IP8800/S2200・IP8800/S2100・IP8800/SS1250・
IP8800/SS1240 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. 2.7 対応

IP8800SS1240-S001-A0

■対象製品

このマニュアルは次に示すモデル，ソフトウェアでサポートする機能を対象に記載しています。

- IP8800/S2200：Ver.2.7　OS-LT4，オプションライセンス
- IP8800/S2100：Ver.2.7　OS-LT5 （オプションライセンス未サポート）
- IP8800/SS1250：Ver.2.7　OS-LT3，オプションライセンス
- IP8800/SS1240：Ver.2.7　OS-LT2，オプションライセンス

■輸出時の注意

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

■商標一覧

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

■マニュアルはよく読み，保管してください。

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

■ご注意

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

■発行

２０１８年　3月 (第１１版) IP8800SS1240-S001-A0

■著作権

Copyright(C) NEC Corporation 2008,2018. All rights reserved.

変更履歴

【Ver. 2.7（第 11 版)】

表　変更履歴

章タイトル	追加・変更内容
1　本装置の概要	• MC 運用モード機能を追加しました。
10　装置の管理	• バックアップおよびリストア実行時の対象情報を変更しました。 • 内蔵フラッシュメモリへ保存時の注意事項を変更しました。
11　MC 運用モード機能【S2100】	• 本章を追加しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【Ver. 2.6（第 10 版)】

表　変更履歴

章タイトル	追加・変更内容
シリーズの追加	• IP8800/S2100 の記述を追加しました。
装置構成	• IP8800/S2100 の記述を追加しました。
収容条件	• IP8800/S2100 の記述を追加しました。
コマンド操作	• コマンド入力モードの記述を変更しました。
装置の管理	• IP8800/S2100 の記述を追加しました。
省電力機能	• IP8800/S2100 の記述を追加しました。
イーサネット	• IP8800/S2100 の記述を追加しました。
リンクアグリゲーション	• 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の記述を変更しました。
DHCP snooping	• コンフィグレーションガイド Vol.2 へ移動しました。

【Ver. 2.5（第 9 版)】

表　変更履歴

章タイトル	追加・変更内容
コマンド操作	• コマンド入力モードの記述を変更しました。
装置の管理	• 装置のバックアップ・リストアの記述を変更しました。 • 障害部位と復旧内容の記述を変更しました
イーサネット	• フローコントロールの記述を変更しました。
DHCP snooping	• DHCP パケットの監視の記述を変更しました。
IGMP snooping/MLD snooping の解説	• IGMP 即時離脱機能を追加しました。

【Ver. 2.4（第 7 版)】

表　変更履歴

章タイトル	追加・変更内容
シリーズの追加	• IP8800/S2200 の記述を追加しました。
装置構成	• IP8800/S2200 の記述を追加しました。

章タイトル	追加・変更内容
収容条件	• IP8800/S2200 の記述を追加しました。
装置の管理	• IP8800/S2200 の記述を追加しました。
省電力機能	• IP8800/S2200 の記述を追加しました。
イーサネット	• IP8800/S2200 の記述を追加しました。

【Ver. 2.3（第 6 版）】

表　変更履歴

章タイトル	追加・変更内容
収容条件	•「(6)Ring Protocol」に多重障害監視機能の収容条件を追加しました。
コマンド操作	• CLI の注意事項の「補完機能，ヘルプ機能の表示制限」の記述を変更しました。
MAC アドレス学習	• MAC アドレステーブルのクリア契機に，下記を追加しました。 スパニングツリーと Ring Protocol 併用構成でのフラッシュ制御フレームの受信契機 GSRP と Ring Protocol 併用構成でのフラッシュ制御フレームの受信契機 多重障害監視機能適用時のフラッシュ制御フレームの受信契機
Ring Protocol の解説	• 多重障害監視機能の記述を追加しました。
Ring Protocol の設定と運用	• 多重障害監視機能の記述を追加しました。
Ring Protocol とスパニングツリー / GSRP の併用	• Ring Protocol とスパニングツリーの併用装置が存在するリング構成で本装置の対応可能に伴い記述を変更しました。 • Ring Protocol と GSRP の併用装置が存在するリング構成で本装置の対応可能に伴い記述を変更しました。

