ブレードサーバ内蔵 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

Ver. 10.7 対応

BSELANSW-S007-00

HITACHI

■対象製品

このマニュアルはブレードサーバ内蔵 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. 10.7 の機能について記載しています。ソフトウェア機能は，ソフトウェア OS-L3A 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，外国為替および外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上，必要な手続きをお取りください。
なお，ご不明な場合は，弊社担当営業にお問い合わせください。

■商標一覧

Cisco は，米国 Cisco Systems, Inc. の米国および他の国々における登録商標です。
Ethernet は，米国 Xerox Corp. の商品名称です。
Internet Explorer は，米国 Microsoft Corporation の米国及びその他の国における登録商標または商標です。
IPX は，Novell,Inc. の商標です。
Microsoft は，米国およびその他の国における米国 Microsoft Corp. の登録商標です。
Netscape は，米国およびその他の国における Netscape Communications Corporation の登録商標です。
Octpower は，日本電気（株）の登録商標です。
sFlow は，米国およびその他の国における米国 InMon Corp. の登録商標です。
UNIX は，X/Open Company Limited が独占的にライセンスしている米国ならびに他の国における登録商標です。
VitalQIP，VitalQIP Registration Manager は，Lucent technologies の商標です。
VLANaccessClient は，NEC ソフトの商標です。
VLANaccessController，VLANaccessAgent は，NEC の商標です。
Windows は，米国およびその他の国における米国 Microsoft Corp. の登録商標です。
イーサネットは，富士ゼロックス（株）の商品名称です。
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

２００９年　　３月　（初版）　ＢＳＥＬＡＮＳＷ－Ｓ００７－００

■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

このマニュアルはブレードサーバ内蔵 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. 10.7 の機能について記載しています。ソフトウェア機能は，ソフトウェア OS-L3A 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

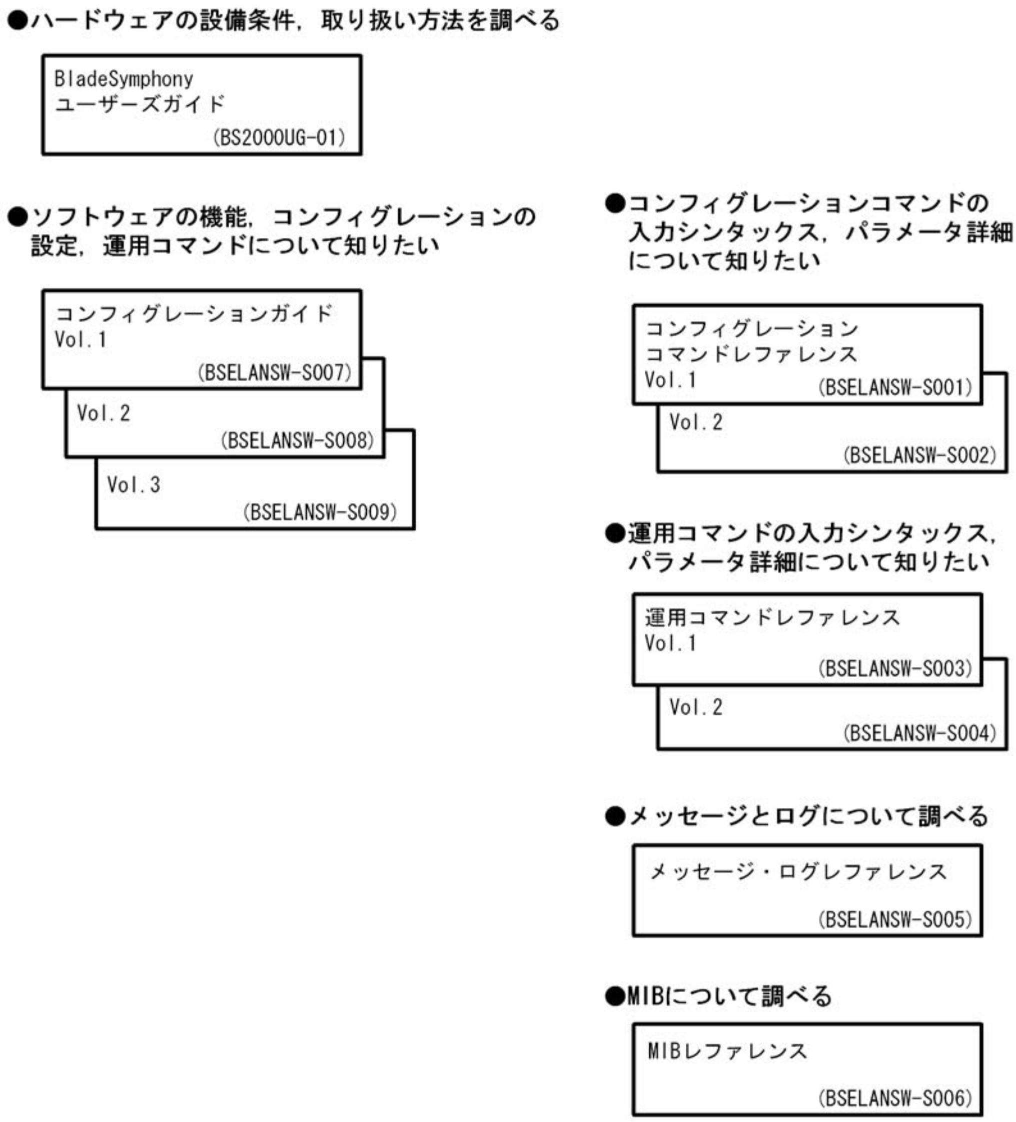
本装置を利用したネットワークシステムを構築し，運用するシステム管理者の方を対象としています。

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
CDP	Cisco Discovery Protocol
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network System
CONS	Connection Oriented Network System
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
ES	End System
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FTTH	Fiber To The Home
GBIC	GigaBit Interface Converter
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCP	IP Control Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IP Version 6 Control Protocol
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Internal Spanning Tree
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLQ+3WFQ	Low Latency Queueing + 3 Weighted Fair Queueing
LSP	Label Switched Path
LSP	Link State PDU
LSR	Label Switched Router
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MIB	Management Information Base
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
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
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SPF	Shortest Path First
SSAP	Source Service Access Point
STP	Spanning Tree Protocol
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
TLV	Type, Length, and Value
TOS	Type Of Service
TPID	Tag Protocol Identifier
TTL	Time To Live
UDLD	Uni-Directional Link Detection
UDP	User Datagram Protocol
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
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
```

■常用漢字以外の漢字の使用について

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

- 宛て（あて）
- 宛先（あてさき）
- 溢れ（あふれ）
- 迂回（うかい）
- 鍵（かぎ）
- 個所（かしょ）
- 筐体（きょうたい）
- 桁（けた）
- 毎（ごと）
- 閾値（しきいち）
- 芯（しん）
- 溜まる（たまる）
- 誰（だれ）
- 必須（ひっす）
- 輻輳（ふくそう）
- 閉塞（へいそく）
- 漏洩（ろうえい）

■ kB(バイト)などの単位表記について

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

目次

第 3 編　ネットワークインタフェース

付録

索引

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 1Gbit/s 以上で接続

- 1Gb LAN スイッチモジュールでは全 24 ポートで 1Gbit/s 通信サポート
  サーバブレードとは 1Gbit/s 全二重で通信 (ポート 0/5 ～ 0/24)
  外部機器との接続は 1000BASE-T/100BASE-TX/10BASE-T をサポート (ポート 0/1 ～ 0/4)
- 1/10Gb LAN スイッチモジュールでは外部接続機器との 10Gbit/s 通信サポート
  外部機器とは 10GBASE-R(XFP) を 2 ポート (ポート 0/25 ～ 0/26) サポート，1000BASE-T/100BASE-TX/10BASE-T を 4 ポート (ポート 0/1 ～ 0/4) で接続
  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の冗長化が可能
  本装置をブレードサーバに 2 台搭載して，サーバブレードのチーミング機能等を使用することで，冗長構成を構築することができます。

（2） 高速で多様な VLAN 機能をサポート

● レイヤ 2 の VLAN 機能

- ポート VLAN，プロトコル VLAN，MAC VLAN 機能を実装
- 用途に応じた VLAN 構築が可能

● スパニングツリープロトコル

- スパニングツリー（IEEE802.1D），高速スパニングツリー（IEEE802.1w），PVST+，マルチプルスパニングツリー（IEEE802.1s）を実装

● VLAN トンネリングによる L2-VPN の実現

（3） 強固なセキュリティ機能

● 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
- L2/L3/L4 ヘッダの一部指定が可能
- 多条件指定可能なスケーラビリティ
  フィルタエントリ数は，装置当たり最大 1024 エントリを定義できます。

● RADIUS ／ TACACS+ による装置へのログイン・パスワード認証およびユーザごとに実行可能コマンドの制限を設定可能

（4） ハードウェアによる強力な QoS で通信品質を保証

- ハードウェアによる高性能な QoS 処理
- きめ細かなパラメータ（L2/L3/L4 ヘッダ）指定で，高い精度の QoS 制御が可能
- 多様な QoS 制御機能
  L2-QoS（IEEE802.1p，帯域制御，優先制御，廃棄制御など），IP-QoS（Diff-Serv，帯域制御，優先制御，廃棄制御など）
- 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できます。

(5) 10G アップリンク対応

● 10G アップリンク対応

- 10G イーサネットではトランシーバとして今後の主流となる XFP（10GBASE-SR/LR）を採用。

(6) 実績あるルーティング機能

● 安定した高機能ルーティング

- 広域イーサネットサービスや IP-VPN サービスを利用した拠点間接続に，OSPF 機能や BGP 機能を使用した信頼性の高いルーティングと，マルチパスを使った負荷分散を実現
- ルーティングソフトウェアには，実績ある AlaxalA 社 AX3600S シリーズと同等のものを搭載

● IPv6 マルチキャスト対応

- IPv4 と IPv6 で同一ピーク性能の実現
- 10 ギガビット・イーサネットでフルワイヤレートの IPv6 ルーティングを実現
- 豊富な IPv6 ルーティングプロトコル（スタティック，RIPng，OSPFv3，BGP4+，PIM-SM，PM-SSM，MLD）によって，多様で柔軟な IPv6 ネットワークを実現可能
- IPv4/IPv6 デュアルスタック，IPv6-only 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

● 充実した IPv4 ルーティングプロトコル

- 豊富な IPv4 ルーティングプロトコルをサポート
（スタティック，RIP，OSPF，BGP4，PIM-SM/SSM，IGMP）

(7) 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

- 高速な経路切り替え
高速スパニングツリープロトコル（IEEE802.1w，IEEE802.1s），GSRP※1，Autonomous Extensible Ring Protocol※2（以降，Ring Protocol と呼びます。），リンクアグリゲーション（IEEE802.3ad），ホットスタンバイ（VRRP），スタティック／ VRRP ポーリング※3 など
- サーバブレードを含んだ通信経路切り替え
サーバブレードのチーミング機能等との併用で，外部装置接続用ポートがリンクダウンした場合に，サーバブレードを含んだ通信経路を切り替えるアップリンクフェイルオーバー機能※4
- ロードバランス
OSPF イコールコストマルチパスによる IP レベルの均等トラフィック分散

注※ 1
GSRP（Gigabit Switch Redundancy Protocol）。詳細については，マニュアル「コンフィグレーションガイド Vol.2　9. GSRP の解説」を参照してください。

注※ 2
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。

注※ 3
指定経路上の可達性をポーリングによって確認し，動的に VRRP やスタティックルーティングと連動して経路を切り替えるための監視機能。

注※ 4

アップリンクフェイルオーバー機能の詳細については，マニュアル「コンフィグレーションガイド Vol.2　12. アップリンクフェイルオーバー」を参照してください。

（8） 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 MIB，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能）
- 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
- 全イーサネットポート，コンソールポート，メモリカードスロットを前面に配置

1.2　本装置のモデル

本装置は，1Gb LAN スイッチモジュールと 1/10Gb LAN スイッチモジュールの 2 種類のモジュール型ギガビット・イーサネットスイッチです。

1Gb LAN スイッチモジュールは，外部装置との接続用に 10/100/1000BASE-T ポートを 4 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 ポートを装備しています。

1/10Gb LAN スイッチモジュールは，外部装置との接続用に 10/100/1000BASE-T ポートを 4 ポートと XFP スロット（最大 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 ポートを装備しています。

また，高度なフィルタ／ QoS 機能をサポートし，ワイヤーレート／ノンブロッキングのスイッチングに対応します。

本装置は，リンクアグリゲーション，VLAN，スパニングツリー，GSRP，IGMP/MLD snooping 機能などを備え，IPv4/IPv6 ユニキャスト，IPv4/v6 マルチキャストのハードウェアルーティングに対応し，RIP/OSPF/BGP4 などのさまざまなルーティングプロトコルをサポートしています。

本装置のモデルは，以下の通りです。

- HITACHI 1Gb LAN スイッチモジュール
- HITACHI 1/10Gb LAN スイッチモジュール

1.2.1　収容インタフェース数

本装置が収容できる最大インタフェース数を次の表に示します。

表 1-1　モデルごとのインタフェース数

インタフェース種別	モデル名	
	HITACHI 1Gb LAN スイッチモジュール	HITACHI 1/10Gb LAN スイッチモジュール
10GBASE-R（XFP）※1	－	2
10/100/1000BASE-T	4	4
SERDES※2【1Gbit/s】	20	20

注※ 1　10GBASE-R は，10GBASE-SR と 10GBASE-LR の 2 種類サポートしています。（10GBASE-ER と 10GBASE-ZR は使用できません。）

注※ 2　SERDES は，サーバブレード接続専用ポートですので，他装置との接続としては使用できません。
また，BS2000 では SERDES とサーバブレードが未接続となるポートがあります。この未接続となるポートは，LAN スイッチモジュールを設置するスイッチベイによって異なります。詳細は「表 1-2　BS2000 サーバブレードと未接続の SEREDES のポート番号」を参照願います。

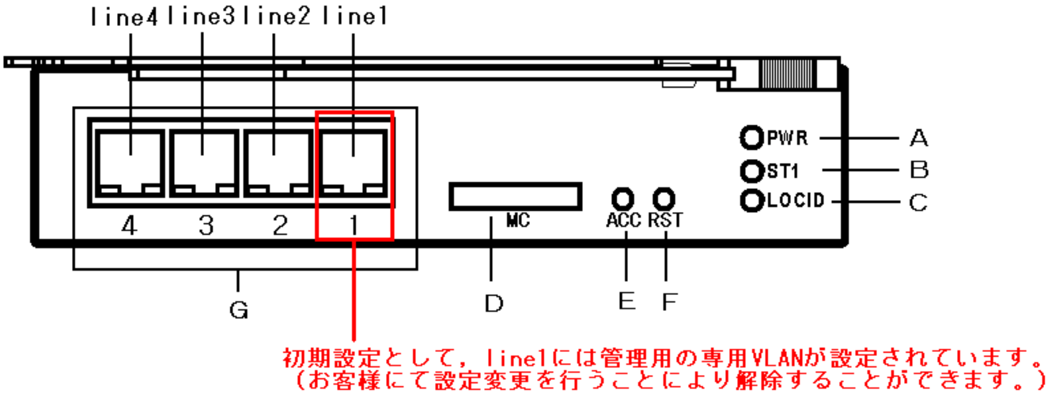
表 1-2　BS2000 サーバブレードと未接続の SEREDES のポート番号

<table>
<tr><th rowspan="2">項目</th><th colspan="6">LAN スイッチモジュールを設置するスイッチベイ番号</th></tr>
<tr><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th></tr>
<tr><td>サーバブレードと未接続となる SERDES のポート番号</td><td colspan="2">13~24</td><td colspan="4">13,14,23,24</td></tr>
</table>

1.2.2　装置の外観

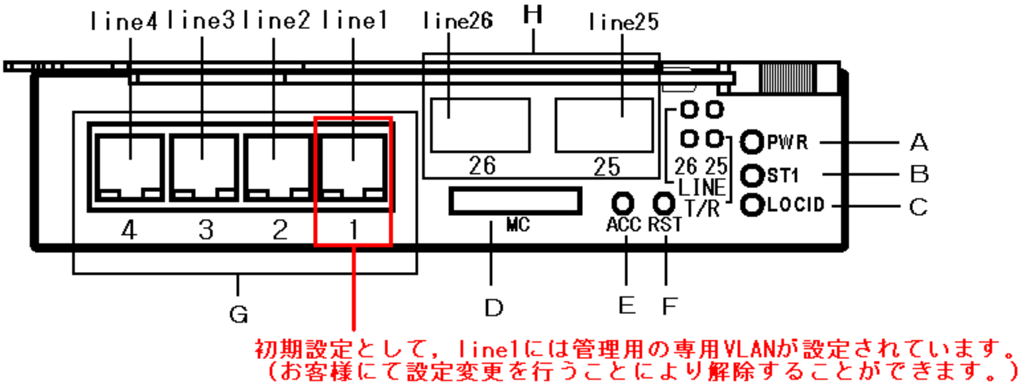
装置外観図を次の図に示します。

図 1-1　HITACHI 1Gb LAN スイッチモジュール



A　POWER ランプ
B　STATUS1 ランプ
C　LOCATION ID ランプ
D　Memory Card スロット
E　アクセスランプ
F　リセットボタン
G　LAN インタフェースコネクタ 1 ～ 4

図 1-2　HITACHI 1/10Gb LAN スイッチモジュール



A　POWER ランプ
B　STATUS1 ランプ
C　LOCATION ID ランプ
D　Memory Card スロット
E　アクセスランプ
F　リセットボタン
G　1Gbit/s LAN インタフェースコネクタ 1 ～ 4
H　10Gbit/s LAN インタフェースコネクタ 25 ～ 26

上記の詳細につきましては，ブレードサーバ装置添付のマニュアル「BladeSymphony ユーザーズガイド」を参照してください。

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

各モデルの最大収容可能回線数を次の表に示します。

表 2-1 最大収容可能回線数

モデル	イーサネット		
	10GBASE-R (XFP)	10/100/1000 BASE-T	SERDES(1Gbit/s)
HITACHI 1Gb LAN スイッチモジュール	−	4	20 ※
HITACHI 1/10Gb LAN スイッチモジュール	2	4	20 ※

（凡例）－：該当なし
注※ BS2000 では SERDES とサーバブレードが未接続となるポートがあります。この未接続となるポートは，スイッチモジュールを設置するスイッチベイによって異なります。詳細は「表 1-2 BS2000 サーバブレードと未接続の SEREDES のポート番号」を参照願います。

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フラッシュ・MC 容量

項目	HITACHI 1Gb LAN スイッチモジュール HITACHI 1/10Gb LAN スイッチモジュール
メインボード搭載メモリ量	512MB
フラッシュ容量	128MB
MC 容量	128MB

2.2　収容条件

(1)　テーブルエントリ数

本装置では，装置の適用形態に合わせ，テーブルエントリ数の配分パターンを変更することができます。配分パターンとして，IPv4 モードと IPv4/IPv6 モードの 2 種類があり，コンフィグレーションコマンド swrt_table_resource によって指定できます。

各モードに対応するテーブルエントリ数の一覧を次の表に示します。

ただし，マルチパス経路のエントリ数については，「コンフィグレーションガイド Vol.3　表 6-5 マルチパス仕様」を参照してください。

表 2-3　テーブルエントリ数

項目		エントリ数	
		IPv4 モード	IPv4/IPv6 モード
IPv4	ユニキャスト経路	12288	8192
	マルチキャスト経路	1024	256
	ARP	3072	1024
IPv6	ユニキャスト経路	－	2048
	マルチキャスト経路	－	128
	NDP	－	1024
L2	MAC アドレステーブル	32768	
	VLAN	4094	

（凡例）－：該当なし

(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 2-4　リンクアグリゲーションの収容条件

モデル	チャネルグループ当たりの最大ポート数	装置当たりの最大チャネルグループ
全モデル共通	8	32

注

SERDES(サーバ接続ポート) に対してのリンクアグリゲーションの設定は，サーバブレード側のチーミング機能などと組み合わせて，本製品とサーバブレードの通信経路の負荷分散や冗長化を実現する場合に使用します。リンクアグリゲーションの注意事項のついては，「13.1.3　サポート仕様　[注意事項]」を参照してください。

(3)　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 2-5　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

モデル	装置当たり	
	最大エントリ数	スタティックエントリ数
全モデル共通	32768	256

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 学習は行われません。したがって，未学習の MAC アドレス宛てのパケットは該当する 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。

（4） 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 2-6　VLAN のサポート数

モデル	ポート当たり VLAN	装置当たり VLAN	ポートごと VLAN 数の装置での合計
全モデル共通	4094	4094	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，ポート 1 からポート 10 では設定している VLAN 数が 2000，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 20014 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。

（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 VLAN の収容条件を次の表に示します。

表 2-7　プロトコル VLAN のプロトコルの種類数

モデル	ポート当たり	装置当たり
全モデル共通	16	16

表 2-8　プロトコル VLAN 数

モデル	ポート当たり	装置当たり
全モデル共通	48※	48

注※　トランクポートに設定できるプロトコル VLAN 数。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

モデル	コンフィグレーションによる最大登録 MAC アドレス数	L2 認証機能による最大登録 MAC アドレス数	同時登録最大 MAC アドレス数
全モデル共通	1024	1024	1024

なお，コンフィグレーションコマンド mac-based-vlan static-only が設定された場合は，次の表に示す収容条件となります。

表 2-10　mac-based-vlan static-only 設定時の登録 MAC アドレス数

モデル	コンフィグレーションによる最大登録 MAC アドレス数	L2 認証機能による最大登録 MAC アドレス数
全モデル共通	1024	0

(c) VLAN トンネリング

コンフィグレーションによって設定できる VLAN トンネリングの数を次の表に示します。

表 2-11　VLAN トンネリングの数

モデル	装置当たり
全モデル共通	4094

(d) タグ変換

コンフィグレーションによって設定できる VLAN タグ変換情報数を次の表に示します。

表 2-12　タグ変換情報数

モデル	装置当たり
全モデル共通	768

(5) 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 2-13　PVST+ の収容条件

モデル	Ring Protocol 共存有無	対象 VLAN 数	VLAN ポート数※1
全モデル共通	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 2-14 シングルスパニングツリーの収容条件

モデル	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）
全モデル共通	共存なし	1024※3	5000	1000
	共存あり	1024※3	4000	800

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+ の対象ポート含み合計の最大値が 1000 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 2-15 マルチプルスパニングツリーの収容条件

モデル	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
全モデル共通	共存なし	1024	5000	16	50
	共存あり	1024	4000	16	50

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 1024 となります。

（6） Ring Protocol

（a） Ring Protocol

Ring Protocol の収容条件を次の表に示します。

表 2-16 Ring Protocol の収容条件

項目	リング当たり	装置当たり
リング数	－	8
VLAN マッピング数	－	128
VLAN グループ数	2	16
VLAN グループの VLAN 数	1023※1	1023※1
リングポート数※2	2	16

（凡例）－：該当なし

注※1
装置として推奨する VLAN の最大数です。
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※ 2
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 2-17　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

(7) IGMP snooping ／ MLD snooping

IGMP snooping の収容条件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
VLAN ポート数※ 1	512
登録エントリ数※ 2 ※ 3	500

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
登録エントリ数の最大数には，ルーティングプロトコルなどで使用する制御パケットのマルチキャストアドレスも含みます。該当するエントリは，制御パケットに対するグループ参加要求を受信した場合に登録します。VLAN 内で複数のルーティングプロトコルを同時に使用する場合，該当するプロトコルの制御パケットが使用するマルチキャストアドレス分だけエントリを使用します。

注※ 3
IPv4 マルチキャストまたは IPv6 マルチキャストと同時に使用しない場合は，各 VLAN で学習したマルチキャスト MAC アドレスの総和です。IPv4 マルチキャストまたは IPv6 マルチキャストと同時に使用する場合は，各 VLAN で学習したマルチキャスト IP アドレスの総和です。

MLD snooping の収容条件を次の表に示します。

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	500

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

登録エントリ数の最大数には，ルーティングプロトコルなどで使用する制御パケットのマルチキャストアドレスも含みます。該当するエントリは，制御パケットに対するグループ参加要求を受信した場合に登録します。VLAN 内で複数のルーティングプロトコルを同時に使用する場合，該当するプロトコルの制御パケットが使用するマルチキャストアドレス分だけエントリを使用します。

注※ 3

IPv6 マルチキャストと同時に使用しない場合は，各 VLAN で学習したマルチキャスト MAC アドレスの総和です。IPv6 マルチキャストと同時に使用する場合は，各 VLAN で学習したマルチキャスト IP アドレスの総和です。

(8) 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「(a) 受信側フィルタ・QoS エントリ数」を，送信側のエントリ数については「(b) 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。

(a) 受信側フィルタ・QoS エントリ数

● layer3-1 を選択した場合のフィルタエントリ数

受信側フロー検出モード layer3-1 を選択した場合に設定できるフィルタ最大エントリ数を次の表に示します。このモードは，MAC 条件および IPv4 条件それぞれのフロー検出条件ごとに上限値があります。

表 2-20 モード layer3-1 のフィルタ最大エントリ数

モデル	インタフェース種別	受信側フィルタ最大エントリ数※1			
		インタフェース当たり		装置当たり	
		MAC 条件	IPv4 条件	MAC 条件	IPv4 条件
全モデル共通	イーサネット	256	256	768※2	768※2
	VLAN	256	256	256	256

注※ 1

フィルタエントリ追加時，該当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：254 エントリ使用可能
（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：249 エントリ使用可能

注※ 2
ポート番号の範囲ごとにエントリ数の上限値があります。「表 2-21　モード layer3-1 のフィルタ最大エントリ数（ポート番号範囲ごと）」を参照してください。

装置当たりに設定できるポート番号の範囲ごとのフィルタ最大エントリ数を次の表に示します。表に示すモデルでは，インタフェース種別がイーサネットの場合，ポート番号の範囲ごとにエントリ数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。

表 2-21　モード layer3-1 のフィルタ最大エントリ数（ポート番号範囲ごと）

モデル	ポート番号の範囲	受信側フィルタ最大エントリ数※ 1	
		MAC 条件	IPv4 条件
全モデル共通	ポート 1 〜 8，(25，26) ※ 2	256	256
	ポート 9 〜 16	256	256
	ポート 17 〜 24	256	256

注※ 1
「表 2-20　モード layer3-1 のフィルタ最大エントリ数」の注※ 1 を参照してください。

注※ 2
括弧内は，HITACHI 1/10Gb LAN スイッチモジュールの 10Gbit/s のポート番号を示します。

● layer3-1 を選択した場合の QoS エントリ数

受信側フロー検出モード layer3-1 を選択した場合に設定できる QoS 最大エントリ数を次の表に示します。このモードは，MAC 条件および IPv4 条件それぞれのフロー検出条件ごとに上限値があります。

表 2-22　モード layer3-1 の QoS 最大エントリ数

モデル	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	MAC 条件	IPv4 条件
全モデル共通	イーサネット	128	128	128	128
	VLAN	128	128	128	128

注※
ポート番号の範囲ごとにエントリ数の上限値があります。「表 2-21　モード layer3-1 のフィルタ最大エントリ数（ポート番号範囲ごと）」を参照してください。

装置当たりに設定できるポート番号の範囲ごとの QoS 最大エントリ数を次の表に示します。表に示すモデルでは，インタフェース種別がイーサネットの場合，ポート番号の範囲ごとにエントリ数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。

● layer3-2 を選択した場合のフィルタエントリ数

受信側フロー検出モード layer3-2 を選択した場合に設定できるフィルタ最大エントリ数を次の表に示します。本モードでのフロー検出条件は IPv4 条件を使用できます。また，イーサネットインタフェースに対してだけ設定するモードです。

表 2-23　モード layer3-2 のフィルタ最大エントリ数

モデル	インタフェース種別	受信側フィルタ最大エントリ数※1	
		インタフェース当たり	装置当たり
全モデル共通	イーサネット	256	2048※2
	VLAN	－	－

（凡例）－：該当なし

注※1
「表 2-20　モード layer3-1 のフィルタ最大エントリ数」の注※1 を参照してください。

注※2
ポート番号の範囲ごとにエントリ数の上限値があります。「表 2-24　モード layer3-2 のフィルタ最大エントリ数（ポート番号範囲ごと）」を参照してください。

装置当たりに設定できるポート番号の範囲ごとのフィルタ最大エントリ数を次の表に示します。表に示すモデルでは，インタフェース種別がイーサネットの場合，ポート番号の範囲ごとにエントリ数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。

表 2-24　モード layer3-2 のフィルタ最大エントリ数（ポート番号範囲ごと）

モデル	ポート番号の範囲	受信側フィルタ最大エントリ数※1
全モデル共通	ポート 1 ～ 3，(25，26)※2	256
	ポート 4 ～ 6	256
	ポート 7 ～ 9	256
	ポート 10 ～ 12	256
	ポート 13 ～ 15	256
	ポート 16 ～ 18	256
	ポート 19 ～ 21	256
	ポート 22 ～ 24	256

注※1
「表 2-20　モード layer3-1 のフィルタ最大エントリ数」の注※1 を参照してください。

注※2
括弧内は，HITACHI 1/10Gb LAN スイッチモジュールの 10Gbit/s のポート番号を示します。

● layer3-2 を選択した場合の QoS エントリ数

受信側フロー検出モード layer3-2 を選択した場合に設定できる QoS 最大エントリ数を次の表に示します。本モードでのフロー検出条件は IPv4 条件を使用できます。また，イーサネットインタフェースに対してだけ設定するモードです。

表 2-25　モード layer3-2 の QoS 最大エントリ数

モデル	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
全モデル共通	イーサネット	128	512※
	VLAN	−	−

（凡例）－：該当なし

注※

ポート番号の範囲ごとにエントリ数の上限値があります。「表 2-26　モード layer3-2 の QoS 最大エントリ数（ポート番号範囲ごと）」を参照してください。

装置当たりに設定できるポート番号の範囲ごとの QoS 最大エントリ数を次の表に示します。表に示すモデルでは，インタフェース種別がイーサネットの場合，ポート番号の範囲ごとにエントリ数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。

表 2-26　モード layer3-2 の QoS 最大エントリ数（ポート番号範囲ごと）

モデル	ポート番号の範囲	受信側 QoS 最大エントリ数
全モデル共通	ポート 1 ～ 6，（25，26）※ 1	128
	ポート 7 ～ 12	128
	ポート 13 ～ 18	128
	ポート 19 ～ 24	128

注※ 1

括弧内は，HITACHI 1/10Gb LAN スイッチモジュールの 10Gbit/s のポート番号を示します。

● layer3-3 または layer3-4 を選択した場合のフィルタエントリ数

受信側フロー検出モード layer3-3 または layer3-4 のどちらかを選択した場合に設定できるフィルタ最大エントリ数を次の表に示します。これらのモードは，IPv4 条件および IPv6 条件それぞれのフロー検出条件ごとに上限値があります。また，イーサネットインタフェースに対してだけ設定するモードです。

表 2-27　モード layer3-3 または layer3-4 のフィルタ最大エントリ数

モデル	インタフェース種別	受信側フィルタ最大エントリ数※ 1			
		インタフェース当たり		装置当たり	
		IPv4 条件	IPv6 条件	IPv4 条件	IPv6 条件
全モデル共通	イーサネット	256	256	1024 ※ 2	1024 ※ 2
	VLAN	−	−	−	−

（凡例）－：該当なし

注※ 1

「表 2-20　モード layer3-1 のフィルタ最大エントリ数」の注※ 1 を参照してください。

注※ 2

ポート番号の範囲ごとにエントリ数の上限値があります。「表 2-28　モード layer3-3 または layer3-4 のフィルタ最大エントリ数（ポート番号範囲ごと）」を参照してください。

装置当たりに設定できるポート番号の範囲ごとのフィルタ最大エントリ数を次の表に示します。表に示すモデルでは，インタフェース種別がイーサネットの場合，ポート番号の範囲ごとにエントリ数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。

表 2-28　モード layer3-3 または layer3-4 のフィルタ最大エントリ数（ポート番号範囲ごと）

モデル	ポート番号の範囲	受信側フィルタ最大エントリ数※1	
		IPv4 条件	IPv6 条件
全モデル共通	ポート 1 ～ 6，（25，26）※2	256	256
	ポート 7 ～ 12	256	256
	ポート 13 ～ 18	256	256
	ポート 19 ～ 24	256	256

注※ 1

「表 2-20　モード layer3-1 のフィルタ最大エントリ数」の注※ 1 を参照してください。

注※ 2

括弧内は，HITACHI 1/10Gb LAN スイッチモジュールの 10Gbit/s のポート番号を示します。

● layer3-3 または layer3-4 を選択した場合の QoS エントリ数

受信側フロー検出モード layer3-3 または layer3-4 のどちらかを選択した場合に設定できる QoS 最大エントリ数を次の表に示します。これらのモードは，IPv4 条件および IPv6 条件それぞれのフロー検出条件ごとに上限値があります。また，イーサネットインタフェースに対してだけ設定するモードです。

表 2-29　モード layer3-3 または layer3-4 の QoS 最大エントリ数

モデル	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	
		IPv4 条件	IPv6 条件	IPv4 条件	IPv6 条件
全モデル共通	イーサネット	128	128	256※	256※
	VLAN	－	－	－	－

（凡例）－：該当なし

注※

ポート番号の範囲ごとにエントリ数の上限値があります。「表 2-30　モード layer3-3 または layer3-4 の QoS 最大エントリ数（ポート番号範囲ごと）」を参照してください。

装置当たりに設定できるポート番号の範囲ごとの QoS 最大エントリ数を次の表に示します。表に示すモデルでは，インタフェース種別がイーサネットの場合，ポート番号の範囲ごとにエントリ数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。

表 2-30　モード layer3-3 または layer3-4 の QoS 最大エントリ数（ポート番号範囲ごと）

モデル	ポート番号の範囲	受信側 QoS 最大エントリ数	
		IPv4 条件	IPv6 条件
全モデル共通	ポート 1 ～ 12，(25，26)※1	128	128
	ポート 13 ～ 24	128	128

注※ 1

括弧内は，HITACHI 1/10Gb LAN スイッチモジュールの 10Gbit/s のポート番号を示します。

● layer3-5 を選択した場合のフィルタエントリ数

受信側フロー検出モード layer3-5 を選択した場合に設定できるフィルタ最大エントリ数を次の表に示します。このモードは，IPv4 条件および IPv6 条件それぞれのフロー検出条件ごとに上限値があります。また，イーサネットインタフェースに対してだけ設定するモードです。

表 2-31　モード layer3-5 のフィルタ最大エントリ数

モデル	インタフェース種別	受信側フィルタ最大エントリ数※1			
		インタフェース当たり		装置当たり	
		IPv4 条件	IPv6 条件	IPv4 条件	IPv6 条件
全モデル共通	イーサネット	256	128	1024※2	512※2
	VLAN	―	―	―	―

（凡例）―：該当なし

注※ 1

「表 2-20　モード layer3-1 のフィルタ最大エントリ数」の注※ 1 を参照してください。

注※ 2

ポート番号の範囲ごとにエントリ数の上限値があります。「表 2-32　モード layer3-5 のフィルタ最大エントリ数（ポート番号範囲ごと）」を参照してください。

装置当たりに設定できるポート番号の範囲ごとのフィルタ最大エントリ数を次の表に示します。表に示すモデルでは，インタフェース種別がイーサネットの場合，ポート番号の範囲ごとにエントリ数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。

表 2-32　モード layer3-5 のフィルタ最大エントリ数（ポート番号範囲ごと）

モデル	ポート番号の範囲	受信側フィルタ最大エントリ数※1	
		IPv4 条件	IPv6 条件
全モデル共通	ポート 1 ～ 6，(25，26)※2	256	128
	ポート 7 ～ 12	256	128
	ポート 13 ～ 18	256	128
	ポート 19 ～ 24	256	128

注※ 1

「表 2-20　モード layer3-1 のフィルタ最大エントリ数」の注※ 1 を参照してください。

注※ 2

括弧内は，HITACHI 1/10Gb LAN スイッチモジュールの 10Gbit/s のポート番号を示します。

● layer3-5 を選択した場合の QoS エントリ数

受信側フロー検出モード layer3-5 を選択した場合に設定できる QoS 最大エントリ数を次の表に示します。このモードは，IPv4 条件および IPv6 条件それぞれのフロー検出条件ごとに上限値があります。また，イーサネットインタフェースに対してだけ設定するモードです。

表 2-33　モード layer3-5 の QoS 最大エントリ数

モデル	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	
		IPv4 条件	IPv6 条件	IPv4 条件	IPv6 条件
全モデル共通	イーサネット	128	128	256 ※	256 ※
	VLAN	−	−	−	−

（凡例）−：該当なし

注※

ポート番号の範囲ごとにエントリ数の上限値があります。「表 2-34　モード layer3-5 の QoS 最大エントリ数（ポート番号範囲ごと）」を参照してください。

装置当たりに設定できるポート番号の範囲ごとの QoS 最大エントリ数を次の表に示します。表に示すモデルでは，インタフェース種別がイーサネットの場合，ポート番号の範囲ごとにエントリ数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。

表 2-34　モード layer3-5 の QoS 最大エントリ数（ポート番号範囲ごと）

モデル	ポート番号の範囲	受信側 QoS 最大エントリ数	
		IPv4 条件	IPv6 条件
全モデル共通	ポート 1 ～ 12，(25，26) ※ 1	128	128
	ポート 13 ～ 24	128	128

注※ 1

括弧内は，HITACHI 1/10Gb LAN スイッチモジュールの 10Gbit/s のポート番号を示します。

(b)　送信側フィルタエントリ数

● layer3-1-out を選択した場合のフィルタエントリ数

送信側フロー検出モード layer3-1-out を選択した場合に設定できるフィルタ最大エントリ数を次の表に示します。本モードでのフロー検出条件は IPv4 条件を使用できます。また，イーサネットインタフェースに対してだけ設定するモードです。

表 2-35　モード layer3-1-out のフィルタ最大エントリ数

モデル	インタフェース種別	送信側フィルタ最大エントリ数※1	
		インタフェース当たり	装置当たり
全モデル共通	イーサネット	128	512※2
	VLAN	−	−

（凡例）－：該当なし

注※ 1

「表 2-20　モード layer3-1 のフィルタ最大エントリ数」の注※ 1 を参照してください。

注※ 2

ポート番号の範囲ごとにエントリ数の上限値があります。「表 2-36　モード layer3-1-out のフィルタ最大エントリ数（ポート番号範囲ごと）」を参照してください。

装置当たりに設定できるポート番号の範囲ごとのフィルタ最大エントリ数を次の表に示します。表に示すモデルでは，インタフェース種別がイーサネットの場合，ポート番号の範囲ごとにエントリ数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。

表 2-36　モード layer3-1-out のフィルタ最大エントリ数（ポート番号範囲ごと）

モデル	ポート番号の範囲	送信側フィルタ最大エントリ数※1
全モデル共通	ポート 1 ～ 6，（25，26）※2	128
	ポート 7 ～ 12	128
	ポート 13 ～ 18	128
	ポート 19 ～ 24	128

注※ 1

「表 2-20　モード layer3-1 のフィルタ最大エントリ数」の注※ 1 を参照してください。

注※ 2

括弧内は，HITACHI 1/10Gb LAN スイッチモジュールの 10Gbit/s のポート番号を示します。

● layer3-2-out を選択した場合のフィルタエントリ数

送信側フロー検出モード layer3-2-out を選択した場合に設定できるフィルタ最大エントリ数を次の表に示します。このモードは，MAC 条件，IPv4 条件および IPv6 条件それぞれのフロー検出条件ごとに上限値があります。また，イーサネットインタフェースに対してだけ設定するモードです。

表 2-37　モード layer3-2-out のフィルタ最大エントリ数

モデル	インタフェース種別	送信側フィルタ最大エントリ数※1					
		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
全モデル共通	イーサネット	128	128	128	128	128	128
	VLAN	−	−	−	−	−	−

（凡例）－：該当なし

注※ 1

「表 2-20　モード layer3-1 のフィルタ最大エントリ数」の注※ 1 を参照してください。

装置当たりに設定できるポート番号の範囲ごとのフィルタ最大エントリ数を次の表に示します。表に示すモデルでは，インタフェース種別がイーサネットの場合，ポート番号の範囲ごとにエントリ数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。

● layer3-3-out を選択した場合のフィルタエントリ数

送信側フロー検出モード layer3-3-out を選択した場合に設定できる最大エントリ数を次の表に示します。このモードは，MAC 条件，IPv4 条件および IPv6 条件それぞれのフロー検出条件ごとに上限値があります。また，VLAN インタフェースに対してだけ設定するモードです。

表 2-38　モード layer3-3-out のフィルタ最大エントリ数

モデル	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
全モデル共通	イーサネット	－	－	－	－	－	－
	VLAN	128	128	128	128	128	128

（凡例）－：該当なし

注※

「表 2-20　モード layer3-1 のフィルタ最大エントリ数」の注※ 1 を参照してください。

(c) 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 2-39　TCP/UDP ポート番号検出パターン収容条件

モデル	フロー検出モード	装置当たりの最大数
全モデル共通	全モード共通	16

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 2-40　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
		全モード共通	全モード共通
送信元ポート番号	単一指定 (eq)	−	−
	範囲指定 (range)	○	指定不可
宛先ポート番号	単一指定 (eq)	−	−
	範囲指定 (range)	○	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。

TCP/UDP ポート番号検出パターンを使用する例を次の表に示します。

表 2-41　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送信元ポート番号の範囲が異なるため， ・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 ～ 20) ・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 ～ 20) ・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 ～ 20) 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 ～ 20) 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。

パターンの使用例※	使用するパターン数
QoS エントリで ・IPv4 条件で送信元ポート番号の範囲指定（10 ～ 20） QoS エントリで ・IPv6 条件で送信元ポート番号の範囲指定（10 ～ 20）	上記 4. 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 ～ 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。 ・送信元ポート番号の範囲指定（10 ～ 20）の 1 パターンを使用します。

注※　（）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。

（9） IEEE802.1X

IEEE802.1X の収容条件を次に示します。

本装置の IEEE802.1X では，三つの認証モードをサポートしています。

- ポート単位認証
- VLAN 単位認証（静的）
- VLAN 単位認証（動的）

VLAN 単位認証を使用する場合に，IEEE802.1X を設定できる装置当たりの総ポート数を次の表に示します。

表 2-42　IEEE802.1X を設定できる装置当たりの総ポート数

モデル	IEEE802.1X を設定できる装置当たりの総ポート数※
全モデル共通	1024

注※

IEEE802.1X を設定できる装置当たりの総ポート数とは，VLAN 単位認証を設定した VLAN での VLAN ポート数の総和の最大値です。VLAN 内にチャネルグループが含まれている場合は，チャネルグループを構成する物理ポート数に関係なく，チャネルグループを 1 ポートとして計算します。また，1 ポートに VLAN が Tag で多重化されている場合も個別に数えます。例えば，一つのポートに Tag で多重化された 10 個の VLAN が設定されていた場合，その 10 個の VLAN で VLAN 単位認証を動作させると，総ポート数は 10 ポートになります。

各認証モードでの単位当たりの最大認証端末数を次の表に示します。

表 2-43　各認証モード単位当たりの最大認証端末数

モデル	認証モード		
	ポート単位認証	VLAN 単位認証（静的）	VLAN 単位認証（動的）
全モデル共通	64/ ポート	256/VLAN	1024※ / 装置

注※

IEEE802.1X（VLAN 単位認証（動的））および Web 認証（ダイナミック VLAN モード）を同時に動作した場合は，それぞれの認証端末数の合計で装置当たり 1024 までとなります。

本装置の最大認証端末数を次の表に示します。

表 2-44　本装置の最大認証端末数

モデル	3 モード合計での最大認証端末数
全モデル共通	1024※ / 装置

注※

IEEE802.1X（ポート単位認証および VLAN 単位認証（静的）），Web 認証（固定 VLAN モード）および MAC 認証を同時に動作させた場合は，それぞれの認証端末数の合計で装置当たり 1024 までとなります。

(10) Web 認証

Web 認証の収容条件を次の表に示します。

表 2-45　Web 認証の装置当たりの収容条件

項目		最大数
最大認証数	固定 VLAN モード	1024 ※1
	ダイナミック VLAN モード	1024 ※2
	レガシーモード	1024 ※3
内蔵 Web 認証 DB 登録ユーザ数		300 ※4
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
認証画面入れ替えで指定できるファイル数		100
認証前端末用に設定できる IPv4 アクセスリスト数		1
認証前端末用 IPv4 アクセスリストに指定できるフィルタ条件数		20

注※ 1

Web 認証（固定 VLAN モード），IEEE802.1X（ポート単位認証および VLAN 単位認証（静的））および MAC 認証（固定 VLAN モード）を同時に動作させた場合は，それぞれの認証端末数の合計で装置当たり 1024 までとなります。

注※ 2

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）および IEEE802.1X（VLAN 単位認証（動的））を同時に動作した場合は，それぞれの認証端末数の合計で装置当たり 1024 までとなります。

注※ 3

Web 認証（レガシーモード）および IEEE802.1X（VLAN 単位認証（動的））を同時に動作した場合は，それぞれの認証端末数の合計で装置当たり 1024，までとなります。

注※ 4

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，最大認証端末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。

(11) MAC 認証

MAC 認証の収容条件を次の表に示します。

表 2-46　MAC 認証の装置当たりの収容条件

項目		最大数
最大認証数	固定 VLAN モード	1024 ※1
	ダイナミック VLAN モード	1024 ※2
内蔵 MAC 認証 DB 登録ユーザ数		1024

注※ 1

MAC 認証（固定 VLAN モード），IEEE802.1X（ポート単位認証および VLAN 単位認証（静的））および Web 認

証（固定 VLAN モード）を同時に動作させた場合は，それぞれの認証端末数の合計で 1024 までとなります。

注※ 2

MAC 認証（ダイナミック VLAN モード），Web 認証（ダイナミック VLAN モード）および IEEE802.1X（VLAN 単位認証（動的））を同時に動作した場合は，それぞれの認証端末数の合計で装置当たり 1024 までとなります。

（12）GSRP

GSRP の収容条件を次の表に示します。レイヤ 3 冗長切替機能を使用する場合には，VLAN ポート数が 5000 となります。

表 2-47　GSRP 収容条件

モデル	VLAN グループ最大数	VLAN グループ当たりの VLAN 最大数
全モデル共通	64	1024

（13）VRRP

VRRP に関する収容条件を次の表に示します。

表 2-48　VRRP 収容条件

モデル	仮想ルータ最大数		障害監視インタフェースと VRRP ポーリング最大数	
	インタフェース当たり	装置当たり	仮想ルータ当たり	装置当たり
全モデル共通	255 ※ 1	255 ※ 1	16 ※ 2	255 ※ 2

注※ 1　IPv4/IPv6 の仮想ルータの合計数です。

注※ 2　障害監視インタフェースと VRRP ポーリングの合計数です。

（14）IEEE802.3ah/UDLD

全物理ポートでの運用を可能にします。1 ポート 1 対地を原則とするため，同一ポートから複数装置の情報を受信する場合（禁止構成）でも，保持する情報は 1 装置分だけです。IEEE802.3ah/UDLD の収容条件を次の表に示します。

表 2-49　最大リンク監視情報数

機能モデル	最大リンク監視情報数
HITACHI 1Gb LAN スイッチモジュール	24 ※
HITACHI 1/10Gb LAN スイッチモジュール	26 ※

注※　BS2000 では SERDES とサーバブレードが未接続となるポートがあります。この未接続となるポートは，スイッチモジュールを設置するスイッチベイによって異なります。詳細は「表 1-2　BS2000 サーバブレードと未接続の SEREDES のポート番号」を参照願います。

（15）L2 ループ検知

L2 ループ検知の 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 2-50　L2 ループ検知フレーム送信レート

モデル	L2 ループ検知フレームの送信レート（装置当たり）※1	
	スパニングツリー，GSRP，Ring Protocol のどれかを使用している場合	スパニングツリー，GSRP，Ring Protocol のどれも使用していない場合
全モデル共通	30pps（推奨値）※2	200pps（最大値）※3

- L2 ループ検知フレーム送信レート算出式
  L2 ループ検知フレーム送信対象の VLAN ポート数÷ L2 ループ検知フレームの送信レート（pps）≦送信間隔（秒）

注※ 1
送信レートは上記の条件式に従って，自動的に 200pps 以内で変動します。

注※ 2
スパニングツリー，GSRP，Ring Protocol のどれかを使用している場合は，30pps 以下に設定してください。30pps より大きい場合，スパニングツリー，GSRP，Ring Protocol の正常動作を保障できません。

注※ 3
200pps 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。必ず 200pps 以下に設定してください。

（16）隣接装置情報（LLDP/OADP）

隣接装置情報（LLDP/OADP）の収容条件を次の表に示します。

表 2-51　隣接装置情報（LLDP/OADP）の収容条件

項目	最大収容数
LLDP 隣接装置情報	50
OADP 隣接装置情報	100

（17）IP アドレス

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について説明します。また，設定できる IP アドレスの最大数について説明します。

（a） IP アドレスを設定できるインタフェース数

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 との合計の値です。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 2-52　最大インタフェース数

モデル	インタフェース数（装置当たり）
全モデル共通	512

（b） 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。

(i) IPv4 の場合

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 2-53 マルチホームの最大サブネット数（IPv4 の場合）

モデル	マルチホーム サブネット数 （インタフェース当たり）
全モデル共通	256

(ii) IPv6 の場合

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，ここで示す値にはリンクローカルアドレスを含みます。一つのインタフェースには必ず一つのリンクローカルアドレスが設定されます。このため，すべてのインタフェースで IPv6 グローバルアドレスだけを設定した場合，実際に装置に設定される IPv6 アドレス数は，表の数値に自動生成される IPv6 リンクローカルアドレス数 1 を加算した 8 になります。

表 2-54 マルチホームの最大サブネット数（IPv6 の場合）

モデル	マルチホーム サブネット数 （インタフェース当たり）
全モデル共通	7

(c) IP アドレス最大設定数

(i) 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。なお，この表で示す値は，通信用インタフェースに設定できる IPv4 アドレス数です。

表 2-55 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

モデル	IPv4 アドレス数（装置当たり）
全モデル共通	512

(ii) 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する IPv6 アドレスの数です。また，IPv6 リンクローカルアドレスの数も含みます。一つのインタフェースには必ず一つの IPv6 リンクローカルアドレスが設定されます。このため，すべてのインタフェースに IPv6 グローバルアドレスを設定した場合，インタフェースには自動で IPv6 リンクローカルアドレスが付与され，実際に装置に設定される IPv6 アドレスの数は「表 2-57 コンフィグレーションで装置に設定できる IPv6 アドレス数と，装置に設定される IPv6 アドレス数の関係」に示す値となります。

表 2-56 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

モデル	IPv6 アドレス数（装置当たり）
全モデル共通	128

表 2-57　コンフィグレーションで装置に設定できる IPv6 アドレス数と，装置に設定される IPv6 アドレス数の関係

コンフィグレーションで設定する IPv6 アドレスの数		コンフィグレーションで設定する IPv6 アドレスの合計数	自動で設定する IPv6 リンクローカルアドレスの数	装置に設定される IPv6 アドレス数
IPv6 リンクローカルアドレス	IPv6 グローバルアドレス			
128(128 × 1)	0	128	0	128
0	128(128 × 1)	128	128	256

注　( ) 内数字の意味：
(A × B)　A：インタフェース数　B：各インタフェースに設定するアドレス数

(18) 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，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 2-58　ARP エントリの最大数

モデル	ARP エントリ数	
	インタフェース当たり	装置当たり
全モデル共通	3072(1024)	3072(1024)

注 1　(　) は，IPv4/IPv6 モードの場合のエントリ数を示します。
注 2　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 2-59　NDP エントリ数

モデル	NDP エントリ数	
	インタフェース当たり	装置当たり
全モデル共通	1024	1024

注　スタティック NDP は 128 個です。

(c) RA の最大相手端末数

RA ではルータから通知される IPv6 アドレス情報を基に端末でアドレスを生成します。本装置での最大相手端末数を次の表に示します。

表 2-60 RA の最大相手端末数

モデル略称	RA の最大相手端末数	
	インタフェース当たり	装置当たり
全モデル共通	128	128

(19) DHCP/BOOTP リレー

DHCP/BOOTP リレーで設定できるインタフェース数およびリレー先アドレス数を次の表に示します。

表 2-61 DHCP/BOOTP リレーの最大数

項目	最大数
DHCP/BOOTP リレーインタフェース数	128
DHCP/BOOTP リレー先アドレス数	16

(20) 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 2-62 DHCP サーバの最大数

項目	装置当たりの最大数
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※	2000
配布可能固定 IP アドレス数	160

注※ 配布可能固定 IP アドレス数を含みます。

(21) IPv6 DHCP サーバ

IPv6 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 IPv6 プレフィックス数などを次の表に示します。

表 2-63 IPv6 DHCP サーバの最大数

項目	装置当たりの最大数
インタフェース数	128
最大配布可能 Prefix 数	1024

(22) ルーティングリソース

(a) 最大隣接ルータ数

最大隣接ルータ数を次の表に示します。

表 2-64 最大隣接ルータ数

ルーティングプロトコル	最大隣接ルータ数
スタティックルーティング (IPv4,IPv6 の合計)	128 ※

ルーティングプロトコル	最大隣接ルータ数
RIP，OSPF，BGP4，RIPng，OSPFv3，BGP4+ の合計	50

注※
動的監視機能を使用する隣接ルータは，ポーリング間隔によって数が制限されます。詳細は，次の表を参照してください。

表 2-65　スタティックの動的監視機能を使用できる最大隣接ルータ数

ポーリング周期	動的監視機能を使用できる最大隣接ルータ数
1 秒	60
2 秒	120
3 秒	128

最大隣接ルータ数の定義を次の表に示します。

表 2-66　最大隣接ルータ数の定義

ルーティングプロトコル	定義
スタティックルーティング	ネクストホップ・アドレスの数
RIP	RIP が動作するインタフェース数
RIPng	RIPng が動作するインタフェース数
OSPF	OSPF が動作する各インタフェースにおける下記の総計 1. 該当インタフェースが指定ルータまたはバックアップ指定ルータになる場合 該当インタフェースと接続されるほかの OSPF ルータの数 2. 該当インタフェースが指定ルータまたはバックアップ指定ルータにならない場合 該当インタフェースと接続される指定ルータおよびバックアップ指定ルータの数 上記は，運用コマンド show ip ospf neighbor で表示される隣接ルータの状態 (State) が”Full”となる隣接ルータの数と同じ意味となります。
OSPFv3	OSPFv3 が動作する各インタフェースにおける下記の総計 1. 該当インタフェースが指定ルータまたはバックアップ指定ルータになる場合 該当インタフェースと接続されるほかの OSPFv3 ルータの数 2. 該当インタフェースが指定ルータまたはバックアップ指定ルータにならない場合 該当インタフェースと接続される指定ルータおよびバックアップ指定ルータの数 上記は，運用コマンド show ipv6 ospf neighbor で表示される隣接ルータの状態 (State) が”Full”となる隣接ルータの数と同じ意味となります。
BGP4	BGP4 ピア数
BGP4+	BGP4+ ピア数

(b) 経路エントリ数と最大隣接ルータ数の関係

最大経路エントリ数と最大隣接ルータ数の関係について，IPv4 モードの場合と IPv4/IPv6 モードの場合を次の表に示します。

表 2-67　経路エントリ数と最大隣接ルータ数の関係 (RIP，OSPF，BGP4)（IPv4 モード）

ルーティングプロトコル	最大経路エントリ数※1	最大隣接ルータ数※2
RIP	1000	50

ルーティングプロトコル	最大経路エントリ数※1	最大隣接ルータ数※2
OSPF※3	2000	50
	10000	10
BGP4	12288	50

注※1　最大経路エントリ数は代替経路を含みます。
注※2　各ルーティングプロトコル（RIP，OSPF，BGP4）を併用して使用する場合の最大隣接ルータ数は，各々 1/n（n：使用ルーティングプロトコル数）となります。
注※3　OSPF の最大経路エントリ数は LSA 数を意味します。

表 2-68　経路エントリ数と最大隣接ルータ数の関係 (RIP/RIPng，OSPF/OSPFv3，BGP4/BGP4+)（IPv4/IPv6 モード）

ルーティングプロトコル	最大経路エントリ数※1	最大隣接ルータ数※2
RIP	1000	50
RIPng	1000	50
OSPF※3	2000	50
	8000	12
OSPFv3※3	1000	50
	2000	25
BGP4	8192	50
BGP4+	2048	50

注※1　最大経路エントリ数は代替経路を含みます。
注※2　各ルーティングプロトコル（RIP，RIPng，OSPF，OSPFv3，BGP4，BGP4+）を併用して使用する場合の最大隣接ルータ数は，各々 1/n（n：使用ルーティングプロトコル数）となります。
注※3　OSPF/OSPFv3 の最大経路エントリ数は LSA 数を意味します。

(23) IPv4 マルチキャスト

IPv4 マルチキャストを設定できるインタフェース数およびルーティングテーブルのエントリ数を次の表に示します。本装置は IPv4 マルチキャストルーティングプロトコルとして PIM-SM または PIM-SSM をサポートします。PIM-SM と PIM-SSM は同時に動作できます。

表 2-69　IPv4 マルチキャストの最大数

項　目	最大数
PIM-SM/SSM マルチキャストインタフェース数※1※2	31 ／装置
IGMP 動作インタフェース数※1	127 ／装置
1 グループ当たりの送信元数	128 ／グループ
PIM-SM/SSM マルチキャスト経路情報のエントリ ((S,G) エントリ，(*,G) エントリ，およびネガティブキャッシュ) 数 S：送信元 IP アドレス G：グループアドレス※3	1024 ／装置

項　目	最大数
IGMPv2/IGMPv3（EXCLUDE モード）で PIM-SSM を連携動作させる設定数（ソース，グループのペア数）※ 4	256 ／装置
IGMPv3 で 1Report につき処理できる record 情報※ 5	32record ／メッセージ 32 ソース／ record
IGMP 加入グループ数※ 6	256 ／装置
マルチキャストルータ隣接数	32 ／装置
ランデブーポイント数	2 ／グループ
1 装置当たりランデブーポイントで設定できるグループ数	128 ／装置
1 システム当たりランデブーポイントで設定できる延べグループ数	128 ／システム
BSR 候補数	16 ／システム
静的グループ加入数※ 7	256 ／装置
静的ランデブーポイント（RP）ルータアドレス数	16 ／装置
インタフェース当たりの IGMP 加入グループ数※ 6	256 ／インタフェース
IGMP グループ当たりのソース数	128 ／グループ

注※ 1

マルチホームはサポートしていません。

注※ 2

PIM-SM/PIM-SSM として他ルータと隣接するインタフェース数。

注※ 3

IPv4 単独動作の場合です。IPv6 を同時に動作させる場合はエントリ数が 256 になります。また，次の条件を同時に満たす環境で PIM-SM を使用する場合，最大エントリ数は 128 になります。

- マルチキャストブロードバンド通信
- 本装置が first hop router またはランデブーポイント

また，本装置に設定された IP インタフェース数（マルチキャストインタフェース数ではない）によってもエントリ数が変わります。エントリ単位の入出力ポート数を全エントリ分合算したポート数が「表 2-73　IP インタフェース設定数に対するマルチキャスト入出力ポート数」に示す範囲内になるように使用してください。
1 エントリ内の入出力ポート数は，入出力インタフェースで同一のポートを使用している場合は 1 で数えます。例えば，入力インタフェースでポート 0/1 および 0/2，出力インタフェース 1 でポート 0/2，0/3 および 0/4，出力インタフェース 2 でポート 0/3，0/4 および 0/5 を使用している場合，該当するエントリの入出力ポート数は 5 となります。
IP インタフェース設定数が 64 の場合，1 エントリ当たりの平均入出力ポート数が 32 であれば 127 エントリまで，平均入出力ポート数が 16 であれば 255 エントリまで使用できます。

注※ 4

マルチキャストで使用するインタフェース数および加入グループ数によって設定できる数が変わります。「表 2-71　使用インタフェース数に対する IGMPv2/IGMPv3（EXCLUDE モード）で PIM-SSM を連動させる設定可能数」および「表 2-72　加入グループ数に対する IGMPv2/IGMPv3（EXCLUDE モード）で PIM-SSM を連動させる設定可能数」に示す範囲内で使用してください。加入グループ数は，動的および静的加入グループ数の総計です。同一グループアドレスが異なるインタフェースに加入している場合，加入グループ数は一つではなく，加入したインタフェースの数になり

ます。一つのIGMPv3（EXCLUDEモード）ReportでPIM-SSMを連携動作させる設定数は256になります。例えば，一つのIGMPv3（EXCLUDEモード）Report内に三つのrecordがあり，各recordに対応するPIM-SSMを連携動作させる設定数の合計が256を超えた場合，以降のrecordに対する本設定は無視します。

注※5

一つのReportメッセージで処理できるソース数はのべ256ソースまでです。ソース情報のないrecordも1ソースとして数えます。IGMPv3でのEXCLUDEモードでSSMに接続する設定をした場合，受信したReportメッセージ内のrecordのソース数がのべ256を超えた以降のrecordは無視します。

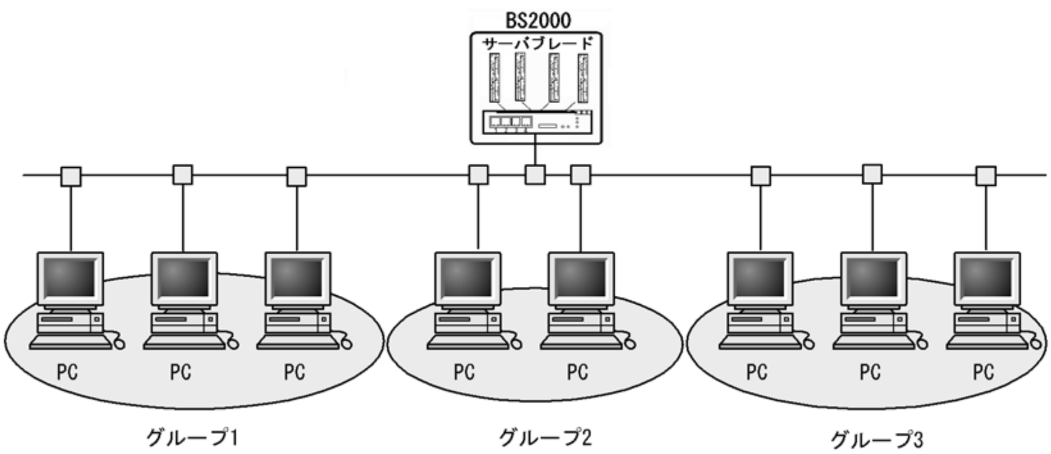
例えば，IGMPv3 EXCLUDEモードでSSMに接続する設定をマスク指定で1グループに対し256ソースを設定した場合，次のようになります。

1. 受信したIGMPv3 Reportメッセージ内の先頭からこの設定に一致する二つのEXCLUDEのrecordが存在した場合，2record目以降を無視します。
2. 受信したIGMPv3 Reportメッセージ内に1ソースのINCLUDEのrecordがあり，この設定に一致するグループのEXCLUDEが1recordあっても，無視します。

注※6

本装置に直接接続しているグループの数を示します。IGMPv3使用時に送信元を指定する場合のグループ数は，送信元とグループの組み合わせの数となります。「図2-1　マルチキャストグループ数の例」の例では3です。インタフェース当たりの加入可能グループ数については，「表2-70　IPv4でのインタフェース当たりの加入可能グループ数」を参照してください。

図2-1　マルチキャストグループ数の例



注※7

静的グループ加入数とは，各マルチキャストインタフェースで静的加入するグループアドレスの総数です。同一グループアドレスを複数の異なるインタフェースに静的加入設定した場合，静的グループ加入数は一つではなく，静的加入設定したインタフェースの数になります。一つのインタフェースに設定できる静的グループ加入数は256までです。

表 2-70　IPv4 でのインタフェース当たりの加入可能グループ数

使用インタフェース数	インタフェース当たりの加入可能グループ数
31	256
63	128
127	64

表 2-71　使用インタフェース数に対する IGMPv2/IGMPv3（EXCLUDE モード）で PIM-SSM を連動させる設定可能数

使用インタフェース数	IGMPv2/IGMPv3（EXCLUDE モード）で PIM-SSM を連動させる設定可能数
31	256
63	128
127	64

表 2-72　加入グループ数に対する IGMPv2/IGMPv3（EXCLUDE モード）で PIM-SSM を連動させる設定可能数

加入グループ（延べ数）	IGMPv2/IGMPv3（EXCLUDE モード）で PIM-SSM を連動させる設定数
64	256
128	128
256	64
512	32
1024	16
2048	8
4096	4
8128	2

表 2-73　IP インタフェース設定数に対するマルチキャスト入出力ポート数

装置に設定された IP インタフェース数	エントリ単位の入出力ポート数を全エントリ分合算したポート数
	全モデル共通
64 以下	4095
65 ～ 128	2047
129 ～ 192	1365
193 ～ 256	1023
257 ～ 320	819
321 ～ 384	682
385 ～ 448	585
449 ～ 512	511

(24) IPv6 マルチキャスト

IPv6 マルチキャストを設定できるインタフェース数およびルーティングテーブルのエントリ数を次の表に示します。本装置は IPv6 マルチキャストルーティングプロトコルとして PIM-SM および PIM-SSM をサポートしています。PIM-SM と PIM-SSM は同時に動作できます。

表 2-74　IPv6 マルチキャストエントリ最大数

項　目	最大数
PIM-SM/SSM マルチキャストインタフェース数※ 1 ※ 2	31 ／装置
MLD 動作インタフェース数※ 1	127 ／装置
1 グループ当たりの送信元数	128 ／グループ
PIM-SM/SSM マルチキャストルーティングエントリ ((S,G) エントリ，(*,G) エントリ，およびネガティブキャッシュ) 数 S : 送信元 IP アドレス G : グループアドレス※ 3	128 ／装置
MLDv1/MLDv2（EXCLUDE モード）で PIM-SSM を連携動作させる設定数	256 ／装置
MLDv2 で 1Report に対し処理できる record 情報※ 4	32record ／メッセージ 32 ソース／ record
MLD 加入グループ数※ 5	256 ／装置
マルチキャストルータ隣接数	32 ／装置
ランデブーポイント数	1 ／グループ
1 装置当たりランデブーポイントで設定できるグループ数	128 ／装置
1 システム当たりランデブーポイントで設定できる延べグループ数	128 ／システム
BSR 候補数	1 ／システム
静的グループ加入数※ 5	256 ／装置
静的ランデブーポイント（RP）ルータアドレス数	16 ／装置
インタフェース当たりの MLD 加入グループ数※ 5	256 ／インタフェース
MLD グループ当たりのソース数	256 ／グループ
遠隔のマルチキャストサーバアドレスを直接接続サーバとして扱う設定数	256 ／装置 16 ／インタフェース

注※ 1

マルチホームをサポートする。

注※ 2

PIM-SM/PIM-SSM として他ルータと隣接するインタフェース数。

注※ 3

IPv4 と同時動作させた場合です。IPv6 単独では動作できません。
また，本装置に設定された IP インタフェース数（マルチキャストインタフェース数ではない）によってもエントリ数が変わります。エントリ単位の入出力ポート数を全エントリ分合算したポート数が「表 2-73　IP インタフェース設定数に対するマルチキャスト入出力ポート数」に示す範囲内になるように使用してください。
なお，IPv4 と IPv6 を同時動作させた場合は IPv4 と IPv6 のエントリの合計となります。
1 エントリ内の入出力ポート数は，入出力インタフェースで同一のポートを使用している場合は 1 で

数えます。例えば，入力インタフェースでポート 0/1 および 0/2，出力インタフェース 1 でポート 0/2，0/3 および 0/4，出力インタフェース 2 でポート 0/3，0/4 および 0/5 を使用している場合，該当するエントリの入出力ポート数は 5 となります。

IP インタフェース設定数が 64 の場合，1 エントリ当たりの平均入出力ポート数が 32 であれば 127 エントリまで，平均入出力ポート数が 16 であれば 255 エントリまで使用できます。

注※ 4

一つの Report メッセージで処理できるソース数はのべ 1024 ソースまでです。ソース情報のないレコードも 1 ソースとして数えます。

MLDv2 での EXCLUDE モードで SSM に接続する設定をした場合，受信した Report メッセージ内の record のソース数がのべ 1024 を超えた以降の record は無視します。

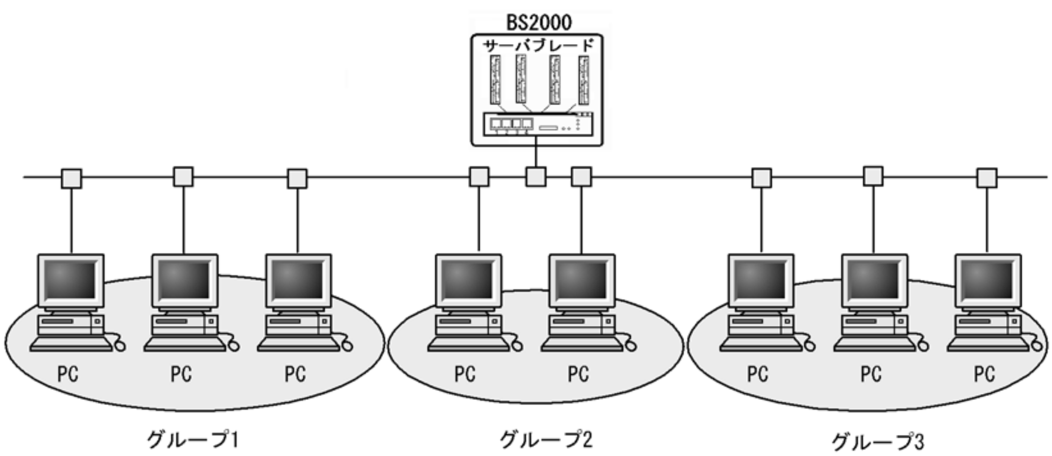
例えば，MLDv2 EXCLUDE モードで SSM に接続する設定をマスク指定で 1 グループに対し 256 ソースの設定をした場合，次のようになります。

1. 受信した MLDv2 Report メッセージ内の先頭からこの設定に一致する二つの EXCLUDE の record が存在した場合，5record 目以降を無視します。
2. 受信した MLDv2 Report メッセージ内に 1 ソースの INCLUDE の record があり，この設定に一致するグループの EXCLUDE が 4record あった場合，4record 目以降から無視します。

注※ 5

本装置に直接接続しているグループの数を示します。MLDv2 使用時に送信元を指定する場合のグループ数は，送信元とグループの組み合わせの数となります。「図 2-2　マルチキャストグループ数の例」の例では 3 です。インタフェース当たりの加入可能グループ数については，「表 2-75　IPv6 でのインタフェース当たりの加入可能グループ数」を参照してください。

図 2-2　マルチキャストグループ数の例



注※ 6

静的グループ加入数とは，各マルチキャストインタフェースで静的加入するグループアドレスの総数です。同一グループアドレスを複数の異なるインタフェースに静的加入設定した場合，静的グループ加入数は一つではなく，静的加入設定したインタフェースの数になります。一つのインタフェースに設定できる静的グループ加入数は 256 までです。

表 2-75　IPv6 でのインタフェース当たりの加入可能グループ数

使用インタフェース数	インタフェース当たりの加入可能グループ数
31	256
63	128
127	64

(25) 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

(a) IPv4 機能を使用する場合

IPv4 機能を使用する場合の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。ダイナミックエントリとスタティックエントリの合計値が，最大装置エントリ数を超えないようにしてください。

表 2-76　ダイナミック・スタティック最大エントリ数

分類	項　目	最大装置エントリ数	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	12288	12288	2048※
	マルチキャスト経路エントリ	1024	1024	−

（凡例）－：未サポート
注※　コンフィグレーションで設定できる行数です。

(b) IPv4 機能と IPv6 機能を併用する場合

IPv4 機能と IPv6 機能を併用する場合の，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。

表 2-77　ダイナミック・スタティック最大エントリ数

分類	項　目	最大装置エントリ数	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	8192	8192	2048※
	マルチキャスト経路エントリ	256	256	−
IPv6	ユニキャスト経路エントリ	2048	2048	2048※
	マルチキャスト経路エントリ	128	128	−

（凡例）－：未サポート
注※　コンフィグレーションで設定できる行数です。

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

3.1.1 運用端末

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 RS232C に接続する端末，リモート運用端末は IP ネットワーク経由で接続する端末です。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。運用端末の接続形態を「図 3-1　運用端末の接続形態」に，運用端末の条件を「表 3-1　運用端末の条件」に示します。

図 3-1　運用端末の接続形態

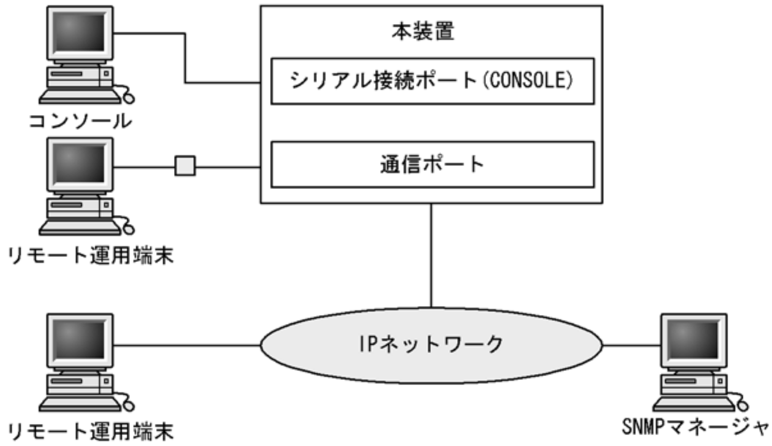


表 3-1　運用端末の条件

端末種別	接続形態	必要機能
コンソール	シリアル接続（RS232C）	RS232C(回線速度：19200，9600，4800，2400，1200) ZMODEM 手順
リモート運用端末	通信用ポート接続	TCP/IP telnet ftp

(1) コンソール

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 VT-100 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：9600bps
- 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 9600bps 以外（1200 ／ 2400 ／ 4800 ／ 19200bps）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。ただし，実際に設定が反映されるのはコンソールからいったんログアウトしたあとになります。

図 3-2　コンソールの通信速度の設定例

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

注意事項

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 VT-100 の制御文字を使用して画面サイズを取得・設定します。VT-100 に対応していないコンソール端末では，不正な文字列が表示されたり，最初の CLI プロンプトがずれて表示されたりして，画面サイズが取得・設定できません。
また，ログインと同時にキー入力した場合，VT-100 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。

（2） リモート運用端末

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リモート運用端末として使用できます。

注意事項

本装置の telnet サーバは，改行コードとして [CR] を認識します。一部のクライアント端末では，改行コードとして [CR] および [LF] を送信します。これらの端末から接続した場合，空行が表示されたり，（y/n）確認時にキー入力ができなかったりするなどの現象がおこります。このような場合は，各クライアント端末の設定を確認してください。

3.1.2　運用端末の接続形態

運用端末の接続形態ごとの特徴を次の表に示します。

表 3-2　運用端末の接続形態ごとの特徴

運用機能	シリアル	通信用ポート
接続運用端末	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	zmodem 手順	ftp
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

（1） シリアル接続ポート

シリアル接続ポートには運用端末としてコンソールを接続します。コンフィグレーションの設定なしに本ポートを介してログインできるので，初期導入時には本ポートからログインし，初期設定を行えます。

（2） 通信用ポート

通信用ポートを介して，遠隔のリモート運用端末からの本装置に対するログインや SNMP マネージャによるネットワーク管理ができます。このポートを介して telnet や ftp によって本装置へログインするためには，本装置のコンフィグレーションで IP アドレスおよびリモートアクセスの設定をする必要があります。

3.1.3 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	リモート操作コマンドなどをサポートします。
ログ・統計情報	過去に発生した障害情報および回線使用率などの統計情報を表示します。
LED および障害部位の表示	LED 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。

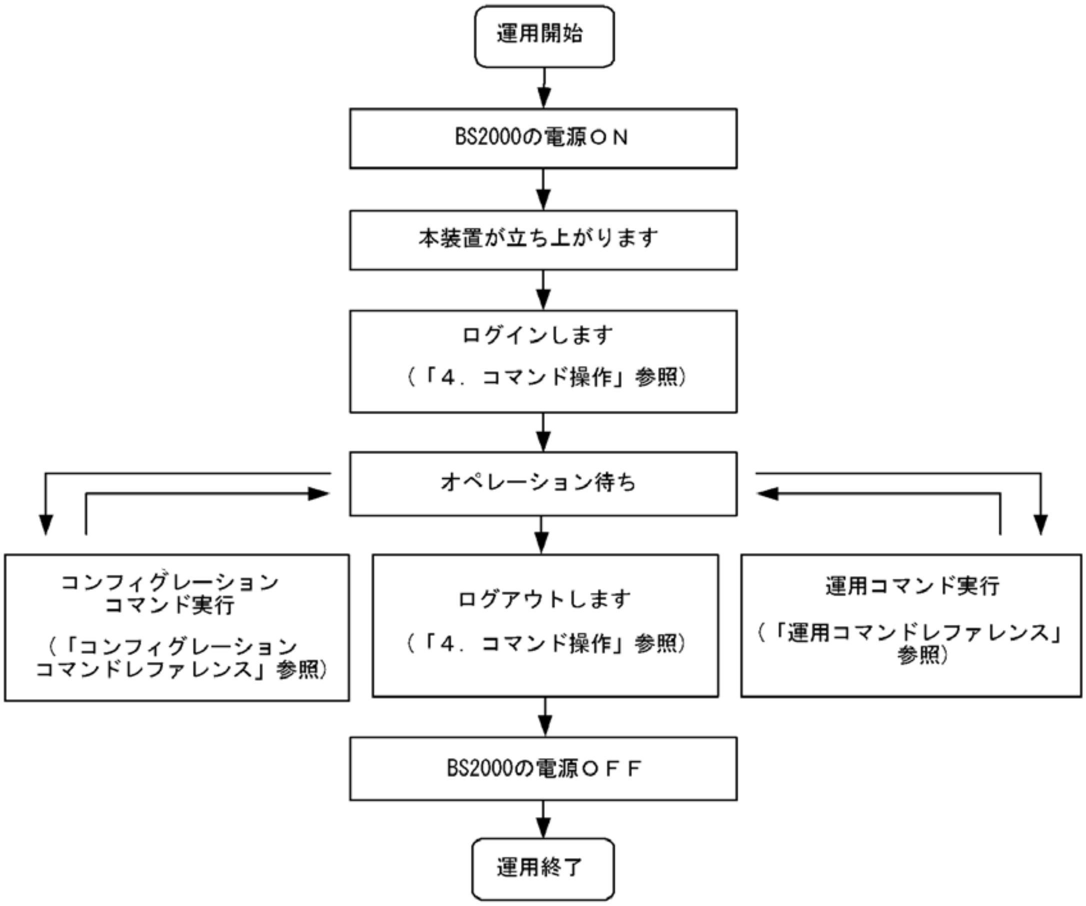
3.2　装置起動

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　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，BS2000 装置添付のマニュアル「BladeSymphony ユーザーズガイド」を参照してください。

図 3-3　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	本装置の電源 OFF からの立ち上げです。	BS2000 の電源スイッチを ON にします。
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。	reload コマンドを実行します。

起動の種類	内容	操作方法
デフォルトリスタート	パスワードを忘れた場合に行います。 パスワードによるセキュリティチェックを行いませんのでデフォルトリスタートによる起動を行う場合は十分に注意してください。なお，アカウント，コンフィグレーションはデフォルトリスタート前のものが使用されます。 また，ログインユーザ名を忘れると，デフォルトリスタートで起動してもログインできないので注意してください。 デフォルトリスタート中に設定したパスワードは，装置再起動後に有効になります。	本体のリセットスイッチを 5 秒以上押します。

BS2000 の電源スイッチを ON にするとことで，連動して本装置が起動します。本装置を起動，再起動したときに STATUS ランプ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 ランプ表示内容の詳細は，BS2000 装置添付のマニュアル「BladeSymphony ユーザーズガイド」を参照してください。

3.2.3　装置の停止

本装置の電源を OFF にする場合は，BS2000 の電源スイッチを OFF にします。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。運用コマンド reload stop で装置を停止させたあとに電源を OFF にすることを推奨します。

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。この画面でユーザ名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，ユーザ名 operator でパスワードなしでログインができます。

図 3-4　ログイン画面

