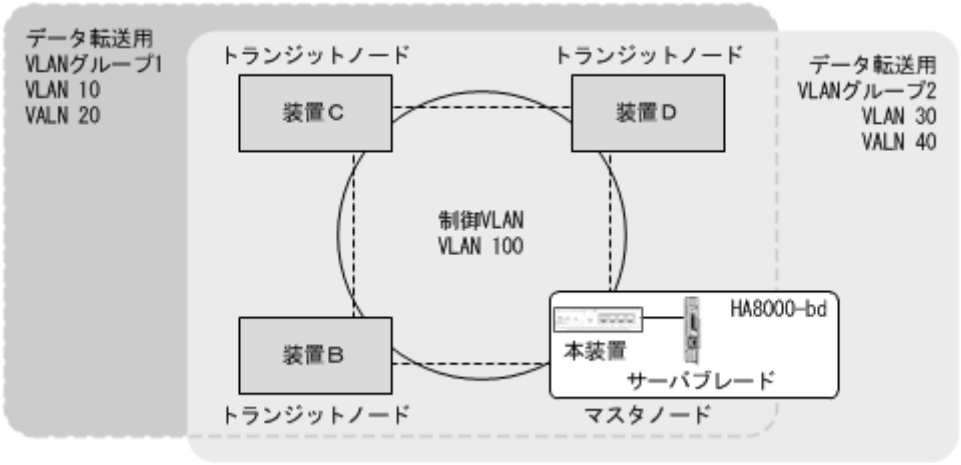
19.2.1　ネットワーク構成

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

（1） シングルリング構成

シングルリング構成について，次の図に示します。

図 19-4　シングルリング構成

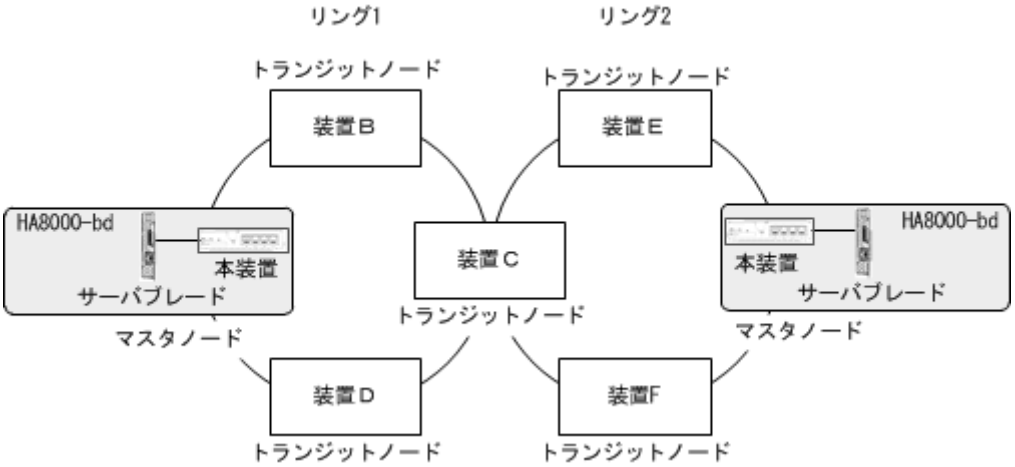


マスタノード 1 台とトランジットノード数台から成る一つのリング構成をシングルリング構成と呼びます。リングを構成するノード間は，リングポートとして，物理ポートまたはリンクアグリゲーションで接続されます。また，リングを構成するすべてのノードに，制御 VLAN として同一の VLAN，およびデータフレームの転送用として共通の VLAN を使用する必要があります。マスタノードから送信した制御フレームは，制御 VLAN 内を巡回します。データフレームの送受信に使用する VLAN は，VLAN グループと呼ばれる一つの論理的なグループに束ねて使用します。VLAN グループは複数の VLAN をまとめるこ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

（2） マルチリング構成

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

図 19-5 マルチリング構成

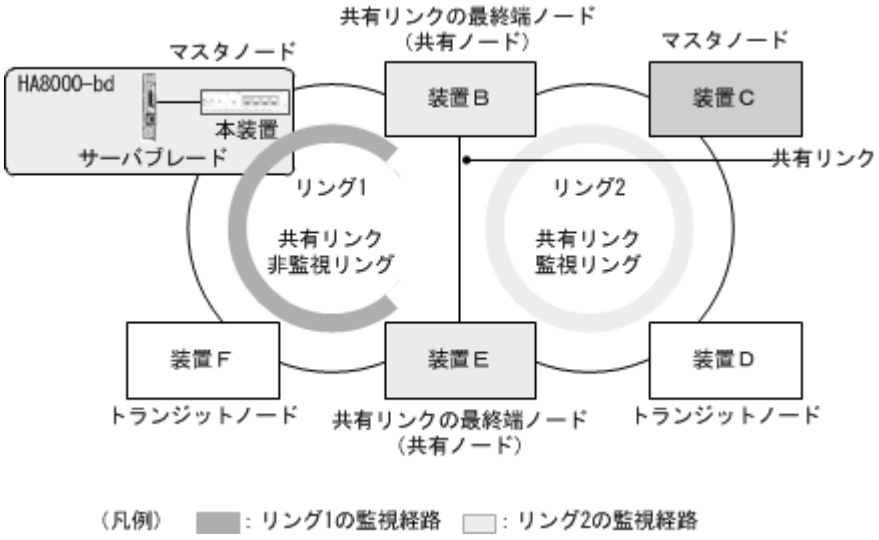


それぞれのリングを構成しているノードは独立したシングルリングとして動作します。このため，リング障害の検出および復旧の検出はそれぞれのリングで独立して行われます。

(3) 共有リンクありのマルチリング構成

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

図 19-6 共有リンクありのマルチリング構成



複数のシングルリングが，二つ以上のノードで接続されている場合，複数のリングでリンクを共有することになります。このリンクを共有リンクと呼び，共有リンクのあるマルチリング構成を，共有リンクありのマルチリング構成と呼びます。これに対し，(2) 図 19-5 マルチリング構成のように，複数のシングルリングが一つのノードで接続されている場合には，共有リンクがありませんので，共有リンクなしのマルチリング構成と呼びます。

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

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

19.2.2 制御 VLAN

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

19.2.3 障害監視方法

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

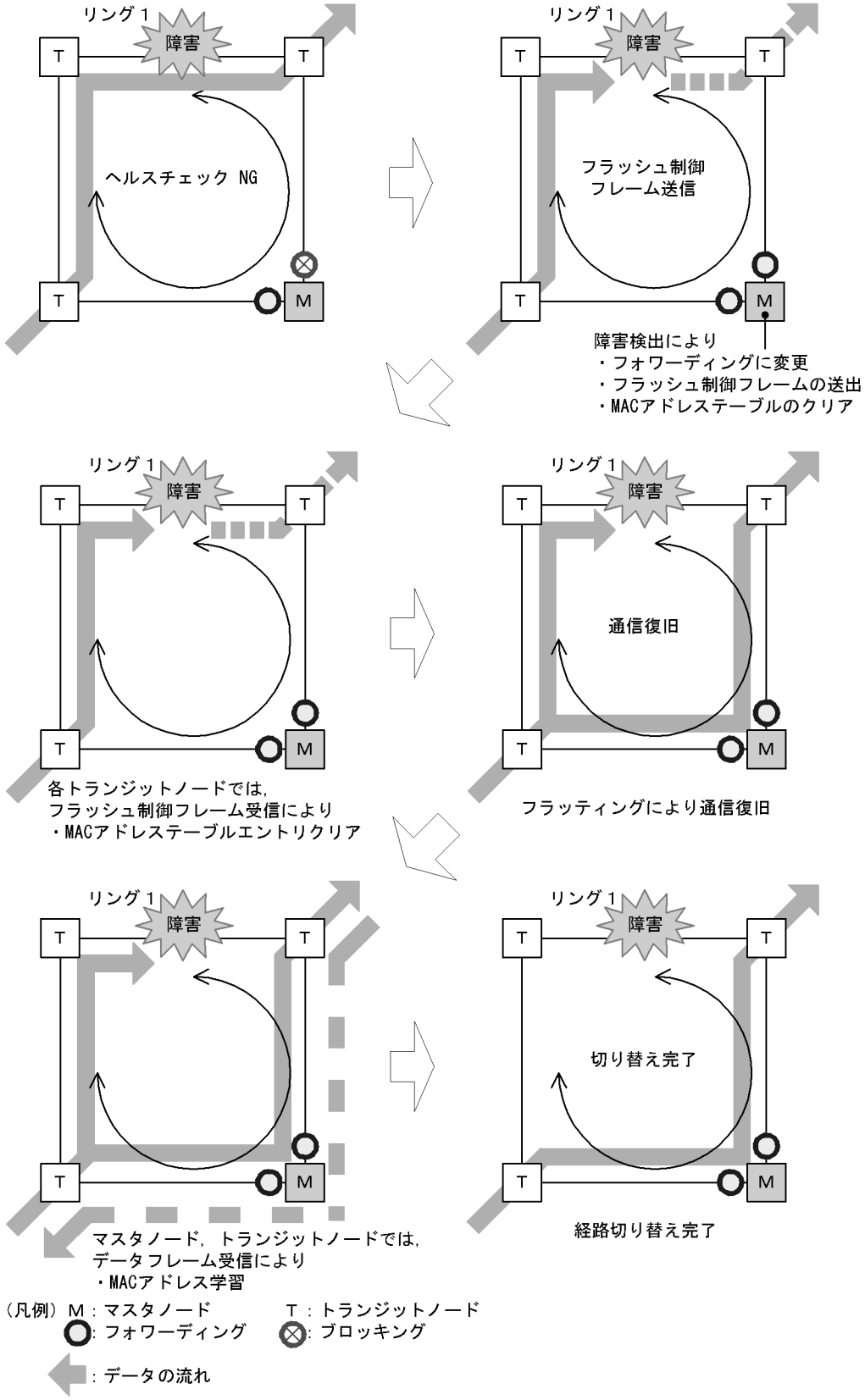
19.2.4 通信経路の切り替え

マスタノードは，リング障害の検出による迂回経路への切り替えのために，セカンダリポートをブロッキングからフォワーディングに変更します。また，リング障害の復旧検出による経路の切り戻しのために，セカンダリポートをフォワーディングからブロッキングに変更します。これに併せて，早急な通信の復旧を行うために，リング内のすべてのノードで，MAC アドレステーブルエントリのクリアが必要です。

MAC アドレステーブルエントリのクリアが実施されないと，切り替え（または切り戻し）前の情報によりデータフレームの転送が行われるため，正しくデータが届かないおそれがあります。従って，通信を復旧させるために，リングを構成するすべてのノードで MAC アドレステーブルエントリのクリアを実施します。

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

図 19-7　Ring Protocol の経路切り替え動作概要



（1） マスタノードの経路切り替え

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

（2） トランジットノードの経路切り替え

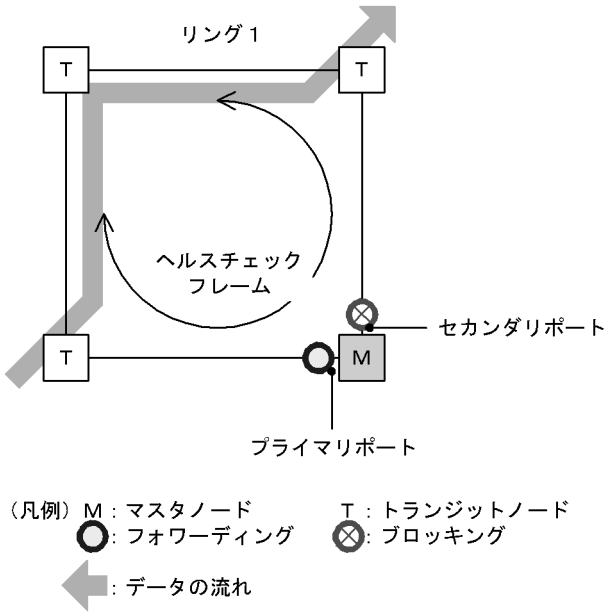
マスタノードがリングの障害を検出すると，同一の制御 VLAN を持つリング内の，そのほかのトランジットノードに対して MAC アドレステーブルエントリのクリアを要求するために，フラッシュ制御フレームと呼ぶ制御フレームを送信します。トランジットノードでは，このフラッシュ制御フレームを受信すると，リングポートでの MAC アドレステーブルエントリのクリアを行います。これによって，MAC アドレスの学習が行われるまでフラッディングを行います。新しい経路でのフレームの送受信によって MAC アドレス学習が行われ，通信経路の切り替えが完了します。

19.3　シングルリングの動作概要

19.3.1　リング正常時の動作

シングルリングでのリング正常時の動作について次の図に示します。

図 19-8　リング正常時の動作



（1）マスタノード動作

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

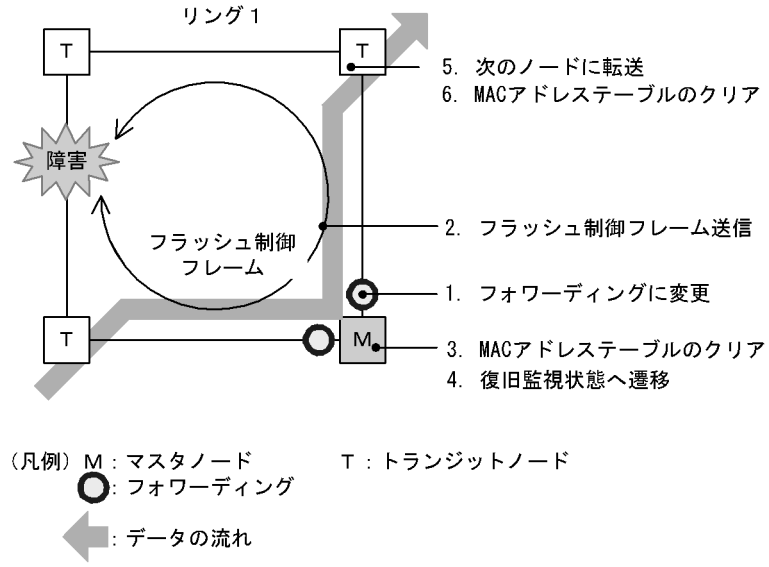
（2）トランジットノード動作

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

19.3.2　障害検出時の動作

シングルリングでのリング障害検出時の動作について次の図に示します。

図 19-9 リング障害時の動作



（1） マスタノード動作

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

1. データ転送用リング VLAN 状態の変更
   セカンダリポートのリング VLAN 状態をブロッキングからフォワーディングに変更します。障害検出時のリング VLAN 状態は次の表のように変更します。

表 19-2 障害検出時のデータ転送用リング VLAN 状態

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

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

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

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

（2） トランジットノード動作

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

5. フラッシュ制御フレームの転送
   受信したフラッシュ制御フレームを次のノードに転送します。

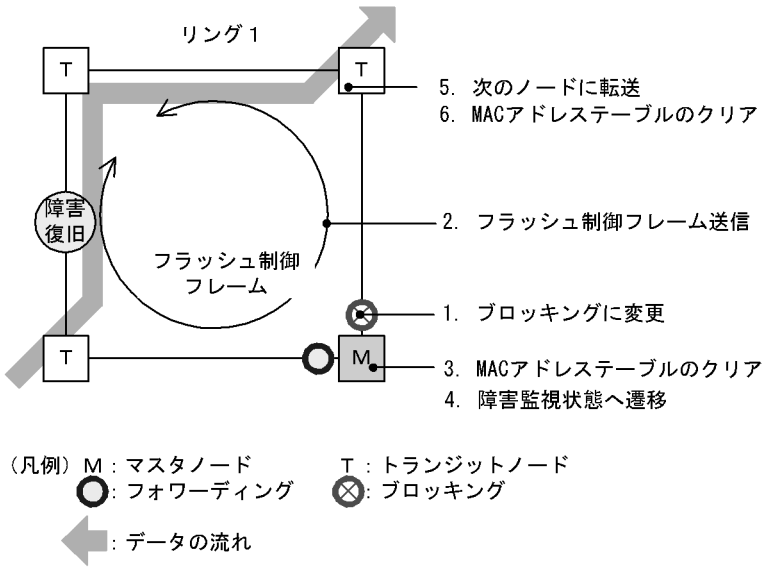
6. MAC アドレステーブルのクリア

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

19.3.3　復旧検出時の動作

シングルリングでのリング障害復旧時の動作について次の図に示します。

図 19-10　障害復旧時の動作



（1）マスタノード動作

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

1.　データ転送用リング VLAN 状態の変更

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

表 19-3　復旧検出時のデータ転送用リング VLAN 状態

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

2.　フラッシュ制御フレームの送信

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

3.　MAC アドレステーブルのクリア

リングポートに関する MAC アドレステーブルエントリのクリアを行います。

MAC アドレステーブルエントリをクリアすることで，通常の通信経路へ切り替えられます。

4.　監視状態の変更

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

（2） トランジットノード動作

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

5. フラッシュ制御フレームの転送
   受信したフラッシュ制御フレームを次のノードに転送します。

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

また，リンク障害が発生したトランジットノードでは，リンク障害が復旧した際のループの発生を防ぐため，リングポートのリング VLAN 状態はブロッキング状態となります。ブロッキング状態を解除する契機は，マスタノードが送信するフラッシュ制御フレームを受信したとき，またはトランジットノードでリングポートのフラッシュ制御フレーム受信待ち保護時間（コンフィグレーションコマンド forwarding-shift-time）がタイムアウトしたときとなります。フラッシュ制御フレーム受信待ち保護時間（コンフィグレーションコマンド forwarding-shift-time）は，リングポートのリンク障害復旧時に設定されます。

19.3.4 経路切り戻し抑止および解除時の動作

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

なお，経路切り戻し抑止状態は，次の契機で解除します。

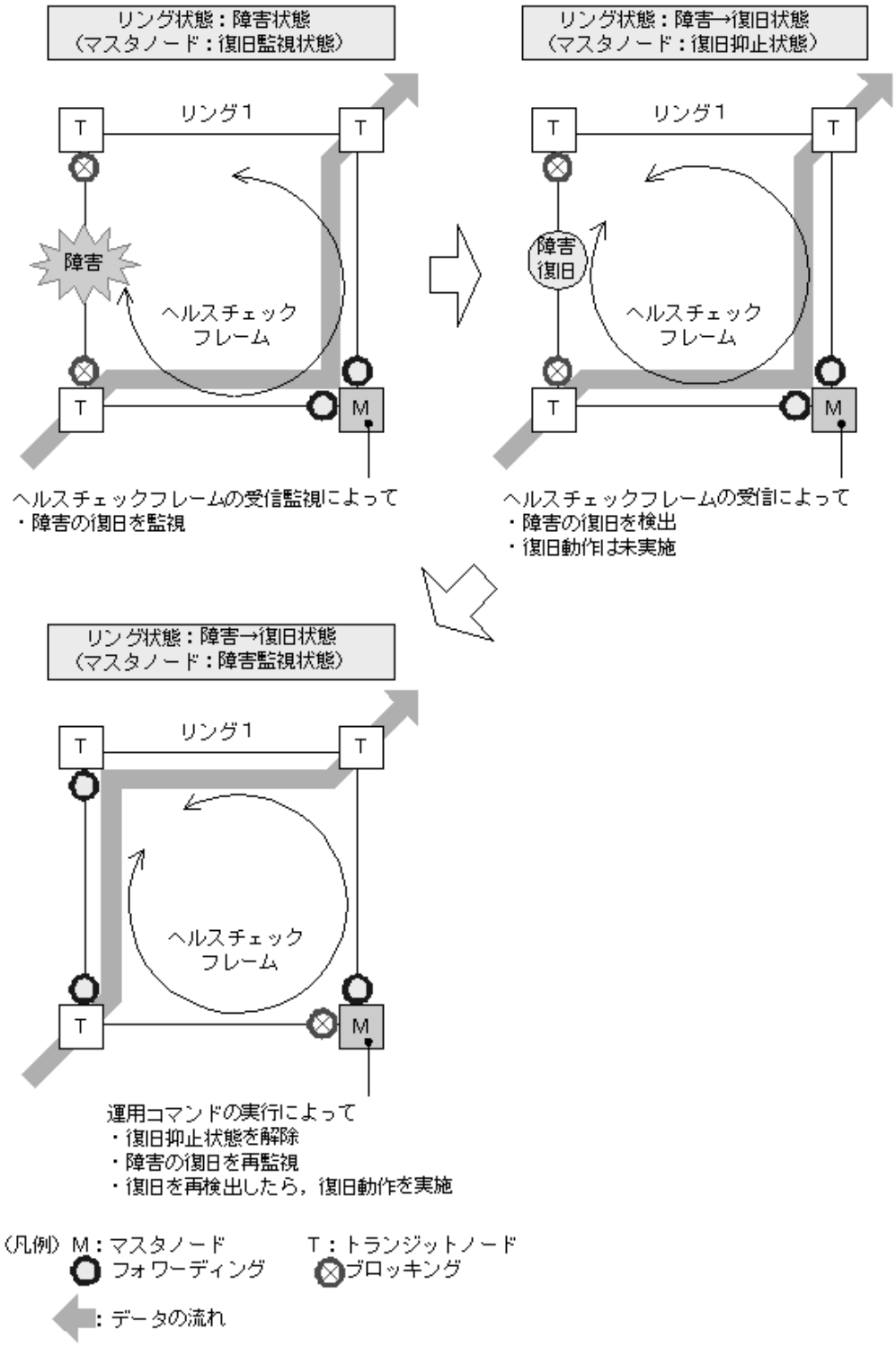
- 運用コマンド clear axrp preempt-delay の実行によって，経路切り戻し抑止が解除された場合
- コンフィグレーションコマンド preempt-delay で指定した，経路切り戻し抑止時間が経過した場合
- 経路切り戻し抑止機能を有効にするコンフィグレーションコマンド preempt-delay を削除した場合

復旧抑止状態が解除されると，マスタノードは再度，復旧監視状態に遷移します。その後リング障害の復旧を再検出すると，復旧動作を行います。復旧が完了すると，マスタノードは障害監視状態に遷移します。

また，経路切り戻し抑止状態でリングの障害が発生しても，マスタノードは復旧抑止状態を維持します。運用コマンド clear axrp preempt-delay の実行によって経路切り戻し抑止状態が解除されると，マスタノードは再度，復旧監視状態に遷移します。このとき，リング障害の復旧は検出しないため，復旧動作は行いません。その後，リングネットワーク上のすべての障害が復旧すると，マスタノードは障害の復旧を検出して，すぐに復旧動作を行います。

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

図 19-11　運用コマンドの実行によって経路切り戻し抑止を解除した場合の動作



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

- 装置起動（運用コマンド reload および ppupdate の実行を含む）

19.4　マルチリングの動作概要

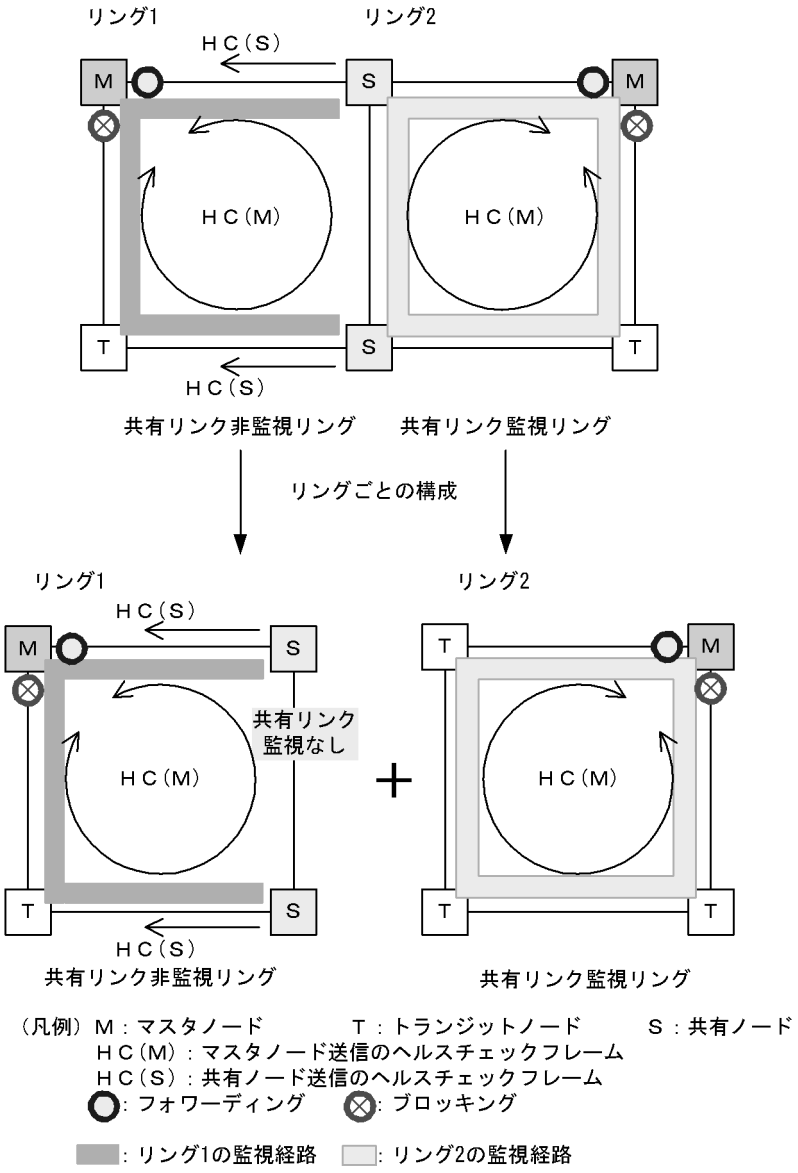
マルチリング構成のうち，共有リンクありのマルチリング構成について説明します。共有リンクなしのマルチリング構成については，シングルリング時の動作と同様ですので，「19.3　シングルリングの動作概要」を参照してください。