【Ver. 2.3（第 5 版）】

表　変更履歴

章タイトル	追加・変更内容
収容条件	•「(13) レイヤ 2 認証機能」その他の認証共通収容条件を変更しました。 •「(15) アップリンク・リダンダントの収容条件」を追加しました。
コマンド操作	• CLI の注意事項の「補完機能，ヘルプ機能の表示制限」の記述を変更しました。
ログインセキュリティと RADIUS	• RADIUS サーバグループのサポートに伴い，RADIUS を使用した認証の記述を変更しました。 • RADIUS サーバグループのサポートに伴い，ログイン認証方式の設定例を変更しました。 • end-by-reject のサポートに伴い，RADIUS を使用した認証の記述を変更しました。 • end-by-reject のサポートに伴い，ログイン認証方式の設定例を変更しました。
時刻の設定と NTP	• 時刻の確認について記述を追加しました。
装置の管理	• 装置の環境状態および温度履歴情報の確認について記述を追加しました。
省電力機能	• 冷却 FAN 制御に FAN 動作条件について記述を追加しました。 • ポート省電力の記述を変更しました。 • スケジュール抑止モードの自動解除サポートに伴い，スケジュール起動モードの記述を変更しました。
イーサネット	• PoE の接続装置に関する注意事項を追加しました。

【Ver. 2.2（第 4 版）】

表　変更履歴

章タイトル	追加・変更内容
シリーズの追加	• IP8800/SS1250 の記述を追加しました。
装置構成	• IP8800/SS1250 の記述を追加しました。 • 100BASE-FX(SFP) サポートに伴い記述を追加しました。
収容条件	• IP8800/SS1250 の記述を追加しました。 • 100BASE-FX(SFP) サポートに伴い記述を追加しました。
時刻の設定と NTP	• IP8800/SS1250 の記述を追加しました。 • 障害部位と復旧内容について記述を追加しました。
イーサネット	• 100BASE-FX(SFP) サポートに伴い記述を追加しました。

【Ver. 2.2（第 3 版）】

表　変更履歴

章タイトル	追加・変更内容
収容条件	• ログインセキュリティと RADIUS の収容条件を追加しました。 • Ring Protocol の収容条件を追加しました。 • IEEE802.1X，Web 認証，MAC 認証に，認証方式グループの収容条件を追加しました。 • Web 認証にカスタムファイルセットの収容条件を追加しました。 • CFM の収容条件を追加しました。
ログインセキュリティと RADIUS	• RADIUS サーバグループの記述を追加しました。
装置の管理	•「IP8800/SS1200 シリーズ間の互換性」で，入力形式が変更された運用コマンド名を追加しました。
レイヤ 2 スイッチ概説	• レイヤ 2 スイッチ機能と他機能の共存に「Ring Protocol での制限事項」を追加しました。
MAC アドレス学習	• MAC アドレステーブルのクリアについて記述を追加しました。
VLAN 拡張機能	• ポート間中継遮断機能使用時の注意事項に CFM を使用時の注意事項を追加しました。
Ring Protocol の解説	• 本章を追加しました。
Ring Protocol の設定と運用	• 本章を追加しました。
Ring Protocol とスパニングツリー / GSRP の併用	• 本章を追加しました。
IPv4 インタフェース	• IP 重複検出の記述を追加しました。

【Ver. 2.1（第 2 版）】

表　変更履歴

章タイトル	追加・変更内容
収容条件	• IEEE802.1X，Web 認証，MAC 認証に，認証専用 RADIUS サーバの収容条件を追加しました。
装置へのログイン	• 本装置の起動から停止までの概略フロー図を変更しました。
リモート運用端末から本装置へのログイン	• 運用コマンド一覧に ftp を追加しました。