```
login: operator
Password: *******                                                     …1
Copyright (c) 2005-2009 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表示しません。
   また，パスワードの入力文字は表示しません。
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 3-5　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コンフィグレーションコマンド username，または運用コマンド 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およびユーティ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 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。
quit	現在のコマンド入力モードを終了します。
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。
diff	指定した二つのファイル同士を比較し，相違点を表示します。
grep	指定したファイルを検索して，指定したパターンを含む行を出力します。
more	指定したファイルの内容を一画面分だけ表示します。
less	指定したファイルの内容を一画面分だけ表示します。
sort	指定したファイルのすべての行をソートし，結果を表示します。
tail	指定したファイルの指定された位置以降を出力します。
hexdump	ヘキサダンプを表示します。

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，adduser 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)#

注※

コンフィグレーションの編集中に運用コマンドを実行したい場合，quit コマンドや exit コマンドによってコマンド入力モードを装置管理者モードに切り替えなくても，運用コマンドの先頭に「$」を付けた形式で入力することで実行できます。

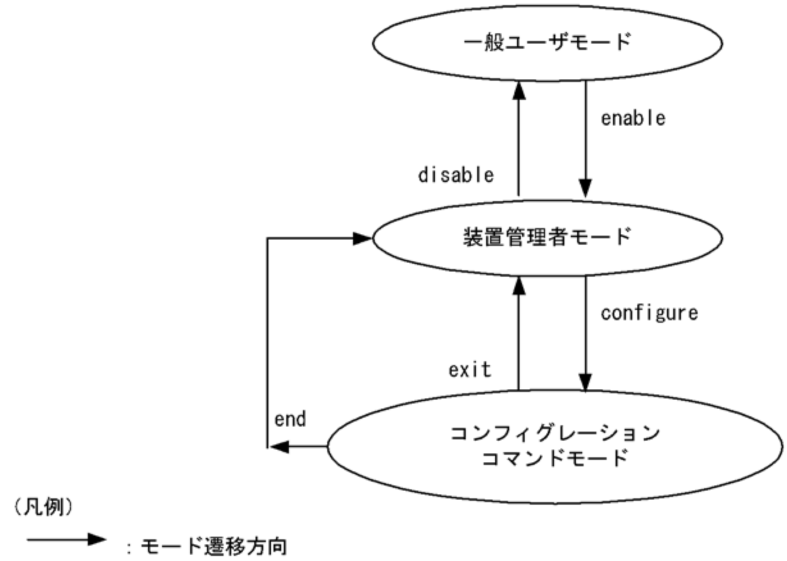
＜例＞

コンフィグレーションコマンドモードで運用コマンド show ip arp を実行する場合

```
(config)# $show ip arp
```

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がプロンプトの先頭に表示されます。

1. コンフィグレーションコマンド hostname でホスト名称を設定している場合，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)# save
OFFICE1(config)# quit
OFFICE1# quit
OFFICE1>
```

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 4-3 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］押下で使用できるパラメータやファイル名の一覧が表示されます。

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

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 4-4 ［?］入力時の表示例

```
> show vlan ?
  <vlan id list>        1 to 4094 ex. "5", "10-20" or "30,40"
  channel-group-number  Display the VLAN information specified by
                        channel-group-number
  detail                Display the detailed VLAN information
  list                  Display the list of VLAN information
  mac-vlan              Display the MAC VLAN information
  port                  Display the VLAN information specified by port number
  summary               Display the summary of VLAN information
  <cr>
> show vlan
```

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。また，コマンドパラメータで ? 文字を使用する場合は，［Ctrl］＋［V］を入力後，［?］を入力してください。

4.2.3 入力エラー位置指摘機能

コマンドまたはパラメータを不正に入力した際，エラー位置を「ˆ」で指摘し，次行にエラーメッセージ（マニュアル「運用コマンドレファレンス Vol.1　入力エラー位置指摘で表示するメッセージ」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。

「ˆ」の指摘個所と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。入力エラー位置指摘の表示例を「図 4-5　スペルミスをしたときの表示例」および「図 4-6　パラメータ入力途中の表示例」に示します。

図 4-5　スペルミスをしたときの表示例

```
(config)# interface gigabitehternet 0/1
interface gigabitehternet 0/1
                  ^
% illegal parameter at '^' marker
(config)# interface gigabitehternet 0/1
```

図 4-6　パラメータ入力途中の表示例

```
(config)# interface gigabitethernet 0/1
(config-if)# speed
speed
      ^
% Incomplete command at '^' marker
(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 4-7　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 2009/11/15 19:37:02 UTC
Total: 1 entries
 IP Address       Linklayer Address  Netif             Expire     Type
 192.168.0.1      0012.e2d0.e9f5     VLAN0010          3h44m57s   arpa
>
```

なお，「表 6-1　コンフィグレーションコマンド一覧」にあるコンフィグレーションの編集および操作に関するコマンドは，コンフィグレーションモードの第一階層以外で短縮実行できません。

また，* を含むパラメータを指定した場合は，それ以降のパラメータについて短縮実行できません。

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 4-8　ヒストリ機能を使用したコマンド入力の簡略化

```
> ping 192.168.0.1 numeric count 1                          …1
PING 192.168.0.1 (192.168.0.1): 56 data bytes
64 bytes from 192.168.0.1: icmp_seq=0 ttl=31 time=1.329 ms

--- 192.168.0.1 PING Statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max = 1.329/1.329/1.329 ms
>                                                           …2
> ping 192.168.0.1 numeric count 1                          …3
PING 192.168.0.1 (192.168.0.1): 56 data bytes
64 bytes from 192.168.0.1: icmp_seq=0 ttl=31 time=1.225 ms

--- 192.168.0.1 PING Statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max = 1.225/1.225/1.225 ms
>                                                           …4
> ping 192.168.0.2 numeric count 1                          …5
PING 192.168.0.2 (192.168.0.2): 56 data bytes

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

1. 192.168.0.1 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 192.168.0.1 numeric count 1」が表示されるので，［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. 192.168.0.1 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 192.168.0.1 numeric count 1」が表示されるので，IP アドレスの「1」の部分を「2」に変更して［Enter］キーを入力しています。
5. 192.168.0.2 に対して ping コマンドを実行します。

ヒストリ機能に次の表に示す文字列を使用した場合，コマンド実行前に過去に実行したコマンド文字列に変換したあとにコマンドを実行します。なお，コンフィグレーションコマンドでは，コマンド文字列変換はサポートしていません。

表 4-3　ヒストリのコマンド文字列変換で使用できる文字一覧

項番	指定	説明
1	!!	直前に実行したコマンドへ変換して実行します。
2	!n	ヒストリ番号 n※のコマンドへ変換して実行します。
3	!-n	n 回前のコマンドへ変換して実行します。
4	!str	文字列 str で始まる過去に実行した最新のコマンドへ変換して実行します。
5	^str1^str2	直前に実行したコマンドの文字列 str1 を str2 に置換して実行します。

注※
　運用コマンド show history で表示される配列番号のこと。

注意
　通信ソフトウェアによって方向キー（［↑］，［↓］，［←］，［→］）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　パイプ機能

パイプ機能を利用することによって，コマンドの実行結果を別のコマンドに引き継ぐことができます。実行結果を引き継ぐコマンドに grep コマンドや sort コマンドを使うことによって，コマンドの実行結果をよりわかりやすくすることができます。「図 4-9　show sessions コマンド実行結果」に show sessions コマンドの実行結果を，「図 4-10　show sessions コマンド実行結果を grep コマンドでフィルタリング」に show sessions コマンドの実行結果を grep コマンドでフィルタリングした結果を示します。

図 4-9　show sessions コマンド実行結果

```
> show sessions
operator console  ----- 0  Jan 6 14:16
operator ttyp0    ----- 1  Jan 6 14:16(192.168.3.7)
operator ttyp1    ----- 2  Jan 6 14:16(192.168.3.7)
operator ttyp2    admin 3  Jan 6 14:16(192.168.3.7)
```

図 4-10　show sessions コマンド実行結果を grep コマンドでフィルタリング

```
> show sessions | grep admin
operator ttyp2    admin 3  Jan 6 14:16(192.168.3.7)
>
```

4.2.7　リダイレクト

リダイレクト機能を利用することによって，コマンドの実行結果をファイルに出力できます。show interfaces コマンドの実行結果をファイルに出力する例を次の図に示します。

図 4-11　show interfaces コマンド実行結果をファイルに出力

```
> show interfaces nif 0 line 1 > show_interface.log
>
```

4.2.8　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。ただし，リダイレクトがあるときにはページングを行いません。なお，ページングはコンフィグレーションコマンド username，または運用コマンド 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。

4.2.9　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。
ヘルプ機能	ヘルプメッセージで表示するコマンドの一覧を設定できます。 初期導入時のデフォルト設定は，運用コマンドのヘルプメッセージを表示する際に，入力可能なすべての運用コマンドの一覧を表示します。

これらの CLI 環境情報は，ユーザごとに，コンフィグレーションコマンド username，または次に示す運用コマンドで設定できます。

- set exec-timeout
- set terminal pager
- set terminal help

コンフィグレーションコマンド username による設定は，運用コマンドによる設定よりも優先されます。三つの CLI 環境情報のうち，どれか一つでもコンフィグレーションコマンドで設定した場合，その対象ユーザには，運用コマンドによる設定値は使用されません。コンフィグレーションコマンドの設定値または省略時の初期値で動作します。

運用コマンドによる設定は，コンフィグレーションコマンドによる設定がない場合に使用されます。コンフィグレーションコマンドで一つも CLI 環境情報を設定していないユーザは，運用コマンドによる設定値が使用されます。なお，運用コマンドによる設定では，設定状態を表示できないため，各機能の動作状態で確認してください。

運用コマンドによる設定内容は，コマンド実行直後から動作に反映されます。さらに，コンフィグレーションコマンドによる設定で動作している場合でも，一時的に該当セッションでの動作を変更できます。

なお，運用コマンドによる設定の場合，adduser コマンドで no-mc 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

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つか，再度ログインし直して，ログインしたままの状態になっているユーザを運用コマンド killuser で削除してください。

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

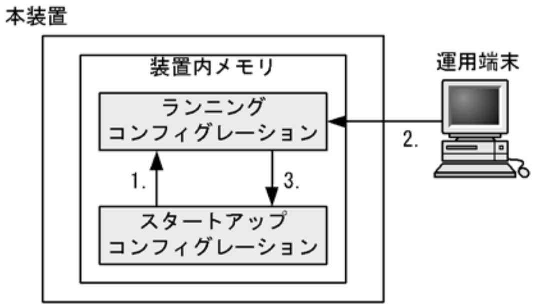
運用開始時または運用中，ネットワークの運用環境に合わせて，本装置に接続するネットワークの構成および動作条件などのコンフィグレーションを設定する必要があります。初期導入時，コンフィグレーションは設定されていません。

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，装置内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 save(write) コマンドを使用することで，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，装置内メモリのスタートアップコンフィグレーションが読み出され，ランニングコンフィグレーションとしてロードされる。ランニングコンフィグレーションの内容で運用を開始する。
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る。
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に保存する。

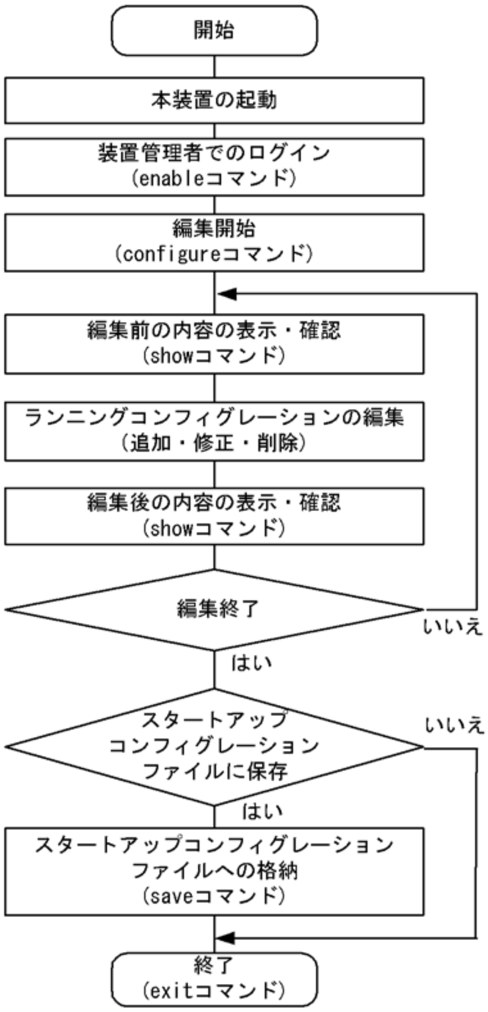
5.1.2 運用中のコンフィグレーション

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。save(write) コマンドを使用することで，ランニングコンフィグレーションが装置内メモリにあるスタートアップコンフィグレーションに保存されます。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

グローバルコンフィグモード（第一階層）	モード遷移コマンド	コンフィグモード（第二階層）	モード遷移コマンド	コンフィグモード（第三階層）
config	vlan	config-vlan		
	spanning-tree mst configuration	config-mst		
	interface loopback	config-if		
	interface port-channel	config-if		
	interface gigabitethernet	config-if		
	interface range gigabitethernet	config-if-range		
	interface tengigabitethernet	config-if		
	interface range tengigabitethernet	config-if-range		
	interface vlan	config-if		
	interface range vlan	config-if-range		
	axrp	config-axrp		
	gsrp	config-gsrp		
	router rip	config-router		
	router ospf	config-router		
	router bgp	config-router	address-family ipv6	config-router-af
	ipv6 router rip	config-rtr-rip		
	ipv6 router ospf	config-rtr		
	ip access-list standard	config-std-nacl		
	ip access-list extended	config-ext-nacl		
	ipv6 access-list	config-ipv6-acl		
	mac access-list extended	config-ext-macl		
	route-map	config-route-map		
	ip qos-flow-list	config-ip-qos		
	ipv6 qos-flow-list	config-ipv6-qos		
	mac qos-flow-list	config-mac-qos		
	ip dhcp pool	dhcp-config		
	ipv6 dhcp pool	config-dhcp		
	line console	config-line		
	line vty	config-line		
	parser view	config-view		
	auto-config	config-auto-cf		
	netconf	config-netconf		

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。
quit(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。
status	編集中のコンフィグレーションの状態を表示します。
top	コンフィグレーションコマンドモード（第二階層以下）からグローバルコンフィグモード（第一階層）に戻ります。

コンフィグレーションの編集および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を表示します。
copy	コンフィグレーションをコピーします。
erase configuration	ランニングコンフィグレーションの内容を初期導入時のものに戻します。
show file	ローカルまたはリモートサーバ上のファイルの内容と行数を表示します。
cd	現在のディレクトリ位置を移動します。
pwd	カレントディレクトリのパス名を表示します。
ls	ファイルおよびディレクトリを表示します。
dir	復元可能な形式で削除された本装置用のファイルの一覧を表示します。
cat	指定されたファイルの内容を表示します。
cp	ファイルをコピーします。
mkdir	新しいディレクトリを作成します。
mv	ファイルの移動およびファイル名の変更をします。
rm	指定したファイルを削除します。
rmdir	指定したディレクトリを削除します。
delete	本装置用のファイルを復元可能な形式で削除します。
undelete	復元可能な形式で削除された本装置用のファイルを復元します。
squeeze	復元可能な形式で削除された本装置用の deleted ファイルを完全に消去します。
chmod	指定されたファイルやディレクトリのアクセス権を変更します。
zmodem	本装置と RS232C で接続されているコンソールとの間でファイル転送をします。

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，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

```
OFFICE01# show running-config                 …1
#default configuration file for XXXXXX-XX
!
hostname "OFFICE01"
!
vlan 1
  name "VLAN0001"
!
vlan 100
  state active
!
vlan 200
  state active
!
interface gigabitethernet 0/1
  switchport mode access
  switchport access vlan 100
!
interface gigabitethernet 0/2
  switchport mode access
  switchport access vlan 200
!
OFFICE01#
```

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。

図 5-6　コンフィグレーションの内容をすべて表示

```
OFFICE01(config)# show                 …1
#default configuration file for XXXXXX-XX
!
hostname "OFFICE01"
!
vlan 1
  name "VLAN0001"
!
vlan 100
  state active
!
vlan 200
  state active
!
interface gigabitethernet 0/1
  switchport mode access
  switchport access vlan 100
!
interface gigabitethernet 0/2
  switchport mode access
  switchport access vlan 200
!
OFFICE01(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　設定済みのすべてのインタフェース情報を表示

```
OFFICE01(config)# show interface gigabitethernet        …1
interface gigabitethernet 0/1
  switchport mode access
  switchport access vlan 100
!
interface gigabitethernet 0/2
  switchport mode access
  switchport access vlan 200
!
OFFICE01(config)#
```

1. ランニングコンフィグレーションのうち，設定済みのすべてのインタフェースを表示します。

図 5-8　指定のインタフェース情報を表示

```
OFFICE01(config)# show interface gigabitethernet 0/1       …1
!
interface gigabitethernet 0/1
  switchport mode access
  switchport access vlan 100
!
OFFICE01(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 0/1 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

```
OFFICE01(config)# interface gigabitethernet 0/1
OFFICE01(config-if)# show                                 …1
interface gigabitethernet 0/1
  switchport mode access
  switchport access vlan 100
OFFICE01(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 0/1 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 0/1             …3
(config-if)# switchport mode access                 …4
(config-if)# switchport access vlan 100             …5
(config-if)# exit
(config)#
(config)# vlan 100                                  …6
(config-vlan)# state suspend                        …7
(config-vlan)# exit
(config)#
(config)# interface gigabitethernet 0/1             …8
(config-if)# no switchport access vlan              …9
```

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 0/1 にモードを遷移します。
4. ポート 0/1 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 0/1 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)# no ip domain lookup                          …1
(config)# ip domain name router.mydomain.co.jp         …2
(config)# ip name-server 192.168.0.1                   …3
(config)# ip domain lookup                             …4
```

1. DNS リゾルバ機能を無効にします。
2. ドメイン名を router.mydomain.co.jp に設定します。
3. ネームサーバを 192.168.0.1 に設定します。
4. DNS リゾルバ機能を有効にします。

(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が表示されて，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が表示されます。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 0/1
(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 tengigabitethernet 0/1
(config-if)# description
description
            ^
% Incomplete command at '^' marker
(config-if)#
```

5.4.5　コンフィグレーションの運用への反映

コンフィグレーションの変更は，コンフィグレーションコマンドの入力を契機に即時に運用に反映されます。ただし，BGP に関するフィルタ設定の変更内容を運用に反映する場合は，運用コマンド clear ip bgp を実行する必要があります。

運用コマンド clear ip bgp を使用すると，次に示すコマンドで変更した内容を運用に反映できます。

- access-list コマンド
- prefix-list コマンド
- route-map コマンド
- distribute-list in コマンド
- distribute-list out コマンド
- redistribute コマンド
- neighbor in コマンド
- neighbor out コマンド

コマンドの入力例を次の図に示します。

図 5-14　コマンド入力例

```
(config)# ip access-list standard 1  ............................(1)
(config-std-nacl)# permit 10.0.0.0 0.255.255.255  ................(2)
(config-std-nacl)# permit 172.16.0.0 0.0.255.255  ................(3)
(config-std-nacl)# exit
(config)# ip prefix-list PEER-OUT seq 10 permit 172.16.1.0/24  ...(4)
(config)# route-map SET-COMM 10  .................................(5)
(config-route-map)# match ip address prefix-list PEER-OUT  .......(6)
(config-route-map)# set community no-export  .....................(7)
(config-route-map)# exit
(config)# router bgp 65530
(config-router)# distribute-list 1 in  ...........................(8)
(config-router)# redistribute static  ............................(9)
(config-router)# neighbor 192.168.1.1 remote-as 65531
(config-router)# neighbor 192.168.1.2 remote-as 65532
(config-router)# neighbor 192.168.1.2 send-community
(config-router)# neighbor 192.168.1.2 route-map SET-COMM out  ....(10)
(config-router)# exit
(config)# save
(config)# exit
# clear ip bgp * both                                            …1
```

1. (1) ～ (10) の変更内容が運用に使用されます。

5.4.6　コンフィグレーションのファイルへの保存（save コマンド）

save(write) コマンドを使用することで，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 5-15　コンフィグレーションの保存例

```
# 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。

5.4.7　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モードで exit コマンドを実行します。コンフィグレーションを編集したあと，save コマンドで変更後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へ保存していない場合は，exit コマンドを実行すると確認のメッセージが表示されます。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ないでコンフィグレーションコマンドモードを終了する場合は「y」を入力してください。「y」以外が入力されるとコンフィグレーションコマンドモードを終了できません。コンフィグレーションの編集終了例を「図 5-16　コンフィグレーションの編集終了例」と「図 5-17　変更内容を保存しない場合のコンフィグレーションの編集終了例」に示します。

図 5-16　コンフィグレーションの編集終了例

```
!(config)# save
(config)# exit              …1
```

1. 編集を終了します。

図 5-17　変更内容を保存しない場合のコンフィグレーションの編集終了例

```
# configure                                                             …1
(config)#
       :
       :                                                                …2
       :
!(config)# exit
Unsaved changes found! Do you exit "configure" without save ? (y/n): y …3
!#
```

1. 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. 確認メッセージが表示されます。

5.4.8　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

設定されたコンフィグレーションはメモリに保持されるため，設定できるコンフィグレーションのコマンド数はメモリ量によって決まります。設定するコンフィグレーションに比べてメモリ量が少なかったり，制限を超えるようなコンフィグレーションを編集したりした場合は，「Maximum number of entries are already defined (config memory shortage). <IP>」または「Maximum number of entries are already defined.<IP>」のメッセージが表示されます。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，一度に入力できる文字数は約 1000 文字（スペース，改行を含む）です。1000 文字以上を一度にペーストすると正しくコンフィグレーションを設定できない状態になるので注意してください。

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　コンフィグレーションのバックアップ

運用コマンド copy を使用することで，コンフィグレーションをリモートサーバや本装置上にバックアップすることができます。ただし，本装置にバックアップ用のコンフィグレーションファイルを格納する場合，スタートアップコンフィグレーションファイルの格納ディレクトリ（/config）は指定できません。バックアップ用のコンフィグレーションファイルはログインユーザのホームディレクトリに作成してください。

バックアップできるコンフィグレーションは，スタートアップコンフィグレーションとランニングコンフィグレーションの 2 種類です。運用中にコンフィグレーションを変更し保存していない場合は，スタートアップコンフィグレーションをバックアップしても，バックアップしたコンフィグレーションファイルの内容は運用中のコンフィグレーションと異なります。それぞれのバックアップ例を次の図に示します。

図 5-18　スタートアップコンフィグレーションのバックアップ例

```
> enable
# copy startup-config ftp://staff@[2001:240:400::101]/backup.cnf
Configuration file copy to ftp://staff@[2001:240:400::101]/backup.cnf?
(y/n): y

Authentication for 2001:240:400::101.
User: staff
Password: xxx                              …1
transferring…

Data transfer succeeded.
#
```

1. リモートサーバ上のユーザ staff のパスワードを入力します。

図 5-19　ランニングコンフィグレーションのバックアップ例

```
> enable
# copy running-config ftp://staff@[2001:240:400::101]/backup.cnf
Configuration file copy to ftp://staff@[2001:240:400::101]/backup.cnf?
(y/n): y

Authentication for 2001:240:400::101.
User: staff
Password: xxx                              …1
transferring…

Data transfer succeeded.
#
```

1. リモートサーバ上のユーザ staff のパスワードを入力します。

5.5.2　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反映

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またはランニングコンフィグレーションに反映する場合は，運用コマンド copy を使用します。それぞれの反映例を次の図に示します。

図 5-20　スタートアップコンフィグレーションへの反映例

```
> enable
# copy ftp://staff@[2001:240:400::101]/backup.cnf startup-config
Configuration file copy to startup-config?
(y/n): y

Authentication for 2001:240:400::101.
User: staff
Password: xxx                              …1
transferring…

Data transfer succeeded.
#
```

1. リモートサーバ上のユーザ staff のパスワードを入力します。

図 5-21　ランニングコンフィグレーションへの反映例

```
> enable
# copy ftp://staff@[2001:240:400::101]/backup.cnf running-config
Configuration file copy to running-config?
(y/n): y

Authentication for 2001:240:400::101.
User: staff
Password: xxx                              …1
transferring…

Data transfer succeeded.
#
```

1. リモートサーバ上のユーザ staff のパスワードを入力します。

5.5.3　zmodem コマンドを使用したファイル転送

本装置と RS232C ケーブルで接続されているコンソールとの間でファイル転送をするときは zmodem コマンドを使用します。

(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するディレクトリ（/usr/home/operator）にバックアップコンフィグレーションファイルを転送後，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にコピーします。zmodem コマンド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本装置に転送する例を次の図に示します。

図 5-22　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（zmodem コマンド）

```
> cd /usr/home/operator
> zmodem get backup.cnf                                    …1
**B000000027fed4
**B000000027fed4
> enable
# copy /usr/home/operator/backup.cnf startup-config        …2
Configuration file copy to startup-config ? (y/n): y       …3
#
```

1. バックアップコンフィグレーションファイルを転送します。転送後のファイル名は転送元で指定した

ファイル名と同じになります。

2. backup.cnf 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に使用します。
3. 入れ替えてよいかどうかの確認です。

(2) バックアップコンフィグレーションファイルをコンソールに転送する場合

本装置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コンソールに転送する例を次の図に示します。

図 5-23　バックアップコンフィグレーションファイルのコンソールへのファイル転送例

```
> cd /usr/home/operator
> enable
# copy running-config backup.cnf                       …1
Configuration file copy to /usr/home/operator/backup.cnf? (y/n) : y
# exit
> zmodem put backup.cnf                                …2
**000000000000
>
```

1. 運用しているコンフィグレーションファイルをバックアップコンフィグレーションファイルへコピーします。
2. バックアップコンフィグレーションファイルを転送します。

5.5.4　ftp コマンド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 コマンドを使用します。

(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するディレクトリ（/usr/home/operator）にバックアップコンフィグレーションファイルを転送後，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にコピーします。ftp コマンド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本装置に転送する例を次の図に示します。

図 5-24　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（ftp コマンド）

```
> cd /usr/home/operator
> ftp 192.168.0.1
Connect to 192.168.0.1.
220  FTP server (Version wn-2.4(4) Wed Jan 1 00:00:00 JST 1999) ready.
Name (192.168.0.1:operator): test
331 Password required for test.
Password:xxxxxx
230 User test logged in.
Remote system type UNIX.
Using binary mode to transfer files.
ftp> get backup.cnf                                         …1
local: backup.cnf remote: backup.cnf
200 PORT command successful.
150 Opening BINARY mode data connection for backup.cnf (12,345 bytes)
226 Transfer complete.
ftp> bye
221 Goodby
> enable
# copy /usr/home/operator/backup.cnf startup-config         …2
Configuration file copy to startup-config ? (y/n): y        …3
#
```

1. バックアップコンフィグレーションファイルを転送します。
2. backup.cnf 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に使用します。
3. 入れ替えてよいかどうかの確認です。

(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。

図 5-25　バックアップコンフィグレーションファイルのリモート運用端末へのファイル転送例

```
> cd /usr/home/operator
> enable
# copy running-config backup.cnf                          …1
Configuration file copy to /usr/home/operator/backup.cnf? (y/n) : y
# exit
> ftp 192.168.0.1
Connect to 192.168.0.1.
220  FTP server (Version wn-2.4(4) Fri Jan 1 00:00:00 JST 1999) ready.
Name (192.168.0.1:operator): test
331 Password required for test.
Password:xxxxxx
230 User test logged in.
Remote system type UNIX.
Using binary mode to transfer files.
ftp> put backup.cnf                                       …2
local: backup.cnf remote: backup.cnf
200 PORT command successful.
150 Opening BINARY mode data connection for backup.cnf (12,345 bytes)
226 Transfer complete.
ftp> bye
221 Goodby
>
```

1. 運用しているコンフィグレーションファイルをバックアップコンフィグレーションファイルへコピーします。
2. バックアップコンフィグレーションファイルを転送します。

5.5.5 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 cp コマンドを使用します。

（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するディレクトリ（/usr/home/operator）にバックアップコンフィグレーションファイルを MC から転送後，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にコピーします。cp コマンド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本装置に転送する例を次の図に示します。

図 5-26 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（cp コマンド）

```
> cd /usr/home/operator
> cp mc-file backup.cnf backup.cnf                          …1
> enable
# copy /usr/home/operator/backup.cnf startup-config          …2
Configuration file copy to startup-config? (y/n): y          …3
#
```

1. バックアップコンフィグレーションファイルを MC から転送します。
2. backup.cnf のバックアップコンフィグレーションファイルを運用に使用します。
3. 入れ替えてよいかどうかの確認です。

（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

本装置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 MC に転送する例を次の図に示します。

図 5-27 バックアップコンフィグレーションファイルの MC へのファイル転送例

```
> cd /usr/home/operator
> enable
# copy running-config backup.cnf                            …1
Configuration file copy to /usr/home/operator/backup.cnf? (y/n) : y
# exit
> cp backup.cnf mc-file backup.cnf                          …2
>
```

1. 運用しているコンフィグレーションファイルをバックアップコンフィグレーションファイルへコピーします。
2. バックアップコンフィグレーションファイルを MC へ転送します。

5.5.6 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ランニングコンフィグレーションにコピーする場合，運用中のポートが再起動しますので，ネットワーク経由で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。本装置の構成と一致していないバックアップコンフィグレーションファイルに copy コマンドを実行すると，copy コマンドがエラー終了するか，copy コマンドが正常終了しても運用には正常に反映されないことがあります。その際は，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，再度 copy コマンドを実行してください。

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。

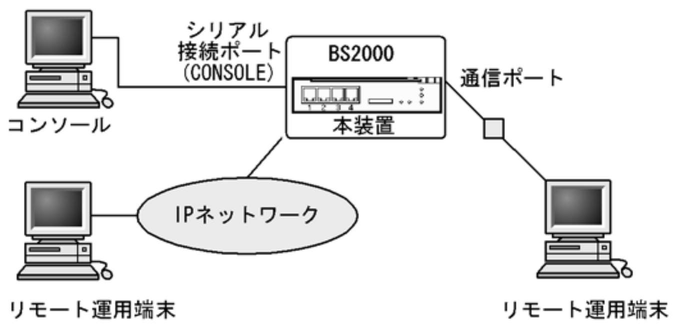
6.1 解説

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，ポート 0/1 に管理用として専用が設定されています。

工場出荷設定に関しては，BS2000 装置添付のマニュアル「BladeSymphony 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 アドレスなどの追加をされる場合には，ポート 0/1 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。

図 6-1　リモート運用端末およびコンソール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（RS232C）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（RS232C）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。

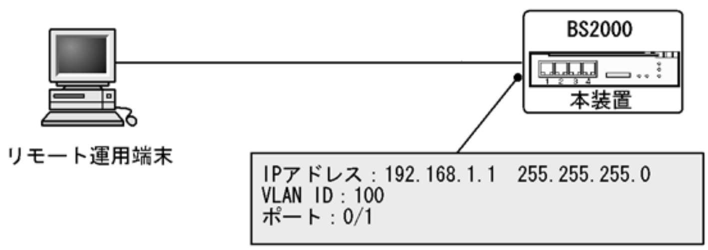
VLAN の設定，および IPv4/IPv6 インタフェースの設定に関するコンフィグレーションコマンドについては，「16　VLAN」，マニュアル「コンフィグレーションガイド Vol.3　2. IP・ARP・ICMP の設定と運用」，または「コンフィグレーションガイド Vol.3　16. IPv6・NDP・ICMPv6 の設定と運用」を参照してください。

6.2.2　本装置への IP アドレスの設定

［設定のポイント］

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（ポート 0/1）に設定している IP アドレスを使用するか，または新規に接続するインタフェースに対して IP アドレスを設定しておく必要があります。
工場出荷設定に関しては，BS2000 装置添付のマニュアル「BladeSymphony ユーザーズガイド」を参照してください。

図 6-2　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，VLAN 100 の VLAN コンフィグレーションモードに移行します。

2. **(config)# interface gigabitethernet 0/1**
   (config-if)# switchport mode access

(config-if)# switchport access vlan 100
(config-if)# exit
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。ポート 0/1 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　本装置に設定している IP アドレスの変更

［設定のポイント］

既に設定済みの IP アドレスを変更する場合，no ip address コマンドで IP アドレスを削除してから，再度 IP アドレスを設定します。
リモート運用端末で本装置に telnet プロトコルによるリモートログインをして，リモート運用端末が接続しているポートの VLAN の IP アドレスを変更する場合，no ip address コマンドで IP アドレスを削除した時点でリモート運用端末から本装置へのアクセスが出来なくなりますので，コンソール端末からログインして，IP アドレスを変更することをお勧めします。

図 6-3　コンソール端末で接続して IP アドレスを変更する例

［コマンドによる設定］

1. **(config)# interface vlan 100**
   (config-if)# no ip address 192.168.1.1
   VLAN ID 100 のインタフェースコンフィグモードに移行します。VLAN ID 100 の IPv4 アドレス 192.168.1.1 を削除します。

2. **(config-if)# ip address 192.168.100.1 255.255.255.0**
   (config-if)# exit
   (config)#
   VLAN ID 100 に IPv4 アドレス 192.168.100.1，サブネットマスク 255.255.255.0 を設定します。

3. **(config)# interface gigabitethernet 0/2**
   (config-if)# switchport mode access

(config-if)# switchport access vlan 100
(config-if)# exit
ポート 0/2 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 を VLAN 100 のアクセスポートに設定します。

6.2.4　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 2**
(config-line)#
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。また，装置に同時にリモートログインできるユーザ数を最大 3 に設定します。

6.2.5　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 help	ヘルプメッセージで表示するコマンドの一覧を設定します。
set terminal pager	ページングの実施／未実施を設定します。
show history	過去に実行した運用コマンドの履歴を表示します（コンフィグレーションコマンドの履歴は表示しません）。
stty	標準入力になっているデバイスの端末属性を表示します。
telnet	指定された IP アドレスのリモート運用端末と仮想端末と接続します。
ftp	本装置と TCP/IP で接続されているリモート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端末との間で UDP でファイル転送をします。

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」，マニュアル「コンフィグレーションガイド Vol.3　2. IP・ARP・ICMP の設定と運用」，または「コンフィグレーションガイド Vol.3　16. IPv6・NDP・ICMPv6 の設定と運用」を参照してください。

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 や ping ipv6 などを用いて確認できます。詳細は，マニュアル「コンフィグレーションガイド Vol.3　2. IP・ARP・ICMP の設定と運用」，または「コンフィグレーションガイド Vol.3　16. IPv6・NDP・ICMPv6 の設定と運用」を参照してください。

7 ログインセキュリティと RADIUS/TACACS+

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，アカウンティング，および RADIUS/TACACS+ 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 authorization commands	RADIUS サーバまたは TACACS+ サーバによるコマンド承認をする場合に指定します。
banner	ユーザのログイン前およびログイン後に表示するメッセージを設定します。
commands exec	ローカル（コンフィグレーション）によるコマンド承認で使用するコマンドリストに，コマンド文字列を追加します。
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。
parser view	ローカル（コンフィグレーション）によるコマンド承認で使用するコマンドリストを生成します。
username	指定ユーザに，ローカル（コンフィグレーション）によるコマンド承認で使用するコマンドリストまたはコマンドクラスを設定します。

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変更します。
clear password	ログインユーザのパスワードを削除します。
show sessions	本装置にログインしているユーザを表示します。
show whoami	本装置にログインしているユーザの中で，このコマンドを実行したログインユーザだけを表示します。
killuser	ログイン中のユーザを強制的にログアウトさせます。

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 によるコマンドの使用範囲の制限やパスワードによるチェックを設けています。
2. 複数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 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，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。
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. キー入力が最大 60 分間ない場合は自動的にログアウトします。
9. 運用コマンド killuser を使用してユーザを強制ログアウトできます。

7.1.3　ログインユーザの作成と削除

adduser コマンド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　ユーザ 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
# quit
>
```

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。

作成したログインユーザ名は忘れないようにしてください。ログインユーザ名を忘れると，デフォルトリスタートで起動してもログインできないので注意してください。

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 2
(config-line)#
```

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。line vty コマンドの <num> 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。2 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 1
(config-line)#
```

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の制限

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。

（1） ログインを許可する IP アドレスを設定する

［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，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 個の登録ができます。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。なお，アクセスを許可していない（コンフィグレーションで登録していない）端末からのアクセスがあった場合，すでにログインしているそのほかの端末には，アクセスがあったことを示す”Unknown host address <IP アドレス >”のメッセージが表示されます。

［コマンドによる設定］（IPv4 の場合）

1. **(config)# ip access-list standard REMOTE**
   (config-std-nacl)# 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するアクセスリスト情報 REMOTE を設定します。

2. **(config)# line vty 0 2**
   (config-line)# ip access-group REMOTE in
   (config-line)#
   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)# 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するアクセスリスト情報 REMOTE6 を設定します。

2. **(config)# line vty 0 2**
   (config-line)# ipv6 access-class REMOTE6 in
   (config-line)#
   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。

（2） RADIUS/TACACS+ を使用して認証する

リモート運用端末から本装置へのログイン時，RADIUS/TACACS+ を使用した認証が可能です。

7.1.8　ログインバナーの設定

コンフィグレーションコマンド banner でログインバナーの設定を行うと，console から，またはリモート

運用端末の telnet や ftp クライアントなどから本装置に接続したとき，ログインする前やログインしたあとにメッセージを表示できます。

［設定のポイント］

リモート運用端末の telnet や ftp クライアントからネットワークを介して本装置の telnet や ftp サーバへ接続するとき，ログインする前に次のメッセージを表示させます。

```
##########################################
Warning!!! Warning!!! Warning!!!
This is our system. You should not login.
Please close connection.
##########################################
```

［コマンドによる設定］

1. **(config)# banner login plain-text**
   ```
   --- Press CTRL+D or only '.' line to end ---
   ##########################################
   Warning!!! Warning!!! Warning!!!
   This is our system. You should not login.
   Please close connection.
   ##########################################
   .
   ```
   ログイン前メッセージのスクリーンイメージを入力します。
   入力が終わったら，"."（ピリオド）だけの行（または CTRL+D）を入力します。

2. **(config)# show banner**
   ```
   banner login encode
   "IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjCldhcm5pbmchISEgV2F
   ybmluZyEhISBXYXJuaW5nISEhClRoaXMgaXMgb3VyIHN5c3RlbS4gWW91IHNob3VsZCBub3QgbG9
   naW4uClBsZWFzZSBjbG9zZSBjb25uZWN0aW9uLgojIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyM
   jIyMjIyMjIyMjIyMjIyMK"
   ```
   入力されたメッセージは自動的にエンコードされて設定されます。

3. **(config)# show banner login plain-text**
   ```
   ##########################################
   Warning!!! Warning!!! Warning!!!
   This is our system. You should not login.
   Please close connection.
   ##########################################
   (config)#
   ```
   show の際に plain- text パラメータを指定すると，テキスト形式で確認できます。

設定が完了したら，リモート運用端末の telnet または ftp クライアントから本装置へ接続します。接続後，クライアントにメッセージが表示されます。

図 7-6　リモート運用端末から本装置へ接続した例

●telnetで接続した場合

```
> telnet 10.10.10.10
Trying 10.10.10.10...
Connected to 10.10.10.10.
Escape character is '^]'.

##########################################
Warning!!! Warning!!! Warning!!!
This is our system. You should not login.
Please close connection.
##########################################
login:
```

●ftpで接続した場合

```
> ftp 10.10.10.10
Connected to 10.10.10.10.
220-
##########################################
Warning!!! Warning!!! Warning!!!
This is our system. You should not login.
Please close connection.
##########################################
220 10.10.10.10 FTP server (NetBSD-ftpd) ready.
Name (10.10.10.10:staff):
```

7.2 RADIUS/TACACS+ の解説

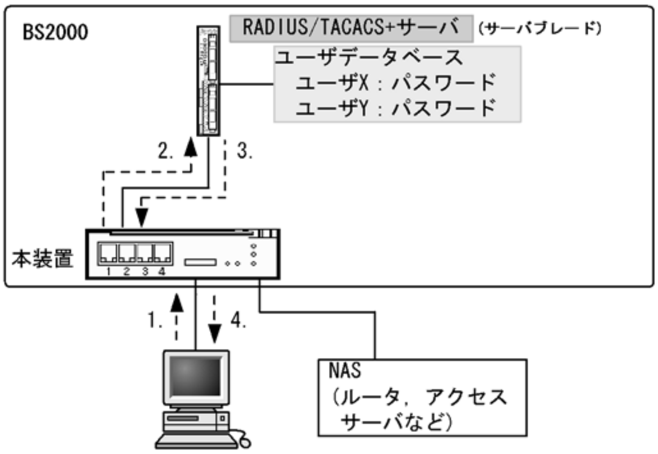
7.2.1 RADIUS/TACACS+ の概要

RADIUS （Remote Authentication Dial In User Service），TACACS+（Terminal Access Controller Access Control System Plus）とは，NAS（Network Access Server）に対して認証，承認，およびアカウンティングを提供するプロトコルです。NAS は RADIUS/TACACS+ のクライアントとして動作するリモートアクセスサーバ，ルータなどの装置のことです。NAS は構築されている RADIUS/TACACS+ サーバに対してユーザ認証，コマンド承認，およびアカウンティングなどのサービスを要求します。RADIUS/TACACS+ サーバはその要求に対して，サーバ上に構築された管理情報データベースに基づいて要求に対する応答を返します。本装置は NAS の機能をサポートします。

RADIUS/TACACS+ を使用すると一つの RADIUS/TACACS+ サーバだけで，複数 NAS でのユーザパスワードなどの認証情報や，コマンド承認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/TACACS+ サーバに対してユーザ認証，コマンド承認，およびアカウンティングを要求できます。

RADIUS/TACACS+ 認証の流れを次の図に示します。

図 7-7　RADIUS/TACACS+ 認証の流れ



1. リモート運用端末からユーザXが本装置にtelnetを実行する。
2. 本装置はコンフィグレーションで指定したRADIUS/TACACS+サーバに対して認証を要求する。
3. RADIUS/TACACS+サーバはユーザデータベースに基づいてユーザXを認証し，本装置にユーザXを認証したことを通知する。
4. 本装置はRADIUS/TACACS+認証に基づいて，ユーザXのリモート運用端末からのtelnet許可する。
5. 本装置はコンフィグレーションでコマンド承認を設定した場合，RADIUS/TACACS+サーバに設定してあるコマンドリストに従って，ユーザが投入する運用コマンドを許可／制限する。

7.2.2 RADIUS/TACACS+ の適用機能および範囲

本装置では RADIUS/TACACS+ を，リモート運用端末からのログイン時のユーザ認証，コマンド承認，およびアカウンティングに使用します。また，RADIUS は IEEE802.1X および Web 認証の端末認証にも使用します。RADIUS/TACACS+ 機能のサポート範囲を次に示します。

（1） RADIUS/TACACS+ の適用範囲

RADIUS/TACACS+ 認証を適用できる操作を次に示します。

- 本装置への telnet（IPv4/IPv6）
- 本装置への ftp（IPv4/IPv6）

次に示す操作は RADIUS/TACACS+ 認証を適用できません。

- コンソール（RS232C）からのログイン

RADIUS/TACACS+ コマンド承認を適用できる操作を次に示します。

- 本装置への telnet（IPv4/IPv6）

RADIUS/TACACS+ アカウンティングを適用できる操作を次に示します。

- 本装置への telnet（IPv4/IPv6）によるログイン・ログアウト
- 本装置への ftp（IPv4/IPv6）によるログイン・ログアウト
- RS232C からのログイン・ログアウト
- CLI でのコマンド入力（TACACS+ だけサポート）

（2） RADIUS 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／コマンド承認で使用する次のタイプ • Access-Request (送信) • Access-Accept (受信) • Access-Reject (受信) アカウンティングで使用する次のタイプ • Accounting-Request (送信) • Accounting-Response (受信)

分類	内容
属性	ログイン認証で使用する次の属性 • User-Name • User-Password • Service-Type • NAS-IP-Address • NAS-IPv6-Address • NAS-Identifier • Reply-Message コマンド承認で使用する次の属性 • Class • Vendor-Specific(Vendor-ID=21839) アカウンティングで使用する次の属性 • User-Name • NAS-IP-Address • NAS-IPv6-Address • NAS-Port • NAS-Port-Type • Service-Type • Calling-Station-Id • Acct-Status-Type • Acct-Delay-Time • Acct-Session-Id • Acct-Authentic • Acct-Session-Time

(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。

RADIUS サーバを利用してコマンド承認する場合は，認証時に下の表に示すような Class や Vendor-Specific を返すようにあらかじめ RADIUS サーバを設定しておく必要があります。RADIUS サーバには，ベンダー固有属性を登録 (dictionary ファイルなどに設定) してください。コマンド承認の属性詳細については「7.2.4　RADIUS/TACACS+/ ローカルを使用したコマンド承認」を参照してください。

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 Accounting-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。
Service-Type	6	Access-Request Accounting-Request	Login(値 =1)。Access-Accept および Access-Reject に添付された場合は無視します。
NAS-IP-Address	4	Access-Request Accounting-Request	本装置の IP アドレス。ローカルアドレスが設定されている場合はローカルアドレス，ローカルアドレスが設定されていない場合は送信インタフェースの IP アドレスになります。

属性名	属性値	パケットタイプ	内容
NAS-IPv6-Address	95	Access-Request Accounting-Request	本装置の IPv6 アドレス。ローカルアドレスが設定されている場合はローカルアドレス，ローカルアドレスが設定されていない場合は送信インタフェースの IPv6 アドレスになります。ただし，IPv6 リンクローカルアドレスで通信する場合は，ローカルアドレス設定の有無にかかわらず送信インタフェースの IPv6 リンクローカルアドレスになります。
NAS-Identifier	32	Access-Request Accounting-Request	本装置の装置名。装置名が設定されていない場合は添付されません。
Reply-Message	18	Access-Accept Access-Reject Accounting-Response	サーバからのメッセージ。添付されている場合は，運用ログとして出力されます。
Class	25	Access-Accept	ログインクラス。コマンド承認で適用します。
Vendor-Specific	26	Access-Accept	ログインリスト。コマンド承認で適用します。
NAS-Port	5	Accounting-Request	ユーザが接続されている NAS のポート番号を指します。本装置では，tty ポート番号を格納します。ただし，ftp の場合は 100 を格納します。
NAS-Port-Type	61	Accounting-Request	NAS に接続した方法を指します。本装置では，telnet/ftp は Virtual(5)，コンソールは Async(0) を格納します。
Calling-Station-Id	31	Accounting-Request	利用者の識別 ID を指します。本装置では，telnet/ftp はクライアントの IPv4/IPv6 アドレス，コンソールは“console”を格納します。
Acct-Status-Type	40	Accounting-Request	Accounting-Request がどのタイミングで送信されたかを指します。本装置では，ユーザのログイン時に Start(1)，ログアウト時に Stop(2) を格納します。
Acct-Delay-Time	41	Accounting-Request	送信する必要のあるイベント発生から Accounting-Request を送信するまでにかかった時間 (秒) を格納します。
Acct-Session-Id	44	Accounting-Request	セッションを識別するための文字列を指します。本装置では，セッションのプロセス ID を格納します。
Acct-Authentic	45	Accounting-Request	ユーザがどのように認証されたかを指します。本装置では，RADIUS(1)，Local(2)，Remote(3) の 3 種類を格納します。
Acct-Session-Time	46	Accounting-Request （Acct-Status-Type が Stop の場合だけ）	ユーザがサービスを利用した時間 (秒) を指します。本装置では，ユーザがログイン後ログアウトするまでの時間 (秒) を格納します。

- 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，Accounting-Response 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。

(3) TACACS+ のサポート範囲

TACACS+ 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 7-5　TACACS+ のサポート範囲

分類		内容
パケットタイプ		ログイン認証で使用する次のタイプ • Authentication Start（送信） • Authentication Reply(受信） • Authentication Continue（送信） コマンド承認で使用する次のタイプ • Authorization Request（送信） • Authorization Response（受信） アカウンティングで使用する次のタイプ • Accounting Request（送信） • Accounting Reply（受信）
ログイン認証	属性	• User • Password
コマンド承認	service	• taclogin
	属性	• class • allow-commands • deny-commands
アカウンティング	flag	• TAC_PLUS_ACCT_FLAG_START • TAC_PLUS_ACCT_FLAG_STOP
	属性	• task_id • start_time • stop_time • elapsed_time • timezone • service • priv-lvl • cmd

(a) 使用する TACACS+ 属性の内容

使用する TACACS+ 属性の内容を次の表に示します。

TACACS+ サーバを利用してコマンド承認する場合は，認証時に class または allow-commands や deny-commands 属性とサービスを返すように TACACS+ サーバ側で設定します。コマンド承認の属性詳細については「7.2.4　RADIUS/TACACS+/ ローカルを使用したコマンド承認」に示します。

表 7-6　使用する TACACS+ 属性の内容

service	属性	説明
-	User	認証するユーザの名前。
	Password	認証ユーザのパスワード。送信時には暗号化されます。
taclogin	class	コマンドクラス
	allow-commands	許可コマンドリスト
	deny-commands	制限コマンドリスト

（凡例）－：該当なし

アカウンティング時に使用する TACACS+ flag を次の表に示します。

表 7-7　TACACS+ アカウンティング flag 一覧

flag	内容
TAC_PLUS_ACCT_FLAG_START	アカウンティング START パケットを示します。ただし，aaa コンフィグレーションで送信契機に stop-only を指定している場合は，アカウンティング START パケットは送信しません。
TAC_PLUS_ACCT_FLAG_STOP	アカウンティング STOP パケットを示します。ただし，aaa コンフィグレーションで送信契機に stop-only を指定している場合は，このアカウンティング STOP パケットだけを送信します。

アカウンティング時に使用する TACACS+ 属性 (Attribute-Value) の内容を次の表に示します。

表 7-8　TACACS+ アカウンティング Attribute-Value 一覧

Attribute	Value
task_id	イベントごとに割り当てられる ID です。本装置ではアカウンティングイベントのプロセス ID を格納します。
start_time	イベントを開始した時刻です。本装置ではアカウンティングイベントが開始された時刻を格納します。この属性は次のイベントで格納されます。 • 送信契機 start-stop 指定時のログイン時，コマンド実行前 • 送信契機 stop-only 指定時のコマンド実行前
stop_time	イベントを終了した時刻です。本装置ではアカウンティングイベントが終了した時刻を格納します。この属性は次のイベントで格納されます。 • 送信契機 start-stop 指定時のログアウト時，コマンド実行後 • 送信契機 stop-only 指定時のログアウト時
elapsed_time	イベント開始からの経過時間 (秒) です。本装置ではアカウンティングイベントの開始から終了までの時間 (秒) を格納します。この属性は次のイベントで格納されます。 • 送信契機 start-stop 指定時のログアウト時，コマンド実行後 • 送信契機 stop-only 指定時のログアウト時
timezone	タイムゾーン文字列を格納します。
service	文字列“shell”を格納します。
priv-lvl	コマンドアカウンティング設定時に，入力されたコマンドが運用コマンドの場合は 1，コンフィグレーションコマンドの場合は 15 を格納します。
cmd	コマンドアカウンティング設定時に，入力されたコマンド文字列（最大 250 文字）を格納します。

7.2.3　RADIUS/TACACS+ を使用した認証

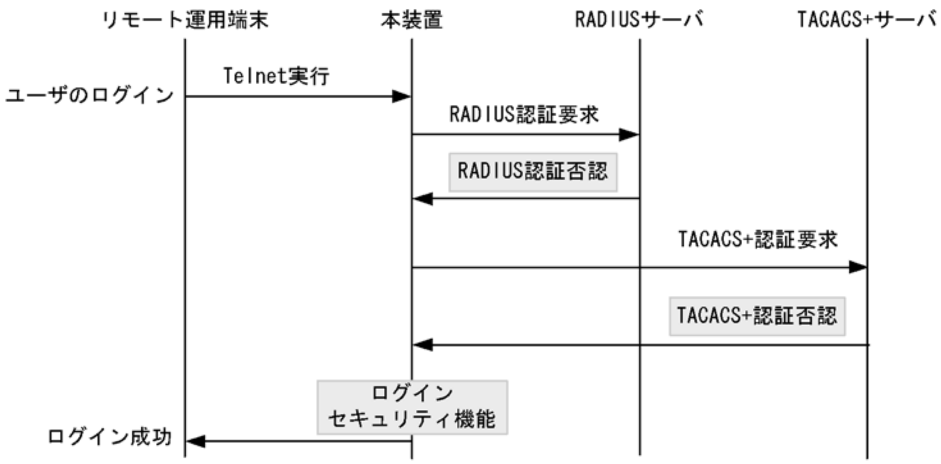
RADIUS/TACACS+ を使用した認証方法について説明します。

（1） ログイン認証サービスの選択

リモートログインの認証に使用するサービスは複数指定できます。指定できるサービスは RADIUS，TACACS+ および adduser/password コマンドによる本装置単体でのログインセキュリティ機能です。これらの認証方式は単独でも同時でも指定でき，同時に指定された場合は先に指定された方式で認証に失敗した場合に，次に指定された方式で認証できます。

認証方式として RADIUS，TACACS+，単体でのログインセキュリティの順番で指定した場合の認証方式シーケンスを次の図に示します。

図 7-8　認証方式シーケンス



この図で端末からユーザが本装置に telnet を実行すると，RADIUS サーバに対し本装置から RADIUS 認証を要求します。RADIUS サーバと通信不可または RADIUS サーバでの認証に失敗すると，次に TACACS+ サーバに対し本装置から TACACS+ 認証を要求します。TACACS+ サーバと通信不可または TACACS+ サーバでの認証に失敗すると，次に本装置のログインセキュリティ機能での認証を実行します。ここで認証に成功し，ユーザは本装置へのログインに成功します。