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

19.4.1　リング正常時の動作

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

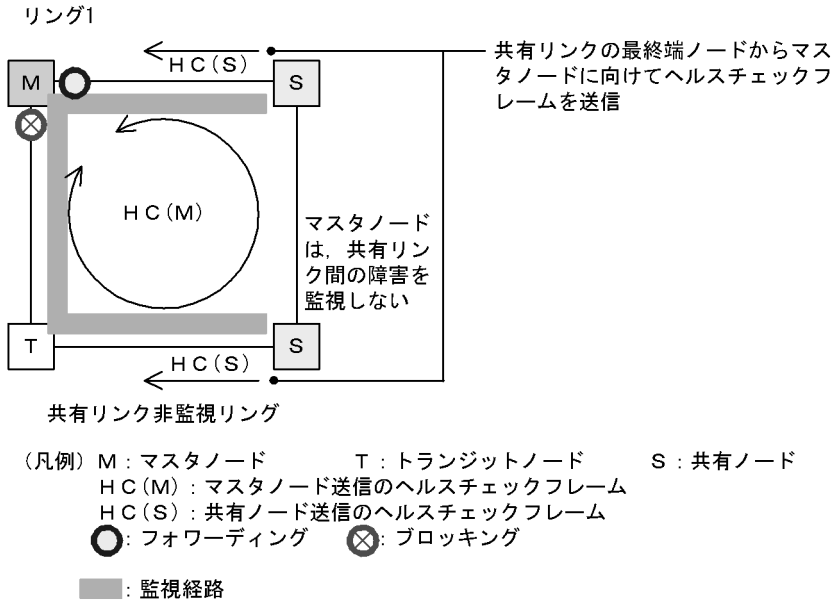
図 19-12　リング正常時の状態



(1) 共有リンク非監視リング

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

図 19-13　共有リンク非監視リングでの正常時の動作



(a) マスタノード動作

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

(b) トランジットノード動作

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

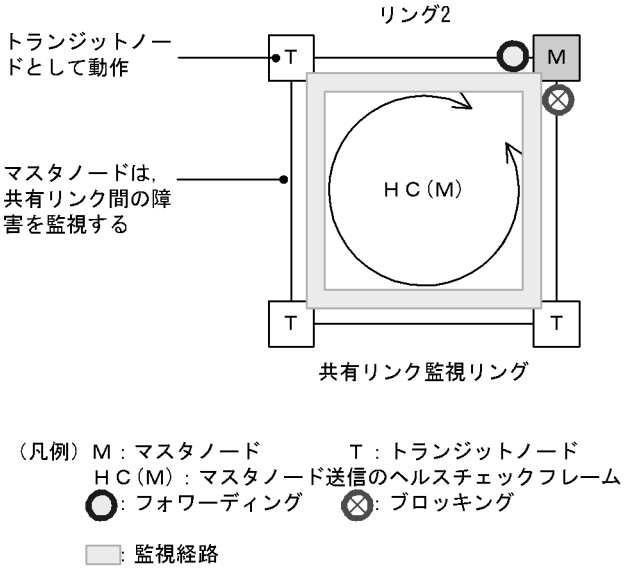
(c) 共有リンク非監視リングの最終端ノード動作

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

(2) 共有リンク監視リング

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

図 19-14　共有リンク監視リングでの正常時の動作



(a) マスタノード動作

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

(b) トランジットノード動作

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

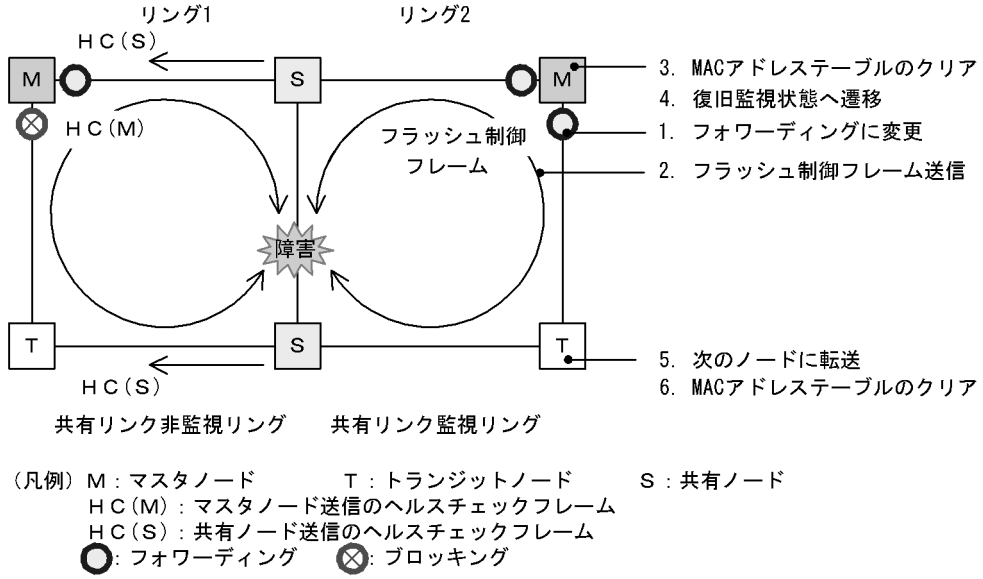
19.4.2　共有リンク障害・復旧時の動作

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

(1) 障害検出時の動作

共有リンクの障害を検出した際の動作について次の図に示します。

図 19-15 共有リンク障害時の動作



(a) 共有リンク監視リングのマスタノード動作

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

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

(b) 共有リンク監視リングのトランジットノード動作

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

5. フラッシュ制御フレームの転送
6. MAC アドレステーブルのクリア

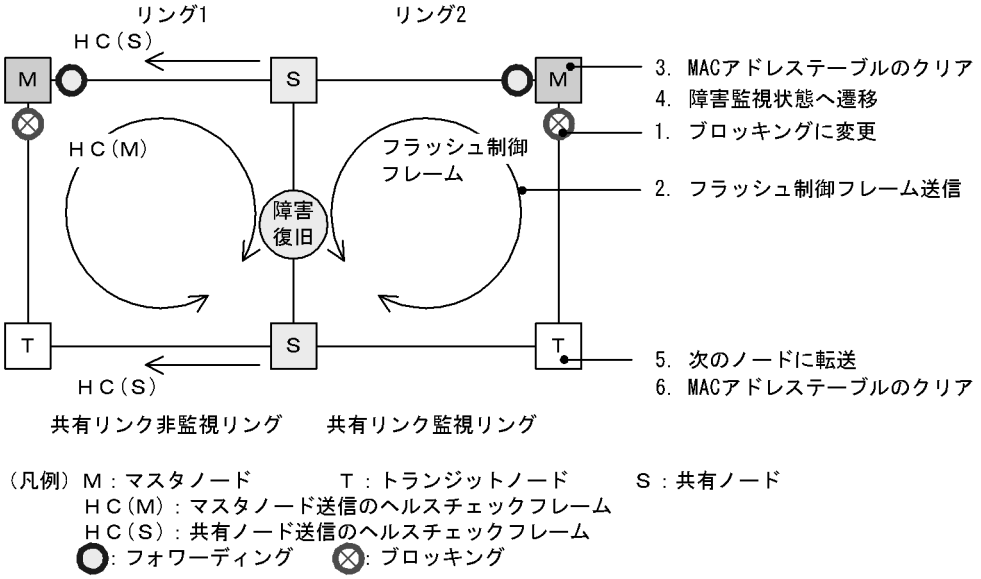
(c) 共有リンク非監視リングのマスタノードおよびトランジットノード動作

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

(2) 復旧検出時の動作

共有リンクの障害復旧を検出した際の動作について次の図に示します。

図 19-16　共有リンク復旧時の動作



(a) 共有リンク監視リングのマスタノード動作

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

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

(b) 共有リンク監視リングのトランジットノード動作

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

5. フラッシュ制御フレームの転送
6. MAC アドレステーブルのクリア

(c) 共有リンク非監視リングのマスタノードおよびトランジットノード動作

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

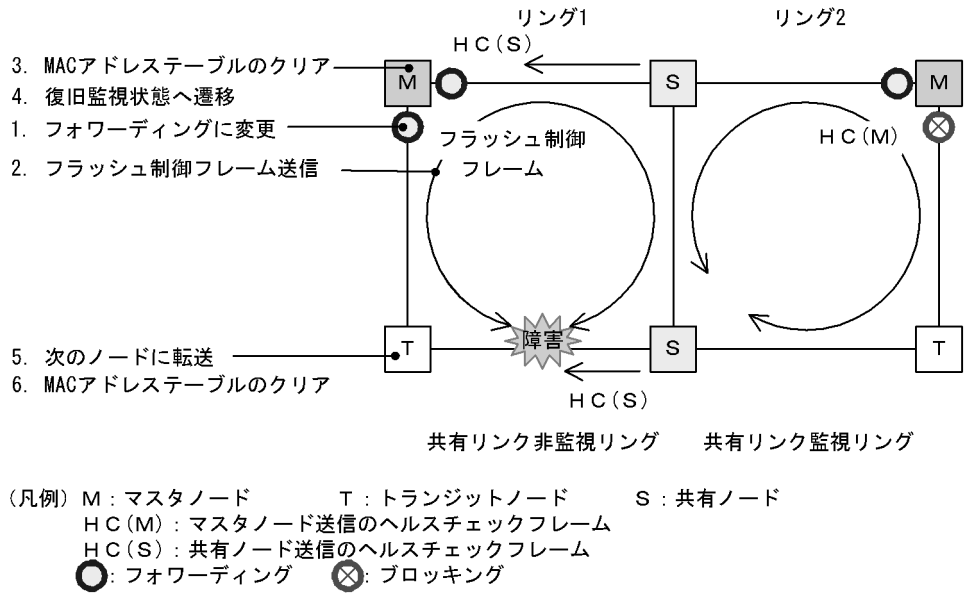
19.4.3　共有リンク非監視リングでの共有リンク以外の障害・復旧時の動作

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

(1) 障害検出時の動作

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

図 19-17　共有リンク非監視リングにおける共有リンク以外のリング障害時の動作



(a) 共有リンク非監視リングのマスタノード動作

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

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

(b) 共有リンク非監視リングのトランジットノードおよび共有ノード動作

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

5. フラッシュ制御フレームの転送
6. MAC アドレステーブルのクリア

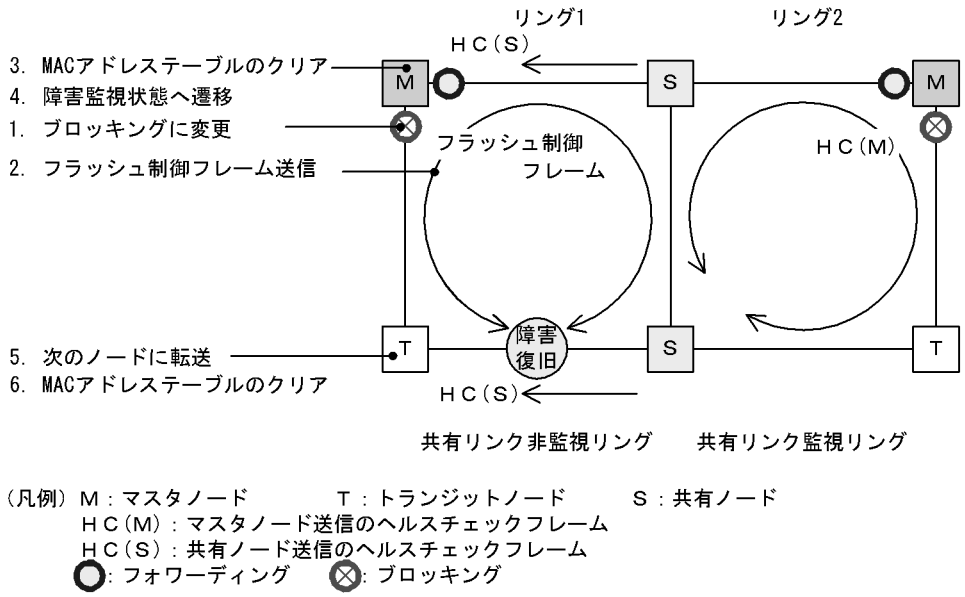
(c) 共有リンク監視リングのマスタノードおよびトランジットノード動作

共有リンク監視リング内では障害が発生していないため，障害動作は行いません。

(2) 復旧検出時の動作

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

図 19-18　共有リンク非監視リングでの共有リンク以外のリング障害復旧時の動作



(a) 共有リンク非監視リングのマスタノード動作

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

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

(b) 共有リンク非監視リングのトランジットノードおよび共有ノード動作

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

5. フラッシュ制御フレームの転送
6. MAC アドレステーブルのクリア

(c) 共有リンク監視リングのマスタノードおよびトランジットノード動作

共有リンク監視リング内では障害が発生していないため，復旧動作は行いません。

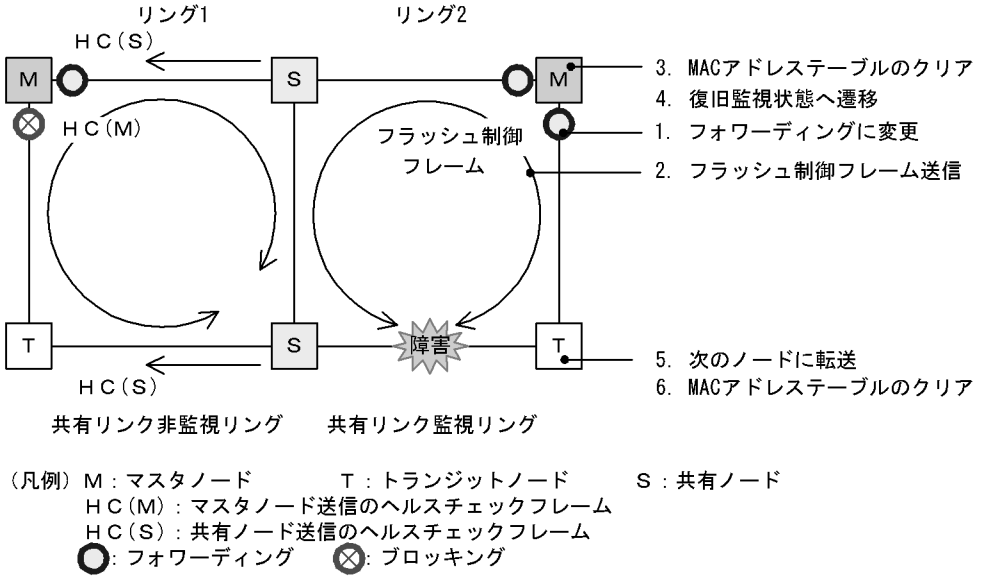
19.4.4　共有リンク監視リングでの共有リンク以外の障害・復旧時の動作

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

(1) 障害検出時の動作

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

図 19-19 共有リンク監視リングでの共有リンク以外のリング障害時の動作



(a) 共有リンク監視リングのマスタノード動作

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

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

(b) 共有リンク監視リングのトランジットノード動作

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

5. フラッシュ制御フレームの転送
6. MAC アドレステーブルのクリア

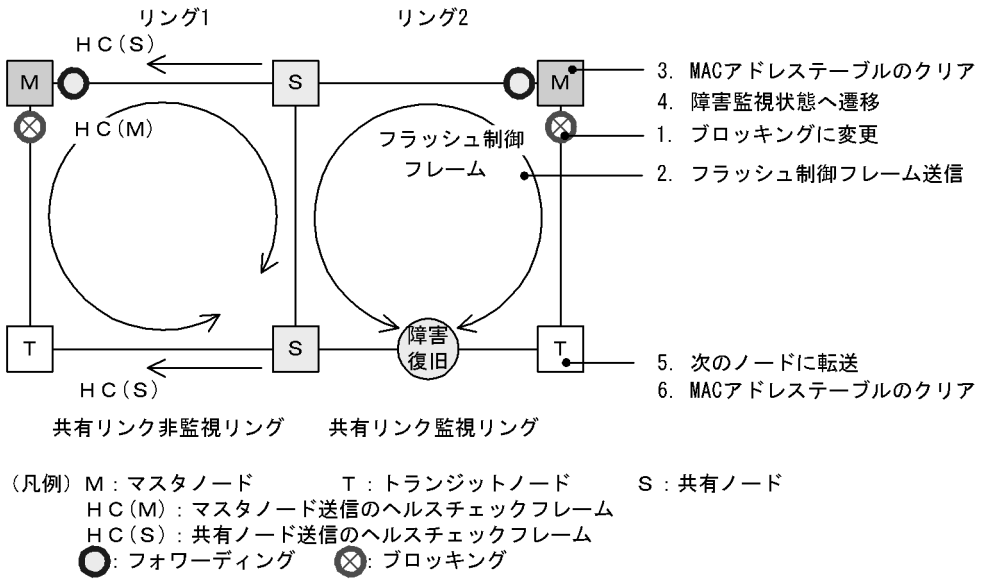
(c) 共有リンク非監視リングのマスタノードおよびトランジットノード（共有ノード）動作

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

(2) 復旧検出時の動作

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

図 19-20　共有リンク監視リングでの共有リンク以外のリング障害復旧時の動作



(a) 共有リンク監視リングのマスタノード動作

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

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

(b) 共有リンク監視リングのトランジットノード動作

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

5. フラッシュ制御フレームの転送
6. MAC アドレステーブルのクリア

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

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

19.4.5　経路切り戻し抑止および解除時の動作

マルチリング構成での経路切り戻し抑止および解除時の動作については，シングルリング時の動作と同様ですので，「19.3　シングルリングの動作概要」を参照してください。

19.5　Ring Protocol の多重障害監視機能

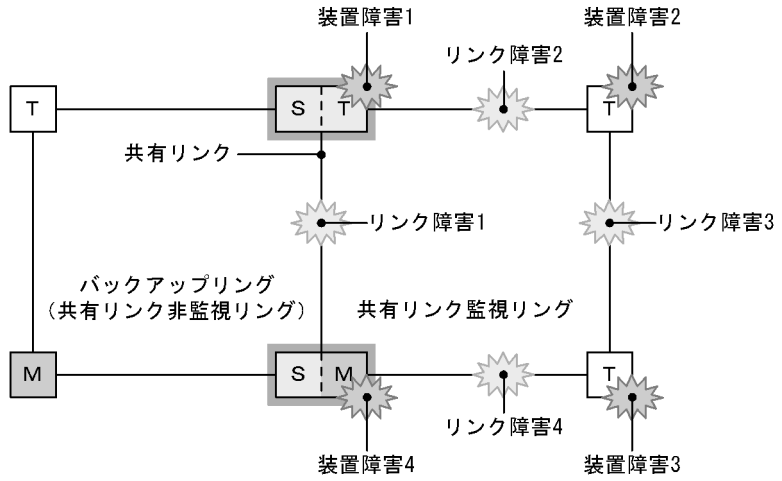
19.5.1　概要

多重障害監視機能は，共有リンクありのマルチリング構成での共有リンク監視リングの多重障害を監視して，多重障害を検出した場合に共有リンク非監視リングに経路を切り替える機能です。このとき，経路の切り替えに使用する共有リンク非監視リングを**バックアップリング**と呼びます。

多重障害監視機能で検出の対象となるのは，共有リンク障害と，共有リンク監視リング内のその他のリンク障害およびリンク障害を伴う装置障害です。

共有リンク監視リングでの障害発生例と，多重障害監視機能で検出できる障害の組み合わせを次に示します。

図 19-21　共有リンク監視リングでの障害発生例



（凡例）M：マスタノード　　T：トランジットノード
　　S：共有リンクの最終端ノード（トランジットノード）　：共有ノード

表 19-4　多重障害監視機能で検出できる障害の組み合わせ

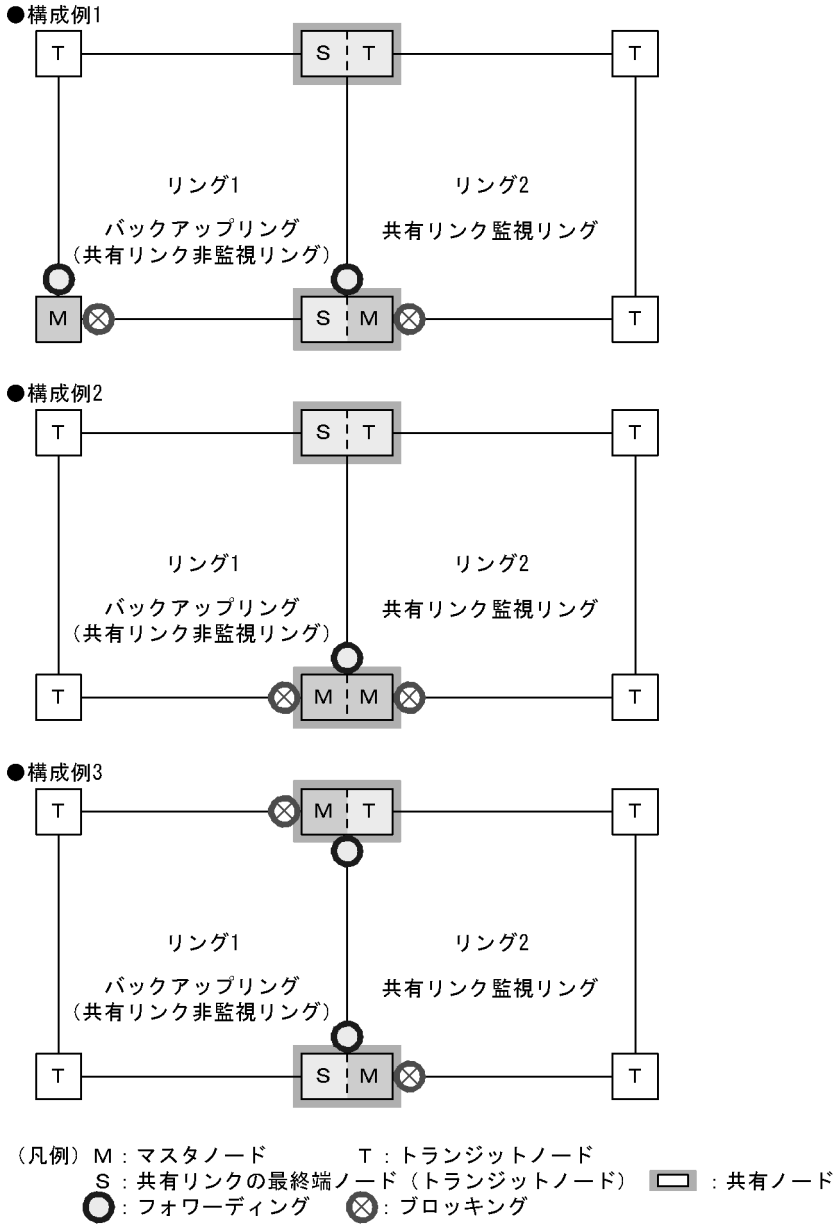
障害種別	検出可能な組み合わせ	
リンク障害	リンク障害１（共有リンク障害）	リンク障害２（その他のリンク障害）
	リンク障害１（共有リンク障害）	リンク障害３（その他のリンク障害）
	リンク障害１（共有リンク障害）	リンク障害４（その他のリンク障害）
装置障害	装置障害１（共有ノード障害）だけ	
	装置障害４（共有ノード障害）だけ	
	装置障害２（トランジットノード障害）	リンク障害１（共有リンク障害）
	装置障害３（トランジットノード障害）	リンク障害１（共有リンク障害）

19.5.2　多重障害監視機能の基本構成

多重障害監視機能を適用できる共有リンクありのマルチリング構成は，共有リンク監視リングとバックアップリングとなる共有リンク非監視リングをそれぞれ１リングずつ対応づけた構成です。このとき，共有ノードを共有リンク監視リングのマスタノードとして設定します。多重障害監視機能の基本構成例を次

の図に示します。

図 19-22　多重障害監視機能の基本構成例

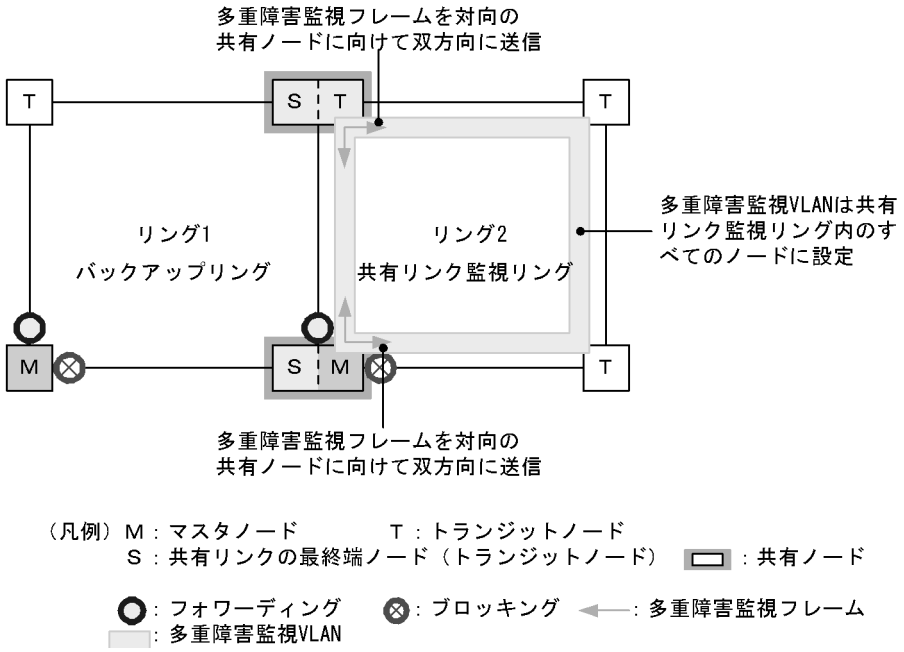


19.5.3　多重障害監視の動作概要

多重障害は，共有リンクありのマルチリング構成で共有リンクの両端に位置する共有ノードで監視します。共有ノードは，共有リンク監視リングの多重障害を監視するための制御フレーム（**多重障害監視フレーム**と呼びます）を送信します。対向の共有ノードでは，多重障害監視フレームの受信を監視します。なお，多重障害監視フレームは専用の VLAN（**多重障害監視 VLAN** と呼びます）上に送信します。

多重障害監視の動作概要を次の図に示します。

図 19-23　多重障害監視の動作概要



(1) 共有リンク監視リングの各ノードの動作

共有リンク監視リングのマスタノードおよびトランジットノードの動作は，マルチリング時の動作と同様ですので，「19.4.1　リング正常時の動作　(2) 共有リンク監視リング」を参照してください。

共有ノードでは，共有リンク監視リングの多重障害を監視します。共有ノードは，多重障害監視フレームを両リングポートから送信するとともに，対向の共有ノードが両リングポートから送信した多重障害監視フレームをあらかじめ設定した時間内に受信するかを監視します。

(2) バックアップリングの各ノードの動作

バックアップリングのマスタノードおよびトランジットノードの動作は，マルチリング時の動作と同様ですので，「19.4.1　リング正常時の動作　(1) 共有リンク非監視リング」を参照してください。

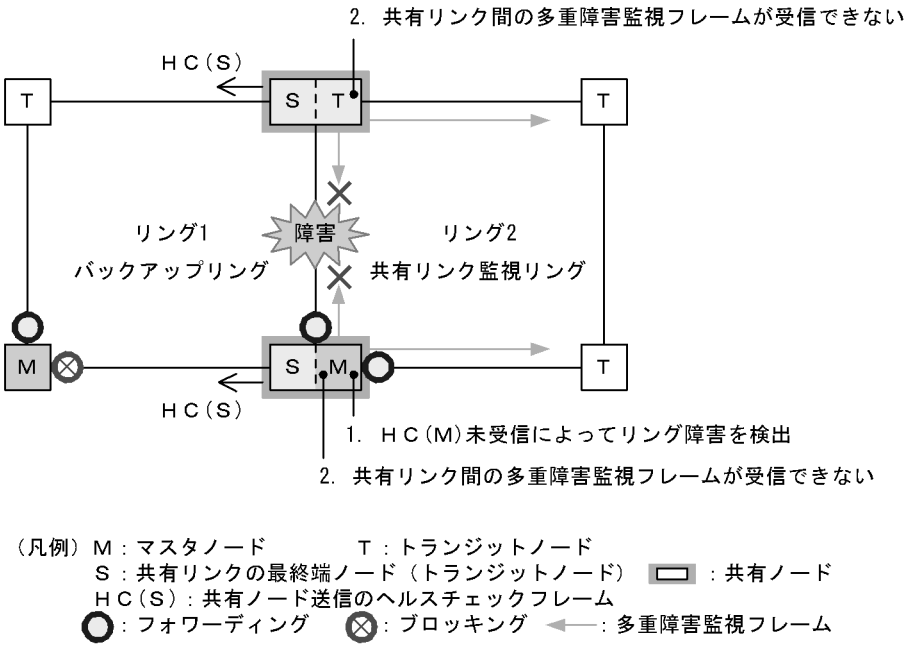
19.5.4　多重障害発生時の動作

共有リンク監視リングで，共有リンク障害とその他のリンク障害による多重障害が発生した場合の動作について説明します。

(1) 共有リンク障害時の動作

共有リンク監視リングでの共有リンク障害時の動作について，次の図に示します。

図 19-24　共有リンク障害時の動作



（a） 共有リンク監視リングの各ノードの動作

1. HC(M) 未受信によってリング障害を検出

マスタノードが両方向の HC(M) を受信できなくなり，リング障害を検出します。リング障害検出時のマスタノードおよびトランジットノードの動作は，マルチリング時の動作と同様ですので，「19.4.2 共有リンク障害・復旧時の動作 （1）障害検出時の動作」を参照してください。

2. 共有リンク間の多重障害監視フレームが受信できない

共有ノードは共有リンク間での多重障害監視フレームの受信ができなくなりますが，もう一方のリングポートでは受信できているため，多重障害の監視を継続します。

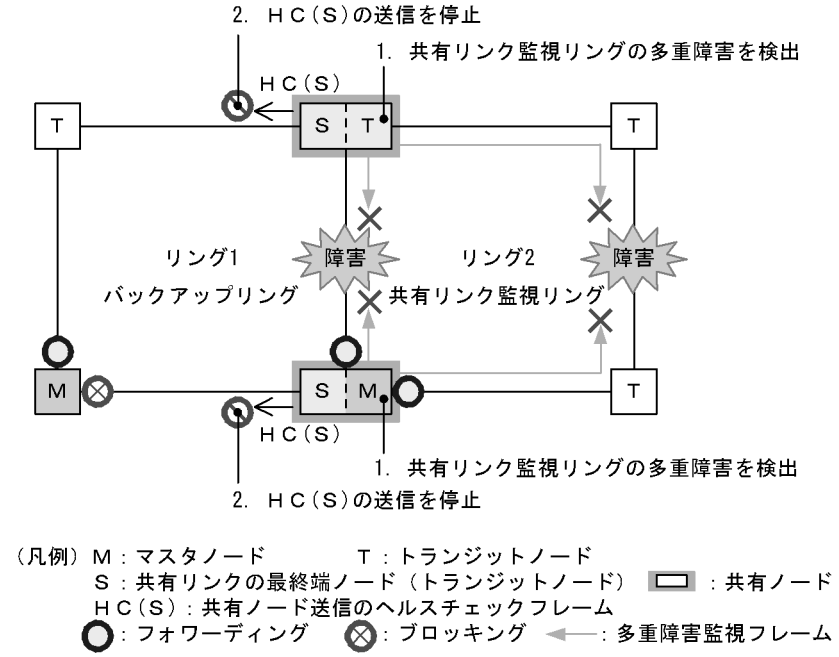
（b） バックアップリングの各ノードの動作

バックアップリングではマスタノードが送信した HC(M) の受信はできなくなりますが，共有ノードが送信した HC(S) は受信できているため，障害検出時の動作は行いません。

（2） 多重障害発生時の動作

共有リンク障害と共有リンク監視リング内のその他のリンク障害による多重障害発生時の動作について，次の図に示します。

図 19-25　多重障害発生時の動作



（a）共有リンク監視リングの各ノードの動作

1.　共有リンク監視リングの多重障害を検出

共有ノードは両リングポートで多重障害監視フレームを受信できなくなり，多重障害を検出します。

（b）バックアップリングの各ノードの動作

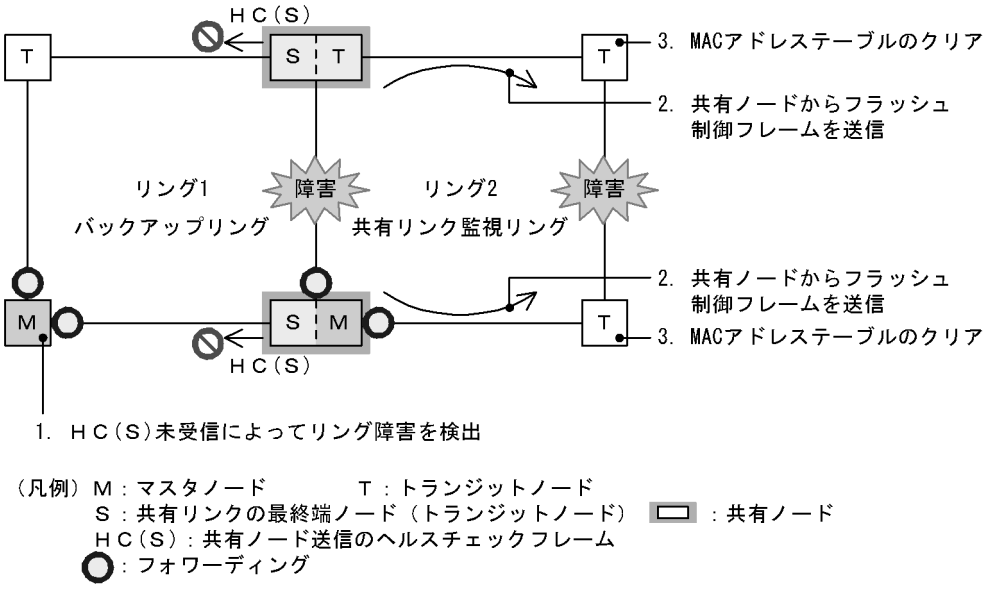
2.　HC(S) の送信を停止

多重障害を検出した共有ノードは，バックアップリングの HC(S) の送信を停止します。

（3）バックアップリングへの切り替え動作

多重障害検出によるバックアップリングへの切り替え動作について，次の図に示します。

図 19-26　バックアップリングへの切り替え動作



（a） バックアップリングの各ノードの動作

1. HSC(S) 未受信によってリング障害を検出

マスタノードは自身が送信した両方向の HC(M) と共有ノードが送信した HC(S) がどちらも未受信となり，リング障害を検出します。リング障害検出時のマスタノードおよびトランジットノードの動作は，マルチリング時の動作と同様ですので，「19.4.3　共有リンク非監視リングでの共有リンク以外の障害・復旧時の動作　（1）障害検出時の動作」を参照してください。

（b） 共有リンク監視リングの各ノードの動作

2.　共有ノードからフラッシュ制御フレームを送信

バックアップリングのマスタノードから送信されたフラッシュ制御フレームを受信すると，共有ノードは共有リンク監視リングに向けて，MAC アドレステーブルのクリアだけをするフラッシュ制御フレームを送信します。

3. MAC アドレステーブルのクリア

トランジットノードは共有ノードから送信されたフラッシュ制御フレームを受信して，MAC アドレステーブルをクリアします。

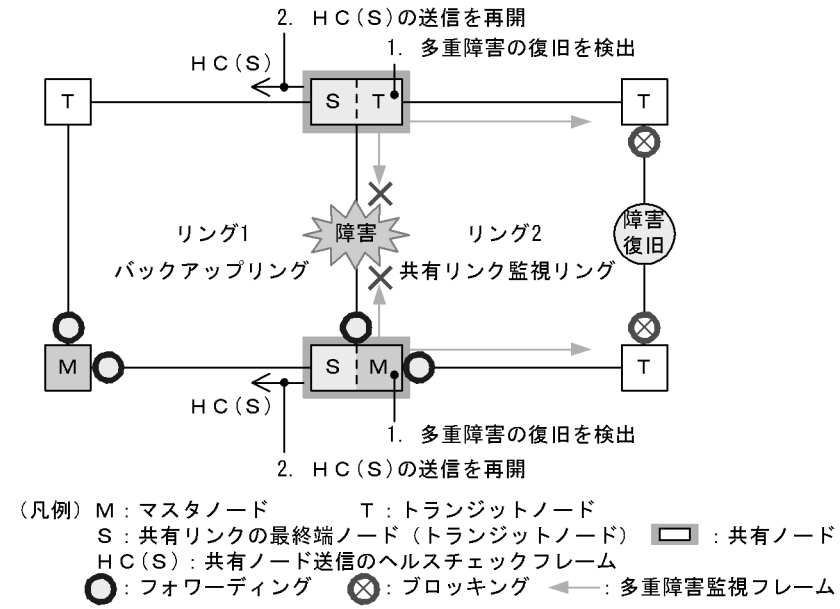
19.5.5　多重障害復旧時の動作

共有リンク監視リングでの多重障害が復旧した場合の動作について説明します。

（1） 多重障害からの一部復旧時の動作

共有リンク監視リングで多重障害からの一部復旧時の動作について，次の図に示します。

図 19-27　多重障害からの一部復旧時の動作



（a） 共有リンク監視リングの各ノードの動作

1. 多重障害の復旧を検出

共有ノードは対向の共有ノードが送信した多重障害監視フレームを受信して，多重障害の復旧を検出します。

（b）バックアップリングの各ノードの動作

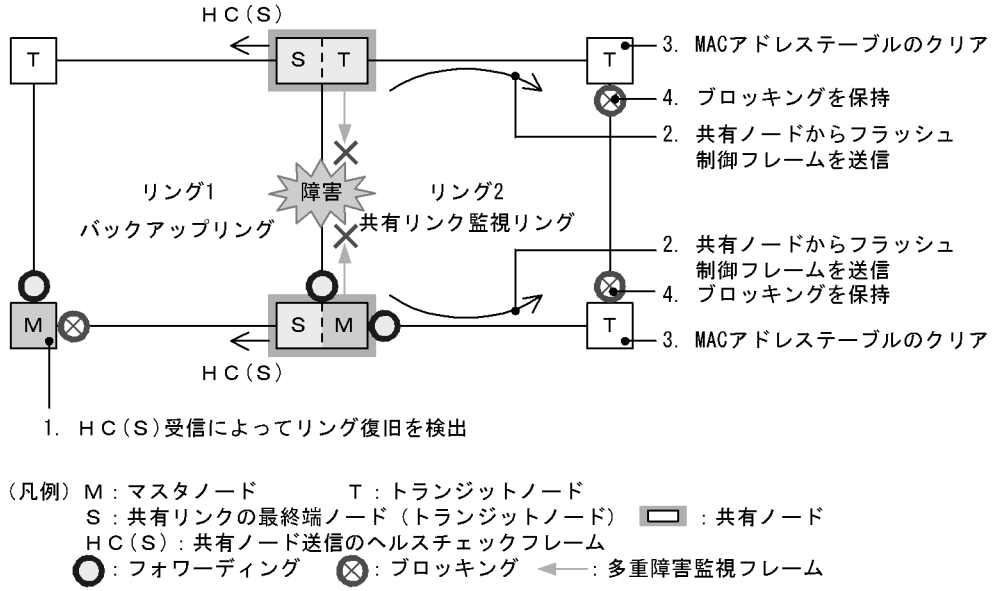
2.　HC(S) の送信を再開

多重障害の復旧を検出した共有ノードは，バックアップリングの HC(S) の送信を再開します。

（2）バックアップリングからの切り戻し動作

バックアップリングからの切り戻し動作について，次の図に示します。

図 19-28　バックアップリングからの切り戻し動作



（a）バックアップリングの各ノードの動作

1.　HC(S) 受信によってリング復旧を検出

マスタノードは共有ノードが送信した HC(S) を両方向から受信すると，リング障害が復旧したと判断して復旧動作を行います。復旧検出時のマスタノードおよびトランジットノードの動作は，マルチリング時の動作と同様ですので，「19.4.3　共有リンク非監視リングでの共有リンク以外の障害・復旧時の動作　(2) 復旧検出時の動作」を参照してください。

（b）共有リンク監視リングの各ノードの動作

2.　共有ノードからフラッシュ制御フレームを送信

バックアップリングのマスタノードから送信されたフラッシュ制御フレームを受信すると，共有ノードは共有リンク監視リングに向けて，MAC アドレステーブルのクリアだけをするフラッシュ制御フレームを送信します。

3.　MAC アドレステーブルのクリア

トランジットノードは共有ノードから送信されたフラッシュ制御フレームを受信して，MAC アドレステーブルをクリアします。

4.　ブロッキングを保持

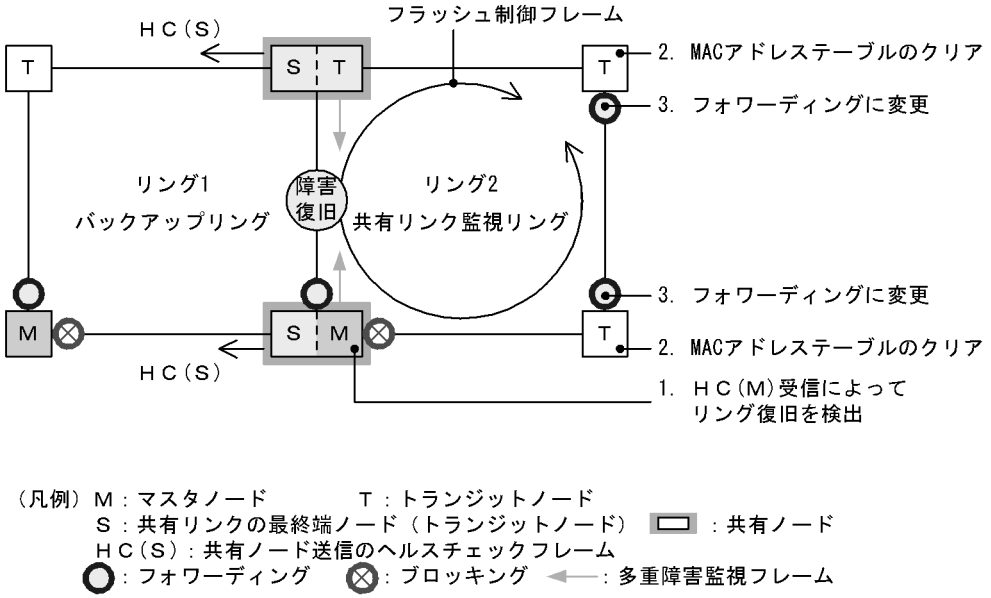
リンク障害から復旧したリングポートのリング VLAN 状態は，マスタノードがリング復旧を検出していないため，ブロッキングを保持します。