章タイトル	追加・変更内容
ログインセキュリティと RADIUS	• 認証専用 RADIUS サーバ情報の追加に伴い，「RADIUS サーバの選択」と「RADIUS サーバの復旧」の説明を，コンフィグレーションガイド Vol.2「5 レイヤ 2 認証機能の概説」へ移動しました。
装置の管理	• 運用コマンド一覧（リソース情報の確認）に show cpu，show memory summary を追加しました。
省電力機能	• LED 自動動作の記述を追加しました。 • ポート省電力の記述を追加しました。 • 装置スリープの記述を追加しました。 • 冷却 FAN 制御の記述を追加しました。 • 省電力機能のスケジューリングを追加しました。
レイヤ 2 スイッチ概説	• レイヤ 2 スイッチ機能と他機能の共存で「IGMP/MLD snooping での制限事項」からリンクアグリゲーションを削除しました。
MAC アドレス学習	• レイヤ 2 認証機能を使用時のエージング時間について 注意事項を追加しました。
VLAN	• MAC VLAN 解説の注意事項に，レイヤ 2 認証連携時の MAC ポートに対する自動 VLAN 割当の記述を追加しました。
VLAN 拡張機能	• ポート間中継遮断機能使用時の注意事項に DHCP snooping，IGMP/MLD snooping を使用時の注意事項を追加しました。

はじめに

■対象製品およびソフトウェアバージョン

このマニュアルは次に示すモデル，ソフトウェアでサポートする機能を対象に記載しています。

- IP8800/S2200：Ver.2.7　OS-LT4，オプションライセンス
- IP8800/S2100：Ver.2.7　OS-LT5 （オプションライセンス未サポート）
- IP8800/SS1250：Ver.2.7　OS-LT3，オプションライセンス
- IP8800/SS1240：Ver.2.7　OS-LT2，オプションライセンス

操作を行う前にこのマニュアルをよく読み，書かれている指示や注意を十分に理解してください。また，このマニュアルは必要なときにすぐ参照できるよう使いやすい場所に保管してください。
なお，このマニュアルでは特に断らないかぎり IP8800/S2200，IP8800/S2100，IP8800/SS1250，IP8800/SS1240 に共通の機能について記載しますが，機種固有の機能については以下のマークで示します。

【S2200】:
IP8800/S2200 についての記述です。

【S2100】:
IP8800/S2100 についての記述です。

【SS1250】:
IP8800/SS1250 についての記述です。

【SS1240】:
IP8800/SS1240 についての記述です。

また，このマニュアルでは特に断らないかぎり OS-LT5，OS-LT4，OS-LT3，OS-LT2 の機能について記載しますが，オプションライセンスの機能については以下のマークで示します。

【OP-WOL】:
オプションライセンス OP-WOL でサポートする機能です。

【OP-OTP】:
オプションライセンス OP-OTP でサポートする機能です。

■このマニュアルの訂正について

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

■対象読者

本装置を利用したネットワークシステムを構築し，運用するシステム管理者の方を対象としています。
また，次に示す知識を理解していることを前提としています。

- ネットワークシステム管理の基礎的な知識

■このマニュアルの URL

このマニュアルの内容は下記 URL に掲載しております。
https://jpn.nec.com/ip88n/

■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。

●初期導入時の基本的な設定について知りたい，
ハードウェアの設備条件，取扱方法を調べる

IP8800/S2200・IP8800/S2100・
IP8800/SS1250・IP8800/SS1240
ハードウェア取扱説明書
(IP8800SS1240-H001)

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

コンフィグレーションガイド
Vol.1
(IP8800SS1240-S001)

Vol.2
(IP8800SS1240-S002)

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

コンフィグレーション
コマンドレファレンス
(IP8800SS1240-S003)

●運用コマンドの入力シンタックス，
パラメータ詳細について知りたい

運用コマンドレファレンス
(IP8800SS1240-S004)

●メッセージとログについて調べる

メッセージ・ログレファレンス
(IP8800SS1240-S005)