（2） RADIUS/TACACS+ サーバの選択

RADIUS サーバ，TACACS+ サーバはそれぞれ最大四つまで指定できます。一つのサーバと通信できず，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。

また，RADIUS サーバ，TACACS+ サーバをホスト名で指定したときに，複数のアドレスが解決できた場合は，優先順序に従い，アドレスを一つだけ決定し，RADIUS サーバ，TACACS+ サーバと通信します。

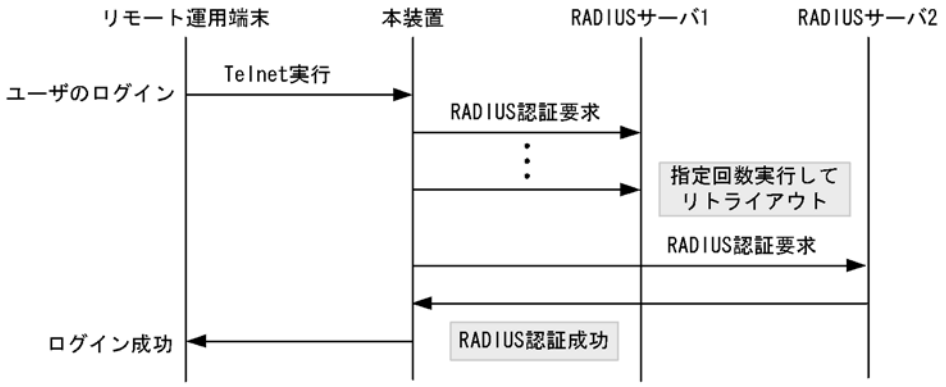
優先順序についての詳細は，「9　ホスト名と DNS　9.1　解説」を参照してください。

注意

DNS サーバを使用してホスト名を解決する場合，DNS サーバとの通信に時間が掛かることがあります。このため，RADIUS サーバ，TACACS+ サーバは IP アドレスで指定することをお勧めします。

RADIUS/TACACS+ サーバと通信不可を判断するタイムアウト時間を設定できます。デフォルト値は 5 秒です。また，各 RADIUS サーバでタイムアウトした場合は，再接続を試行します。この再試行回数も設定でき，デフォルト値は 3 回です。このため，ログイン方式として RADIUS が使用できないと判断するまでの最大時間は，タイムアウト時間×リトライ回数× RADIUS サーバ設定数になります。なお，各 TACACS+ サーバでタイムアウトした場合は，再接続を試行しません。このため，ログイン方式として TACACS+ が使用できないと判断するまでの最大時間は，タイムアウト時間× TACACS+ サーバ設定数になります。RADIUS サーバ選択のシーケンスを次の図に示します。

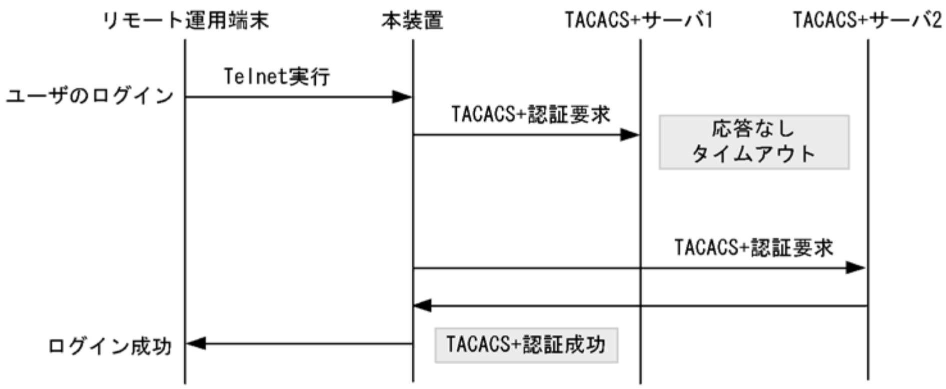
図 7-9　RADIUS サーバ選択のシーケンス



この図でリモート運用端末からユーザが本装置に telnet を実行すると，RADIUS サーバ 1 に対し本装置から RADIUS 認証を要求します。RADIUS サーバ 1 と通信できなかった場合は，続いて RADIUS サーバ 2 に対して RADIUS 認証を実行します。ここで認証に成功し，ユーザは本装置へのログインに成功します。

TACACS+ サーバ選択のシーケンスを次の図に示します。

図 7-10　TACACS+ サーバ選択のシーケンス



この図でリモート運用端末からユーザが本装置に telnet を実行すると，TACACS+ サーバ 1 に対し本装置から TACACS+ 認証を要求します。TACACS+ サーバ 1 と通信できなかった場合は，続いて TACACS+ サーバ 2 に対して TACACS+ 認証を実行します。ここで認証に成功し，ユーザは本装置へのログインに成功します。

(3)　ログインユーザ情報

RADIUS/TACACS+ 認証機能を使用するには，RADIUS/TACACS+ サーバにユーザ名およびパスワードを登録します。RADIUS/TACACS+ サーバへ登録するユーザ名には次に示す 2 種類があります。

- 本装置に adduser コマンドを使用して登録済みのユーザ名
  本装置に登録されたユーザ情報を使用してログイン処理を行います。
- 本装置に未登録のユーザ名
  次に示す共通のユーザ情報でログイン処理を行います。
  - ユーザ ID：remote_user
  - ホームディレクトリ：/usr/home/remote_user

本装置に未登録のユーザでログインした場合の注意点を示します。

- ファイルの管理
  ファイルを作成した場合，すべて remote_user 管理となって，別のユーザでも，作成したファイルの読み込みおよび書き込みができます。重要なファイルは ftp などで外部に保管するなど，ファイルの管理に注意してください。

7.2.4 RADIUS/TACACS+/ ローカルを使用したコマンド承認

RADIUS/TACACS+/ ローカル（コンフィグレーション）を使用したコマンド承認方法について説明します。

（1） コマンド承認の概要

RADIUS サーバ，TACACS+ サーバ，またはローカルパスワードによる認証の上ログインしたユーザに対し，使用できる運用コマンドの種類を制限することができます。これをコマンド承認と呼びます。使用できる運用コマンドは，RADIUS サーバまたは TACACS+ サーバから取得する，コマンドクラスおよびコマンドリスト，またはコンフィグレーションで設定したコマンドクラスおよびコマンドリストに従い制御を行います。また，制限した運用コマンドは，CLI の補完機能で補完候補として表示しません。なお，<option> や <Host Name> などの，<> で囲まれたパラメータ部分の値や文字列を含んだ運用コマンドを，許可するコマンドリストに指定した場合は，<> 部分は補完候補として表示しません。

図 7-11　RADIUS/TACACS+ サーバによるログイン認証，コマンド承認

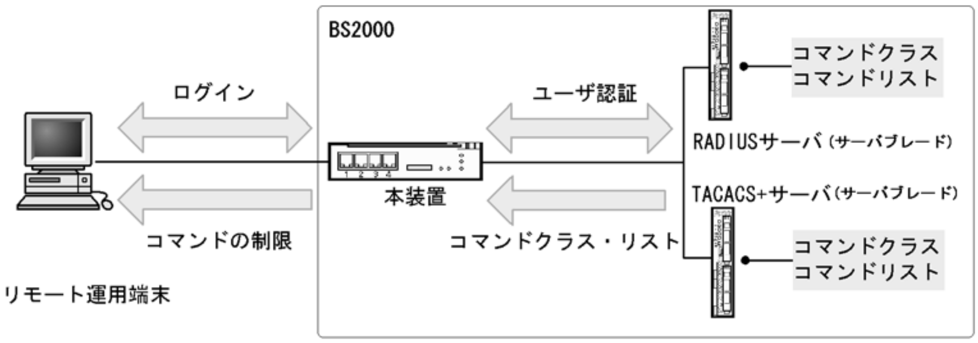
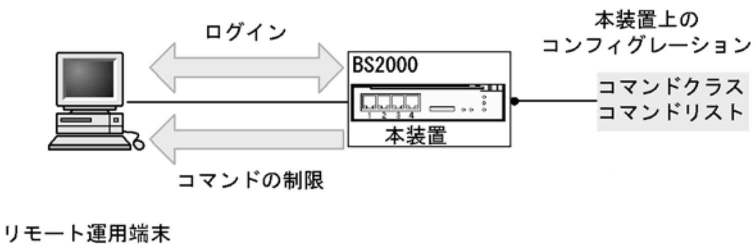


図 7-12　ローカルによるログイン認証，コマンド承認



本装置の aaa コンフィグレーションでコマンド承認を設定すると，RADIUS/TACACS+ 指定時は，ログイン認証と同時に，サーバからコマンドリストを取得します。ローカル指定時は，ログイン認証と同時に，コンフィグレーションで設定されたコマンドリストを使用します。本装置ではこれらのコマンドリストに従ってログイン後の運用コマンドを許可／制限します。

図 7-13　RADIUS/TACACS+ サーバによるコマンド承認のシーケンス

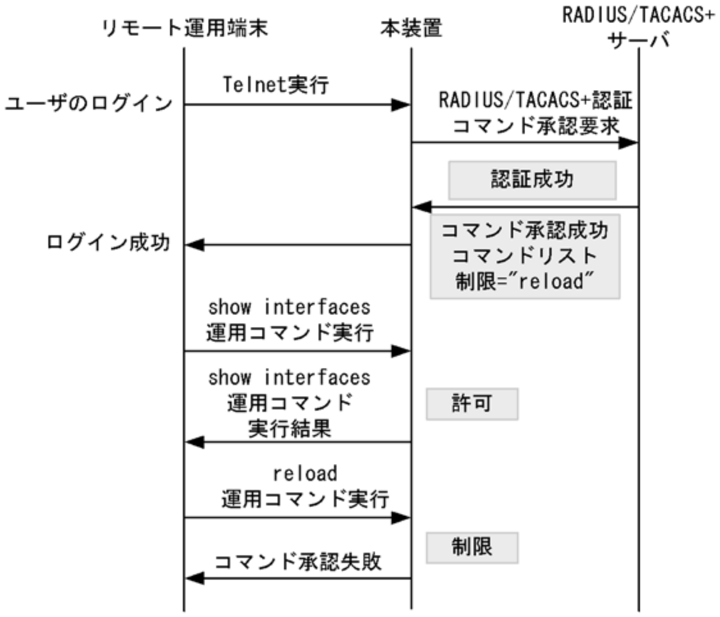
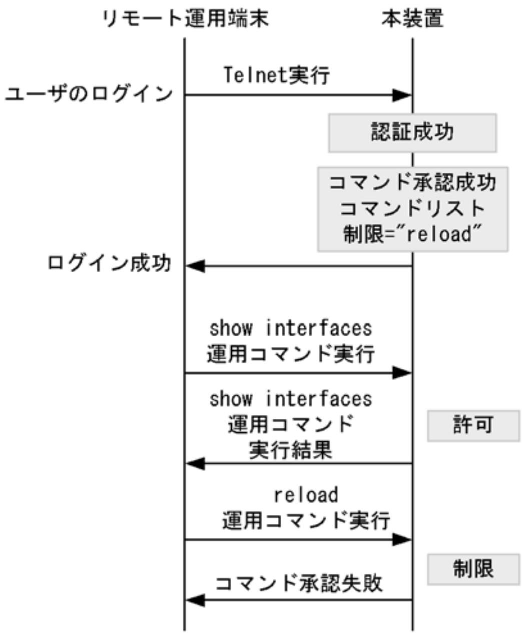


図 7-14　ローカルコマンド承認のシーケンス



「図 7-13　RADIUS/TACACS+ サーバによるコマンド承認のシーケンス」で端末からユーザが本装置に telnet を実行すると，RADIUS/TACACS+ サーバに対し本装置から認証，コマンド承認を要求します。認証成功時に RADIUS/TACACS+ サーバからコマンドリストを取得し，ユーザは本装置にログインします。

「図 7-14　ローカルコマンド承認のシーケンス」で端末からユーザが本装置に telnet を実行すると，ローカル認証を行います。認証成功時にコンフィグレーションからコマンドリストを取得し，ユーザは本装置にログインします。

ログイン後，ユーザは本装置で運用コマンド show interfaces などを実行できますが，運用コマンド reload はコマンドリストによって制限されているために実行できません。

注意事項

RADIUS/TACACS+ サーバのコマンドリストの設定を変更した場合またはコンフィグレーションのコマンドリストを変更した場合は，次回のログイン認証後から反映されます。

（2） RADIUS/TACACS+/ ローカルコマンド承認設定手順

RADIUS/TACACS+ によるコマンド承認を使用するためには，次の手順で RADIUS/TACACS+ サーバや本装置を設定します。

1. コマンド制限のポリシーを決める。
   各ユーザに対し，運用コマンドの中で，制限・許可するコマンドのポリシーを決めます。
2. コマンドリストを指定する。
   コマンドクラス以外に，許可／制限コマンドリストとして，許可コマンドと制限コマンドをそれぞれ指定できます。
3. RADIUS/TACACS+ サーバを設定する。
   決定したコマンド制限ポリシーを基に，RADIUS または TACACS+ のリモート認証サーバに，コマンド制限のための設定を行います。
4. 本装置のリモート認証を設定する。
   本装置で RADIUS または TACACS+ サーバのコンフィグレーション設定と aaa コンフィグレーション設定を行います。
5. コマンド承認の動作を確認する。
   RADIUS/TACACS+ を使用したリモート運用端末から本装置へログインし，確認を行います。

ローカルコマンド承認を使用するためには，次の手順で本装置を設定します。

1. コマンド制限のポリシーを決める。
   各ユーザに対し，運用コマンドの中で，制限・許可するコマンドのポリシーを決めます。
2. コマンドリストを作成する。
   コマンドクラス以外に，コマンドリストとして許可コマンドと制限コマンドをそれぞれ指定できます。
   決定したコマンド制限ポリシーを基に，コマンドリストのコンフィグレーション設定を行います。
   なお，コマンドクラスだけを使用する場合は作成不要です。
3. ユーザにコマンドクラスまたはコマンドリストを割り当てる。
   各ユーザに対し，コマンドクラスまたはコマンドリストを割り当てる username コンフィグレーション設定を行います。
   その後に，aaa コンフィグレーション設定を行います。
4. コマンド承認の動作を確認する。
   本装置へローカル認証でログインし確認を行います。

（3） コマンド制限のポリシー決定

各ユーザに対し，運用コマンドの中で，制限・許可するコマンドのポリシーを決めます。ここでは，各ユーザがログインしたときに，あるコマンド群は許可し，それ以外のコマンドは制限するなどを決めます。ポリシーは「(5) RADIUS/TACACS+/ ローカルコマンド承認の設定」で設定します。

コマンド制限・許可の対象となるのは，運用コマンドです。マニュアル未掲載のデバッグコマンド（PS コマンドなど）は対象外で，常に制限されます（許可が必要な場合は，次に説明するコマンドクラスで root を指定してコマンド無制限クラスとしてください）。なお，logout，exit，quit，disable，end，set terminal，show whoami，who ami コマンドに関しては常に許可されます。

本装置には，あらかじめ「コマンドクラス」として，以下のポリシーが定義されています。規定のコマンドクラスを選択することで，そのクラスの応じたコマンド制限を行うことができます。

表 7-9　コマンドクラス一覧

コマンドクラス	許可コマンド	制限コマンド
root 全コマンド無制限クラス	従来どおりすべてのコマンド（マニュアル未掲載のデバッグコマンドを含む）	なし
allcommand 運用コマンド無制限クラス	すべての運用コマンド "all"	なし（マニュアル未掲載のデバッグコマンドは不可）
noconfig コンフィグレーション変更制限クラス（コンフィグレーションコマンド指定も制限します）	制限以外の運用コマンド	"config, copy, erase configuration"
nomanage ユーザ管理コマンド制限クラス	制限以外の運用コマンド	"adduser, rmuser, clear password, password, killuser"
noenable 装置管理者モードコマンド制限クラス	制限以外の運用コマンド	"enable"

また，コマンドクラス以外に，許可コマンドリストと制限コマンドリストをそれぞれ指定することもできます。

(4) コマンドリストの指定方法について

コマンドクラス以外に，許可／制限コマンドリストとして，許可コマンドと制限コマンドをそれぞれ指定できます。コマンドを指定する場合は，各コマンドリストに設定対象のコマンド文字列をスペースも意識して指定します。複数指定する場合はコンマ（,）で区切って並べます。なお，ローカルコマンド承認では，コマンド文字列をコンフィグレーションコマンド commands exec で一つずつ設定します。本装置では，その設定されたコマンド文字列をコンマ（,）で連結したものをコマンドリストとして使用します。

コマンドリストで指定されたコマンド文字列と，ユーザが入力したコマンドの先頭部分とが，合致するかどうかを判定します (前方一致)。なお，特別な文字列として，all を指定できます。all は運用コマンドすべてを意味します。

判定時に，許可コマンドリストと制限コマンドリストの両方に合致した場合は，合致したコマンド文字数が多い方の動作を採用します（ただし，all 指定は文字数を 1 とします）。その際，許可コマンドリストと制限コマンドリストに同じコマンド文字列が指定されていた場合は，許可として判定されます。

また，コマンドクラスと許可／制限コマンドリストを同時に指定した場合は，コマンドクラスごとに規定されているコマンドリスト（「表 7-9　コマンドクラス一覧」中の " " で囲まれているコマンドリストに対応）と許可／制限コマンドリストを合わせて判定を行います。なお，コマンドクラスに root を指定した場合，許可／制限コマンドクラスの設定は無効となり，マニュアル未掲載のデバッグコマンド（PS コマンドなど）を含むすべてのコマンドが実行できるようになります。

例 1 ～ 7 にある各コマンドリストを設定した場合，本装置でどのようなコマンドが許可／制限されるかを示します。

(例 1)

許可コマンドリストだけを設定した場合，設定されたコマンドだけが実行を許可されます。

表 7-10　コマンドリスト例 1

コマンドリスト	指定コマンド	判定
許可コマンドリスト ="show ,ping" 制限コマンドリスト 設定なし	show ip arp	許可
	ping ipv6 ::1	許可

コマンドリスト	指定コマンド	判定
	reload	制限

(例 2)

許可コマンドリストと制限コマンドリストの両方に合致した場合は，合致したコマンド文字数が多い方の動作とします(ただし，all 指定は文字数 1 とします)。

表 7-11　コマンドリスト例 2

コマンドリスト	指定コマンド	判定
許可コマンドリスト ="show ,ping ipv6" 制限コマンドリスト ="show ip,ping"	show system	許可
	show ipv6 neighbors	制限
	ping ipv6 ::1	許可
	ping 10.10.10.10	制限

(例 3)

許可コマンドリストと制限コマンドリストの両方を設定し，両方に合致しない場合は，許可として判定されます。

表 7-12　コマンドリスト例 3

コマンドリスト	指定コマンド	判定
許可コマンドリスト ="show" 制限コマンドリスト ="reload"	ping 10.10.10.10	許可
	reload	制限

(例 4)

許可コマンドリストと制限コマンドリストに同じコマンド文字列が指定されている場合は，許可として判定されます。

表 7-13　コマンドリスト例 4

コマンドリスト	指定コマンド	判定
許可コマンドリスト ="show" 制限コマンドリスト ="show,ping"	show system	許可
	ping ipv6 ::1	制限

(例 5)

コマンドリストをまったく設定しなかった場合は，logout などのコマンド以外はすべて制限されます。

表 7-14　コマンドリスト例 5

コマンドリスト	指定コマンド	判定
許可コマンドリスト 設定なし 制限コマンドリスト 設定なし	すべて	制限
	logout，exit，quit，disable，end，set terminal，show whoami，who ami	許可

(例 6)

クラスとして root を指定した場合は，従来どおりすべてのコマンドが実行可能となります。なお，コマンドクラスに root を指定した場合，許可／制限コマンドクラスの制限は無効となり，マニュアル未掲載のデバッグコマンド（PS コマンドなど）を含むすべてのコマンドが実行可能となります。

表 7-15　コマンドリスト例 6

コマンドリスト	指定コマンド	判定
コマンドクラス ="root"	すべて（マニュアル未掲載のデバッグコマンドを含む）	許可

(例 7)

制限コマンドリストだけを設定した場合は，リストに合致しない運用コマンドはすべて許可となります。

表 7-16　コマンドリスト例 7

コマンドリスト	指定コマンド	判定
許可コマンドリスト 設定なし 制限コマンドリスト = "reload"	reload 以外の運用コマンドすべて	許可
	reload	制限

本マニュアルでは，例として次表のようなポリシーでコマンド制限を行います。

表 7-17　コマンド制限のポリシー例

ユーザ名	コマンドクラス	許可コマンド	制限コマンド
staff	allcommand	運用コマンドすべて	なし
guest	なし	制限以外の運用コマンドすべて許可	reload …※ inactivate …※ enable …※
test	なし	show ip …※ (show ipv6 …は制限)	許可以外，すべて制限

注※　…は任意のパラメータを意味します（show ip …は show ip arp など）。

(5) RADIUS/TACACS+/ ローカルコマンド承認の設定

「表 7-17　コマンド制限のポリシー例」で決定したコマンド制限ポリシーを基に，RADIUS または TACACS+ のリモート認証サーバでは，通常のログイン認証の設定以外に，以下の属性値を使用したコマンド制限のための設定を行います。

なお，サーバ側でコマンド承認の設定を行っていない場合，ユーザが認証されログインできても logout，exit，quit，disable，end，set terminal，show whoami，who ami 以外のすべてのコマンドが制限され，コマンドを実行できなくなりますのでご注意ください。その場合は，コンソールからログインしてください。

● RADIUS サーバを使用する場合

RADIUS サーバを利用してコマンド制限する場合は，認証時に以下のような属性を返すようにサーバで設定します。

表 7-18　RADIUS 設定属性一覧

属性	ベンダー固有属性	値
25 Class	－	クラス 次の文字列のどれか一つを指定します。 root，allcommand，noconfig，nomanage，noenable
26 Vendor-Specific Vendor-Id: 21839	ALAXALA-Allow-Command s Vendor type: 101	許可コマンドリスト 許可するコマンドの前方一致文字列をコンマ（,）で区切って指定します。空白も区別します。 運用コマンドすべては "all" を指定します。 許可コマンドリストだけ設定した場合は，許可コマンドリスト以外のコマンドはすべて制限となります。 （例：ALAXALA-Allow-Commands="show ,ping ,telnet "）
	ALAXALA-Deny-Commands Vendor type: 102	制限コマンドリスト 制限するコマンドの前方一致文字列をコンマ（,）で区切って指定します。空白も区別します。 運用コマンドすべては "all" を指定します。 制限コマンドリストだけ設定した場合は，制限コマンドリスト以外はすべて許可となります。 （例：ALAXALA-Deny-Commands="enable,reload, inactivate"）

（凡例）－：該当なし

RADIUS サーバには，上記のベンダー固有属性を登録（dictionary ファイルなどに設定）してください。

図 7-15　RADIUS サーバでのベンダー固有属性の dictionary ファイル登録例

```
VENDOR          ALAXALA                        21839
ATTRIBUTE       ALAXALA-Allow-Commands         101       string  ALAXALA
ATTRIBUTE       ALAXALA-Deny-Commands          102       string  ALAXALA
```

「表 7-17　コマンド制限のポリシー例」で決定したポリシーを一般的な RADIUS サーバに設定する場合，以下のような設定例になります。

図 7-16　RADIUS サーバ設定例

```
staff  Password = "******"
       Class = "allcommand"                                … 1

guest  Password = "******"
       Alaxala-Deny-Commands = "enable,reload,inactivate"  … 2

test  Password = "******"
      Alaxala-Allow-Commands = "show ip "                  … 3
```

注 ****** の部分には各ユーザのパスワードを設定します。

1. クラス "allcommand" で運用コマンドすべてを許可します。
2. enable，reload，および inactivate で始まるコマンドを制限します。
   allow-commands が指定されていないため，ほかのコマンドは許可となります。
3. 空白の有無が意味を持ちます。
   "show ip " の後ろに空白があるため，show ip arp などのコマンドは許可されますが，show ipv6 neighbors などのコマンドは許可されません。
   ほかのコマンドはすべて制限となります。

注意

- 本装置では Class エントリを複数受信した場合，1 個目の Class を認識し 2 個目以降の Class エントリは無効となります。

図 7-17　複数 Class エントリ設定例

```
Class = "noenable"                                           … 1
Class = "allcommand"
```

1. 本装置では一つ目の noenable だけ有効となります。

- 本装置では Class エントリに複数のクラス名を記述した場合，1 個目のクラス名を認識し 2 個目以降のクラス名は無効となります。例えば，class="nomanage,noenable" と記述した場合，nomanage だけが有効になります。
- ALAXALA-Deny-Commands, ALAXALA-Allow-Commands のそれぞれにおいて，同一属性のエントリを複数受信した場合，一つの属性につきコンマ（,）と空白も含み 1024 文字までを認識し，1025 文字以降は受信しても無効となります。なお，下記の例のように同一属性を複数エントリ記述し，本装置で 2 個目以降のエントリを受信した場合にはエントリの先頭に自動的にコンマ（,）を設定します。

図 7-18　複数 Deny-Commands エントリ設定例

```
ALAXALA-Deny-Commands = "inactivate,reload"                  … 1
ALAXALA-Deny-Commands = "activate,test,..........."          … 1
```

1. 本装置では下線の部分を合計 1024 文字まで認識します。
　上記の Deny-Commands を受信した場合は，下記のように 2 個目のエントリの先頭である activate コマンドの前にコンマ（,）が自動的に設定されます。
　Deny-Commands = "inactivate,reload,activate,test,........."

● TACACS+ サーバを使用する場合

TACACS+ サーバを使用してコマンド制限をする場合は，TACACS+ サーバで承認の設定として以下のような属性－値のペアを設定します。

表 7-19　TACACS+ 設定属性一覧

service	属性	値
taclogin	class	コマンドクラス 次の文字列のどれかを指定 root，allcommand，noconfig，nomanage，noenable
	allow-commands	許可コマンドリスト 許可するコマンドの前方一致文字列をコンマ（,）で区切って指定します。空白も区別します。 運用コマンドすべては "all" を指定します。 許可コマンドリストだけ設定した場合は，許可コマンドリスト以外のコマンドはすべて制限となります。 （例：allow-commands="show ,ping ,telnet "）
	deny-commands	制限コマンドリスト 制限するコマンドの前方一致文字列をコンマ（,）で区切って指定します。空白も区別します。 運用コマンドすべては "all" を指定します。制限コマンドリストだけ設定した場合は，制限コマンドリスト以外はすべて許可となります。 （例：deny-commands="enable,reload,inactivate"）

「表 7-17　コマンド制限のポリシー例」で決定したポリシーを一般的な TACACS+ サーバに設定する場合，以下のような設定ファイルイメージになります。

図 7-19　TACACS+ サーバの設定例

```
user=staff {
    login = cleartext "******"
    service = taclogin {                                 … 1
        class = "allcommand"
    }
}

user=guest {
    login = cleartext "******"
    service = taclogin {
        deny-commands = "enable,reload,inactivate"       … 2
}

user=test {
    login = cleartext "******"
    service = taclogin {
        allow-commands = "show ip "                      … 3
}
```

注 ****** の部分には各ユーザのパスワードを設定します。

1. service 名は taclogin と設定します。
   クラス "allcommand" で運用コマンドすべてを許可します。
2. enable，reload，および inactivate で始まるコマンドを制限します。
   allow-commands が指定されていないため，ほかのコマンドは許可となります。
3. 空白の有無が意味を持ちます。
   "show ip " の後ろに空白があるため，show ip arp などのコマンドは許可されますが，show ipv6 neighbors などのコマンドは許可されません。
   ほかのコマンドはすべて制限となります。

注意

- 本装置では class エントリに複数のクラス名を記述した場合，1 個目のクラス名を認識し 2 個目以降のクラス名は無効となります。例えば class="nomanage,noenable" と記述した場合，nomanage だけが有効になります。
- deny-commands，allow-commands のそれぞれにおいて，一つの属性につきコンマ (,) と空白も含み 1024 文字までを認識し，1025 文字以降は受信しても無効となります。

● ローカルコマンド承認を使用する場合

「表 7-17　コマンド制限のポリシー例」で決定したポリシーをローカルコマンド承認で設定する場合，次のようなコンフィグレーションの設定になります。

図 7-20 コンフィグレーションの設定例

```
username guest view guest_view
username staff view-class allcommand                        … 1
username test view test_view
!
parser view guest_view
  commands exec exclude all "enable"                        … 2
  commands exec exclude all "inactivate"                    … 2
  commands exec exclude all "reload"                        … 2
!
parser view test_view
  commands exec include all "show ip "                      … 3
!
aaa authentication login default local
aaa authorization commands default local
```

1. ユーザ "staff" に対し，クラス "allcommand" で運用コマンドすべてを許可します。
2. enable，inactivate，および reload で始まるコマンドを制限します。
   commands exec include が指定されていないため，ほかのコマンドは許可となります。
3. 空白の有無が意味を持ちます。
   "show ip " の後ろに空白があるため，show ip arp などのコマンドは許可されますが，show ipv6 neighbors などのコマンドは許可されません。
   ほかのコマンドはすべて制限となります。

(a) ログインしての確認

設定が完了した後，RADIUS/TACACS+/ ローカルを使用したリモート運用端末から本装置へのログインを行います。ログイン後，show whoami コマンドでコマンドリストが設定されていること，コマンドを実行して制限・許可していることを確認してください。

図 7-21 staff がログイン後の確認例

```
> show whoami
staff: ttyp0    ----- 2  Jan 6 14:17:03(10.10.10.10)

Home-directory: /usr/home/staff
Authentication: TACACS+ (Server 192.168.10.1)
Class: allcommand
      Allow: "all"
      Deny : -----
Command-list: -----
>
> show cal
Wed Jan 07 17:21:15  2009
> /bin/date
% Command not authorized.
>
```

図 7-22　guest がログイン後の確認例

```
>show whoami
guest: ttyp0    ----- 2  Jan 6 14:17:03(10.10.10.20)

Home-directory: /usr/home/guest
Authentication: RADIUS (Server 192.168.10.1)
Class: -----
Command-list:
      Allow: -----
      Deny : "enable,reload,inactivate"
>
> show cal
Wed Jan 07 17:21:15  2009
> reload
% Command not authorized.
>
```

図 7-23　test がログイン後の確認例

```
>show whoami
test: ttyp0    ----- 2  Jan 6 14:17:03(10.10.10.30)

Home-directory: /usr/home/test
Authentication: LOCAL
Class: -----
Command-list:
      Allow: "show ip "
      Deny : -----
>
> show ip arp
***コマンド実行されます***
> show ipv6 neighbors
% Command not authorized.
>
```

7.2.5　RADIUS/TACACS+ を使用したアカウンティング

RADIUS/TACACS+ を使用したアカウンティング方法について説明します。

(1) アカウンティングの指定

本装置の RADIUS/TACACS+ コンフィグレーションと aaa accounting コンフィグレーションのアカウンティングを設定すると，運用端末から本装置へのログイン・ログアウト時に RADIUS または TACACS+ サーバへアカウンティング情報を送信します。また，本装置へのコマンド入力時に TACACS+ サーバへアカウンティング情報を送信します。

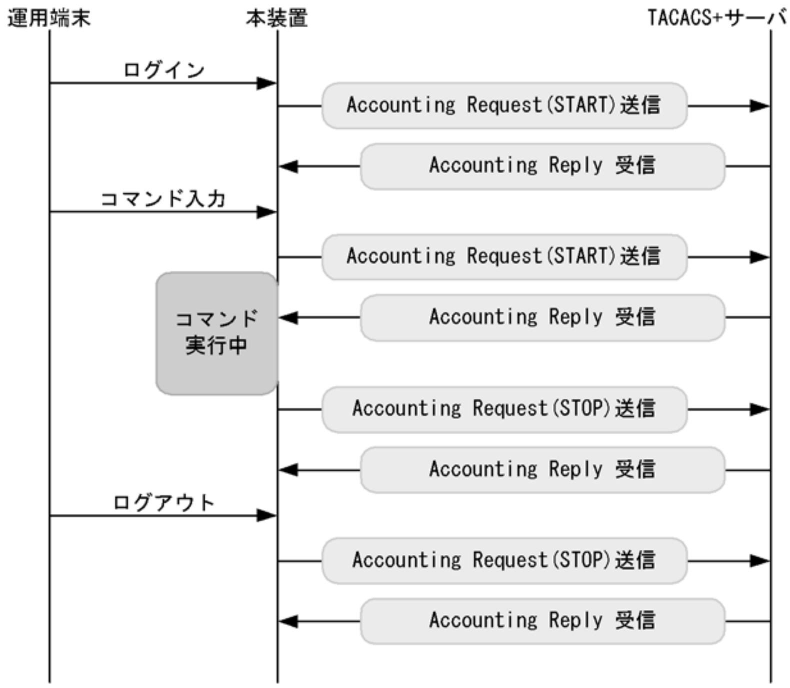
アカウンティングの設定は，ログインとログアウトのイベントを送信するログインアカウンティング指定と，コマンド入力のイベントを送信するコマンドアカウンティング指定があります。コマンドアカウンティングは TACACS+ だけでサポートしています。

それぞれのアカウンティングに対して，アカウンティング START と STOP を両方送信するモード（start-stop）と STOP だけを送信するモード（stop-only）を選択できます。さらに，コマンドアカウンティングに対しては，入力したコマンドをすべて送信するモードとコンフィグレーションだけを送信するモードを選択できます。また，設定された各 RADIUS/TACACS+ サーバに対して，通常はどこかのサーバでアカウンティングが成功するまで順に送信しますが，成功したかどうかにかかわらずすべてのサーバへ順に送信するモード（broadcast）も選択できます。

(2) アカウンティングの流れ

ログインアカウンティングとコマンドアカウンティングの両方を START-STOP 送信モードで TACACS+ サーバへ送信する設定をした場合のシーケンスを次の図に示します。

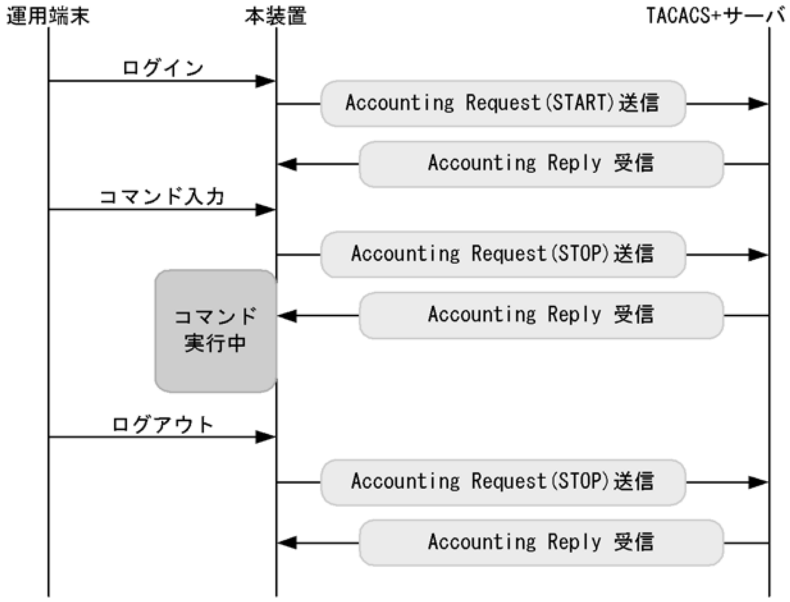
図 7-24　TACACS+ アカウンティングのシーケンス（ログイン・コマンドアカウンティングの START-STOP 送信モード時）



この図で運用端末から本装置にログインが成功すると，本装置から TACACS+ サーバに対しユーザ情報や時刻などのアカウンティング情報を送信します。また，コマンドの入力前後にも本装置から TACACS+ サーバに対し入力したコマンド情報などのアカウンティング情報を送信します。最後に，ログアウト時には，ログインしていた時間などの情報を送信します。

ログインアカウンティングは START-STOP 送信モードのままで，コマンドアカウンティングだけを STOP-ONLY 送信モードして TACACS+ サーバへ送信する設定をした場合のシーケンスを次の図に示します。

図 7-25　TACACS+ アカウンティングのシーケンス（ログインアカウンティング START-STOP，コマンドアカウンティング STOP-ONLY 送信モード時）



「図 7-24　TACACS+ アカウンティングのシーケンス（ログイン・コマンドアカウンティングの START-STOP 送信モード時)」の例と比べると，ログイン・ログアウトでのアカウンティング動作は同じですが，コマンドアカウンティングで STOP-ONLY を指定している場合，コマンドの入力前にだけ本装置から TACACS+ サーバに対し入力したコマンド情報などのアカウンティング情報を送信します。

（3） アカウンティングの注意事項

RADIUS/TACACS+ コンフィグレーション，aaa accounting コンフィグレーションのアカウンティングの設定や interface loopback コンフィグレーションで IPv4 装置アドレスを変更した場合は，送受信途中や未送信のアカウンティングイベントと統計情報はクリアされ，新しい設定で動作します。

多数のユーザが，コマンドを連続して入力したり，ログイン・ログアウトを繰り返したりした場合，アカウンティングイベントが大量に発生するため，一部のイベントでアカウンティングできないことがあります。

アカウンティングイベントの大量な発生による本装置・サーバ・ネットワークへの負担を避けるためにも，コマンドアカウンティングは STOP-ONLY で設定することをお勧めします。また，正常に通信できない RADIUS/TACACS+ サーバは指定しないでください。

運用コマンド clear accounting でアカウンティング統計情報をクリアする場合，clear accounting コマンドの入力時点で各サーバへの送受信途中のアカウンティングイベントがあるときは，そのイベントの送受信終了後に，各サーバへの送受信統計のカウントを開始します。

7.2.6　RADIUS/TACACS+ との接続

（1） RADIUS サーバとの接続

（a） RADIUS サーバでの本装置の識別

RADIUS プロトコルでは NAS を識別するキーとして，要求パケットの発信元 IP アドレスを使用するよう規定されています。本装置では要求パケットの発信元 IP アドレスに次に示すアドレスを使用します。

- コンフィグレーションコマンド interface loopback 0 のローカルアドレスが設定されている場合は，ローカルアドレスを発信元 IP アドレスとして使用します。
- ローカルアドレスが設定されていない場合は，送信インタフェースの IP アドレスを使用します。

このため，ローカルアドレスが設定されている場合は，RADIUS サーバに本装置を登録するためにローカルアドレスで指定した IP アドレスを使用する必要があります。これによって，RADIUS サーバと通信するインタフェースが特定できない場合は，ローカルアドレスを設定することで RADIUS サーバを確実に識別できる本装置の情報を登録できるようになります。

(b) RADIUS サーバのメッセージ

RADIUS サーバは応答に Reply-Message 属性を添付して要求元にメッセージを送付する場合があります。本装置では，RADIUS サーバからの Reply-Message 属性の内容を運用ログに出力します。RADIUS サーバとの認証に失敗する場合は，運用ログを参照してください。

(c) RADIUS サーバのポート番号

RADIUS の認証サービスのポート番号は，RFC2865 で 1812 と規定されています。本装置では特に指定しないかぎり，RADIUS サーバへの要求に 1812 のポート番号を使用します。しかし，一部の RADIUS サーバで 1812 ではなく初期の実装時に使用されていた 1645 のポート番号を使用している場合があります。このときはコンフィグレーション 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。

(2) TACACS+ サーバとの接続

(a) TACACS+ サーバの設定

- 本装置と TACACS+ サーバを接続する場合は，Service と属性名などに注意してください。TACACS+ サーバの属性については，「7.2.4　RADIUS/TACACS+/ ローカルを使用したコマンド承認」を参照してください。
- コンフィグレーションコマンド interface loopback 0 のローカルアドレスが設定されている場合は，ローカルアドレスを発信元 IP アドレスとして使用します。

7.3　RADIUS/TACACS+ 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/TACACS+，アカウンティング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 7-20　コンフィグレーションコマンド一覧（RADIUS）

コマンド名	説明
radius-server host	認証，承認，アカウンティングに使用する RADIUS サーバを設定します。
radius-server key	認証，承認，アカウンティングに使用する RADIUS サーバ鍵を設定します。
radius-server retransmit	認証，承認，アカウンティングに使用する RADIUS サーバへの再送回数を設定します。
radius-server timeout	認証，承認，アカウンティングに使用する RADIUS サーバの応答タイムアウト値を設定します。

表 7-21　コンフィグレーションコマンド一覧（TACACS+）

コマンド名	説明
tacacs-server host	認証，承認，アカウンティングに使用する TACACS+ サーバを設定します。
tacacs-server key	認証，承認，アカウンティングに使用する TACACS+ サーバの共有秘密鍵を設定します。
tacacs-server timeout	認証，承認，アカウンティングに使用する TACACS+ サーバの応答タイムアウト値を設定します。

表 7-22　コンフィグレーションコマンド一覧（アカウンティング）

コマンド名	説明
aaa accounting commands	コマンドアカウンティングを行うときに設定します。
aaa accounting exec	ログイン・ログアウトアカウンティングを行うときに設定します。

7.3.2　RADIUS サーバによる認証の設定

［設定のポイント］

RADIUS サーバ，およびローカル認証を行う設定例を示します。RADIUS 認証に失敗した場合には，本装置によるローカル認証を行うように設定します。

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，ローカル認証の順に設定します。

2. **(config)# radius-server host 192.168.10.1 key "039fkllf84kxm3"**
   RADIUS 認証に使用するサーバ 192.168.10.1 の IP アドレスと共有鍵を設定します。

7.3.3　TACACS+ サーバによる認証の設定

［設定のポイント］

TACACS+ サーバおよびローカル認証を行う設定例を示します。TACACS+ 認証に失敗した場合には，本装置によるローカル認証を行うように設定します。

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 tacacs+ local**
   使用するログイン認証方式を TACACS+ 認証，ローカル認証の順に設定します。

2. **(config)# tacacs-server host 192.168.10.1 key "4h8dlir9r-w2"**
   TACACS+ 認証に使用するサーバ 192.168.10.1 の IP アドレスと共有鍵を設定します。

7.3.4　RADIUS/TACACS+/ ローカルによるコマンド承認の設定

（1） RADIUS サーバによるコマンド承認の設定例

［設定のポイント］

RADIUS サーバによるコマンド承認を行う設定例を示します。

あらかじめ，RADIUS 認証を使用する設定を行ってください。

［コマンドによる設定］

1. **(config)# aaa authentication login default group radius local**
   (config)# radius-server host 192.168.10.1 key "RaD#001"
   あらかじめ，RADIUS サーバによる認証の設定を行います。

2. **(config)# aaa authorization commands default group radius**
   RADIUS サーバを使用して，コマンド承認を行います。

［注意事項］

本設定後にユーザが RADIUS 認証されてログインしたとき，RADIUS サーバ側でコマンド承認の設定がされていなかった場合は，コマンドがすべて制限されて実行できなくなります。設定ミスなどでコマンドの実行ができない場合は，コンソールからログインして修正してください。

（2） TACACS+ サーバによるコマンド承認の設定例

［設定のポイント］

TACACS+ サーバによるコマンド承認を行う設定例を示します。

あらかじめ，TACACS+ 認証を使用する設定を行ってください。

［コマンドによる設定］

1. **(config)# aaa authentication login default group tacacs+ local**
   (config)# tacacs-server host 192.168.10.1 key "TaC#001"
   あらかじめ，TACACS+ サーバによる認証の設定を行います。

2. **(config)# aaa authorization commands default group tacacs+**

TACACS+ サーバを使用して，コマンド承認を行います。

［注意事項］

本設定後にユーザが TACACS+ 認証されてログインしたとき，TACACS+ サーバ側でコマンド承認の設定がされていなかった場合は，コマンドがすべて制限されて実行できなくなります。設定ミスなどでコマンドの実行ができない場合は，コンソールからログインして修正してください。

(3) ローカルコマンド承認の設定例

［設定のポイント］

ローカルコマンド承認を行う設定例を示します。

あらかじめ，ユーザ名とそれに対応したコマンドクラス（username view-class）またはコマンドリスト（username view・parser view・commands exec）の設定を行ってください。

また，ローカルパスワード認証を使用する設定を行ってください。

［コマンドによる設定］

1. **(config)# parser view Local_001**
   (config-view)# commands exec include all "show"
   (config-view)# commands exec exclude all "reload"
   コマンドリストを使用する場合は，あらかじめコマンドリストの設定を行います。
   なお，コマンドクラスだけを使用する場合は，コマンドリストの設定は必要ありません。

2. **(config)# username user001 view Local_001**
   (config)# username user001 view-class noenable
   指定ユーザにコマンドクラスまたはコマンドリストの設定を行います。
   なお，コマンドクラスとコマンドリストを同時に設定することもできます。

3. **(config)# aaa authentication login default local**
   ローカルパスワードによる認証の設定を行います。

4. **(config)# aaa authorization commands default local**
   ローカル認証を使用して，コマンド承認を行います。

［注意事項］

ローカルコマンド承認を設定すると，ローカル認証でログインしたすべてのユーザに適用されますので，設定に漏れがないようご注意ください。

コマンドクラスまたはコマンドリストの設定がされていないユーザは，コマンドがすべて制限されて実行できなくなります。

設定ミスなどでコマンドの実行ができない場合は，コンソールからログインして修正してください。

7.3.5 RADIUS/TACACS+ によるログイン・ログアウトアカウンティングの設定

(1) RADIUS サーバによるログイン・ログアウトアカウンティングの設定例

［設定のポイント］

RADIUS サーバによるログイン・ログアウトアカウンティングを行う設定例を示します。あらかじめ，アカウンティング送信先となる RADIUS サーバホスト側の設定を行ってください。

［コマンドによる設定］

1. **(config)# radius-server host 192.168.10.1 key "RaD#001"**
   あらかじめ，RADIUS サーバの設定を行います。

2. **(config)# aaa accounting exec default start-stop group radius**
   ログイン・ログアウトアカウンティングの設定を行います。

［注意事項］

radius-server コンフィグレーションの設定がされていない状態で aaa accounting exec を設定した場合，ユーザがログイン・ログアウトしたときに System accounting failed という運用ログが表示されます。使用する radius-server コンフィグレーションを設定してください。

(2) TACACS+ サーバによるログイン・ログアウトアカウンティングの設定例

［設定のポイント］

TACACS+ サーバによるログイン・ログアウトアカウンティングを行う設定例を示します。あらかじめ，アカウンティング送信先となる TACACS+ サーバホスト側の設定を行ってください。

［コマンドによる設定］

1. **(config)# tacacs-server host 192.168.10.1 key "TaC#001"**
   あらかじめ，TACACS+ サーバの設定を行います。

2. **(config)# aaa accounting exec default start-stop group tacacs+**
   ログイン・ログアウトアカウンティングの設定を行います。

［注意事項］

tacacs-server コンフィグレーションの設定がされていない状態で aaa accounting exec を設定した場合，ユーザがログイン・ログアウトしたときに System accounting failed という運用ログが表示されます。使用する tacacs-server コンフィグレーションを設定してください。

7.3.6　TACACS+ サーバによるコマンドアカウンティングの設定

(1) TACACS+ サーバによるコマンドアカウンティングの設定例

［設定のポイント］

TACACS+ サーバによるコマンドアカウンティングを行う設定例を示します。
あらかじめ，アカウンティング送信先となる TACACS+ サーバホスト側の設定を行ってください。

［コマンドによる設定］

1. **(config)# tacacs-server host 192.168.10.1 key "TaC#001"**
   TACACS+ サーバの設定を行います。

2. **(config)# aaa accounting commands 0-15 default start-stop group tacacs+**
   コマンドアカウンティングを設定します。

［注意事項］

tacacs-server コンフィグレーションの設定がされていない状態で aaa accounting commands を設定した場合，ユーザがコマンドを入力したときに System accounting failed という運用ログが表示されます。使用する tacacs-server コンフィグレーションを設定してください。

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 NTP 確認

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。なお，本装置は RFC1305 NTP バージョン 3 に準拠しています。

8.1.1　コンフィグレーションコマンド・運用コマンド一覧

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 8-1　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 access-group	アクセスグループを作成し，IPv4 アドレスフィルタによって，NTP サービスへのアクセスを許可または制限できます。
ntp authenticate	NTP 認証機能を有効化します。
ntp authentication-key	認証鍵を設定します。
ntp broadcast	インタフェースごとにブロードキャストで NTP パケットを送信し，ほかの装置が本装置に同期化するように設定します。
ntp broadcast client	接続したサブネット上の装置からの NTP ブロードキャストメッセージを受け付けるための設定をします。
ntp broadcastdelay	NTP ブロードキャストサーバと本装置間で予測される遅延時間を指定します。
ntp master	ローカルタイムサーバの設定を指定します。
ntp peer	NTP サーバに，シンメトリック・アクティブ／パッシブモードを構成します。
ntp server	NTP サーバをクライアントモードに設定し，クライアントサーバモードを構成します。
ntp trusted-key	ほかの装置と同期化する場合に，セキュリティ目的の認証をするように鍵番号を設定します。

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 8-2　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。
show clock	現在設定されている日付，時刻を表示します。
show ntp associations	接続されている ntp サーバの動作状態を表示します。
restart ntp	ローカル ntp サーバを再起動します。

8.1.2　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。

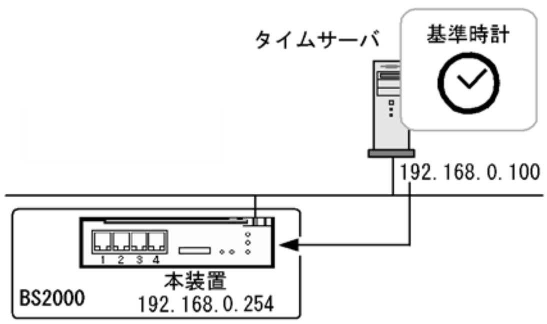
2. **(config)# save**
   (config)# exit
   保存し，コンフィグレーションモードから装置管理者モードに移行します。

3. **# set clock 0901211530**
   Wed Jan 21 15:30:00 2005 JST
   2009 年 1 月 22 日 15 時 30 分に時刻を設定します。

8.1.3　NTP によるタイムサーバと時刻同期の設定

NTP 機能を用いて，本装置の時刻をタイムサーバの時刻に同期させます。

図 8-1　NTP 構成図（タイムサーバへの時刻の同期）



［設定のポイント］

タイムサーバの時刻を本装置の時刻に同期させることはできません。
タイムサーバを複数設定した場合の本装置の同期先は，ntp server コマンドの prefer パラメータを指定されたタイムサーバが選択されます。また，prefer パラメータが指定されなかった場合は，タイムサーバの stratum 値が最も小さいタイムサーバが選択され，すべての stratum 値が同じ場合の同期先は任意となります。

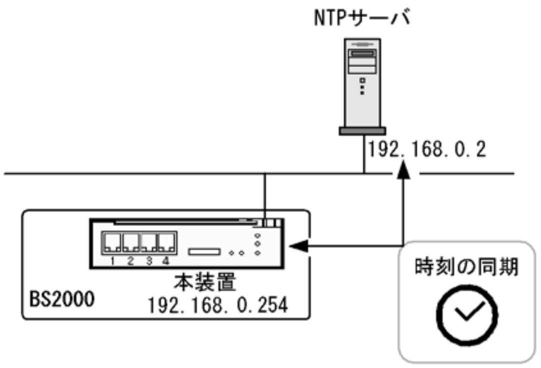
［コマンドによる設定］

1. **(config)# ntp server 192.168.0.100**
   IP アドレス 192.168.0.100 のタイムサーバに本装置を同期させます。

8.1.4　NTP サーバとの時刻同期の設定

NTP 機能を用いて，本装置の時刻と NTP サーバの時刻をお互いに調整しながら，同期させます。

図 8-2　NTP 構成図（NTP サーバとの時刻の同期）



［設定のポイント］

複数の NTP サーバと本装置を同期する場合には，ntp peer コマンドを用いて複数設定する必要があります。

NTP サーバを複数設定した場合の本装置の同期先は，ntp peer コマンドの prefer パラメータを指定された NTP サーバが選択されます。また，prefer パラメータが指定されなかった場合は，NTP サーバの stratum 値が最も小さい NTP サーバが選択され，すべての stratum 値が同じ場合の同期先は任意となります。

［コマンドによる設定］

1. **(config)# ntp peer 192.168.0.2**
   IP アドレス 192.168.0.2 の NTP サーバとの間を peer 関係として設定します。

8.1.5　NTP 認証の設定

［設定のポイント］

NTP 機能でほかの装置と時刻の同期を行う場合に，セキュリティ目的の認証を行います。

［コマンドによる設定］

1. **(config)# ntp authenticate**
   NTP 認証機能を有効化します。

2. **(config)# ntp authentication-key 1 md5 NtP#001**
   NTP 認証鍵として，鍵番号 1 に「NtP#001」を設定します。

3. **(config)# ntp trusted-key 1**
   NTP 認証に使用する鍵番号 1 を指定します。

8.1.6　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，時刻が変更された時点で 0 にクリアされます。
- OSPF または OSPFv3 使用時に，時刻補正を HelloInterval 時間（デフォルト 10 秒）内に連続して実行（(RouterDeadInterval 時間－ HelloInterval 時間) / 3 回以上（デフォルトは 30/3 ＝ 10 回以上)）した場合，隣接関係が切断されることがあります。

- スタティック経路の動的監視機能の連続失敗回数を 1 回で使用したとき，現在時刻より 3 秒以上進めた場合に，該当経路を使用した通信が一時的に切断されることがあります。
- BGP4 または BGP4+ 使用時に，時刻補正を HoldTime 内に連続して実行（連続時刻補正回数× 10 秒 ＞ HoldTime）した場合，隣接関係が切断されることがあります。また，HoldTime を 10 秒以下で使用した場合，1 回の時刻補正で隣接関係が切断されることがあります。

8.1.7　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 8-3　時刻の確認

```
> show clock
Wed Jan 21 15:30:00 2009 JST
>
```

また，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っている場合，運用コマンド show ntp associations で動作状態を確認できます。次の図に例を示します。

図 8-4　NTP サーバの動作状態の確認

```
> show ntp associations   [Enter]キー押下
remote           refid      st t when poll reach   delay   offset    disp
==============================================================================
*timesvr    192.168.1.100    3 u    1   64  377     0.89   -2.827    0.27
>
```

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，本装置のログ情報などのコンフィグレーションを設定するときに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一覧

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 host	IPv4 アドレスに付与するホスト名情報を設定します。
ipv6 host	IPv6 アドレスに付与するホスト名情報を設定します。
ip domain lookup	DNS リゾルバ機能を無効化または有効化します。
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 name-server	DNS リゾルバが参照するネームサーバを設定します。

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 router.mydomain.co.jp**
   ドメイン名を router.mydomain.co.jp に設定します。

2. **(config)# ip nameserver 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の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 recovery	no system recovery コマンドを設定すると，装置の障害が発生した際に，障害部位の復旧処理を行わないようにし，障害発生以降に障害部位を停止したままにします。
swrt_multicast_table	IPv4/IPv6 マルチキャストと IGMP/MLD snooping を同時に使用する場合に設定します。
swrt_table_resource	装置のルーティングのテーブルエントリ数の配分パターンを設定します。

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。
clear control-counter	障害による装置再起動回数および部分再起動回数を 0 クリアします。
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に関する情報を表示します。
show tcpdump	本装置に対して送受信されるパケットをモニタします。

表 10-3 運用コマンド一覧（装置内メモリと MC の確認）

コマンド名	説明
show flash	装置内メモリの使用状態を表示します。
show mc	MC の形式と使用状態を表示します。
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。

表 10-5 運用コマンド一覧（リソース情報とダンプ情報の確認）

コマンド名	説明
show cpu	CPU 使用率を表示します。
show processes	装置の現在実行中のプロセスの情報を表示します。

コマンド名	説明
show memory	装置の現在使用中のメモリの情報を表示します。
df	ディスクの空き領域を表示します。
du	ディレクトリ内のファイル容量を表示します。
erase dumpfile	ダンプファイルを消去します。
show dumpfile	ダンプファイル格納ディレクトリに格納されているダンプファイルの一覧を表示します。

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 software
Date 2009/01/26 18:57:57 UTC
S/W: OS-L3A Ver. 10.7.D
H/W: GV-BE2LSW1N1 [JJ0BSA24T001S0A00111057:80330300:304:1B
>
```

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 2009/01/26 19:04:50 UTC
System: GV-BE2LSW1N1, OS-L3A Ver. 10.7.D
Node : Name=slot0
    Contact=Contact Address
    Locate=Location
    Elapsed time : 00:16:28
    Machine ID : 0000.8712.18dc
    Main Board : Active
        Boot : 2009/01/26 18:48:31 , operation reboot
        Fatal restart : CPU 0 times ,  SW 0 times
        Lamp : Power LED=green , Status LED1=green
        Board : CPU=PowerPC 533MHz , Memory=524,288kB(512MB)
        Management port: active up)
             100BASE-TX full 0000.8712.18f5
        Temperature : normal(45degree)
        Flash :
                  user area   config area     dump area    area total
            used   20,052kB          59kB           0kB      20,111kB
            free   17,141kB       7,206kB       7,144kB      31,491kB
            total  37,193kB       7,265kB       7,144kB      51,602kB
        MC : Disconnect
    Device resources
        Current selected swrt_table_resource : l3switch-1
        Current selected swrt_multicast_table : Off
        IP Routing Entry :
            Unicast : current number=7 , max number=12288
            Multicast : current number=0 , max number=1024
            ARP : current number=1 , max number=3072
        IPv6 Routing Entry :
            Unicast : current number=0 , max number=0
            Multicast : current number=0 , max number=0
            NDP : current number=0 , max number=0
        MAC-Address table entry(Unit1) : current number=7 , max number=32768
        MAC-Address table entry(Unit2) : current number= - , max number= -
        Flow detection mode : layer3-2
          Used resources for filter inbound(Used/Max)
                                     MAC     IPv4     IPv6
            Port 0/ 1- 3       :     n/a    0/256      n/a
            Port 0/ 4- 6       :     n/a    0/256      n/a
            Port 0/10-12       :     n/a    0/256      n/a
            Port 0/13-15       :     n/a    0/256      n/a
            Port 0/16-18       :     n/a    0/256      n/a
            Port 0/19-21       :     n/a    0/256      n/a
            Port 0/22-24       :     n/a    0/256      n/a
            VLAN               :     n/a      n/a      n/a
          Used resources for QoS(Used/Max)
                                     MAC     IPv4     IPv6
            Port 0/ 1- 6       :     n/a    0/128      n/a
            Port 0/ 7-12       :     n/a    0/128      n/a
            Port 0/13-18       :     n/a    0/128      n/a
            Port 0/19-24       :     n/a    0/128      n/a
            VLAN               :     n/a      n/a      n/a
          Used resources for UPC(Used/Max)
                                     MAC     IPv4     IPv6
            Port 0/ 1- 6       :     n/a    0/128      n/a
            Port 0/ 7-12       :     n/a    0/128      n/a
            Port 0/13-18       :     n/a    0/128      n/a
            Port 0/19-24       :     n/a    0/128      n/a
            VLAN               :     n/a      n/a      n/a
          Used resources for TCP/UDP port detection pattern
            Resources(Used/Max):  0/16
        Flow detection out mode : layer3-1-out
          Used resources for filter outbound(Used/Max)
                                     MAC     IPv4     IPv6
            Port 0/ 1- 6       :     n/a    0/128      n/a
            Port 0/ 7-12       :     n/a    0/128      n/a
            Port 0/13-18       :     n/a    0/128      n/a
            Port 0/19-24       :     n/a    0/128      n/a
            VLAN               :     n/a      n/a      n/a
```

```
>
```

10.1.4　装置内メモリの確認

運用コマンド show flash で装置内メモリ上のファイルシステムの使用状況を確認できます。もし，使用量が合計容量の 95% を超える場合は，次の図に例を示します。

図 10-3　Flash 容量の確認

```
> show flash
Date 2009/01/14 17:53:11 UTC
Flash :
          user area   config area     dump area    area total
    used   37,063kB          65kB          16kB      37,144kB
    free      616kB       7,199kB       8,152kB      15,967kB
    total  37,679kB       7,265kB       8,168kB      53,112kB
>
```

10.1.5　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，回線が障害状態から回復した場合は回線が回復したメッセージを，回線が障害になって運用を停止した場合は回線が障害になったメッセージを表示します。運用メッセージの詳細については，マニュアル「メッセージ・ログレファレンス　2. ルーティングのイベント情報」を参照してください。

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は，コンソールやリモート運用端末上には一部しか表示しませんので，運用コマンド show logging で確認してください。

10.1.6　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。

- オペレータの操作および応答メッセージ
- 運用メッセージ

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

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

た，grep を使用してパターン文字列の指定を実施することで，特定のログ情報だけを表示することもできます。例えば，障害に関するログは show logging | grep EVT や show logging | grep ERR の実行でまとめて表示できます。障害に関するログの表示例を次の図に示します。

図 10-5　障害に関するログ表示

```
> show logging | grep EVT
    :
(途中省略)
    :
EVT 01/10 20:39:38 E3 SOFTWARE 00005002 1001:000000000000 Login operator from
LOGHOST1 (ttyp1).
EVT 01/10 20:41:43 E3 SOFTWARE 00005003 1001:000000000000 Logout operator from
LOGHOST1 (ttyp1).
    :
(以下省略)
    :
>
```

10.1.7　ルーティングテーブルのエントリ数の配分パターンの設定

本装置では，装置の適用形態に合わせ，ルーティングテーブルのエントリ数の配分パターンを変更することができます。配分パターンは 2 種類提供しており，コンフィグレーションコマンド swrt_table_resource で l3switch-1，または l3switch-2 を指定することで指定できます。

なお，配分パターンとテーブルのエントリ数に関する情報は，運用コマンド show system により確認できます。

配分パターンと対応するテーブルエントリ数の一覧を次の表に示します。

表 10-6　パターンとテーブルエントリ数の一覧

項目		パターン	
		l3switch-1※	l3switch-2
IPv4	ユニキャスト経路	12288	8192
	マルチキャスト経路	1024	256
	ARP	3072	1024
IPv6	ユニキャスト経路	0	2048
	マルチキャスト経路	0	128
	NDP	0	1024

注※　初期状態は，l3switch-1 です。

［設定のポイント］

初期状態は，l3switch-1 です。また，本設定の変更を有効にするには，本装置の再起動が必要となるため，初期導入時に設定することをお勧めします。

［コマンドによる設定］

1. **(config)# swrt_table_resource l3switch-2**
   コンフィグレーションモードで，テーブルエントリ数の配分パターンを l3switch-2 に設定します。

2. **(config)# save**
   (config)# exit
   保存して，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ます。

3. **# reload**
   本装置を再起動します。

10.1.8　IPv4/IPv6 マルチキャストと IGMP/MLD snooping 同時使用時の設定

本装置では，コンフィグレーションコマンド swrt_multicast_table を設定することで，IPv4/IPv6 マルチキャストと IGMP/MLD snooping を同時に使用できます。

なお，swrt_multicast_table の設定情報は，運用コマンド show system で確認できます。

［設定のポイント］

初期状態では swrt_multicast_table は設定されていません。swrt_multicast_table を設定したあと，有効にするには本装置の再起動が必要となるため，初期導入時に設定することをお勧めします。

［コマンドによる設定］

1. **(config)# swrt_multicast_table**
   コンフィグレーションモードで，swrt_multicast_table を設定します。

2. **(config)# save**
   (config)# exit
   保存して，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ます。

3. **# reload**
   本装置を再起動します。

10.2　運用情報のバックアップ・リストア

装置障害または交換時の運用情報の復旧手順を示します。

次に示す「10.2.2　backup/restore コマンドを用いる手順」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 10-7　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 またはリモートの ftp サーバに保存します。
restore	MC 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旧します。

10.2.2　backup/restore コマンドを用いる手順

（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，backup コマンドを用いてバックアップを作成しておきます。backup コマンドは，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 または外部の FTP サーバに保存します。

これらの情報に変更があった場合，backup コマンドによるバックアップの作成をお勧めします。

- ソフトウェアを稼働中のバージョンにアップデートするためのファイル
- ソフトウェアアップグレードの有無
- startup-config
- 電源運用モード
- ユーザアカウント／パスワード
- オプションライセンスの有無
- Web 認証データベース
- Web 認証用に登録された認証画面ファイル
- MAC 認証データベース
- IPv6 DHCP サーバ DUID ファイル

backup コマンド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。

- show logging コマンドで表示される運用ログ情報など
- 装置内に保存されているダンプファイルなどの障害情報
- ユーザアカウントごとに設けられるホームディレクトリにユーザが作成および保存したファイル

（2） 情報のリストア

backup コマンドで作成されたバックアップファイルから情報を復旧する場合，restore コマンドを用います。

restore コマンドを実行すると，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。

10.3 障害時の復旧

本装置では運用中に障害が発生した場合は自動的に復旧処理を行います。障害部位に応じて復旧処理を局所化して行い，復旧処理による影響範囲を狭めることによって，正常運用部分が中断しないようにします。

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
ポートで検出した障害	自動復旧を無限回行います。	該当するポートの再初期化を行います。	該当するポートを介する通信が中断されます。
メインボード障害	自動復旧を 6 回／ 1 時間行います。障害継続中は 1 時間経過後に再度復旧処理を実行します。	該当するメインボードの再初期化を行います。	装置内の全ポートを介する通信が中断されます。

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，自動復旧を行いません。

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。

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

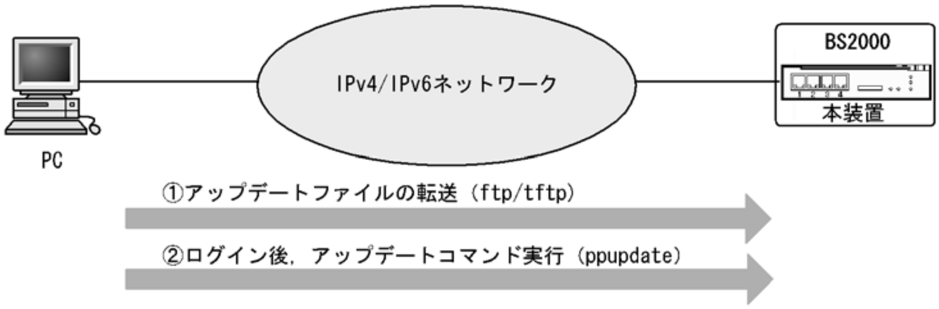
コマンド名	説明
ppupdate	ftp，tftp などでダウンロードした新しいソフトウェアにアップデートします。

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，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。