なお，ブロッキングの解除については，「19.7　Ring Protocol 使用時の注意事項　(18) 多重障害の一部復旧時の通信について」を参照してください。

（3） 共有リンク障害復旧時の動作

共有リンク障害復旧時の動作について，次の図に示します。

図 19-29　共有リンク障害復旧時の動作



（凡例）Ｍ：マスタノード　　Ｔ：トランジットノード
Ｓ：共有リンクの最終端ノード（トランジットノード）　：共有ノード
ＨＣ（Ｓ）：共有ノード送信のヘルスチェックフレーム
：フォワーディング　：ブロッキング　：多重障害監視フレーム

（a） 共有リンク監視リングの各ノードの動作

1. HC(M) 受信によってリング復旧を検出

マスタノードは自身が送信した HC(M) を受信すると，リング障害が復旧したと判断して復旧動作を行います。復旧検出時のマスタノードおよびトランジットノードの動作は，マルチリング時の動作と同様ですので，「19.4.2　共有リンク障害・復旧時の動作　（2）復旧検出時の動作」を参照してください。

2. MAC アドレステーブルのクリア

トランジットノードはマスタノードから送信されたフラッシュ制御フレームを受信して，MAC アドレステーブルをクリアします。

3.　フォワーディングに変更

トランジットノードはマスタノードが送信したフラッシュ制御フレームの受信によって，リンク障害から復旧したリングポートのリング VLAN 状態をフォワーディングに変更します。

19.6　Ring Protocol のネットワーク設計

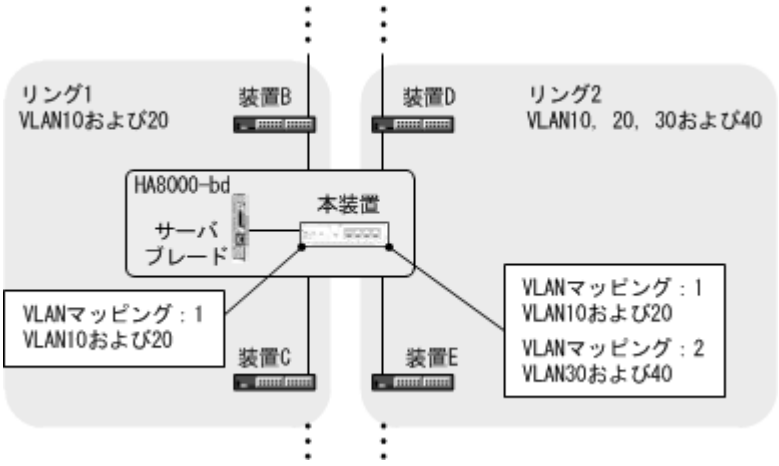
19.6.1　VLAN マッピングの使用方法

（1） VLAN マッピングとデータ転送用 VLAN

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

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

図 19-30　リングごとの VLAN マッピングの割り当て例



（2） PVST+ と併用する場合の VLAN マッピング

Ring Protocol と PVST+ を併用する場合は，PVST+ に使用する VLAN を VLAN マッピングにも設定します。このとき，VLAN マッピングに割り当てる VLAN は一つだけにしてください。PVST+ と併用する VLAN 以外のデータ転送用 VLAN は，別の VLAN マッピングに設定して，PVST+ と併用する VALN マッピングと合わせて VLAN グループに設定します。

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

トランジットノードの装置起動で，Ring Protocol が初期状態から動作する場合，データ転送用 VLAN は論理ブロックされています。トランジットノードは，マスタノードが送信するフラッシュ制御フレームを受信することでこの論理ブロックを解除します。しかし，装置再起動時で，マスタノードの障害監視時間（コンフィグレーションコマンド health-check holdtime）が長いと，リングネットワークの状態変化を認識できないおそれがあります。この場合，フラッシュ制御フレーム受信待ち保護時間（コンフィグレーションコマンド forwarding-shift-time）がタイムアウトするまで論理ブロックは解除されないため，トランジットノードのデータ VLAN は通信できない状態になります。制御 VLAN のフォワーディング遷移時間（コンフィグレーションコマンド control-vlan のパラメータ forwarding-delay-time）を設定すると次に示す手順で動作するため，このようなケースを回避できます。

1. トランジットノードは，装置起動直後に，制御 VLAN をいったん論理ブロックします。
2. トランジットノードの制御 VLAN が論理ブロックされたので，マスタノードで障害を検出します（ただし，装置起動時はこれ以前に障害を検出しています）。このため，通信は迂回経路に切り替わります。
3. トランジットノードは，制御 VLAN のフォワーディング遷移時間（コンフィグレーションコマンド control-vlan のパラメータ forwarding-delay-time）のタイムアウトによって制御 VLAN のブロッキングを解除します。
4. マスタノードはヘルスチェックフレームを受信することで復旧を検出し，フラッシュ制御フレームを送信します。
5. トランジットノードは，このフラッシュ制御フレームを受信することでデータ転送用 VLAN の論理ブロックを解除します。これによってデータ転送用 VLAN での通信が再開され，リングネットワーク全体でも通常の通信経路に復旧します。

（1） 制御 VLAN のフォワーディング遷移時間（コンフィグレーションコマンド control-vlan のパラメータ forwarding-delay-time）と障害監視時間（コンフィグレーションコマンド health-check holdtime）の関係について

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

19.6.3 プライマリポートの自動決定

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

表 19-5 プライマリポートの選択方式（VLAN グループ #1）

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

表 19-6 プライマリポートの選択方式（VLAN グループ #2）

リングポート #1	リングポート #2	優先ポート
物理ポート	物理ポート	ポート番号の大きい方がプライマリポートとして動作
物理ポート	チャネルグループ	チャネルグループ側がプライマリポートとして動作
チャネルグループ	物理ポート	チャネルグループ側がプライマリポートとして動作
チャネルグループ	チャネルグループ	チャネルグループ番号の大きい方がプライマリポートとして動作

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

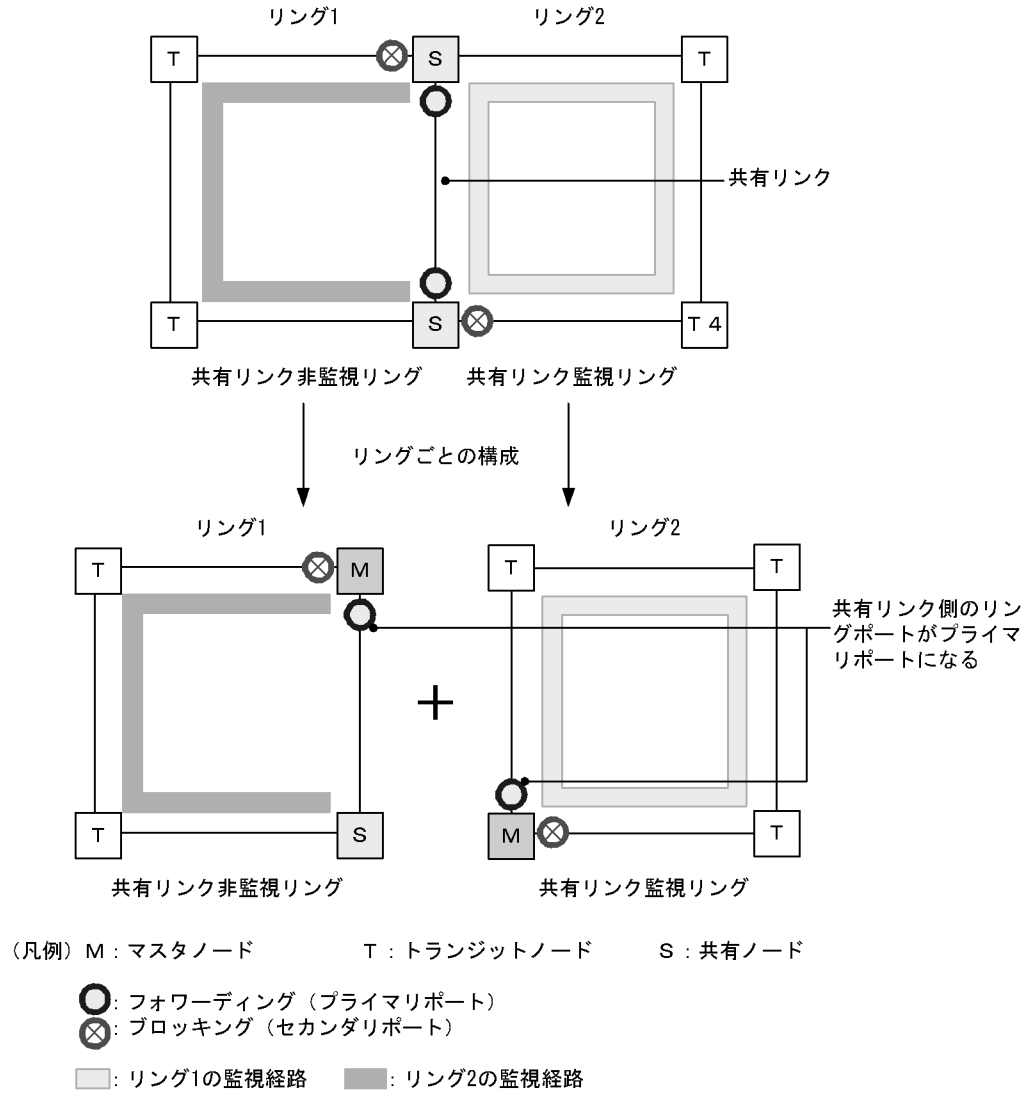
19.6.4　同一装置内でのノード種別混在構成

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

19.6.5　共有ノードでのノード種別混在構成

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

図 19-31　共有ノードをマスタノードとした場合のポート状態



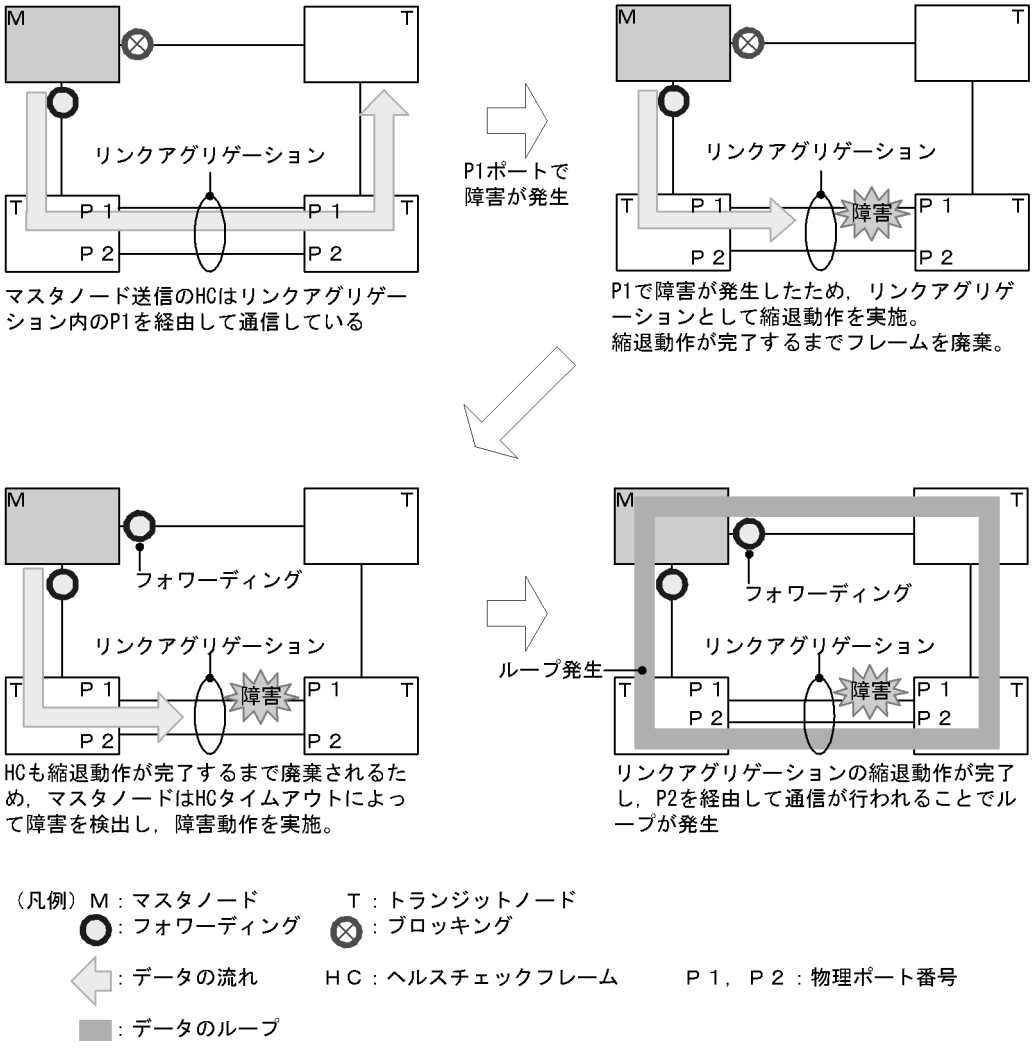
19.6.6　リンクアグリゲーションを用いた場合の障害監視時間の設定

リングポートをリンクアグリゲーションで構成した場合に，ヘルスチェックフレームが転送されているリンクアグリゲーション内のポートに障害が発生すると，リンクアグリゲーションの切り替えまたは縮退動作が完了するまでの間，制御フレームが廃棄されてしまいます。このため，マスタノードの障害監視時間（コンフィグレーションコマンド health-check holdtime）がリンクアグリゲーションの切り替えまたは縮退動作が完了する時間よりも短いと，マスタノードがリングの障害を誤検出し，経路の切り替えを行います。この結果，ループが発生するおそれがあります。

リングポートをリンクアグリゲーションで構成した場合は，マスタノードの障害監視時間をリンクアグリゲーションによる切り替えまたは縮退動作が完了する時間よりも大きくする必要があります。

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

図 19-32　リンクアグリゲーション使用時の障害検出



19.6.7　IEEE802.3ah/UDLD 機能との併用

本プロトコルでは，片方向リンク障害での障害の検出および切り替え動作は実施しません。片方向リンク障害発生時にも切り替え動作を実施したい場合は，IEEE802.3ah/UDLD 機能を併用してください。リング内のノード間を接続するリングポートに対して IEEE802.3ah/UDLD 機能の設定を行います。
IEEE802.3ah/UDLD 機能によって，片方向リンク障害が検出されると，該当ポートを閉塞します。これによって，該当リングを監視するマスタノードはリング障害を検出し，切り替え動作を行います。

19.6.8　リンクダウン検出タイマおよびリンクアップ検出タイマとの併用

リングポートに使用しているポート（物理ポートまたはリンクアグリゲーションに属する物理ポート）のリンク状態が不安定な場合，マスタノードがリング障害やリング障害復旧を連続で検出してリングネットワークが不安定な状態になり，ループや長時間の通信断が発生するおそれがあります。このような状態を防ぐには，リングポートに使用しているポートに対して，リンクダウン検出タイマおよびリンクアップ検出タイマを設定します。リンクダウン検出タイマおよびリンクアップ検出タイマの設定については，「12.2.6　リンクダウン検出タイマの設定」および「12.2.7　リンクアップ検出タイマの設定」を参照してください。

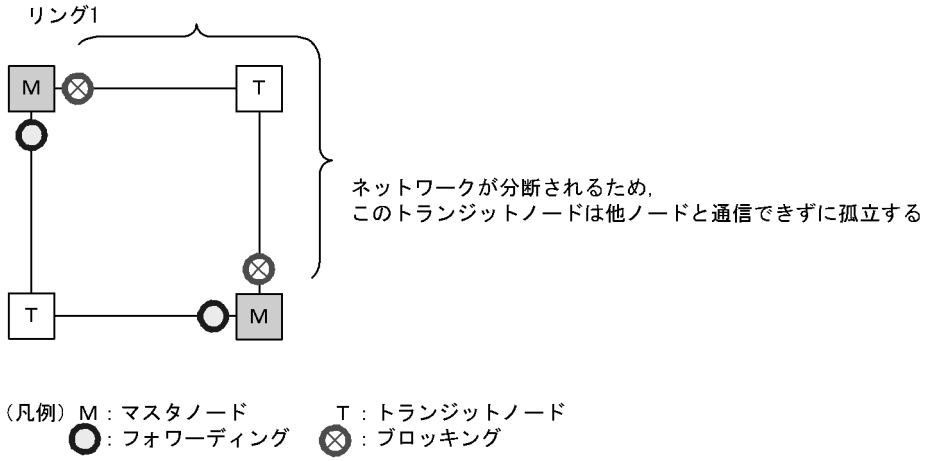
19.6.9　Ring Protocol の禁止構成

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

（1） 同一リング内に複数のマスタノードを設定

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

図 19-33　同一リング内に複数のマスタノードを設定

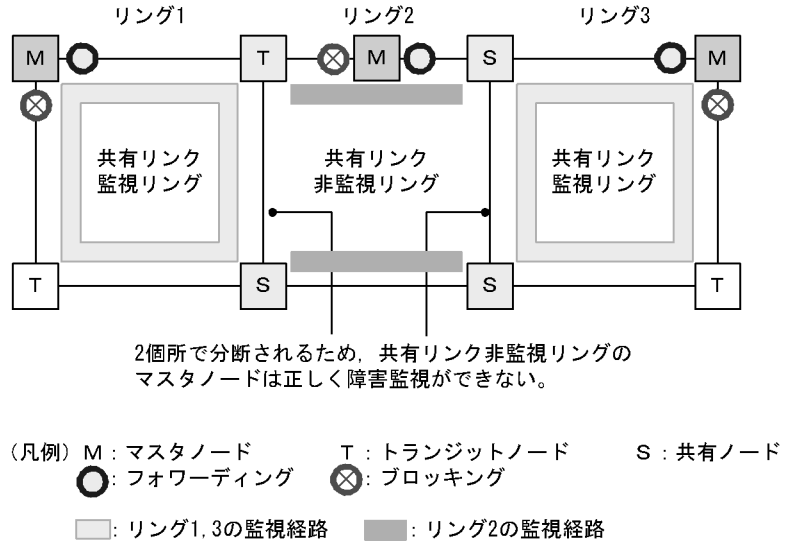


（2） 共有リンク監視リングが複数ある構成

共有リンクありのマルチリング構成では，共有リンク監視リングはネットワーク内で必ず一つとなるように構成してください。共有リンク監視リングが複数あると，共有リンク非監視リングでの障害監視が分断

されるため，正しい障害監視ができなくなります。

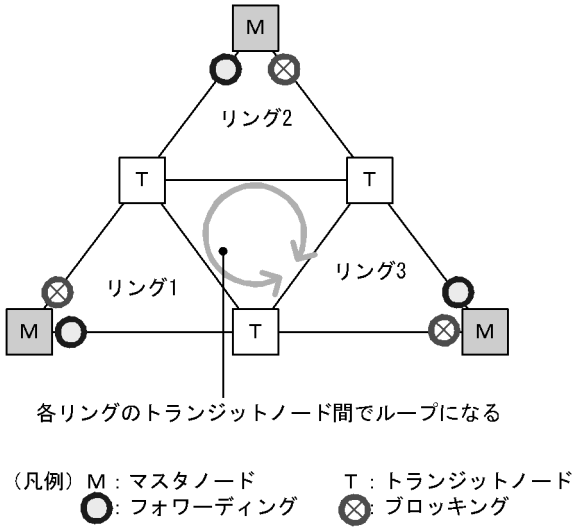
図 19-34　共有リンク監視リングが複数ある構成



（3） ループになるマルチリング構成例

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

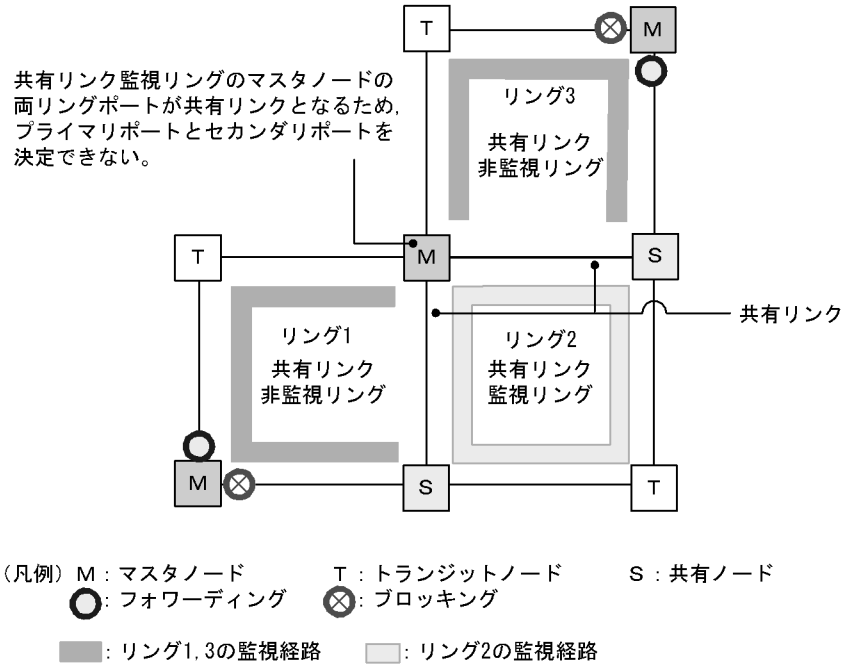
図 19-35　ループになるマルチリング構成



（4） マスタノードのプライマリポートが決定できない構成

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

図 19-36　マスタノードのプライマリポートが決定できない構成



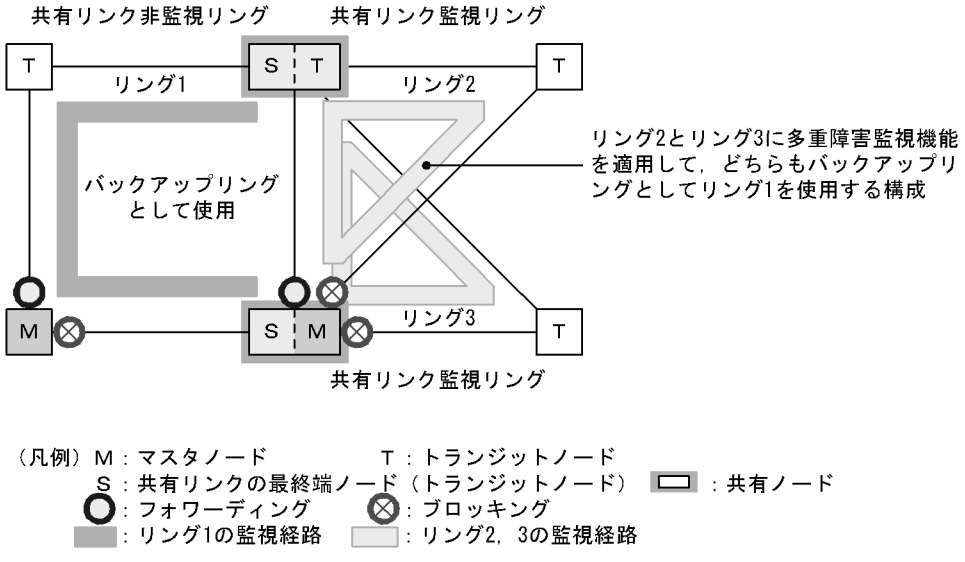
19.6.10　多重障害監視機能の禁止構成

多重障害監視機能使用時の禁止構成について次に示します。

（1）複数の共有リンク監視リングが同じバックアップリングを使用する構成

共有リンク監視リングと，多重障害検出時にバックアップリングとして使用する共有リンク非監視リングは，１対１に対応づけて構成する必要があります。複数の共有リンク監視リングが同じ共有リンク非監視リングをバックアップリングとして使用した場合，ある共有リンク監視リングで多重障害を検出したときに，別の共有リンク監視リングがバックアップリングにわたるループ構成となります。

図 19-37　複数の共有リンク監視リングが同じバックアップリングを使用する構成

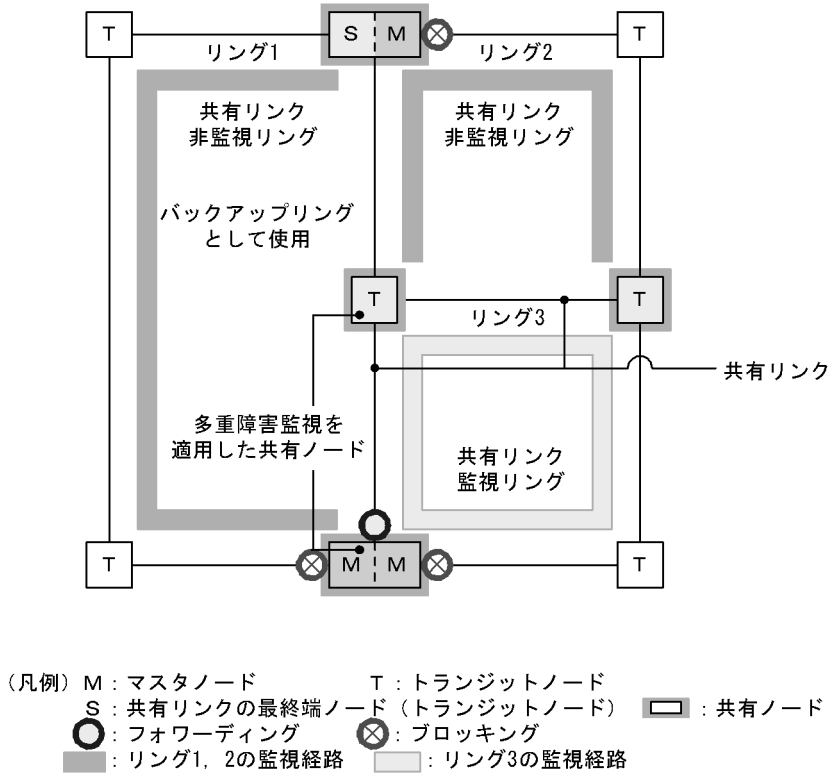


（2） 共有リンク内の共有ノードで多重障害を監視する構成

多重障害を監視する共有ノードは，共有リンクの最終端に位置する必要があります。このため，次の図に示すような構成では，共有リンクの共有ノードが多重障害を監視することになり正常に監視できません。

また，多重障害発生時にバックアップリングへの切り替えが正常にできません。

図 19-38　共有リンク内の共有ノードで多重障害を監視する構成

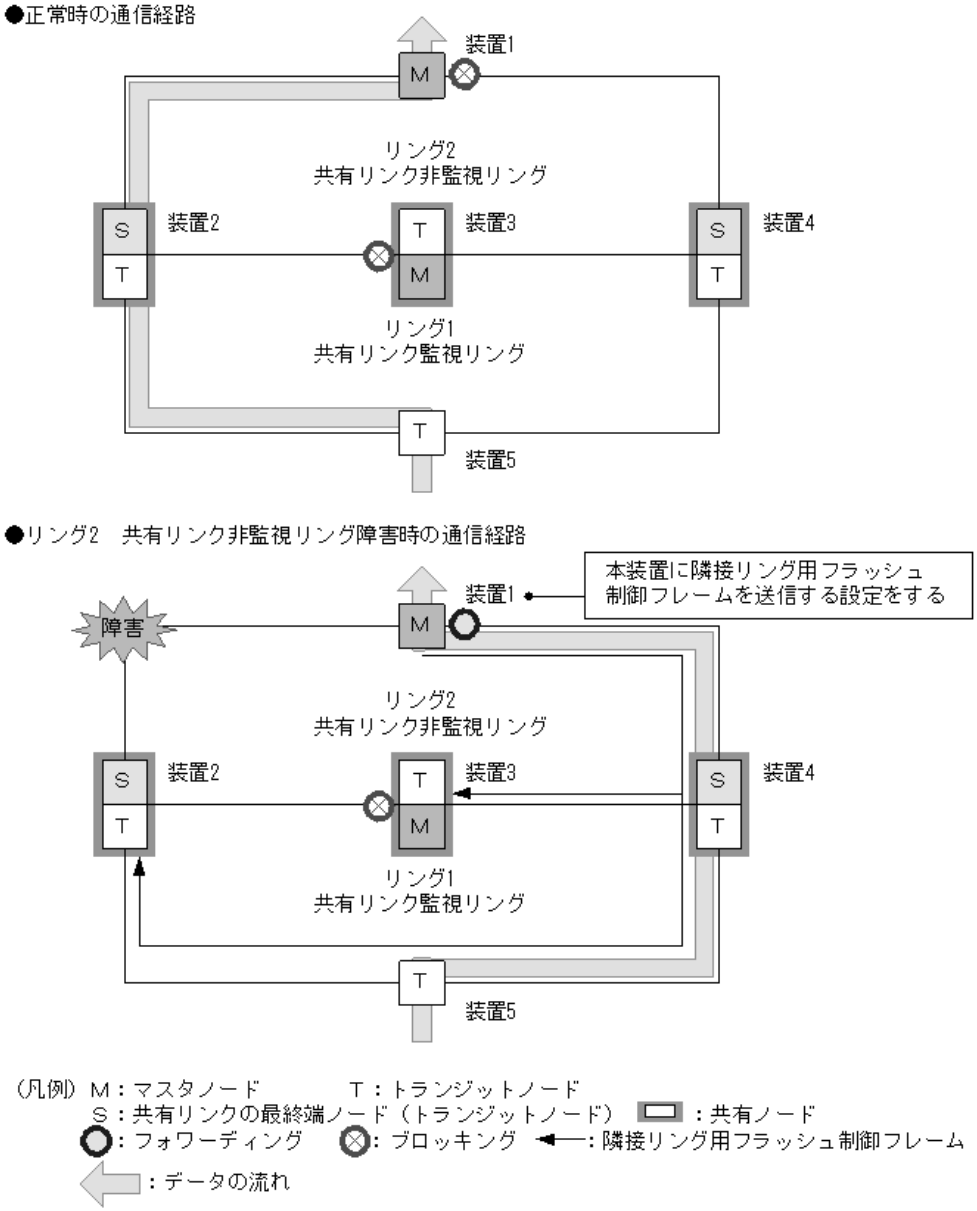


19.6.11　マスタノードの両リングポートが共有リンクとなる構成

次の図のように両リングポートが共有リンクとなるマスタノード（リング１の装置３）が存在する共有リンクありのマルチリング構成では，共有リンク非監視リングのマスタノード（リング２の装置１）に，コンフィグレーションコマンド flush-request-transmit vlan で隣接リング用フラッシュ制御フレームを送信する設定をしてください。

この設定によって，共有リンク非監視リングでリング障害が発生するとマスタノードは隣接するリングを構成する装置（以降，隣接リング構成装置）に隣接リング用フラッシュ制御フレームを送信するため，すぐに新しい通信経路に切り替えられます。なお，共有リンク非監視リングのリング障害が復旧した場合も同様になります。

図 19-39　マスタノードの両リングポートが共有リンクとなる構成例



このような構成で隣接リング用フラッシュ制御フレームを送信する設定をしない場合，共有リンク非監視リングでリング障害が発生すると，共有リンク非監視リングでは経路の切り替えが実施されますが，隣接する共有リンク監視リングでは実施されません。この結果，共有リンク監視リングを構成する装置では古い MAC アドレス学習の情報が残るため，すぐに新しい通信経路に切り替わらないおそれがあります。また，共有リンク非監視リングのリング障害が復旧した場合も同様になります。

19.7　Ring Protocol 使用時の注意事項

（1） 運用中のコンフィグレーション変更について

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

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

これらのコンフィグレーションは，次の手順で変更することを推奨します。

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

（2） 他機能との共存

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

（3） 制御 VLAN に使用する VLAN について

Ring Protocol の制御フレームは Tagged フレームになります。このため，制御 VLAN に使用する VLAN は，トランクポートの allowed vlan（ネイティブ VLAN は不可）に設定してください。

なお，デフォルト VLAN（VLAN ID=1）は設定できません。

（4） トランジットノードのリング VLAN 状態について

トランジットノードでは，装置またはリングポートが障害となり，その障害が復旧した際，ループの発生を防ぐために，リングポートのリング VLAN 状態はブロッキング状態となります。このブロッキング状態解除の契機の一つとして，フラッシュ制御フレーム受信待ち保護時間（コンフィグレーションコマンド forwarding-shift-time）のタイムアウトがあります。このとき，フラッシュ制御フレーム受信待ち保護時間（コンフィグレーションコマンド forwarding-shift-time）がマスタノードのヘルスチェック送信間隔（コンフィグレーションコマンド health-check interval）よりも短い場合，マスタノードがリング障害の復旧を検出して，セカンダリポートをブロッキング状態に変更するよりも先に，トランジットノードのリングポートがフォワーディング状態となることがあり，ループが発生するおそれがあります。従って，フラッシュ制御フレーム受信待ち保護時間（コンフィグレーションコマンド forwarding-shift-time）はヘルスチェック送信間隔（コンフィグレーションコマンド health-check interval）より大きい値を設定してください。

（5） 共有リンクありのマルチリングでの VLAN 構成について

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

（6） Ring Protocol 使用時のネットワーク構築について

Ring Protocol 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。従って，次の手順でネットワークを構築し，ループを防止してください。

- Ring Protocol のコンフィグレーション設定時，事前にリング構成ノードのリングポート（物理ポートまたはチャネルグループ）を shutdown に設定するなどダウン状態にしてください。
- ネットワーク内のすべての装置に Ring Protocol の設定が完了した時点でリングポートの shutdown を解除してください。

（7） ヘルスチェックフレームの送信間隔と障害監視時間について

障害監視時間（コンフィグレーションコマンド health-check holdtime）は送信間隔（コンフィグレーションコマンド health-check interval）より大きな値を設定してください。送信間隔よりも小さな値を設定すると，受信タイムアウトとなり障害を誤検出します。また，障害監視時間と送信間隔はネットワーク構成や運用環境などを十分に考慮した値を設定してください。障害監視時間は送信間隔の 3 倍以上を目安として設定することを推奨します。 3 倍未満に設定すると，ネットワークの負荷や装置の CPU 負荷などによって遅延が発生した場合に障害を誤検出するおそれがあります。

（8） 相互運用

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

（9） リングを構成する装置について

- Ring Protocol を用いたネットワーク内で，本装置間に Ring Protocol をサポートしていない他社スイッチや伝送装置などを設置した場合，本装置のマスタノードが送信するフラッシュ制御フレームを解釈できないため，即時に MAC アドレステーブルエントリがクリアされません。その結果，通信経路の切り替え（もしくは切り戻し）前の情報に従ってデータフレームの転送が行われるため，正しくデータが届かないおそれがあります。
- AX6700S，AX6600S，または AX6300S シリーズをマスタノード，本装置をトランジットノードとしてリングネットワークを構成した際は，マスタノードのヘルスチェックフレームの送信間隔を，本装置で指定できるヘルスチェックフレーム送信間隔の最小値以上の値に設定してください。本装置のヘルスチェックフレーム送信間隔の最小値より小さい値を設定すると，本装置の CPU 使用率が上昇し，正常にリングの動作が行われないおそれがあります。