●MIBについて調べる

MIBレファレンス
(IP8800SS1240-S006)

●トラブル発生時の対処方法について知りたい

トラブルシューティングガイド
(IP8800SS1240-T001)

■このマニュアルでの表記

AC	Alternating Current
ACK	ACKnowledge
ADSL	Asymmetric Digital Subscriber Line
ALG	Application Level Gateway
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
AS	Autonomous System
AUX	Auxiliary
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol - version 4
BGP4+	Multiprotocol Extensions for Border Gateway Protocol - version 4
bit/s	bits per second　*bpsと表記する場合もあります。
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
CC	Continuity Check
CDP	Cisco Discovery Protocol
CFM	Connectivity Fault Management
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network System
CONS	Connection Oriented Network System

CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNP	Complete Sequence Numbers PDU
CST	Common Spanning Tree
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DHCP	Dynamic Host Configuration Protocol
DIS	Draft International Standard/Designated Intermediate System
DNS	Domain Name System
DR	Designated Router
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EFM	Ethernet in the First Mile
ES	End System
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FQDN	Fully Qualified Domain Name
FTTH	Fiber To The Home
GBIC	GigaBit Interface Converter
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCP	IP Control Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IP Version 6 Control Protocol
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Internal Spanning Tree
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLQ+3WFQ	Low Latency Queueing + 3 Weighted Fair Queueing
LSP	Label Switched Path
LSP	Link State PDU
LSR	Label Switched Router
MA	Maintenance Association
MAC	Media Access Control
MC	Memory Card
MD5	Message Digest 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface crossover
MEP	Maintenance association End Point
MIB	Management Information Base
MIP	Maintenance domain Intermediate Point
MLD	Multicast Listener Discovery
MRU	Maximum Receive Unit
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transfer Unit
NAK	Not AcKnowledge
NAS	Network Access Server
NAT	Network Address Translation
NCP	Network Control Protocol
NDP	Neighbor Discovery Protocol

NET	Network Entity Title
NLA ID	Next-Level Aggregation Identifier
NPDU	Network Protocol Data Unit
NSAP	Network Service Access Point
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OADP	Octpower Auto Discovery Protocol
OAM	Operations,Administration,and Maintenance
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
packet/s	packets per second　　*ppsと表記する場合もあります。
PAD	PADding
PAE	Port Access Entity
PC	Personal Computer
PCI	Protocol Control Information
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
PID	Protocol IDentifier
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PIM-SSM	Protocol Independent Multicast-Source Specific Multicast
PoE	Power over Ethernet
PRI	Primary Rate Interface
PS	Power Supply
PSNP	Partial Sequence Numbers PDU
QoS	Quality of Service
RA	Router Advertisement
RADIUS	Remote Authentication Dial In User Service
RDI	Remote Defect Indication
REJ	REJect
RFC	Request For Comments
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RMON	Remote Network Monitoring MIB
RPF	Reverse Path Forwarding
RQ	ReQuest
RSTP	Rapid Spanning Tree Protocol
SA	Source Address
SD	Secure Digital
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SEL	NSAP SELector
SFD	Start Frame Delimiter
SFP	Small Form factor Pluggable
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SPF	Shortest Path First
SSAP	Source Service Access Point
STP	Spanning Tree Protocol
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
TLV	Type, Length, and Value
TOS	Type Of Service
TPID	Tag Protocol Identifier
TTL	Time To Live
UDLD	Uni-Directional Link Detection
UDP	User Datagram Protocol
ULR	Uplink Redundant
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
VAA	VLAN Access Agent
VLAN	Virtual LAN
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queueing
WRED	Weighted Random Early Detection
WS	Work Station