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



12 イーサネット

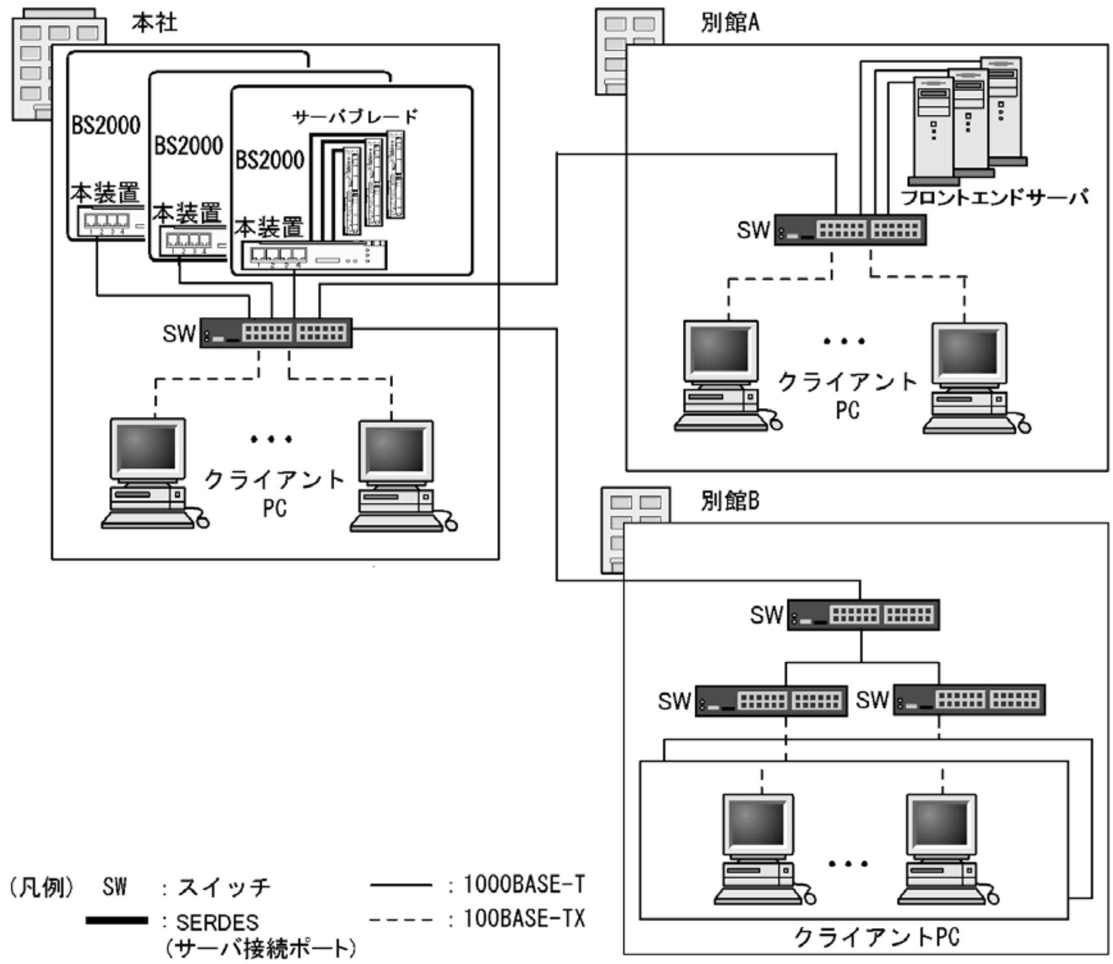
この章では，本装置のイーサネットについて説明します。

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

本装置を使用した代表的なイーサネットの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 3 種類があります。

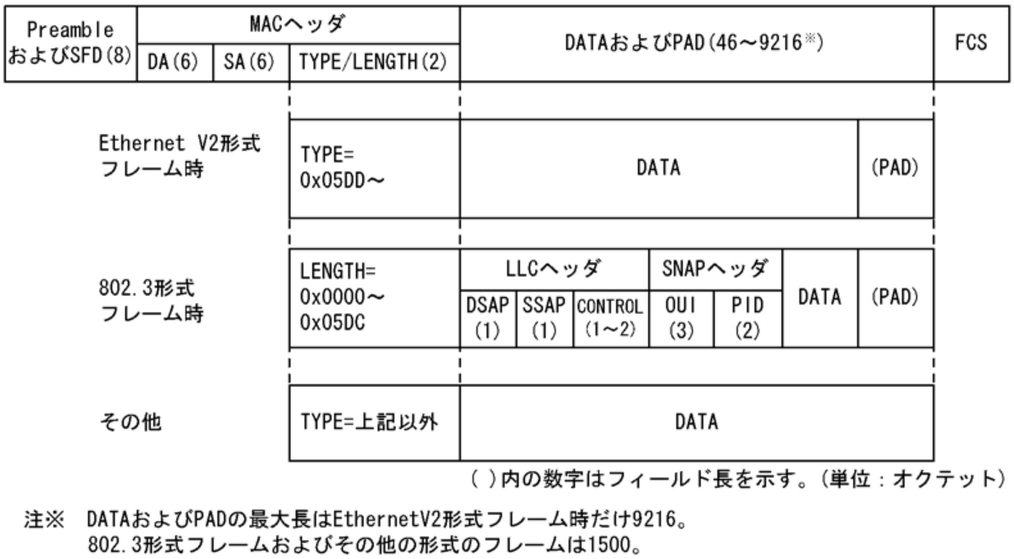
- IEEE802.3 に準拠した 10BASE-T ／ 100BASE-TX ／ 1000BASE-T のツイストペアケーブル（UTP）を使用したインタフェース
- IEEE802.3ae に準拠した 10GBASE-R の光ファイバを使用したインタフェース

  注※　IEEE802.3ah を含みます。

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



(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 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 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） LLC の扱い

IEEE802.2 の LLC タイプ 1 をサポートしています。また，次に示す条件に合致したフレームだけを中継の対象にします。次に示す条件以外のフレームは，廃棄します。

（a） CONTROL フィールド

CONTROL フィールドの値と送受信サポート内容を「表 12-2　CONTROL フィールドの値と送受信サポート内容」に示します。また，「表 12-2　CONTROL フィールドの値と送受信サポート内容」に示す TEST フレームおよび XID フレームについては，「表 12-3　XID および TEST レスポンス」に示す形で応答を返します。

表 12-2　CONTROL フィールドの値と送受信サポート内容

種別	コード (16 進数)	コマンド	レスポンス	備考
TEST	F3 または E3	受信サポート	送信サポート	IEEE802.2 の仕様に従って，TEST レスポンスを返送します。
XID	BF または AF	受信サポート	送信サポート	IEEE802.2 の仕様に従って，XID レスポンスを返送します。ただし，XID レスポンスの情報部は 129.1.0(IEEE802.2 の規定による ClassI を示す値) とします。

表 12-3　XID および TEST レスポンス

MAC ヘッダの DA	フレーム種別	DSAP	応答
ブロードキャストまたはマルチキャスト	XID および TEST	AA(SNAP) 42(BPDU) 00(null) FF(global)	返す
		上記以外	返さない
個別アドレスで 自局アドレス	XID および TEST	AA(SNAP) 42(BPDU) 00(null) FF(global)	返す
		上記以外	返さない
個別アドレスで 他局アドレス	XID および TEST	すべてのアドレス	返さない

(4) 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

(5) 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，レイヤ 3 インタフェースの MAC アドレスや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 12-4　装置 MAC アドレスを使用する機能

機能	用途
VLAN	レイヤ 3 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
GSRP	装置識別子
LLDP	装置識別子
OADP	装置識別子
IEEE802.3ah/UDLD	装置識別子
L2 ループ検知	装置識別子

12.2 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 12-5 コンフィグレーションコマンド一覧

コマンド名	説明
bandwidth	帯域幅を設定します。
description	補足説明を設定します。
duplex	duplex を設定します。
flowcontrol	フローコントロールを設定します。
frame-error-notice	フレーム受信エラーおよびフレーム送信エラー発生時のエラーの通知条件を設定します。
interface gigabitethernet	10BASE-T/100BASE-TX/1000BASE-T インタフェースおよび，SERDES（サーバ接続ポート）のコンフィグレーションを指定します。
interface tengigabitethernet	10GBASE-R のコンフィグレーションを指定します。
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	自動 MDIX 機能を設定します。
mtu	イーサネットの MTU を設定します。
shutdown	イーサネットをシャットダウンします。
speed	速度を設定します。
system flowcontrol off	装置内の全ポートでフローコントロールを無効にします。
system mtu	イーサネットの MTU の装置としての値を設定します。

12.2.2 複数インタフェースの一括設定

［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，複数のインタフェースに同じ情報を設定することがあります。このような場合，複数のインタフェースを 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 gigabitethernet 0/1-2, tengigabitethernet 0/25**
   1G ビットイーサネットインタフェース 0/1 から 0/2，および 10G ビットイーサネットインタフェース 0/25 への設定を指定します。

2. **(config-if-range)# ＊＊＊＊＊**
   複数のインタフェースに同じコンフィグレーションを一括して設定します。

12.2.3 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イーサネッ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。したがって，最初にイーサネッ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イーサネットのシャットダウンを解除することを推奨します。なお，使用しないイーサネッ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 0/4**
   イーサネットインタフェース 0/10 の設定を指定します。

2. **(config-if)# shutdown**
   イーサネットインタフェースをシャットダウンします。

3. **(config-if)# ＊＊＊＊＊**
   イーサネットインタフェース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
   イーサネットインタフェース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 でイーサネットの運用を停止することもできます。ただし，inactivate コマンドで inactive 状態とした場合は，装置を再起動するとイーサネットが active 状態になります。イーサネットをシャットダウンした場合は，装置を再起動してもイーサネットは 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。

12.2.4　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。

ジャンボフレームを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 タグ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 タグが二つ付く場合は，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）ポート単位の MTU の設定

［設定のポイント］

ポート 0/10 のポートの MTU を 8192 オクテットに設定します。この設定によって，VLAN タグの付かないフレームであれば 8206 オクテット，VLAN タグ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 0/4**
   (config-if)# shutdown

(config-if)# mtu 8192
ポート 0/4 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]

本装置の全イーサネットインタフェースでポートの MTU を 4096 オクテットに設定します。この設定によって，VLAN タグの付かないフレームであれば 4110 オクテット，VLAN タグ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**
装置の全ポートで，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。

12.2.5　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 0/4**
イーサネットインタフェース 0/4 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。

12.2.6　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 0/4**
   イーサネットインタフェース 0/4 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。

12.2.7　フレーム送受信エラー通知の設定

軽度のエラーが発生してフレームの受信または送信に失敗した場合，本装置はフレームが廃棄された原因を統計情報として採取します。30 秒間に発生したエラーの回数とエラーの発生する割合が閾値を超えた場合は，エラーの発生をログおよびプライベートトラップで通知します。

本装置では，閾値とエラーが発生した場合の通知について設定ができます。設定がない場合，30 秒間に 15 回エラーが発生したときに最初の 1 回だけログを表示します。

(1)　エラーフレーム数を閾値にしての通知

[設定のポイント]

エラーの通知条件のうち，エラーの発生回数（エラーフレーム数）の閾値を本装置に設定する場合は，frame-error-notice コマンドで error-frames を設定します。

[コマンドによる設定]

1. **(config)# frame-error-notice error-frames 50**
   エラーの発生回数（エラーフレーム数）の閾値を 50 回に設定します。

(2) エラーレートを閾値にしての通知

[設定のポイント]

エラーの通知条件のうち，エラーの発生割合（エラーレート）の閾値を本装置に設定する場合は，frame-error-notice コマンドで error-rate を設定します。

[コマンドによる設定]

1. **(config)# frame-error-notice error-rate 20**

   エラーの発生割合の閾値を 20% に設定します。

(3) 通知時のログ表示設定

[設定のポイント]

エラーの通知条件のうち，エラーが発生したときのログの表示を設定する場合は，frame-error-notice コマンドで onetime-display，または everytime-display を設定します。ログを表示しないようにする場合は，off を設定します。この設定は，プライベートトラップには関係しません。

[コマンドによる設定]

1. **(config)# frame-error-notice everytime-display**

   エラーが発生するたびにログを表示します。

(4) 条件の組み合わせ設定

[設定のポイント]

エラーの通知条件を複数組み合わせて設定する場合は，frame-error-notice コマンドで，複数の条件を同時に設定します。frame-error-notice コマンド入力前に設定していた通知条件は無効となりますので，引き続き同じ通知条件を設定する場合は，frame-error-notice コマンドで再度設定し直してください。

[コマンドによる設定]

すでにエラーが発生するたびにログを表示することを設定していて，さらにエラーの発生割合（エラーレート）の閾値を設定する場合の設定例を示します。

1. **(config)# frame-error-notice error-frames 50 everytime-display**

   エラーの発生回数（エラーフレーム数）の閾値を 50 回に設定し，エラーが発生するたびにログを表示します。

[注意事項]

プライベートトラップを使用する場合は，snmp-server host コマンドでフレーム受信エラー発生時のトラップとフレーム送信エラー発生時のトラップを送信するように設定してください。

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

イーサネットで使用する運用コマンド一覧を次の表に示します。

表 12-6　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。
show port statistics	イーサネットの統計情報を一覧で表示します。
show port transceiver	トランシーバ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。
show power inline	PoE 情報を表示します。

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

show port コマンドを実行すると，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。

show port コマンドの実行結果を次の図に示します。

図 12-3 「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
Date 2009/01/21 15:16:19 UTC
Port Counts: 24
Port  Name           Status   Speed        Duplex     FCtl FrLen ChGr/Status
 0/ 1 geth0/1        up       1000BASE-T   full(auto) off   1518   -/-
 0/ 2 geth0/2        down     -            -          -     -      -/-
 0/ 3 geth0/3        up       100BASE-TX   full(auto) off   1518   -/-
 0/ 4 geth0/4        up       1000BASE-T   full(auto) off   1518   -/-
 0/ 5 geth0/5        up       SERDES       full(auto) off   1518   -/-
      :
      :
```

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（UTP）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 にインタフェースはポート 0/1 から 0/4 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，全二重および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 12-7　伝送速度および，全二重および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
	10BASE-T/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
	10BASE-T/100BASE-TX/1000BASE-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，伝送速度および，全二重および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 12-7　伝送速度および，全二重および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。

(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 12-8　フローコントロールの送信動作」，「表 12-9　フローコントロールの受信動作」および「表 12-10　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 12-8　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 12-10　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 12-10　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 12-9　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 12-10　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 12-10　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 12-10　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	行わない	行う
			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	行わない	行う
			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	行わない
			無効	off	off	行わない	行わない
			desired	on	off	行う	行わない
		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 12-11　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。コンフィグレーションコマンド ip mtu の MTU 長を合わせて変更することで，IP パケットをフラグメント化するサイズを大きくすることもできます。

本装置では，Ethernet V2 形式フレームだけをサポートします。802.3 形式フレームはサポートしていません。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 12-12　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※1	IEEE802.3※1	
フレーム長（オクテット）	1519 ～ 9234	×	MAC ヘッダの DA ～データの長さ。FCS は含みません。
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※ 1　「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） 10BASE-T ／ 100BASE-TX ／ 1000BASE-T 接続時の注意事項

- 伝送速度，および全二重および半二重モードが相手装置と不一致の場合，接続できないので注意してください。
  不一致の状態で通信を行うと，以降の通信が停止することがあります。この場合，当該ポートに対して inactivate コマンド，activate コマンドを実行してください。
- 全二重インタフェースはコリジョン検出とループバック機能を行わないことによって実現しています。このため，10BASE-T または 100BASE-TX を全二重インタフェース設定で使用する場合，相手接続ポートは必ず全二重インタフェースに設定して接続してください。
- 1000BASE-T を使用する場合は全二重のオートネゴシエーションだけとなります。

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

12.5.1　イーサネットの設定

（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。デフォルトではオートネゴシエーションで，相手装置と伝送速度と duplex を決定します。なお本装置の 10BASE-T ／ 100BASE-TX ／ 1000BASE-T にインタフェースはポート 0/1 から 0/4 です。

(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 0/1**
   (config-if)# shutdown
   (config-if)# speed 10
   (config-if)# duplex half
   相手装置と 10BASE-T 半二重で接続する設定をします。

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

(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 0/1**
   (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

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。

本装置では，フローコントロールをポート単位に設定したり，装置内の全ポートでフローコントロールを無効にしたりできます。装置内の全ポートでフローコントロールを無効にすると，ポート単位のフローコントロールの設定はコンフィグレーションファイルに残りますが，動作しません。

(1) ポート単位のフローコントロールの設定

[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 0/1**
   (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

(2) 全ポート共通のフローコントロールの設定

[設定のポイント]

装置内の全ポートでフローコントロールを無効にします。本設定は装置を再起動するか，VLAN プログラムを再起動したときに有効になります。

[コマンドによる設定]

1. **(config)# system flowcontrol off**
   全ポートで相手装置とのポーズパケット送受信の停止を設定します。

2. **(config)# save**
   (config)# exit
   保存して，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ます。

3. **# restart vlan**
   VLAN プログラムを再起動します。全ポートで相手装置とのポーズパケット送受信を停止します。すべてのイーサネットインタフェースが再初期化され，VLAN を構成しているポートは一時的にデータの送受信ができなくなります。

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。

[設定のポイント]

自動 MDIX を MDI-X に固定する場合に，固定したいインタフェースに設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/2**
   イーサネットインタフェース 0/2 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　サーバ接続ポートの解説

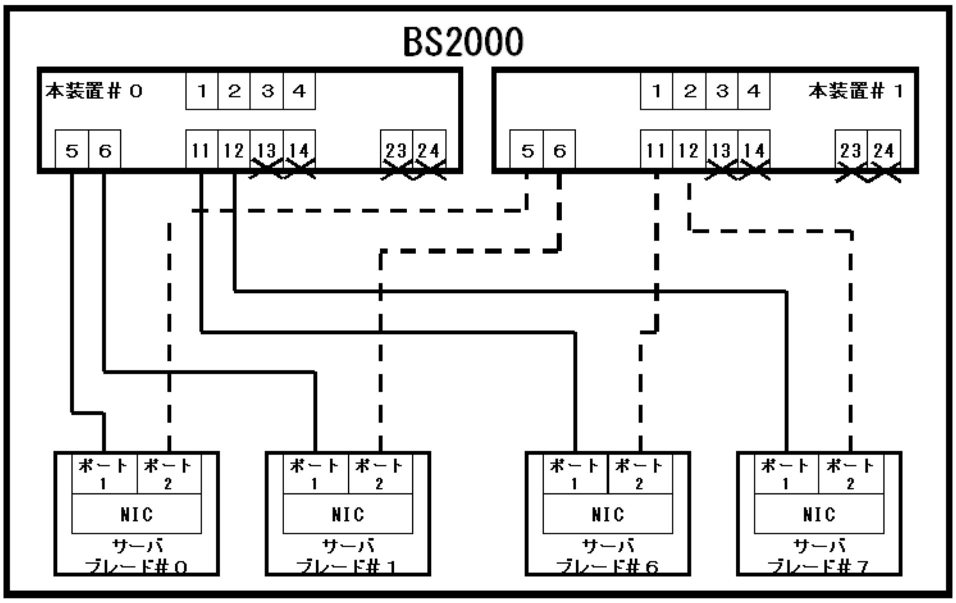
12.6.1　機能一覧

本装置のポート 0/5 からポート 0/24 は，BS2000 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となっております。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

サーバ接続ポートとサーバブレードは BS2000 内で以下のように接続しています。

図 12-4　サーバ接続ポートとサーバブレードの接続



「図 12-4　サーバ接続ポートとサーバブレードの接続」は，BS2000 に本装置２台（スイッチベイ＃０とスイッチベイ＃１に設置）とサーバブレード８台設置）の接続図です。上記図のように本装置をスイッチベイ＃０とスイッチベイ＃１に搭載すると，サーバ接続ポートのポート 0/13 から 0/24 はサーバブレードと未接続になります。BS2000 では SERDES とサーバブレードが未接続となるポートがあります。この未接続となるポートは，スイッチモジュールを設置するスイッチベイによって異なります。詳細は「表 1-2　BS2000 サーバブレードと未接続の SEREDES のポート番号」を参照願います。

（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 12-13　サーバ接続ポート仕様」に示します。

表 12-13　サーバ接続ポート仕様

項目	内容	備考
伝送速度	1000Mbit/s（固定）	通信速度の変更不可 ※
通信タイプ	全二重（固定）	半二重の変更不可 ※
オートネゴシエーション	有り	

項目	内容	備考
伝送速度	1000Mbit/s（固定）	通信速度の変更不可 ※
フローコントロール	有り	
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※　伝送速度および通信タイプは 1000Mbit/s 全二重固定であるため，変更することはできません。

(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

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，サーバブレード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，サーバブレード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って決定したモードを選択できます。本装置とサーバブレード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，サーバブレードのポーズパケット受信は有効に設定してください。本装置とサーバブレードの設定内容と実行動作モードを「表 12-14　フローコントロールの送信動作，「表 12-15　フローコントロールの受信動作」および「表 12-16　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 12-14　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 12-16　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 12-16　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 12-15　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 12-16　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 12-16　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 12-16　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	行わない	行う
			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	行わない	行う
			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	行わない
			無効	off	off	行わない	行わない
			desired	on	off	行う	行わない
		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	行う	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

(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。コンフィグレーションコマンド ip mtu の MTU 長を合わせて変更することで，IP パケットをフラグメント化するサイズを大きくすることも可能となります。

本装置では，Ethernet V2 形式フレームだけをサポートします。802.3 形式フレームはサポートしていません。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。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 12-17　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）	1519 ～ 9234	×	MAC ヘッダの DA ～データの長さ。FCS は含みません。
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。

12.7　サーバ接続ポートのコンフィグレーション

12.7.1　サーバ接続ポートの設定値

（1）速度と duplex の設定値

本装置のサーバ接続ポートの速度と duplex の設定値を以下に示します。

表 12-18　サーバ接続ポートの速度と duplex の設定値

ポート番号	伝送速度	duplex
ポート 0/5 〜 0/24	1000Mbit/s 固定	全二重 固定

[注意事項]

サーバ接続ポートに設定値を上記「表 12-18　サーバ接続ポートの速度と duplex の設定値」から変更すると，サーバブレードとの通信障害となるケースがありますので，この設定値のままご使用ください。

12.7.2　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サーバブレードに送信規制を要求します。サーバブレード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。

サーバブレード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サーバブレード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，サーバブレード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 0/5
(config-if)# flowcontrol send off
(config-if)# flowcontrol receive off
(config-if)# exit
```
相手装置とのポーズパケット送受信を停止します。

12.7.3　ジャンボフレームの設定

イーサネットインタフェースでジャンボフレームを受信できるようにするためには，ポートの MTU を設定します。ポートの MTU の設定には，その回線で送受信できる IPv4 パケットの最大長を指定します。本装置では，指定された MTU の IPv4 パケットに，VLAN タグ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。

[設定のポイント]

ポートの MTU の設定値は，ネットワークおよびサーバブレードと合わせて決定します。VLAN トンネリングなどで，VLAN タグが二つ付く場合は，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。
ここでは，ポートのMTUを8192オクテットに設定します。この設定によって，VLANタグの付かないフレームであれば8206オクテット，VLANタグ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-if)# mtu 8192**
   ポートのMTUを8192オクテットに設定します。

12.8　10GBASE-R の解説

12.8.1　機能一覧

10GBASE-R の光ファイバを使用したインタフェースについて説明します。

(1) 接続インタフェース

(a) 10GBASE-R

10GBASE-SR，10GBASE-LR をサポートしています。回線速度は 10Gbit/s 全二重固定です。

10GBASE-SR：
　短距離間を接続するために使用します。(マルチモード，伝送距離：最大 300m※)

　注※
　　伝送距離は使用するケーブルによって異なります。。

10GBASE-LR：
　中距離間を接続するために使用します。(シングルモード，伝送距離：最大 10km)

［注意事項］

10GBASE-ER と 10GBASE-ZR はサポートしていませんので，使用することはできません。

(b) 10GBASE-R 接続仕様

10GBASE-SR の物理仕様を「表 12-19　10GBASE-SR 物理仕様」，10GBASE-LR の物理仕様を「表 12-20　10GBASE-LR 物理仕様」に示します。

表 12-19　10GBASE-SR 物理仕様

項目	物理仕様				
ケーブル種	マルチモード				
コア / クラッド径	50/125μm			62.5/125μm	
伝送帯域	400MHz・km	500MHz・km	2000MHz/・km	160MHz/・km	200MHz・km
発光中心波長	0.840 ～ 0.860μm				
光送信電力（平均値）	－ 7.3 ～ － 1.0dBm				
光受信電力（平均値）	－ 9.9 ～ － 1.0dBm				
光伝送損失（最大値）	2.6dB				
伝送距離	2m ～ 66m	2m ～ 82m	2m ～ 300m	2m ～ 26m	2m ～ 33m

表 12-20　10GBASE-LR 物理仕様

項目	物理仕様
ケーブル種	シングルモード
コア / クラッド径	62.5/125μm
発光中心波長	1.260 ～ 1.355μm
光送信電力（平均値）	－ 8.2 ～ + 0.5dBm

項目	物理仕様
光受信電力（平均値）	− 14.4 ～ ＋ 0.5dBm
光伝送損失（最大値）	6.2dB
伝送距離	2m ～ 10Km

（2） 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。

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，送信と受信とでそれぞれ設定でき，有効または無効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を「表 12-21　フローコントロールの送信動作」および「表 12-22　フローコントロールの受信動作」に示します。

表 12-21　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 : 有効

表 12-22　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 : 有効

（3） 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。コンフィグレーションコマンド ip mtu の MTU 長を合わせて変更することで，IP パケットをフラグメント化するサイズを大きくすることもできます。

本装置では，Ethernet V2 形式フレームだけをサポートします。802.3 形式フレームはサポートしていません。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。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 12-23　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※1	IEEE802.3※1	
フレーム長（オクテット）	1519 ～ 9234	×	MAC ヘッダの DA ～データの長さ。FCS は含みません。
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※ 1 「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。

（4） 10GBASE-R 接続時の注意事項

- 10GBASE-R の半二重およびオートネゴシエーションは IEEE802.3ae 規格にないので，全二重固定接続だけになります。
- マニュアル「BladeSymphony ユーザーズガイド」に示すトランシーバ以外を使用した場合の動作は保証できません。

12.9　10GBASE-R のコンフィグレーション

12.9.1　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。また，相手装置で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，フローコントロールをポート単位に設定したり，装置内の全ポートでフローコントロールを無効にしたりできます。装置内の全ポートでフローコントロールを無効にすると，ポート単位のフローコントロールの設定はコンフィグレーションファイルに残りますが，動作しません。

（1） ポート単位のフローコントロールの設定

［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 tengigabitethernet 0/25**
   (config-if)# shutdown
   イーサネットインタフェースをシャットダウンします。

2. **(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。

3. **(config-if)# no shutdown**
   (config-if)# exit
   イーサネットインタフェースのシャットダウンを解除します。

（2） 全ポート共通のフローコントロールの設定

［設定のポイント］

　装置内の全ポートでフローコントロールを無効にします。

［コマンドによる設定］

1. **(config)# system flowcontrol off**
   全ポートで相手装置とのポーズパケット送受信の停止を設定します。

2. **(config)# save**
   (config)# exit
   保存して，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ます。

3. **# restart vlan**
   VLAN プログラムを再起動します。全ポートで相手装置とのポーズパケット送受信を停止します。すべてのイーサネットインタフェースが再初期化され，VLAN を構成しているポートは一時的にデータの送受信ができなくなります。

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

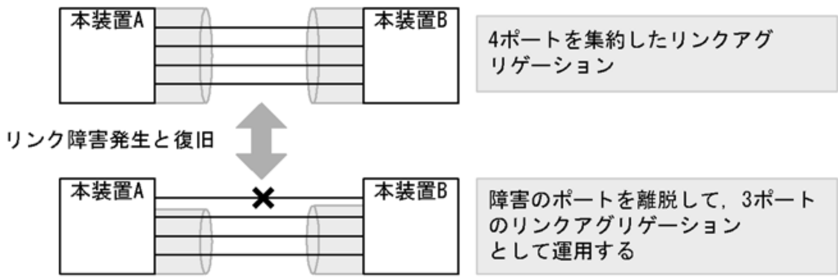
13.1.1　概要

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
装置当たりのリンクアグリゲーショングループ数	32	−
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	デフォルト時：同一速度だけを使用します。 異速度混在モード時：異なる速度を同時に使用します。	デフォルト時：遅い回線は離脱します。 異速度混在モード時：回線速度による離脱はありません。
Duplex モード	全二重だけ	−

（凡例）　−：該当しない

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

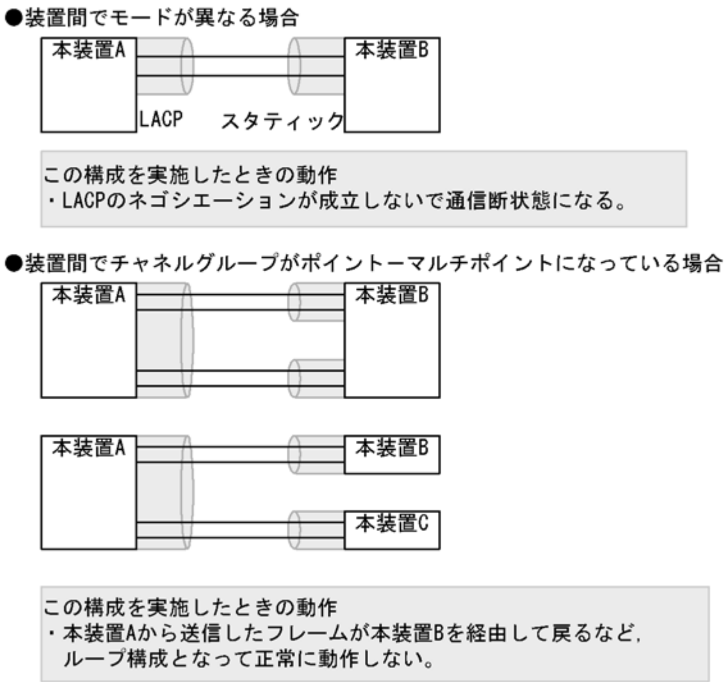
中継	フレームの種類	振り分けに使用する情報
レイヤ 3 中継	IP ユニキャスト IP ブロードキャスト	宛先 IP アドレス 送信元 IP アドレス 宛先 TCP/UDP ポート番号 送信元 TCP/UDP ポート番号
	IP マルチキャスト	宛先 IP アドレス 送信元 IP アドレス 受信ポート番号または受信チャネルグループ番号
レイヤ 2 中継	MAC アドレス未学習フレーム（ブロードキャスト，マルチキャスト含む）	宛先 MAC アドレス 送信元 MAC アドレス 受信ポート番号または受信チャネルグループ番号
	MAC アドレス学習済の IP フレーム	宛先 IP アドレス 送信元 IP 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



（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，タイムアウトのメッセージ出力，一時的な通信断になることがあります。過負荷状態が頻発する場合は，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登録します。
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を設定します。 チャネルグループのパラメータもポートチャネルインタフェースモードで設定します。
lacp port-priority	LACP のポート優先度を設定します。
lacp system-priority	LACP システム優先度のデフォルト値を設定します。
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 channel-group mode コマンド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 channel-group mode コマンド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 0/1-2**
   ポート 0/1，0/2 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 10 mode on**
   (config-if-range)# exit
   ポート 0/1，0/2 を，スタティックモードのチャネルグループ 10 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 channel-group mode コマンド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 0/1-2**
   ポート 0/1，0/2 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 10 mode active**
   (config-if-range)# exit
   ポート 0/1，0/2 を LACP モードのチャネルグループ 10 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。本装置では，システム優先度は拡張機能の離脱ポート制限機能で使用します。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 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 10**
   (config-if)# channel-group lacp system-priority 50
   (config-if)# exit
   チャネルグループ 10 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 0/1**
   (config-if)# lacp port-priority 100
   (config-if)# exit
   ポート 0/1 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 10**
(config-if)# channel-group periodic-timer short
(config-if)# exit
チャネルグループ 10 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 channel-group mode コマンド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機能を設定します。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 channel-group mode コマンドを設定すると，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，channel-group mode コマンド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 channel-group mode コマンドを設定する場合，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，channel-group mode コマンド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。

ポートチャネルインタフェースとイーサネットインタフェースで一致している必要のある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 trunk
	switchport protocol
	switchport mac
	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
GSRP	gsrp direct-link
	gsrp reset-flush-port
	gsrp no-flush-port
	gsrp exception-port
OADP	oadp enable
IEEE802.1X	dot1x port-control
	dot1x force-authorize-port
	dot1x multiple-hosts
	dot1x multiple-authentication
	dot1x max-supplicant
	dot1x reauthentication
	dot1x timeout reauth-period
	dot1x timeout tx-period
	dot1x timeout supp-timeout
	dot1x timeout server-timeout
	dot1x timeout keep-unauth
	dot1x timeout quiet-period
	dot1x max-req
	dot1x ignore-eapol-start
	dot1x supplicant-detection
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 0/1-2**
   (config-if-range)# channel-group 10 mode on
   (config-if-range)# exit
   ポート 0/1，0/2 をスタティックモードのチャネルグループ 10 に登録します。また，チャネルグループ 10 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 10**
   チャネルグループ 10 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**
   チャネルグループ 10 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 0/1-2**
   (config-if-range)# channel-group 10 mode on
   (config-if-range)# exit
   ポート 0/1，0/2 をスタティックモードのチャネルグループ 10 として登録します。

2. **(config)# interface port-channel 10**
   (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 0/1，0/2 の通信が停止し，チャネルグループ 10 は停止状態になります。

13.2.5　サーバ接続ポートへのリンクアグリゲーションの設定方法

サーバ接続ポートにはデフォルトで spanning-tree portfast trunk を設定しています。サーバ接続ポートにリンクアグリゲーションの設定を行う場合は，ポートチャネルインタフェースに spanning-tree portfast trunk を設定しておく必要があります。

[設定のポイント]

コンフィグレーションコマンドでポートチャネルインタフェースの設定を行い，このポートチャネルインタフェースに spanning-tree portfast trunk を設定します。その後イーサネットインタフェース

モードで channel-group mode コマンドを設定します。ここではポート 0/5 とポート 0/6 をスタティックリングアグリゲーションで設定する例を示します。

［コマンドによる設定］

1. **(config)# interface port-channel 10**
   チャネルグループ 10 のチャネルグループを設定します。

2. **(config-if)# spanning-tree portfast trunk**
   (config-if)# exit
   チャネルグループ 10 に PortFast 機能を設定します。

3. **(config)# interface gigabitethernet 0/5**
   (config-if)# channel-group 10 mode on
   (config-if)# exit
   ポート 0/5 をスタテックモードのチャネルグループ 10 に登録します。

4. **(config)# interface gigabitethernet 0/6**
   (config-if)# channel-group 10 mode on
   (config-if)# exit
   ポート 0/6 をスタテックモードのチャネルグループ 10 に登録します。

13.2.6　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 に設定しておく必要があります。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 0/1**
   (config-if)# shutdown
   ポート 0/1 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 0/1 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 channel-group mode コマンド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 0/1-2**
   (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 10**
   チャネルグループ 10 を削除します。ポート 0/1，0/2 に設定されている channel-group mode コマンド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だけ使用できます。

（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。

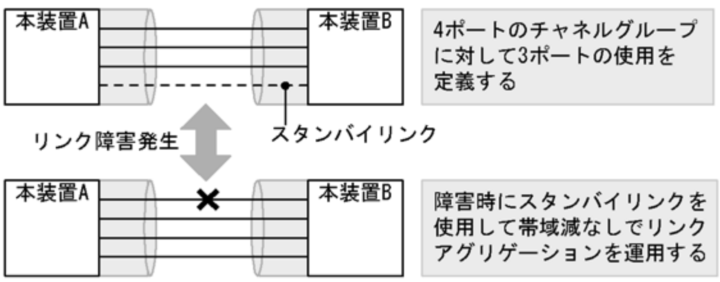
待機用ポートは，コンフィグレーションで設定するポート優先度，ポート番号から選択されます。待機用ポートは，次の表に示すように選択優先度の高い順に決定します。

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



（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，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。

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，次に示すどちらかの状態です。

- 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。
- 異速度混在モードを未設定で，最高速のポートが一つだけ，そのほかのポートが一つ以上ある状態。

13.3.2　離脱ポート制限機能

離脱ポート制限機能は，リンクに障害が発生したポートを離脱して残りのポートで運用を継続する機能を抑止します。チャネルグループのどれかのポートに障害が発生するとグループ全体を障害とみなして，該当チャネルグループの運用を停止します。グループ内の全ポートが復旧するとグループの運用を再開します。

GSRP などの冗長化機能と合わせて運用することで，チャネルグループ内に 1 ポートだけ障害が発生した場合でも，グループ単位で経路を切り替えることができます。

この機能は LACP リンクアグリゲーションだけ使用できます。

離脱ポート制限機能の集約動作は，チャネルグループで接続する装置間で，優先度の高い装置が，自装置および対向装置のチャネルグループ内の全ポートで集約可能な状態と判断できた場合に集約します。そうすることで，一部のポートだけが集約することがないようにしており，帯域保証しています。

優先度は，コンフィグレーションで設定する LACP システム優先度，チャネルグループの MAC アドレスによって，次の表に示すように決定します。すなわち LACP システム優先度が同じだった場合は，チャネルグループの MAC アドレスで判断します。

表 13-6　チャネルグループ内の全ポートが集約可能か判定する装置の決定方法

優先度	パラメータ	備考
高 ↑	LACP システム優先度	LACP システム優先度の値が小さい装置が優先
↓ 低	チャネルグループの MAC アドレス	MAC アドレスの小さい装置が優先

13.3.3　異速度混在モード

異なる速度のポートを一つのチャネルグループで同時に使用するモードです。通常は同じ速度のポートでチャネルグループを構成しますが，異なる速度のポートで構成することで，スタンバイリンクに低速ポートを使用することや，チャネルグループの構成変更を容易に行えます。本機能の適用例を次に示します。

なお，フレーム送信時のポート振り分けにはポートの速度は反映しません。例えば，異速度混在モードで 1Gbit/s のポートと 10Gbit/s のポートを使用していても，その速度の差はフレーム振り分けには反映しません。通常の運用時は同じ速度のポートで運用することをお勧めします。

（1）スタンバイリンク機能での適用例

高速なポートに対して低速なポートを待機用ポートにすることができます。例えば，10Gbit/s ポートで接続する際に，最大ポート数を 1 としてスタンバイリンク機能を適用して，待機用ポートに 1Gbit/s のポー

トを設定します。10Gbit/s のポートに障害が発生した場合にも 1Gbit/s のポートで通信を継続できます。

異速度混在モードでスタンバイリンクを適用する際は，最大ポート数を 1 とすることをお勧めします。最大ポート数を 2 以上とした場合は，通常運用に異なる速度のポートが混在することがあります。また，最大ポート数を 1 として運用する場合は，非リンクダウンモードを使用することをお勧めします。リンクダウンモードで最大ポート数が 1 の場合は，切り替え時にチャネルグループがいったんダウンします。

(2) チャネルグループの構成変更手順での適用例

本機能によって，チャネルグループで利用するポートの速度を変更（ネットワーク構成の変更）する際に，チャネルグループをダウンさせないで構成を変更できます。

異速度混在モードを利用したチャネルグループの速度移行について，移行手順の具体例を次に示します。

1. 従来状態で運用（100Mbit/s のポート 0/1 〜 0/2 の 2 ポートとします）

図 13-4　従来状態で運用

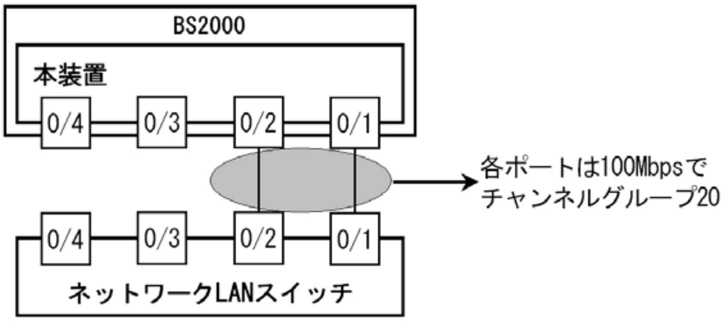


図 13-5　従来状態の設定内容例

```
interface gigabitethernet 0/1
  speed 100
  duplex full
  switchport mode access
  channel-group 20 mode on

interface gigabitethernet 0/2
  speed 100
  duplex full
  switchport mode access
  channel-group 20 mode on

interface gigabitethernet 0/3
  speed 1000
  duplex full
  switchport mode access

interface gigabitethernet 0/4
  speed 1000
  duplex full
  switchport mode access
```

2. 異速度混在モードを設定

(config)# inteface channel-group 20

チャンネルグループ 20 のポートチャン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。

(config-if)# channel-group multi-speed

(config-if)# exit

チャネルグループ 20 に異速度混在モードを設定します。

3. チャネルグループに 1Gbit/s の 2 ポートを追加

(config)# interface range gigabitethernet 0/3-4

(config-if-range)# channel-group 20 mode on

(config-if-range)# exit

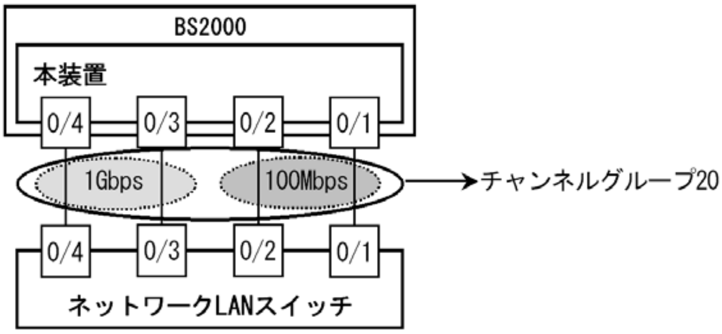
ポート 0/3，0/4 をチャネルグループ 20 として登録します。

注

手順 2 で異速度混在モードを設定しないと，この手順でリンクアグリゲーションがいったんダウンします。

4. 手順 3 で追加した 1Gbit/s の 2 ポート (ポート 0/3 と 0/4) をリンクアップ

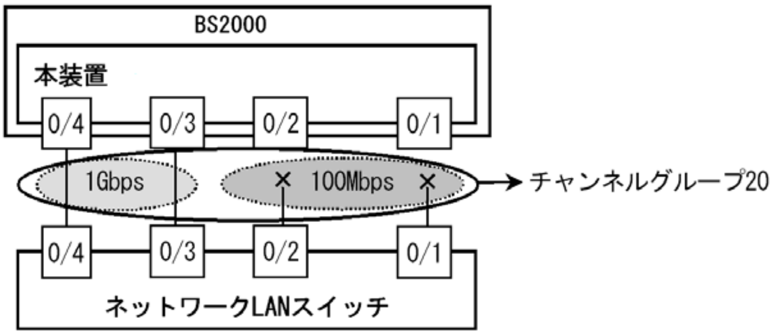
図 13-6　異速度混在モード状態 (100Mbit/s の 2 ポートと 1Gbit/s の 2 ポート)



注
手順 3 を実施する前に追加するポートをリンクアップさせると，フレーム周回してしまうため，必ず追加するポートをチャンネルグループに登録してから，リンクアップしてください。

5. 従来の 100Mbit/s の 2 ポートをリンクダウン

図 13-7　異速度混在モード状態 (100Mbit/s の 2 ポートと 1Gbit/s の 2 ポート)



従来の 100Mbit/s の 2 ポートをリンクダウンさせます。

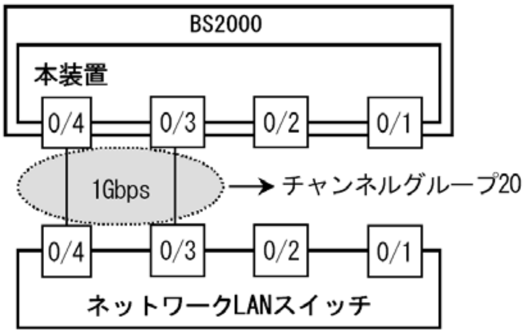
6. 従来の 100Mbit/s の 2 ポートをチャネルグループから削除

```
(config)# interface range gigabitethernet 0/1-2
(config-if-range)# no channel-group
(config-if-range)# exit
```

ポート 0/1，0/2 からチャネルグループの設定を解除します。

7. 1Gbit/s の 2 ポートに移行完了

図 13-8　1Gbit/s の 2 ポートに移行完了状態



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 13-7　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。離脱ポート制限機能で集約条件を判定する装置を決定します。
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。
channel-group max-detach-port	離脱ポート制限機能を設定します。
channel-group multi-speed	異速度混在モードを設定します。
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	システム優先度のデフォルト値を設定します。離脱ポート制限機能で集約条件を判定する装置を決定します。

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 10**
   チャネルグループ 10 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 10 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 10 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 20**
   (config-if)# channel-group max-active-port 1 no-link-down
   (config-if)# exit
   チャネルグループ 20 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 0/1**
   (config-if)# channel-group 20 mode on

(config-if)# lacp port-priority 300
(config-if)# exit
チャネルグループ 20 にポート 0/1 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。

13.4.3 離脱ポート制限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離脱ポート制限機能を設定します。本コマンドではチャネルグループから離脱することを許容する最大ポート数に 0 と 7 のどちらかを指定します。7 を指定した場合は離脱ポート制限機能を設定しない場合と同じです。

離脱ポート制限機能をサポートしている装置と接続する場合，接続先の装置と本設定を合わせてください。離脱ポート制限機能をサポートしていない装置と接続する場合，本装置の LACP システム優先度を高くしてください。LACP システム優先度は値が小さいほど優先度が高くなります。

離脱ポート制限機能は，LACP リンクアグリゲーションだけで使用できます。

［コマンドによる設定］

1. **(config)# interface port-channel 10**
   チャネルグループ 10 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-detach-port 0**
   チャネルグループ 10 に離脱ポート制限機能を設定します。離脱を許容する最大ポート数を 0 とし，障害などによって 1 ポートでも離脱した場合にチャネルグループ全体を障害とみなします。

3. **(config-if)# channel-group lacp system-priority 100**
   (config-if)# exit
   チャネルグループ 10 のシステム優先度を 100 に設定します。

13.4.4 異速度混在モード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異速度混在モードを設定します。本機能を設定すると，ポートの速度は離脱条件ではなくなります。

［コマンドによる設定］

1. **(config)# interface port-channel 10**
   チャネルグループ 10 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 multi-speed**
   (config-if)# exit
   チャネルグループ 10 に異速度混在モードを設定します。

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 13-8　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。
restart link-aggregation	リンクアグリゲーションプログラムを再起動します。
dump protocols link-aggregation	リンクアグリゲーションの詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。

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 show channel-group コマンドで表示します。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。

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

図 13-9　show channel-group コマンドの実行結果

```
> show channel-group 1
Date 2009/01/07 13:13:38 UTC
channel-group Counts:1
ChGr:1    Mode:LACP
CH Status    :Up        Elapsed Time:10:10:39
Multi Speed  :Off
Max Active Port:8
Max Detach Port:7
MAC address: 0012.e2ac.8301     VLAN ID:10
Periodic Timer:Short
Actor   information: System Priority:1     MAC: 0012.e212.ff02
                     KEY:1
Partner information: System Priority:10000 MAC: 0012.e2f0.69be
                     KEY:10
Port(4)        :0/1/4
Up Port(2)     :0/1-2
Down Port(2)   :0/3-4
>
```

(2)　各ポートの運用状態の確認

show channel-group detail コマンド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。Status が Down 状態のときは Reason で理由を確認できます。

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

図 13-10　show channel-group detail コマンドの実行結果

```
> show channel-group detail
Date 2009/01/07 13:13:38 UTC
channel-group Counts:1
ChGr:1    Mode:LACP
  CH Status    :Up       Elapsed Time:00:13:51
  Multi Speed  :Off
  Max Active Port:8
  Max Detach Port:7
  MAC address: 0012.e205.0545     VLAN ID:10
  Periodic Timer:Long
  Actor   information: System Priority:128   MAC: 0012.e205.0540
                       KEY:1
  Partner information: System Priority:128   MAC: 0012.e2c4.2b5b
                       KEY:1
  Port Counts:4        Up Port Counts:2
  Port:0/1   Status:Up    Reason:-
             Speed :100M  Duplex:Full  LACP Activity:Active
             Actor   Priority:128     Partner Priority:128
  Port:0/2   Status:Up    Reason:-
             Speed :100M  Duplex:Full  LACP Activity:Active
             Actor   Priority:128     Partner Priority:128
  Port:0/3   Status:Down  Reason:Duplex Half
             Speed :100M  Duplex:Half  LACP Activity:Active
             Actor   Priority:128     Partner Priority:0
  Port:0/4   Status:Down  Reason:Port Down
             Speed :-     Duplex:-     LACP Activity:Active
             Actor   Priority:128     Partner Priority:0
>
```

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。

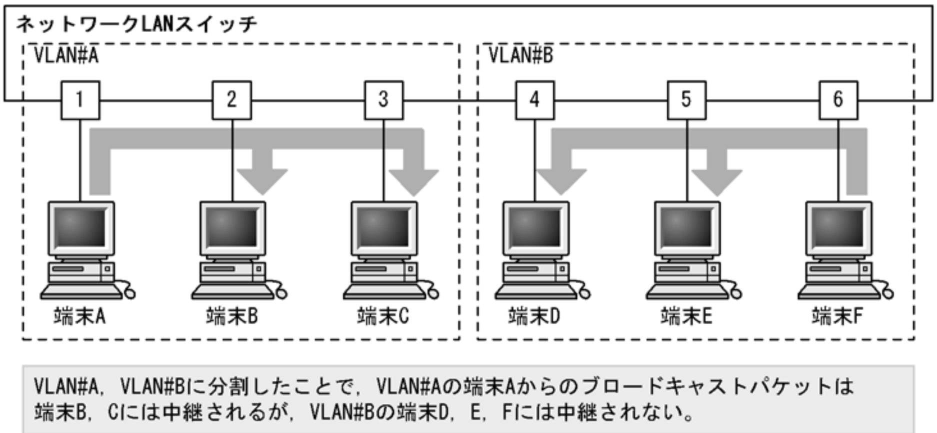
レイヤ 2 スイッチは，MAC アドレステーブルのエントリに従ってフレームを中継します。フレームの宛先 MAC アドレスに一致するエントリがあると，そのエントリのポートに中継します（エントリのポートが受信したポートである場合は中継しません)。一致するエントリがない場合，受信したポート以外のすべてのポートにフレームを中継します。この中継をフラッディングと呼びます。

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
	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 変換機能	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。
	VLAN ごと MAC アドレス	レイヤ 3 インタフェースの MAC アドレスを VLAN ごとに異なるアドレスにする機能
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
		IEEE802.1X ポート単位認証	一部制限あり※2
		IEEE802.1X VLAN 単位認証 (動的)	共存不可
		ポートミラーリング (ミラーポート)	
	プロトコル VLAN	デフォルト VLAN	共存不可
		VLAN トンネリング	
		PVST+	
		IEEE802.1X ポート単位認証	
		IEEE802.1X VLAN 単位認証 (静的)	
		IEEE802.1X VLAN 単位認証 (動的)	
		ポートミラーリング (ミラーポート)	
		Web 認証（固定 VLAN モード）	一部制限あり※3
		Web 認証（ダイナミック VLAN モード）	一部制限あり※4
		MAC 認証（固定 VLAN モード）	一部制限あり※5
		MAC 認証（ダイナミック VLAN モード）	一部制限あり※6
	MAC VLAN	デフォルト VLAN	共存不可
		VLAN トンネリング	
		PVST+	
		IEEE802.1X ポート単位認証	
		IEEE802.1X VLAN 単位認証 (静的)	
		IEEE802.1X VLAN 単位認証 (動的)	一部制限あり※7
		ポートミラーリング (ミラーポート)	共存不可
		Web 認証（固定 VLAN モード）	一部制限あり※3※8
		MAC 認証（固定 VLAN モード）	一部制限あり※5
デフォルト VLAN		プロトコル VLAN	共存不可
		MAC VLAN	
		IGMP snooping	
		MLD snooping	
		IEEE802.1X VLAN 単位認証 (静的)	
		IEEE802.1X VLAN 単位認証 (動的)	

使用したい機能		制限のある機能	制限の内容
		ポートミラーリング (ミラーポート)	
VLAN 拡張機能	Tag 変換機能	PVST+	共存不可
		IGMP snooping	
		MLD snooping	
	VLAN トンネリング	ポート VLAN	一部制限あり※ 1
		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	
		IEEE802.1X ポート単位認証	
		IEEE802.1X VLAN 単位認証 (静的)	
		IEEE802.1X VLAN 単位認証 (動的)	
		Web 認証（固定 VLAN モード）	一部制限あり※ 3
		Web 認証（ダイナミック VLAN モード）	一部制限あり※ 4
		MAC 認証（固定 VLAN モード）	一部制限あり※ 5
		MAC 認証（ダイナミック VLAN モード）	一部制限あり※ 6
	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	
		MSTP	
	L2 プロトコルフレーム透過機能 (EAP)	IEEE802.1X ポート単位認証	共存不可
		IEEE802.1X VLAN 単位認証 (静的)	
		IEEE802.1X VLAN 単位認証 (動的)	

注※ 1
VLAN トンネリング機能を使用する場合は，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
トランクポートでは，IEEE802.1X のポート単位認証を使用できません。

注※ 3
Web 認証（固定 VLAN モード）の認証ポートには使用できません。

注※ 4
Web 認証（ダイナミック VLAN モード）の認証ポートには使用できません。

注※ 5
MAC 認証（固定 VLAN モード）の認証ポートには使用できません。

注※ 6
MAC 認証（ダイナミック VLAN モード）の認証ポートには使用できません。

注※ 7

IEEE802.1X の VLAN 単位認証（動的）は，MAC ポートだけで使用できます。MAC VLAN のトランクポートは，自動的に認証除外ポートになります。

注※ 8

Web 認証（ダイナミック VLAN モード）で MAC VLAN のポートが使用できます。

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 変換機能	
	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	
	GSRP	
	アップリンクフェイルオーバー	
	IEEE802.1X	一部制限あり※
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	
	GSRP	
	アップリンクフェイルオーバー	
	IEEE802.1X	一部制限あり※
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	
	GSRP	
	アップリンクフェイルオーバー	
	IEEE802.1X	一部制限あり※

注※

スパニングツリーと IEEE802.1X を同時に使用する場合，認証を行うポートには PortFast を設定するか，またはルートブリッジで認証するかしてください。

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	IEEE802.1X	一部制限あり※

注※

Ring Protocol と IEEE802.1X を同時に使用する場合，認証を行うポートに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
	Tag 変換機能	
	VLAN トンネリング	
	Web 認証（固定 VLAN モード）	
	Web 認証（ダイナミック VLAN モード）	
	MAC 認証（固定 VLAN モード）	
	MAC 認証（ダイナミック VLAN モード）	
MLD snooping	デフォルト VLAN	共存不可
	Tag 変換機能	
	VLAN トンネリング	

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むだなトラフィックを抑止します。

MAC アドレス学習では，チャネルグループを一つのポートとして扱います。

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タイムアウトまで保持します。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。異なる VLAN であれば同一の MAC アドレスを学習することもできます。

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，エージングタイム内に同じ送信元 MAC アドレスからフレームを受信しなかった場合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。エージングタイム内にフレームを受信した場合は，エージングタイマを更新しエントリを保持します。エージングタイムを設定できる範囲を次に示します。

- エージングタイムの範囲：0，10 〜 1000000（秒）
  0 は無限を意味し，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。また，ポートを指定するのではなく「廃棄」を指定することもできます。その場合，指定の宛先 MAC アドレスまたは送信元 MAC アドレスのフレームはどのポートにも中継されないで廃棄されます。

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 アドレスが指定できます。
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／廃棄指定	一つのポートまたはチャネルグループを指定できます。また，項番 1，2 に該当するフレームを廃棄する指定ができます。

15.1.6　注意事項

（1） MAC アドレス学習と ARP，NDP について

本装置では，レイヤ 3 中継で ARP や NDP によってアドレス解決した NextHop の MAC アドレスは MAC アドレステーブルに登録されている必要があります。そのため，次の点に注意してください。

- MAC アドレス学習の情報をコマンドやエージングなどによってクリアすると，MAC アドレスに対応する ARP や NDP の情報がいったんクリアされます。クリアされた ARP や NDP のエントリは，通信の必要に応じて再解決を行います。
- MAC アドレス学習のエージングタイムが ARP や NDP のエージングタイムより短い場合，MAC アドレス学習のエージングによって対応する ARP や NDP のエントリをクリアします。このクリアは，MAC アドレス学習のエージングタイムを ARP や NDP のエージングタイム以上の時間にすることで回避できます。

（2） MAC アドレス学習移動検出の制限

収容するイーサネットインタフェース数が 48 ポート以上のモデルで，ポート 1 ～ 24 および 49 ～ 50 とポート 25 ～ 48 との間で PC などの端末を移動した場合，移動前のポートで学習した MAC アドレスが

残った状態になることがあります。

その状態では，移動前のポートにフレームを送信しようとするため，通信が正常に行えないことがあります。

この現象が発生した場合は，移動前のポートで学習したエントリがエージングにより削除されるのを待つか，clear mac-address-table コマンドで移動前のポートで学習したエントリを削除してください。

(3) ユニキャスト通信の制限

収容するイーサネットインタフェース数が 48 ポート以上のモデルで，ポート 1 ～ 24 および 49 ～ 50 に接続されている端末同士がユニキャスト通信を行っている場合，そのどちらかの端末に対しポート 25 ～ 48 に接続されている端末からユニキャスト通信を行うと，VLAN 内の一部にフラッディングされることがあります。

この現象が発生した場合，宛先としている端末からマルチキャストまたはブロードキャストが送信されるか，双方向通信をすると解消されます。

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 15-3　コンフィグレーションコマンド一覧

コマンド名	説明
mac-address-table aging-time	MAC アドレス学習のエージングタイムを設定します。
mac-address-table static	スタティックエントリを設定します。

15.2.2　エージングタイムの設定

［設定のポイント］

MAC アドレス学習のエージングタイムを変更できます。設定は装置単位です。設定しない場合，エージングタイムは 300 秒で動作します。

［コマンドによる設定］

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

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，廃棄のどれかを指定します。

(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 0012.e200.1122 vlan 10 interface gigabitethernet 0/1**
VLAN 10 で，宛先 MAC アドレス 0012.e200.1122 のフレームの出力先をポート 0/1 に設定します。

［注意事項］

VLAN 10 で，送信元 MAC アドレス 0012.e200.1122 のフレームをポート 0/1 以外から受信した場合は廃棄します。

(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 0012.e200.1122 vlan 10 interface port-channel 5**
   VLAN 10 で，宛先 MAC アドレス 0012.e200.1122 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 0012.e200.1122 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。

(3) 廃棄を指定するスタティックエントリ

［設定のポイント］

指定した MAC アドレス宛および指定した MAC アドレスからのフレームを廃棄に設定します。

［コマンドによる設定］

1. **(config)# mac-address-table static 0012.e200.1122 vlan 10 drop**
   VLAN 10 で，宛先および送信元 MAC アドレス 0012.e200.1122 のフレームを廃棄に設定します。

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 15-4　運用コマンド一覧

コマンド名	説明
show mac-address-table	MAC アドレステーブルの情報を表示します。 learning-counter パラメータを指定すると，MAC アドレス学習の学習アドレス数をポート単位に表示します。
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 show mac-address-table コマンドで表示します。MAC アドレステーブルに登録されている MAC アドレスとその MAC アドレスを宛先とするフレームの中継先を確認してください。このコマンドで表示されない MAC アドレスを宛先とするフレームは VLAN 全体にフラッディングされます。

show mac-address-table コマンドでは，MAC アドレス学習によって登録したエントリ，スタティックエントリ，IEEE802.1X，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 コマンドの実行結果

```
> show mac-address-table
Date 2009/01/14 12:08:41 UTC
MAC address         VLAN    Type     Port-list
0012.e22d.eefa         1    Dynamic  0/2
0012.e212.2e5f         1    Dynamic  0/5
0012.e205.0641      4094    Dynamic  0/1
0012.e28e.0602      4094    Dynamic  0/1
>
```

15.3.3　MAC アドレス学習数の確認

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

```
> show mac-address-table learning-counter port 0/1-12
Date 2009/01/14 12:09:40 UTC
Port counts:12
Port       Count
0/1            0
0/2            1
0/3            0
0/4            0
0/5            1
0/6            0
0/7            0
0/8           20
0/9            0
0/10           0
0/11           0
0/12           0
>
```

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。	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。	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。	すべての種類の VLAN
トンネリングポート	VLAN トンネリングのポート VLAN 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

アクセスポート，プロトコルポート，MAC ポートは Untagged フレームを扱うポートです。これらのポートで Tagged フレームを扱うことはできません。Tagged フレームを受信したときは廃棄し，また送信することもありません。

Tagged フレームはトランクポートでだけ扱うことができます。トランクポートの Untagged フレームはネイティブ VLAN が扱います。

トンネリングポートは，VLAN トンネリングをするポートで，フレームが Untagged か，Tagged かを区別しないで扱います。

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。プロトコル VLAN と MAC VLAN は同じポートで使用できません。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

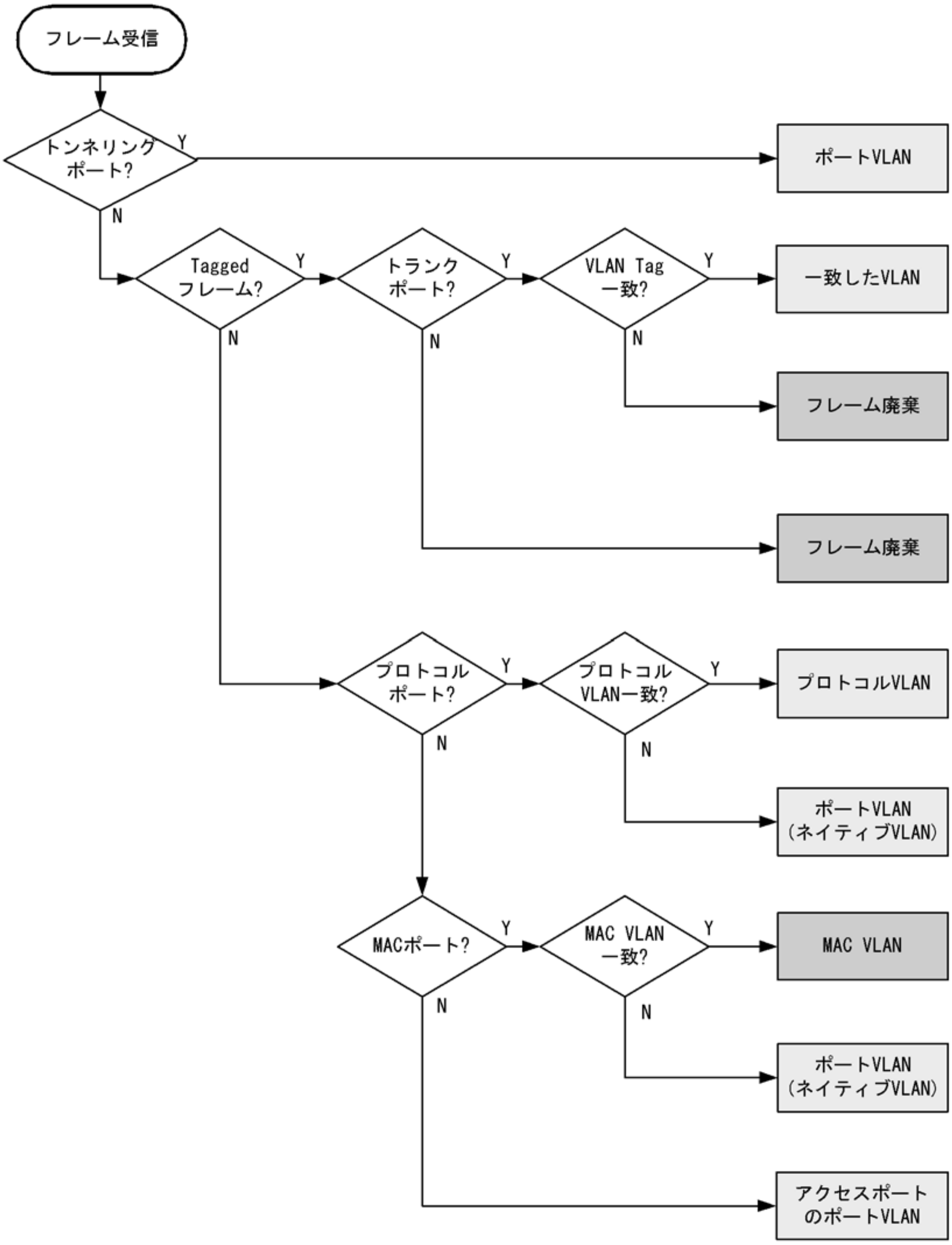
フレームを受信したとき，受信したフレームの VLAN を判定します。VLAN 判定の優先順位を次の表に示します。

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	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

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



16.1.5　VLAN Tag

(1)　概要

IEEE802.1Q 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。

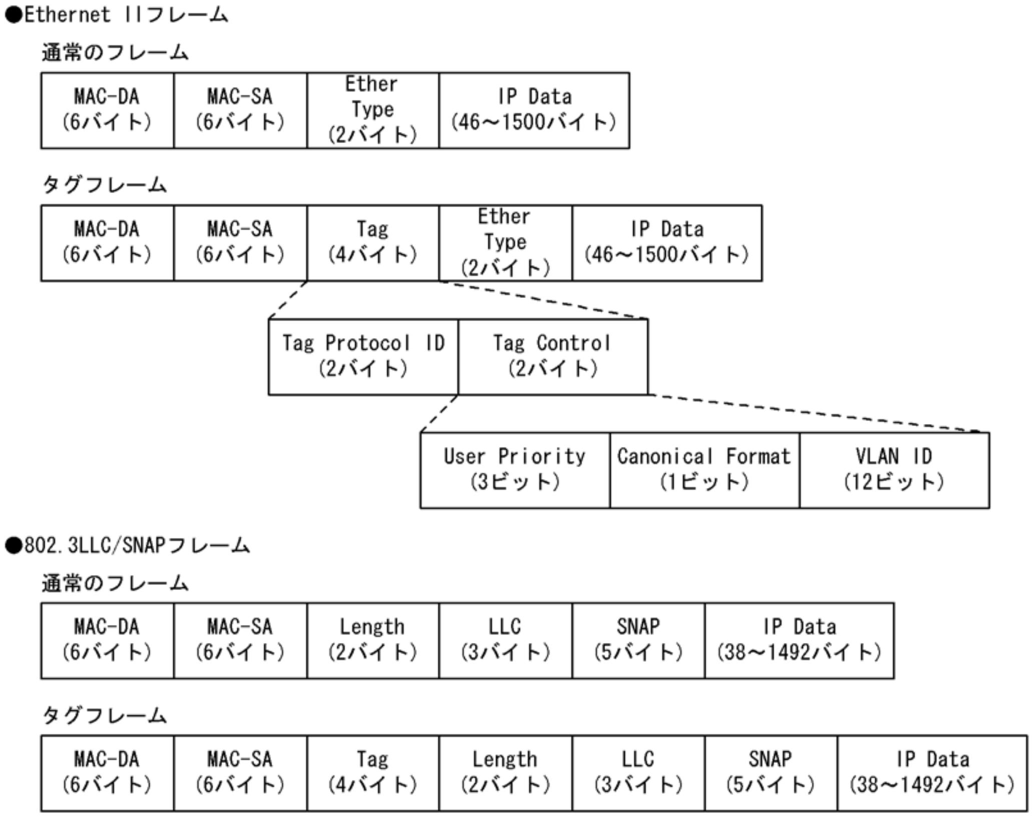
VLAN Tag はトランクポートで使用します。トランクポートはその対向装置も VLAN Tag を認識できなければなりません。