（10） マスタノード障害時について

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

（11）ネットワーク内の多重障害時について

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

なお，多重障害監視機能を適用すると，障害の組み合わせによっては多重障害を検出できる場合があります。多重障害監視機能については，「19.5　Ring Protocol の多重障害監視機能」を参照してください。

（12）VLAN のダウンを伴う障害発生時の経路切り替えについて

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

（13）フラッシュ制御フレームの送信回数について

リングネットワークに適用している VLAN 数や VLAN マッピング数などの構成に応じて，マスタノードが送信するフラッシュ制御フレームの送信回数を調整してください。

一つのリングポートに 64 個以上の VLAN マッピングを使用している場合には，送信回数を 4 回以上に設定してください。3 回以下の場合，MAC アドレステーブルエントリが適切にクリアできず，経路の切り替えに時間がかかることがあります。

（14）VLAN のダウンを伴うコンフィグレーションコマンドの設定について

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

- axrp
- axrp vlan-mapping
- axrp-ring-port
- axrp-primary-port
- axrp virtual-link

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

（15）マスタノードの装置起動時のフラッシュ制御フレーム送受信について

マスタノードの装置起動時に，トランジットノードがマスタノードと接続されているリングポートのリンクアップをマスタノードよりも遅く検出すると，マスタノードが初期動作時に送信するフラッシュ制御フレームを受信できない場合があります。このとき，フラッシュ制御フレームを受信できなかったトランジットノードのリングポートはブロッキング状態となります。該当するリングポートはフラッシュ制御フレーム受信待ち保護時間（コンフィグレーションコマンド forwarding-shift-time）が経過するとフォワーディング状態となり，通信が復旧します。

隣接するトランジットノードでフラッシュ制御フレームが受信できない場合には，マスタノードのフラッシュ制御フレームの送信回数を調節すると，受信できることがあります。また，フラッシュ制御フレーム未受信による通信断の時間を短縮したい場合は，トランジットノードのフラッシュ制御フレーム受信待ち保護時間（初期値：10 秒）を短くしてください。

（16）経路切り戻し抑止機能運用時のフラッシュ制御フレーム受信待ち保護時間の設定について

経路切り戻し抑止機能を動作させる場合，トランジットノードでのフラッシュ制御フレーム受信待ち保護時間（コンフィグレーションコマンド forwarding-shift-time）には infinity を指定するか，または経路切り戻し抑止時間（コンフィグレーションコマンド preempt-delay）よりも大きな値を指定してください。経路切り戻し抑止中，トランジットノードでのフラッシュ制御フレーム受信待ち保護時間がタイムアウトして該当リングポートの論理ブロックを解除してしまうと，マスタノードはセカンダリポートの論理ブロック状態を解除しているため，ループが発生するおそれがあります。

（17）多重障害監視機能の監視開始タイミングについて

共有ノードでは，多重障害監視機能を適用したあと，対向の共有ノードが送信する多重障害監視フレームを最初に受信したときに多重障害の監視を開始します。このため，多重障害監視機能を設定するときにリングネットワークに障害が発生していると，多重障害の監視を開始できません。多重障害監視機能は，リングネットワークが正常な状態で設定してください。

（18）多重障害の一部復旧時の通信について

多重障害の一部復旧時はマスタノードがリング復旧を検出しないため，トランジットノードのリングポートはフラッシュ制御フレームの受信保護待ち時間（コンフィグレーションコマンド forwarding-shift-time）が経過するまでの間，論理ブロック状態となります。論理ブロック状態を解除したい場合は，フラッシュ制御フレーム受信待ち保護時間（初期値：10 秒）を短くするか，残りのリンク障害を復旧してマスタノードにリング復旧を検出させてください。なお，フラッシュ制御フレームの受信待ち保護時間を設定するときは，多重障害監視フレームの送信間隔（コンフィグレーションコマンド multi-fault-detection interval）よりも大きい値を設定してください。小さい値を設定すると，一時的にループが発生するおそれがあります。

（19）多重障害監視機能と経路切り戻し抑止機能の併用について

共有リンク非監視リングに経路切り戻し抑止機能を設定すると，多重障害が復旧したときに，セカンダリポートは復旧抑止状態を解除するまでの間フォワーディング状態を維持するため，ループ構成となるおそれがあります。多重障害監視機能と経路切り戻し抑止機能を併用する場合は，次のどれかで運用してください。

- 共有リンク監視リングだけに経路切り戻し抑止機能を設定する。
- 共有リンク監視リングの切り戻し抑止時間を，共有リンク非監視リングの切り戻し抑止時間よりも十分長くなるように設定する。
- 共有リンク監視リングおよび共有リンク非監視リングの切り戻し抑止時間に infinity を設定する場合は，共有リンク非監視リングの復旧抑止状態を解除してから共有リンク監視リングの復旧抑止状態を解除する。

（20）リングポートに指定したリンクアグリゲーションのダウンについて

リングネットワークを構成するノード間をリンクアグリゲーション（スタティックモードまたは LACP モード）で接続していた場合，リンクアグリゲーションの該当チャネルグループをコンフィグレーションコマンド shutdown でダウン状態にするときは，あらかじめチャネルグループに属するすべての物理ポートをコンフィグレーションコマンド shutdown でダウン状態に設定してください。

なお，該当チャネルグループをコンフィグレーションコマンド no shutdown でアップ状態にするときは，あらかじめチャネルグループに属するすべての物理ポートをコンフィグレーションコマンド shutdown でダウン状態に設定してください。

20 Ring Protocol の設定と運用

この章では，Ring Protocol の設定例について説明します。

20.1　コンフィグレーション

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

20.1.1　コンフィグレーションコマンド一覧

Ring Protocol のコンフィグレーションコマンド一覧を次の表に示します。

表 20-1　コンフィグレーションコマンド一覧

コマンド名	説明
axrp	リング ID を設定します。
axrp vlan-mapping	VLAN マッピング，およびそのマッピングに参加する VLAN を設定します。
axrp-primary-port	プライマリポートを設定します。
axrp-ring-port	リングポートを設定します。
control-vlan	制御 VLAN として使用する VLAN を設定します。
disable	Ring Protocol 機能を無効にします。
flush-request-count	フラッシュ制御フレームを送信する回数を設定します。
flush-request-transmit vlan	隣接するリング構成の装置に対して，隣接リング用フラッシュ制御フレームを送信する VLAN を設定します。
forwarding-shift-time	フラッシュ制御フレームの受信待ちを行う保護時間を設定します。
health-check holdtime	ヘルスチェックフレームの保護時間を設定します。
health-check interval	ヘルスチェックフレームの送信間隔を設定します。
mode	リングでの動作モードを設定します。
multi-fault-detection holdtime	多重障害監視フレームの受信待ち保護時間を設定します。
multi-fault-detection interval	多重障害監視フレームの送信間隔を設定します。
multi-fault-detection mode	多重障害監視の監視モードを設定します。
multi-fault-detection vlan	多重障害監視 VLAN として使用する VLAN を設定します。
name	リングを識別するための名称を設定します。
preempt-delay	経路切り戻し抑止機能を有効にして抑止時間を設定します。
vlan-group	Ring Protocol 機能で運用する VLAN グループ，および VLAN マッピング ID を設定します。

20.1.2　Ring Protocol 設定の流れ

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

（1）スパニングツリーの停止

Ring Protocol を使用する場合には，事前にスパニングツリーを停止することを推奨します。ただし，本装置で Ring Protocol とスパニングツリーを併用するときは，停止する必要はありません。スパニングツリーの停止については，「18　スパニングツリー」を参照してください。

（2） Ring Protocol 共通の設定

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

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

（3） モードとポートの設定

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

- モード
- リングポート

（4） 各種パラメータ設定

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

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

20.1.3 リング ID の設定

[設定のポイント]

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

[コマンドによる設定]

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

20.1.4 制御 VLAN の設定

（1） 制御 VLAN の設定

[設定のポイント]

制御 VLAN として使用する VLAN を指定します。なお，下記に該当する VLAN は設定できません。

- データ転送用 VLAN に使用されている VLAN
- 異なるリングで使用されている VLAN ID と同じ値の VLAN ID
- デフォルト VLAN（VLAN=1）

［コマンドによる設定］

1. **(config)# axrp 1**
   リング ID 1 の axrp コンフィグレーションモードに移行します。

2. **(config-axrp)# control-vlan 2**
   (config-axrp)# exit
   制御 VLAN として VLAN2 を指定します。

（2） 制御 VLAN のフォワーディング遷移時間の設定

［設定のポイント］

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

［コマンドによる設定］

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

20.1.5 VLAN マッピングの設定

（1） VLAN 新規設定

［設定のポイント］

データ転送用に使用する VLAN を VLAN マッピングに括り付けます。一つの VLAN マッピングを共通定義として複数のリングで使用できます。設定できる VLAN マッピングの最大数は 128 個です。
VLAN マッピングに設定する VLAN はリストで複数指定できます。
リングネットワーク内で使用するデータ転送用 VLAN は，すべてのノードで同じにする必要があります。ただし，VLAN グループに指定した VLAN マッピングの VLAN が一致していればよいため，リングネットワーク内のすべてのノードで VLAN マッピング ID を一致させる必要はありません。

［コマンドによる設定］

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

（2） VLAN 追加

［設定のポイント］

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

［コマンドによる設定］

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

（3） VLAN 削除

［設定のポイント］

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

［コマンドによる設定］

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

20.1.6 VLAN グループの設定

［設定のポイント］

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

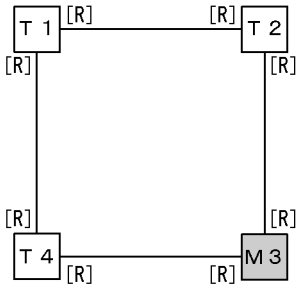
［コマンドによる設定］

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

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

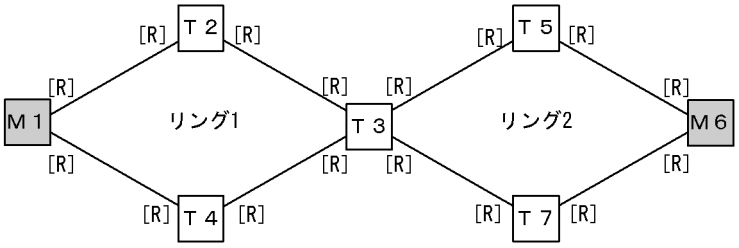
シングルリング構成を「図 20-1　シングルリング構成」に，共有リンクなしマルチリング構成を「図 20-2　共有リンクなしマルチリング構成」に示します。

図 20-1　シングルリング構成



（凡例）　M：マスタノード　　T：トランジットノード
[R]：リングポート

図 20-2　共有リンクなしマルチリング構成



（凡例）　M：マスタノード　　T：トランジットノード
[R]：リングポート

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

(1) マスタノード

[設定のポイント]

リングでの本装置の動作モードをマスタモードに設定します。イーサネットインタフェースまたはポートチャネルインタフェースをリングポートとして指定します。リングポートは一つのリングに対して二つ設定してください。「図 20-1　シングルリング構成」では M3 ノード，「図 20-2　共有リンクなしマルチリング構成」では M1 および M6 ノードがこれに該当します。

[コマンドによる設定]

1. **(config)# axrp 2**
   (config-axrp)# mode master
   (config-axrp)# exit
   リング ID 2 の動作モードをマスタモードに設定します。

2. **(config)# interface gigabitethernet 0/3**
   (config-if)# axrp-ring-port 2
   (config-if)# exit
   (config)# interface gigabitethernet 0/4
   (config-if)# axrp-ring-port 2
   (config-if)# exit

ポート 0/3 および 0/4 のインタフェースモードに移行し，該当するインタフェースをリング ID 2 のリングポートとして設定します。

（2） トランジットノード

［設定のポイント］

リングでの本装置の動作モードをトランジットモードに設定します。イーサネットインタフェースまたはポートチャネルインタフェースをリングポートとして指定します。リングポートは一つのリングに対して二つ設定してください。「図 20-1　シングルリング構成」では T1，T2 および T4 ノード，「図 20-2　共有リンクなしマルチリング構成」では T2，T3，T4，T5 および T7 ノードがこれに該当します。

［コマンドによる設定］

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

2. **(config)# interface gigabitethernet 0/3**
   (config-if)# axrp-ring-port 2
   (config-if)# exit
   (config)# interface gigabitethernet 0/4
   (config-if)# axrp-ring-port 2
   (config-if)# exit
   ポート 0/3 および 0/4 のインタフェースモードに移行し，該当するインタフェースをリング ID 2 のリングポートとして設定します。

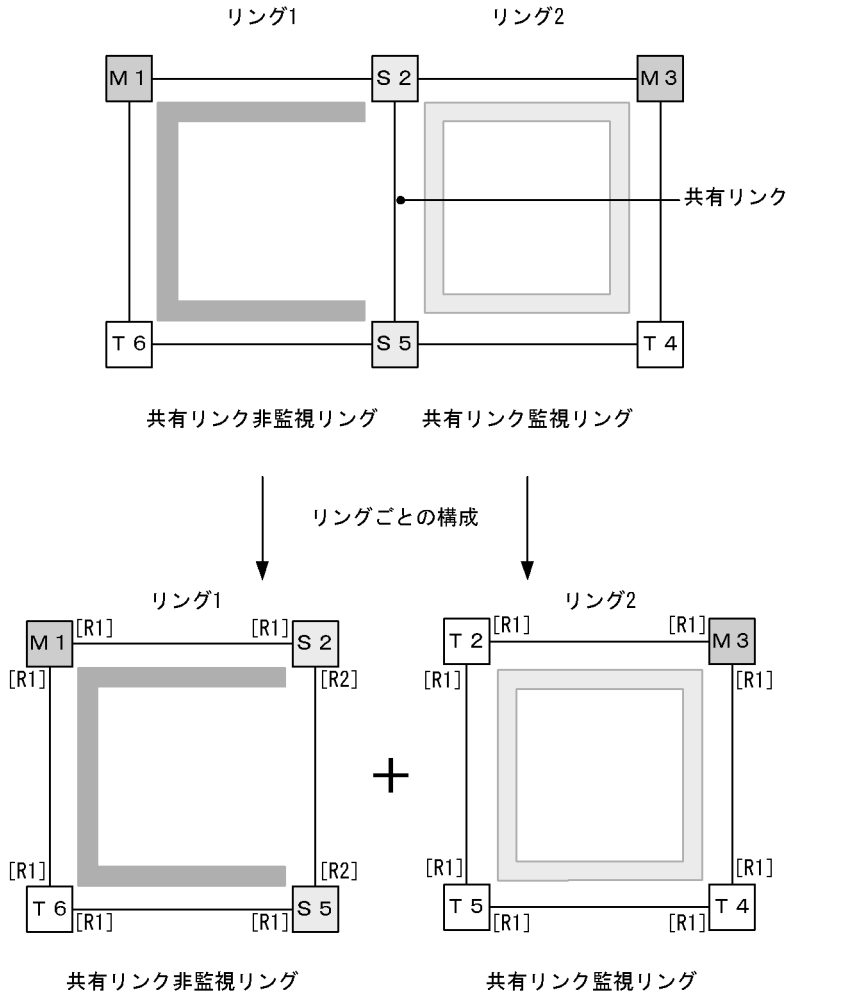
20.1.8　モードとリングポートに関する設定（共有リンクありマルチリング構成）

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

（1） 共有リンクありマルチリング構成（基本構成）

共有リンクありマルチリング構成（基本構成）を次の図に示します。

図 20-3　共有リンクありマルチリング構成（基本構成）



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

(a) 共有リンク監視リングのマスタノード

シングルリングのマスタノード設定と同様です。「20.1.7　モードとリングポートに関する設定（シングルリングと共有リンクなしマルチリング構成）（1）マスタノード」を参照してください。「図 20-3　共有リンクありマルチリング構成（基本構成）」では M3 ノードがこれに該当します。

(b) 共有リンク監視リングのトランジットノード

シングルリングのトランジットノード設定と同様です。「20.1.7　モードとリングポートに関する設定（シングルリングと共有リンクなしマルチリング構成）（2）トランジットノード」を参照してください。「図 20-3　共有リンクありマルチリング構成（基本構成）」では T2，T4 および T5 ノードがこれに該当します。

(c) 共有リンク非監視リングのマスタノード

[設定のポイント]

リングでの本装置の動作モードをマスタモードに設定します。また，本装置が構成しているリングの属性，およびそのリングでの本装置の位置づけを共有リンク非監視リングに設定します。イーサネットインタフェースまたはポートチャネルインタフェースをリングポートとして指定します。リングポートは一つのリングに対して二つ設定してください。「図 20-3　共有リンクありマルチリング構成（基本構成）」では M1 ノードがこれに該当します。

[コマンドによる設定]

1. **(config)# axrp 1**
   (config-axrp)# mode master ring-attribute rift-ring
   (config-axrp)# exit
   リング ID 1 の動作モードをマスタモード，リング属性を共有リンク非監視リングに設定します。

2. **(config)# interface gigabitethernet 0/3**
   (config-if)# axrp-ring-port 1
   (config-if)# exit
   (config)# interface gigabitethernet 0/4
   (config-if)# axrp-ring-port 1
   (config-if)# exit
   ポート 0/3 および 0/4 のインタフェースモードに移行し，該当するインタフェースをリング ID 1 のリングポートとして設定します。

(d) 共有リンク非監視リングのトランジットノード

シングルリングのトランジットノード設定と同様です。「20.1.7　モードとリングポートに関する設定（シングルリングと共有リンクなしマルチリング構成）(2) トランジットノード」を参照してください。「図 20-3　共有リンクありマルチリング構成（基本構成）」では T6 ノードがこれに該当します。

(e) 共有リンク非監視リングの最終端ノード（トランジット）

[設定のポイント]

リングでの本装置の動作モードをトランジットモードに設定します。また，本装置が構成しているリングの属性，およびそのリングでの本装置の位置づけを共有リンク非監視リングの最終端ノードに設定します。構成上二つ存在する共有リンク非監視リングの最終端ノードの区別にはエッジノード ID（1 または 2）を指定します。「図 20-3　共有リンクありマルチリング構成（基本構成)）」では S2 および S5 ノードがこれに該当します。リングポート設定は共有リンク側のポートにだけ shared-edge を指定します。「図 20-3　共有リンクありマルチリング構成（基本構成）」では S2 および S5 ノードのリングポート [R2] がこれに該当します。

[コマンドによる設定]

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

2. **(config)# interface gigabitethernet 0/3**

```
(config-if)# axrp-ring-port 1
(config-if)# exit
(config)# interface gigabitethernet 0/4
(config-if)# axrp-ring-port 1 shared-edge
(config-if)# exit
```

ポート 0/3 および 0/4 のインタフェースモードに移行し，該当するインタフェースをリング ID 1 のリングポートとして設定します。このとき，ポート 0/4 を共有リンクとして shared-edge パラメータも設定します。

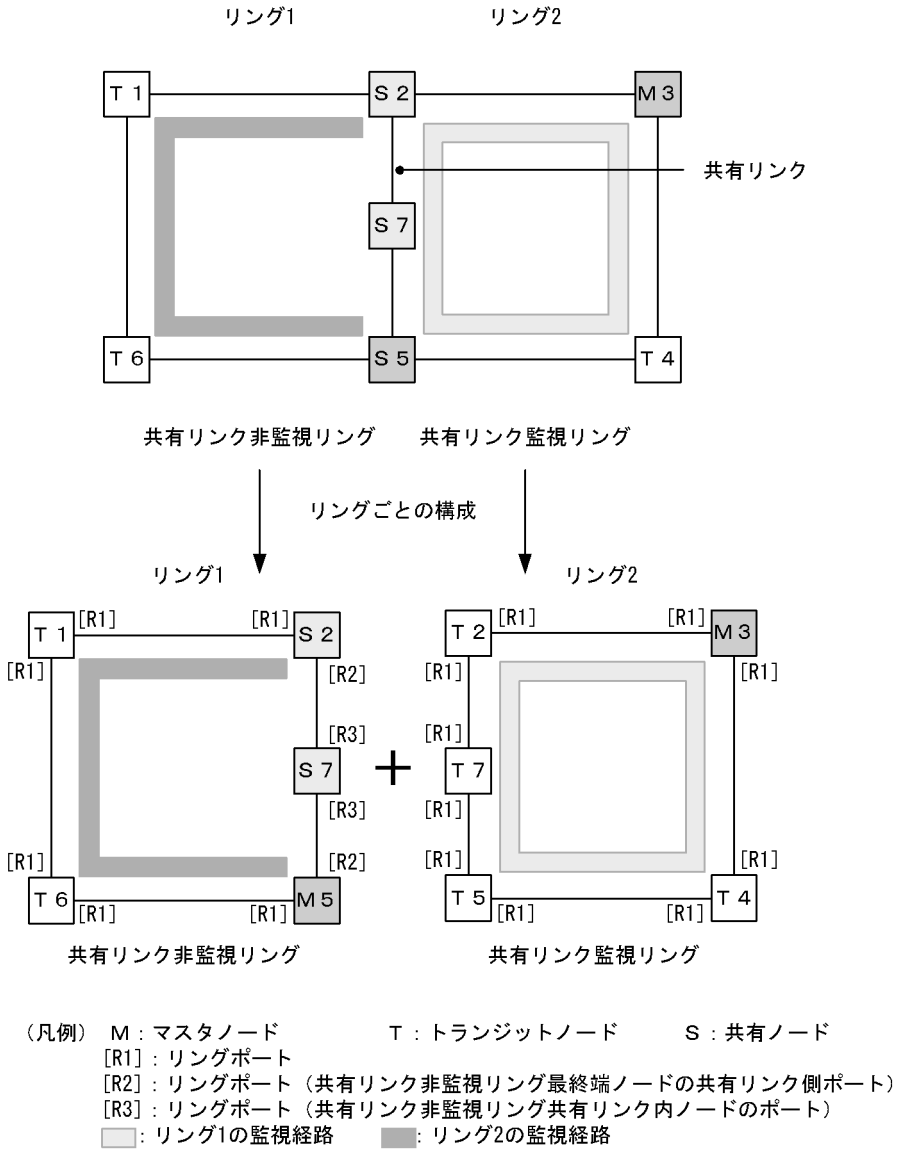
［注意事項］

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

（2） 共有リンクありのマルチリング構成（拡張構成）

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

図 20-4　共有リンクありのマルチリング構成（拡張構成）



(a) 共有リンク非監視リングの最終端ノード（マスタノード）

[設定のポイント]

リングでの本装置の動作モードをマスタモードに設定します。また，本装置が構成しているリングの属性，およびそのリングでの本装置の位置づけを共有リンク非監視リングの最終端ノードに設定します。構成上二つ存在する共有リンク非監視リングの最終端ノードの区別にはエッジノード ID（1 または 2）を指定します。「図 20-4　共有リンクありのマルチリング構成（拡張構成）」では M5 ノードがこれに該当します。リングポート設定は共有リンク側のポートにだけ shared-edge を指定します。「図 20-4　共有リンクありのマルチリング構成（拡張構成）」では M5 ノードのリングポート [R2] がこれに該当します。

[コマンドによる設定]

1. **(config)# axrp 1**
   (config-axrp)# mode master ring-attribute rift-ring-edge 2
   (config-axrp)# exit

リング ID 1 の動作モードをマスタモード，リング属性を共有リンク非監視リングの最終端ノード，エッジノード ID を 2 に設定します。

2. **(config)# interface gigabitethernet 0/3**
   (config-if)# axrp-ring-port 1
   (config-if)# exit
   (config)# interface gigabitethernet 0/4
   (config-if)# axrp-ring-port 1 shared-edge
   (config-if)# exit
   ポート 0/3 および 0/4 のインタフェースモードに移行し，該当するインタフェースをリング ID 1 のリングポートとして設定します。このとき，ポート 0/4 を共有リンクとして shared-edge パラメータも設定します。

［注意事項］

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

(b) 共有リンク非監視リングの共有リンク内ノード（トランジット）

［設定のポイント］

リングでの本装置の動作モードをトランジットモードに設定します。「図 20-4　共有リンクありのマルチリング構成（拡張構成）」では S7 ノードがこれに該当します。リングポートは両ポート共に shared パラメータを指定し，共有ポートとして設定します。「図 20-4　共有リンクありのマルチリング構成（拡張構成）」では S7 ノードのリングポート [R3] がこれに該当します。

［コマンドによる設定］

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

2. **(config)# interface gigabitethernet 0/3**
   (config-if)# axrp-ring-port 1 shared
   (config-if)# exit
   (config)# interface gigabitethernet 0/4
   (config-if)# axrp-ring-port 1 shared
   (config-if)# exit
   ポート 0/3 および 0/4 のインタフェースモードに移行し，該当するインタフェースをリング ID 1 の共有リンクポートに設定します。

［注意事項］

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

20.1.9　各種パラメータの設定

（1） Ring Protocol 機能の無効

［設定のポイント］

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

［コマンドによる設定］

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

（2） ヘルスチェックフレーム送信間隔

［設定のポイント］

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

［コマンドによる設定］

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

［注意事項］

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

（3） ヘルスチェックフレーム受信待ち保護時間

［設定のポイント］

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

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

［コマンドによる設定］

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

(4) フラッシュ制御フレーム受信待ち保護時間

[設定のポイント]

トランジットノードでのフラッシュ制御フレームの受信待ち保護時間を設定します。それ以外のノードでは，本設定を実施しても，無効となります。トランジットノードでのフラッシュ制御フレームの受信待ちの保護時間（forwarding-shift-time コマンドでの設定値）は，マスタノードでのヘルスチェックフレームの送信間隔（health-check interval コマンドでの設定値）よりも大きい値を設定してください。設定誤りからマスタノードが復旧を検出するよりも先にトランジットノードのリングポートがフォワーディング状態になってしまった場合，一時的にループが発生するおそれがあります。

[コマンドによる設定]

1. **(config)# axrp 1**
   (config-axrp)# forwarding-shift-time 100
   (config-axrp)# exit
   フラッシュ制御フレームの受信待ちの保護時間を 100 秒に設定します。

(5) プライマリポートの設定

[設定のポイント]

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

[コマンドによる設定]

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

(6) 経路切り戻し抑止機能の有効化および抑止時間の設定

[設定のポイント]

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

[コマンドによる設定]

1. **(config)# axrp 1**
   (config-axrp)# preempt-delay infinity
   (config-axrp)# exit
   リング ID 1 のコンフィグレーションモードに移行し，経路切り戻し抑止時間を infinity に設定します。

20.1.10 多重障害監視機能の設定

(1) 多重障害監視 VLAN の設定

[設定のポイント]

共有リンク監視リングの各ノードに多重障害監視 VLAN として使用する VLAN を設定します。なお，制御 VLAN とデータ転送用 VLAN に使われている VLAN は使用できません。また，異なるリングで使用されている多重障害監視 VLAN の VLAN ID と同じ値の VLAN ID は使用できません。

[コマンドによる設定]

1. **(config)# axrp 1**
   (config-axrp)# multi-fault-detection vlan 20
   (config-axrp)# exit
   リング ID 1 のコンフィグレーションモードに移行し，多重障害監視 VLAN として VLAN 20 を設定します。

[注意事項]

多重障害監視 VLAN は多重障害監視機能を適用する共有リンク監視リングのすべてのノードに設定してください。

(2) 多重障害監視の監視モードの設定

[設定のポイント]

共有リンク監視リングの各ノードに多重障害監視の監視モードと，多重障害検出時にバックアップリングに使用する共有リンク非監視リングのリング ID を設定します。監視モードは，多重障害監視を行う共有ノードに monitor-enable，その他の装置に transport-only を設定します。バックアップリングのリング ID は共有ノードに設定します。

(a) 共有リンク監視リングの共有ノード

[コマンドによる設定]

1. **(config)# axrp 1**
   (config-axrp)# multi-fault-detection mode monitor-enable backup-ring 2
   (config-axrp)# exit
   リング ID 1 のコンフィグレーションモードに移行し，多重障害監視の監視モードを monitor-enable，バックアップリングのリング ID を 2 に設定します。

[注意事項]

多重障害監視の監視モード monitor-enable は，共有リンクの両端に位置する 2 台の共有ノードに設定してください。1 台だけ設定した場合，多重障害監視は行われません。

(b) 共有リンク監視リングのその他のノード

[コマンドによる設定]

1. **(config)# axrp 1**
   (config-axrp)# multi-fault-detection mode transport-only
   (config-axrp)# exit
   リング ID 1 のコンフィグレーションモードに移行し，多重障害監視の監視モードを transport-only に設定します。

（3） 多重障害監視フレームの送信間隔

［設定のポイント］

共有リンク監視リングの共有ノードでの多重障害監視フレームの送信間隔を設定します。それ以外のノードでは，本設定を実施しても無効となります。

［コマンドによる設定］

1. **(config)# axrp 1**
   (config-axrp)# multi-fault-detection interval 1000
   (config-axrp)# exit
   リング ID 1 のコンフィグレーションモードに移行し，多重障害監視フレームの送信間隔を 1000 ミリ秒に設定します。

（4） 多重障害監視フレームの受信待ち保護時間

［設定のポイント］

共有リンク監視リングの共有ノードでの多重障害監視フレームの受信待ち保護時間を設定します。それ以外のノードでは，本設定を実施しても無効となります。

［コマンドによる設定］

1. **(config)# axrp 1**
   (config-axrp)# multi-fault-detection holdtime 3000
   (config-axrp)# exit
   リング ID 1 のコンフィグレーションモードに移行し，多重障害監視フレームの受信待ち保護時間を 3000 ミリ秒に設定します。

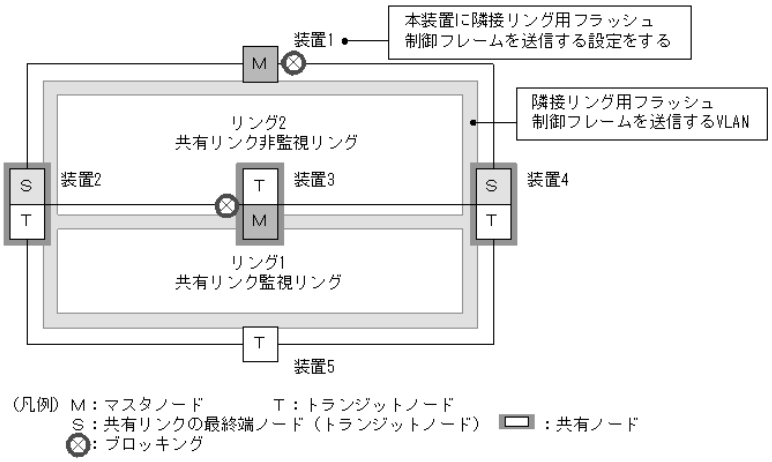
［注意事項］

受信待ち保護時間（multi-fault-detection holdtime コマンドでの設定値）には，対向の共有ノードの送信間隔（multi-fault-detection interval コマンドでの設定値）よりも大きい値を設定してください。

20.1.11 隣接リング用フラッシュ制御フレームの送信設定

マスタノードの両リングポートが共有リンクとなる構成を次の図に示します。このような構成では，共有リンク非監視リングのマスタノードで隣接リング用フラッシュ制御フレームを送信する設定をしてください。

図 20-5 マスタノードの両リングポートが共有リンクとなる構成



［設定のポイント］

「図 20-5　マスタノードの両リングポートが共有リンクとなる構成」のように両リングポートが共有リンクとなるマスタノード（リング 1 の装置 3）が存在する共有リンクありのマルチリング構成では，共有リンク非監視リングのマスタノード（リング 2 の装置 1）で隣接リング用フラッシュ制御フレームを送信する設定をしてください。

このとき，隣接リング用フラッシュ制御フレームの送信に使用する VLAN として，この図にあるように送信対象となるリングの各ノードで VLAN マッピングに括り付けられた VLAN を設定してください。

また，この VLAN は隣接リング用フラッシュ制御フレームの送信専用として，データ転送に使用しないでください。

［コマンドによる設定］

1. **(config)# axrp 2**
   (config-axrp)# flush-request-transmit vlan 10
   (config-axrp)# exit
   リング ID 2（共有リンク非監視リングのマスタノード）のコンフィグレーションモードに移行して，リング ID 2 の障害発生／復旧時に VLAN ID 10 に対して隣接リング用フラッシュ制御フレームを送信する設定をします。

20.2　オペレーション

20.2.1　運用コマンド一覧

Ring Protocol の運用コマンド一覧を次の表に示します。

表 20-2　運用コマンド一覧

コマンド名	説明
show axrp	Ring Protocol 情報を表示します。
clear axrp	Ring Protocol の統計情報をクリアします。
clear axrp preempt-delay	リングの経路切り戻し抑止状態を解除します。
show port ※1	ポートの Ring Protocol 使用状態を表示します。
show vlan ※2	VLAN の Ring Protocol 使用状態を表示します。

注※1
「運用コマンドレファレンス　12. イーサネット」を参照してください。

注※2
「運用コマンドレファレンス　15.VLAN」を参照してください。

20.2.2　Ring Protocol の状態確認

(1) コンフィグレーション設定と運用の状態確認

運用コマンド show axrp で Ring Protocol の設定と運用状態を確認できます。コンフィグレーションコマンドで設定した Ring Protocol の設定内容が正しく反映されているかどうかを確認してください。リング単位の状態情報確認には運用コマンド show axrp <Ring ID list> を使用できます。

表示される情報は，項目 "Oper State" の内容により異なります。"Oper State" に "enable" が表示されている場合は Ring Protocol 機能が動作しています。このとき，表示内容は全項目について運用の状態を示しています。"Oper State" に "-" が表示されている場合は必須であるコンフィグレーションコマンドが揃っていない状態です。また，"Oper State" に "Not Operating" が表示されている場合，コンフィグレーションに矛盾があるなどの理由で，Ring Protocol 機能が動作できていない状態です。"Oper State" の表示状態が "-"，または "Not Operating" 時には，コンフィグレーションを確認してください。