WWW	World-Wide Web
XFP	10 gigabit small Form factor Pluggable

■ kB(バイト) などの単位表記について

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

目次

第 1 編　本装置の概要と収容条件

1 本装置の概要 1

1.1 本装置の概要 2

1.2 本装置の特長 3

2 装置構成 7

2.1 本装置のモデル 8

2.1.1 装置の外観 8

2.2 装置の構成要素 13

2.2.1 ハードウェア 13

2.2.2 ソフトウェア 18

3 収容条件 19

3.1 搭載条件 20

3.1.1 収容回線数 20

3.1.2 搭載メモリ量 20

3.2 収容条件 22

3.2.1 ログインセキュリティと RADIUS 22

3.2.2 リンクアグリゲーション 22

3.2.3 レイヤ 2 スイッチ機能 22

3.2.4 IP インタフェース 26

3.2.5 フィルタ・QoS 27

3.2.6 レイヤ 2 認証機能 29

3.2.7 セキュリティ 33

3.2.8 冗長化構成による高信頼化機能 33

3.2.9 ネットワークの障害検出による高信頼化機能 34

3.2.10 隣接装置情報（LLDP） 35

第 2 編　運用管理

4 装置へのログイン 37

4.1 運用端末による管理 38

4.1.1 運用端末 38

4.1.2 運用端末の接続形態 39

4.1.3 運用管理機能の概要 40

4.2 装置起動 41
4.2.1 本装置の起動から停止までの概略 41
4.2.2 装置の起動 42
4.2.3 装置の停止 42
4.3 ログイン・ログアウト 43

5 コマンド操作 45
5.1 コマンド入力モード 46
5.1.1 運用コマンド一覧 46
5.1.2 コマンド入力モード 46
5.2 CLI での操作 49
5.2.1 補完機能 49
5.2.2 ヘルプ機能 49
5.2.3 入力エラー指摘機能 49
5.2.4 コマンド短縮実行 50
5.2.5 ヒストリ機能 50
5.2.6 ページング 51
5.2.7 キーボードコマンド機能 51
5.3 CLI の注意事項 53

6 コンフィグレーション 57
6.1 コンフィグレーション 58
6.1.1 起動時のコンフィグレーション 58
6.1.2 運用中のコンフィグレーション 58
6.2 ランニングコンフィグレーションの編集概要 59
6.3 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 60
6.4 コンフィグレーションの編集方法 61
6.4.1 コンフィグレーション・運用コマンド一覧 61
6.4.2 configure（configure terminal）コマンド 61
6.4.3 コンフィグレーションの表示・確認（show コマンド） 62
6.4.4 コンフィグレーションの追加・変更・削除 64
6.4.5 コンフィグレーションのファイルへの保存 65
6.4.6 コンフィグレーションの編集終了（exit コマンド） 66
6.4.7 コンフィグレーションの編集時の注意事項 66
6.5 コンフィグレーションの操作 67
6.5.1 ftp を使用したファイル転送 67
6.5.2 MC を使用したファイル転送 68
6.5.3 バックアップコンフィグレーションファイル反映時の注意事項 69

7 リモート運用端末から本装置へのログイン 71
7.1 解説 72
7.2 コンフィグレーション 73
7.2.1 コンフィグレーションコマンド一覧 73
7.2.2 本装置への IP アドレスの設定 73
7.2.3 telnet によるログインを許可する 74
7.2.4 ftp によるログインを許可する 74
7.3 オペレーション 75
7.3.1 運用コマンド一覧 75
7.3.2 リモート運用端末と本装置との通信の確認 75

8 ログインセキュリティと RADIUS 77
8.1 ログインセキュリティの設定 78
8.1.1 コンフィグレーション・運用コマンド一覧 78
8.1.2 ログイン制御の概要 78
8.1.3 ログインユーザの変更 79
8.1.4 装置管理者モード移行のパスワードの設定 79
8.1.5 リモート運用端末からのログインの許可 79
8.1.6 同時にログインできるユーザ数の設定 80
8.1.7 リモート運用端末からのログインの制限 80
8.2 RADIUS の解説 82
8.2.1 RADIUS の概要 82
8.2.2 RADIUS 認証の適用機能および範囲 82
8.2.3 RADIUS を使用した認証 84
8.2.4 RADIUS サーバとの接続 87
8.3 RADIUS のコンフィグレーション 89
8.3.1 コンフィグレーションコマンド一覧 89
8.3.2 ログイン認証方式の設定 89
8.3.3 RADIUS サーバグループの設定 90
8.4 RADIUS のオペレーション 92
8.4.1 運用コマンド一覧 92
8.4.2 有効 RADIUS サーバ情報の表示 92