(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。

VLAN Tag 付き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　VLAN Tag 付き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 変換機能を使用している場合，Tag 変換機能で設定した 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。受信したフレームが Untagged フレームの場合および自発送信の場合は，User Priority がデフォルト値の 3 になります。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，「コンフィグレーションガイド Vol.2　3.7 マーカー解説」を参照してください。

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 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 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。

vlan コマンドによって，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 0/1**
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 access**
(config-if)# exit
ポート 0/1 をアクセスポートに設定します。ポート 0/1 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 10**
チャネルグループ 10 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 10 をトランクポートに設定します。ポートチャネル 10 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，switchport mode コマンドを設定しただけではどの VLAN にも所属していません。このポートで扱う VLAN は switchport trunk allowed vlan コマンドによって設定します。

VLAN の追加と削除は，switchport trunk vlan add コマンドおよび switchport trunk vlan remove コマンドによって行います。すでに switchport trunk allowed vlan コマンドを設定した状態でもう一度 switchport trunk allowed vlan コマンドを実行すると，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)# interface gigabitethernet 0/1
(config-if)# switchport mode trunk
VLAN 10 ～ 20，100，200 ～ 300 を作成します。また，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，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 0/1 に VLAN 10 〜 20 を設定します。ポート 0/1 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 0/1 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 0/1 で扱う VLAN から VLAN 15 および VLAN 16 を削除します。この状態で，ポート 0/1 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 0/1 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。

トランクポートで，一度に削除する VLAN 数が 30 以上の場合，および所属している VLAN 数が 30 以上のときにモードをトランクポート以外に変更する場合は，該当ポートの mac-address-table，ARP および NDP を削除します。そのため，L3 中継を行っている場合は，いったん ARP/NDP を再学習して通信が中断するので注意してください。

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。vlan-dot1q-ethertype コマンドで装置のデフォルト値を，switchport dot1q ethertype コマンド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 9100 として動作します。

2. **(config)# interface gigabitethernet 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。

3. **(config-if)# switchport dot1q ethertype 8100**
   (config-if)# exit

ポート 0/1 の TPID を 0x8100 に設定します。ポート 0/1 は 0x8100 を VLAN Tag として認識します。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

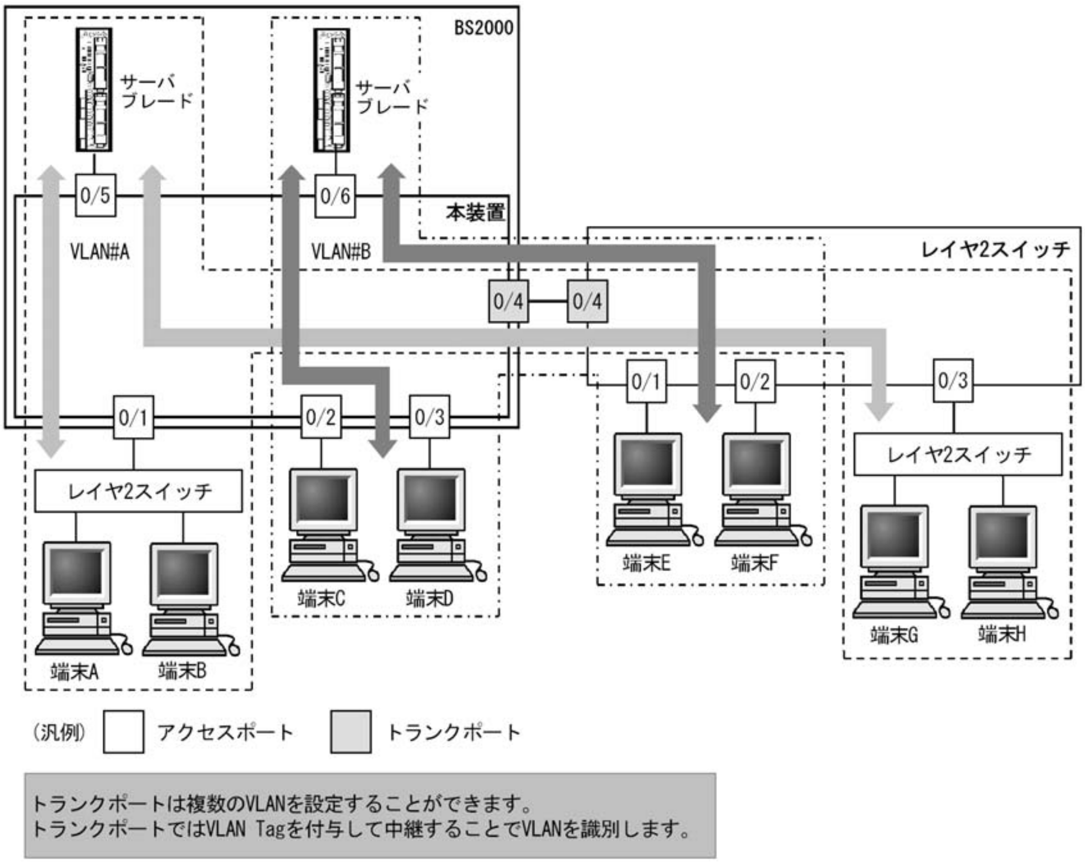
ポート単位に VLAN のグループ分けを行います。

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 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 スイッチのポート 0/4 とは，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。

(2) MAC VLAN 混在時の注意事項

同一ポートにポート VLAN と MAC VLAN が混在する場合，マルチキャスト使用時の注意事項があります。詳細は，「16.7.4　VLAN 混在時のマルチキャストについて」を参照してください。

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

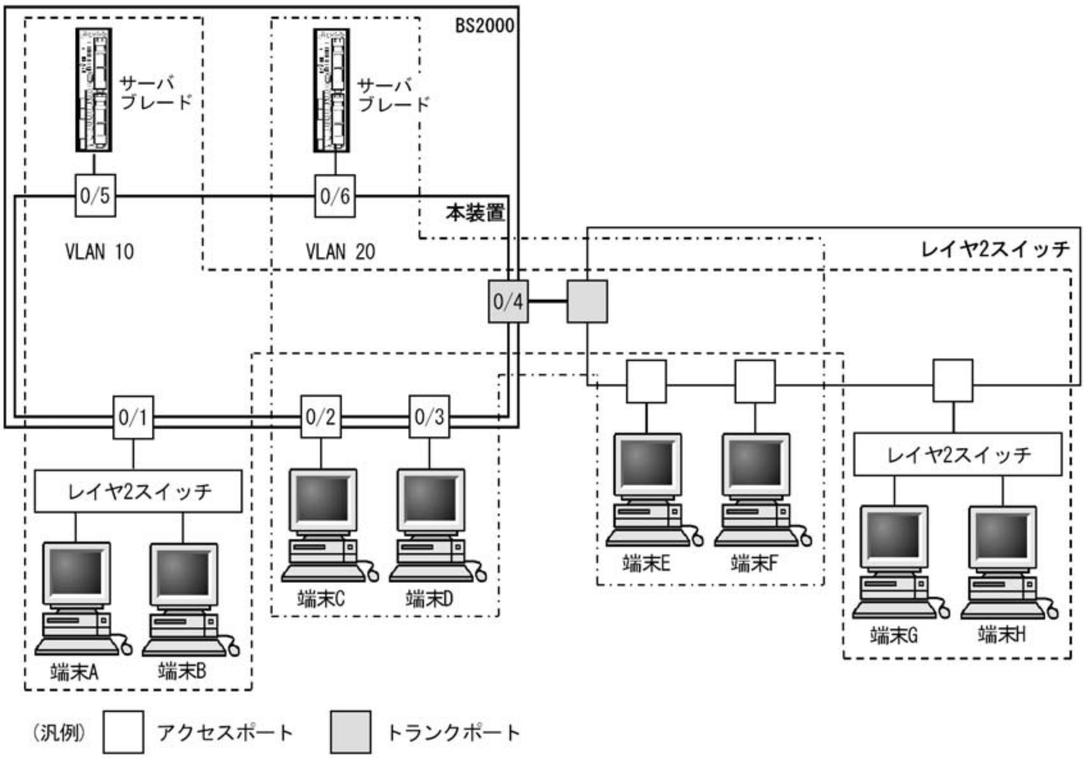
コマンド名	説明
switchport access	アクセスポートの VLAN を設定します。
switchport mode	ポートの種類（アクセス，トランク）を設定します。
switchport trunk	トランクポートの VLAN を設定します。
vlan	ポート VLAN を作成します。また，VLAN コンフィグレーションモードで VLAN に関する項目を設定します。

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 はポート VLAN 10 を設定します。ポート 0/2，0/3 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**
   VLAN ID 10，VLAN ID 20 をポート 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) アクセスポートの設定

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

［設定のポイント］

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

［コマンドによる設定］

1. **(config)# interface gigabitethernet 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 access**
   (config-if)# switchport access vlan 10
   (config-if)# exit
   ポート 0/1 をアクセスポートに設定します。また，VLAN 10 を設定します。

3. **(config)# interface range gigabitethernet 0/2-3**
   ポート 0/2，0/3 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 0/2，0/3 は同じコンフィグレーションとなるため，一括して設定します。

4. **(config-if-range)# switchport mode access**
   (config-if-range)# switchport access vlan 20
   (config-if-range)# exit
   ポート 0/2，0/3 をアクセスポートに設定します。また，VLAN 20 を設定します。

(3) トランクポートの設定

［設定のポイント］

Tagged フレームを扱うポートはトランクポートとして設定し，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 だけを設定できます。

ネイティブ VLAN の VLAN ID を switchport trunk allowed vlan コマンドで指定すると，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)# interface gigabitethernet 0/1**
   (config-if)# switchport mode trunk
   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，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 0/1 のネイティブ VLAN はデフォルト VLAN です。

3. **(config-if)# switchport trunk native vlan 10**
   (config-if)# switchport trunk allowed vlan 1,10,20
   (config-if)# exit
   トランクポート 0/1 のネイティブ VLAN を VLAN 10 に設定します。また，VLAN 1，10，20 を設定します。ネイティブ VLAN である VLAN 10 が Untagged フレームを扱い，VLAN 1（デフォルト VLAN），VLAN 20 は Tagged フレームを扱います。

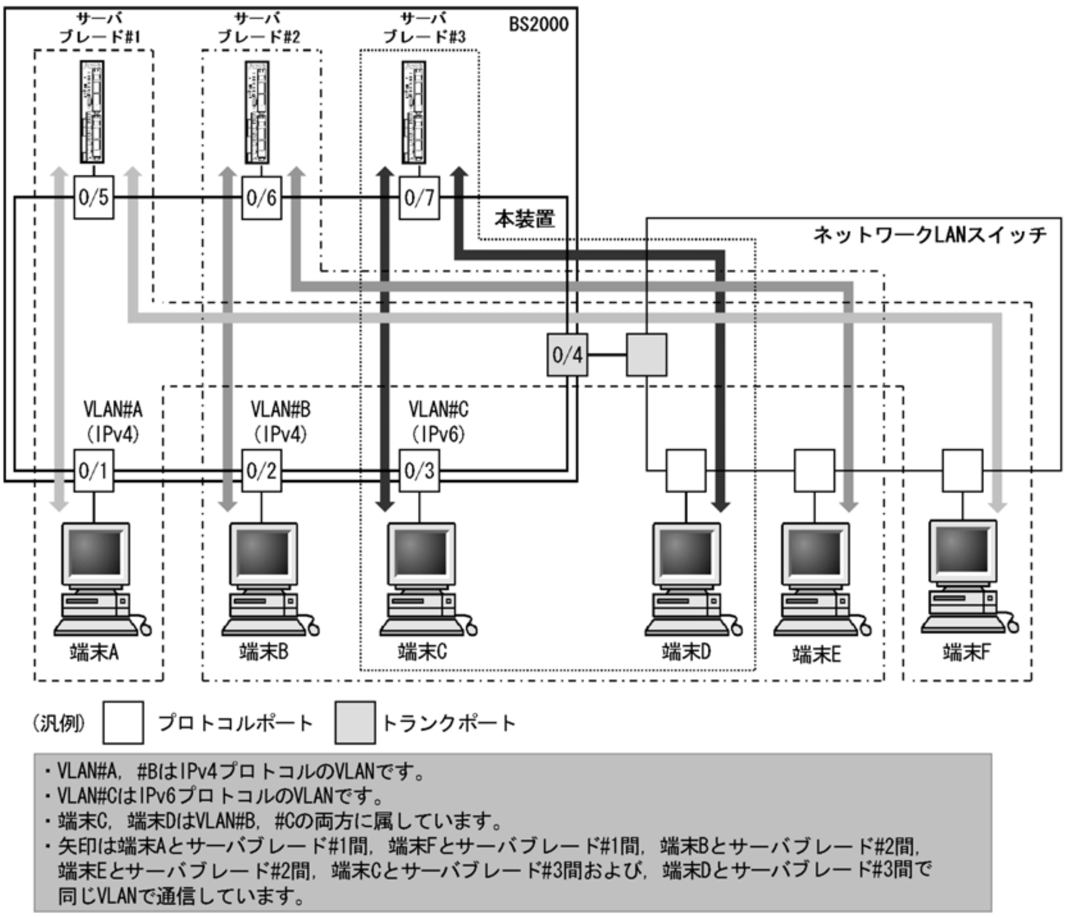
16.5　プロトコル VLAN の解説

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
Ether-type 値	EthernetV2 形式フレームの Ether-type 値によってプロトコルを識別します。
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。

識別する値	概要
SNAP Ether-type 値	802.3 形式フレームの Ether-type 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

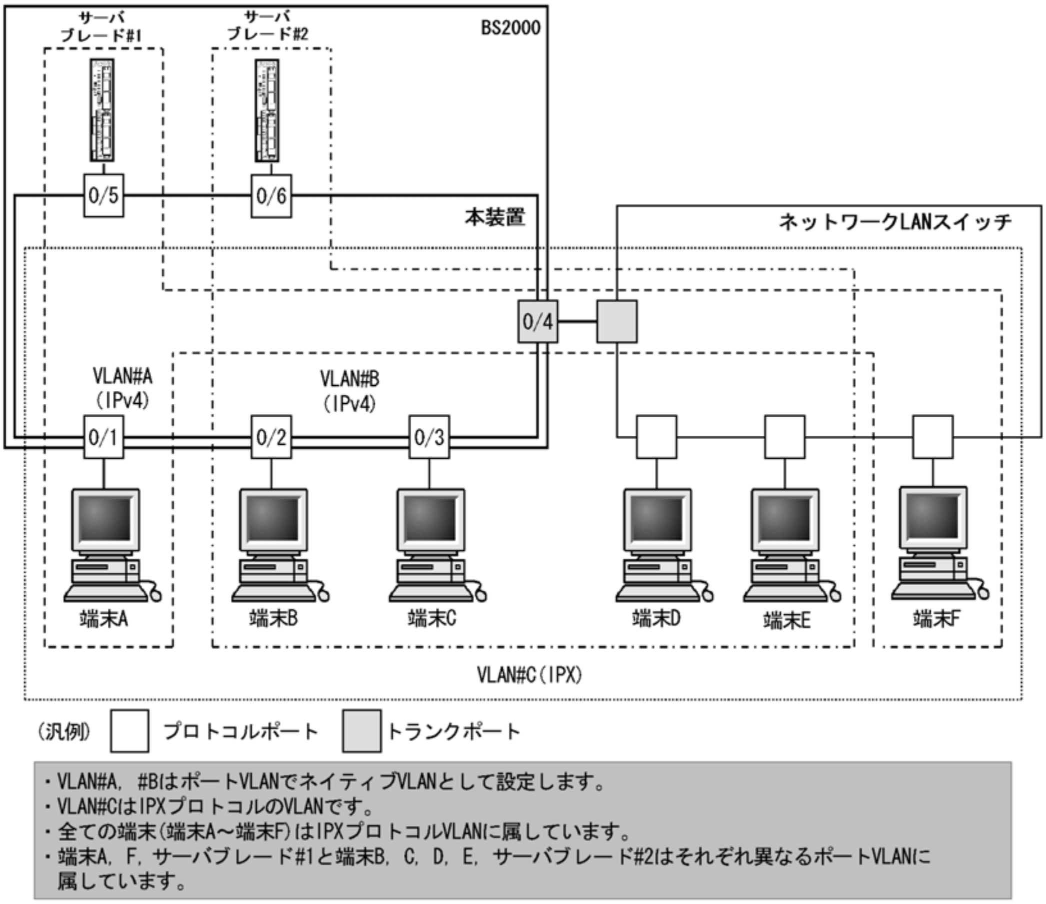
プロトコルポートは Untagged フレームのプロトコルを識別します。プロトコル VLAN として使用するポートはプロトコルポートを設定します。プロトコルポートには複数のプロトコルで異なる VLAN を割り当てることもできます。複数のプロトコル VLAN をほかの LAN スイッチなどに接続するためにはトランクポートを使用します。なお，トランクポートは VLAN Tag によって VLAN を識別するため，プロトコルによる識別は行いません。

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



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

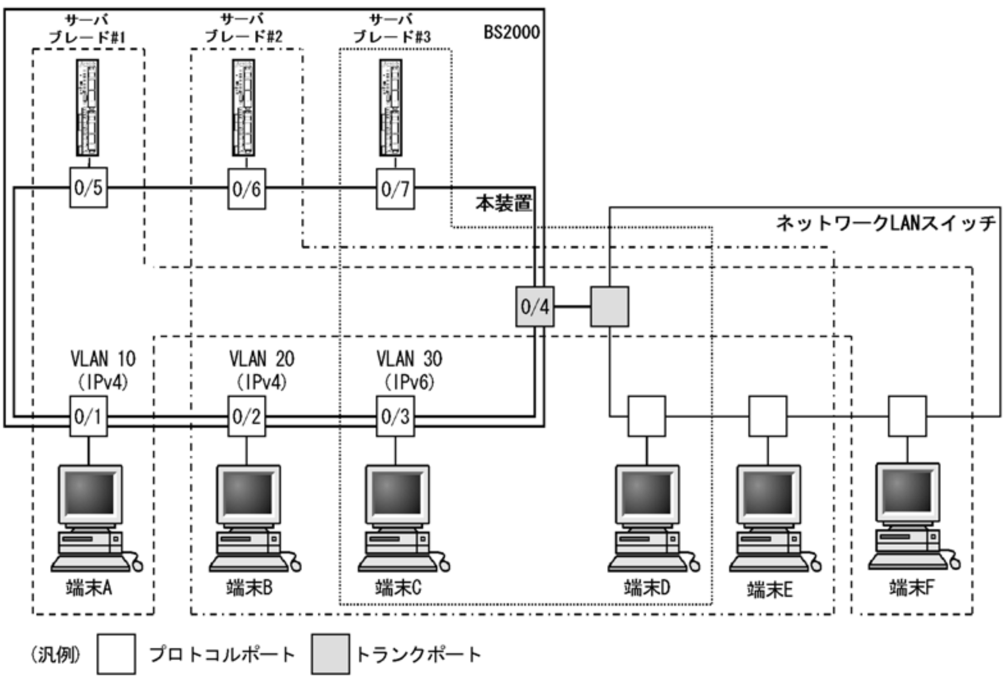
コマンド名	説明
protocol	プロトコル VLAN で VLAN を識別するプロトコルを設定します。
switchport mode	ポートの種類（プロトコル，トランク）を設定します。
switchport protocol vlan	プロトコルポートの VLAN を設定します。
switchport trunk	トランクポートの VLAN を設定します。
vlan-protocol	プロトコル VLAN 用のプロトコル名称とプロトコル値を設定します。
vlan protocol-based	プロトコル VLAN を作成します。また，VLAN コンフィグレーションモードで VLAN に関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 0/1，0/5 は IPv4 プロトコル VLAN 10 を設定します。ポート 0/2，0/3，0/6 は IPv4 プロトコル VLAN 20 を設定します。ポート 0/7 は IPv6 プロトコル VLAN 30 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 Ether-type と同時に ARP の Ether-type 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 ethertype 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 Ether-type 値 0800 と ARP の Ether-type 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 Ether-type 値 86DD を関連づけます。

（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 プロトコルを指定します。

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 プロトコルを指定します。

（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 gigabitethernet 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 gigabitethernet 0/5**
   (config-if)# switchport mode protocol-vlan
   (config-if)# switchport protocol vlan 10
   (config-if)# exit
   ポート 0/5 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。

4. **(config)# interface range gigabitethernet 0/2-3**
   (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。

5. **(config)# interface gigabitethernet 0/6**
   (config-if) #switchport mode protocol-vlan
   (config-if)# switchport protocol vlan 20
   (config-if)# exit
   ポート 0/6 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。

6. **(config)# interface gigabitethernet 0/7**
   (config-if) #switchport mode protocol-vlan
   (config-if)# switchport protocol vlan 30
   (config-if)# exit
   ポート 0/7 をプロトコルポートに設定します。また，VLAN 30 を設定します。

7. **(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 0/5 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)# switchport mode trunk**
   (config-if)# switchport trunk allowed vlan 10,20,30
   (config-if)# exit
   ポート 0/5 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 だけを設定できます。

ネイティブ VLAN の VLAN ID を switchport protocol native vlan コマンドで指定すると，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 0/1**
   (config-if)# switchport mode protocol-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，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 0/1 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

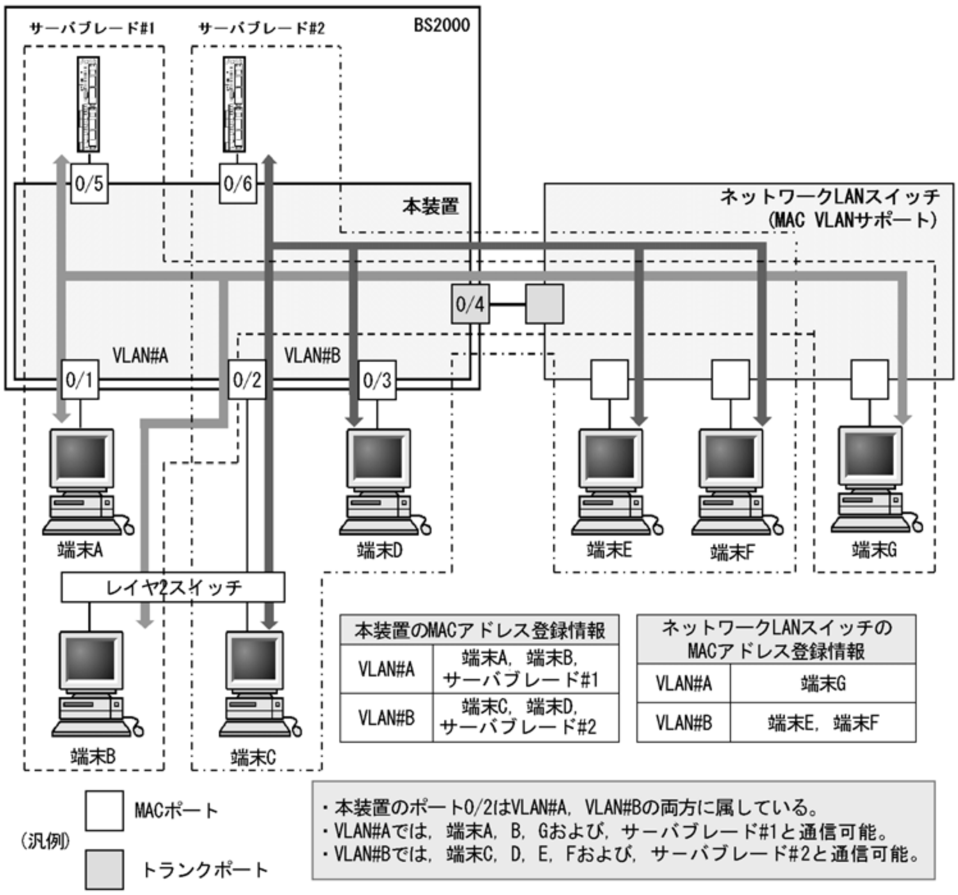
送信元の MAC アドレス単位に VLAN のグループ分けを行います。VLAN への MAC アドレスの登録は，コンフィグレーションによる登録と，レイヤ 2 認証機能による動的な登録ができます。

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。

さらに，コンフィグレーションコマンド mac-based-vlan static-only を設定すると，MAC VLAN の最大収容数までコンフィグレーションコマンド mac-address で MAC アドレスを設定できます。なお，この場合，レイヤ 2 認証機能を動作させることはできません。

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



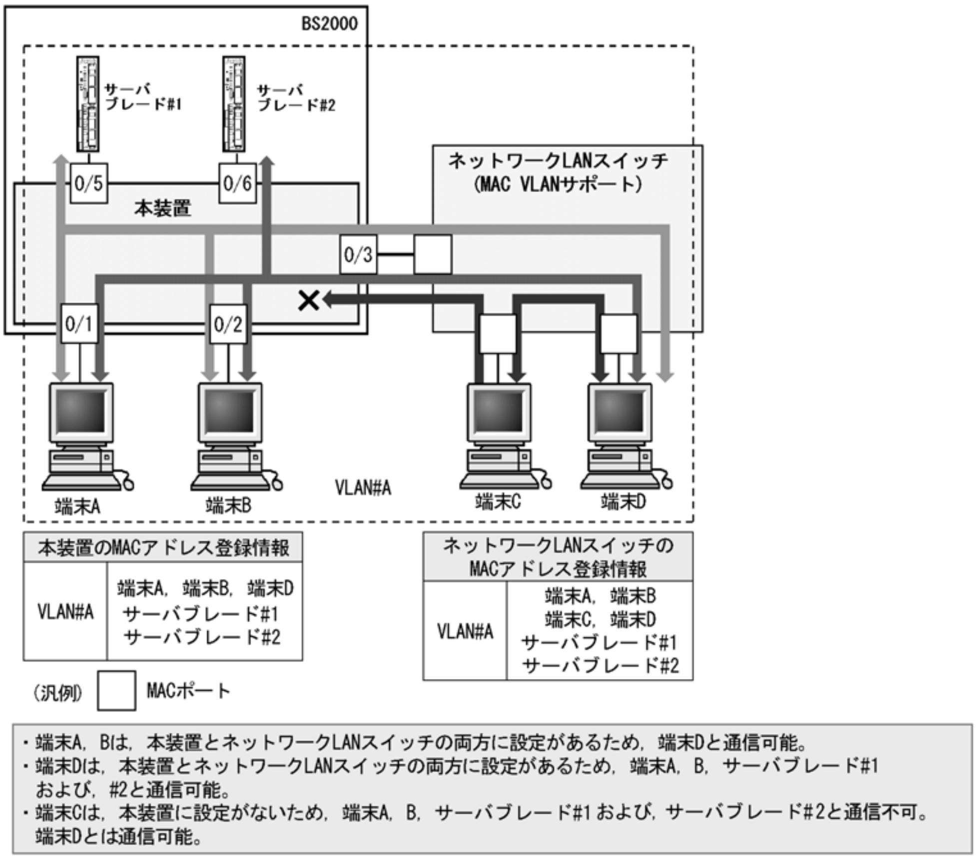
16.7.2 装置間の接続と MAC アドレス設定

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



16.7.3 レイヤ 2 認証機能との連携について

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
- Web 認証
- MAC 認証

プリンタやサーバなど，レイヤ 2 認証機能を動作させないで MAC ポートと接続する端末は，その MAC アドレスをコンフィグレーションで VLAN に登録します。

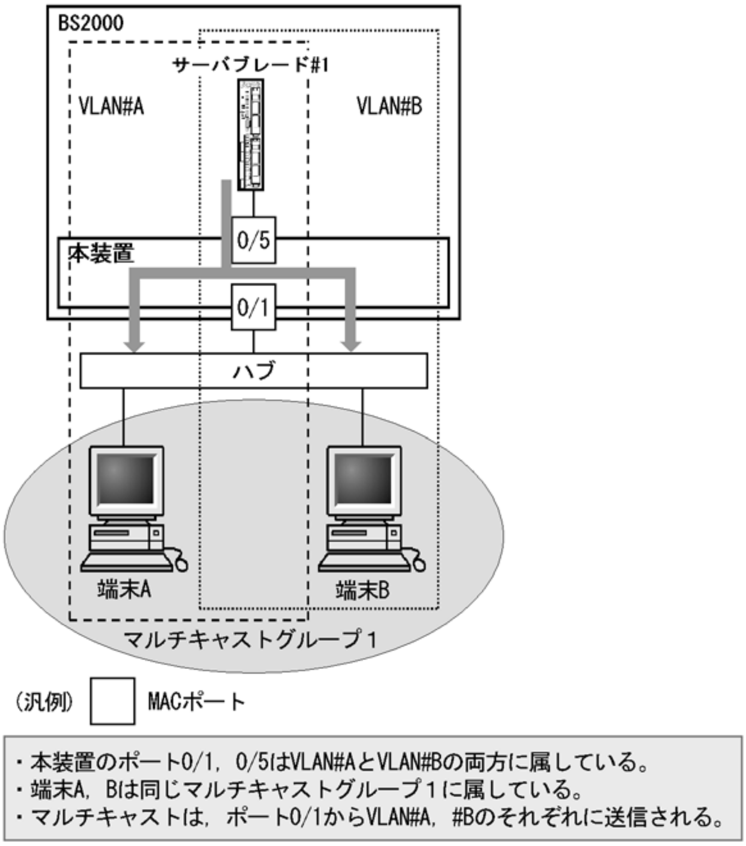
コンフィグレーションとレイヤ 2 認証機能で同じ MAC アドレスを設定した場合，コンフィグレーションの MAC アドレスを登録します。

16.7.4　VLAN 混在時のマルチキャストについて

同一ポートに複数の MAC VLAN が混在した場合やポート VLAN と MAC VLAN が混在した場合，それぞれの VLAN に所属する端末が同じマルチキャストグループに所属すると，そのポートへは VLAN ごとに同じマルチキャストフレームを送信するため，端末は同じフレームを重複して受信します。

端末でマルチキャストデータを重複して受信してしまうネットワークの構成例を次に示します。

図 16-10　VLAN 混在時のマルチキャスト



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 16-10　コンフィグレーションコマンド一覧

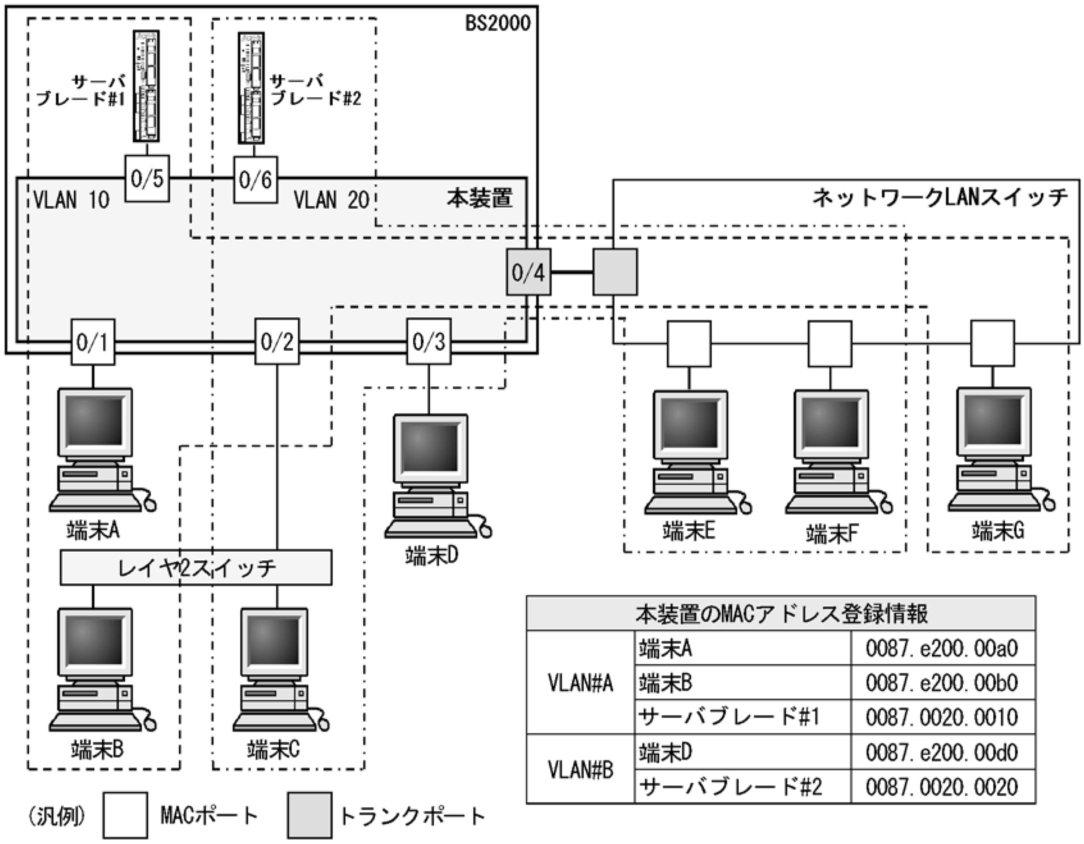
コマンド名	説明
mac-address	MAC VLAN で VLAN に所属する端末の MAC アドレスをコンフィグレーションによって設定します。
mac-based-vlan static-only	コンフィグレーションコマンド mac-address による MAC アドレスの登録数を拡張します。
switchport mac-vlan	MAC ポートの VLAN を設定します。
switchport mode	ポートの種類（MAC，トランク）を設定します。
switchport trunk	トランクポートの VLAN を設定します。
vlan mac-based	MAC VLAN を作成します。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。IEEE802.1X 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　6. IEEE802.1X 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 16-11　MAC VLAN の設定例



本装置のMACアドレス登録情報		
VLAN#A	端末A	0087.e200.00a0
	端末B	0087.e200.00b0
	サーバブレード#1	0087.0020.0010
VLAN#B	端末D	0087.e200.00d0
	サーバブレード#2	0087.0020.0020

(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 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端末にするので登録しません。

[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 0012.e200.0001**
   (config-vlan)# mac-address 0012.e200.0002
   (config-vlan)# exit

   端末 A（0012.e200.0001），端末 B（0012.e200.0002）を MAC VLAN 10 に登録します。

3. **(config)# vlan 20 mac-based**
   (config-vlan)# mac-address 0012.e200.0003
   (config-vlan)# exit

   VLAN 20 を MAC VLAN として作成し，端末 C（0012.e200.0003）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 gigabitethernet 0/1-2**
   ポート 0/1，0/2 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 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 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 gigabitethernet 0/2-3**
   (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 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 は新規の設定と同じ意味になります。

4. **(config)# interface gigabitethernet 0/5**
   ポート 05 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。

5. **(config-if)# switchport mode mac-vlan**
   (config-if)# switchport mac vlan 10
   (config-if)# exit
   ポート 0/5 を MAC ポートに設定します。また，VLAN 10 を設定します。

6. **(config)# interface gigabitethernet 0/6**
   ポート 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。

7. **(config-if)# switchport mode mac-vlan**
   (config-if)# switchport mac vlan 20
   (config-if)# exit
   ポート 0/6 を MAC ポートに設定します。また，VLAN 20 を設定します。

［注意事項］

switchport mac 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 MAC VLAN を運用中のポートで VLAN の追加や削除を行う場合は，switchport mac vlan add コマンドおよび switchport mac vlan remove コマンド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 switchport mac native vlan コマンドで指定すると，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 gigabitethernet 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 のネイティブ VLAN をポート VLAN 30 に設定します。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 アドレス登録数拡張の設定

［設定のポイント］

コンフィグレーションコマンド mac-based-vlan static-only を設定することで，コンフィグレーションコマンド mac-address による登録数を MAC VLAN の収容条件まで拡張できます。

［コマンドによる設定］

1. **(config)# mac-based-vlan static-only**
   (config)# vlan 10 mac-based
   (config-vlan)# mac-address 0012.e200.0004
   (config-vlan)# exit
   (config)# vlan 20 mac-based
   (config-vlan)# mac-address 0012.e200.0005
   (config-vlan)# exit
   VLAN 10 を MAC VLAN として作成し，MAC アドレス（0012.e200.0004）を登録します。さらに，VLAN 20 を MAC VLAN として作成し，MAC アドレス（0012.e200.0005）を登録します。

16.9　VLAN インタフェース

16.9.1　IP アドレスを設定するインタフェース

本装置をレイヤ 3 スイッチとして使用するためには，VLAN に IP アドレスを設定します。複数の VLAN を作成し，各 VLAN に IP アドレスを設定することで本装置はレイヤ 3 スイッチとして動作します。

IP アドレスはコンフィグレーションコマンド interface vlan によって設定します。このインタフェースのことを VLAN インタフェースと呼びます。

16.9.2　VLAN インタフェースの MAC アドレス

IP アドレスを設定した VLAN インタフェースは，本装置の持つ MAC アドレスの一つをそのインタフェースの MAC アドレスとして使用します。使用する MAC アドレスを次に示します。

- 装置 MAC アドレス
- VLAN ごとの MAC アドレス

デフォルトでは装置 MAC アドレスを使用します。コンフィグレーションによって VLAN ごとの MAC アドレスを設定できます。

VLAN インタフェースの MAC アドレスは，コンフィグレーションによって運用中に変更できます。運用中に変更すると，隣接するレイヤ 3 装置（ルータ，レイヤ 3 スイッチ，端末など）が ARP や NDP で学習した MAC アドレスと，本装置の MAC アドレスが不一致となり，一時的に通信ができなくなる場合があるため注意してください。

16.10　VLAN インタフェースのコンフィグレーション

16.10.1　コンフィグレーションコマンド一覧

VLAN インタフェースに IP アドレスを設定し，レイヤ 3 スイッチとして使用するための基本的な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 16-11　コンフィグレーションコマンド一覧

コマンド名	説明
interface vlan	VLAN インタフェースを設定します。また，インタフェースモードへ移行します。
ip address	インタフェースの IPv4 アドレスを設定します。
vlan-mac	VLAN ごとの MAC アドレスを使用することを設定します。
vlan-mac-prefix	VLAN ごとの MAC アドレスのプレフィックスを設定します。

16.10.2　レイヤ 3 インタフェースとしての VLAN の設定

［設定のポイント］

VLAN は IP アドレスを設定してレイヤ 3 インタフェースとして使用できます。interface vlan コマンドおよび VLAN インタフェースコンフィグレーションモードでさまざまなレイヤ 3 機能を設定できます。

ここでは，VLAN インタフェースに IPv4 アドレスを設定する例を示します。VLAN インタフェースで設定できるレイヤ 3 機能については，使用する各機能の章を参照してください。

［コマンドによる設定］

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

   VLAN 10 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ます。interface vlan コマンドで指定した VLAN ID が未設定の VLAN ID の場合，自動的にポート VLAN を作成して vlan コマンドが設定されます。

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

   VLAN 10 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。

16.10.3　VLAN インタフェースの MAC アドレスの設定

本装置の VLAN インタフェースの MAC アドレスは，デフォルトではすべての VLAN で装置 MAC アドレスを使用します。通常，LAN スイッチは VLAN ごとに MAC アドレス学習を行うため，異なる VLAN で同じ MAC アドレスを使用できます。しかし，VLAN ごとではなく装置単位に一つの MAC アドレステーブルを管理する LAN スイッチを同じネットワーク上で使用している場合，異なる VLAN で同じ MAC アドレスを使用すると MAC アドレス学習が安定しなくなる場合があります。そのような場合に VLAN インタフェースの MAC アドレスを VLAN ごとに変更することによってネットワークを安定させることができます。

［設定のポイント］

VLAN をレイヤ 3 インタフェースとして使用する場合，VLAN インタフェースの MAC アドレスを変更できます。MAC アドレスは vlan-mac-prefix コマンドおよび vlan-mac コマンドで設定します。

VLAN ごとの MAC アドレスは，vlan-mac-prefix コマンドで上位 34bit までのプレフィックスを指定し，かつ VLAN ごとに vlan-mac コマンドで，VLAN ごとの MAC アドレスを使用することを設定します。MAC アドレスは下位 12bit に VLAN ID を使用します。

［コマンドによる設定］

1. **(config)# vlan-mac-prefix 0012.e200.0000 ffff.ffff.c000**
   VLAN ごと MAC アドレスに使用するプレフィックス（上位 34bit）を指定します。マスクは 34bit で指定する場合 ffff.ffff.c000 になります。

2. **(config)# vlan 10**
   VLAN 10 の VLAN コンフィグレーションモードに移行します。

3. **(config-vlan)# vlan-mac**
   (config-vlan)# exit
   VLAN 10 で VLAN ごと MAC アドレスを使用することを設定します。MAC アドレスは下位 12bit に VLAN ID を使用し，この場合 VLAN 10 の MAC アドレスは 0012.e200.000a になります。
   MAC アドレスの値は運用コマンド show vlan で確認できます。

［注意事項］

VLAN ごと MAC アドレスの設定で，VLAN インタフェースの MAC アドレスが変更になります。これによって，隣接するレイヤ 3 装置（ルータ，レイヤ 3 スイッチ，端末など）が ARP や NDP で学習した MAC アドレスと本装置の VLAN インタフェースの MAC アドレスが不一致となり，一時的に通信できなくなる場合があります。本機能の設定は VLAN インタフェースの運用開始前に設定するか，または通信の影響が少ないときに行うことをお勧めします。

16.11　VLAN のオペレーション

16.11.1　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 16-12　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。
restart vlan	VLAN プログラムを再起動します。
dump protocols vlan	VLAN プログラムで採取している詳細イベントトレース情報および制御テーブルをファイルへ出力します。

16.11.2　VLAN の状態の確認

(1)　VLAN の設定状態の確認

VLAN の情報は show vlan コマンドで確認できます。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 コマンドの実行結果

```
> show vlan
Date 2009/01/26 17:01:40 UTC
VLAN counts:4
VLAN ID:1     Type:Port based      Status:Up
  Learning:On            Tag-Translation:
  BPDU Forwarding:       EAPOL Forwarding:
  Router Interface Name:VLAN0001
  IP Address:10.215.201.1/24
  Source MAC address: 0012.e212.ad1e(System)
  Description:VLAN0001
  Spanning Tree:PVST+(802.1D)
  AXRP RING ID:      AXRP VLAN group:
  GSRP ID:      GSRP VLAN group:    L3:
  IGMP snooping:     MLD snooping:
  Untagged(4)  :0/1-4
VLAN ID:3     Type:Port based      Status:Up
  Learning:On            Tag-Translation:On
  BPDU Forwarding:       EAPOL Forwarding:
  Router Interface Name:VLAN0003
  IP Address:10.215.196.1/23
             3ffe:501:811:ff08::5/64
  Source MAC address: 0012.e212.ad1e(System)
  Description:VLAN0003
  Spanning Tree:Single(802.1D)
  AXRP RING ID:      AXRP VLAN group:
  GSRP ID:      GSRP VLAN group:    L3:
  IGMP snooping:     MLD snooping:
  Untagged(8)   :0/5-12
  Tagged(2)     :0/25-26
  Tag-Trans(2)  :0/25-26
VLAN ID:120   Type:Protocol based  Status:Up
  Protocol VLAN Information  Name:ipv6
  EtherType:08dd  LLC:  Snap-EtherType:
  Learning:On            Tag-Translation:On
  BPDU Forwarding:       EAPOL Forwarding:
  Router Interface Name:VLAN0120
  IP Address:
  Source MAC address: 0012.e212.ad1e(System)
  Description:VLAN0120
  Spanning Tree:
  AXRP RING ID:      AXRP VLAN group:
  GSRP ID:      GSRP VLAN group:    L3:
  IGMP snooping:     MLD snooping:
  Untagged(3)   :0/5,7,9
  Tagged(2)     :0/25-26
  Tag-Trans(2)  :0/25-26
VLAN ID:1340  Type:Mac based       Status:Up
  Learning:On            Tag-Translation:On
  BPDU Forwarding:       EAPOL Forwarding:
  Router Interface Name:VLAN1340
  IP Address:10.215.202.1/24
  Source MAC address: 0012.e2de.053c(VLAN)
  Description:VLAN1340
  Spanning Tree:
  AXRP RING ID:      AXRP VLAN group:
  GSRP ID:      GSRP VLAN group:    L3:
  IGMP snooping:     MLD snooping:
  Untagged(6)   :0/13-18
  Tagged(2)     :0/25-26
  Tag-Trans(2)  :0/25-26
>
```

(2) VLAN の通信状態の確認

VLAN の通信状態は show vlan detail コマンドで確認できます。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 コマンドの実行結果

```
> show vlan 3,1000-1500 detail
Date 2009/01/26 17:01:40 UTC
VLAN counts:2
VLAN ID:3     Type:Port based      Status:Up
  Learning:On            Tag-Translation:On
  BPDU Forwarding:       EAPOL Forwarding:
  Router Interface Name:VLAN0003
  IP Address:10.215.196.1/23
             ee80::220:afff:fed7:8f0a/64
  Source MAC address: 0012.e212.ad1e(System)
  Description:VLAN0003
  Spanning Tree:Single(802.1D)
  AXRP RING ID:      AXRP VLAN group:
  GSRP ID:      GSRP VLAN group:    L3:
  IGMP snooping:     MLD snooping:
  Port Information
   0/5          Up   Forwarding      Untagged
   0/6          Up   Blocking(STP)   Untagged
   0/7          Up   Forwarding      Untagged
   0/8          Up   Forwarding      Untagged
   0/9          Up   Forwarding      Untagged
   0/10         Up   Forwarding      Untagged
   0/11         Up   Forwarding      Untagged
   0/12         Up   Forwarding      Untagged
   0/25(CH:9)   Up   Forwarding      Tagged   Tag-Translation:103
   0/26(CH:9)   Up   Blocking(CH)    Tagged   Tag-Translation:103
VLAN ID:1340  Type:Mac based       Status:Up
  Learning:On            Tag-Translation:On
  BPDU Forwarding:       EAPOL Forwarding:
  Router Interface Name:VLAN1340
  IP Address:10.215.202.1/24
  Source MAC address: 0012.e2de.053c(VLAN)
  Description:VLAN1340
  Spanning Tree:
  AXRP RING ID:      AXRP VLAN group:
  GSRP ID:      GSRP VLAN group:    L3:
  IGMP snooping:     MLD snooping:
  Port Information
   0/25(CH:9)   Up   Forwarding      Tagged   Tag-Translation:104
   0/26(CH:9)   Up   Blocking(CH)    Tagged   Tag-Translation:104
>
```

(3) VLAN ID 一覧の確認

show vlan summary コマンドで，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 コマンドの実行結果

```
> show vlan summary
Date 2009/01/14 12:14:38 UTC
Total(4)            :1,10,20,4094
Port based(2)       :1,4094
Protocol based(1)   :10
MAC based(1)        :20
>
```

（4） VLAN のリスト表示による確認

show vlan list コマンドは 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 コマンドの実行結果

```
> show vlan list
Date 2009/01/26 17:01:40 UTC
VLAN counts:4
ID   Status  Fwd/Up /Cfg Name             Type  Protocol       Ext.    IP
   1 Up       16/ 18/ 18 VLAN0001         Port  STP PVST+:1D   - - - - 4
   3 Up        9/ 10/ 10 VLAN0003         Port  STP Single:1D  - - T - 4/6
 120 Up        4/  5/  5 VLAN0120         Proto -              - - - - -
1340 Disable   0/  8/  8 VLAN1340         Mac   -              - - - - 4
     AXRP (Control-VLAN)
     GSRP GSRP ID:VLAN Group ID(Master/Backup)
     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，show vlan mac-vlan コマンドで確認できます。

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」は IEEE802.1X で登録した MAC アドレス

図 16-16　show vlan mac-vlan コマンドの実行結果

```
> show vlan mac-vlan
Date 2009/01/14 12:16:04 UTC
VLAN counts:2    Total MAC Counts:5
VLAN ID:20   MAC Counts:4
   0012.e200.0001 (static)    0012.e200.0002 (static)
   0012.e200.0003 (static)    0012.e200.0004 (dot1x)
VLAN ID:200  MAC Counts:1
   0012.e200.1111 (dot1x)
>
```

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

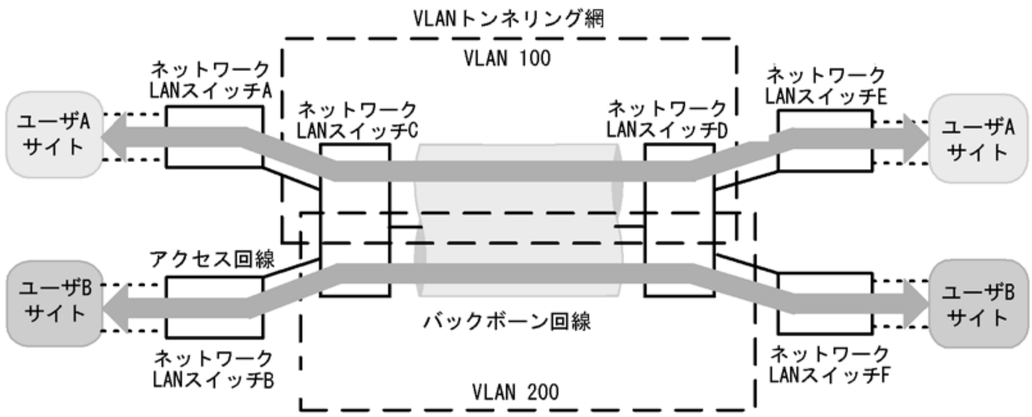
17.1.1 概要

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。本装置に VLAN トンネリング機能を適用します。VLAN トンネリングでは，VLAN Tag をスタックすることで VLAN トンネリング網内の VLAN を識別します。ユーザサイトを収容するポートをアクセス回線，VLAN トンネリング網内に接続するポートをバックボーン回線と呼びます。アクセス回線からのフレームに VLAN Tag を追加してバックボーン回線に中継します。バックボーン回線からのフレームは VLAN Tag を外しアクセス回線へ中継します。

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 3.7 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
mtu	バックボーン回線でジャンボフレームを設定します。
switchport access	アクセス回線を設定します。
switchport mode	アクセス回線，バックボーン回線を設定するためにポートの種類を設定します。
switchport trunk	バックボーン回線を設定します。

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 0/1**
   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 dot1q-tunnel**
   (config-if)# switchport access vlan 10
   (config-if)# exit
   ポート 0/1 をトンネリングポートに設定します。また，VLAN 10 を設定します。

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，「12.2.4　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

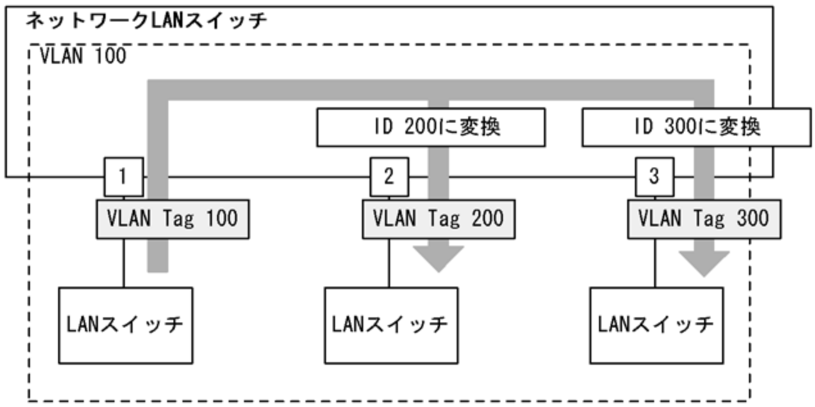
17.3.1　概要

Tag 変換機能は，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 変換機能は，トランクポートで指定します。Tag 変換機能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 変換機能を指定した場合はその ID を使用します。

Tag 変換機能の構成例を次の図に示します。図では，ポート 1 で Tag 変換機能が未指定であり，ポート 2 およびポート 3 にそれぞれ Tag 変換機能を設定し，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 変換機能の構成例



17.3.2　Tag 変換使用時の注意事項

（1） Tag 変換使用時の VLAN Tag のユーザ優先度について

Tag 変換を設定したポートで Tag 変換するフレームを受信した場合，VLAN Tag のユーザ優先度が，デフォルトの”3”となります。Tag 変換使用時にユーザ優先度をデフォルト値から変更したい場合は，QoS 制御のマーカー機能によって変更してください。

（2） Tag 変換使用時の TPID について

Tag 変換を使用するポートに対して TPID を 0x8100 以外設定しないでください。

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

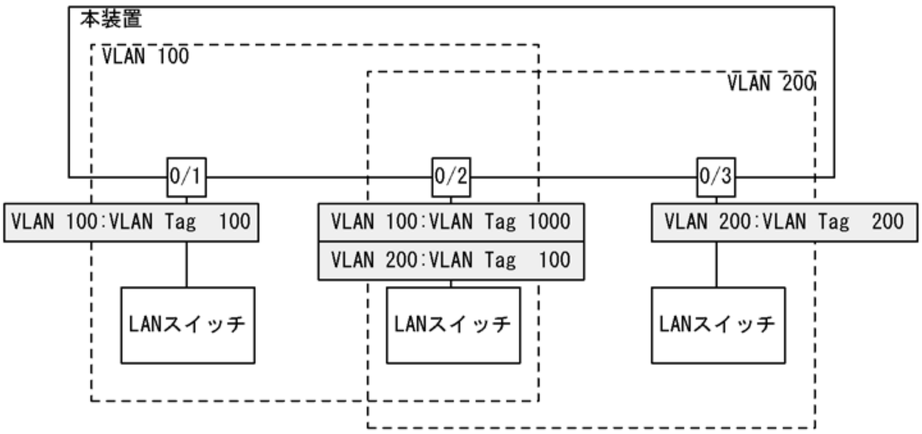
コマンド名	説明
switchport vlan mapping	変換する ID を設定します。
switchport vlan mapping enable	指定したポートで Tag 変換を有効にします。

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 0/2 の設定例を示します。

構成例では，ポート 0/2 に Tag 変換を適用します。ポート 0/2 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 0/2 では VLAN Tag 200 のフレームを VLAN 200 として扱わないで，未設定の VLAN Tag として廃棄します。

図 17-3 Tag 変換の設定例



［設定のポイント］

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

Tag 変換は switchport vlan mapping コマンドで設定します。設定した変換を有効にするためには，switchport vlan mapping enable コマンドを設定します。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 0/2
(config-if)# switchport mode trunk
(config-if)# switchport trunk allowed vlan 100,200
```

ポート 0/2 をトランクポートに設定して，VLAN 100，200 を設定します。

2. **(config-if)# switchport vlan mapping 1000 100**
   (config-if)# switchport vlan mapping 100 200
   ポート 0/2 で VLAN 100，200 に Tag 変換を設定します。VLAN 100 では VLAN Tag 1000 でフレームを送受信して，VLAN 200 では VLAN Tag 100 でフレームを送受信するように設定します。

3. **(config-if)# switchport vlan mapping enable**
   (config-if)# exit
   ポート 0/2 で Tag 変換を有効にします。本コマンドを設定するまでは Tag 変換は動作しません。

［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。

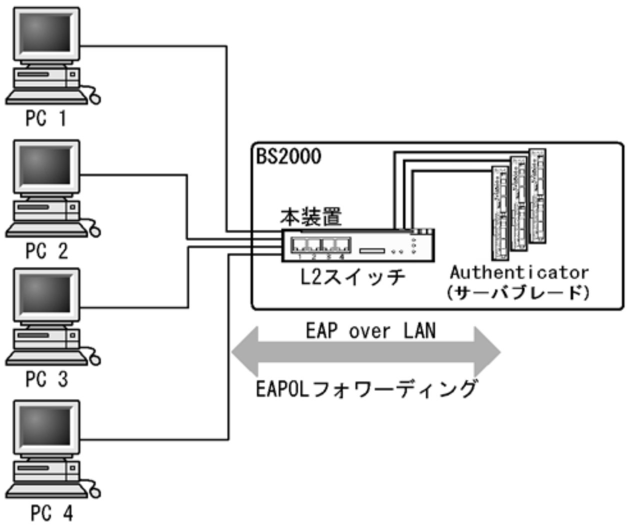
(1)　BPDU フォワーディング機能

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 L2 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 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。

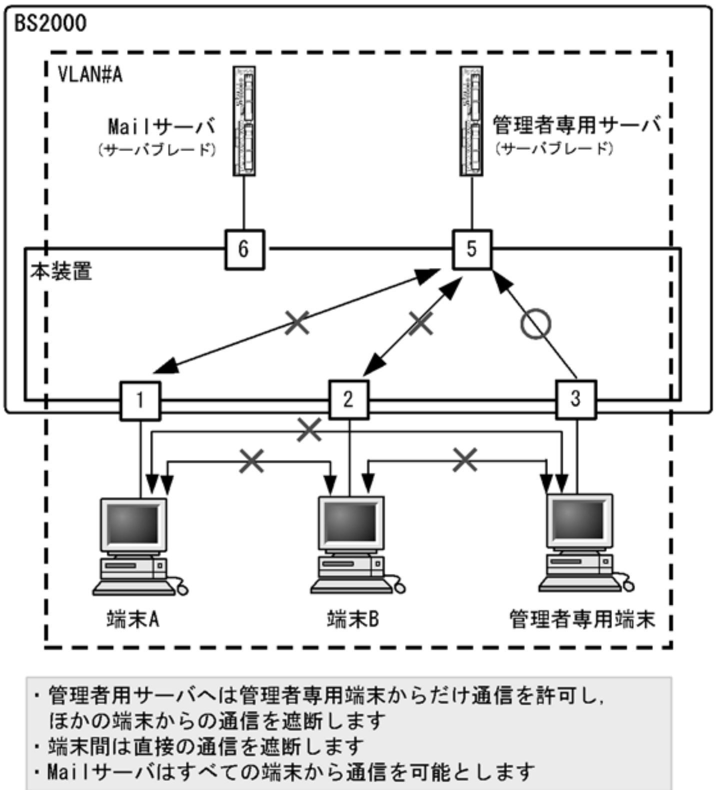
17.7　ポート間中継遮断機能の解説

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）一つのポートに複数の VLAN を設定したポート間の遮断について

ポート間中継遮断機能は，VLAN 内のレイヤ 2 中継，VLAN 間のレイヤ 3 中継のどちらもすべての通信を遮断します。トランクポートなどで一つのポートに複数の VLAN を設定したポート間での通信を遮断した場合，そのポート間では VLAN 間のレイヤ 3 中継もできなくなります。

（2）スパニングツリーを同時に使用するときの注意事項

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。

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 17-4　コンフィグレーションコマンド一覧

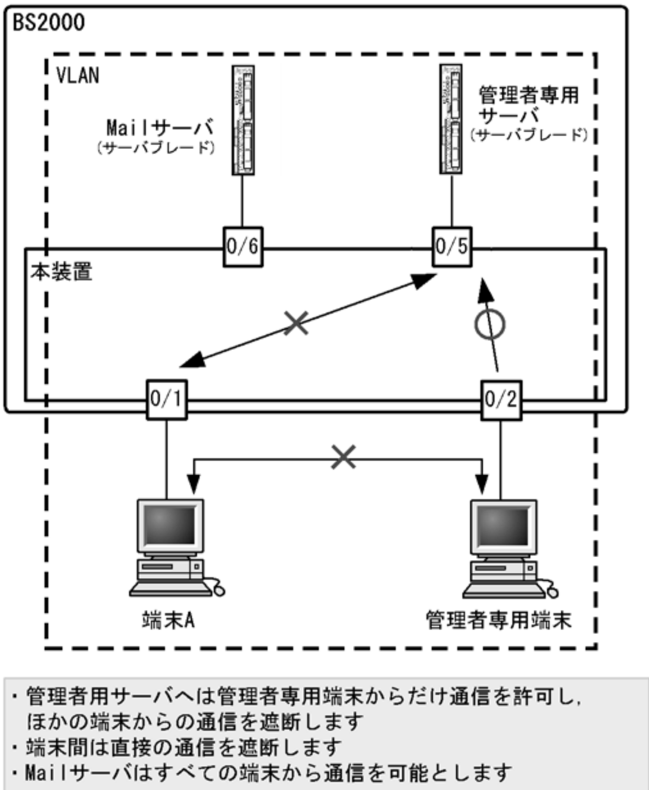
コマンド名	説明
switchport isolation	指定したポートへの中継を遮断します。

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 からポート 0/5 へ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 0/1**

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 isolation interface gigabitethernet 0/ 2,gigabitethernet 0/5**
   (config-if)# exit
   ポート 0/1 でポート 0/2，0/5 からの中継を遮断します。この設定で，ポート 0/1 から発信する片方向の中継を遮断します。

3. **(config)# interface gigabitethernet 0/2**
   (config-if)# switchport isolation interface gigabitethernet 0/1
   (config-if)# exit
   ポート 0/2 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 0/2 でポート 0/1 からの中継を遮断します。この設定によって，ポート 0/1，0/2 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 0/1
   (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 0/1 からの中継を遮断します。この設定によって，ポート 0/1，0/5 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］

switchport isolation add コマンドおよび switchport isolation remove コマンド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 switchport isolation <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 0/1**
   (config-if)# switchport isolation interface gigabitethernet 0/2-10
   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，ポート 0/1 からポート 0/2 ～ 0/10 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 0/1 からの遮断にポート 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，ポート 0/1 はポート 0/2 ～ 0/4，0/6 ～ 0/11 への通信を遮断します。

3. **(config-if)# switchport isolation interface gigabitethernet 0/3-4**
   (config-if)# exit
   ポート 0/1 からの中継を遮断するポートを 0/3 ～ 0/4 に設定します。以前の設定はすべて上書きされ，ポート 0/3 ～ 0/4 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 debounce 機能の解説

17.9.1　概要

VLAN インタフェースは VLAN が通信可能な状態になったときにアップし，VLAN のポートがダウンした場合や，スパニングツリーなどの機能でブロッキング状態になり通信できなくなった場合にダウンします。

VLAN debounce 機能は，VLAN インタフェースのアップやダウンを遅延させて，ネットワークトポロジーの変更や，ログメッセージ，SNMP Trap などを削減する機能です。

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

レイヤ 3 での冗長構成を使用する場合，マスター側に障害が発生したあとの回復時に，両系がマスターとして動作することを防ぐために VLAN インタフェースのアップを遅延させたいとき，VLAN debounce 機能で VLAN インタフェースのアップを遅延できます。

17.9.2　VLAN debounce 機能と他機能との関係

（1）　スパニングツリー

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

（2）　Ring Protocol

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

このようなときに VLAN がいったんダウンすることを防ぐためには，VLAN インタフェースのダウン遅延時間を設定してください。なお，ダウン遅延時間は health-check holdtime コマンドで設定する保護時間以上に設定してください。

（3）　その他の冗長化機能

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

17.9.3　VLAN debounce 機能使用時の注意事項

（1）　ダウン遅延時間の注意事項

ダウン遅延時間を設定すると，回復しない障害が発生した場合でも VLAN のダウンが遅延します。VLAN debounce 機能でダウンが遅延している間は，通信できない状態です。ダウン遅延時間は，ネットワークの

構成や運用に応じて必要な値を設定してください。

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

(2) アップ遅延時間の注意事項

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

(3) 遅延時間の誤差に関する注意事項

アップまたはダウン遅延時間は，ソフトウェアのタイマを使用しているため，CPU 利用率が高い場合には設定した時間より大きくなることがあります。

17.10　VLAN debounce 機能のコンフィグレーション

17.10.1　コンフィグレーションコマンド一覧

VLAN debounce 機能のコンフィグレーションコマンド一覧を次の表に示します。

表 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
down-debounce	VLAN インタフェースのダウン遅延時間を指定します。
up-debounce	VLAN インタフェースのアップ遅延時間を指定します。

17.10.2　VLAN debounce 機能の設定

VLAN debounce 機能を設定する手順を次に示します。

［設定のポイント］

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

［コマンドによる設定］

1. **(config)# interface vlan 100**
   VLAN 100 の VLAN インタフェースモードに移行します。

2. **(config-if)# down-debounce 2**
   (config-if)# exit
   VLAN 100 のダウン遅延時間を 2 秒に設定します。

3. **(config)# interface range vlan 201-300**
   VLAN 201-300 の複数 VLAN インタフェースモードに移行します。

4. **(config-if-range)# down-debounce 3**
   (config-if-range)# exit
   VLAN 201-300 のダウン遅延時間を 3 秒に設定します。

17.11 VLAN 拡張機能のオペレーション

17.11.1 運用コマンド一覧

VLAN 拡張機能の運用コマンド一覧を次の表に示します。

表 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。

17.11.2 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 show vlan detail コマンドで確認できます。show vlan detail コマンドによる 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 コマンドによる 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。
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 コマンドの実行結果

```
>show vlan 10 detail
Date 2009/01/15 16:28:23 UTC
VLAN counts:1   VLAN tunneling enabled                                  …1
VLAN ID:10    Type:Port based      Status:Up
  Learning:On            Tag-Translation:On
  BPDU Forwarding:On     EAPOL Forwarding:                              …3
               :
               :
  Port Information
   0/2          Up   Forwarding      Tagged   Tag-Translation:1000      …2
   0/3          Down -               Tagged   Tag-Translation:2000      …2
   0/4          Up   Forwarding      Tagged
>
```

1. VLAN トンネリングが有効であることを示します。
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が設定され，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。

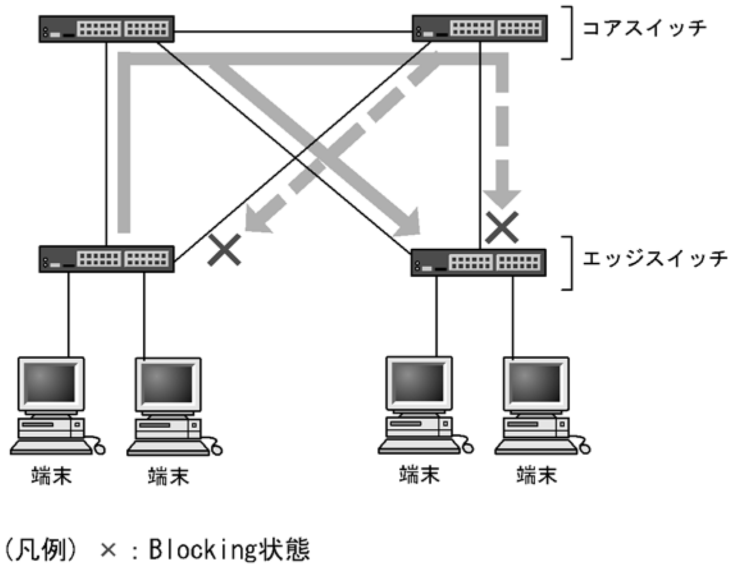
18.1　スパニングツリーの概説

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



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。

名称	構築単位	概要
シングルスパニングツリー	装置単位	装置全体のポートを対象とし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。IEEE802.1D 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。IEEE802.1w 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

状態	状態の概要	次の状態への遷移
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 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。

ブリッジの役割	概要
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

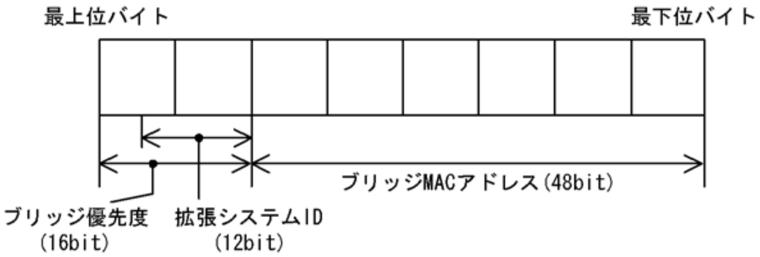
ポートの役割	概要
ルートポート	指定ブリッジからルートブリッジへ向かう通信経路のポートです。通信可能なポートとなります。
指定ポート	ルートポート以外の通信可能なポートです。ルートブリッジからの通信経路でトポロジーの下流へ接続するポートです。
非指定ポート	ルートポート，指定ポート以外のポートで，通信不可の状態のポートです。障害が発生した際に通信可能になり代替経路として使用します。