運用コマンド show axrp，運用コマンド show axrp detail の表示例を次に示します。

図 20-6　show axrp コマンドの実行結果

```
> show axrp
```

```
Date 20XX/07/02 17:08:17 UTC
Total Ring Counts:3

Ring ID:5
 Name:
 Oper State:enable           Mode:Transit    Attribute:rift-ring-edge(2)
 Shared Edge Port:64(ChGr)

 VLAN Group ID  Ring Port  Role/State            Ring Port  Role/State
 1              0/4        -/down                64(ChGr)   -/-
 2              -          -/-                   -          -/-

Ring ID:10
 Name:
 Oper State:enable           Mode:Master     Attribute:-

 VLAN Group ID  Ring Port  Role/State            Ring Port  Role/State
 1              0/1        secondary/forwarding  64(ChGr)   primary/down
 2              -          -/-                   -          -/-

Ring ID:11
 Name:
 Oper State:enable           Mode:Transit    Attribute:rift-ring-edge(2)
 Shared Edge Port:64(ChGr)

 VLAN Group ID  Ring Port  Role/State            Ring Port  Role/State
 1              0/3        -/forwarding          64(ChGr)   -/-
 2              -          -/-                   -          -/-

>
```

運用コマンド show axrp detail を使用すると，リング状態などについての詳細情報を確認できます。

図 20-7　show axrp detail のコマンド実行結果

```
> show axrp detail

Date 20XX/07/02 17:08:24 UTC
Total Ring Counts:3

Ring ID:5
 Name:
 Oper State:enable           Mode:Transit    Attribute:rift-ring-edge(2)
 Shared Edge Port:64(ChGr)
 Control VLAN ID:5
 Health Check Interval  (msec):500
 Forwarding Shift Time (sec):10
 Last Forwarding:flush request receive

 VLAN Group ID:1
  VLAN ID:50-99
  Ring Port:0/4         Role:-            State:down
  Ring Port:64(ChGr)    Role:-            State:-

 VLAN Group ID:2
  VLAN ID:-
  Ring Port:-           Role:-            State:-
  Ring Port:-           Role:-            State:-

Ring ID:10
 Name:
 Oper State:enable           Mode:Master     Attribute:-
 Control VLAN ID:10          Ring State:fault
 Health Check Interval  (msec):200
 Health Check Hold Time (msec):500
 Flush Request Counts:3

 VLAN Group ID:1
  VLAN ID:50-99
  Ring Port:0/1         Role:secondary    State:forwarding
  Ring Port:64(ChGr)    Role:primary      State:down

 VLAN Group ID:2
```

```
  VLAN ID:-
  Ring Port:-           Role:-            State:-
  Ring Port:-           Role:-            State:-

 Last Transition Time:2012/03/02 17:07:45
 Fault Counts    Recovery Counts    Total Flush Request Counts
 32              31                 327

Ring ID:11
 Name:
 Oper State:enable           Mode:Transit    Attribute:rift-ring-edge(2)
 Shared Edge Port:64(ChGr)
 Control VLAN ID:11
 Health Check Interval  (msec):500
 Forwarding Shift Time (sec):10
 Last Forwarding:flush request receive

 VLAN Group ID:1
  VLAN ID:50-99
  Ring Port:0/3         Role:-            State:forwarding
  Ring Port:64(ChGr)    Role:-            State:-

 VLAN Group ID:2
  VLAN ID:-
  Ring Port:-           Role:-            State:-
  Ring Port:-           Role:-            State:-

>
```

多重障害監視機能を適用すると，運用コマンド show axrp detail で多重障害の監視状態についての情報を確認できます。

図 20-8　多重障害監視機能適用時の運用コマンド show axrp detail の実行結果

```
> show axrp 10 detail

Date 20XX/07/02 17:10:32 UTC
Total Ring Counts:1

Ring ID:10
 Name:
 Oper State:enable           Mode:Master     Attribute:-
 Control VLAN ID:10          Ring State:fault
 Health Check Interval  (msec):200
 Health Check Hold Time (msec):500
 Flush Request Counts:3

 VLAN Group ID:1
  VLAN ID:50-99
  Ring Port:0/1         Role:secondary    State:forwarding
  Ring Port:64(ChGr)    Role:primary      State:down

 VLAN Group ID:2
  VLAN ID:-
  Ring Port:-           Role:-            State:-
  Ring Port:-           Role:-            State:-

 Last Transition Time:2012/03/02 17:09:45
 Fault Counts    Recovery Counts    Total Flush Request Counts
 32              31                 347

 Multi Fault Detection State:fault
  Mode:monitoring    Backup Ring ID:11
  Control VLAN ID:999
  Multi Fault Detection Interval  (msec):2000
  Multi Fault Detection Hold Time (msec):6000

>
```

21 Ring Protocol とスパニングツリー / GSRP の併用

この章では，同一装置での Ring Protocol とスパニングツリーの併用，および同一装置での Ring Protocol と GSRP の併用について説明します。

21.1　Ring Protocol とスパニングツリーとの併用

本装置では，Ring Protocol とスパニングツリーの併用ができます。Ring Protocol と併用可能なスパニングツリーのプロトコル種別については，「14.3　レイヤ 2 スイッチ機能と他機能の共存について」，Ring Protocol の詳細については，「19　Ring Protocol の解説」を参照してください。

21.1.1　概要

同一装置で Ring Protocol とスパニングツリーを併用して，コアネットワークを Ring Protocol，アクセスネットワークをスパニングツリーとしたネットワークを構成できます。例えば，すべてをスパニングツリーで構成していたネットワークを，コアネットワークだけ Ring Protocol に変更することで，アクセスネットワークの既存設備の多くを変更することなく流用できます。なお，Ring Protocol は，シングルリングおよびマルチリング（共有リンクありのマルチリングを含む）のどちらの構成でも，スパニングツリーと併用できます。

シングルリング構成，またはマルチリング構成での Ring Protocol とスパニングツリーとの併用例を次の図に示します。装置 A － G － I 間，B － F － J 間，C － D － K 間でそれぞれスパニングツリートポロジーを構成しています。なお，装置 A ～ D および F ～ G では，Ring Protocol とスパニングツリーが同時に動作しています。

図 21-1　Ring Protocol とスパニングツリーの併用例（シングルリング構成）

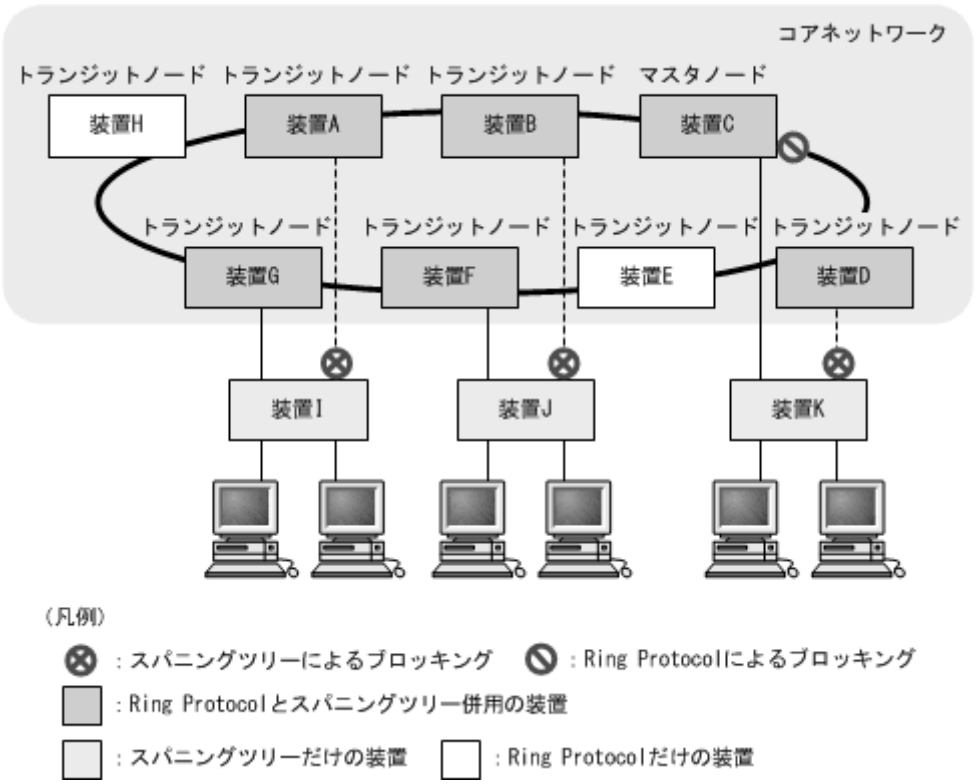
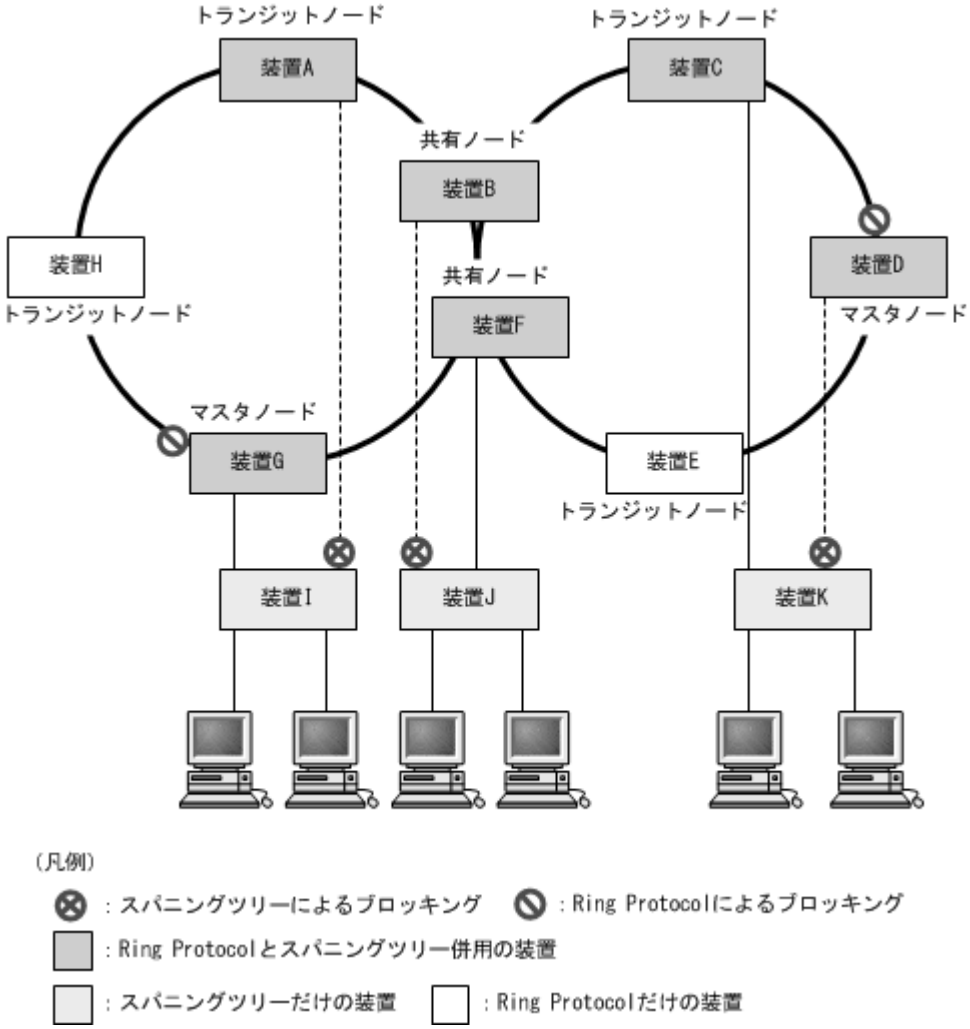


図 21-2　Ring Protocol とスパニングツリーの併用例（マルチリング構成）



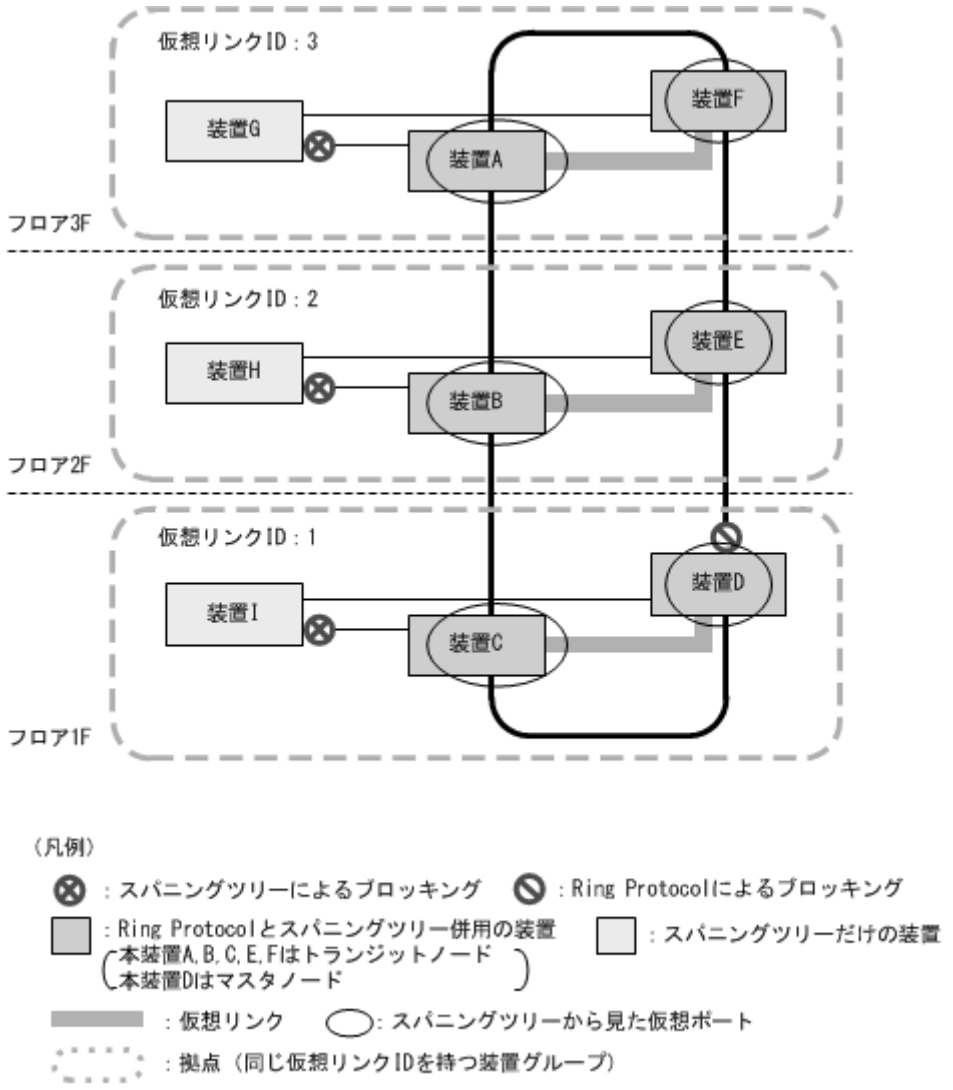
21.1.2　動作仕様

Ring Protocol とスパニングツリーを併用するには，二つの機能が共存している任意の 2 装置間を仮想的な回線で接続する必要があります。この仮想的な回線を仮想リンクと呼びます。仮想リンクは，リングネットワーク上の 2 装置間に構築されます。仮想リンクの構築には，仮想リンクを識別するための仮想リンク ID と，仮想リンク間で制御フレームの送受信を行うための仮想リンク VLAN が必要です。

Ring Protocol とスパニングツリーを併用するノードは，自装置の仮想リンク ID と同じ仮想リンク ID を持つ装置同士でスパニングツリートポロジーを構成します。同じ仮想リンク ID を持つ装置グループを拠点と呼び，各拠点では独立したスパニングツリートポロジーを構成します。

仮想リンクの概要を次の図に示します。

図 21-3 仮想リンクの概要



注 各フロアはそれぞれ独立したスパニングツリートポロジーを構成しています。

（1） 仮想リンク VLAN

仮想リンク間での制御フレームの送受信には，仮想リンク VLAN を使用します。この仮想リンク VLAN は，リングポートのデータ転送用 VLAN として管理している VLAN のうちの一つを使用します。また，仮想リンク VLAN は，複数の拠点で同一の VLAN ID を使用できます。

（2） Ring Protocol の制御 VLAN の扱い

Ring Protocol の制御 VLAN は，スパニングツリーの対象外となります。

そのため，PVST+ では当該 VLAN のツリーを構築しません。また，シングルスパニングツリーおよびマルチプルスパニングツリーの転送状態も適用されません。

（3） リングポートの状態とコンフィグレーションの設定値

リングポートのデータ転送用 VLAN の転送状態は，Ring Protocol で決定されます。

例えば，スパニングツリートポロジーでブロッキングと判断しても，Ring Protocol でフォワーディングと

判断すれば，そのポートはフォワーディングとなります。従って，スパニングツリーでリングポートがブロッキングとなるトポロジーを構築すると，ループとなるおそれがあります。このため，リングポートが常にフォワーディングとなるよう，Ring Protocol と共存したスパニングツリーでは，本装置がルートブリッジまたは 2 番目の優先度になるようにブリッジ優先度の初期値を自動的に高くして動作します。なお，コンフィグレーションで値を設定している場合は，設定した値で動作します。

ブリッジ優先度の設定値を次の表に示します。

表 21-1　ブリッジ優先度の設定値

設定項目	関連するコンフィグレーション	初期値
ブリッジ優先度	spanning-tree single priority spanning-tree vlan priority spanning-tree mst root priority	0

また，仮想リンクのポートは固定値で動作し，コンフィグレーションによる設定値は適用されません。

仮想リンクのポートの設定値を次の表に示します。

表 21-2　仮想リンクポートの設定値

設定項目	関連するコンフィグレーション	初期値
リンクタイプ	spanning-tree link-type	point-to-point
ポート優先度	spanning-tree single priority spanning-tree vlan priority spanning-tree mst root priority	0
パスコスト	spanning-tree cost spanning-tree single cost spanning-tree vlan cost spanning-tree mst cost	1

(4) リングポートでのスパニングツリー機能について

リングポートでは次に示すスパニングツリー機能は動作しません。

- BPDU フィルタ
- BPDU ガード
- ループガード機能
- ルートガード機能
- PortFast 機能

(5) スパニングツリートポロジー変更時の MAC アドレステーブルクリア

スパニングツリーでのトポロジー変更時に，シングルリングまたはマルチリングネットワーク全体に対して，MAC アドレステーブルエントリのクリアを促すフラッシュ制御フレームを送信します。これを受信したリングネットワーク内の各装置は，Ring Protocol が動作中のリングポートに対する，MAC アドレステーブルエントリをクリアします。なお，トポロジー変更が発生した拠点の装置は，スパニングツリープロトコルで MAC アドレステーブルエントリをクリアします。

(6) リングポート以外のポートの一時的なブロッキングについて

Ring Protocol とスパニングツリーを併用する装置で，次に示すイベントが発生した場合，リングポート以外のスパニングツリーが動作しているポートを一時的にブロッキング状態にします。

- 装置起動（装置再起動も含む）

スパニングツリーが仮想リンク経由の制御フレームを送受信できるようになる前にアクセスネットワーク内だけでトポロジを構築した場合，それだけではループ構成とならないためどのポートもブロッキングしません。従って，このままでは，リングネットワークとアクセスネットワークにわたるループ構成となります。このため，本装置で一時的にブロッキングしてループを防止します。本機能は PortFast 機能を設定しているポートでも動作します。本機能でのブロッキングは，次のどちらかで行われます。

- イベント発生から 20 秒間
- イベント発生から 20 秒以内に仮想リンク経由で制御フレームを受信した場合は受信から 6 秒間

本機能を有効に動作させるため，次の表に示すコンフィグレーションを「設定値」の範囲内で設定してください。範囲内の値で設定しなかった場合，一時的にループが発生するおそれがあります。

表 21-3 リングポート以外のポートを一時的にブロッキング状態にするときの設定状態

設定項目	関連するコンフィグレーション	初期値
Ring Protocol フラッシュ制御フレームの受信待ち保護時間	forwarding-shift-time	10 秒以下 （デフォルト値 10 秒）
スパニングツリー制御フレーム送信間隔	spanning-tree single hello-time spanning-tree vlan hello-time spanning-tree mst hello-time	2 秒以下 （デフォルト値 2 秒）

21.1.3 各種スパニングツリーとの共存について

（1） PVST+ との共存

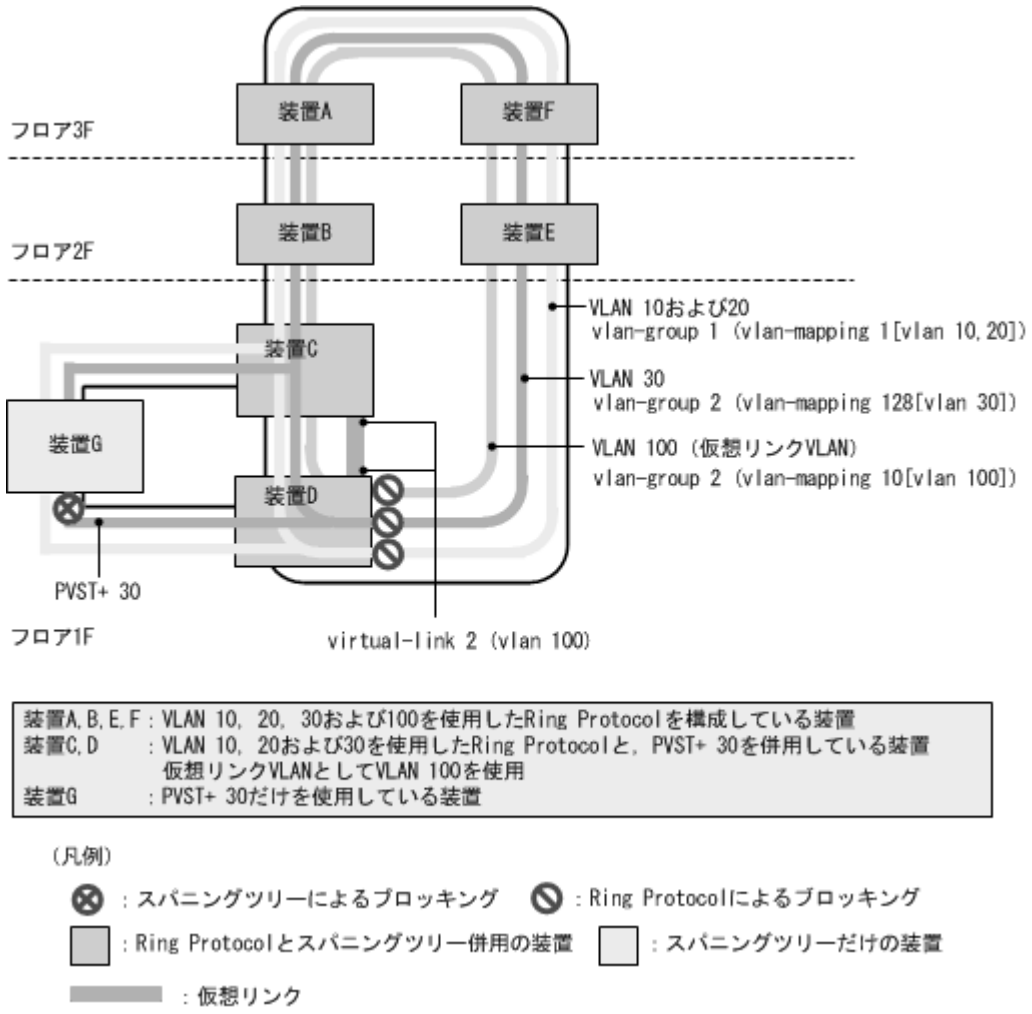
PVST+ は，Ring Protocol の VLAN マッピングに設定された VLAN が一つだけであれば，その VLAN で Ring Protocol と共存できます。コンフィグレーションコマンド axrp virtual-link で仮想リンクを設定すると，仮想リンクによるトポロジーを構築し Ring Protocol との共存を開始します。

最初の Ring Protocol のコンフィグレーション設定によって，動作中の PVST+ はすべて停止します。その後，VLAN マッピングが設定された VLAN で順次 PVST+ が動作します。VLAN マッピングに複数の VLAN を設定した場合，その VLAN では PVST+ は動作しません。なお，PVST+ が停止している VLAN はループとなるおそれがあります。ポートを閉塞するなどしてループ構成にならないように注意してください。

また，コンフィグレーションコマンド axrp virtual-link で仮想リンクを設定していない場合は，仮想リンクを構築できないので意図したトポロジーが構築されません。その結果，ループが発生するおそれがあります。

PVST+ と Ring Protocol の共存構成を次の図に示します。ここでは，VLAN マッピング 128 には VLAN 30 が一つだけ設定されているので，PVST+ が動作します。VLAN マッピング 1 には複数 VLAN が設定されているので，PVST+ は動作しません。また，装置 C および装置 D では VLAN 100 を仮想リンク VLAN に設定しているので，両装置間に仮想リンクを構築します。

図 21-4　PVST+ と Ring Protocol の共存構成



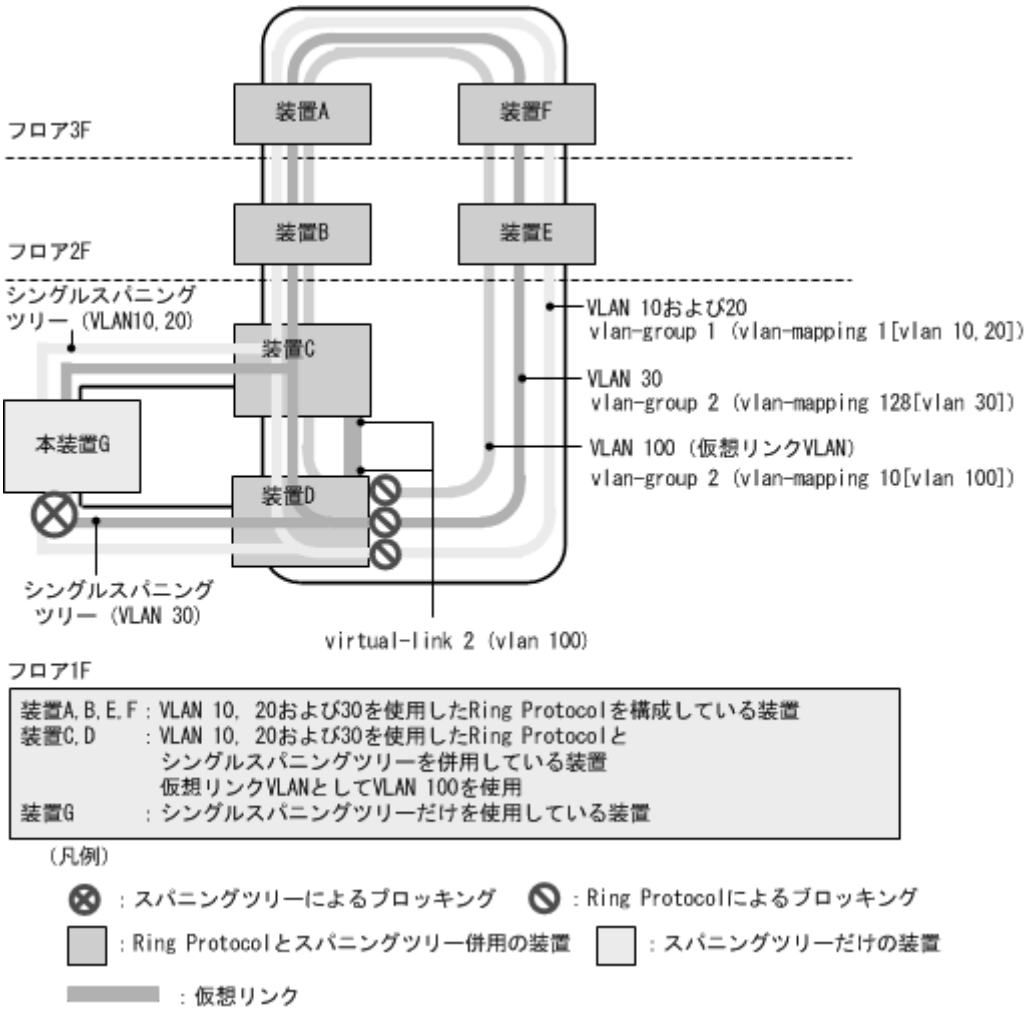
(2) シングルスパニングツリーとの共存

シングルスパニングツリーは Ring Protocol で運用するすべてのデータ VLAN と共存できます。

シングルスパニングツリーは，コンフィグレーションコマンド axrp virtual-link で仮想リンクを設定すると，仮想リンクによるトポロジーを構築し Ring Protocol との共存を開始します。コンフィグレーションコマンド axrp virtual-link で仮想リンクを設定していない場合は，仮想リンクを構築できないので意図したトポロジーが構築されません。その結果ループが発生するおそれがあります。

シングルスパニングツリーと Ring Protocol の共存構成を次の図に示します。ここでは，装置 C，D，および G にシングルスパニングツリーを設定し，装置 A，B，C，D，E，および F に Ring Protocol の VLAN グループを二つ設定しています。シングルスパニングツリーのトポロジーは，全 VLAN グループ（全 VLAN マッピング）に所属している VLAN にそれぞれ反映されます。また，装置 C および D では VLAN 100 を仮想リンク VLAN に設定しているので，両装置間に仮想リンクを構築します。

図 21-5 シングルスパニングツリーと Ring Protocol の共存構成

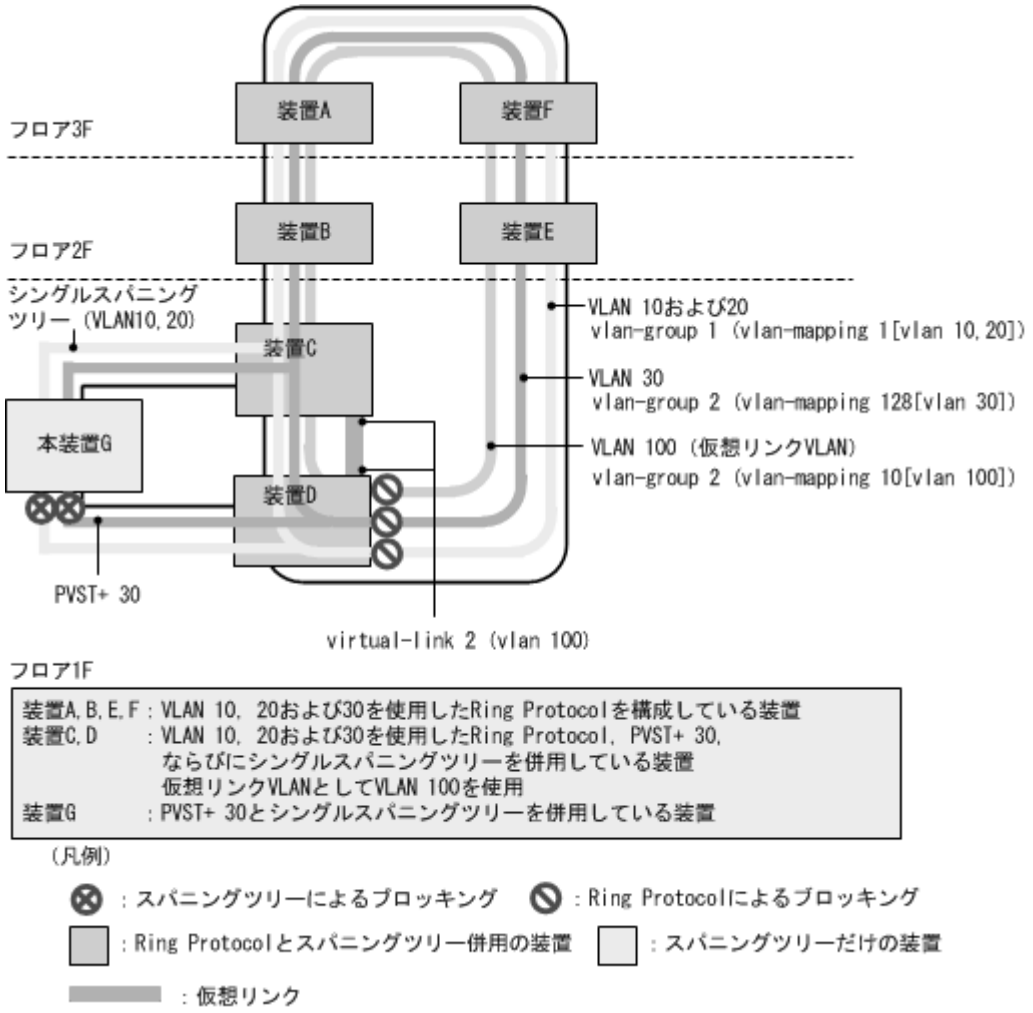


（3） PVST+ とシングルスパニングツリーの同時動作について

Ring Protocol と共存している場合でも，PVST+ とシングルスパニングツリーの同時動作は可能です。この場合，PVST+ で動作していない VLAN はすべてシングルスパニングツリーとして動作します。（通常の同時動作と同じです。）

シングルスパニングツリー，PVST+，および Ring Protocol の共存構成を次の図に示します。ここでは，VLAN マッピング 128 には VLAN 30 が一つだけ設定されているので，PVST+ が動作します。VLAN マッピング 1 では PVST+ が動作しないので，シングルスパニングツリーとして動作し，トポロジーを反映します。また，装置 C および D では VLAN 100 を仮想リンク VLAN に設定しているので，両装置間に仮想リンクを構築します。

図 21-6　シングルスパニングツリー，PVST+，および Ring Protocol の共存構成



（4） マルチプルスパニングツリーとの共存

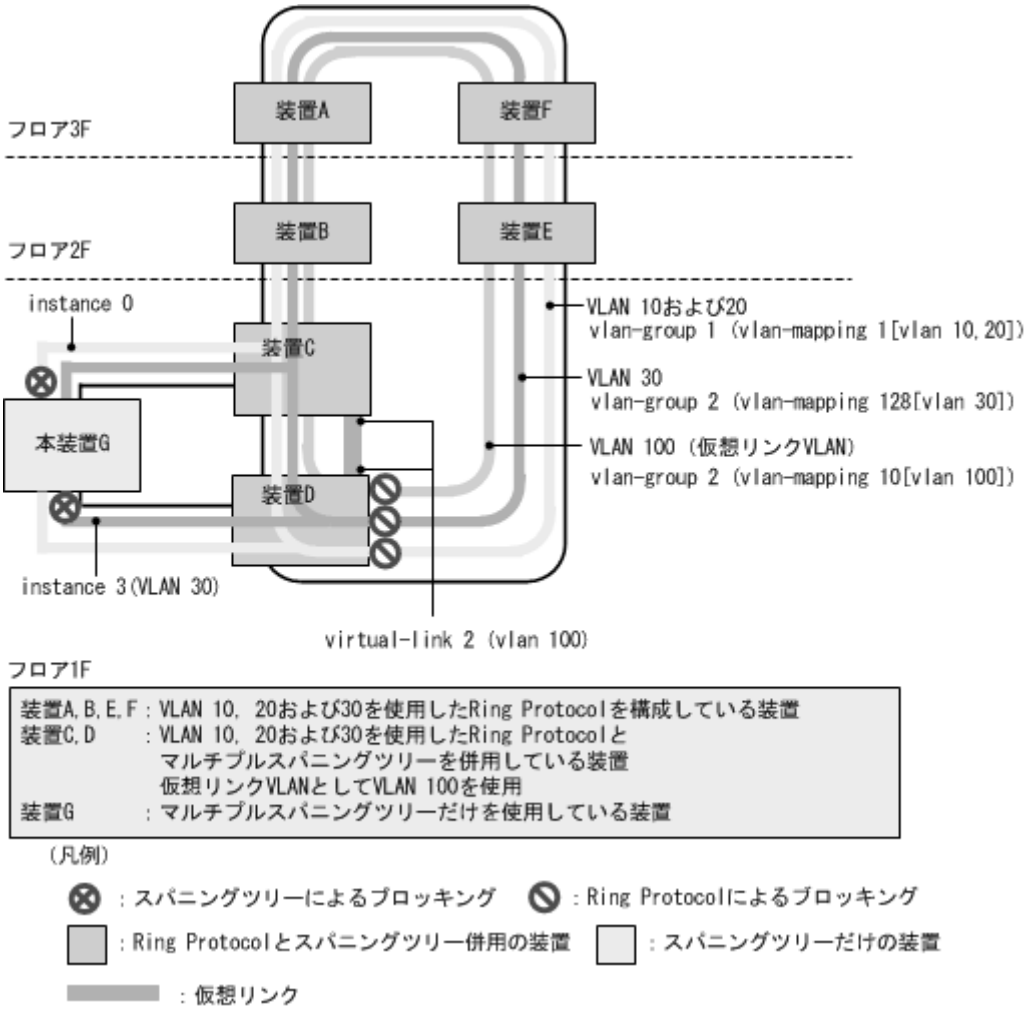
マルチプルスパニングツリーは Ring Protocol で運用するすべてのデータ転送用 VLAN と共存できます。

マルチプルスパニングツリーは，コンフィグレーションコマンド axrp virtual-link で仮想リンクを設定すると，仮想リンクによるトポロジーを構築し Ring Protocol との共存を開始します。コンフィグレーションコマンド axrp virtual-link で仮想リンクを設定していない場合は，仮想リンクを構築できないので意図したトポロジーが構築されません。その結果ループが発生するおそれがあります。

MST インスタンスに所属する VLAN と，Ring Protocol の VLAN マッピングで同じ VLAN を設定すると，MST インスタンスと Ring Protocol で共存動作できるようになります。設定した VLAN が一致しない場合，一致していない VLAN はブロッキング状態になります。

マルチプルスパニングツリーと Ring Protocol の共存構成を次の図に示します。ここでは，装置 C，D，および G にマルチプルスパニングツリーを設定し，装置 A，B，C，D，E，および F に Ring Protocol の VLAN グループを二つ設定しています。Ring Protocol の VLAN グループ 1 には CIST，VLAN グループ 2 には MST インスタンス 3 としてマルチプルスパニングツリーのトポロジーに反映されます。また，装置 C および D では VLAN 100 を仮想リンク VLAN に設定しているので，両装置間に仮想リンクを構築します。

図 21-7 マルチプルスパニングツリーと Ring Protocol の共存構成



(5) 共存して動作させない VLAN について

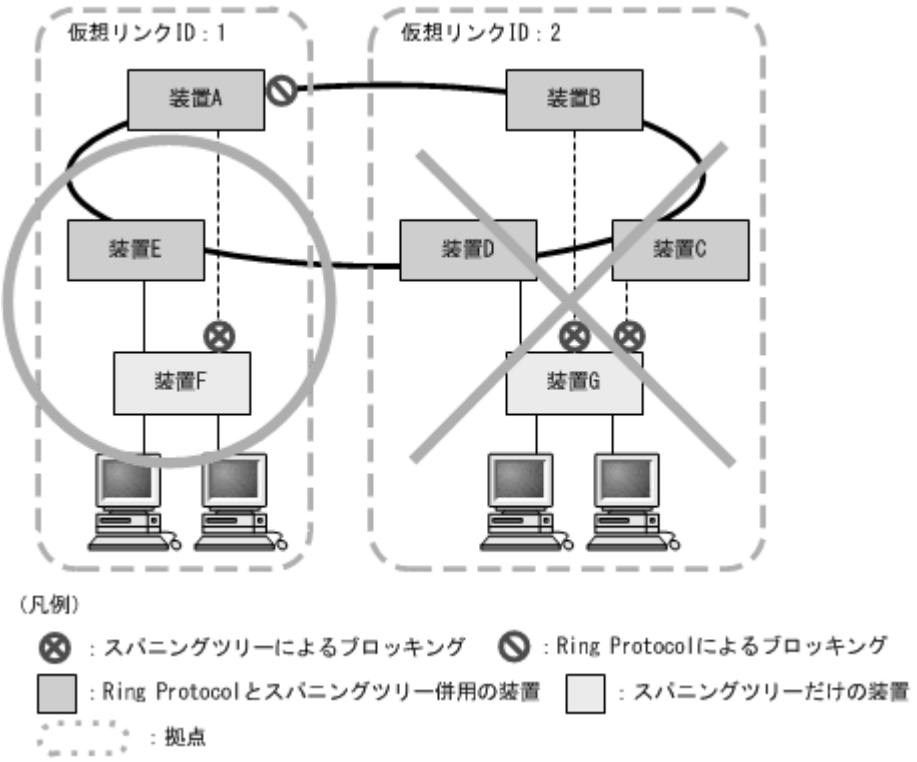
1. Ring Protocol だけを適用させる VLAN
   PVST+ をコンフィグレーション設定などで停止させると，その VLAN は Ring Protocol だけが適用される VLAN となります。
   シングルスパニングツリー動作時，またはマルチプルスパニングツリー動作時，Ring Protocol が扱うデータ転送 VLAN は必ず共存して動作します。
2. PVST+ だけを適用させる VLAN
   Ring Protocol で VLAN グループに所属していない VLAN マッピングを設定すると，PVST+ だけが適用される VLAN となります。
3. シングルスパニングツリーだけを適用させる VLAN
   Ring Protocol で VLAN グループに所属しない VLAN は，シングルスパニングツリーだけが適用される VLAN となります。
4. マルチプルスパニングツリーだけを適用させる VLAN
   Ring Protocol で VLAN グループに所属しない VLAN は，マルチプルスパニングツリーだけが適用される VLAN となります。

21.1.4　禁止構成

（1）１拠点当たりの装置数

Ring Protocol とスパニングツリーを併用した本装置は，1 拠点に 2 台配置できます。3 台以上で 1 拠点を構成することはできません。仮想リンクの禁止構成を次の図に示します。

図 21-8　仮想リンクの禁止構成



21.1.5　Ring Protocol とスパニングツリー併用時の注意事項

（1）仮想リンク VLAN と VLAN マッピングの対応づけについて

仮想リンク VLAN に指定する VLAN は，リング内のデータ転送用 VLAN に所属（VLAN マッピングおよび VLAN グループに設定）している必要があります。

（2）仮想リンク VLAN の設定範囲について

● リングネットワークへの設定

仮想リンクを構成しているリングネットワークでは，シングルリングおよびマルチリング（共有リンクありのマルチリング構成も含む）どちらの場合でも，仮想リンク間で制御フレームを送受信する可能性のあるすべてのノードに対して仮想リンク VLAN をデータ転送用 VLAN に設定しておく必要があります。設定が不足していると，拠点ノード間で仮想リンクを使って制御フレームの送受信ができず，障害の誤検出を起こすおそれがあります。

● スパニングツリーネットワークへの設定

仮想リンク VLAN は，リングネットワーク内で使用するため，下流側のスパニングツリーには使用できません。このため，スパニングツリーで制御する下流ポートに対して仮想リンク VLAN を設定すると，ループするおそれがあります。

（3） 仮想リンク VLAN を設定していない場合のスパニングツリーについて

仮想リンク VLAN を設定していない場合は，仮想リンクを構築できないので意図したトポロジーが構築されません。その結果ループが発生するおそれがあります。

（4） Ring Protocol の設定によるスパニングツリー停止について

最初の Ring Protocol のコンフィグレーション設定によって，動作中の PVST+ およびマルチプルスパニングツリーはすべて停止します。PVST+ またはマルチプルスパニングツリーが停止すると当該 VLAN はループとなるおそれがあります。ポートを閉塞するなどしてループ構成にならないように注意してください。

（5） Ring Protocol とスパニングツリー併用時のネットワーク構築について

Ring Protocol およびスパニングツリー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。既設のリングネットワークに対し，アクセスネットワークにスパニングツリーを構築する際は，スパニングツリーネットワーク側の構成ポート（物理ポートまたはチャネルグループ）を shutdown に設定するなどダウン状態にした上で構築してください。

（6） Ring Protocol の障害監視時間とスパニングツリーの BPDU の送信間隔について

Ring Protocol のヘルスチェックフレームの障害監視時間（health-check holdtime）は，スパニングツリーの BPDU のタイムアウト検出時間（hello-time × 3（秒））よりも小さな値を設定してください。大きな値を設定すると，リングネットワーク内で障害が発生した際に，Ring Protocol が障害を検出する前にスパニングツリーが BPDU のタイムアウトを検出してしまい，トポロジー変更が発生し，ループするおそれがあります。

（7） トランジットノードでの装置再起動時の対応について

装置再起動する際は，スパニングツリーネットワーク側の構成ポート（物理ポートまたはチャネルグループ）を shutdown に設定するなどダウン状態にした上で実施してください。再起動後は，トランジットノードのフラッシュ制御フレーム受信待ち保護時間（forwarding-shift-time）のタイムアウトを待つか，制御 VLAN のフォワーディング遷移時間（forwarding-delay-time）を利用して経路を切り替えたあとで，ダウン状態にしたポートの shutdown などを解除してください。

（8） リングネットワークでの片方向リンク障害の対応について

Ring Protocol は，片方向リンク障害でのリング障害は検出しません。リングネットワークで片方向リンク障害が発生すると，仮想リンク制御フレームを送受信できなくなるため，スパニングツリーが BPDU タイムアウトを誤検出してしまうことがあります。その結果，ループが発生し，ループ状態は片方向リンク障害が解消されるまで継続するおそれがあります。

Ring Protocol と IEEE802.3ah/UDLD 機能を併用すれば，片方向リンク障害を検出できるようになるため，片方向リンク障害によるループの発生を防止できます。

（9） スパニングツリー併用環境での多重障害からの復旧手順について

リングネットワーク内で 2ヶ所以上の障害（多重障害）が発生したことによって，仮想リンク制御フレームを送受信できなくなり，スパニングツリーのトポロジー変更が発生する場合があります。多重障害には，Ring Protocol とスパニングツリーを併用した装置で両リングポートに障害が発生した場合も含みます。この状態からリングネットワーク内のすべての障害を復旧する際は，次に示す手順で復旧してください。

1. スパニングツリーネットワークの構成ポート（物理ポートまたはチャネルグループ）を shutdown にす

るなどダウン状態にします。
2. リングネットワーク内の障害箇所を復旧し，マスタノードでリング障害の復旧を検出させます。
3. スパニングツリーネットワーク側の構成ポートの shutdown などを解除し，復旧させます。

（10）Ring Protocol の VLAN マッピングとマルチプルスパニングツリーの MST インスタンスに所属する VLAN との整合性について

コンフィグレーションの変更過程で，Ring Protocol の VLAN マッピングとマルチプルスパニングツリーの MST インスタンスに所属する VLAN の設定が完全に一致しない場合，一致していない VLAN はブロッキング状態になり，通信できないおそれがあります。

21.2　Ring Protocol と GSRP との併用

本装置では，Ring Protocol と GSRP の併用ができません。ただし，リング構成に GSRP と併用する装置（AX2400S/AX3600S/AX6700S シリーズなど）が存在する場合，本装置をリング構成に含めることができます。

21.2.1　動作概要

障害の監視や障害発生時の経路切り替えは，リングネットワークでは Ring Protocol で，GSRP ネットワークでは GSRP で，独立して実施します。ただし，GSRP ネットワークで経路の切り替え時にマスタに遷移した装置は，GSRP スイッチおよび aware/unaware 装置の MAC アドレステーブルをクリアします。同時に，リングネットワーク用のフラッシュ制御フレームを送信して，リングネットワークを構成する装置の MAC アドレステーブルもクリアします。

Ring Protocol と GSRP との併用例を次の図に示します。

図 21-9　Ring Protocol と GSRP の併用例と本装置の位置づけ（ダイレクトリンクをリングネットワークで使用する場合）

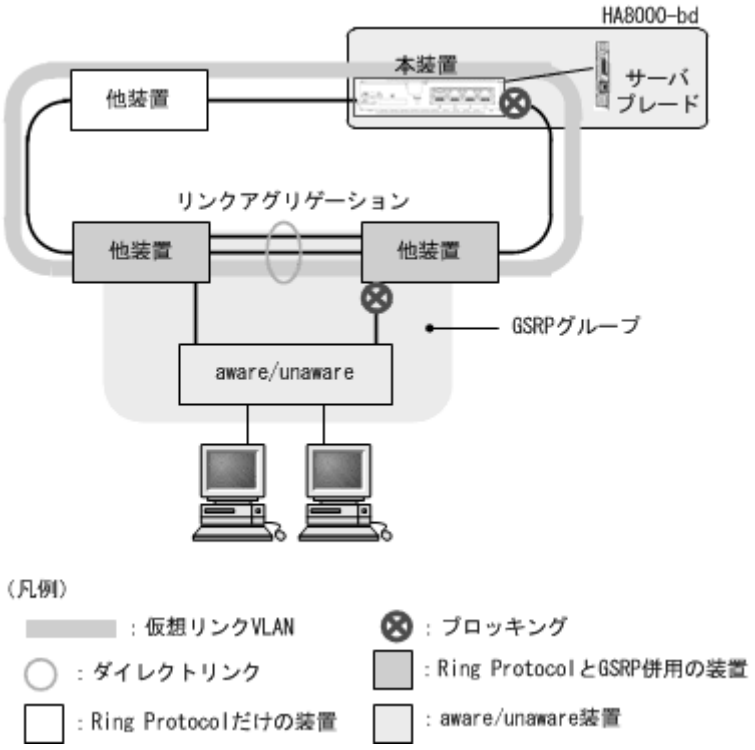
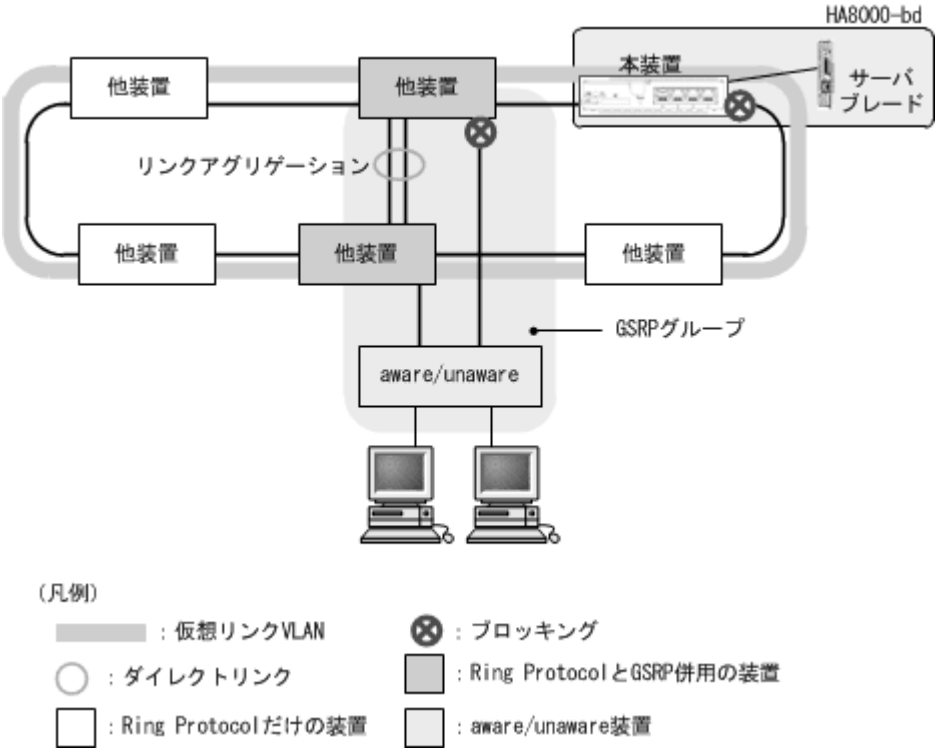


図 21-10　Ring Protocol と GSRP の併用例と本装置の位置づけ（ダイレクトリンクをリングネットワークで使用しない場合）



本装置は，後述の仮想リンク制御フレームの中継と MAC アドレステーブルクリアだけを行います。Ring Protocol と GSRP の併用動作および仮想リンクなどの詳細は，AX シリーズのマニュアル (AX2400S/AX3600S/AX6700S など）を参照してください。

（1） GSRP の仮想リンク制御フレームの中継

Ring Protocol と GSRP を併用する装置では，前述の Ring Protocol とスパニングツリーの併用装置と同様に，リングネットワーク上の 2 装置間に仮想リンクが構築されます。仮想リンク制御フレームの送受信は，リングネットワーク上に設定された仮想リンク VLAN が使用されます。この仮想リンク VLAN は，リングポートのデータ転送用 VLAN グループに所属する VLAN が使用されます。

GSRP スイッチから仮想リンク制御フレームが送信されると，本装置を含むリングネットワーク上の装置は，仮想リンク制御フレームを中継します。

（2） GSRP ネットワーク切り替え時の MAC アドレステーブルクリア

Ring Protocol と GSRP を併用する場合，GSRP ネットワークの経路切り替え時にはリングネットワークを構成する装置の MAC アドレステーブルをクリアする必要があります。MAC アドレステーブルをクリアしないと，すぐに通信が復旧しないおそれがあります。リングネットワーク上の装置の MAC アドレステーブルをクリアするために，GSRP のマスタに遷移した際，リングネットワーク上に設定した仮想リンク VLAN を使用して，リングネットワーク用のフラッシュ制御フレームを送信します。

GSRP のマスタから送信されたフラッシュ制御フレームを，本装置を含むリングネットワーク上の装置が受信すると，MAC アドレステーブルをクリアします。

21.3 仮想リンクのコンフィグレーション

Ring Protocol とスパニングツリープロトコルを同一装置で併用するための仮想リンクを設定します。

Ring Protocol と GSRP を併用するための仮想リンクは，GSRP スイッチ（AX2400S/AX3600S/AX6700S シリーズなど）側で設定しますので，本装置では設定不要です。

21.3.1 コンフィグレーションコマンド一覧

仮想リンクのコンフィグレーションコマンド一覧を次の表に示します。

表 21-4 コンフィグレーションコマンド一覧

コマンド名	説明
axrp virtual-link	仮想リンク ID を設定します。

21.3.2 仮想リンクの設定

［設定のポイント］

仮想リンク ID および仮想リンク VLAN を設定します。仮想リンクを設定することで，Ring Protocol とスパニングツリーの併用が可能になります。同一拠点内の対向装置にも，同じ仮想リンク ID と仮想リンク VLAN を設定してください。また，仮想リンク VLAN は必ずデータ転送用 VLAN に使用している VLAN から一つ選んで使用してください。

［コマンドによる設定］

1. **(config)# axrp virtual-link 10 vlan 100**
   仮想リンク ID を 10 に，仮想リンク VLAN を 100 に設定します。

21.3.3 Ring Protocol と PVST+ との併用設定

［設定のポイント］

Ring Protocol と PVST+ とを併用する場合は，併用したい VLAN ID を VLAN マッピングに設定する必要があります。その際，VLAN マッピングに指定する VLAN ID は一つだけです。VLAN マッピングに対して，PVST+ と併用する VLAN 以外の VLAN ID が設定されている場合，その VLAN では PVST+ が動作しません。

［コマンドによる設定］

1. **(config)# axrp vlan-mapping 1 vlan 10**
   VLAN マッピング ID を 1 として，PVST+ と併用する VLAN ID 10 を設定します。

2. **(config)# axrp vlan-mapping 2 vlan 20,30**
   VLAN マッピング ID を 2 として，Ring Protocol だけで使用する VLAN ID 20 および 30 を設定します。

3. **(config)# axrp 1**
   (config-axrp)# vlan-group 1 vlan-mapping 1-2
   (config-axrp)# exit

VLAN グループ 1 に，VLAN マッピング ID 1 および 2 を設定します。

21.3.4 Ring Protocol とマルチプルスパニングツリーとの併用設定

［設定のポイント］

Ring Protocol とマルチプルスパニングツリーを併用する場合は，併用したい VLAN ID を VLAN マッピングに設定する必要があります。その際，VLAN マッピングに指定する VLAN ID と MST インスタンスに所属する VLAN に指定する VLAN ID を一致させる必要があります。VLAN マッピングと MST インスタンスに所属する VLAN の VLAN ID が一致していない場合，一致していない VLAN の全ポートがブロッキング状態になります。

［コマンドによる設定］

1. **(config)# axrp vlan-mapping 1 vlan 10,20,30**
   VLAN マッピング ID を 1 として，MST インスタンス 10 と併用する VLAN ID 10，20，および 30 を設定します。

2. **(config)# axrp vlan-mapping 2 vlan 40,50**
   VLAN マッピング ID を 2 として，MST インスタンス 20 と併用する VLAN ID 40 および 50 を設定します。

3. **(config)# axrp 1**
   (config-axrp)# vlan-group 1 vlan-mapping 1-2
   (config-axrp)# exit
   VLAN グループ 1 に，VLAN マッピング ID 1 および 2 を設定します。

4. **(config)# spanning-tree mst configuration**
   (config-mst)# instance 10 vlans 10,20,30
   MST インスタンス 10 に所属する VLAN に vlan-mapping 1 で指定した VLAN ID 10，20，および 30 を設定し，Ring Protocol との共存を開始します。

5. **(config-mst)# instance 20 vlans 40,50**
   (config-mst)# exit
   MST インスタンス 20 に所属する VLAN に vlan-mapping 2 で指定した VLAN ID 40 および 50 を設定し，Ring Protocol との共存を開始します。

21.4　仮想リンクのオペレーション

21.4.1　運用コマンド一覧

仮想リンクの運用コマンド一覧を次の表に示します。

表 21-5　運用コマンド一覧

コマンド名	説明
show spanning-tree	スパニングツリーでの仮想リンクの適用状態を表示します。

21.4.2　仮想リンクの状態の確認

仮想リンクの情報は運用コマンド show spanning-tree で確認してください。Port Information で仮想リンクポートが存在していることを確認してください。

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

図 21-11　show spanning-tree の実行結果

```
> show spanning-tree

Date 20XX/06/27 06:39:38 UTC
VLAN 100  PVST+ Spanning Tree:Enabled   Mode:PVST+
  Bridge ID       Priority: 100       MAC Address: 0000.87f0.0008
    Bridge Status: Designated
  Root Bridge ID  Priority: 100       MAC Address: 0000.87f0.0001
    Root Cost: 1
    Root Port: 0/1-2(VL: 250)                                  …1
  Port Information
    VL:250    Up   Status:Forwarding  Role:Root         -       …1

>
```

1.VL は，仮想リンク ID を示しています。

22 IGMP snooping/MLD snooping の解説

IGMP snooping/MLD snooping はレイヤ 2 スイッチで VLAN 内のマルチキャストトラフィックを制御する機能です。この章では，IGMP snooping/MLD snooping について説明します。

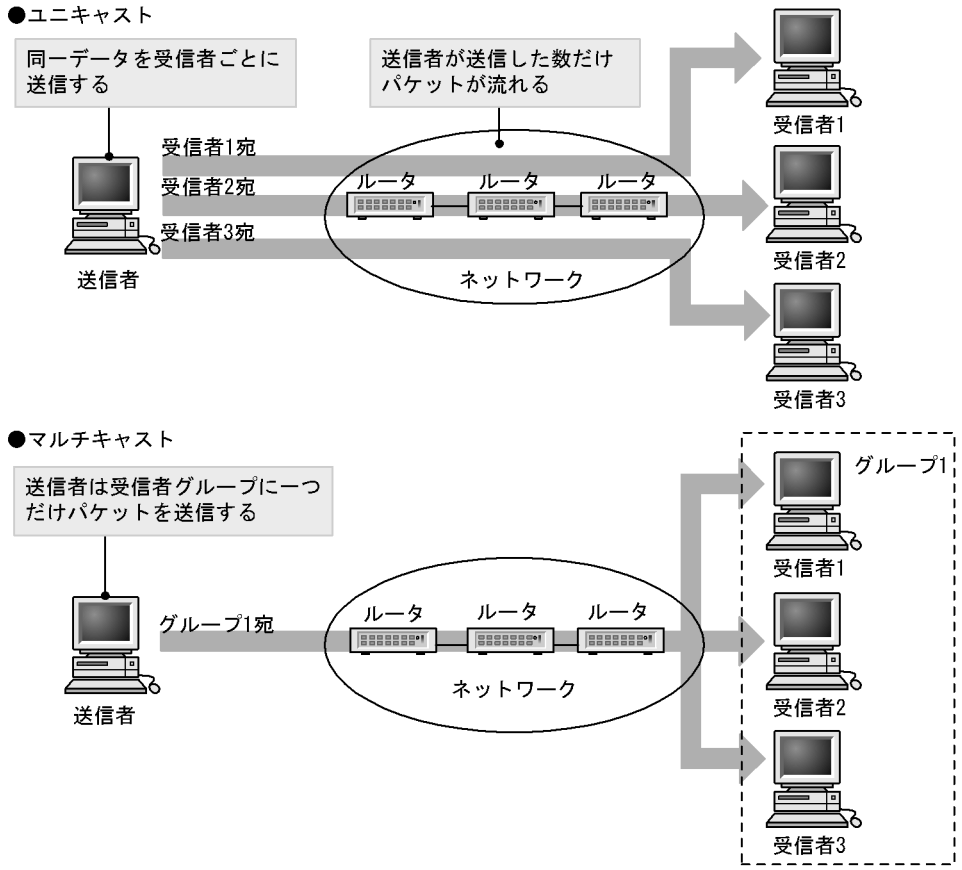
22.1　IGMP snooping/MLD snooping の概要

この節では，マルチキャスト，IGMP snooping および MLD snooping の概要について説明します。

22.1.1　マルチキャスト概要

同一の情報を複数の受信者に送信する場合，ユニキャストでは送信者が受信者の数だけデータを複製して送信するため，送信者とネットワークの負荷が高くなります。マルチキャストでは送信者がネットワーク内で選択されたグループに対してデータを送信します。送信者は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を軽減できます。マルチキャスト概要を次の図に示します。

図 22-1　マルチキャスト概要



マルチキャストで送信する場合に，宛先アドレスにはマルチキャストグループアドレスを使用します。マルチキャストグループアドレスを次の表に示します。

表 22-1　マルチキャストグループアドレス

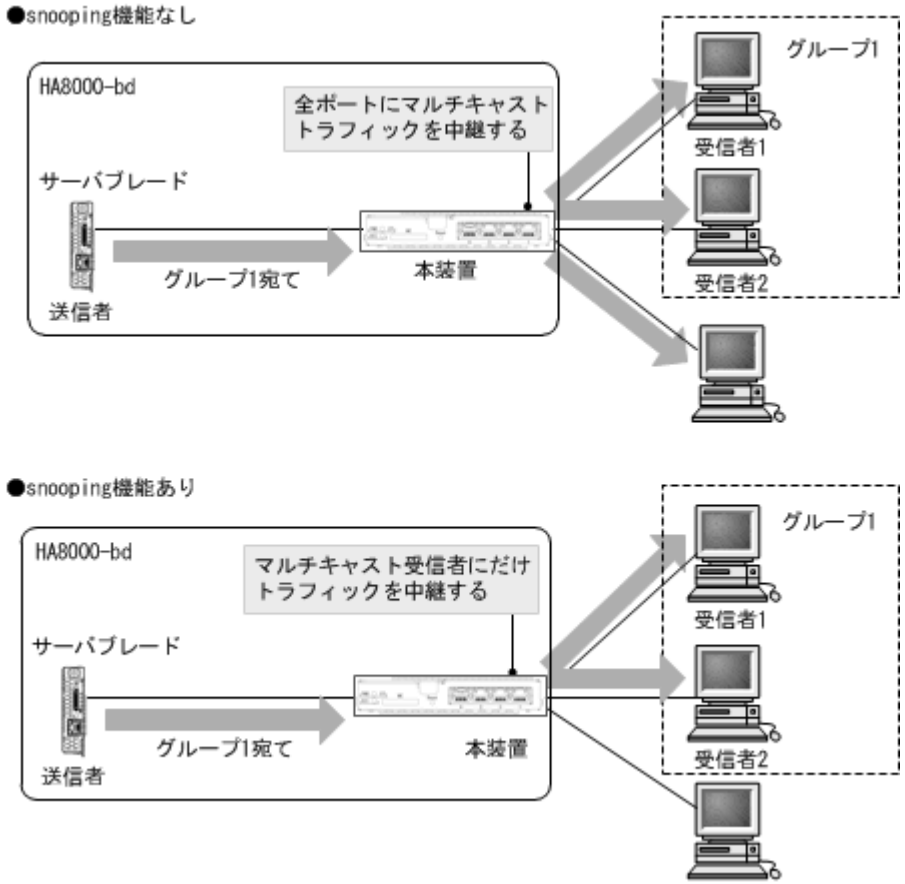
プロトコル	アドレス範囲
IPv4	224.0.0.0 ～ 239.255.255.255
IPv6	上位 8 ビットが ff(16 進数）となる IPv6 アドレス

22.1.2　IGMP snooping および MLD snooping 概要

レイヤ 2 スイッチはマルチキャストトラフィックを VLAN 内の全ポートに中継します。そのため，レイヤ 2 スイッチが接続されているネットワークでマルチキャストを使用すると，マルチキャストトラフィックの受信者がいないポートに不要なマルチキャストトラフィックが流れることになります。

IGMP snooping および MLD snooping は，IGMP あるいは MLD メッセージを監視して，受信者が接続しているポートに対してマルチキャストトラフィックを中継します。この機能を利用することで，不要なマルチキャストトラフィックの中継を抑止し，ネットワークを効率的に利用することができます。IGMP snooping/MLD snooping 概要を次の図に示します。

図 22-2　IGMP snooping/MLD snooping 概要



マルチキャストトラフィックの受信者が接続するポートを検出するため，本装置はグループ管理プロトコルのパケットを監視します。グループ管理プロトコルは，ルータホスト間でグループメンバーシップ情報を送受信するプロトコルで，IPv4 ネットワークでは IGMP が使用され，IPv6 ネットワークでは MLD が使用されます。ホストから送信されるグループ参加・離脱報告を示すパケットを検出することで，どの接続ポートへマルチキャストトラフィックを中継すべきかを学習します。

22.2 IGMP snooping/MLD snooping サポート機能

本装置がサポートする IGMP snooping/MLD snooping 機能を次の表に示します。

表 22-2 サポート機能

項 目		サポート内容	備考
インタフェース種別		全イーサネットをサポート フレーム形式は Ethernet V2 だけ	－
IGMP サポートバージョン MLD サポートバージョン		IGMP: Version 1，2，3 MLD: Version 1，2	－
この機能による学習 MAC アドレス範囲	IPv4	0100.5e00.0000 ～ 0100.5e7f.ffff	RFC1112 を参照
	IPv6	3333.0000.0000 ～ 3333.ffff.ffff	RFC2464 を参照
IGMP クエリア MLD クエリア		クエリア動作は，IGMPv2/IGMPv3，MLDv1/MLDv2 の仕様に従う	－
マルチキャストルータ接続ポートの設定		コンフィグレーションによる static 設定	－
IGMP 即時離脱機能		IGMP Leave メッセージ，またはマルチキャストアドレスレコードタイプが CHANGE_TO_INCLUDE_MODE の IGMPv3 Report（離脱要求）メッセージの受信による即時離脱	－

（凡例） －：該当なし

22.3　IGMP snooping

ここでは，IGMP snooping の機能と動作について説明します。本装置が送受信する IGMP メッセージのフォーマットおよびタイマは RFC2236 に従います。また，IGMP バージョン 3（以降，IGMPv3）メッセージのフォーマットおよび設定値は RFC3376 に従います。

IGMP snooping は MAC アドレス制御方式でマルチキャストトラフィックの中継制御を行います。

22.3.1　MAC アドレス制御方式

（1） MAC アドレスの学習

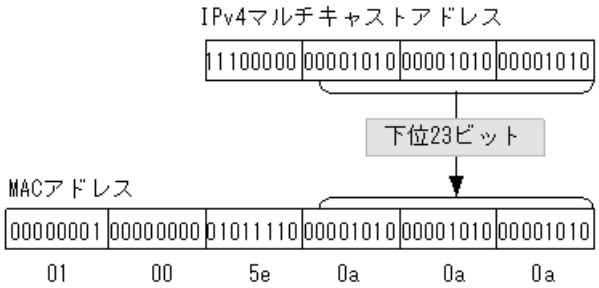
IGMP snooping が設定された VLAN で IGMP メッセージを受信することによってマルチキャスト MAC アドレスをダイナミックに学習します。学習したマルチキャスト MAC アドレスは MAC アドレステーブルに登録します。

（a） エントリの登録

IGMPv1/IGMPv2 Report メッセージおよび，IGMPv3 Report（加入要求）メッセージを受信すると，メッセージに含まれるマルチキャストグループアドレスからマルチキャスト MAC アドレスを学習し，IGMPv1/IGMPv2/IGMPv3 Report メッセージを受信したポートにだけマルチキャストグループ宛てのトラフィックを転送するエントリを作成します。