（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。

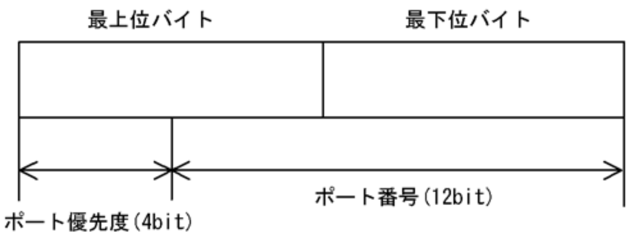
（5） ポート識別子

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。

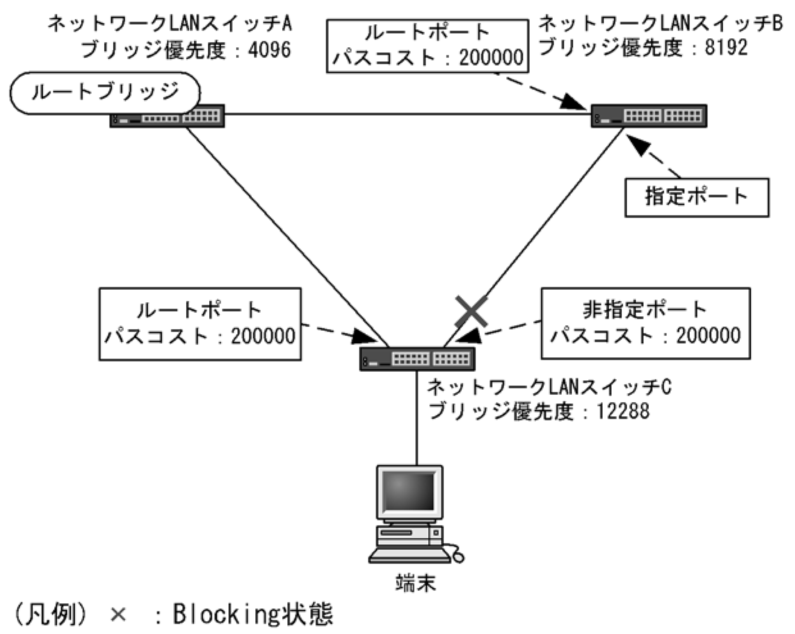
図 18-3　ポート識別子



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



(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，ネットワーク LAN スイッチ A がルートブリッジになるように設定します。ネットワーク LAN スイッチ B，ネットワーク LAN 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ネット

ワーク LAN スイッチ B になるように設定します。ネットワーク LAN 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

ネットワーク LAN スイッチ B，ネットワーク LAN 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，ネットワーク LAN スイッチ C のネットワーク LAN 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

ネットワーク LAN スイッチ B，ネットワーク LAN 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ネットワーク LAN スイッチ B が指定ポート，ネットワーク LAN スイッチ C が非指定ポートとなり，ネットワーク LAN スイッチ C が Blocking 状態となります。Blocking 状態になるポートをネットワーク LAN スイッチ B にしたい場合は，パスコストを調整してネットワーク LAN 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

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

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

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

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

（2） 復旧機能

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

（3） 自動復旧機能

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

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

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

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 で本装置にスパニングツリー機能を適用すると，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

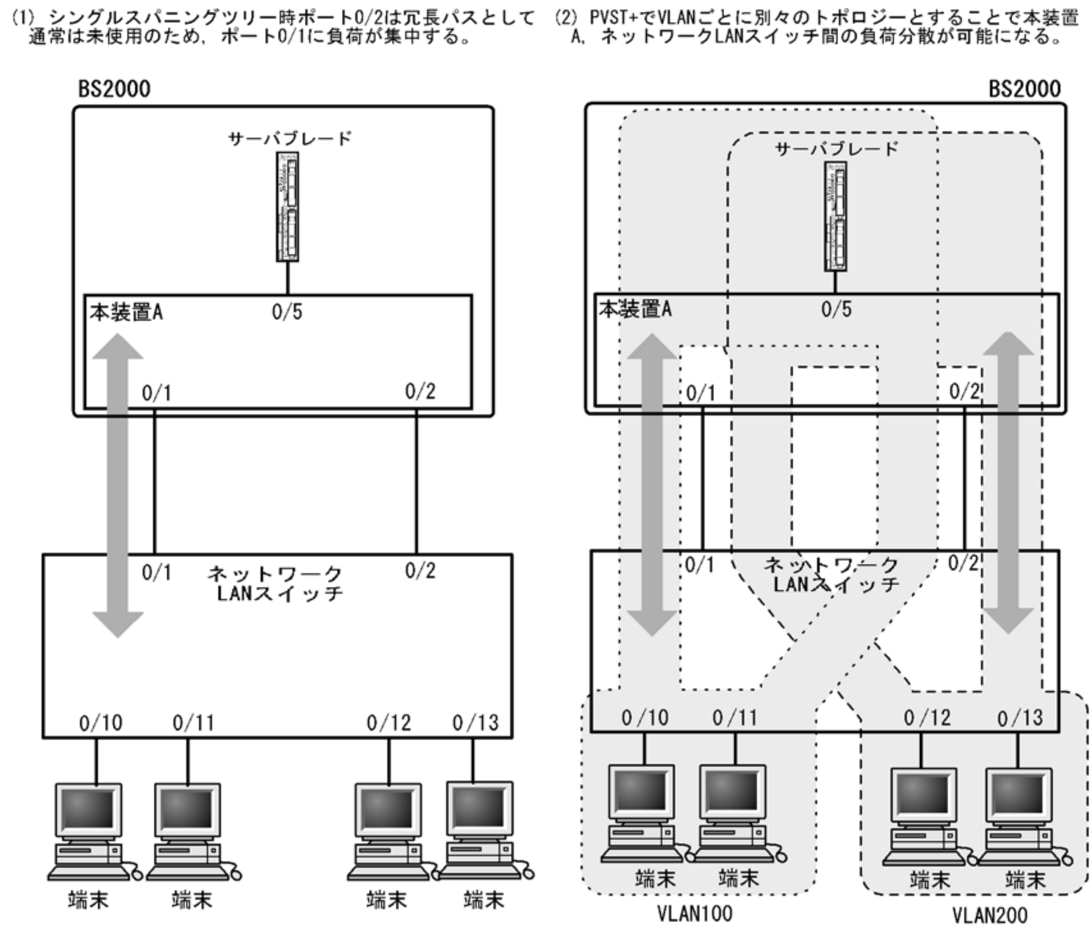
PVST+ は，VLAN 単位にツリーを構築します。VLAN 単位にツリーを構築できるため，ロードバランシングが可能です。また，アクセスポートでは，シングルスパニングツリーで動作しているスイッチと接続できます。

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，B 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，B 間のポート 1 に集中します。そこで，複数の VLAN を組み，PVST+ によって VLAN ごとに別々のトポロジ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 18-5　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+

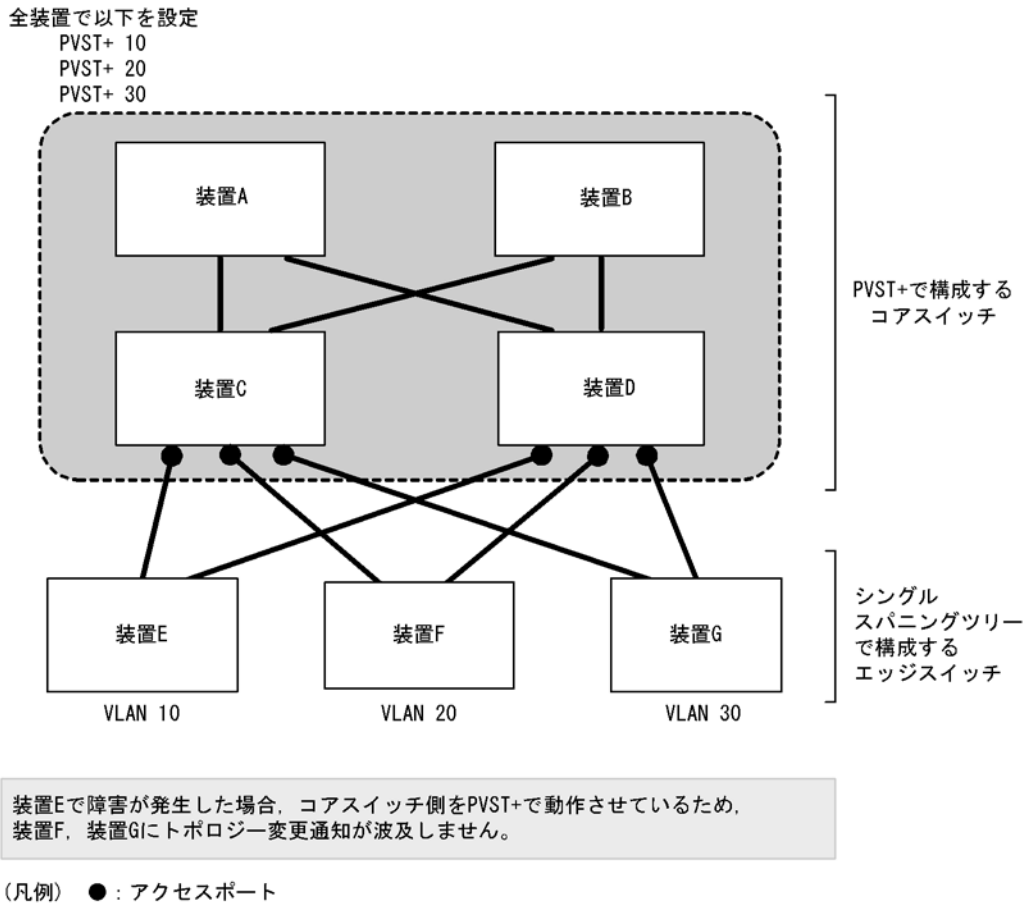
(1)　解説

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 18-6　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

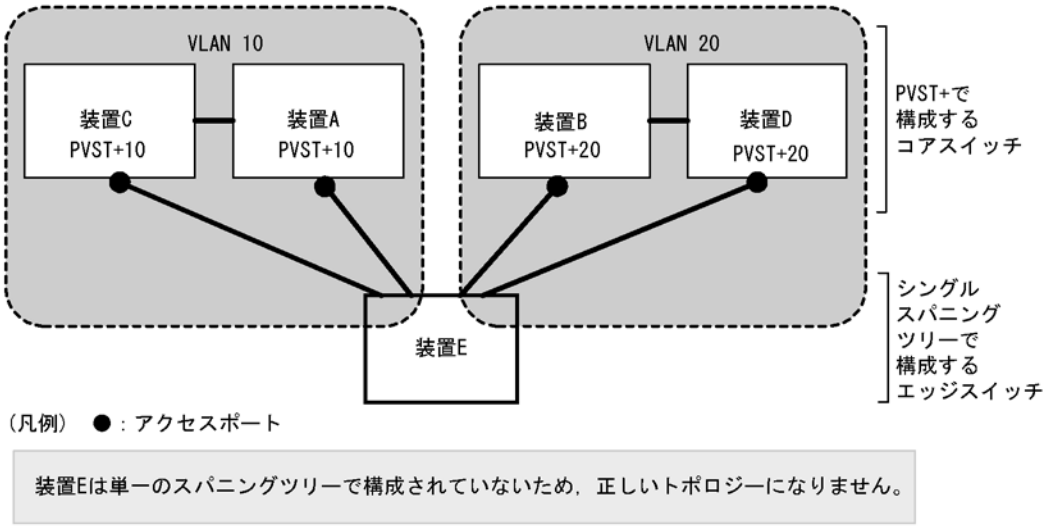
シングルスパニングツリーと VLAN 1 の PVST+ を同時に動作させることはできません。シングルスパニングツリーを動作させると VLAN 1 の PVST+ は停止します。

(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 18-7　シングルスパニングツリーとの禁止構成例



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

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，no spanning-tree vlan コマンドを使用します。

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

[コマンドによる設定]

1. **(config)# no spanning-tree vlan 20**
   VLAN 20 の PVST+ の動作を停止します。

2. **(config)# spanning-tree vlan 20**
   停止した VLAN 20 の PVST+ を動作させます。

[注意事項]

- PVST+ はコンフィグレーションに表示がないときは自動的に動作しています。no spanning-tree vlan コマンドで停止すると，停止状態であることがコンフィグレーションで確認できます。
- PVST+ は最大 250 個のポート VLAN まで動作します。それ以上のポート VLAN を作成しても自動的には動作しません。

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。10 ギガビットイーサネットを使用する場合は long（32bit 値）を使用することをお勧めします。デフォルトでは short（16bit 値）で動作します。イーサネットインタフェースの速度による自動的な設定は，short（16bit 値）か long（32bit 値）かで設定内容が異なります。パスコストのデフォルト値を次の表に示します。

表 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 0/1**
   (config-if)# spanning-tree cost 100

```
(config-if)# exit
```
ポート 0/1 のパスコストを 100 に設定します。

2. ```
(config)# spanning-tree pathcost method long
(config)# interface gigabitethernet 0/1
(config-if)# spanning-tree vlan 10 cost 200000
```
long（32bit 値）のパスコストを使用するように設定した後に，ポート 0/1 の VLAN 10 をコスト値 200000 に変更します。ポート 0/1 では VLAN 10 だけパスコスト 200000 となり，そのほかの VLAN は 100 で動作します。

［注意事項］

リンクアグリゲーションを使用する場合，チャネルグループのパスコストのデフォルト値は，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。リンクアグリゲーションの異速度混在モードを使用している場合は，最も遅い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 0/1
(config-if)# spanning-tree port-priority 64
(config-if)# exit
```
ポート 0/1 のポート優先度を 64 に設定します。

2. ```
(config)# interface gigabitethernet 0/1
(config-if)# spanning-tree vlan 10 port-priority 144
```
ポート 0/1 の VLAN 10 をポート優先度 144 に変更します。ポート 0/1 では VLAN 10 だけポート優先度 144 となり，そのほかの VLAN は 64 で動作します。

## 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プログラムの負荷を軽減できます。

[設定のポイント]

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

[コマンドによる設定]

1. **(config)# spanning-tree vlan 10 hello-time 3**
   VLAN 10 の PVST+ の BPDU 送信間隔を 3 秒に設定します。

[注意事項]

BPDU の送信間隔を短くすると，トポロジ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プログラムの負荷が増加します。本パラメータをデフォルト値（2 秒）より短くすることでタイムアウトのメッセージ出力やトポロジ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 に設定します。

（4） 状態遷移時間の設定

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

［設定のポイント］

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

［コマンドによる設定］

1. **`(config)# spanning-tree vlan 10 forward-time 10`**
   VLAN 10 の PVST+ の状態遷移時間を 10 に設定します。

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。
restart spanning-tree	スパニングツリープログラムを再起動します。
dump protocols spanning-tree	スパニングツリーで採取している詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。

18.5.2　PVST+ の状態の確認

PVST+ の情報は show spanning-tree コマンド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 18-8　show spanning-tree コマンドの実行結果

```
> show spanning-tree vlan 1
Date 2009/01/04 11:39:43 UTC
VLAN 1              PVST+ Spanning Tree:Enabled  Mode:PVST+
  Bridge ID        Priority:32769       MAC Address:0012.e205.0900
    Bridge Status:Designated
  Root Bridge ID   Priority:32769       MAC Address:0012.e201.0900
    Root Cost:1000
    Root Port:0/1
  Port Information
    0/1        Up    Status:Forwarding  Role:Root
    0/2        Up    Status:Forwarding  Role:Designated
    0/3        Up    Status:Blocking    Role:Alternate
    0/4        Down  Status:Disabled    Role:-
    0/10       Up    Status:Forwarding  Role:Designated PortFast
    0/11       Up    Status:Forwarding  Role:Designated PortFast
    0/12       Up    Status:Forwarding  Role:Designated PortFast
>
```

18.6　シングルスパニングツリー解説

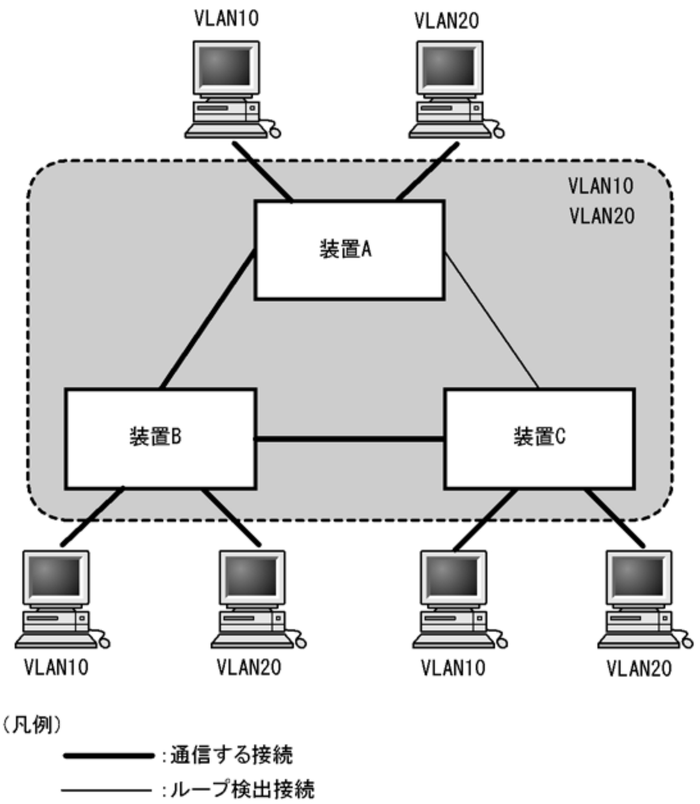
シングルスパニングツリーは装置全体を対象としトポロジーを構築します。

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 18-9　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（no spanning-tree vlan コマンドで指定）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のデフォルト値を設定します。
spanning-tree pathcost method	ポートごとにパスコストに使用する値の幅のデフォルト値を設定します。
spanning-tree port-priority	ポートごとにポート優先度のデフォルト値を設定します。
spanning-tree single	シングルスパニングツリーの動作，停止を設定します。
spanning-tree single cost	シングルスパニングツリーのパスコストを設定します。
spanning-tree single forward-time	ポートの状態遷移に必要な時間を設定します。
spanning-tree single hello-time	BPDU の送信間隔を設定します。
spanning-tree single max-age	送信 BPDU の最大有効時間を設定します。
spanning-tree single pathcost method	シングルスパニングツリーのパスコストに使用する値の幅を設定します。
spanning-tree single port-priority	シングルスパニングツリーのポート優先度を設定します。
spanning-tree single priority	ブリッジ優先度を設定します。
spanning-tree single transmission-limit	hello-time 当たりに送信できる最大 BPDU 数を設定します。

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。10 ギガビットイーサネットを使用する場合は long（32bit 値）を使用することをお勧めします。デフォルトでは short（16bit 値）で動作します。イーサネットインタフェースの速度による自動的な設定は，short（16bit 値）か long（32bit 値）かで設定内容が異なります。パスコストのデフォルト値を次の表に示します。

表 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 0/1**
   (config-if)# spanning-tree cost 100
   (config-if)# exit

ポート 0/1 のパスコストを 100 に設定します。

2. **(config)# spanning-tree pathcost method long**
   (config)# interface gigabitethernet 0/1
   (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 0/1 のパスコストを 200000 に変更します。ポート 0/1 ではシングルスパニングツリーだけパスコスト 200000 となり，同じポートで使用している PVST+ は 100 で動作します。

［注意事項］

リンクアグリゲーションを使用する場合，チャネルグループのパスコストのデフォルト値は，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。リンクアグリゲーションの異速度混在モードを使用している場合は，最も遅い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 0/1**
   (config-if)# spanning-tree port-priority 64
   (config-if)# exit
   ポート 0/1 のポート優先度を 64 に設定します。

2. **(config)# interface gigabitethernet 0/1**
   (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 0/1 のポート優先度を 144 に変更します。ポート 0/1 ではシングルスパニングツリーだけポート優先度 144 となり，同じポートで使用している PVST+ は 64 で動作します。

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プログラムの負荷を軽減できます。

［設定のポイント］

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

［コマンドによる設定］

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

［注意事項］

BPDU の送信間隔を短くすると，トポロジ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プログラムの負荷が増加します。本パラメータをデフォルト値（2 秒）より短くすること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 に設定します。

（4） 状態遷移時間の設定

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

［設定のポイント］

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

［コマンドによる設定］

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

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。
restart spanning-tree	スパニングツリープログラムを再起動します。
dump protocols spanning-tree	スパニングツリーで採取している詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。

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 show spanning-tree コマンドで確認してください。Mode で STP，Rapid STP の動作モードを確認できます。トポロジ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 18-10　シングルスパニングツリーの情報

```
> show spanning-tree single
Date 2009/01/04 11:42:06 UTC
Single Spanning Tree:Enabled  Mode:Rapid STP
  Bridge ID        Priority:32768       MAC Address:0012.e205.0900
    Bridge Status:Designated
  Root Bridge ID   Priority:32768       MAC Address:0012.e205.0900
    Root Cost:0
    Root Port:-
  Port Information
    0/1        Up    Status:Forwarding  Role:Root
    0/2        Up    Status:Forwarding  Role:Designated
    0/3        Up    Status:Blocking    Role:Alternate
    0/4        Down  Status:Disabled    Role:-
    0/10       Up    Status:Forwarding  Role:Designated PortFast
    0/11       Up    Status:Forwarding  Role:Designated PortFast
    0/12       Up    Status:Forwarding  Role:Designated PortFast
>
```

18.9　マルチプルスパニングツリー解説

18.9.1　概要

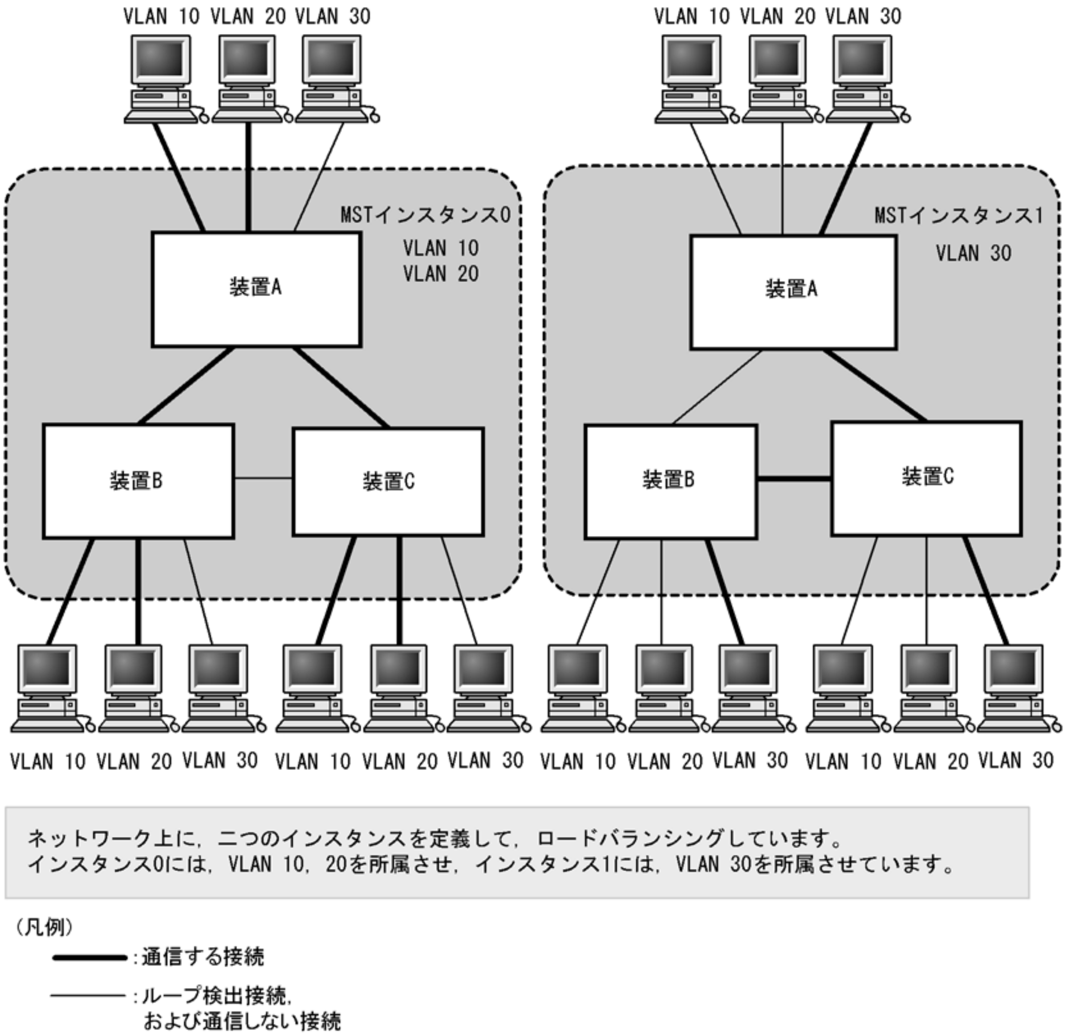
マルチプルスパニングツリーには，次の特長があります。MST インスタンスによってロードバランシングを可能にしています。また，MST リージョンによって，大規模なネットワーク構成を中小構成に分割することでネットワーク設計が容易になります。以降，これらを実現するためのマルチプルスパニングツリーの機能概要を説明します。

（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 18-11　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

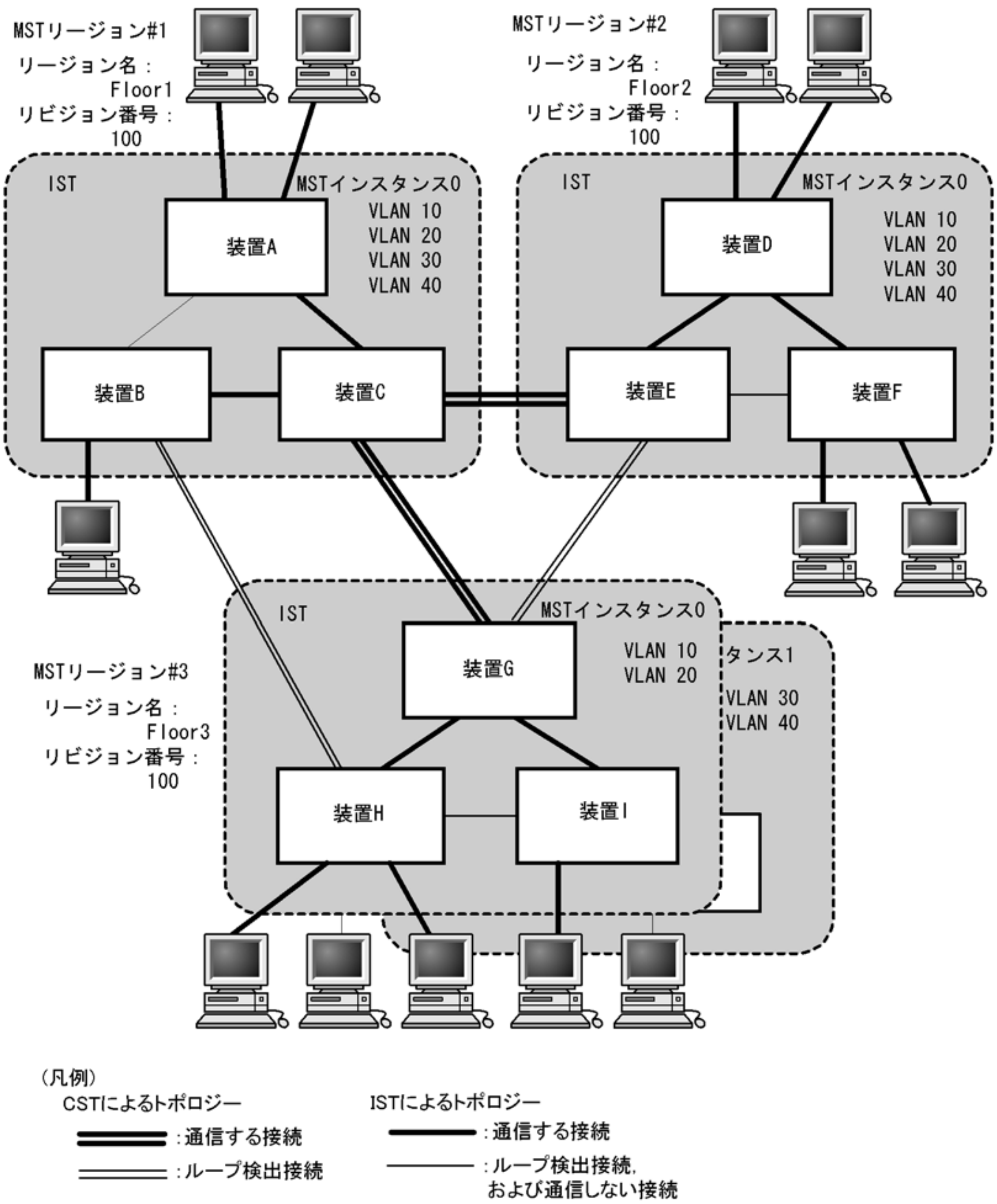
BPDU を送受信する唯一の MST インスタンスとなります。全 MST インスタンスのトポロジー情報は，MST BPDU にカプセル化し通知します。

● 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 18-12　マルチプルスパニングツリー概要



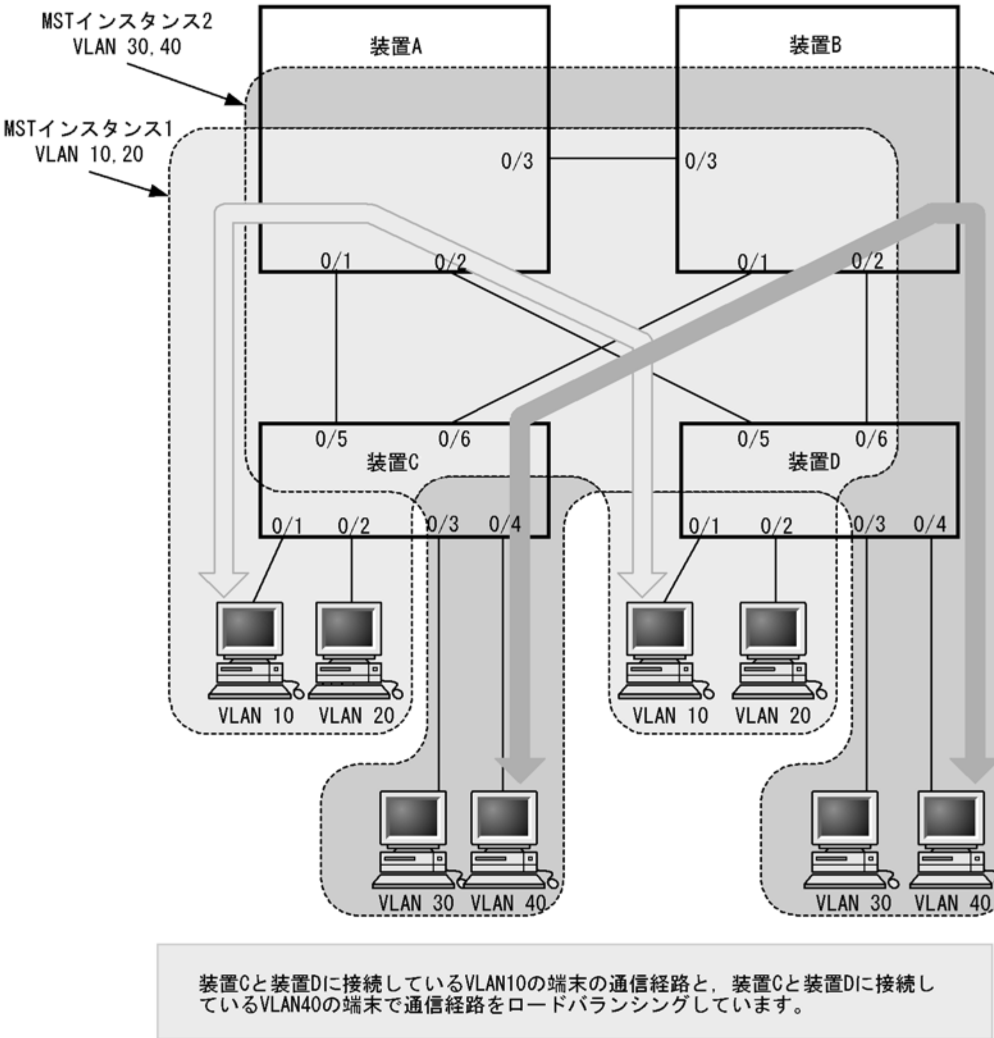
18.9.2　マルチプルスパニングツリーのネットワーク設計

（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 18-13　マルチプルスパニングツリーのロードバランシング構成

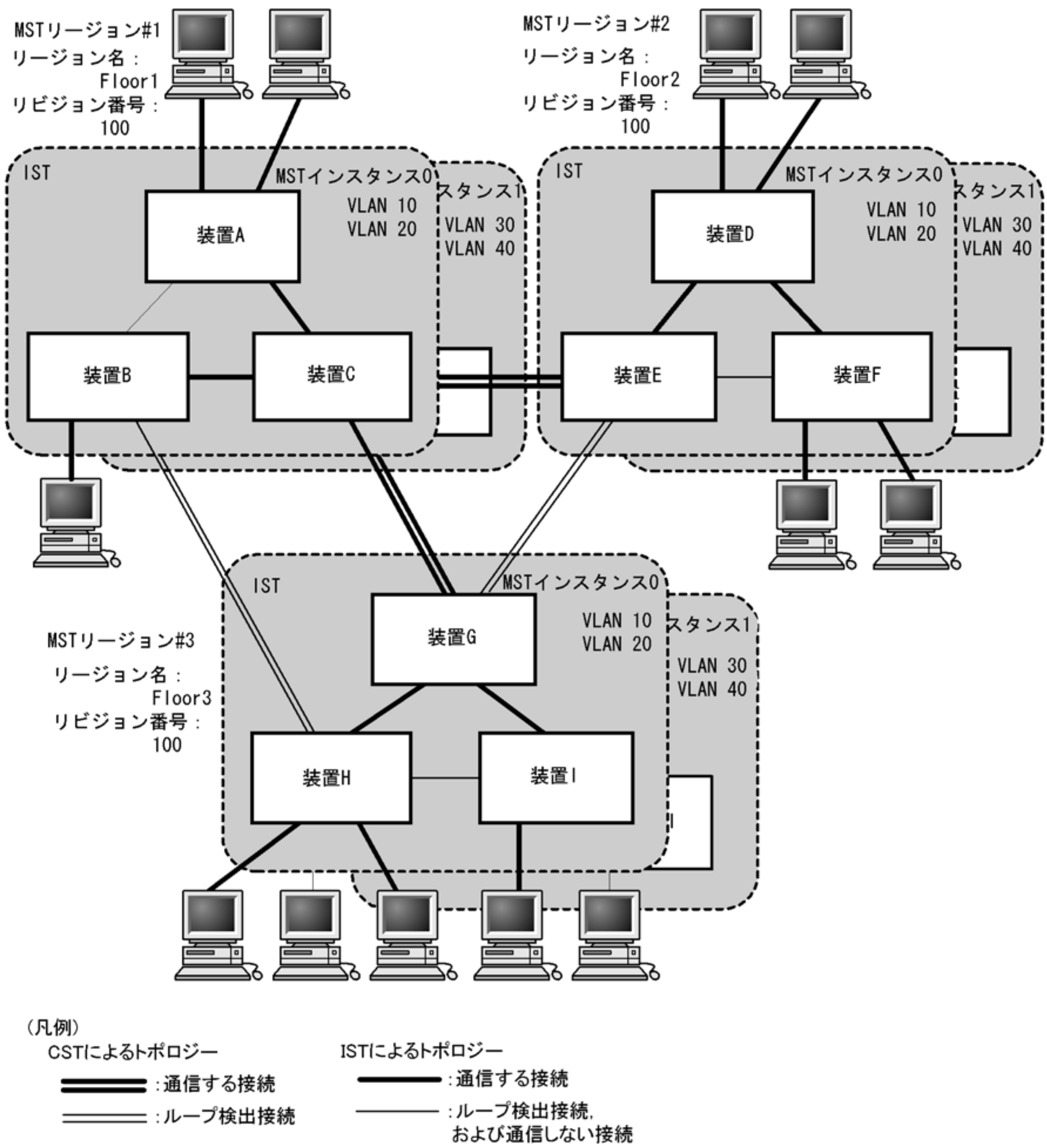


（2） MST リージョンによるネットワーク設計

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

MST リージョンによるネットワーク設計例を次の図に示します。この例では，装置 A，B，C を MST リージョン #1，装置 D，E，F を MST リージョン #2，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 18-14　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

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

（3）トポロジ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

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

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］

no spanning-tree mode コマンドでマルチプルスパニングツリーの動作モード設定を削除すると，デ

フォルトの動作モードである pvst になります。その際，ポート VLAN で自動的に PVST+ が動作を開始します。

(2) リージョン，インスタンスの設定

［設定のポイント］

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

MST インスタンスは，インスタンス番号と所属する VLAN を同時に設定します。リージョンを一致させるために，本装置に未設定の VLAN ID もインスタンスに所属させることができます。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 0/1
   (config-if)# spanning-tree cost 2000
   MST インスタンス 10，20，30 を設定し，ポート 0/1 のパスコストを 2000 に設定します。CIST（インスタンス 0），MST インスタンス 10，20，30 のポート 0/1 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 0/1 のパスコストを 500 に変更します。インスタンス 20 以外は 2000 で動作します。

［注意事項］

リンクアグリゲーションを使用する場合，チャネルグループのパスコストのデフォルト値は，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。リンクアグリゲーションの異速度混在モードを使用している場合は，最も遅い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 0/1**
   (config-if)# spanning-tree port-priority 64
   (config-if)# exit
   ポート 0/1 のポート優先度を 64 に設定します。

2. **(config)# interface gigabitethernet 0/1**
   (config-if)# spanning-tree mst 20 port-priority 144
   (config-if)# exit
   インスタンス 20 のポート 0/1 にポート優先度 144 を設定します。ポート 0/1 ではインスタンス 20 だけポート優先度 144 となり，そのほかのインスタンスは 64 で動作します。

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プログラムの負荷を軽減できます。

［設定のポイント］

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

［コマンドによる設定］

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

［注意事項］

BPDU の送信間隔を短くすると，トポロジ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プログラムの負荷が増加します。本パラメータをデフォルト値（2 秒）より短くすること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 に設定します。

(5) 状態遷移時間の設定

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

［設定のポイント］

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

［コマンドによる設定］

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

   マルチプルスパニングツリーの BPDU の最大有効時間を 10 に設定します。

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。
restart spanning-tree	スパニングツリープログラムを再起動します。
dump protocols spanning-tree	スパニングツリーで採取している詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。

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

図 18-15　show spanning-tree コマンドの実行結果

```
> show spanning-tree mst
Date 2009/01/04 11:41:03 UTC
Multiple Spanning Tree: Enabled
Revision Level: 65535  Configuration Name: MSTP001
CIST Information
  VLAN Mapped: 1-99,151-4095                                                    …1
  CIST Root      Priority: 32768       MAC      : 0012.e207.7200
  External Root Cost     : 2000        Root Port: 0/1
  Regional Root  Priority: 32768       MAC      : 0012.e207.7200
  Internal Root Cost     : 0
  Bridge ID      Priority: 32768       MAC      : 0012.e205.0900
  Regional Bridge Status : Designated
  Port Information
    0/1        Up   Status:Forwarding  Role:Root
    0/2        Up   Status:Discarding  Role:Backup
    0/3        Up   Status:Discarding  Role:Alternate
    0/4        Up   Status:Forwarding  Role:Designated
MST Instance 10
  VLAN Mapped: 100-150
  Regional Root  Priority: 32778       MAC      : 0012.e207.7200
  Internal Root Cost     : 2000        Root Port: 0/1
  Bridge ID      Priority: 32778       MAC      : 0012.e205.0900
  Regional Bridge Status : Designated
  Port Information
    0/1        Up   Status:Forwarding  Role:Root
    0/2        Up   Status:Discarding  Role:Backup
    0/3        Up   Status:Discarding  Role:Alternate
    0/4        Up   Status:Forwarding  Role:Designated
>
```

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。

(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。

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

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。

(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，トポロジーにループが発生するおそれがあるため，注意してください。

18.12.3 ループガード

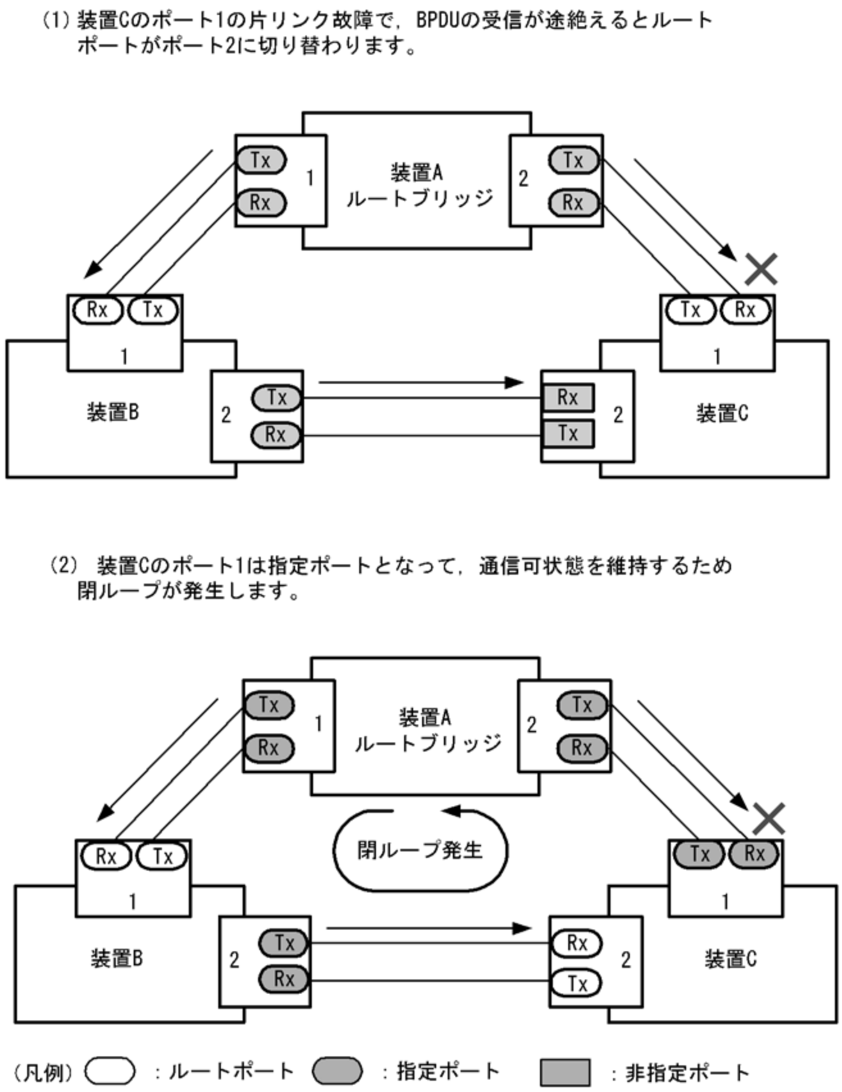
(1) 概要

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 18-16　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，端末を接続するポートを指定する機能である PortFast を設定したポート，またはルートガード機能を設定したポートには設定できません。

(2) ループガードに関する注意事項

ループガードはマルチプルスパニングツリーでは使用できません。

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

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

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

また，両ポートにループガードを設定した場合でも，指定ポートで BPDU を一度も受信せずに，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

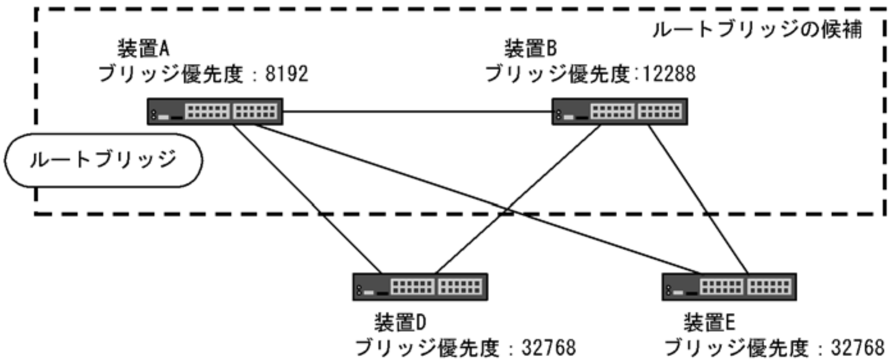
（1） 概要

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。

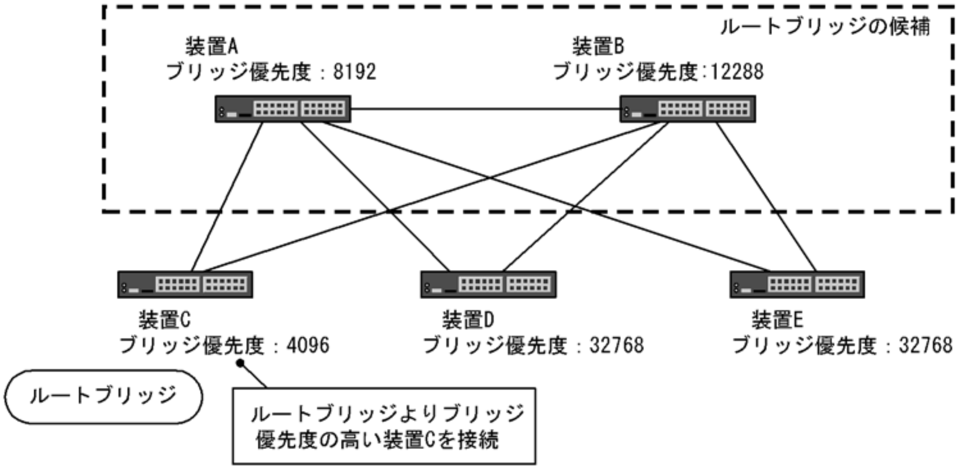
● 装置 A，装置 B をルートブリッジの候補として運用

図 18-17　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 を接続すると本装置 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 18-18　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。

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 18-20　コンフィグレーションコマンド一覧

コマンド名	説明
spanning-tree bpdufilter	ポートごとに BPDU フィルタ機能を設定します。
spanning-tree 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］

spanning-tree portfast default コマンドを設定すると，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，spanning-tree portfast disable コマンドを設定します。
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 0/1**
   (config-if)# switchport mode access
   (config-if)# spanning-tree portfast disable
   (config-if)# exit
   ポート 0/1（アクセスポート）で PortFast 機能を使用しないように設定します。

3. **(config)# interface gigabitethernet 0/3**
   (config-if)# switchport mode trunk
   (config-if)# spanning-tree portfast trunk

(config-if)# exit

ポート 0/3 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。

spanning-tree portfast bpduguard default コマンドは PortFast 機能を適用しているすべてのポートにデフォルトで BPDU ガードを適用します。デフォルトで適用するときに BPDU ガード機能を無効にしたい場合は，spanning-tree bpduguard disable コマンドを設定します。

[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 0/1**
   (config-if)# spanning-tree bpduguard disable
   (config-if)# exit
   ポート 0/1(アクセスポート）で BPDU ガード機能を使用しないように設定します。ポート 0/1 は通常の PortFast 機能を適用します。

3. **(config)# interface gigabitethernet 0/2**
   (config-if)# switchport mode trunk
   (config-if)# spanning-tree portfast trunk
   (config-if)# exit
   ポート 0/2（トランクポート）に PortFast 機能を設定します。また，BPDU ガード機能を設定します。トランクポートはデフォルトでは PortFast 機能を適用しないためポートごとに設定します。デフォルトで BPDU ガード機能を設定している場合は，PortFast 機能を設定すると自動的に BPDU ガードも適用します。デフォルトで設定していない場合は，spanning-tree bpduguard enable コマンドで設定します。

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 0/1**
   (config-if)# spanning-tree bpdufilter enable
   (config-if)# exit
   ポート 0/1 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，このようにループの発生を防止したい場合に設定します。

［設定のポイント］

ループガードは，PortFast 機能を設定していないポートで動作します。

spanning-tree loopguard default コマンドを設定すると，PortFast を設定したポート以外のすべてのポートにループガードを適用します。デフォルトで適用する場合に，ループガードを無効にしたい場合は spanning-tree guard 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 0/1**
   (config-if)# spanning-tree guard none
   (config-if)# exit
   デフォルトでループガードを適用するように設定した状態で，ポート 0/1 はループガードを無効にするように設定します。

3. **(config)# no spanning-tree loopguard default**
   (config)# interface gigabitethernet 0/2
   (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 0/2 に対してポートごとの設定でループガードを適用します。

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 0/1**
   (config-if)# spanning-tree guard root
   (config-if)# exit
   ポート 0/1 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 0/1**
   (config-if)# spanning-tree link-type point-to-point
   (config-if)# exit
   ポート 0/1 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 18-21　運用コマンド一覧

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

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 show spanning-tree detail コマンドで確認してください。VLAN 10 の PVST+ の例を次の図に示します。

PortFast はポート 0/3，0/4，0/5 に設定していることを PortFast の項目で確認できます。ポート 0/3 は PortFast を設定していて，ポート 0/4 は PortFast に加えて BPDU ガードを設定しています。どちらのポートも意図しない BPDU を受信しないで正常に動作していることを示しています。ポート 0/5 は BPDU フィルタを設定しています。

ループガードはポート 0/2 に設定していることを Loop Guard の項目で確認できます。ルートガードはポート 0/6 に設定していることを Root Guard の項目で確認できます。リンクタイプは各ポートの Link Type の項目で確認できます。すべてのポートが point-to-point で動作しています。

図 18-19　スパニングツリーの情報

```
> show spanning-tree vlan 10 detail
Date 2009/01/21 18:13:59 UTC
VLAN 10             PVST+ Spanning Tree:Enabled  Mode:Rapid PVST+
  Bridge ID
    Priority:32778                  MAC Address:0012.e210.3004
    Bridge Status:Designated        Path Cost Method:Short
    Max Age:20                      Hello Time:2
    Forward Delay:15
  Root Bridge ID
    Priority:32778                  MAC Address:0012.e210.1004
    Root Cost:4
    Root Port:0/1
    Max Age:20                      Hello Time:2
    Forward Delay:15
  Port Information
  Port:0/1 Up
    Status:Forwarding               Role:Root
    Priority:128                    Cost:4
    Link Type:point-to-point        Compatible Mode:-
    Loop Guard:OFF                  PortFast:OFF
    BpduFilter:OFF                  Root Guard:OFF
    BPDU Parameters(2009/01/21 18:13:59):
      Designated Root
        Priority:32778              MAC address:0012.e210.1004
      Designated Bridge
        Priority:32778              MAC address:0012.e210.1004
        Root Path Cost:0
      Port ID
        Priority:128                Number:1
      Message Age Time:0(3)/20
  Port:0/2 Up
    Status:Discarding               Role:Alternate
    Priority:128                    Cost:4
    Link Type:point-to-point        Compatible Mode:-
    Loop Guard:ON                   PortFast:OFF
    BpduFilter:OFF                  Root Guard:OFF
    BPDU Parameters(2009/01/21 18:13:58):
      Designated Root
        Priority:32778              MAC address:0012.e210.1004
      Designated Bridge
        Priority:32778              MAC address:0012.e210.2004
        Root Path Cost:4
      Port ID
        Priority:128                Number:1
      Message Age Time:1(3)/20
  Port:0/3 Up
    Status:Forwarding               Role:Designated
    Priority:128                    Cost:4
    Link Type:point-to-point        Compatible Mode:-
    Loop Guard:OFF                  PortFast:ON (BPDU not received)
    BpduFilter:OFF                  Root Guard:OFF
  Port:0/4 Up
    Status:Forwarding               Role:Designated
    Priority:128                    Cost:4
    Link Type:point-to-point        Compatible Mode:-
    Loop Guard:OFF                  PortFast:BPDU Guard(BPDU not received)
    BpduFilter:OFF                  Root Guard:OFF
  Port:0/5 Up
    Status:Forwarding               Role:Designated
    Priority:128                    Cost:4
    Link Type:point-to-point        Compatible Mode:-
    Loop Guard:OFF                  PortFast:ON(BPDU not received)
    BpduFilter:ON                   Root Guard:OFF
  Port:0/6 Up
```