IPv4 マルチキャストデータの宛先 MAC アドレスは IP アドレスの下位 23 ビットを MAC アドレスにコピーして生成します。そのため，下位 23 ビットが同じ IP アドレスは MAC アドレスが重複します。例えば，224.10.10.10 と 225.10.10.10 はどちらもマルチキャスト MAC アドレスは 0100.5E0A.0A0A となります。これらのアドレスについては，レイヤ 2 中継で同一 MAC アドレス宛のパケットとして取り扱います。IPv4 マルチキャストアドレスと MAC アドレスの対応を次の図に示します。

図 22-3　IPv4 マルチキャストアドレスと MAC アドレスの対応



（b） エントリの削除

学習したマルチキャスト MAC アドレスは次のいずれかの場合に，すべてのポートにグループメンバーが存在しなくなった時点で削除されます。

- IGMP Leave メッセージを受信した場合
  IGMP Leave メッセージを受信したポートに対して，本装置から Group-Specific Query メッセージを１秒間隔で 2 回送信します（Group-Specific Query メッセージの送信は，クエリア設定時だけです。未設定時は代表クエリアから送信されます）。応答がない場合にエントリからこのポートだけを削除します（このポートへのマルチキャストトラフィックの中継を抑止します）。VLAN 内のすべてのポートにグループメンバーが存在しなくなった場合にエントリ自体を削除します。

IGMP 即時離脱機能を使用している場合は，IGMP Leave メッセージを受信すると，エントリから該当ポートをすぐに削除します。クエリアを設定していても，Group-Specific Query メッセージは送信しません。

- IGMPv3 Report（離脱要求）メッセージを受信した場合
  IGMPv3 Report（離脱要求）メッセージを受信したポートに対して，本装置から Group-Specific Query メッセージを 1 秒間隔で 2 回送信します（Group-Specific Query メッセージの送信は，クエリア設定時だけです。未設定時は代表クエリアから送信されます)。応答がない場合にエントリからこのポートだけを削除します（このポートへのマルチキャストトラフィックの中継を抑止します)。VLAN 内のすべてのポートにグループメンバーが存在しなくなった場合にエントリ自体を削除します。
  ただし，マルチキャストアドレスレコードタイプが BLOCK_OLD_SOURCES の IGMPv3 Report メッセージを受信した場合は，自装置へのクエリア設定を行っている場合だけ Group-Specific Query メッセージの送信および，エントリ削除処理を実行します。
  IGMP 即時離脱機能を使用している場合は，マルチキャストアドレスレコードタイプが CHANGE_TO_INCLUDE_MODE の IGMPv3 Report（離脱要求）メッセージを受信すると，エントリから該当ポートをすぐに削除します。クエリアを設定していても，Group-Specific Query メッセージは送信しません。
- IGMPv1/IGMPv2/IGMPv3 Report（加入要求）メッセージを受信してから一定時間経過した場合
  マルチキャストルータは直接接続するインタフェース上にグループメンバーが存在するかを確認するため，定期的に Query メッセージを送信します。本装置はルータからの IGMP Query メッセージを受信した場合，VLAN 内の全ポートに中継します。IGMP Query メッセージに対する応答がない場合，エントリからこのポートだけを削除します。すべてのポートから応答がない場合は，エントリ自体を削除します。
  本装置では 260 秒間 IGMPv1/IGMPv2/IGMPv3 Report（加入要求）メッセージを受信しない場合，対応するエントリを削除します。
  IGMPv3 で運用している VLAN で他装置が代表クエリアの場合，タイムアウト時間は代表クエリアからの IGMPv3 Query メッセージ（QQIC フィールド）から算出します。自装置が代表クエリアの場合または IGMPv2 で運用している場合は，125 秒となります。この場合，該当する VLAN では Query Interval を 125 秒で運用してください。

  注
  タイムアウト時間は，Query Interval（QQIC フィールドの値）× 2+Query Response Interval で算出します。

（2） IPv4 マルチキャストパケットのレイヤ 2 中継

IPv4 マルチキャストパケットの受信 VLAN 内のレイヤ 2 中継は MAC アドレスベースで処理します。IGMP snooping の結果によってレイヤ 2 中継は，同一 MAC アドレスにマッピングされる IP マルチキャストアドレスの IGMP Report（加入要求）メッセージを受信したポートすべてに中継します。

「(1) MAC アドレスの学習 (a) エントリの登録」の例で述べた 224.10.10.10 と 225.10.10.10 のマルチキャスト MAC アドレスはどちらも 0100.5E0A.0A0A となるので，224.10.10.10 宛のマルチキャストデータをレイヤ 2 中継する際に，225.10.10.10 への IGMP Report（加入要求）メッセージを受信したポートへも中継します。

22.3.2 マルチキャストルータとの接続

マルチキャストパケットの中継先にはグループ加入済みホストだけでなく隣接するマルチキャストルータも対象とします。本装置とマルチキャストルータを接続して IGMP snooping を使用する場合，マルチキャストルータへマルチキャストパケットを中継するためにマルチキャストルータと接続するポート（以

降，マルチキャストルータポートとします）をコンフィグレーションで指定します。

本装置は指定したマルチキャストルータポートへは全マルチキャストパケットを中継します。

また，IGMP はルータホスト間で送受信するプロトコルであるため，IGMP メッセージはルータおよびホストが受け取ります。本装置は IGMP メッセージを次の表に示すように中継します。

表 22-3　IGMPv1/IGMPv2 メッセージごとの動作

IGMP メッセージの種類	VLAN 内転送ポート	備考
Membership Query	全ポートへ中継します。	
Version 2 Membership Report	マルチキャストルータポートにだけ中継します。	
Leave Group	ほかのポートにまだグループメンバーが存在する場合はどのポートにも中継しません。 ほかのポートにグループメンバーが存在しない場合はマルチキャストルータポートに中継します。	※
Version 1 Membership Report	マルチキャストルータポートにだけ中継します。	

注※

自装置にクエリアを設定している場合の中継動作です。クエリアを設定していない場合は，常にマルチキャストルータポートに中継します。ただし，IGMPv1/IGMPv2/IGMPv3 Report（加入要求）メッセージを受信していないポートで IGMP Leave メッセージを受信した場合，クエリアの設定にかかわらず IGMP Leave メッセージは中継しません。

表 22-4　IGMPv3 メッセージごとの動作

IGMPv3 メッセージの種類		VLAN 内転送ポート	備考
Version3 Membership Query		全ポートへ中継します。	
Version 3 Membership Report	加入要求の Report	マルチキャストルータポートにだけ中継します。	
	離脱要求の Report	ほかのポートにまだグループメンバーが存在する場合はどのポートにも中継しません。ほかのポートにグループメンバーが存在しない場合はマルチキャストルータポートに中継します。	※

注※

自装置にクエリアを設定している場合の中継動作です。クエリアを設定していない場合は，常にマルチキャストルータポートに中継します。ただし，IGMPv1/IGMPv2/IGMPv3 Report（加入要求）メッセージを受信していないポートで離脱要求の IGMPv3 Report メッセージを受信した場合，クエリアの設定にかかわらず IGMPv3 Report（離脱要求）メッセージは中継しません。

22.3.3　IGMP クエリア機能

IGMP クエリア機能は，VLAN 内にマルチキャストルータが存在せず，マルチキャストパケットの送信ホストと受信ホストだけが存在する環境で，本装置が IGMP Query メッセージを代理で受信ホストに対して送信する機能です。マルチキャストルータは定期的に IGMP Query メッセージを送信し，ホストからの応答を受け取ることでグループメンバーの存在有無を確認します。マルチキャストルータが存在しない場合，受信ホストからの応答がなくなるためにグループメンバーを監視することができなくなります。この機能によって，VLAN 内にマルチキャストルータが存在しない場合でも，IGMP snooping 機能を使用可能とします。本装置では IGMP Query メッセージを 125 秒間隔で送信します。

IGMP クエリア機能を利用するためには，IGMP snooping 機能を利用する VLAN に IP アドレスを設定する必要があります。

VLAN 内に IGMP Query メッセージを送信する装置が存在する場合，IGMP Query メッセージの送信元 IP アドレスの小さい方が代表クエリアとなって IGMP Query メッセージを送信します。VLAN 内のほかの装置が代表クエリアの場合，本装置は IGMP クエリア機能による Query メッセージの送信を停止します。

代表クエリアが障害などで停止すると新たに代表クエリアを選定します。VLAN 内の他装置が障害などで本装置が代表クエリアに決定すると Query メッセージの送信を開始します。本装置では代表クエリアの監視時間を 255 秒としています。

本装置で送信する IGMP Query のバージョンは，IGMPv2 をデフォルト値としています。装置起動以降，IGMP Query のバージョンは，代表クエリアの IGMP バージョンに従います。

22.3.4 IGMP 即時離脱機能

IGMP 即時離脱機能は，IGMP Leave および IGMPv3 Report（離脱要求）メッセージを受信した場合に，該当ポートへのマルチキャスト通信をすぐに停止する機能です。

IGMPv3 Report（離脱要求）メッセージでは，マルチキャストアドレスレコードタイプが CHANGE_TO_INCLUDE_MODE の IGMPv3 Report（離脱要求）メッセージだけを，本機能のサポート対象とします。

22.4　MLD snooping

ここでは，MLD snooping の機能と動作について説明します。本装置が送受信する MLD メッセージのフォーマットおよび既定値は RFC2710 に従います。また，MLD バージョン 2（以降，MLDv2）メッセージのフォーマットおよび設定値は RFC3810 に従います。

MLD snooping は MAC アドレス制御方式でマルチキャストトラフィックの中継制御を行います。

22.4.1　MAC アドレス制御方式

（1） MAC アドレスの学習

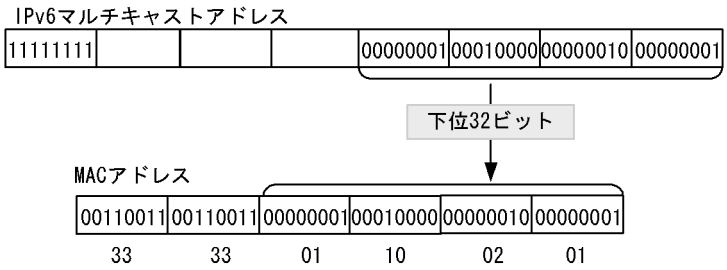
MLD snooping が設定された VLAN で MLD メッセージを受信することによってマルチキャスト MAC アドレスをダイナミックに学習します。学習したマルチキャスト MAC アドレスは MAC アドレステーブルに登録します。

（a） エントリの登録

MLDv1 Report メッセージおよび，MLDv2 Report（加入要求）メッセージを受信すると，メッセージに含まれるマルチキャストグループアドレスからマルチキャスト MAC アドレスを学習し，MLDv1/MLDv2 Report メッセージを受信したポートにだけマルチキャストグループ宛のトラフィックを転送するエントリを作成します。IPv6 マルチキャストデータの宛先 MAC アドレスは IP アドレスの下位 32 ビットを MAC アドレスにコピーして生成します。

IPv6 マルチキャストアドレスはマルチキャストグループを識別するグループ ID フィールドが 112 ビット長のフォーマットと 32 ビット長のフォーマットの 2 種類が規定されています。グループ ID フィールドが 112 ビット長のアドレスフォーマットを使用する場合は，IPv4 マルチキャストアドレスと同様に MAC アドレスの重複が発生します。IPv6 マルチキャストアドレスと MAC アドレスの対応を次の図に示します。

図 22-4　IPv6 マルチキャストアドレスと MAC アドレスの対応



（b） エントリの削除

学習したマルチキャスト MAC アドレスは次のどちらかの場合に，すべてのポートにグループメンバーが存在しなくなった時点で削除されます。

- MLDv1 Done メッセージを受信した場合
  MLDv1 Done メッセージを受信したポートに対して，本装置から Group-Specific Query メッセージを 1 秒間隔で 2 回送信します（Group-Specific Query メッセージの送信は，クエリア設定時だけです。未設定時は代表クエリアから送信されます）。応答がない場合にエントリからこのポートだけを削除します（このポートへのマルチキャストトラフィックの中継を抑止します）。VLAN 内のすべてのポートにグループメンバーが存在しなくなった場合にエントリ自体を削除します。

- MLDv2 Report（離脱要求）メッセージを受信した場合
  MLDv2 Report（離脱要求）メッセージを受信したポートに対して，本装置から Group-Specific Query メッセージを 1 秒間隔で 2 回送信します（Group-Specific Query メッセージの送信は，クエリア設定時だけです。未設定時は代表クエリアから送信されます）。応答がない場合にエントリからこのポートだけを削除します（このポートへのマルチキャストトラフィックの中継を抑止します）。VLAN 内のすべてのポートにグループメンバーが存在しなくなった場合にエントリ自体を削除します。ただし，マルチキャストアドレスレコードタイプが BLOCK_OLD_SOURCES の MLDv2 Report を受信した場合は，自装置へのクエリア設定を行っている場合だけ Group-Specific Query メッセージの送信および，エントリ削除処理を実行します。
- MLDv1/MLDv2 Report（加入要求）メッセージを受信してから一定時間経過した場合
  マルチキャストルータは直接接続するインタフェース上にグループメンバーが存在するかを確認するために，定期的に MLD Query メッセージを送信します。本装置はルータからの MLD Query メッセージを受信した場合，VLAN 内の全ポートに中継します。MLD Query メッセージに対する応答がない場合，エントリからこのポートだけを削除します。すべてのポートから応答がない場合は，エントリ自体を削除します。
  本装置ではエントリを削除するタイムアウト時間を 260 秒（デフォルト値）としています。260 秒間 MLDv1/MLDv2 Report（加入要求）メッセージを受信しない場合に対応するエントリを削除します。

（2） IPv6 マルチキャストパケットのレイヤ 2 中継

IPv6 マルチキャストパケットの受信 VLAN 内のレイヤ 2 中継は IPv4 マルチキャストパケット同様に MAC アドレスベースで処理します。MLD snooping の結果によるレイヤ 2 中継は，同一 MAC アドレスにマッピングされる IPv6 マルチキャストアドレスの MLD Report（加入要求）メッセージを受信したポートすべてに中継します。

22.4.2 マルチキャストルータとの接続

マルチキャストパケットの中継先にはグループ加入済みホストだけでなく隣接するマルチキャストルータも対象とします。本装置とマルチキャストルータを接続して MLD snooping を使用する場合，マルチキャストルータへマルチキャストパケットを中継するためにマルチキャストルータと接続するポート（以降，マルチキャストルータポートとします）をコンフィグレーションで指定します。

本装置は指定したマルチキャストルータポートへは全マルチキャストパケットを中継します。

また，MLD はルータホスト間で送受信するプロトコルであるため，MLD メッセージはルータおよびホストが受け取ります。本装置では MLD メッセージを次の表に示すように中継します。

表 22-5 MLDv1 メッセージごとの動作

MLDv1 メッセージの種類	VLAN 内転送ポート	備考
Multicast Listener Query	全ポートへ中継します。	
Multicast Listener Report	マルチキャストルータポートにだけ中継します。	
Multicast Listener Done	ほかのポートにまだグループメンバーが存在する場合はどのポートにも中継しません。 ほかのポートにグループメンバーが存在しない場合はマルチキャストルータポートに中継します。	※

注※

自装置にクエリアを設定している場合の中継動作です。クエリアを設定していない場合は，常にマルチキャストルータポートに中継します。ただし，MLDv1/MLDv2 Report（加入要求）メッセージを受信していないポートでMLDv1 Done メッセージを受信した場合，クエリアの設定にかかわらず MLDv1 Done メッセージは中継しません。

表 22-6　MLDv2 メッセージごとの動作

MLDv2 メッセージの種類		VLAN 内転送ポート	備考
Version2 Multicast Listener Query		全ポートへ中継します。	
Version2 Multicast Listener Report	加入要求の Report	マルチキャストルータポートにだけ中継します。	
	離脱要求の Report	ほかのポートにまだグループメンバーが存在する場合はどのポートにも中継しません。ほかのポートにグループメンバーが存在しない場合はマルチキャストルータポートに中継します。	※

注※

自装置にクエリアを設定している場合の中継動作です。クエリアを設定していない場合は，常にマルチキャストルータポートに中継します。ただし，MLDv1/MLDv2 Report（加入要求）メッセージを受信していないポートで離脱要求の MLDv2 Report メッセージを受信した場合，クエリアの設定にかかわらず MLDv2 Report（離脱要求）メッセージは中継しません。

22.4.3　MLD クエリア機能

MLD クエリア機能とは，VLAN 内にマルチキャストルータが存在せず，マルチキャストパケットの送信ホストと受信ホストだけが存在する環境で，本装置が MLD Query メッセージを代理で受信ホストに対して送信する機能です。マルチキャストルータは定期的に MLD Query メッセージを送信し，ホストからの応答を受け取ることでグループメンバーの存在有無を確認します。マルチキャストルータが存在しない場合，受信ホストからの応答がなくなるためにグループメンバーを監視することができなくなります。この機能によって，VLAN 内にマルチキャストルータが存在しない場合でも，MLD snooping 機能を使用可能とします。本装置では Query メッセージを 125 秒間隔で送信します。

MLD クエリア機能を利用するためには，MLD snooping 機能を利用する VLAN に MLD Query メッセージの送信元 IP アドレスを設定する必要があります。

VLAN 内に MLD Query メッセージを送信する装置が存在する場合，MLD Query メッセージの送信元 IP アドレスの小さい方が代表クエリアとなって MLD Query メッセージを送信します。VLAN 内のほかの装置が代表クエリアの場合，本装置は MLD クエリア機能による MLD Query メッセージの送信を停止します。

代表クエリアが障害などで停止すると新たに代表クエリアを選定します。VLAN 内の他装置が障害などで本装置が代表クエリアに決定すると MLD Query メッセージの送信を開始します。本装置では代表クエリアの監視時間を 255 秒としています。

本装置で送信する MLD Query のバージョンは，MLDv1 をデフォルト値としています。装置起動以降，MLD Query のバージョンは，代表クエリアの MLD バージョンに従います。

22.5　IGMP snooping/MLD snooping 使用時の注意事項

（1） 他機能との共存

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

（2） 制御パケットのフラッディング

IGMP snooping/MLD snooping が抑止対象とするマルチキャストトラフィックはデータトラフィックであり，ルーティングプロトコルなどの制御パケットは VLAN 内の全ルータや全ホストが受信できるように VLAN 内に flooding する必要があります。そのため，本装置では，次の表に示すアドレス範囲に含まれる宛先 IP アドレスを持つパケットは，VLAN 内の全ポートに中継します。次の表に示すアドレス範囲外の宛先 IP アドレスを持つパケットは，マルチキャスト MAC アドレスの学習結果に従って中継します。

表 22-7　制御パケットのフラッディング

プロトコル	アドレス範囲
IGMP snooping	224.0.0.0 ～ 224.0.0.255
MLD snooping	ff02::/16

ただし，制御パケットのマルチキャスト MAC アドレスと重複するマルチキャストグループアドレスは使用できません。上の表に示したアドレス範囲以外のアドレスで，使用できないマルチキャストグループアドレスを次の表に示します。

表 22-8　MAC アドレス制御方式で使用できないマルチキャストグループアドレス

プロトコル	マルチキャストグループアドレス
IGMP snooping	224.128.0.0/24
	225.0.0.0/24
	225.128.0.0/24
	226.0.0.0/24
	226.128.0.0/24
	227.0.0.0/24
	227.128.0.0/24
	228.0.0.0/24
	228.128.0.0/24
	229.0.0.0/24
	229.128.0.0/24
	230.0.0.0/24
	230.128.0.0/24
	231.0.0.0/24
	231.128.0.0/24
	232.0.0.0/24
	232.128.0.0/24
	233.0.0.0/24
	233.128.0.0/24

プロトコル	マルチキャストグループアドレス
	234.0.0.0/24
	234.128.0.0/24
	235.0.0.0/24
	235.128.0.0/24
	236.0.0.0/24
	236.128.0.0/24
	237.0.0.0/24
	237.128.0.0/24
	238.0.0.0/24
	238.128.0.0/24
	239.0.0.0/24
	239.128.0.0/24

上の表に示したアドレスをマルチキャストグループアドレスに使用した場合，該当マルチキャストグループアドレス宛てのマルチキャストデータは，VLAN 内の全ポートに中継します。

トランクポートを設定している場合は，Untagged 制御パケットを受信しないように注意してください。構成上，トランクポートで Untagged 制御パケットを扱う場合は，ネイティブ VLAN を設定してください。

(3) マルチキャストルータポートの設定

(a) 冗長構成時

スパニングツリーによって冗長構成を採り，スパニングツリーによってトポロジー変更でルータとの接続が変わる可能性がある場合は，ルータと接続する可能性のある全ポートに対してマルチキャストルータポートの設定をしておく必要があります。

(b) レイヤ 2 スイッチ間の接続時

複数のレイヤ 2 スイッチだけで構成される VLAN で，マルチキャストトラフィックの送信ホストを収容するレイヤ 2 スイッチと接続するポートをマルチキャストルータポートに設定しておく必要があります。また，このような構成の場合，各レイヤ 2 スイッチで IGMP/MLD snooping 機能を有効にしてください(snooping 対応のスイッチと接続してください)。

冗長構成を採る場合は，送信ホストを収容するレイヤ 2 スイッチと接続する可能性のある全ポートに対してマルチキャストルータポートの設定をしておく必要があります。

(4) IGMP バージョン 3 ホストとの接続

本装置に IGMPv3 ホストを接続する場合，次の対応が必要です。

- IGMPv3 ルータを接続して該当するルータが代表クエリアになるように IP アドレスを設定してください。

また，IGMPv3 ホストからの IGMPv3 メッセージがフラグメント化されない構成で運用してください。

(5) MLD バージョン 2 ホストとの接続

本装置に MLDv2 ホストを接続する場合，必ず MLDv2 ルータを接続して該当するルータが代表クエリア

になるように IP アドレスを設定してください。代表クエリアが MLDv1 ルータの場合，ネットワークが MLDv1 モードになります。

また，MLDv2 ホストからの MLDv2 メッセージがフラグメント化されない構成で運用してください。

（6） IGMP 即時離脱機能

IGMP 即時離脱機能を使用した場合，IGMP Leave および IGMPv3 Report（離脱要求）メッセージを受信すると，該当ポートへのマルチキャスト通信をすぐに停止します。このため，本機能を使用する場合は，接続ポートに各マルチキャストグループの受信者の端末を 1 台だけ設置することを推奨します。

接続ポートに同一マルチキャストグループの受信者の端末を複数台設置した場合は，一時的にほかの受信者へのマルチキャスト通信が停止します。この場合，受信者からの IGMP Report（加入要求）メッセージを再度受信することで，マルチキャスト通信は再開します。

23 IGMP snooping/MLD snooping の設定と運用

IGMP snooping/MLD snooping はレイヤ 2 で VLAN 内のマルチキャストトラフィックを制御する機能です。この章では，IGMP snooping/MLD snooping の設定と運用方法について説明します。

23.1　IGMP snooping のコンフィグレーション

23.1.1　コンフィグレーションコマンド一覧

IGMP snooping のコンフィグレーションコマンド一覧を次の表に示します。

表 23-1　コンフィグレーションコマンド一覧

コマンド名	説明
ip igmp snooping (global)	no ip igmp snooping 設定時，本装置の IGMP snooping 機能を抑止します。
ip igmp snooping (interface)	指定したインタフェースの IGMP snooping 機能を設定します。
ip igmp snooping fast-leave	IGMP 即時離脱機能を設定します。
ip igmp snooping mrouter	IGMP マルチキャストルータポートを設定します。
ip igmp snooping querier	IGMP クエリア機能を設定します。

23.1.2　IGMP snooping の設定

［設定のポイント］

IGMP snooping を動作させるには，使用する VLAN の VLAN インタフェースコンフィグレーションモードで，次の設定を行います。

VLAN2 に IGMP snooping 機能を有効にする場合を示します。

［コマンドによる設定］

1. **(config)# interface vlan 2**
   (config-if)# ip igmp snooping
   (config-if)# exit
   VLAN2 の VLAN インタフェースコンフィグレーションモードに移行して，IGMP snooping 機能を有効にします。

23.1.3　IGMP クエリア機能の設定

［設定のポイント］

IGMP snooping を設定した VLAN 内にマルチキャストルータが存在しない場合，IGMP クエリア機能を動作させる必要があります。該当 VLAN の VLAN インタフェースコンフィグレーションモードで次の設定を行います。

［コマンドによる設定］

1. **(config)# interface vlan 2**
   (config-if)# ip igmp snooping querier
   (config-if)# exit
   IGMP クエリア機能を有効にします。

［注意事項］

本設定は該当インタフェースに IPv4 アドレスの設定がないと有効になりません。

23.1.4　マルチキャストルータポートの設定

［設定のポイント］

IGMP snooping を設定した VLAN 内にマルチキャストルータを接続している場合，該当 VLAN の VLAN インタフェースコンフィグレーションモードで，次の設定を行います。例として，該当 VLAN 内のポート 0/4 のイーサネットインタフェースにマルチキャストルータを接続している場合を示します。

［コマンドによる設定］

1. **(config)# interface vlan 2**
   (config-if)# ip igmp snooping mrouter interface gigabitethernet 0/4
   (config-if)# exit
   該当インタフェースで，マルチキャストルータポートを指定します。

［注意事項］

ポートチャネルインタフェースに属するポート番号を，マルチキャストルータポートに設定しても動作しません。

23.2　IGMP snooping のオペレーション

23.2.1　運用コマンド一覧

IGMP snooping の運用コマンド一覧を次の表に示します。

表 23-2　運用コマンド一覧

コマンド名	説明
show igmp-snooping	IGMP snooping 情報を表示します。
clear igmp-snooping	IGMP snooping の全情報をクリアします。

23.2.2　IGMP snooping の確認

IGMP snooping 機能を使用した場合の IGMP snooping に関する確認内容には次のものがあります。

（1）コンフィグレーション設定後の確認

運用コマンド show igmp-snooping で，IGMP snooping に関する設定が正しいことを確認してください。

図 23-1　IGMP snooping の設定状態表示

```
> show igmp-snooping

Date 20XX/06/23 14:21:03 UTC
VLAN counts: 3
VLAN: 3253
  IP Address: 192.168.53.100      Querier: enable
  IGMP querying system: 192.168.53.100
  Querier version: V3
  Fast-leave: Off
  Port(4): 0/13-16
  Mrouter-port: 0/1-4
  Group counts: 3
VLAN: 3254
  IP Address: 192.168.54.100      Querier: disable
  IGMP querying system:
  Querier version: V2
  Fast-leave: Off
  Port(4): 0/17-20
  Mrouter-port: 0/17-20
  Group counts: 3
VLAN: 3255
  IP Address: 192.168.55.100      Querier: disable
  IGMP querying system:
  Querier version: V3
  Fast-leave: Off
  Port(4): 0/21-24
  Mrouter-port: 0/21-24
  Group counts: 3

>
```

（2）運用中の確認

次のコマンドで，IGMP snooping の運用中の状態を確認してください。

- 学習した MAC アドレス，VLAN 内に中継される IPv4 マルチキャストアドレスとその中継先ポートリストの状態は，運用コマンド show igmp-snooping group で確認してください。

図 23-2 show igmp-snooping group の実行結果

```
> show igmp-snooping group

Date 20XX/06/23 14:21:41 UTC
Total Groups: 9
VLAN counts: 3
VLAN 3253  Group counts: 3
  Group Address     MAC Address         Version      Mode
  230.0.0.11        0100.5e00.000b      V3           INCLUDE
    Port-list:0/1
  230.0.0.10        0100.5e00.000a      V2,V3        EXCLUDE
    Port-list:0/1
  230.0.0.12        0100.5e00.000c      V1,V2,V3     EXCLUDE
    Port-list:0/1
VLAN 3254  Group counts: 3
  Group Address     MAC Address         Version      Mode
  230.0.0.34        0100.5e00.0022      V1           -
    Port-list:0/17
  230.0.0.33        0100.5e00.0021      V2           -
    Port-list:0/17
  230.0.0.32        0100.5e00.0020      V3           EXCLUDE
    Port-list:0/17
VLAN 3255  Group counts: 3
  Group Address     MAC Address         Version      Mode
  230.0.0.24        0100.5e00.0018      V1,V2        -
    Port-list:0/21
  230.0.0.23        0100.5e00.0017      V1,V3        EXCLUDE
    Port-list:0/21
  230.0.0.22        0100.5e00.0016      V2,V3        EXCLUDE
    Port-list:0/21

>
```

● ポートごとの参加グループ表示例を運用コマンド show igmp-snooping port で確認してください。

図 23-3 show igmp-snooping port の実行結果

```
> show igmp-snooping port 0/1

Date 20XX/06/23 14:23:02 UTC
Port 0/1  VLAN counts: 1
  VLAN: 3253  Group counts: 3
    Group Address     Last Reporter      Uptime     Expires
    230.0.0.11        192.168.53.17      02:15      03:37
    230.0.0.10        192.168.53.16      02:15      03:37
    230.0.0.12        192.168.53.18      02:15      03:37

>
```

23.3　MLD snooping のコンフィグレーション

23.3.1　コンフィグレーションコマンド一覧

MLD snooping のコンフィグレーションコマンド一覧を次の表に示します。

表 23-3　コンフィグレーションコマンド一覧

コマンド名	説明
ipv6 mld snooping (global)	no ipv6 mld snooping 設定時，本装置の MLD snooping 機能を抑止します。
ipv6 mld snooping (interface)	指定したインタフェースの MLD snooping 機能を設定します。
ipv6 mld snooping mrouter	MLD マルチキャストルータポートを設定します。
ipv6 mld snooping querier	MLD クエリア機能を設定します。
ipv6 mld snooping source	本装置から送信される MLD Query メッセージの送信元 IP アドレスを設定します。

23.3.2　MLD snooping の設定

［設定のポイント］

MLD snooping を動作させるには，使用する VLAN の VLAN インタフェースのインタフェースコンフィグレーションモードで，次の設定を行います。例として，VLAN2 に MLD snooping 機能を有効にする場合を示します。

［コマンドによる設定］

1. **(config)# interface vlan 2**
   (config-if)# ipv6 mld snooping
   (config-if)# exit
   VLAN2 の VLAN インタフェースコンフィグレーションモードに移行して，MLD snooping 機能を有効にします。

23.3.3　MLD クエリア機能の設定

［設定のポイント］

MLD snooping を設定した VLAN 内にマルチキャストルータが存在しない場合，MLD クエリア機能を動作させる必要があります。該当 VLAN の VLAN インタフェースコンフィグレーションモードで，次の設定を行います。

［コマンドによる設定］

1. **(config)# interface vlan 2**
   (config-if)# ipv6 mld snooping querier
   (config-if)# exit
   MLD クエリア機能を有効にします。

［注意事項］

本設定は該当インタフェースに，MLD Query メッセージの送信元 IP アドレスの設定がないと有効になりません。

23.3.4　マルチキャストルータポートの設定

［設定のポイント］

MLD snooping を設定した VLAN 内にマルチキャストルータを接続している場合，該当 VLAN の VLAN インタフェースコンフィグレーションモードで，次の設定を行います。例として，該当 VLAN 内のポート 0/3 のイーサネットインタフェースにマルチキャストルータを接続している場合を示します。

［コマンドによる設定］

1. **(config)# interface vlan 2**
   (config-if)# ipv6 mld snooping mrouter interface gigabitethernet 0/4
   (config-if)# exit
   該当インタフェースでマルチキャストルータポートを指定します。

［注意事項］

ポートチャネルインタフェースに属するポート番号を，マルチキャストルータポートに設定しても動作しません。

23.3.5　MLD Query メッセージ送信元 IP アドレスの設定

［設定のポイント］

MLD クエリア機能を使用する際に，本装置から送信される Query メッセージの送信元 IP アドレスを指定する必要があります。MLD クエリア機能を使用する VLAN の VLAN インタフェースコンフィグレーションモードで，次の設定を行います。

［コマンドによる設定］

1. **(config)# interface vlan 2**
   (config-if)# ipv6 mld snooping source fe80::1
   (config-if)# exit
   該当インタフェースの MLD Query メッセージの送信元 IP アドレスを fe80::1 に指定します。

［注意事項］

1. MLD Query メッセージの送信元 IP アドレスにだけ適用されます。
2. 送信元アドレスは，IPv6 リンクローカルアドレスを設定してください。

23.4　MLD snooping のオペレーション

23.4.1　運用コマンド一覧

MLD snooping の運用コマンド一覧を次の表に示します。

表 23-4　運用コマンド一覧

コマンド名	説明
show mld-snooping	MLD snooping 情報を表示します。
clear mld-snooping	MLD snooping の全情報をクリアします。

23.4.2　MLD snooping の確認

MLD snooping 機能を使用した場合の MLD snooping に関する確認内容には次のものがあります。

（1）コンフィグレーション設定後の確認

運用コマンド show mld-snooping を実行し，MLD snooping に関する設定が正しいことを確認してください。

図 23-4　MLD snooping の設定状態表示

```
> show mld-snooping

Date 20XX/06/26 02:01:53 UTC
VLAN counts: 3
VLAN: 100
  IP Address: fe80::1  Querier: enable
  MLD querying system: fe80::1
  Querier version: V1
  Port(1): 0/1
  Mrouter-port:
  Group counts: 2
VLAN: 200
  IP Address: fe80::2  Querier: enable
  MLD querying system: fe80::2
  Querier version: V1
  Port(1): 0/3
  Mrouter-port:
  Group counts: 3
VLAN: 300
  IP Address: fe80::3  Querier: disable
  MLD querying system: fe80::10
  Querier version: V2
  Port(2): 0/11,0/22
  Mrouter-port: 0/11
  Group counts: 3

>
```

（2）運用中の確認

以下のコマンドで，MLD snooping の運用中の状態を確認してください。

● 学習した MAC アドレス，VLAN 内に中継される IPv6 マルチキャストアドレスとその中継先ポートリストの状態は，運用コマンド show mld-snooping group で確認してください。

図 23-5 show mld-snooping group の実行結果

```
> show mld-snooping group

Date 20XX/06/26 02:02:29 UTC
Total Groups: 8
VLAN counts: 3
VLAN 100  Group counts: 2
  Group Address                           MAC Address      Version   Mode
  ff03::10                                3333.0000.0010   V1        -
    Port-list: 0/1
  ff03::11                                3333.0000.0011   V1        -
    Port-list: 0/1
VLAN 200  Group counts: 3
  Group Address                           MAC Address      Version   Mode
  ff03::22                                3333.0000.0022   V1        -
    Port-list: 0/3
  ff03::21                                3333.0000.0021   V1        -
    Port-list: 0/3
  ff03::20                                3333.0000.0020   V1        -
    Port-list: 0/21
VLAN 300  Group counts: 3
  Group Address                           MAC Address      Version   Mode
  ff03::3                                 3333.0000.0003   V2        INCLUDE
    Port-list: 0/22
  ff03::2                                 3333.0000.0002   V2        INCLUDE
    Port-list: 0/22
  ff03::1                                 3333.0000.0001   V2        INCLUDE
    Port-list: 0/22

>
```