```
Status:Forwarding                Role:Designated
Priority:128                     Cost:4
Link Type:point-to-point         Compatible Mode:-
Loop Guard:OFF                   PortFast:OFF
BpduFilter:OFF                   Root Guard:ON
```

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。

本装置の Ring Protocol は，アラクサラネットワークス株式会社の AX3600S シリーズや AX2400S シリーズなどでサポートしている Ring Protocol と互換性があります。本装置と AX3600S シリーズや AX2400S シリーズとのリング構成を構築することは可能です。

Ring Protocol の適用例を次の図に示します。

図 19-1　Ring Protocol の適用例（その 1）

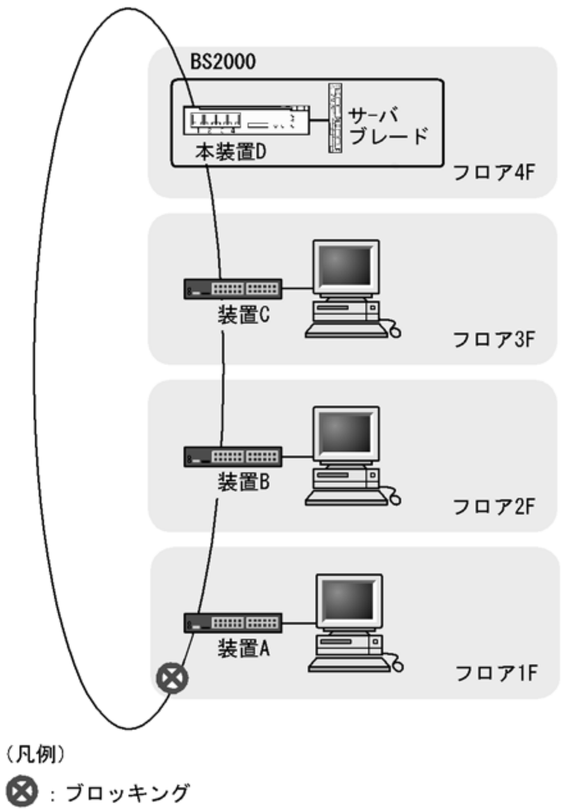
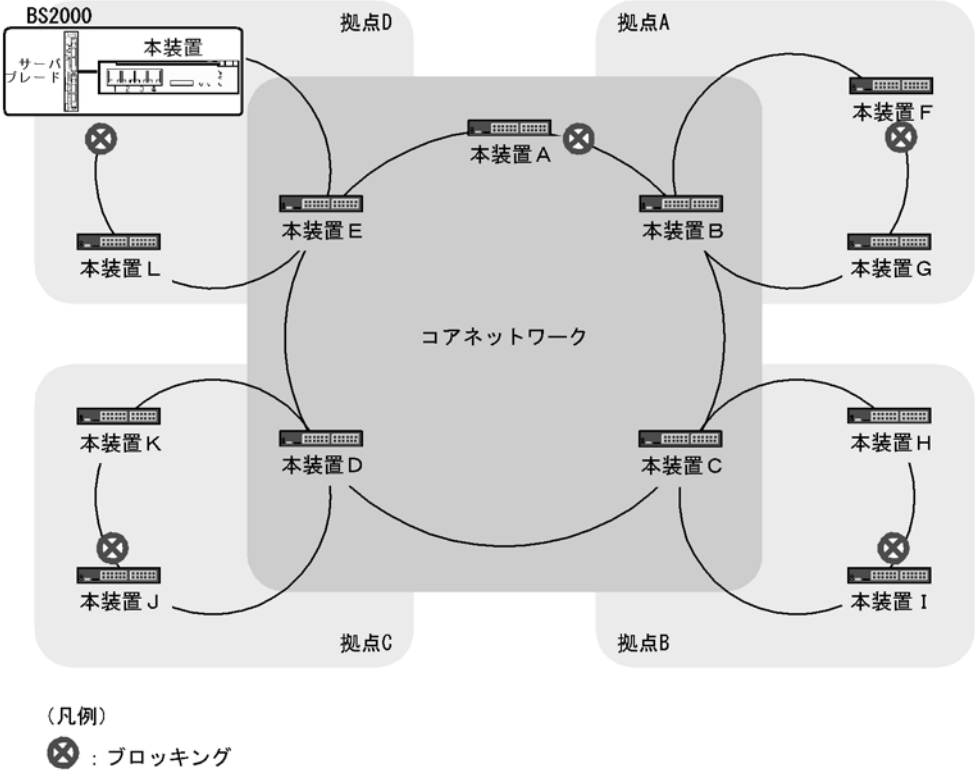
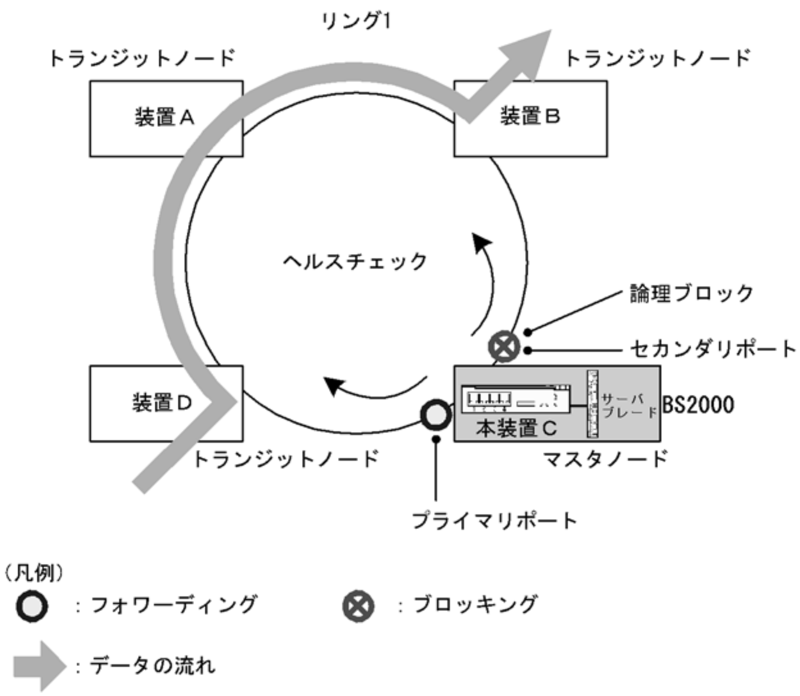


図 19-2　Ring Protocol の適用例（その 2）



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 19-3　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。

(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	○
	レイヤ 3	×
リング構成	シングルリング	○
	マルチリング	○（共有リンクありマルチリング構成含む）
装置当たりのリング ID 最大数		8
リングポート（1 リング ID 当たりのポート数）		2（物理ポートまたはリンクアグリゲーション）

項目		内容
VLAN 数	1 リング ID 当たりの制御 VLAN 数	1（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 最大数	1023
ヘルスチェックフレーム送信間隔		500 〜 60000 ミリ秒の範囲で 1 ミリ秒単位
障害監視時間		500 〜 300000 ミリ秒の範囲で 1 ミリ秒単位
負荷分散方式		二つのデータ転送用 VLAN グループを使用することで可能

（凡例）　○：サポート　×：未サポート

19.2　Ring Protocol の基本原理

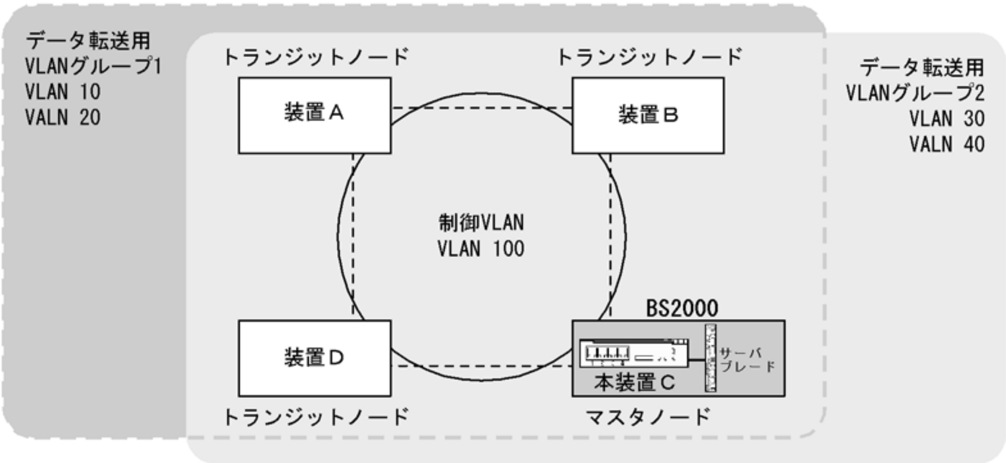
19.2.1　ネットワーク構成

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

（1） シングルリング構成

シングルリング構成について，次の図に示します。

図 19-4　シングルリング構成

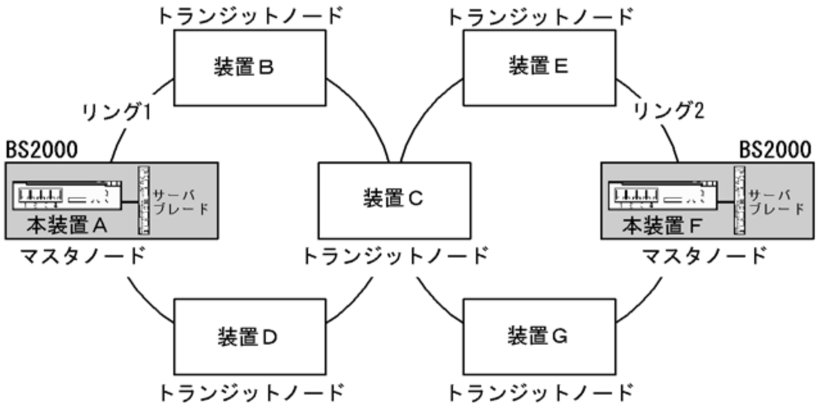


マスタノード 1 台とトランジットノード数台から成る一つのリング構成をシングルリング構成と呼びます。リングを構成するノード間は，リングポートとして，物理ポートまたはリンクアグリゲーションで接続されます。また，リングを構成するすべてのノードに，制御 VLAN として同一の VLAN，およびデータフレームの転送用として共通の VLAN を使用する必要があります。マスタノードから送信した制御フレームは，制御 VLAN 内を巡回します。データフレームの送受信に使用する VLAN は，VLAN グループと呼ばれる一つの論理的なグループに束ねて使用します。VLAN グループは複数の VLAN をまとめるこ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

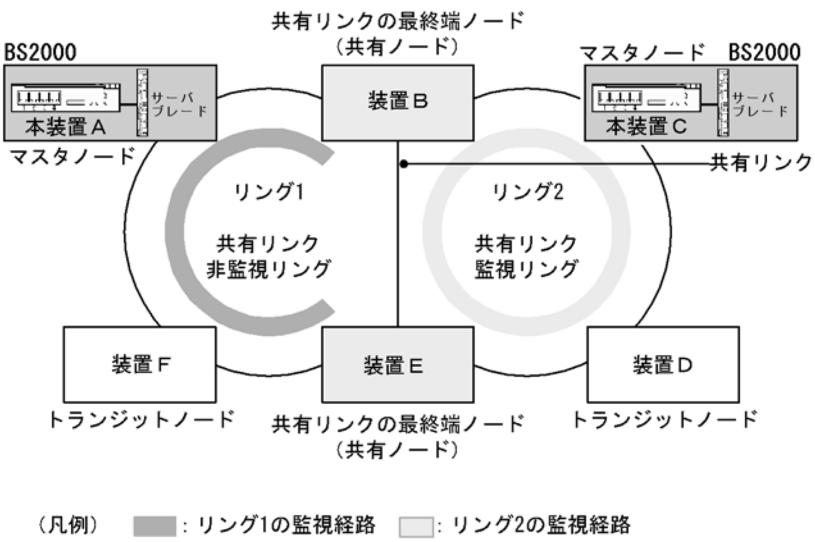


それぞれのリングを構成しているノードは独立したシングルリングとして動作します。このため，リング障害の検出および復旧の検出はそれぞれのリングで独立して行われます。

(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) 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

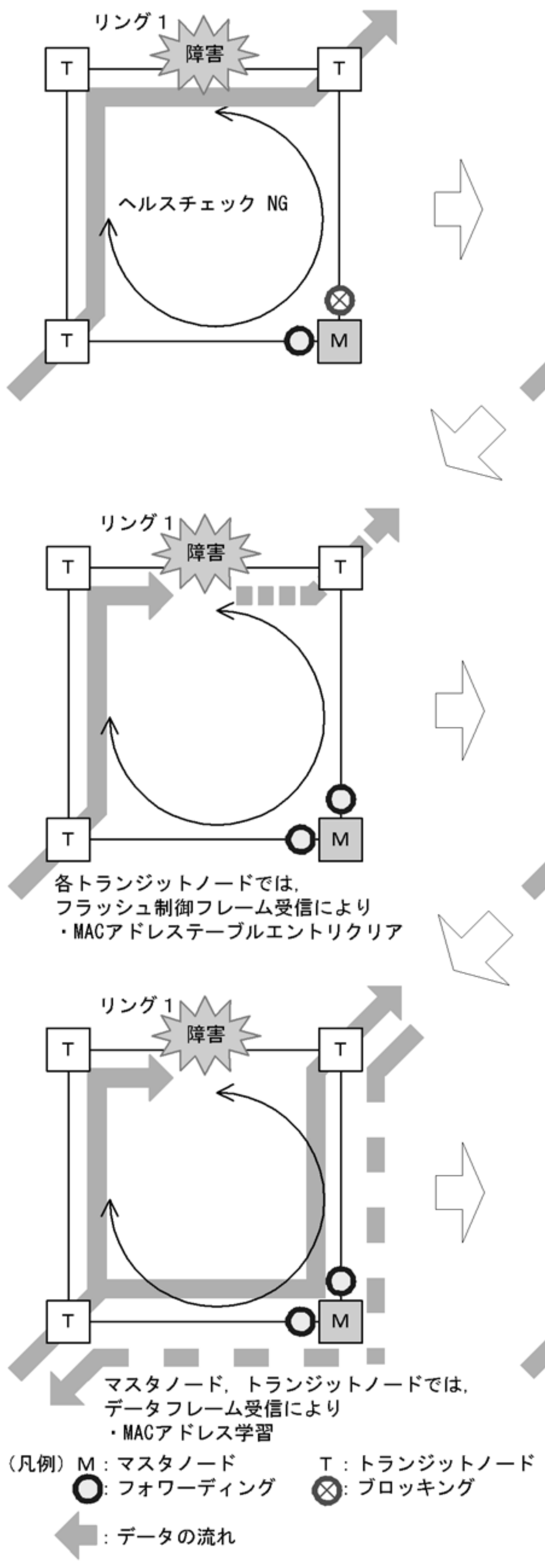
Ring Protocol のリング障害の監視は，マスタノードがヘルスチェックフレームと呼ぶ制御フレームを定期的に送信し，マスタノードがこのヘルスチェックフレームの受信可否を監視することで実現します。マスタノードでは，ヘルスチェックフレームが一定時間到達しないとリング障害が発生したと判断し，障害動作を行います。また，リング障害中に再度ヘルスチェックフレームを受信すると，リング障害が復旧したと判断し，復旧動作を行います。

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）前の情報に従ってデータフレームの転送が行われるため，正しくデータが届かないおそれがあります。したがって，通信を復旧させるために，リングを構成するすべてのノードで MAC アドレステーブルエントリのクリアを実施します。

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

図 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

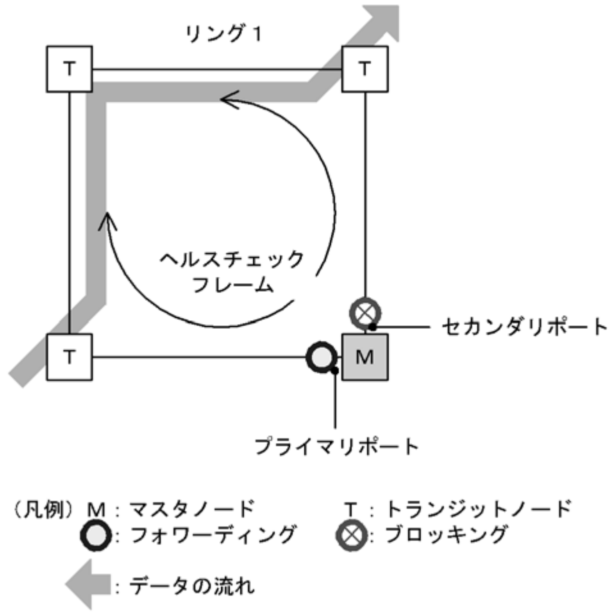
マスタノードがリングの障害を検出すると，同一の制御 VLAN を持つリング内の，そのほかのトランジットノードに対して MAC アドレステーブルエントリのクリアを要求するために，フラッシュ制御フレームと呼ぶ制御フレームを送信します。トランジットノードでは，このフラッシュ制御フレームを受信すると，リングポートでの MAC アドレステーブルエントリのクリアを行います。これによって，MAC アドレスの学習が行われるまでフラッディングを行います。新しい経路でのフレームの送受信によって MAC アドレス学習が行われ，通信経路の切り替えが完了します。

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。

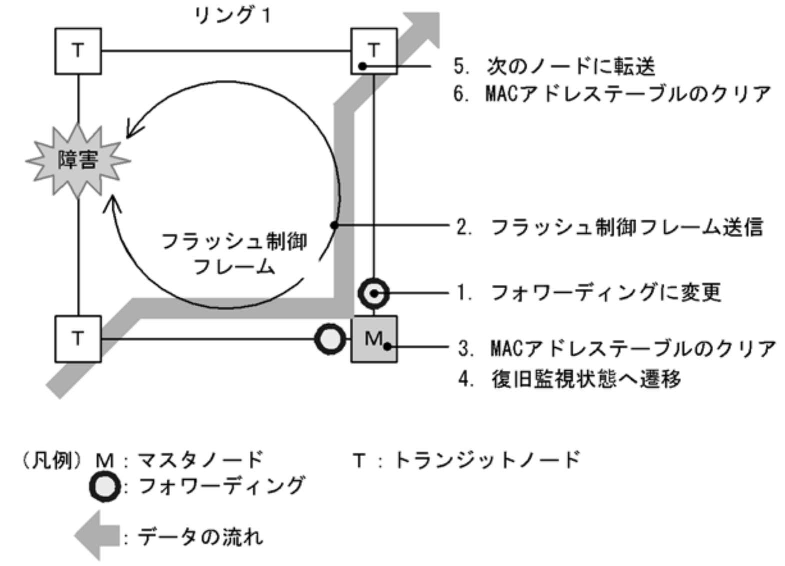
（2） トランジットノード動作

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。

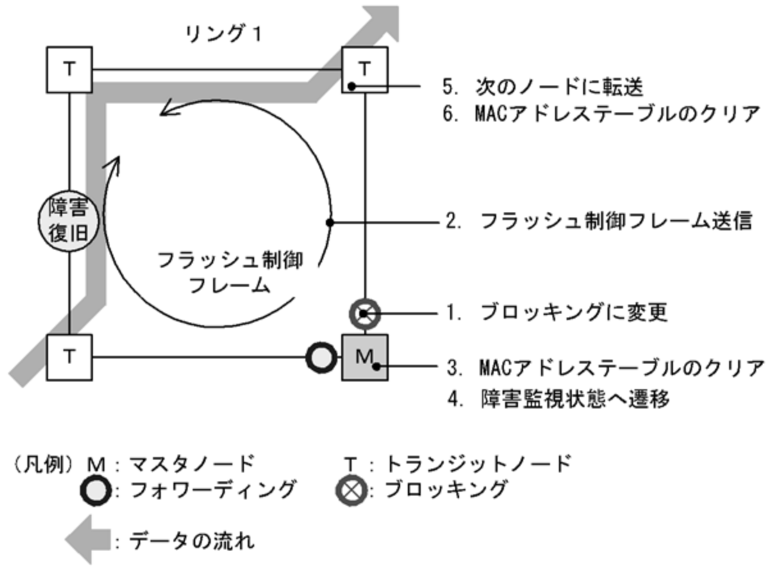
6. **MAC アドレステーブルのクリア**

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，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，迂回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（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（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。

19.4　マルチリングの動作概要

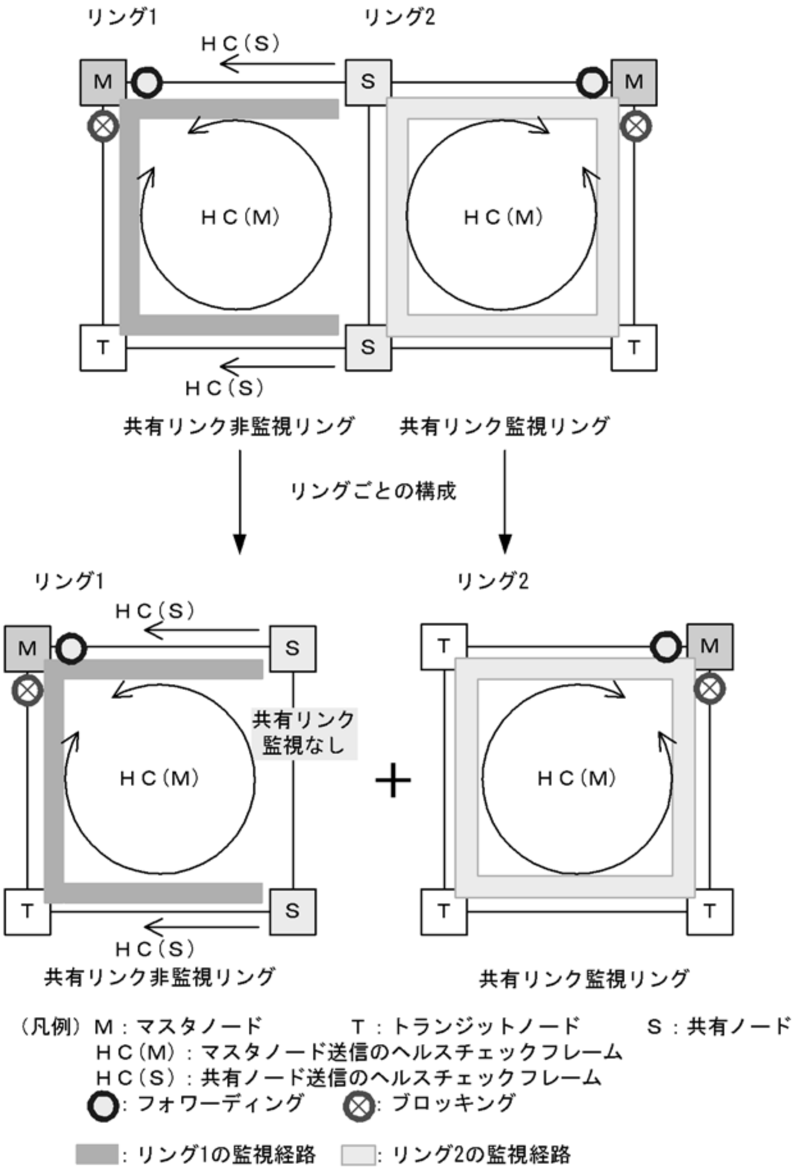
マルチリング構成のうち，共有リンクありのマルチリング構成について説明します。共有リンクなしのマルチリング構成については，シングルリング時の動作と同様ですので，「19.3　シングルリングの動作概要」を参照してください。

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

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。

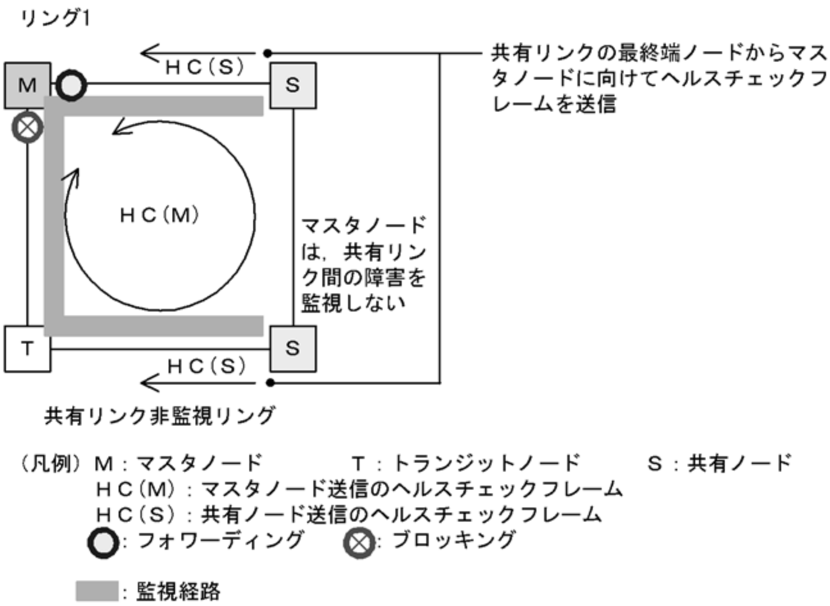
図 19-11　リング正常時の状態



(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 19-12　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。

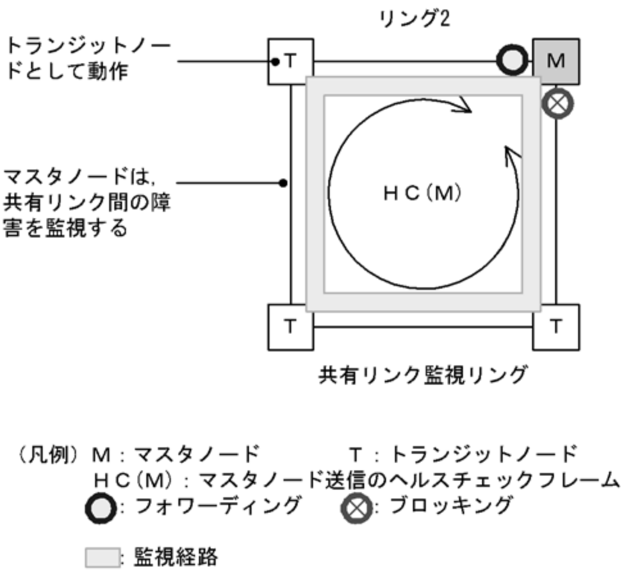
(c) 共有リンク非監視リングの最終端ノード動作

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 19-13　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。

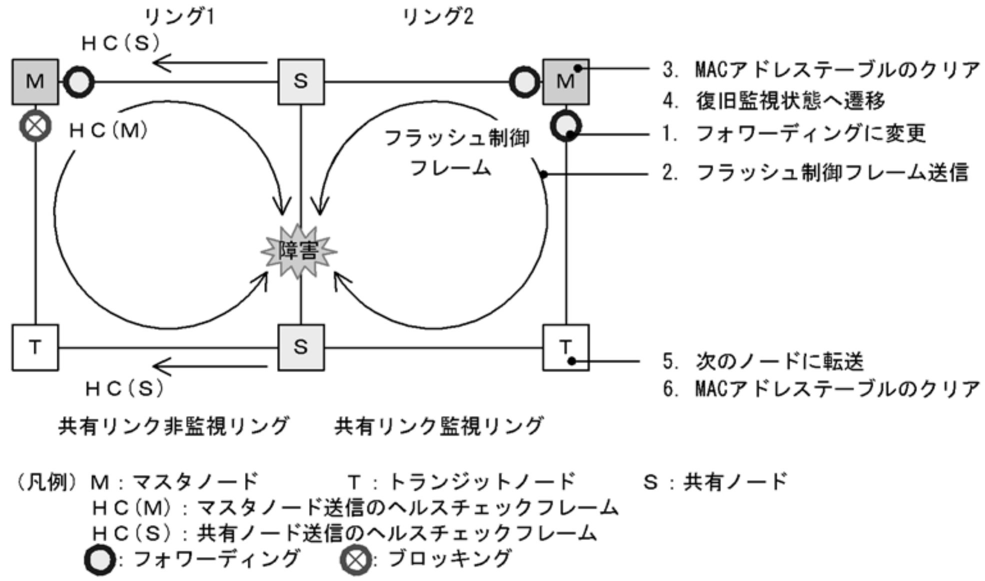
19.4.2　共有リンク障害・復旧時の動作

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 19-14　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

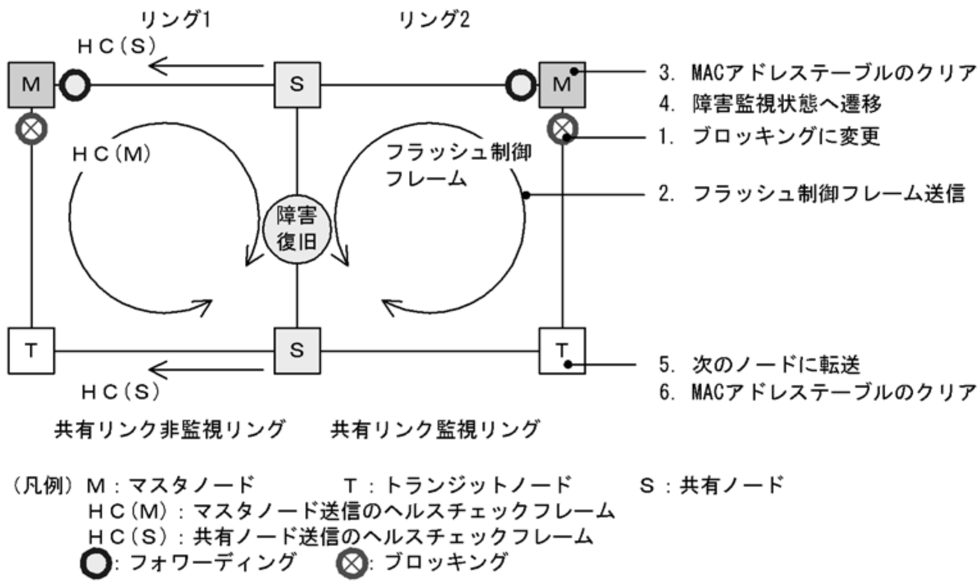
(c) 共有リンク非監視リングのマスタノードおよびトランジットノード動作

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 19-15　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。

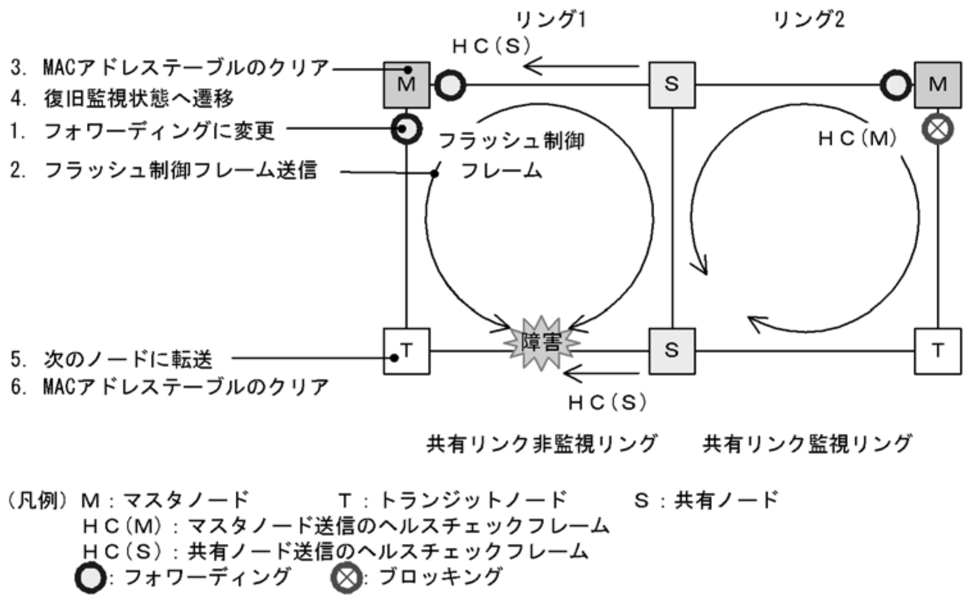
19.4.3　共有リンク非監視リングでの共有リンク以外の障害・復旧時の動作

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 19-16　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

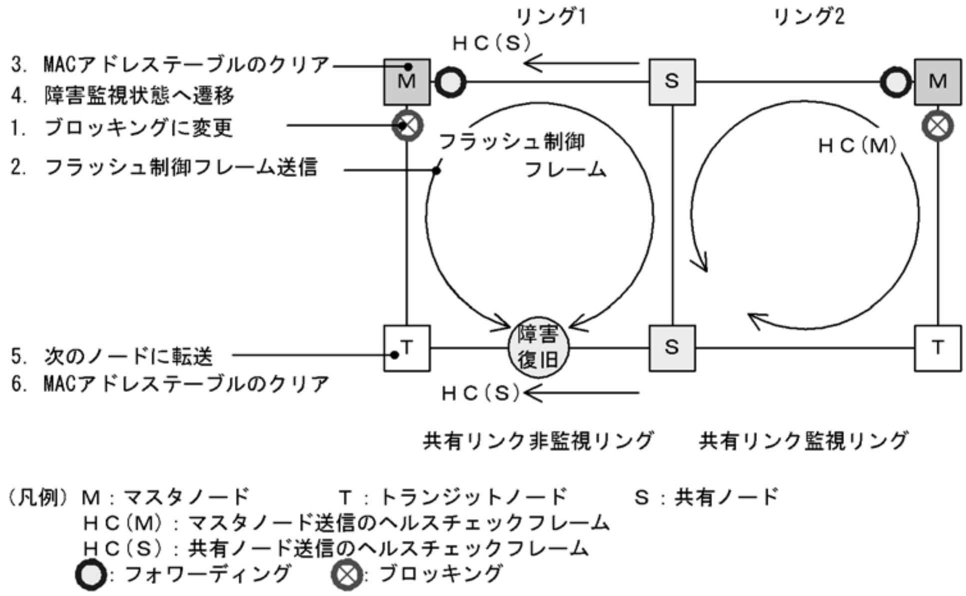
(c)　共有リンク監視リングのマスタノードおよびトランジットノード動作

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 19-17　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。

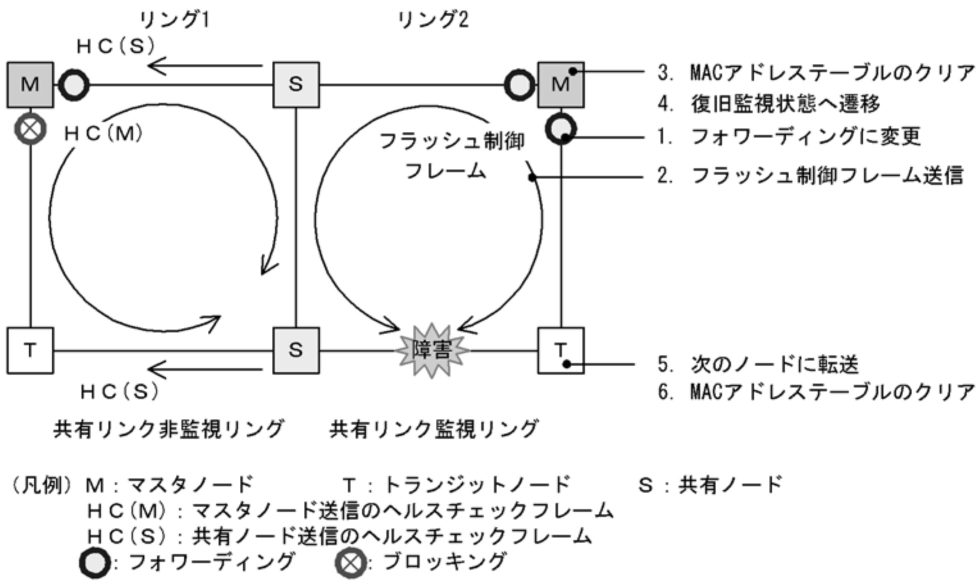
19.4.4　共有リンク監視リングでの共有リンク以外の障害・復旧時の動作

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 19-18　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

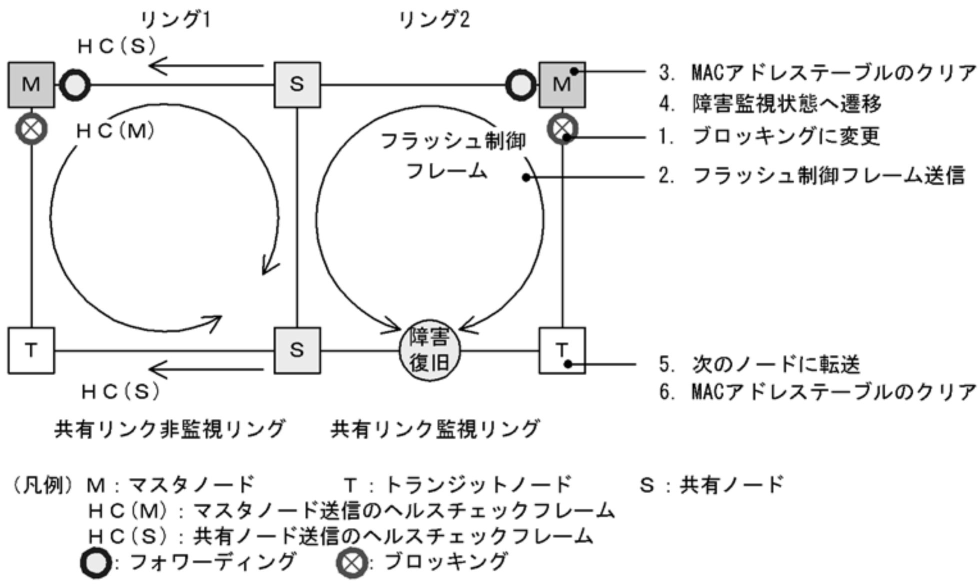
(c) 共有リンク非監視リングのマスタノードおよびトランジットノード（共有ノード）動作

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 19-19　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。

19.5　Ring Protocol のネットワーク設計

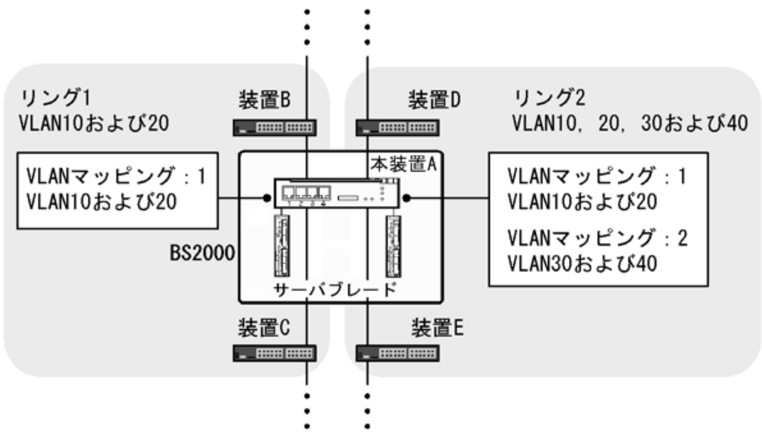
19.5.1　VLAN マッピングの使用方法

（1）VLAN マッピングとデータ転送用 VLAN

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

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

図 19-20　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 VLAN マッピングと合わせて VLAN グループに設定します。

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

トランジットノードの装置起動やプログラム再起動（運用コマンド restart axrp）など，Ring Protocol が初期状態から動作する場合，データ転送用 VLAN は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，プログラム再起動時などは，マスタノードの障害監視時間（health-check holdtime）が長いと，リングネットワークの状態変化を認識できないおそれがあります。この場合，フラッシュ制御フレーム受信待ち保護時間（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（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，装置起動やプログラム再起動直後に，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（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（forwarding-delay-time）と障害監視時間（health-check holdtime）の関係について

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

（2）制御 VLAN のフォワーディング遷移時間（forwarding-delay-time）とフラッシュ制御フレーム受信待ち保護時間（forwarding-shift-time）の関係について

制御 VLAN のフォワーディング遷移時間（forwarding-delay-time）は，データ転送用 VLAN のフラッシュ制御フレーム受信待ち保護時間（forwarding-shift-time）より小さな値を設定してください。フラッシュ制御フレーム受信待ち保護時間（forwarding-shift-time）より大きな値を設定した場合，マスタノードが障害検出するよりも早くデータ転送用 VLAN がフォワーディングとなるため，ループするおそれがあります。

19.5.3　プライマリポートの自動決定

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

表 19-4　プライマリポートの選択方式（VLAN グループ＃ 1）

リングポート＃ 1	リングポート＃ 2	優先ポート
物理ポート	物理ポート	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 19-5　プライマリポートの選択方式（VLAN グループ＃ 2）

リングポート＃ 1	リングポート＃ 2	優先ポート
物理ポート	物理ポート	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。

19.5.4　同一装置内でのノード種別混在構成

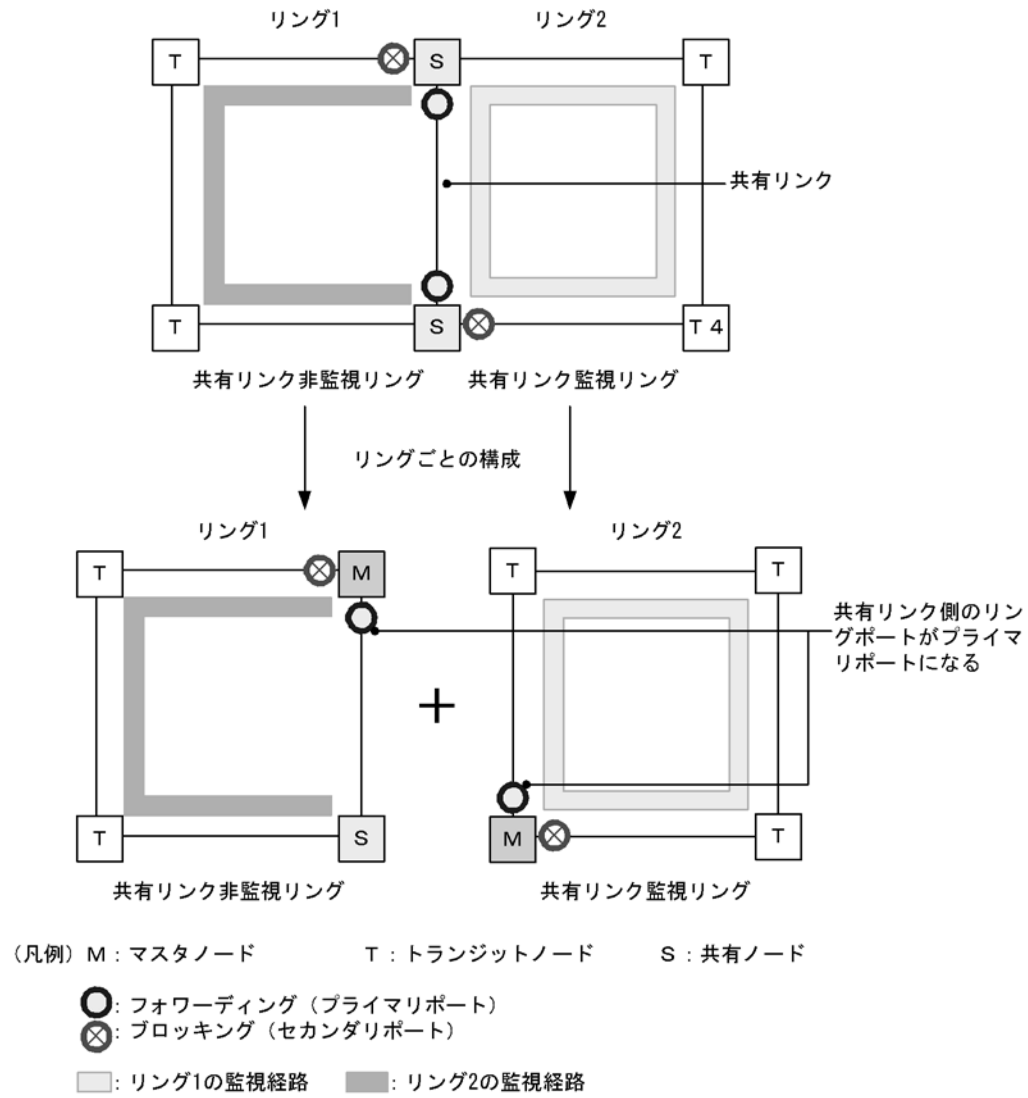
（1）ノード種別の混在設定

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。

19.5.5　共有ノードでのノード種別混在構成

共有リンクありのマルチリング構成で，共有リンクの両端に位置するノードをマスタノードとして動作させることができます。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 19-21　共有ノードをマスタノードとした場合のポート状態



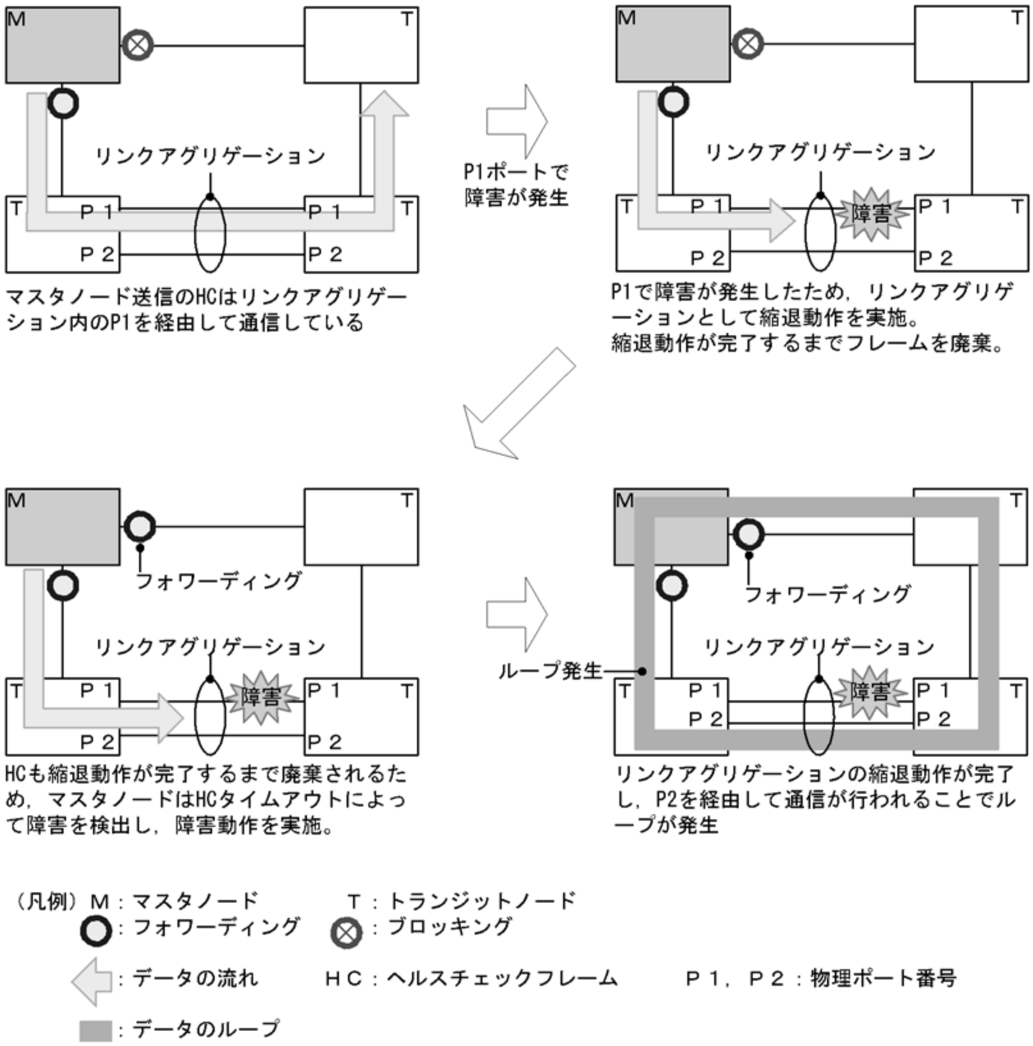
19.5.6　リンクアグリゲーションを用いた場合の障害監視時間の設定

リングポートをリンクアグリゲーションで構成した場合に，ヘルスチェックフレームが転送されているリンクアグリゲーション内のポートに障害が発生すると，リンクアグリゲーションの切り替えまたは縮退動作が完了するまでの間，制御フレームが廃棄されてしまいます。このため，マスタノードの障害監視時間（health-check holdtime）がリンクアグリゲーションの切り替えまたは縮退動作が完了する時間よりも短いと，マスタノードがリングの障害を誤検出し，経路の切り替えを行います。この結果，ループが発生するおそれがあります。

リングポートをリンクアグリゲーションで構成した場合は，マスタノードの障害監視時間をリンクアグリゲーションによる切り替えまたは縮退動作が完了する時間よりも大きくする必要があります。

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 19-22　リンクアグリゲーション使用時の障害検出



19.5.7　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。

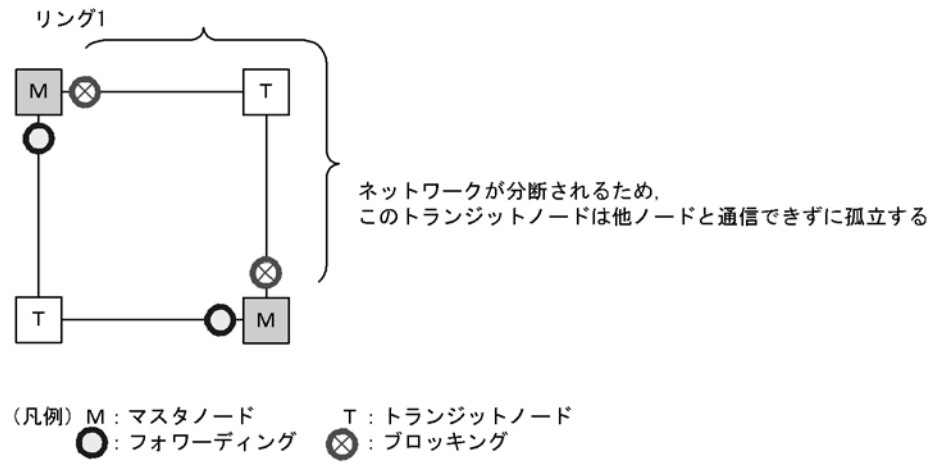
19.5.8　Ring Protocol の禁止構成

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

（1）同一リング内に複数のマスタノードを設定

同一のリング内に 2 台以上のマスタノードを設定しないでください。同一リング内に複数のマスタノードがあると，セカンダリポートが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。

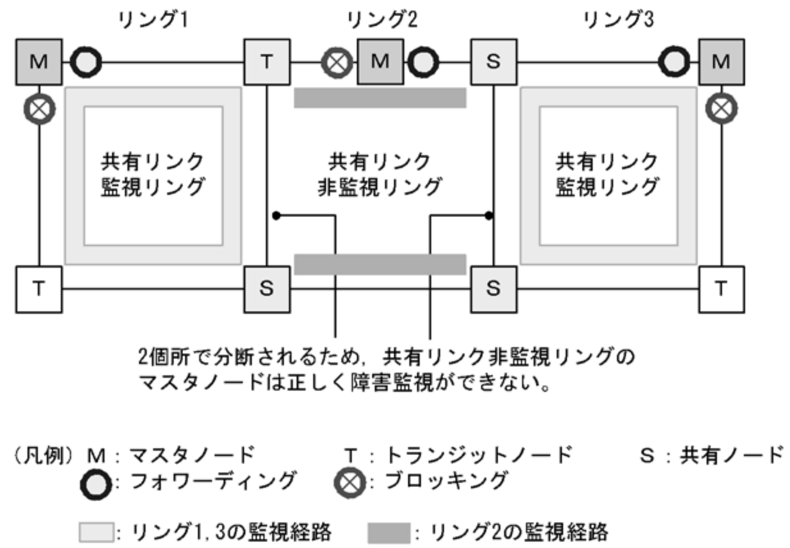
図 19-23　同一リング内に複数のマスタノードを設定



（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。

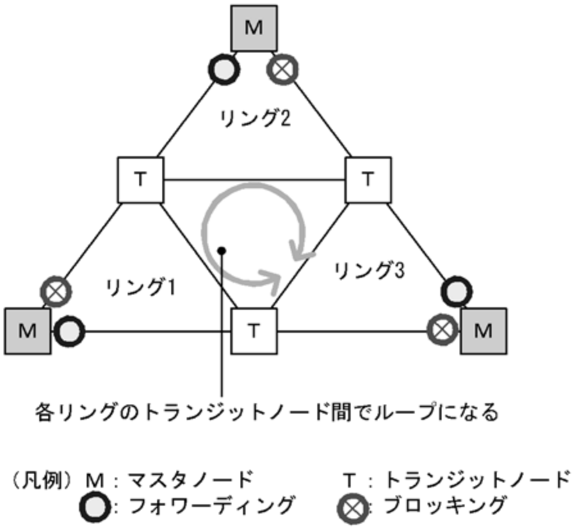
図 19-24　共有リンク監視リングが複数ある構成



（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。

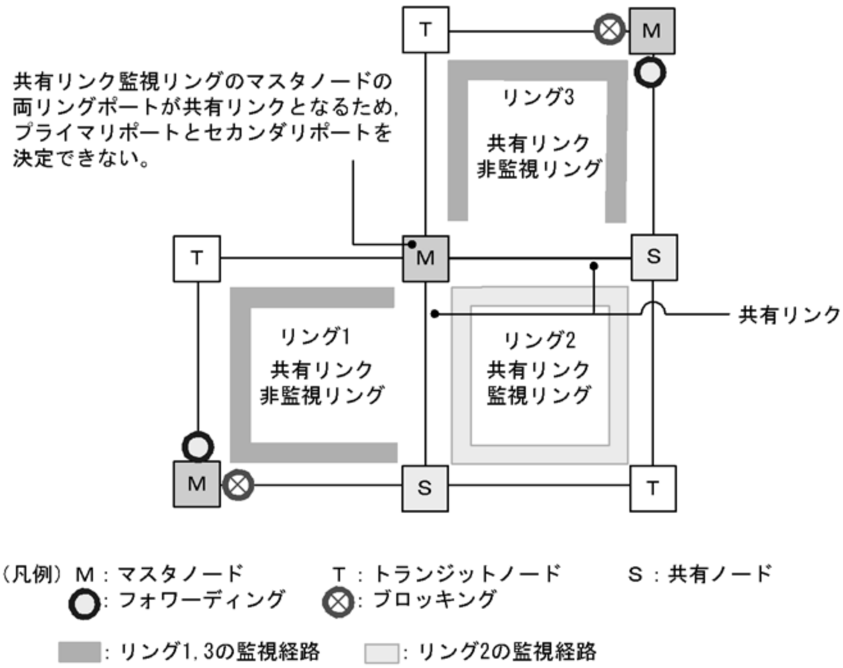
図 19-25　ループになるマルチリング構成



（4） 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

共有リンクありのマルチリング構成で，マスタノードの両リングポートが共有リンクとなるような構成はできません。次の図のようなマルチリング構成を組むと共有リンク監視リングの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，共有リンク監視リング内のプライマリポートとセカンダリポートを決定できません。

図 19-26　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



19.6 Ring Protocol 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 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。

(3) 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（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（forwarding-shift-time）がマスタノードのヘルスチェック送信間隔（health-check interval）よりも短い場合，マスタノードがリング障害の復旧を検出して，セカンダリポートをブロッキング状態に変更するよりも先に，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。したがって，フラッシュ制御フレーム受信待ち保護時間（forwarding-shift-time）はヘルスチェック送信間隔（health-check interval）より大きい値を設定してください。

(4) 共有リンクありのマルチリングでの VLAN 構成について

複数のリングで共通に使用する共有リンクでは，それぞれのリングで同じ VLAN を使用する必要があります。共有リンク間での VLAN のポート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。

(5) 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。ネットワークの構築時は，次に示すような対応を行い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や，Ring Protocol の設定を含むコンフィグレーションファイルのコピー（copy コマンド）を行う際は，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。

(6) 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 のコンフィグレーションを変更する際には，ループが発生しないように注意する必要があります。対象となるコンフィグレーションごとの対応方法を次に示します。

1. 動作モード（mode コマンド）の変更
   Ring Protocol の動作しているノードで，マスタノードからトランジットノード，またはトランジットノードからマスタノードへ動作モードを変更する際には，プロトコル動作がいったん停止しますので，一時的にループが発生するおそれがあります。あらかじめ，リングポートを shutdown するなどループにならないことを確認の上，動作モードを変更してください。

2. 制御 VLAN（control-vlan コマンド），およびデータ転送用 VLAN（axrp vlan-mapping コマンド，vlan-group コマンド）の変更
   リング内で使用する制御 VLAN やデータ転送用 VLAN の変更を行う際には，ネットワークの構成上ループが発生しますので，あらかじめ変更する VLAN を停止するか，リングポートを shutdown してから変更してください。
3. Ring Protocol 動作中のプライマリポートの変更
   Ring Protocol 動作中にマスタノードのプライマリポートの変更が発生する場合があります。このとき，プロトコル動作がいったん停止しますので，一時的にループが発生するおそれがあります。あらかじめ，リングポートを shutdown するなどループにならないことを確認の上，変更してください。プライマリポートが変更されるケースについて次に示します。
   - プライマリポートの設定（コンフィグレーションコマンド axrp-primary-port）によって，プライマリポートの変更が発生した場合
   - 共有リンクありのマルチリング構成を組むときに，共有リンク監視リングのマスタノードとして動作している装置に対して，共有リンク非監視リングの最終端ノードも兼ねるような追加設定によって，それまで動作していた共有リンク監視リングのマスタノードのプライマリポートが変更された場合

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

(8) 相互運用

Ring Protocol は，本装置独自仕様の機能です。ただし，アラクサラネットワークス株式会社の AX シリーズで本 Ring Protocol をサポートしている装置との相互運用は可能です。それ以外の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。
- アラクサラネットワーク株式会社製 AX6300S シリーズまたは，AX6700S シリーズをマスタノード，本装置をそのほかの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，および障害監視時間を 500 ミリ秒以上に設定してください。500 ミリ秒以下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。

（12）CPU 負荷が高いときの動作について

CPU が過負荷な状態になった場合，マスタノードである本装置が送受信する Ring Protocol の制御フレームの廃棄または処理遅延が発生し，障害の誤検出による経路の切り替え，一時的な通信断などが発生することがあります。過負荷状態が頻発する場合は，制御フレームの送信間隔（health-check interval）および障害監視時間（health-check holdtime）を大きい値に設定するなどして運用してください。

（13）VLAN のダウンを伴う障害発生時の経路の切り替えについて

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

なお，VLAN debounce 機能を使用することで VLAN のダウンを回避できる場合があります。VLAN debounce 機能の詳細については，「17.9　VLAN debounce 機能の解説」を参照してください。

（14）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。

（15）ログイン・ログアウト時の Ring Protocol 動作について

Ring Protocol の制御フレームの送信間隔（health-check interval），および受信待ち保護時間（health-check holdtime）に小さな値を設定している場合，本装置へのログイン，もしくは本装置からのログアウトを実施すると，制御フレームの送受信処理で廃棄，または処理遅延が発生し，障害を誤検出するおそれがあります。

障害の誤検出が頻発する場合には，次のコマンドを実行することによって，ログイン・ログアウト時の内蔵フラッシュメモリ書き込みを抑止し，障害の誤検出の発生頻度を軽減できます。これらのコマンドを実行した後も障害の誤検出が発生する場合には，制御フレームの送信間隔，および受信待ち保護時間を大きい値に設定するなどして運用してください。

- ユーザアカウントのホームディレクトリを内蔵フラッシュメモリ上に作成しないで，メモリ上に作成する指定

```
# adduser user1 no-flash
```

- 装置で発生したログを内蔵フラッシュメモリに格納しない設定

```
(config)# no logging syslog-dump
```

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

（17）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（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。

なお，次の場合も同様です。

- VLAN プログラムの再起動（運用コマンド restart vlan の実行）
- コンフィグレーションファイルの運用への反映（運用コマンド copy の実行）

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。
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。
name	リングを識別するための名称を設定します。
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

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。データ転送用 VLAN に使われている VLAN は使用できません。また，異なるリングで使われている VLAN ID と同じ値の VLAN ID は使用できません。

[コマンドによる設定]

1. **(config)# axrp 1**
   リング ID 1 の axrp コンフィグレーションモードに移行します。

2. **(config-axrp)# control-vlan 2**
   (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 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。ただし，フラッシュ制御フレーム受信待ち保護時間（forwarding-shift-time コマンドでの設定値）よりも小さ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となった場合，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)# 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

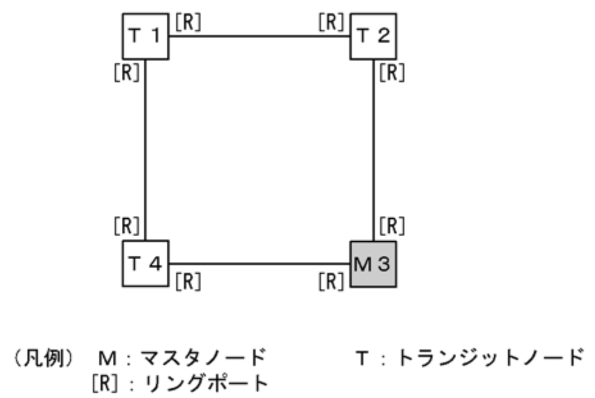
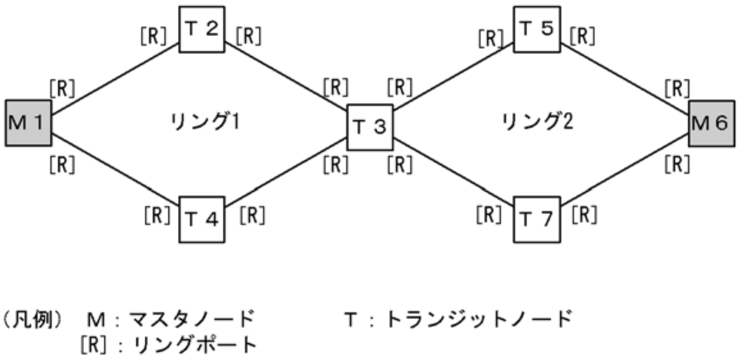


図 20-2　共有リンクなしマルチリング構成



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 0/1**
   (config-if)# axrp-ring-port 2
   (config-if)# exit
   (config)# interface gigabitethernet 0/2
   (config-if)# axrp-ring-port 2
   (config-if)# exit
   ポート 0/1 および 0/2 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 0/1**
   (config-if)# axrp-ring-port 2
   (config-if)# exit
   (config)# interface gigabitethernet 0/2
   (config-if)# axrp-ring-port 2
   (config-if)# exit
   ポート 0/1 および 0/2 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。

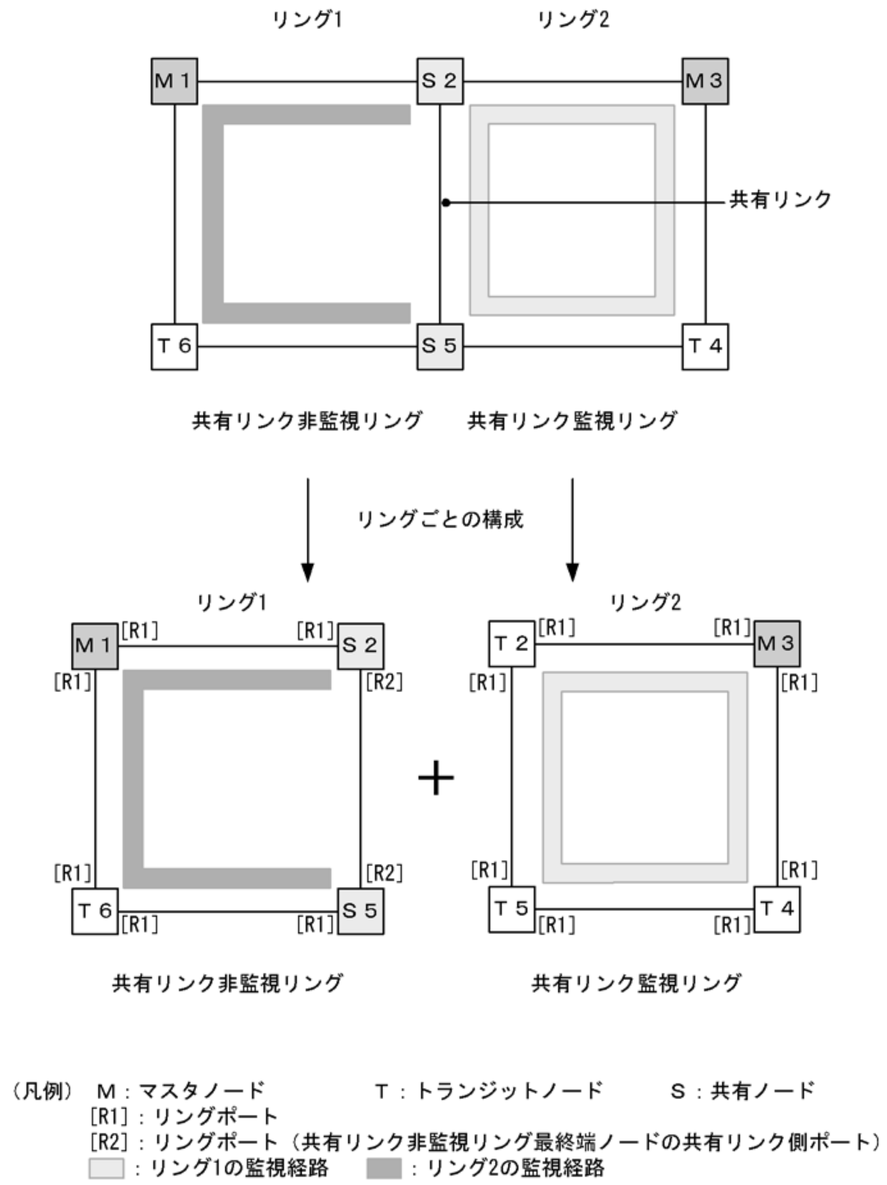
20.1.8　モードとリングポートに関する設定（共有リンクありマルチリング構成）

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）



(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 0/1**
   (config-if)# axrp-ring-port 1
   (config-if)# exit
   (config)# interface gigabitethernet 0/2
   (config-if)# axrp-ring-port 1
   (config-if)# exit
   ポート 0/1 および 0/2 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 での動作モードをトランジットモード，リング属性を共有リンク非監視リングの最終端ノード，エッジノード ID を 1 に設定します。

2. **(config)# interface gigabitethernet 0/1**
   (config-if)# axrp-ring-port 1
   (config-if)# exit

```
(config)# interface gigabitethernet 0/2
(config-if)# axrp-ring-port 1 shared-edge
(config-if)# exit
```

ポート 0/1 および 0/2 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 0/2 を共有リンクとして shared-edge パラメータも設定します。

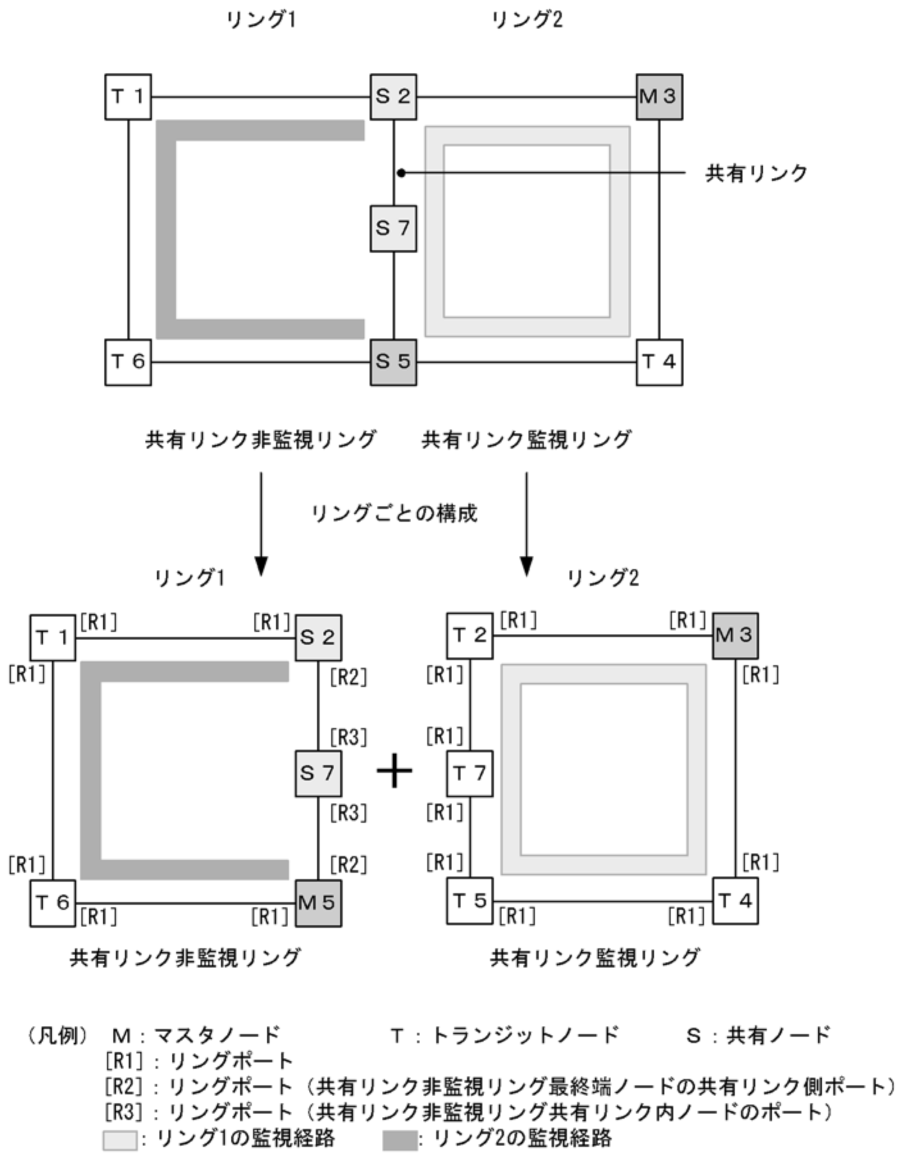
［注意事項］

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

(2) 共有リンクありのマルチリング構成（拡張構成）

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

図 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 での動作モードをマスタモード，リング属性を共有リンク非監視リングの最終端ノード，エッジノード ID を 2 に設定します。

2. **(config)# interface gigabitethernet 0/1**
(config-if)# axrp-ring-port 1
(config-if)# exit
(config)# interface gigabitethernet 0/2
(config-if)# axrp-ring-port 1 shared-edge
(config-if)# exit
ポート 0/1 および 0/2 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 0/2 を共有リンクとして shared-edge パラメータも設定します。

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

(b) 共有リンク非監視リングの共有リンク内ノード（トランジット）

［設定のポイント］
リングでの本装置の動作モードをトランジットモードに設定します。「図 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 0/1**
(config-if)# axrp-ring-port 1 shared
(config-if)# exit
(config)# interface gigabitethernet 0/2
(config-if)# axrp-ring-port 1 shared
(config-if)# exit
ポート 0/1 および 0/2 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 指定でポート設定をした場合，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。

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。
dump protocols axrp	Ring Protocol プログラムで採取している詳細イベントトレース情報および制御テーブル情報をファイルへ出力します。
restart axrp	Ring Protocol プログラムを再起動します。
show port	ポートの Ring Protocol 使用状態を表示します。
show vlan	VLAN の Ring Protocol 使用状態を表示します。

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

show axrp コマンドで Ring Protocol の設定と運用状態を確認できます。コンフィグレーションコマンドで設定した Ring Protocol の設定内容が正しく反映されているかどうかを確認してください。リング単位の状態情報確認には show axrp <ring id list> コマンドを使用できます。

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。

show axrp コマンド，show axrp detail コマンドの表示例を次に示します。

図 20-5　show axrp コマンドの実行結果

```
> show axrp
Date 2009/01/27 12:00:00 UTC

Total Ring Counts:2

Ring ID:1
 Name:RING#1
 Oper State:enable           Mode:Master     Attribute:-

 VLAN Group ID  Ring Port  Role/State            Ring Port  Role/State
 1              0/1        primary/forwarding    0/2        secondary/blocking
 2              0/1        secondary/blocking    0/2        primary/forwarding

Ring ID:2
 Name:RING#2
 Oper State:enable           Mode:Transit    Attribute:-

 VLAN Group ID  Ring Port  Role/State            Ring Port  Role/State
 1              1(ChGr)    -/forwarding          2(ChGr)    -/forwarding
 2              1(ChGr)    -/forwarding          2(ChGr)    -/forwarding

>
```

show axrp detail コマンドを使用すると，統計情報やマスタノードのリング状態などについての詳細情報を確認できます。統計情報については，Ring Protocol 機能が有効（"Oper State" が "enable"）でない限り 0 を表示します。

図 20-6　show axrp detail のコマンド実行結果

```
> show axrp detail
Date 2009/01/27 12:00:00 UTC

Total Ring Counts:2

Ring ID:1
 Name:RING#1
 Oper State:enable           Mode:Master     Attribute:-
 Control VLAN ID:5           Ring State:normal
 Health Check Interval  (msec):1000
 Health Check Hold Time (msec):3000
 Flush Request Counts:3

 VLAN Group ID:1
  VLAN ID:6-10,12
  Ring Port:0/1         Role:primary      State:forwarding
  Ring Port:0/2         Role:secondary    State:blocking

 VLAN Group ID:2
  VLAN ID:16-20,22
  Ring Port:0/1         Role:secondary    State:blocking
  Ring Port:0/2         Role:primary      State:forwarding

Last Transition Time:2007/01/24 10:00:00
Fault Counts    Recovery Counts    Total Flush Request Counts
1               1                  12

Ring ID:2
 Name:RING#2
 Oper State:enable           Mode : Transit    Attribute : -
 Control VLAN ID:15
 Forwarding Shift Time (sec):10
 Last Forwarding:flush request receive

 VLAN Group ID:1
  VLAN ID  :26-30,32
  Ring Port:1(ChGr)     Role:-            State:forwarding
  Ring Port:2(ChGr)     Role:-            State:forwarding

 VLAN Group ID:2
  VLAN ID:36-40,42
  Ring Port:1(ChGr)     Role:-            State:forwarding
  Ring Port:2(ChGr)     Role:-            State:forwarding

>
```

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）

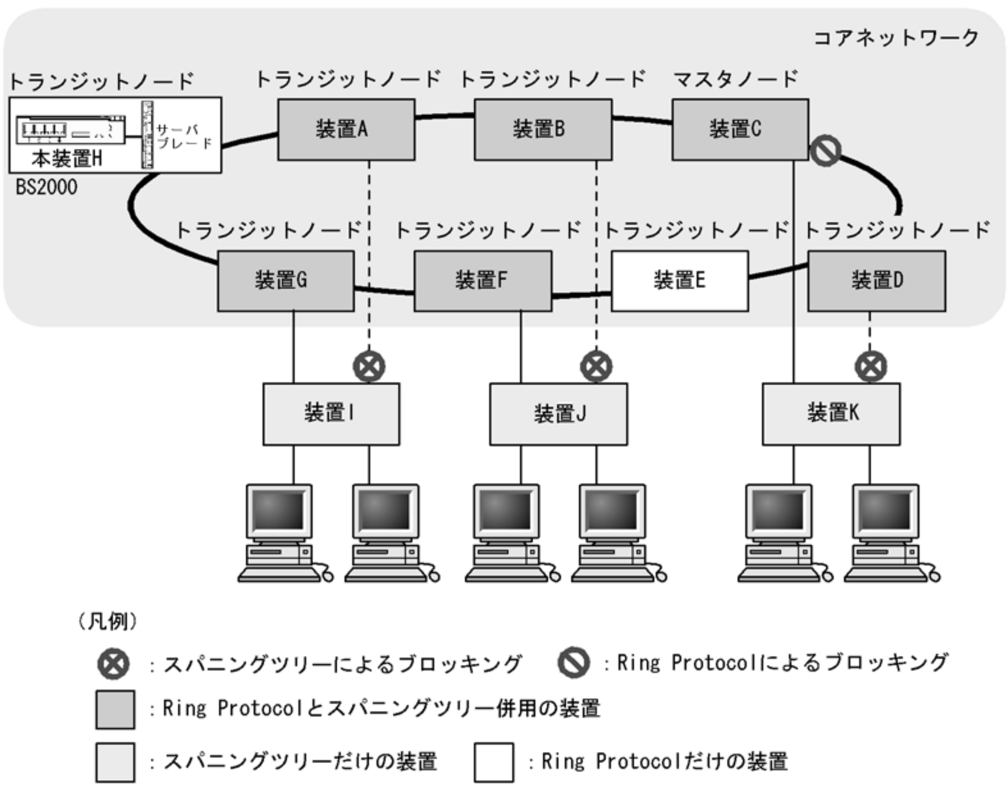
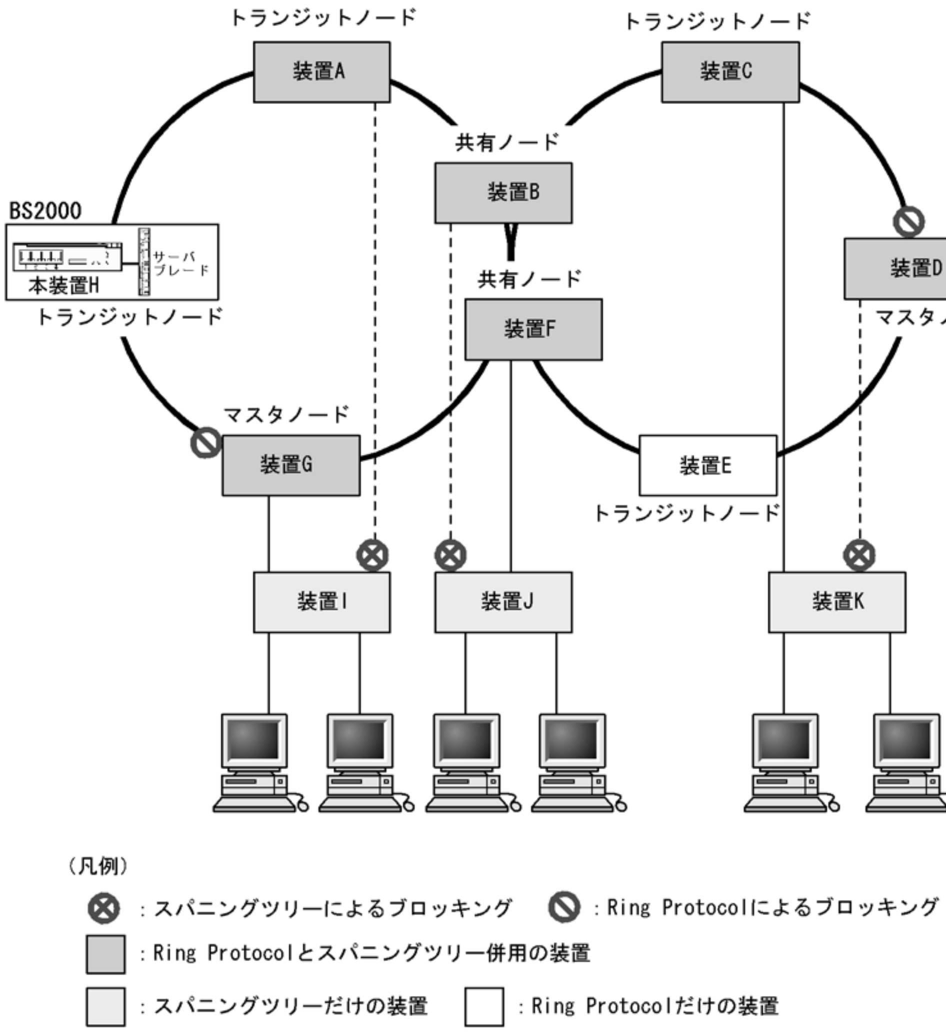


図 21-2　Ring Protocol とスパニングツリーの併用例（マルチリング構成）



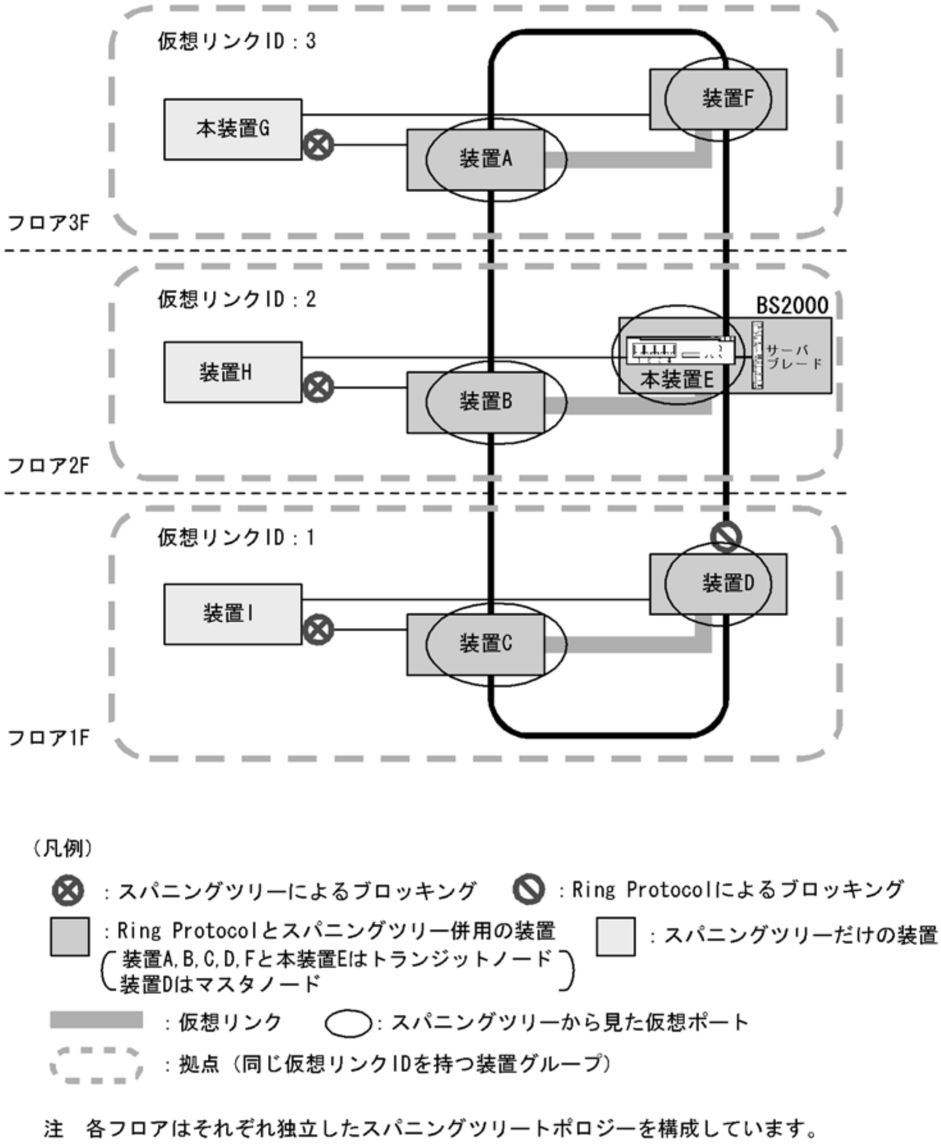
21.1.2　動作仕様

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



（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。したがって，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（固定）
リンクタイプ	spanning-tree link-type	point-to-point
ポート優先度	spanning-tree port-priority spanning-tree single port-priority spanning-tree vlan port-priority spanning-tree mst port-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）
- コンフィグレーションファイルのランニングコンフィグレーションへの反映
- restart vlan コマンド
- restart spanning-tree コマンド

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されません。したがって，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，本機能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値

設定項目	関連するコンフィグレーション	設定値
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

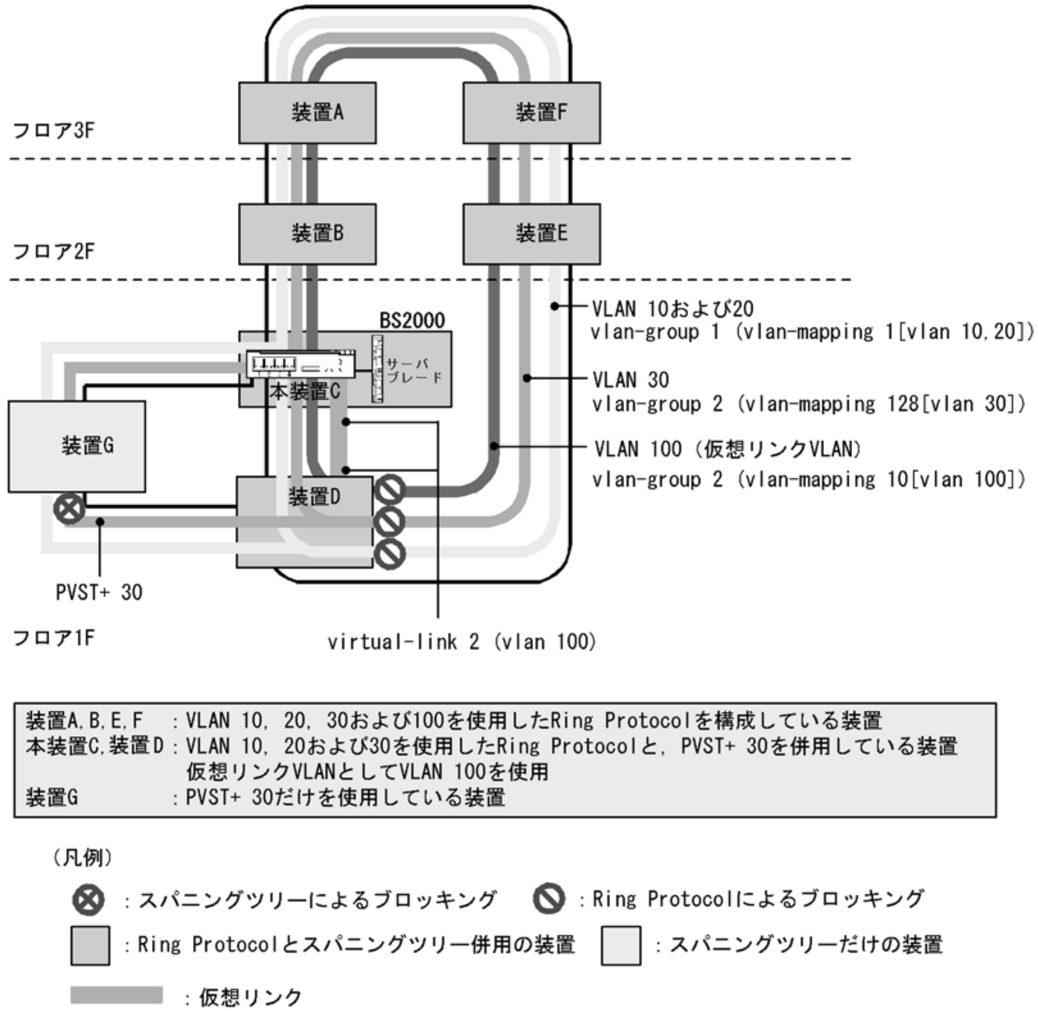
PVST+ は，Ring Protocol の VLAN マッピングに設定された VLAN が一つだけであれば，その VLAN で Ring Protocol と共存できます。コンフィグレーションコマンド axrp virtual-link で仮想リンクを設定すると，仮想リンクによるトポロジーを構築し Ring Protocol との共存を開始します。

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 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



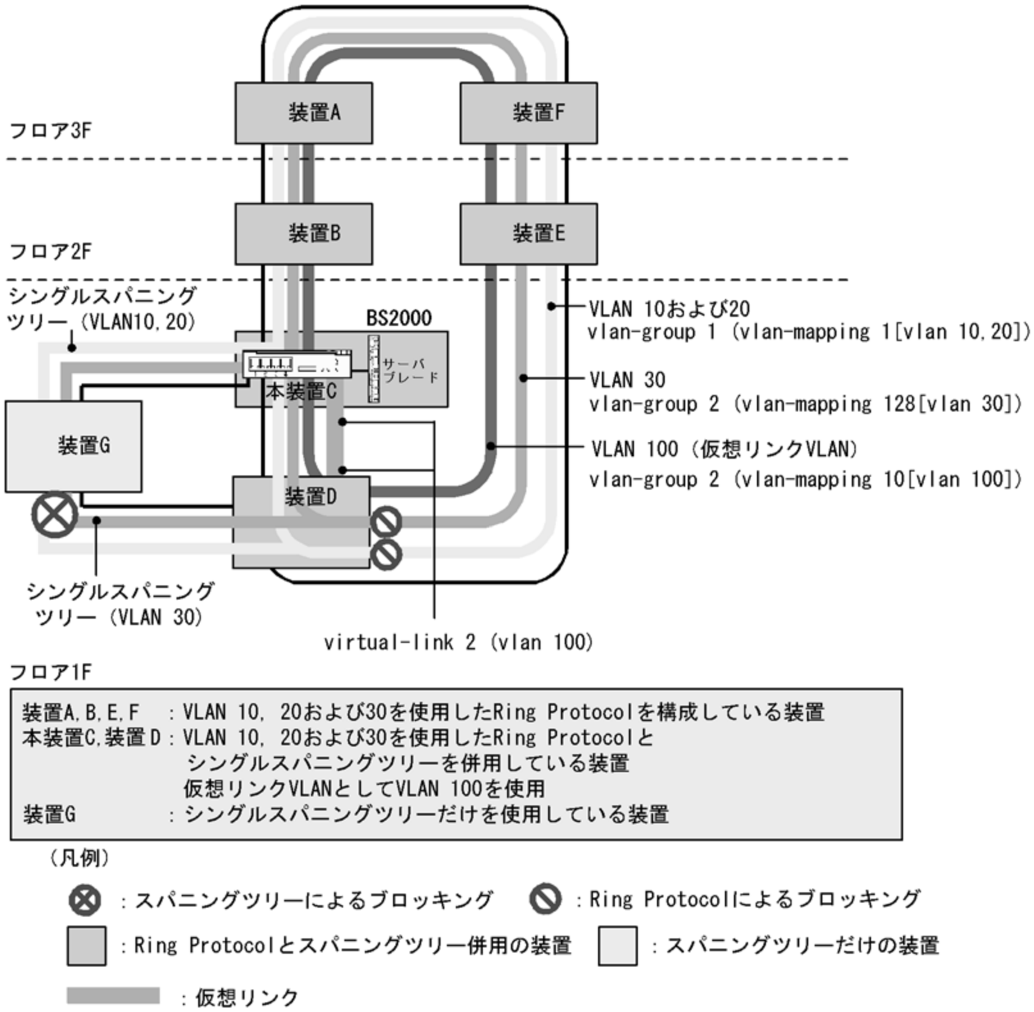
(2)　シングルスパニングツリーとの共存

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，本装置 C，装置 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，D，E，F，および本装置 C 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，本装置 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 21-5　シングルスパニングツリーと Ring Protocol の共存構成

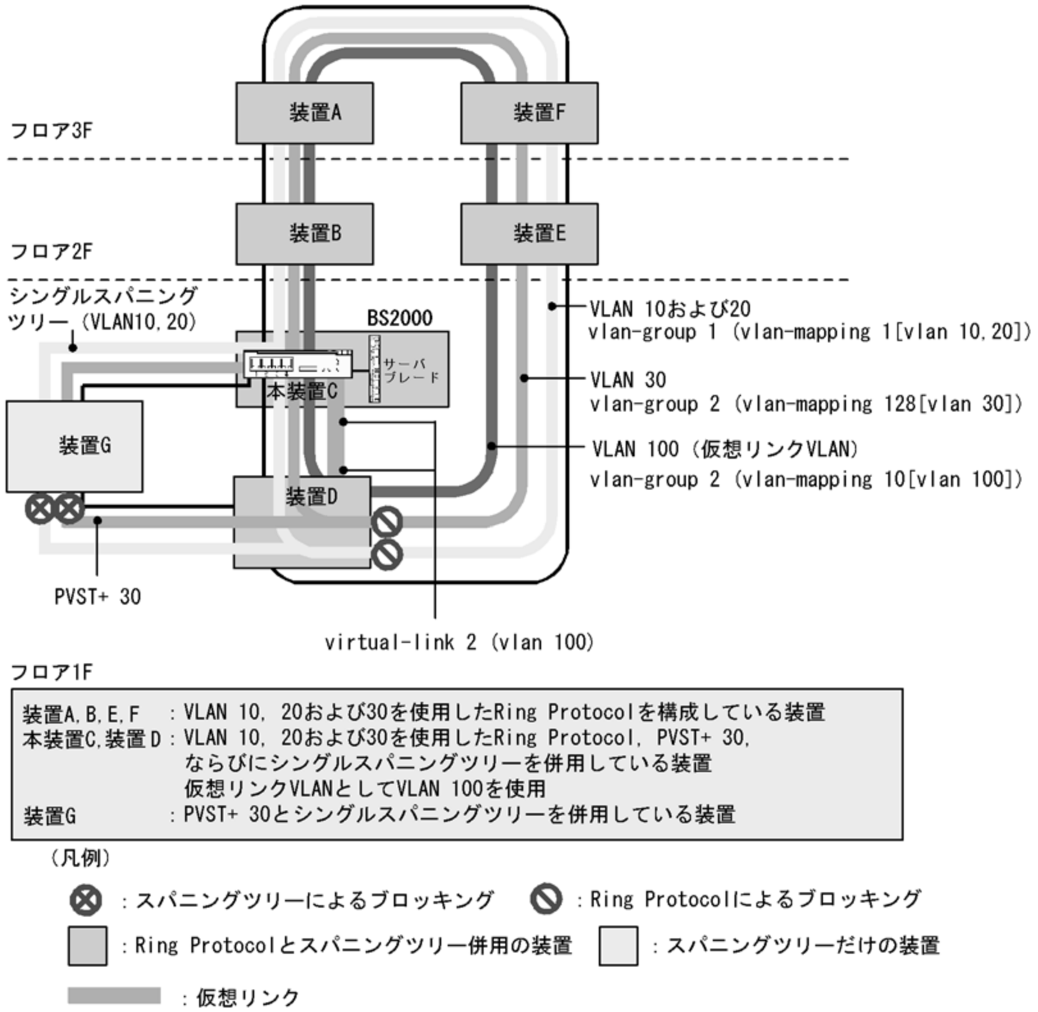


(3) PVST+ とシングルスパニングツリーの同時動作について

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

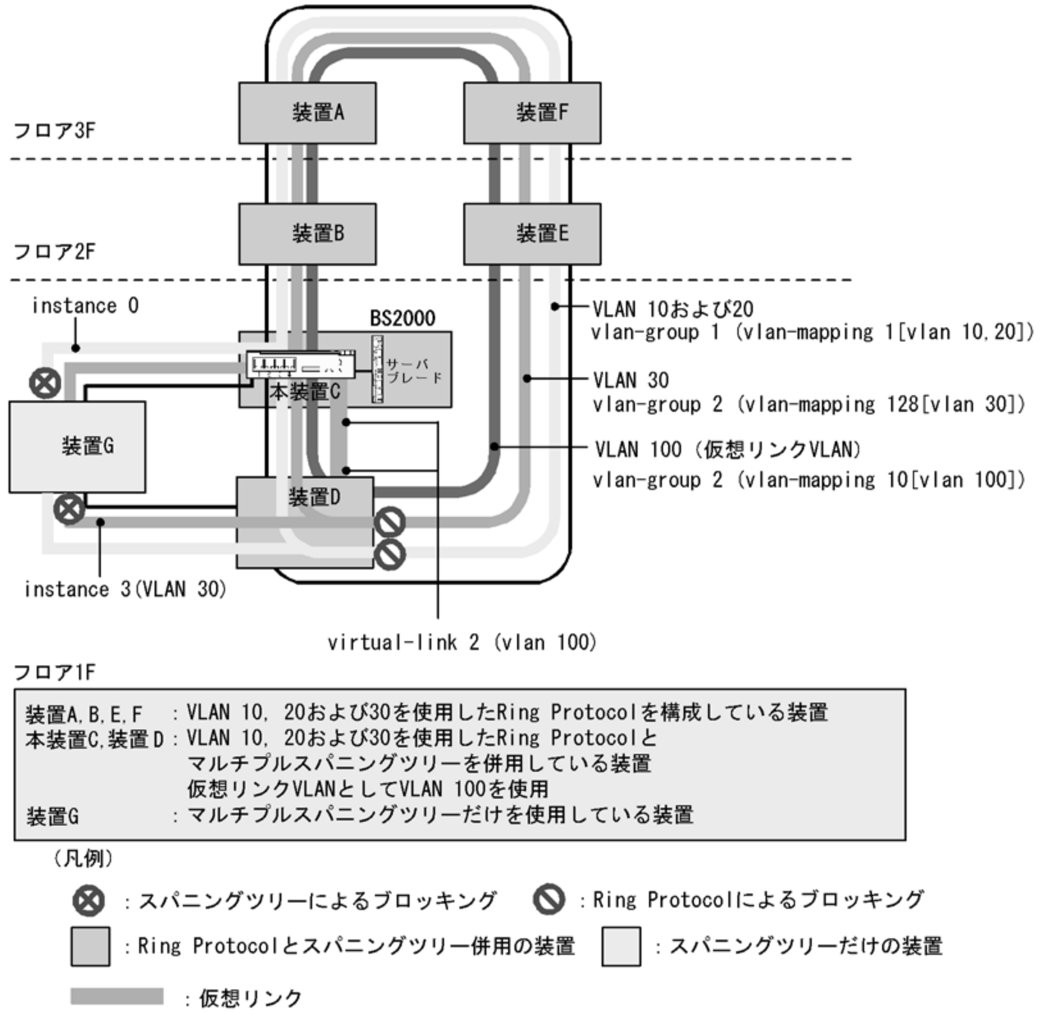
マルチプルスパニングツリーは Ring Protocol で運用するすべてのデータ転送用 VLAN と共存できます。

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，本装置 C，装置 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，D，E，F および本装置 C 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 は CIST，VLAN グループ 2 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，本装置 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 21-7　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

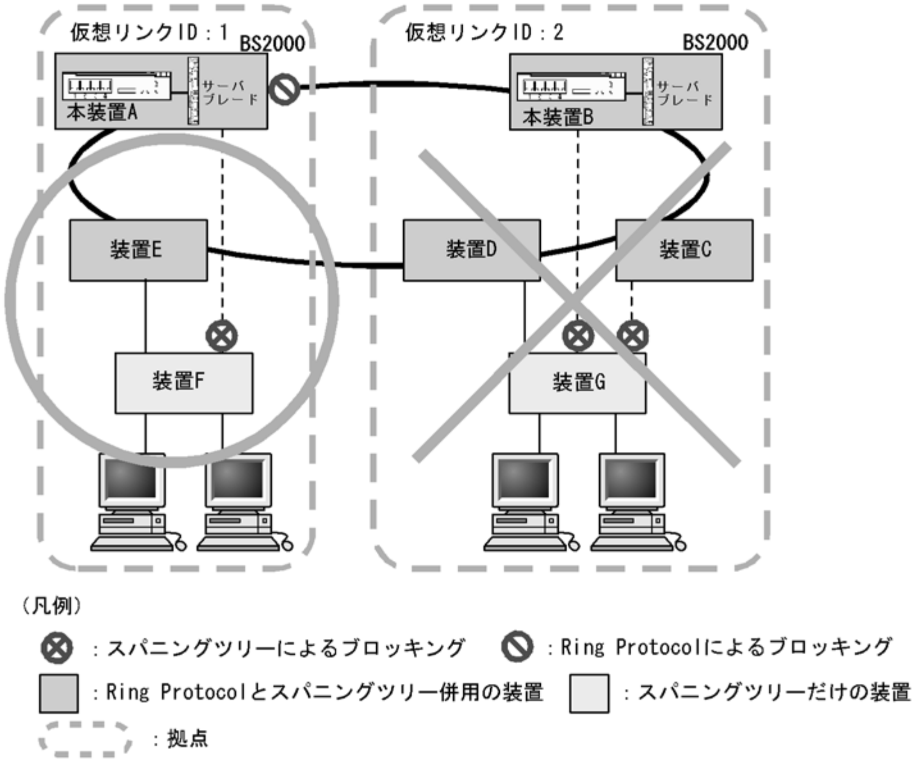
- Ring Protocol だけを適用させる VLAN
  PVST+ をコンフィグレーション設定などで停止させると，その VLAN は Ring Protocol だけが適用される VLAN となります。
  シングルスパニングツリー動作時，またはマルチプルスパニングツリー動作時，Ring Protocol が扱うデータ転送用 VLAN は必ず共存して動作します。
- PVST+ だけを適用させる VLAN
  Ring Protocol で VLAN グループに所属しない VLAN マッピングを設定すると，PVST+ だけが適用される VLAN となります。
- シングルスパニングツリ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。
- 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プログラム再起動時の対応について

Ring Protocol プログラムを再起動（運用コマンド restart axrp）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 か所以上の障害（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個所を復旧し，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 との併用ができます。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。

21.2.1　動作概要

Ring Protocol と GSRP が併用して動作している装置では，Ring Protocol の VLAN マッピングと GSRP の VLAN グループの VLAN 情報が一致している必要があります。この装置のリングポートは GSRP の制御対象外となり，リングポートのデータ転送状態は Ring Protocol で制御します。

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。

GSRP のダイレクトリンクは，リングネットワークと同じ回線を使用できます。また，別の回線にすることもできます。

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（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）

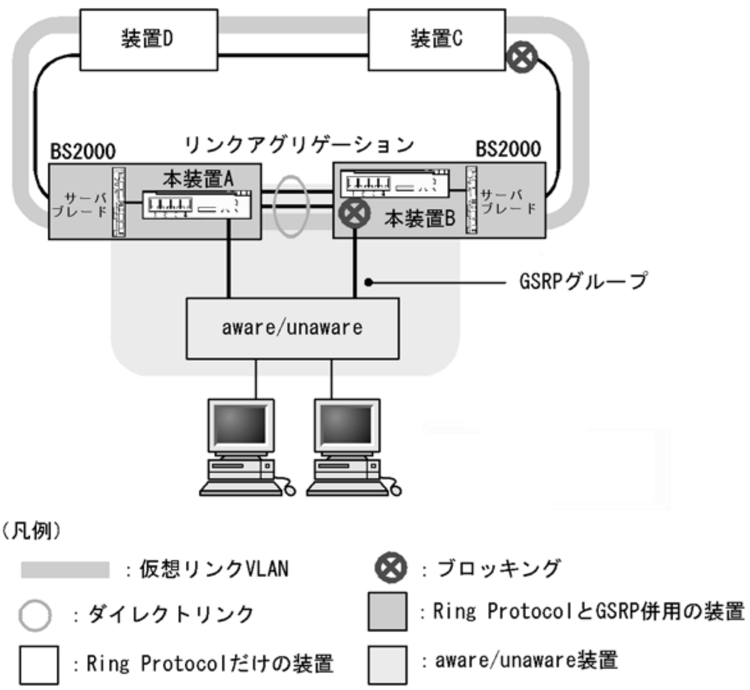
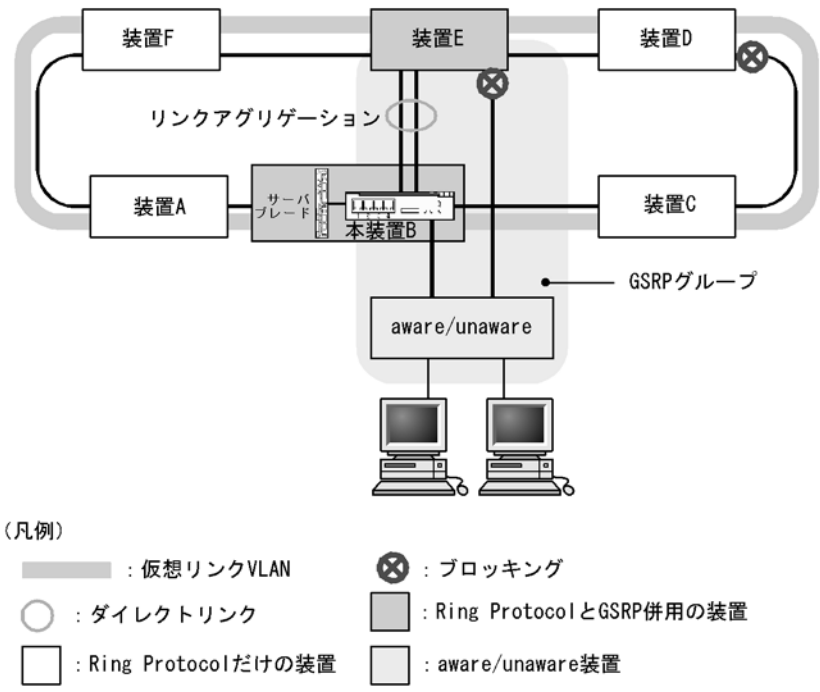


図 21-10　Ring Protocol と GSRP の併用例（ダイレクトリンクをリングネットワークで使用しない場合）



21.2.2　併用条件

Ring Protocol と GSRP の併用条件を示します。

（1） Ring Protocol と GSRP を併用動作させたい VLAN の設定条件

Ring Protocol の VLAN マッピングの VLAN と GSRP の VLAN グループの VLAN をすべて一致させてください。

（2） Ring Protocol または GSRP を単独で動作させたい VLAN の設定条件

すべての VLAN を共存動作させる必要はありません。VLAN 単位に別々のプロトコルを動作させる場合は，Ring Protocol の VLAN マッピングの VLAN と GSRP の VLAN グループの VLAN で一致する VLAN がないようにしてください。

21.2.3　リングポートの扱い

リングポートはコンフィグレーションコマンド gsrp exception-port の設定有無にかかわらず，GSRP の制御対象外ポートとして動作します。リングポートのデータ転送状態は Ring Protocol だけが制御します。

また，リングポートに次のコンフィグレーションコマンドを設定しても無効になります。

- gsrp reset-flush-port（ポートリセット機能を実施するポート）
- gsrp no-flush-port（GSRP Flush request フレームを送信しないポート）

21.2.4　Ring Protocol の制御 VLAN の扱い

Ring Protocol の制御 VLAN を GSRP の VLAN グループに設定した場合，該当する VLAN を VLAN グループの所属外にします。VLAN グループの所属外になった VLAN については，運用コマンド show gsrp

では表示されません。

21.2.5　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。この仮想リンク VLAN は，Ring Protocol のデータ転送用 VLAN グループに所属する必要があります。

GSRP のマスタが送信したフラッシュ制御フレームをリング構成装置が受信すると，MAC アドレステーブルをクリアします。また，送信回数は GSRP のコンフィグレーション（flush-request-count）に従います。

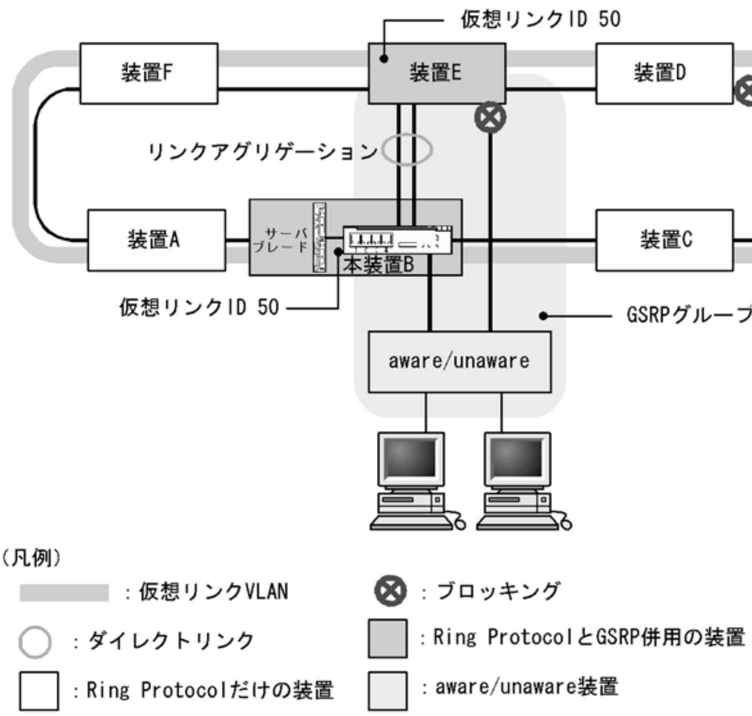
21.2.6　Ring Protocol と GSRP 併用動作時の注意事項

（1）仮想リンク VLAN の設定について

Ring Protocol と GSRP を併用する場合は，フラッシュ制御フレームを送信するために仮想リンク VLAN の設定が必要です。この仮想リンク VLAN は，Ring Protocol のデータ転送用 VLAN グループに所属する必要があります。

仮想リンク ID の設定を次の図に示します。仮想リンク ID には，同じ GSRP グループ装置で同一の仮想リンク ID を設定する必要があります。また，同じ仮想リンク VLAN が設定されているリングネットワーク内で一意となる値を設定する必要があります。同じ GSRP グループではない本装置 A，C，D，および F に仮想リンク ID 50 を設定すると，該当装置では，フラッシュ制御フレームによる MAC アドレステーブルのクリアができなくなります。

図 21-11　仮想リンク ID の設定



（2） Ring Protocol の VLAN マッピングまたは GSRP の VLAN グループの変更について

Ring Protocol と GSRP を併用する場合は，Ring Protocol の VLAN マッピングの VLAN と GSRP の VLAN グループの VLAN をすべて一致させる必要があります。しかし。コンフィグレーションの変更過程で一致しない状態になった場合，設定された VLAN の中で，ブロッキング状態となり，通信できない VLAN が発生するおそれがあります。

このため，Ring Protocol と GSRP を併用するためにコンフィグレーションを変更する場合は，GSRP のバックアップ装置で，priority コマンドや backup-lock コマンドなどの設定によって，マスタへの切り替えが発生しないようにしてから，変更する必要があります。

（3） 1VLAN グループ当たりに設定可能な VLAN 数について

Ring Protocol と併用している VLAN グループに 511 以上の VLAN 数を所属させると，該当する VLAN グループの状態が遷移したときにリングポートが一時的にブロッキング状態になります。

Ring Protocol と併用している VLAN グループに所属させる VLAN 数は 510 以下にしてください。

21.2.7　単独動作時の動作概要（レイヤ 3 冗長切替機能の適用例）

Ring Protocol と GSRP をそれぞれ異なる VLAN で単独動作させている場合は，レイヤ 3 冗長切替機能でリングネットワークと接続します。この場合の例を次の図に示します。下流ネットワーク（PC など）から本装置 A でレイヤ 3 中継し，VLAN 100 のリングネットワークを介して上流ネットワークと通信を行っています。このとき，本装置 A に障害が発生すると，下流ネットワークと上流ネットワークは本装置 B（ダイレクトリンク障害検出機能を設定時）でレイヤ 3 中継し，VLAN 200 のリングネットワークを介して通信を行います。

図 21-12　レイヤ 3 冗長切替機能（通常運用時）

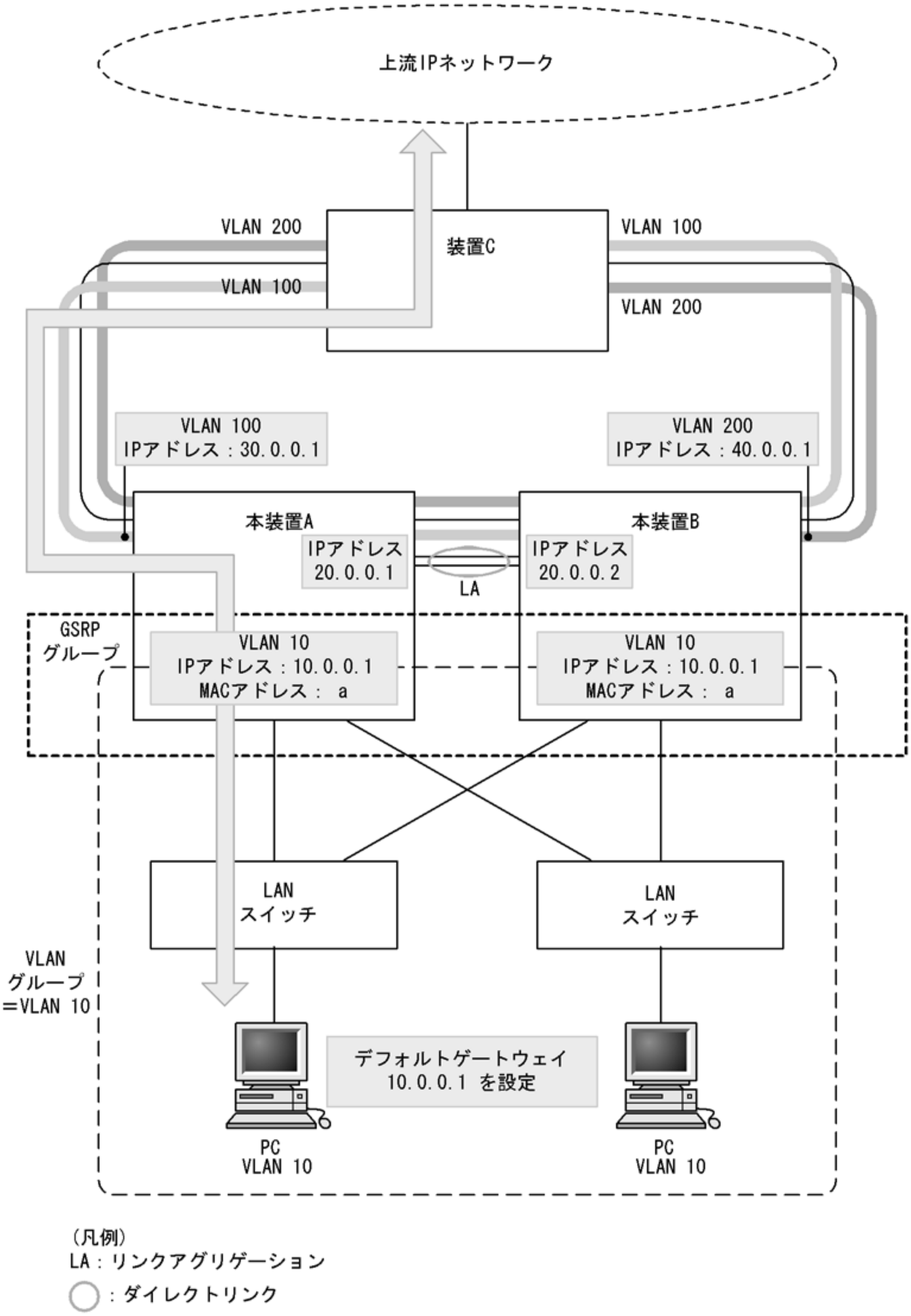
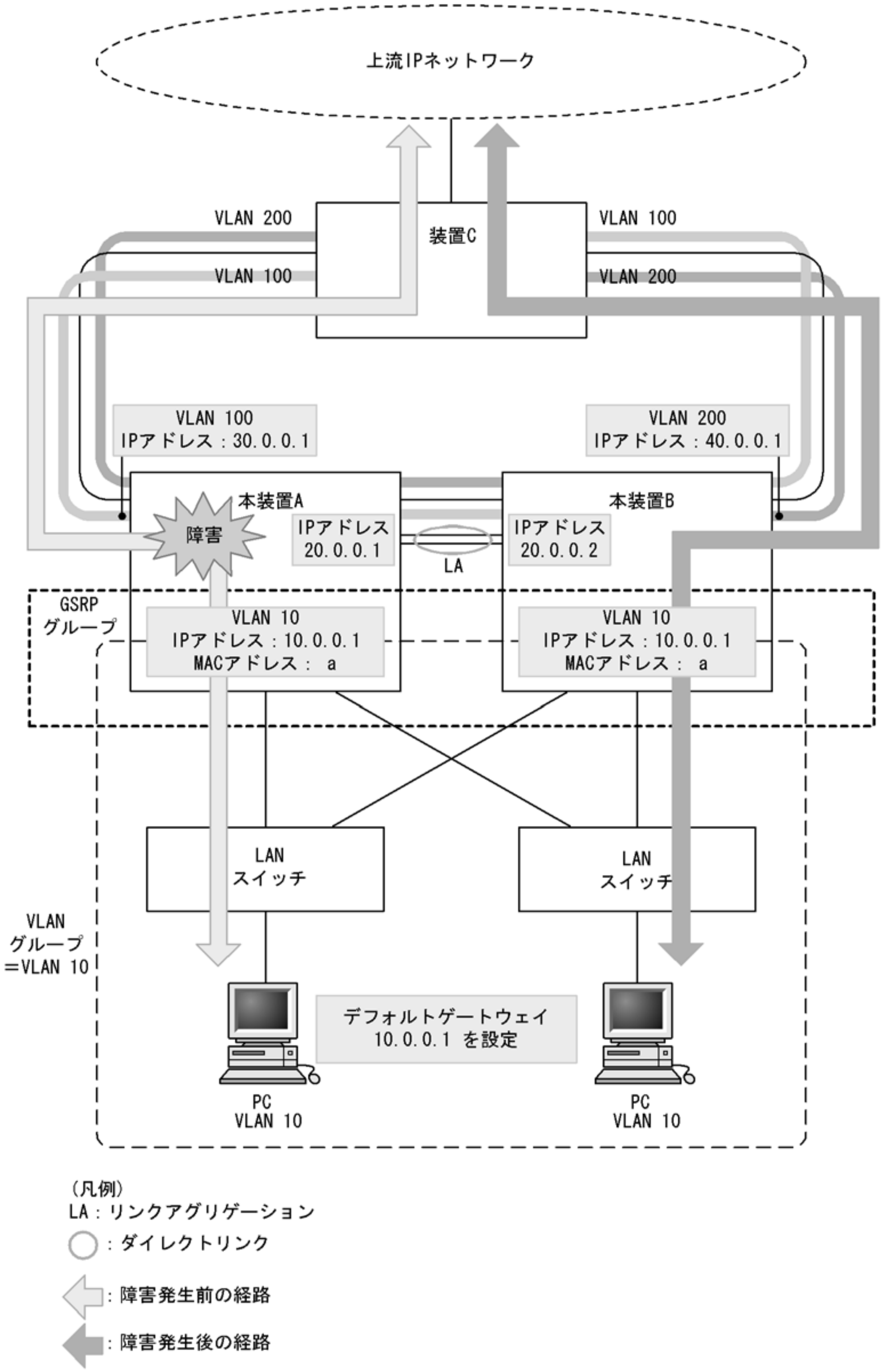


図 21-13　レイヤ 3 冗長切替機能（障害発生時）



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。また，Ring Protocol と GSRP を併用する場合は，フラッシュフレームを送信するために仮想リンク VLAN の設定が必要です。

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，または Ring Protocol と GSRP 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。

21.3.5　Ring Protocol と GSRP との併用設定

［設定のポイント］

Ring Protocol と GSRP とを併用する際には，併用したい VLAN ID を VLAN マッピングと GSRP の VLAN グループに設定する必要があります。この際，VLAN マッピング ID と GSRP の VLAN グループ ID は一致してい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 10,15**
   VLAN マッピング ID を 1 に，GSRP と併用する VLAN ID 10 および 15 を設定します。

2. **(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。

3. **(config)# gsrp 1**
   (config-gsrp)# vlan-group 3 vlan 10,15
   (config-gsrp)# exit
   GSRP の VLAN グループ 3 に Ring Protocol と併用する VLAN ID 10 および 15 を設定します。

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。
show gsrp	GSRP での仮想リンクの適用を表示します。

21.4.2 仮想リンクの状態の確認

仮想リンクの情報は show spanning-tree コマンド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。

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

図 21-14 show spanning-tree コマンドの実行結果

```
> show spanning-tree vlan 2
Date 2009/01/04 11:39:43 UTC
VLAN 2              PVST+ Spanning Tree:Enabled  Mode:PVST+
  Bridge ID        Priority:4096      MAC Address:0012.e205.0900
    Bridge Status:Designated
  Root Bridge ID   Priority:0         MAC Address:0012.e201.0900
    Root Cost:0
    Root Port:0/2-3(VL:10)                          … 1
  Port Information
    0/1     Up     Status:Forwarding  Role:Designated
    VL(10)  Up     Status:Forwarding  Role:Root      … 1
>
```

1. VL は，仮想リンク ID を示しています。

show gsrp detail コマンドで仮想リンクが運用されているか確認できます。Virtual Link ID で仮想リンク ID と仮想リンク VLAN を確認してください。

図 21-15　show gsrp detail コマンドの実行結果

```
>show gsrp detail
Date 2009/01/10 12:00:00 UTC

GSRP ID: 3
 Local MAC Address       : 0012.e2a8.2527
 Neighbor MAC Address    : 0012.e2a8.2505
 Total VLAN Group Counts : 3
 GSRP VLAN ID            : 105
 Direct Port             : 0/1-2
 GSRP Exception Port     : 0/3-4
 No Neighbor To Master   : manual
 Backup Lock             : disable
 Port Up Delay           : 0
 Last Flush Receive Time : -
 Layer 3 Redundancy      : On
 Virtual Link ID         : 100(VLAN ID : 20)

                         Local               Neighbor
 Advertise Hold Time     : 5                   5
 Advertise Hold Timer    : 4                   -
 Advertise Interval      : 1                   1
 Selection Pattern       : ports-priority-mac  ports-priority-mac

 VLAN Group ID      Local State         Neighbor State
 1                  Backup              Master
 2                  (disable)           -
 8                  Master              -
>
```

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。

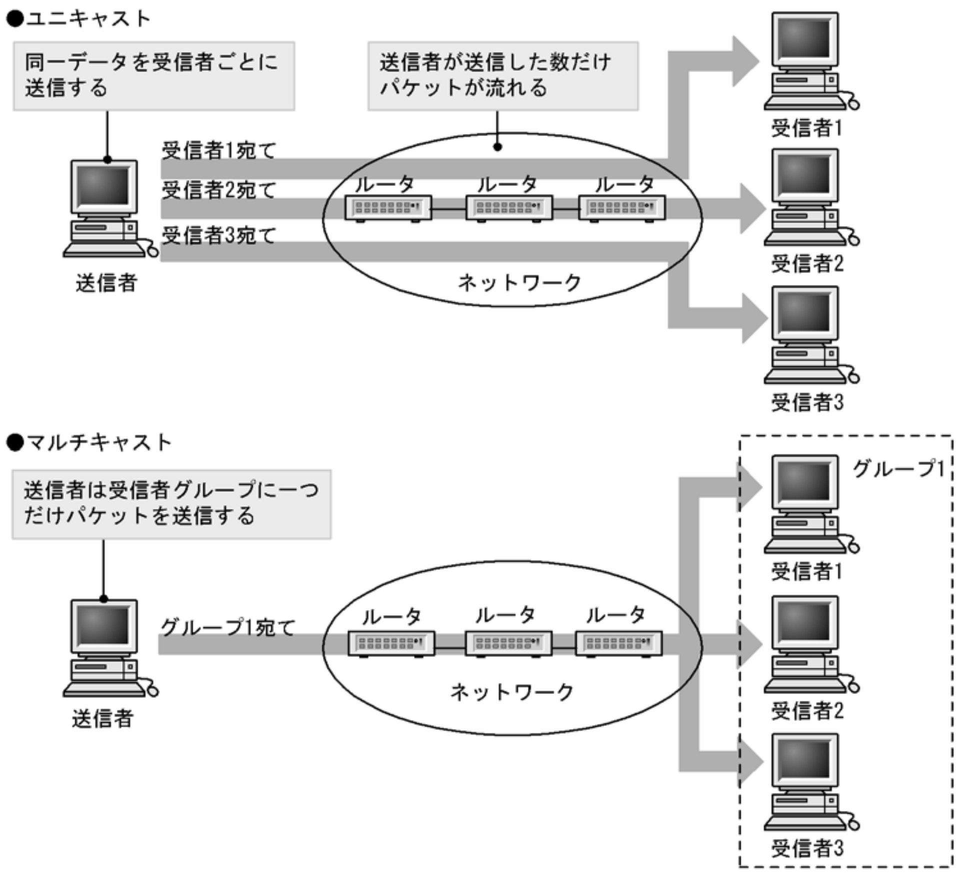
22.1 IGMP snooping/MLD snooping の概要

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

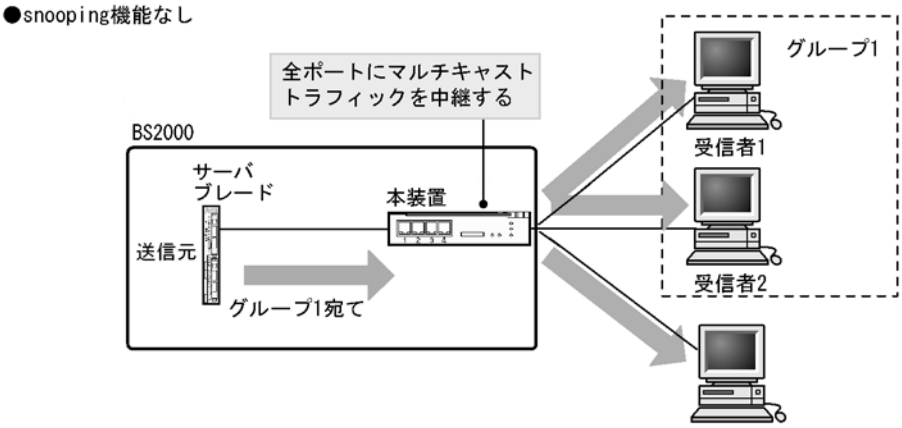
プロトコル	アドレス範囲
IPv4	224.0.0.0 ～ 239.255.255.255
IPv6	上位 8 ビットが ff(16 進数）となる IPv6 アドレス

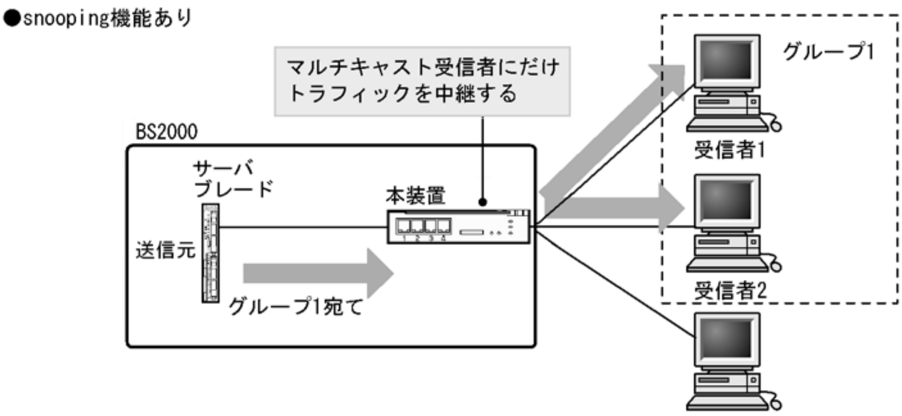
22.1.2　IGMP snooping および MLD snooping 概要

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※1	IPv4	0100.5e00.0000 ～ 0100.5eff.ffff	RFC1112 を参照
	IPv6	3333.0000.0000 ～ 3333.ffff.ffff	RFC2464 を参照
この機能による学習 IP アドレス範囲※2	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	－
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	－

（凡例）　－：該当なし

注※ 1　IPv4/IPv6 マルチキャストを同時に使用しない場合

注※ 2　IPv4/IPv6 マルチキャストを同時に使用する場合

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 IPv4 マルチキャストまたは IPv6 マルチキャストと同時に使用しない場合，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。IPv4 マルチキャストまたは IPv6 マルチキャストと同時にする場合は，IP 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

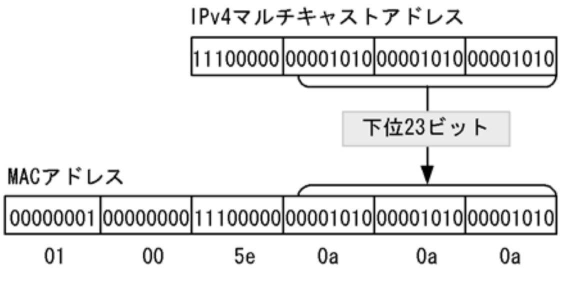
IGMP snooping が設定された VLAN で IGMP メッセージを受信することによってマルチキャスト MAC アドレスをダイナミックに学習します。学習したマルチキャスト MAC アドレスは MAC アドレステーブルに登録します。

（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 アドレス宛てのパケットとして取り扱います。IPv4 マルチキャストアドレスと MAC アドレスの対応を次の図に示します。

図 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。

- IGMPv2 Leave メッセージを受信した場合
  IGMPv2 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。

- 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。
- 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，デフォルト値となります。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 の結果によるレイヤ 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 宛て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 IP アドレス制御方式

本装置では swrt_multicast_table コマンドを設定することによって，IPv4 マルチキャストと IGMP snooping の両方を同一の VLAN 上で同時に使用できます。IPv4 マルチキャストと IGMP snooping を同時に使用する場合，該当する VLAN に必ず IPv4 マルチキャストを使用してください。

（1） IP 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 IP 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 IP アドレスの情報は IPv4 マルチキャスト

のマルチキャスト中継エントリに設定します。

(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 IP 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。

(b) エントリの削除

学習したマルチキャスト IP アドレスは次のどれかの場合に，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。

- IGMPv2 Leave メッセージを受信した場合
  IGMPv2 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，本装置が代表クエリアのときだけです)。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。
- IGMPv3 Report（離脱要求）メッセージを受信した場合
  IGMPv3 Report（離脱要求）メッセージでマルチキャストアドレスレコードタイプが CHANGE_TO_INCLUDE_MODE の IGMPv3 Report（離脱要求）メッセージを受信した場合，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，本装置が代表クエリアのときだけです)。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。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，本装置から Group-and-Source-Specific Query メッセージを 1 秒間隔で 2 回送信します（Group-and-Source-Specific Query メッセージの送信は，本装置が代表クエリアのときだけです)。Group-Source-and-Specific Query メッセージの応答に関わらず，エントリはタイムアウトで削除処理を行います。

  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。
- 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，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 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，デフォルト値となります。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 IP アドレスベースで処理します。IGMP snooping の結果によるレイヤ 2 中継は，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。

（3） IPv4 マルチキャストパケットのレイヤ 3 中継

IPv4 マルチキャストによる VLAN 間のレイヤ 3 中継時に，中継先の VLAN で IGMP snooping が動作している場合，レイヤ 3 中継されたマルチキャストトラフィックは，中継先の VLAN 内で IGMP snooping の学習結果に従って中継されます。

（4） IPv4 マルチキャスト同時使用時の Specific Query 送信

IPv4 マルチキャストが動作することで本装置が VLAN 内の代表クエリアである場合，IGMP Leave メッセージまたは IGMPv3 Report（離脱要求）メッセージ受信による Group-Specific Query または Group-and-Source-Specific Query の送信は，受信ポートだけでなく VLAN 内の全ポートに送信します。

22.3.3 マルチキャストルータとの接続

マルチキャストパケットの中継先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 IGMPv2 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 IGMPv2 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。

22.3.4　IGMP クエリア機能

IGMP クエリア機能は，VLAN 内にマルチキャストルータが存在せず，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。

22.4 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 フレーム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 IPv6 マルチキャストと同時に使用しない場合，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。IPv6 マルチキャストと同時にする場合は，IP 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

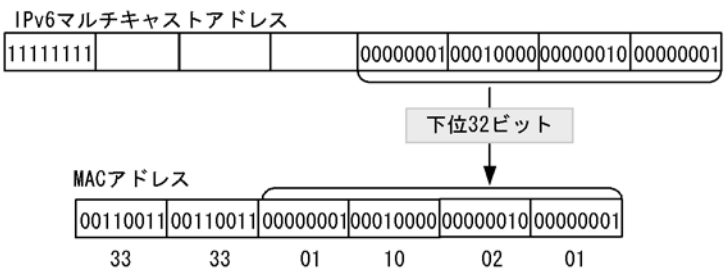
MLD snooping が設定された VLAN で MLD メッセージを受信することによってマルチキャスト MAC アドレスをダイナミックに学習します。学習したマルチキャスト MAC アドレスは MAC アドレステーブルに登録します。

（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て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 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。
- 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 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。
  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。MLDv2 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 MLDv2 Query メッセージ（QQIC フィールド）から算出します。自装置が代表クエリアの場合または MLDv1 で運用している場合は，デフォルト値となります。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） 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 IP アドレス制御方式

本装置では swrt_multicast_table コマンドを設定することによって，IPv6 マルチキャストと MLD snooping の両方を同一の VLAN 上で同時に使用できます。IPv6 マルチキャストと MLD snooping を同時に使用する場合，該当する VLAN に必ず IPv6 マルチキャストを使用してください。

（1） IP 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 IP 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 IP アドレスの情報は IPv6 マルチキャストのマルチキャスト中継エントリに設定します。

(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 IP 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てのトラフィックを転送するエントリを作成します。

(b) エントリの削除

学習したマルチキャスト IP アドレスは次のどれかの場合に，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。

- 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，本装置が代表クエリアのときだけです）。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）メッセージでマルチキャストアドレスレコードタイプが CHANGE_TO_INCLUDE_MODE の MLDv2 Report（離脱要求）メッセージを受信した場合，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，本装置が代表クエリアのときだけです）。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。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。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 メッセージを受信した場合は，本装置から Group-and-Source-Specific Query メッセージを 1 秒間隔で 2 回送信します（Group-and-Source-Specific Query メッセージの送信は，本装置が代表クエリアの時だけです）。Group-and-Source-Specific Query メッセージの応答に関わらず，エントリはタイムアウトで削除処理を行います。

  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。
- 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。
  タイムアウト時間は次に示す場合に，動的に設定します。
  - 他装置が代表クエリア（MLDv2 での運用）
    代表クエリアからの MLDv2 Query メッセージ（QQIC フィールド）から算出します。
  - 自装置が代表クエリア
    MLDv1/MLDv2 にかかわらず，自装置に設定した Query Interval で算出します（ただし，Query Interval を設定していなければ，デフォルト値での運用となります）。
  - 他装置が代表クエリア（MLDv1 での運用）
    自装置に設定した Query Interval で算出します（ただし，Query Interval を設定していなければデ

フォルト値での運用となります)。

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) 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 IP 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，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。

(3) IPv6 マルチキャストパケットのレイヤ 3 中継

IPv6 マルチキャストによる VLAN 間のレイヤ 3 中継時に，中継先の VLAN で MLD snooping が動作している場合，レイヤ 3 中継されたマルチキャストトラフィックは，中継先の VLAN 内で MLD snooping の学習結果に従って中継されます。

(4) IPv6 マルチキャスト同時使用時の Specific Query 送信

IPv6 マルチキャストが動作することで本装置が VLAN 内の代表クエリアである場合，MLD Done メッセージまたは MLDv2 Report（離脱要求）メッセージ受信による Group-Specific Query または Group-and-Source-Specific Query の送信は，受信ポートだけでなく VLAN 内の全ポートに送信します。

22.4.3 マルチキャストルータとの接続

マルチキャストパケットの中継先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

<table>
<tr><th colspan="2">MLDv2 メッセージの種類</th><th>VLAN 内転送ポート</th><th>備考</th></tr>
<tr><td colspan="2">Version2 Multicast Listener Query</td><td>全ポートへ中継します。</td><td></td></tr>
<tr><td rowspan="2">Version2 Multicast Listener Report</td><td>加入要求の Report</td><td>マルチキャストルータポートにだけ中継します。</td><td></td></tr>
<tr><td>離脱要求の Report</td><td>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。</td><td>※</td></tr>
</table>

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。

22.4.4　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 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

「15.3　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，IGMP snooping/MLD snooping 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

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。

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，次のどちらかの対応が必要です。

- 該当する VLAN に IPv4 マルチキャストを使用して，IGMP バージョンを 3 に設定してください。
- IGMPv3 ルータを接続して該当するルータが代表クエリアになるように IP アドレスを設定してください。

（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，次のどちらかの対応が必要です。

- 該当する VLAN に IPv6 マルチキャストを使用して，MLD バージョンを 2 に設定してください。
- MLDv2 ルータを接続して該当するルータが代表クエリアになるように IP アドレスを設定してくだ

さい。

(6) 運用コマンド実行によるエントリの再学習

IGMP/MLD snooping の運用コマンドのほかに，下記のコマンドを実行した場合，それまでに学習したエントリをクリアし，再学習を行います。運用コマンド実行後は，一時的にマルチキャスト通信が中断します。

- copy コマンドで running-config に上書きした場合
- restart vlan コマンド

(7) IPv4 マルチキャスト機能との同時使用

(a) IGMP snooping 設定追加時の一時的通信停止

IPv4 マルチキャストを使用している VLAN に IGMP snooping を追加設定した場合，一時的にマルチキャスト通信が停止します。IGMP snooping 設定後，IGMP Report（加入要求）を受信することでマルチキャスト通信が再開します。

(b) 静的グループ参加機能との併用

IPv4 マルチキャストの静的グループ参加機能を使用している VLAN では，ホストから IGMP Report（加入要求）が送信されないおそれがあります。IGMP snooping と同時使用する場合，IGMP Report（加入要求）が送信されないとマルチキャスト通信ができないため，静的グループ参加機能を使用している VLAN でマルチキャスト通信が必要なポートにはマルチキャストルータポートを設定してください。

(8) IPv6 マルチキャスト機能との同時使用

(a) MLD snooping 設定追加時の一時的通信停止

IPv6 マルチキャストを使用している VLAN に MLD snooping を追加設定した場合，一時的にマルチキャスト通信が停止します。MLD snooping 設定後，MLD Report（加入要求）を受信することでマルチキャスト通信が再開します。

(b) 静的グループ参加機能との併用

IPv6 マルチキャストの静的グループ参加機能を使用している VLAN では，ホストから MLD Report（加入要求）が送信されないおそれがあります。MLD snooping と同時使用する場合，MLD Report（加入要求）が送信されないとマルチキャスト通信ができないため，静的グループ参加機能を使用している VLAN でマルチキャスト通信が必要なポートにはマルチキャストルータポートを設定してください。

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	IGMP snooping 機能を使用することを設定します。
ip igmp snooping mrouter interface	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。
no ip igmp snooping	IGMP snooping 機能の抑止を設定します。

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
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-if)# ip igmp snooping querier**
IGMP クエリア機能を有効にします。

［注意事項］

本設定は該当インタフェースに 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 0/1 のギガビット・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-if)# ip igmp snooping mrouter interface gigabitethernet 0/1**
   (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。

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 情報をクリアします。
restart snooping	snooping プログラムを再起動します。
dump protocols snooping	イベントトレース情報および制御テーブル情報のファイルを出力します。

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

show igmp-snooping コマンドを実行し，IGMP snooping に関する設定が正しいことを確認してください。

図 23-1　IGMP snooping の設定状態表示

```
> show igmp-snooping 100
Date 2009/01/11 15:20:00 UTC
VLAN: 100
  IP address: 192.168.11.20/24    Querier: enable
  IGMP querying system: 192.168.11.20
  Querier version: V2
  IPv4 Multicast routing: Off
  Port(4): 0/1-4
  Mrouter-port: 0/1
  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，show igmp-snooping group コマンドで確認してください。

図 23-2　show igmp-snooping group コマンドの実行結果

```
> show igmp-snooping group 100
Date 2009/01/11 15:20:00 UTC
VLAN counts: 1
VLAN: 100  Group counts: 3  IPv4 Multicast routing: Off
  Group Address     MAC Address         Version         Mode
  224.10.10.10      0100.5e0a.0a0a      V2              -
    Port-list:0/1-3
  225.10.10.10      0100.5e0a.0a0a      V3              INCLUDE
    Port-list:0/1-2
  239.192.1.1       0100.5e40.0101      V2,V3           EXCLUDE
    Port-list:0/1
```

- ポートごとの参加グループ表示例を show igmp-snooping port コマンドで確認してください。

図 23-3　show igmp-snooping port コマンドの実行結果

```
> show igmp-snooping port 0/1
Date 2009/01/11 15:20:00 UTC
Port 0/1  VLAN counts: 2
  VLAN: 100  Group counts: 2
    Group Address     Last Reporter      Uptime     Expires
    224.10.10.10      192.168.1.3        00:10      04:10
    239.192.1.1       192.168.1.3        02:10      03:00
  VLAN: 150  Group counts: 1
    Group Address     Last Reporter      Uptime     Expires
    239.10.120.1      192.168.15.10      01:10      02:30
```

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	MLD snooping 機能を使用することを設定します。
ipv6 mld snooping mrouter interface	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。
no ipv6 mld snooping	MLD snooping 機能の抑止を設定します。

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
   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-if)# ipv6 mld snooping querier**
   MLD クエリア機能を有効にします。

［注意事項］

本設定は該当インタフェースに IPv6 アドレスの設定がないと有効となりません。

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 0/1 のギガビット・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-if)# ipv6 mld snooping mrouter interface gigabitethernet 0/1**
   (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。

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 情報をクリアします。
restart snooping	snooping プログラムを再起動します。
dump protocols snooping	イベントトレース情報および制御テーブル情報のファイルを出力します。

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

show mld-snooping コマンドを実行し，MLD snooping に関する設定が正しいことを確認してください。

図 23-4　MLD snooping の設定状態表示

```
> show mld-snooping 100
Date 2009/01/11 15:20:00 UTC
VLAN: 100
  IP address: fe80::b1    Querier: enable
  MLD querying system: fe80::b1
  Querier version: V1
  IPv6 Multicast routing: Off
  Querier version: V2
  Port(4): 0/1-4
  Mrouter-port: 0/1
  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，show mld-snooping group コマンドで確認してください。

図 23-5　show mld-snooping group コマンドの実行結果

```
> show mld-snooping group 100
Date 2009/01/11 15:20:00 UTC
VLAN: counts: 1
VLAN: 100  Group counts: 2  IPv6 Multicast routing: Off
  Group Address     MAC Address        Version      Mode
  ff35::1           3333:0000:0001     V1,V2        EXCLUDE
    Port-list:0/1-3
  ff35::2           3333:0000:0002     V2           EXCLUDE
    Port-list:0/1-2
```

● ポートごとの参加グループ表示例を show mld-snooping port コマンドで確認してください。

図 23-6　show mld-snooping port コマンドの実行結果

```
> show mld-snooping port 0/1
Date 2009/01/11 15:20:00 UTC
Port  0/1  VLAN counts: 1
  VLAN: 100  Group counts: 2
    Group Address      Last Reporter      Uptime     Expires
    ff35::1            fe80::b2           00:10      04:10
    ff35::2            fe80::b3           02:10      03:00
```

付録

付録 A　準拠規格

付録 A.1　RADIUS/TACACS+

表 A-1　RADIUS/TACACS+ の準拠する規格および勧告

規格番号 (発行年月)	規格名
RFC 2865(2000 年 6 月)	Remote Authentication Dial In User Service(RADIUS)
RFC 2866(2000 年 6 月)	RADIUS Accounting
RFC 3162(2001 年 8 月)	RADIUS and IPv6
draft-grant-tacacs-02.txt (1997 年 1 月)	The TACACS+ Protocol Version 1.78

付録 A.2　NTP

表 A-2　NTP の準拠する規格および勧告

規格番号 (発行年月)	規格名
RFC 1305(1992 年 3 月)	Network Time Protocol (Version 3) Specification, Implementation and Analysis

付録 A.3　DNS

表 A-3　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
RFC 1034(1987 年 3 月)	Domain names - concepts and facilities
RFC 1035(1987 年 3 月)	Domain names - implementation and specification

付録 A.4　イーサネット

表 A-4　イーサネットインタフェースの準拠規格

種別	規格	名称
10BASE-T, 100BASE-TX, 1000BASE-T, 1000BASE-X, 10GBASE-R	IEEE802.3x-1997	IEEE Standards for Local and Metropolitan Area Networks:Specification for 802.3 Full Duplex Operation
	IEEE802.2 1998 Edition	IEEE Standard for Information Technology - Telecommunications andInformation Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 2: Logical Link Control
	IEEE802.3 2000 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
10GBASE-R	IEEE802.3ae Standard-2002	Media Access Control(MAC) Parameters, Physical Layer, and Management Parameters for 10Gb/s Operation

種別	規格	名称
PoE	IEEE802.3af	Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment: Data Terminal Equipment (DTE)Power via Media Dependent Interface (MDI)

付録 A.5　リンクアグリゲーション

表 A-5　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.6　VLAN

表 A-6　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.7　スパニングツリー

表 A-7　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.8　IGMP snooping/MLD snooping

表 A-8　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
RFC 4541(2006 年 5 月)	Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

付録 B　謝辞 (Acknowledgments)

[SNMP]

****

Copyright 1988-1996 by Carnegie Mellon University
All Rights Reserved

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

****

Some of this software has been modified by BBN Corporation and is a derivative of software developed by Carnegie Mellon University. Use of the software remains subject to the original conditions set forth above.

****

Some of this software is Copyright 1989 by TGV, Incorporated but subject to the original conditions set forth above.

****

Some of this software is Copyright (C) 1983,1988 Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of California at Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided "as is" without express or implied warranty.

****

* Primary Author:
Steve Waldbusser

* Additional Contributors:
Erik Schoenfelder (schoenfr@ibr.cs.tu-bs.de): additions, fixes and enhancements for Linux by 1994/1995.
David Waitzman: Reorganization in 1996.

Wes Hardaker <hardaker@ece.ucdavis.edu>: Some bug fixes in his UC
Davis CMU SNMP distribution were adopted by David Waitzman

David Thaler <thalerd@eecs.umich.edu>: Some of the code for making the agent embeddable into another application were adopted by David Waitzman

Many more over the years...

[NTP]

[PIM sparse-mode pimd]

```
/*
 * Part of this program has been derived from mrouted.
 * The mrouted program is covered by the license in the accompanying file
 * named "LICENSE.mrouted".
 *
 * The mrouted program is COPYRIGHT 1989 by The Board of Trustees of
 * Leland Stanford Junior University.
 *
 */
```

[pim6dd]

```
/*
 * Copyright (C) 1998 WIDE Project.
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. Neither the name of the project nor the names of its contributors
 *    may be used to endorse or promote products derived from this software
 *    without specific prior written permission.
 *
 * THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 */
```

[pim6sd]

```
/*
 * Copyright (C) 1999 LSIIT Laboratory.
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
```

[RADIUS]

[totd]

WIDE

University of Tromso

make and grant him and/or the University the rights to redistribute these changes without restrictions.

Invenia Innovation A.S.

Copyright (C) Invenia Innovation A.S., Norway. All rights reserved.

Author: Feike W. Dillema, Invenia Innovation A.S., Norway.

Permission to use, copy, modify and distribute this software and its documentation is hereby granted, provided that both the copyright notice and this permission notice appear in all copies of the software, derivative works or modified versions, and any portions thereof, and that both notices appear in supporting documentation.

INVENIA INNOVATION A.S. ALLOWS FREE USE OF THIS SOFTWARE IN ITS "AS IS" CONDITION. INVENIA INNOVATION A.S. DISCLAIMS ANY LIABILITY OF ANY KIND FOR ANY DAMAGES WHATSOEVER RESULTING FROM THE USE OF THIS SOFTWARE.

The author requests users of this software to send back any improvements or extensions that they make and grant him and/or the Invenia Innovation the rights to redistribute these changes without restrictions.

Todd C. Miller

Copyright (C) 1998 Todd C. Miller <Todd.Miller@courtesan.com> All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES,INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[libtacplus]

Copyright (C) 1998, 2001, 2002, Juniper Networks, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the

distribution.
THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[tftp]

Copyright (C) 1983, 1993
The Regents of the University of California. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

[libfetch]

Copyright (C) 1998 Dag-Erling Coïdan Smørgrav

All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and

[IPv6 DHCP]

[iides]

the following disclaimer.
2. Redistribution with functional modification must include prominent notice stating how and when and by whom it is modified.
3. Redistributions in binary form have to be along with the source code or documentation which include above copyright notice, this list of conditions and the following disclaimer.
4. All commercial advertising materials mentioning features or use of this software must display the following acknowledgement:
 This product includes software developed by Internet Initiative Japan Inc.

THIS SOFTWARE IS PROVIDED BY ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.

[Net-SNMP]

CMU/UCD
Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000
Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Networks Associates Technology, Inc
Copyright (c) 2001-2003, Networks Associates Technology, Inc
All rights reserved.

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written

permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Cambridge Broadband Ltd.
Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.
All rights reserved.

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Sun Microsystems, Inc.
Copyright (c) 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara,
California 95054, U.S.A. All rights reserved.
Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Sparta, Inc
Copyright (c) 2003-2004, Sparta, Inc
All rights reserved.

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Cisco/BUPTNIC
Copyright (c) 2004, Cisco, Inc and Information Network

Apache License Version 2.0

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

   "License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

   "Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

   "Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

   "You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any erivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence),

contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

索引

数字

C

I

L

M

P

R

T

V

X

い

う

お

か

き

こ

さ

し

す

ろ