● ポートごとの参加グループ表示例を運用コマンド show mld-snooping port で確認してください。

図 23-6 show mld-snooping port の実行結果

```
> show mld-snooping port 0/22

Date 20XX/06/26 02:06:58 UTC
Port 0/22  VLAN counts: 1
  VLAN 300  Group counts: 3
    Group Address              Last Reporter              Uptime    Expires
    ff03::3                    fe80::10                   08:24     04:20
    ff03::2                    fe80::10                   08:24     04:20
    ff03::1                    fe80::10                   08:24     04:20

>
```

24 IPv4 インタフェース

この章では，IPv4 インタフェースの解説と操作方法について説明します。

24.1 解説

本装置は管理用として SNMP，Telnet，FTP 通信などを行うために，VLAN に IPv4 アドレスを設定することができます。また，その VLAN には同時に IPv6 アドレスを設定することもできます。ほかのサブネットに通信するには，スタティック経路を設定して，通信を行う必要があります。

本装置では VLAN インタフェースに設定した IPv4 アドレスの重複検出を行います。重複検出を有効にするコンフィグレーションはありません。VLAN インタフェースに IPv4 アドレスを設定することで，自動で重複検出が動作します。

(1) IP アドレスの重複検出

本装置の VLAN インタフェースに設定された，IP アドレスの重複チェックをおこないます。本装置から VLAN インタフェースごとに Gratuitous ARP を送信し，受信した ARP パケットの送信元 IP アドレスで重複をチェックします。

(a) 本装置から送信する Gratuitous ARP

本装置の VLAN インタフェースに設定された IP アドレスを Target Protocol Address フィールドにセットし，Gratuitous ARP を送信します。Gratuitous ARP の送信契機は，VLAN インタフェースがアップするごとに 1 パケットだけ送信します。

(b) 重複検出のチェック対象

重複検出のチェックは，Gratuitous ARP 応答に限らず，通常受信するすべての ARP パケット（下記条件）を対象とします。

- 宛先 MAC アドレスが，本装置の VLAN ユニキャスト，またはブロードキャストであること。
- 本装置のスパニングツリー，アクセスリスト，ダイナミック ARP 検査機能，認証機能などで廃棄されないこと。
- 受信する VLAN インタフェースに IP アドレスが設定されていること。

(c) 検出条件

IP アドレス重複とみなす条件は，下記をすべて満たしている場合です。

- ARP ペイロード中の送信元 MAC アドレスが，本装置のユニキャスト MAC アドレス（全 VLAN 共通）以外であること。
- 送信元 IP アドレスが，本装置に設定されている IP アドレスであること。

(d) 検出時の動作

IP アドレス重複を検出したときは，本装置は以下の情報を含む運用ログを出力します。

表 24-1 IP 重複検出時に出力する運用ログ情報

ログに含める情報	内容
VLAN ID	重複を検出した IP アドレスが設定されている VLAN インタフェース番号
IP アドレス	重複を検出した IP アドレス
MAC アドレス	重複した IP アドレスを持つ相手装置の MAC アドレス（ARP ペイロード中の送信元 MAC アドレス）

ただし，過去 10 分以内に同じ IP アドレスで運用ログを出力している場合は，運用ログを出力しません。

24.2　コンフィグレーション

24.2.1　コンフィグレーションコマンド一覧

IPv4 インタフェースのコンフィグレーションコマンド一覧を次の表に示します。

表 24-2　コンフィグレーションコマンド一覧

コマンド名	説明
arp	スタティック ARP テーブルを作成します。
ip address	インタフェースの IPv4 アドレスを指定します。
ip route	IPv4 のスタティック経路を指定します。

24.2.2　インタフェースの設定

［設定のポイント］

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

［コマンドによる設定］

1. **(config)# interface vlan 100**

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

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

   VLAN ID 100 に IPv4 アドレス 192.168.1.1，サブネットマスク 255.255.255.0 を設定します。

24.2.3　マルチホームの設定

［設定のポイント］

VLAN に複数の IPv4 アドレスを設定します。二つ以降の IPv4 アドレスには secondary パラメータを指定する必要があります。

［コマンドによる設定］

1. **(config)# interface vlan 100**

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

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

   VLAN ID 100 に IPv4 アドレス 192.168.1.1，サブネットマスク 255.255.255.0 を設定します。

3. **(config-if)# ip address 170.1.1.1 255.255.255.0 secondary**
   (config-if)# exit

   VLAN ID 100 にセカンダリ IPv4 アドレス 170.1.1.1，サブネットマスク 255.255.255.0 を設定します。

24.2.4 スタティック経路の設定

［設定のポイント］

本装置はルーティングプロトコル設定をサポートしません。VLAN の外部にあるサブネットと通信するには，スタティック経路を設定する必要があります。

［コマンドによる設定］

1. **(config)# ip route 192.168.2.0 255.255.255.0 192.168.1.254**
   宛先サブネット 192.168.2.0/24 の中継経路を 192.168.1.254 に指定します。

24.2.5 スタティック ARP の設定

［設定のポイント］

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

［コマンドによる設定］

1. **(config)# arp 123.10.1.1 interface vlan 100 0000.8740.0a00**
   VLAN ID 100 にネクストホップ IPv4 アドレス 123.10.1.1，接続先 MAC アドレス 0000.8740.0a00 でスタティック ARP を設定します。

24.3　オペレーション

24.3.1　運用コマンド一覧

IPv4 インタフェースの運用コマンド一覧を次の表に示します。

表 24-3　運用コマンド一覧

コマンド名	説明
show ip-dual interface	IPv4 および IPv6 インタフェースの状態を表示します。
show ip interface	IPv4 インタフェースの状態を表示します。
show ip arp	ARP エントリ情報を表示します。
clear arp-cache	ダイナミック ARP 情報を削除します。
show ip route	ルートテーブルを表示します。
ping	ping コマンドは，目的の IP アドレスを持つ装置に対して通信可能であるかどうかを判定するために使用します。
traceroute	宛先ホストまで ICMP メッセージが通ったルート（通ったゲートウェイのルートとゲートウェイ間の応答時間）を表示します。

24.3.2　IPv4 インタフェースの Up/Down 確認

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

図 24-1 「IPv4 インタフェース状態」の表示例

```
>show ip interface summary

Date 20XX/06/03 13:49:51 UTC
VLAN0001: Up  192.168.0.100/24
              192.168.1.100/24
              192.168.2.100/24
VLAN0010: Down  192.168.10.100/24
VLAN3005: Up  192.168.5.10/24
              192.168.6.10/24
VLAN3253: Down  192.168.53.100/24
VLAN3254: Up  192.168.54.100/24
VLAN3255: Up  192.168.55.100/24
VLAN3256: Down  192.168.56.100/24
VLAN4094: Up  192.168.4.10/24

>
```

24.3.3　宛先アドレスとの通信可否の確認

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

図 24-2 ping の実行結果（通信可の場合）

```
> ping 192.168.100.2
PING 192.168.100.2 (192.168.100.2): 56 data bytes
64 bytes from 192.168.100.2: icmp_seq=0 ttl=128 time=17 ms
64 bytes from 192.168.100.2: icmp_seq=1 ttl=128 time=0 ms
64 bytes from 192.168.100.2: icmp_seq=2 ttl=128 time=0 ms
64 bytes from 192.168.100.2: icmp_seq=3 ttl=128 time=0 ms
64 bytes from 192.168.100.2: icmp_seq=4 ttl=128 time=0 ms
64 bytes from 192.168.100.2: icmp_seq=5 ttl=128 time=0 ms
64 bytes from 192.168.100.2: icmp_seq=6 ttl=128 time=0 ms
64 bytes from 192.168.100.2: icmp_seq=7 ttl=128 time=0 ms
64 bytes from 192.168.100.2: icmp_seq=8 ttl=128 time=0 ms
64 bytes from 192.168.100.2: icmp_seq=9 ttl=128 time=0 ms
64 bytes from 192.168.100.2: icmp_seq=10 ttl=128 time=0 ms
^C
----192.168.100.2 PING Statistics----
11 packets transmitted, 11 packets received, 0.0% packet loss
round-trip min/avg/max = 0/2/17 ms
>
```

図 24-3 ping の実行結果（通信不可の場合）

```
> ping 192.168.254.254
PING 192.168.254.254 (192.168.254.254): 56 data bytes
92 bytes from 192.168.100.253: Destination Host Unreachable (icmp_seq=0)
92 bytes from 192.168.100.253: Destination Host Unreachable (icmp_seq=1)
92 bytes from 192.168.100.253: Destination Host Unreachable (icmp_seq=2)
92 bytes from 192.168.100.253: Destination Host Unreachable (icmp_seq=3)
92 bytes from 192.168.100.253: Destination Host Unreachable (icmp_seq=4)
92 bytes from 192.168.100.253: Destination Host Unreachable (icmp_seq=5)
92 bytes from 192.168.100.253: Destination Host Unreachable (icmp_seq=6)
92 bytes from 192.168.100.253: Destination Host Unreachable (icmp_seq=7)
92 bytes from 192.168.100.253: Destination Host Unreachable (icmp_seq=8)
92 bytes from 192.168.100.253: Destination Host Unreachable (icmp_seq=9)
92 bytes from 192.168.100.253: Destination Host Unreachable (icmp_seq=10)
^C
----192.168.254.254 PING Statistics----
14 packets transmitted, 0 packets received, 100.0% packet loss
>
```

24.3.4 宛先アドレスまでの経路確認

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

図 24-4 traceroute の実行結果

```
> traceroute 192.168.30.1 waittime 1 ttl 2
traceroute to 192.168.30.1 (192.168.30.1), 2 hops max, 8 byte packets
 1  192.168.30.1 (192.168.30.1)  0 ms  0 ms  0 ms
>
```

24.3.5 ARP 情報の確認

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

図 24-5　show ip arp の実行結果

```
> show ip arp

Date 20XX/06/03 12:16:02 UTC
Total: 9
IP Address      Linklayer Address  Interface  Expire     Type
10.0.0.6        00eb.f002.0001     VLAN2000   19min      arpa
10.10.10.3      incomplete         VLAN3333   --         arpa
192.168.254.53  0090.cc42.2dc4     VLAN4094   16min      arpa
192.168.254.77  000f.fefa.f721     VLAN4094   6min       arpa
192.168.254.98  001b.7888.1ffd     VLAN4094   19min      arpa
192.168.254.99  1cc1.de64.f234     VLAN4094   15min      arpa
192.168.254.102 00ce.a4bd.aad8     VLAN4094   Static     arpa
192.168.254.250 0000.8768.b663     VLAN4094   17min      arpa
192.168.254.252 0012.e282.680d     VLAN4094   2min       arpa

>
```

24.3.6　ルートテーブルの確認

IPv4 のルートテーブルを表示します。運用コマンド show ip route で，本装置と別サブネットの装置間のルート情報が設定されているかどうかを確認してください。

図 24-6　show ip route の実行結果

```
> show ip route

Date 20XX/06/10 17:32:39 UTC
Total: 5
Destination         Nexthop           Interface    Protocol
192.168.0.0/24      192.168.0.100     VLAN0001     Connected
192.168.4.0/24      192.168.4.10      VLAN4094     Connected
192.168.5.0/24      192.168.5.10      VLAN3005     Connected
192.168.54.0/24     192.168.54.100    VLAN3254     Connected
192.168.55.0/24     192.168.55.100    VLAN3255     Connected

>
```

25 IPv6 インタフェース

この章では，IPv6 インタフェースの解説と操作方法について説明します。

25.1　解説

本装置は管理用として SNMP，Telnet，FTP 通信などを行うために，VLAN に IPv6 アドレスを設定することができます。また，その VLAN には同時に IPv4 アドレスを設定することもできます。ほかのサブネットに通信するには，デフォルト経路（ゲートウェイ）を設定して，通信を行う必要があります。

（1） RA 受信による IPv6 アドレスの自動生成

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

ルータはアドレスのプレフィックス部だけを一定間隔で配布し，受信した各端末は，端末固有のインタフェース ID 部と RA のプレフィックス情報からアドレスを生成します。こうした特徴によって，RA はサーバレスで端末数に依存しない簡便な Plug & Play を実現します。

本装置では，コンフィグレーションコマンド ipv6 nd accept-ra 設定時，RA 受信による IPv6 アドレスの自動生成が可能です。ルータからプレフィックス部を受信し，装置 MAC アドレスをインタフェース ID として付加した IPv6 グローバルアドレスを自動生成し，受信したインタフェースに設定します。同時に RA 送信元アドレス（=RA を送信したルータのインタフェースリンクローカルアドレス）をデフォルトゲートウェイとして設定します。このデフォルトゲートウェイは，コンフィグレーションコマンド ipv6 default-gateway の設定よりも優先して使用します。

RA で受信した情報が収容条件を超えた場合は，先に受信した情報を優先します。

25.2　コンフィグレーション

25.2.1　コンフィグレーションコマンド一覧

IPv6 インタフェースのコンフィグレーションコマンド一覧を次の表に示します。

表 25-1　コンフィグレーションコマンド一覧

コマンド名	説明
ipv6 address	IPv6 アドレスを設定します。
ipv6 default-gateway	IPv6 デフォルト経路を指定します。
ipv6 enable	インタフェースの IPv6 機能を有効にします。このコマンドによって，リンクローカルアドレスが自動生成されます。
ipv6 nd accept-ra	RA を受信して IPv6 アドレスやデフォルトゲートウェイを自動設定します。
ipv6 neighbor	スタティック NDP テーブルを作成します。

25.2.2　インタフェースの設定

［設定のポイント］

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

［コマンドによる設定］

1. **(config)# interface vlan 100**
   VLAN ID 100 のインタフェースコンフィグレーションモードに移行します。

2. **(config-if)# ipv6 enable**
   VLAN ID 100 に IPv6 アドレス使用可を設定します。

3. **(config-if)# ipv6 address 2001:100::1/64**
   VLAN ID 100 に IPv6 アドレス 2001:100::1，プレフィックス長 64 を設定します。

4. **(config-if)# ipv6 address 2001:200::1/64**
   (config-if)# exit
   VLAN ID 100 に IPv6 アドレス 2001:200::1，プレフィックス長 64 を追加します。

25.2.3　デフォルト経路の設定

［設定のポイント］

本装置はルーティングプロトコル設定をサポートしません。VLAN の外部にあるサブネットと通信するには，デフォルト経路を設定する必要があります。

［コマンドによる設定］

1. **(config)# ipv6 default-gateway interface vlan 100 fe80::100**
   IPv6 デフォルト経路の中継経路（ゲートウェイ）を fe80::100 に指定します。

25.2.4 スタティック NDP の設定

［設定のポイント］

本装置にスタティック NDP を設定します。

［コマンドによる設定］

1. **(config)# ipv6 neighbor 2001:100::2 interface vlan 100 0000.8740.0a00**
   VLAN ID 100 にネクストホップ IPv6 アドレス 2001:100::2，接続先 MAC アドレス 0000.8740.0a00 でスタティック NDP を設定します。

25.2.5 RA 受信による IPv6 アドレスの自動設定

［設定のポイント］

VLAN インタフェースで RA 受信により IPv6 アドレスを自動生成するよう設定します。
ルータからプレフィックス部を受信し，装置 MAC アドレスをインタフェース ID として付加した IPv6 グローバルアドレスを自動生成し，受信したインタフェースに設定します。
同時に RA 送信元アドレス（=RA を送信したルータのインタフェースリンクローカルアドレス）をデフォルトゲートウェイとして設定します。

［コマンドによる設定］

1. **(config)# interface vlan 200**
   VLAN ID 200 のインタフェースコンフィグレーションモードに移行します。

2. **(config-if)# ipv6 nd accept-ra**
   VLAN ID 200 で RA 受信により IPv6 アドレスを自動生成するよう設定します。

3. **(config-if)# ipv6 enable**
   (config-if)# exit
   VLAN ID 200 に IPv6 アドレス使用可を設定します。

［注意事項］

1. RA 受信で設定したデフォルトゲートウェイは，コンフィグレーションコマンド ipv6 default-gateway の設定よりも優先して使用します。
2. コンフィグレーションコマンド ip mtu 未設定の VLAN インタフェースでは，RA 受信による MTU 設定をサポートします。RA 受信は IPv6 の動作ですが，RA 受信による MTU の設定は IPv4 の動作にも影響します。
3. 本コマンドの設定は，コンフィグレーションコマンド ipv6 enable 未設定の状態で行ってください。

25.3　オペレーション

25.3.1　運用コマンド一覧

IPv6 インタフェースの運用コマンド一覧を次の表に示します。

表 25-2　運用コマンド一覧

コマンド名	説明
show ip-dual interface	IPv4 および IPv6 インタフェースの状態を表示します。
show ipv6 interface	IPv6 インタフェースの状態を表示します。
show ipv6 neighbors	NDP 情報を表示します。
clear ipv6 neighbors	ダイナミック NDP 情報をクリアします。
show ipv6 router-advertisement	RA 情報を表示します。
ping ipv6	ping ipv6 コマンドは，目的の IPv6 アドレスを持つ装置に対して通信可能であるかどうかを判定するために使用します。
traceroute ipv6	宛先ホストまで ICMPv6 メッセージが通ったルート（通ったゲートウェイのルートとゲートウェイ間の応答時間）を表示します。

25.3.2　IPv6 インタフェースの Up/Down 確認

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

図 25-1 「IPv6 インタフェース状態」の表示例

```
> show ipv6 interface summary

Date 20XX/06/03 14:33:50 UTC
VLAN0010: Up  2001::1:10/64
              fe80::2eb:f0ff:fe02:1%VLAN0010/64

>
```

25.3.3　宛先アドレスとの通信可否の確認

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

図 25-2　ping ipv6 の実行結果（通信可の場合）

```
> ping ipv6 3000::1
PING6(56=40+8+8 bytes) 3000::2 --> 3000::1
16 bytes from 3000::1, icmp_seq=0 hlim=64 time=17 ms
16 bytes from 3000::1, icmp_seq=1 hlim=64 time=17 ms
16 bytes from 3000::1, icmp_seq=2 hlim=64 time=17 ms
16 bytes from 3000::1, icmp_seq=3 hlim=64 time=0 ms
16 bytes from 3000::1, icmp_seq=4 hlim=64 time=17 ms
16 bytes from 3000::1, icmp_seq=5 hlim=64 time=0 ms
16 bytes from 3000::1, icmp_seq=6 hlim=64 time=17 ms
16 bytes from 3000::1, icmp_seq=7 hlim=64 time=0 ms
16 bytes from 3000::1, icmp_seq=8 hlim=64 time=17 ms
16 bytes from 3000::1, icmp_seq=9 hlim=64 time=0 ms
16 bytes from 3000::1, icmp_seq=10 hlim=64 time=0 ms
```

```
^C
--- 3000::1 ping6 statistics ---
11 packets transmitted, 11 packets received, 0.0% packet loss
round-trip min/avg/max = 0/9/17 ms
>
```

図 25-3　ping ipv6 の実行結果（通信不可の場合）

```
> ping ipv6 3000::1
PING6(56=40+8+8 bytes) 3000::2 --> 3000::1
^C
--- 3000::1 ping6 statistics ---
11 packets transmitted, 0 packets received, 100.0% packet loss
>
```

25.3.4　宛先アドレスまでの経路確認

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

図 25-4　traceroute ipv6 の実行結果

```
> traceroute ipv6 100::2 numeric
traceroute6 to 100::2 (100::2) from 3000::2, 30 hops max, 8 byte packets
 1  3000::1  33 ms  0 ms  0 ms
 2  100::2  33 ms  33 ms  17 ms
>
```

25.3.5　NDP 情報の確認

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

図 25-5　show ipv6 neighbor の実行結果

```
> show ipv6 neighbors interface vlan 4094

Date 20XX/06/07 11:05:51 UTC
Total: 7
Neighbor                        Linklayer Address Interface  Expire    S Flgs
2001:254::2                     782b.cb7f.7fa1    VLAN4094   1s        R
2001:254::99                    1cc1.de64.f234    VLAN4094   14s       R
2001:254::252                   0012.e282.680d    VLAN4094   permanent R S
2001:254::951:b8c:84bd:9cd3     1cc1.de64.f234    VLAN4094   6s        R
fe80::1bc:91af:3b96:2f72%VLAN40 782b.cb7f.7fa1    VLAN4094   19m56s    S
fe80::212:e2ff:fe82:680d%VLAN40 0012.e282.680d    VLAN4094   permanent R S
fe80::951:b8c:84bd:9cd3%VLAN409 1cc1.de64.f234    VLAN4094   19m56s    S

>
```

26 DHCP サーバ機能

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

26.1 解説

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

26.1.1 サポート仕様

本装置の DHCP サーバ機能のサポート仕様を次の表に示します。DHCP サーバとクライアント接続は，同一ネットワーク内での直結で行います。

表 26-1 DHCP サーバ機能のサポート仕様

項目	仕様
接続構成	DHCP クライアントを直接収容 DHCP リレーエージェント経由では収容不可
BOOTP サーバ機能	未サポート
ダイナミック DNS 連携	未サポート
動的 IP アドレス配布機能	サポート
固定 IP アドレス配布機能	サポート

26.1.2 クライアントへの配布情報

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

表 26-2 本装置でクライアントに配布する情報の一覧

項目	仕様
IP アドレス	クライアントが使用可能な IP アドレスを設定します。
IP アドレスリース時間	配布する IP アドレスのリース時間を設定します。本装置では default-lease-time/max-lease-time パラメータとクライアントからの要求によって値が決定されます。(Option No：51)
サブネットマスク	本オプションはコンフィグレーションで指定したネットワーク情報のサブネットマスク長が使用されます。(Option No：1)
ルータオプション	クライアントのサブネット上にあるルータの IP アドレスを指定します。この IP アドレスがクライアントのゲートウェイアドレスとして使用されます。(Option No：3)
DNS オプション	クライアントが利用できるドメインネームサーバのIPアドレスを指定します。(Option No：6)

26.1.3 IP アドレスの二重配布防止

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

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

26.1.4 DHCP サーバ機能使用時の注意事項

DHCP サーバ機能使用時の注意事項について説明します。

（1） マルチホーム接続時の入力インタフェースの IP アドレス

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

26.2 コンフィグレーション

26.2.1 コンフィグレーションコマンド一覧

DHCP サーバのコンフィグレーションコマンド一覧を次の表に示します。

表 26-3 コンフィグレーションコマンド一覧

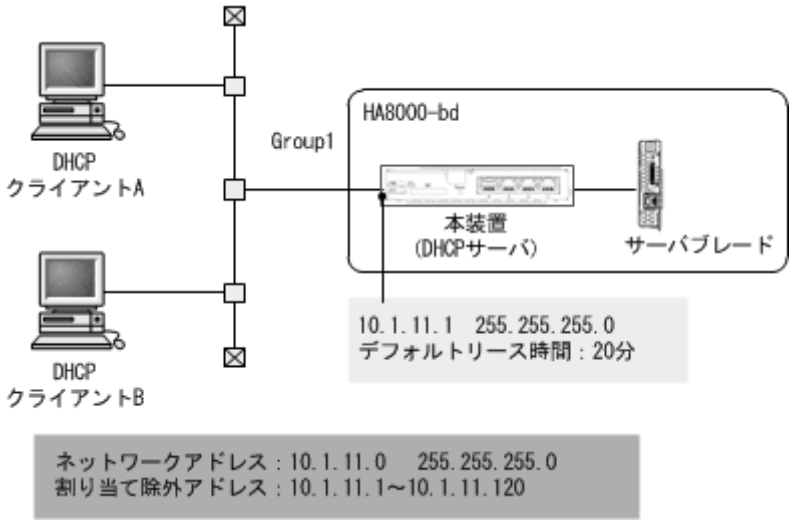
コマンド名	説明
default-router	クライアントに配布するルータオプションを指定します。ルータオプションは，クライアントがサブネット上のルータ IP アドレス（デフォルトルータ）として使用可能な IP アドレスです。「26.2.2 クライアントに IP を配布する設定」のようにクライアントが使用するルータの IP アドレスを設定します。
dns-server	クライアントに配布するドメインネームサーバオプションを設定します。
hardware-address	クライアント装置に固定の IP アドレスを配布する際に，対象となる装置の MAC アドレスを指定します。本コマンドはホストコマンドとセットで使用します。「26.2.3 クライアントに固定 IP を配布する設定」のようにクライアントの MAC アドレスを設定します。
host	クライアント装置に固定の IP アドレスを配布する際に，割り当てる IP アドレスを指定します。本コマンドはハードウェアアドレスコマンドとセットで使用します。「26.2.3 クライアントに固定 IP を配布する設定」のようにクライアントが使用する IP アドレスを設定します。
ip dhcp excluded-address	network コマンドで指定した IP アドレスプールのうち，配布対象から除外する IP アドレスの範囲を指定します。「26.2.2 クライアントに IP を配布する設定」のようにネットワークのアドレス範囲のうち，クライアントへの配布から除外する IP アドレスを設定します。
ip dhcp pool	DHCP アドレスプール情報を設定します。
lease	クライアントに配布する IP アドレスのデフォルトリース時間を指定します。 「26.2.2 クライアントに IP を配布する設定」のようにクライアントが使用する IP アドレスのリース時間を設定します。
max-lease	クライアントがリース時間を指定して IP アドレスを要求した際に，許容する最大リース時間を指定します。
network	DHCP によって動的に IP アドレスを配布するネットワークのサブネットを指定します。実際に DHCP アドレスプールとして登録されるのはサブネットのうち，IP アドレスホスト部のビットがすべて 0，およびすべて 1 のアドレスを除いたものです。「26.2.2 クライアントに IP を配布する設定」のように DHCP によって IP アドレスを配布するネットワークを設定します。
service dhcp	DHCP サーバを有効にするインタフェースを指定します。 本設定を行ったインタフェースでだけ DHCP パケットを受信します。「26.2.2 クライアントに IP を配布する設定」のように DHCP クライアントが接続されている VLAN インタフェースを設定します。

26.2.2 クライアントに IP を配布する設定

［設定のポイント］

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

図 26-1 クライアントーサーバ構成（動的 IP アドレス配布時）



［コマンドによる設定］

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

2. **(config)# service dhcp vlan 10**
   DHCP サーバを有効にする VLAN を設定します。

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

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

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

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

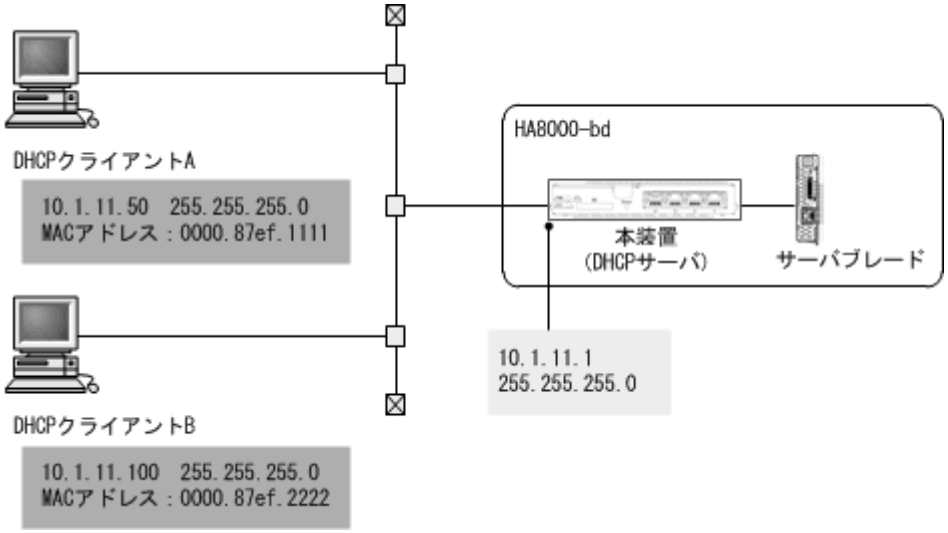
7. **(dhcp-config)# default-router 10.1.11.1**
   (dhcp-config)# exit
   サブネット上にあるルータの IP アドレスを設定します。

26.2.3 クライアントに固定 IP を配布する設定

［設定のポイント］

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

図 26-2 クライアントーサーバ構成（固定 IP アドレス配布時）



［コマンドによる設定］

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

2. **(config)# service dhcp vlan 10**
   DHCP サーバを有効にする VLAN を設定します。

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

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

5. **(dhcp-config)# hardware-address 0000.87ef.1111 ethernet**
   DHCP クライアント A の DHCP アドレスプールに対する MAC アドレスを設定します。

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

7. **(onfig)# ip dhcp pool Client2**
   (dhcp-config)# host 10.1.11.100 255.255.255.0

```
(dhcp-config)# hardware-address 0000.87ef.2222 ethernet
(dhcp-config)# default-router 10.1.11.1
(dhcp-config)# exit
```

項番 3 から 6 と同様に，DHCP クライアント B にもアドレスプール名称，固定 IP アドレス，MAC アドレスを設定します。

26.3 オペレーション

26.3.1 運用コマンド一覧

DHCP サーバの運用コマンド一覧を次の表に示します。

表 26-4 運用コマンド一覧

コマンド名	説明
show ip dhcp binding	DHCP サーバ上の結合情報を表示します。
clear ip dhcp binding	DHCP サーバのデータベースから結合情報を削除します。
show ip dhcp conflict	DHCP サーバによって検出した衝突 IP アドレス情報を表示します。衝突 IP アドレスとは，DHCP サーバのプール IP アドレスでは空きとなっていますが，すでにネットワーク上の端末に割り当てられている IP アドレスを指します。衝突 IP アドレスは，DHCP サーバが DHCP クライアントに対して IP アドレスを割り当てる前に ICMP パケット送出の応答有無，または DECLINE メッセージ受信によって検出します。
clear ip dhcp conflict	DHCP サーバから衝突 IP アドレス情報を取り除きます。
show ip dhcp server statistics	DHCP サーバの統計情報を表示します。
clear ip dhcp server statistics	DHCP サーバの統計情報をリセットします。

26.3.2 DHCP サーバの確認

(1) 割り当て可能な IP アドレス数の確認

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

図 26-3 show ip dhcp server statistics の実行結果

```
> show ip dhcp server statistics

Date 20XX/06/23 08:34:35 UTC
   < DHCP Server use statistics >
     address pools           : 1010
     automatic bindings      : 13
     manual bindings         : 1
     expired bindings        : 0
     over pools request      : 0
     discard packets         : 0
   < Receive Packets >
     DHCPDISCOVER            : 14
     DHCPREQUEST             : 14
     DHCPDECLINE             : 0
     DHCPRELEASE             : 0
     DHCPINFORM              : 1
   < Send Packets >
     DHCPOFFER               : 14
     DHCPACK                 : 15
     DHCPNAK                 : 0

>
```

（2） 配布した IP アドレスの確認

実際に DHCP クライアントへ割り当てられた IP アドレスについては，運用コマンド show ip dhcp binding で確認してください。リースを満了していない IP アドレスを表示します。

図 26-4　show ip dhcp binding の実行結果

```
> show ip dhcp binding

Date 20XX/06/23 08:41:12 UTC
 No   IP Address        MAC Address      Lease Expiration       Type
    1 192.168.1.1       0012.e2c4.a8c7                          Manual
    2 192.168.1.0       0012.e26a.015c   20XX/06/24 08:34:05    Automatic
    3 192.168.1.2       0012.e26a.015f   20XX/06/24 08:34:06    Automatic

>
```

付録

付録 A　準拠規格

付録 A　準拠規格

付録 A.1　TELNET/FTP/TFTP

表 A-1　TELNET/FTP/TFTP の準拠する規格および勧告

規格番号 (発行年月)	規格名
RFC854 (1983 年 5 月)	TELNET PROTOCOL SPECIFICATION
RFC855 (1983 年 5 月)	TELNET OPTION SPECIFICATIONS
RFC959 (1985 年 10 月)	FILE TRANSFER PROTOCOL (FTP)
RFC1350 (1992 年 7 月)	THE TFTP PROTOCOL (REVISION 2)
RFC2428(1998 年 9 月)	FTP Extensions for IPv6 and NATs

付録 A.2　RADIUS

表 A-2　RADIUS 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)
RFC3162(2001 年 8 月)	RADIUS and IPv6

付録 A.3　NTP

表 A-3　NTP の準拠する規格および勧告

規格番号 (発行年月)	規格名
RFC2030(1996 年 10 月)	Simple Network Time Protocol (SNTP) Version4 for IPv4, IPv6 and OSI

付録 A.4　DNS

表 A-4　DNS リゾルバの準拠する規格および勧告

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　イーサネット

表 A-5　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,	IEEE802.2 1998 Edition	IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 2: Logical Link Control
	IEEE802.3 2008 Edition	Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer Specifications
	IEEE802.3ah 2004	Amendment: Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks

付録 A.6　リンクアグリゲーション

表 A-6　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.7　VLAN

表 A-7　VLAN の準拠規格および勧告

規格	名称
IEEE802.1Q (IEEE Std 802.1Q-2003)	Virtual Bridged Local Area Networks ※

注※

GVRP/GMRP はサポートしていません。

付録 A.8　スパニングツリー

表 A-8　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

付録 A.9　IGMP snooping/MLD snooping

表 A-9　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
draft-ietf-magma-snoop-12.txt (2005 年 8 月)	IGMP and MLD snooping switches

付録 A.10　IPv4 インタフェース

表 A-10　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

付録 A.11　IPv6 インタフェース

表 A-11　IP バージョン 6 の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC2373(1998 年 7 月)	IP Version 6 Addressing Architecture
RFC2460(1998 年 12 月)	Internet Protocol, Version 6 (IPv6) Specification
RFC2461(1998 年 12 月)	Neighbor Discovery for IP Version 6 (IPv6)
RFC2462(1998 年 12 月)	IPv6 Stateless Address Autoconfiguration
RFC2463(1998 年 12 月)	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
RFC2710(1999 年 10 月)	Multicast Listener Discovery for IPv6

付録 A.12　DHCP サーバ機能

表 A-12　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

索引

数字

C

D

I

L

M

P

R

T

V

い

う

お

か

く

こ

さ

し

す

せ

そ

た

て

と

に

ね

は

ふ

ほ

ま

り

れ

ろ