9 時刻の設定と NTP 95
9.1 時刻の設定と確認 96
9.1.1 サポート仕様 96
9.1.2 時刻変更に関する注意事項 98
9.2 コンフィグレーション 99
9.2.1 コンフィグレーションコマンド一覧 99

9.2.2 システムクロックの設定 99
9.2.3 NTP サーバから定期的に時刻情報を取得する 99
9.3 オペレーション 100
9.3.1 運用コマンド一覧 100
9.3.2 時刻の確認 100
9.3.3 NTP クライアント情報の表示 100

10 装置の管理 101
10.1 装置の状態確認，および運用形態に関する設定 102
10.1.1 コンフィグレーション・運用コマンド一覧 102
10.1.2 ソフトウェアバージョンの確認 103
10.1.3 装置の状態確認 103
10.1.4 運用ログのモニタ表示実施と停止 105
10.1.5 運用ログ情報の確認 105
10.1.6 システムファンクションリソースを使用する機能【SS1250】【SS1240】 106
10.2 装置情報のバックアップ・リストア 107
10.2.1 運用コマンド一覧 107
10.2.2 バックアップおよびリストア実行時の対象情報 107
10.3 シリーズ間の互換性 109
10.3.1 IP8800/SS1250・IP8800/SS1240 と IP8800/SS1230 の入力コマンドの互換性 109
10.3.2 IP8800/SS1250 と IP8800/SS1240 の装置情報の互換性 110
10.3.3 IP8800/SS1250・IP8800/SS1240 と IP8800/SS1230 の装置情報の互換性 111
10.4 障害時の復旧 113
10.4.1 障害部位と復旧内容 113
10.5 内蔵フラッシュメモリへ保存時の注意事項 115

11 MC 運用モード機能【S2100】 117
11.1 MC 運用モード機能の解説 118
11.1.1 概要 118
11.1.2 MC に保存されるファイル 118
11.1.3 本機能を使用した運用手順 118
11.1.4 障害時の動作 119
11.1.5 他機能との共存 120
11.1.6 MC 運用モード機能使用時の注意事項 120
11.2 MC 運用モード機能のコンフィグレーション 121
11.2.1 コンフィグレーションコマンド一覧 121
11.3 MC 運用モード機能のオペレーション 122
11.3.1 運用コマンド一覧 122

12 省電力機能 123
12.1 省電力機能の解説 124
12.1.1 サポートする省電力機能 124
12.1.2 LED 動作 125
12.1.3 ポート省電力 129
12.1.4 装置スリープ【SS1250】【SS1240】 131
12.1.5 冷却 FAN 制御機能（準 FAN レス動作）【SS1240】 131
12.1.6 省電力機能のスケジューリング 132
12.1.7 省電力機能使用時の注意事項 137
12.2 省電力機能のコンフィグレーション 139
12.2.1 コンフィグレーションコマンド一覧 139
12.2.2 LED 動作の設定 139
12.2.3 リンクダウンポートの省電力機能の設定 140
12.2.4 冷却 FAN 制御機能（準 FAN レス動作）の設定【SS1240】 140
12.2.5 スケジューリングによる省電力の設定 140
12.3 省電力機能のオペレーション 143
12.3.1 運用コマンド一覧 143
12.3.2 LED 動作状態の表示 143
12.3.3 ポート省電力制御状態の表示 143
12.3.4 冷却 FAN 制御状態の表示【SS1240】 143
12.3.5 スケジュール運用状態の表示 143
13 ソフトウェアの管理 145
13.1 運用コマンド一覧 146
13.2 ソフトウェアのアップデート 147
13.2.1 ソフトウェアのアップデートに関する注意事項 147

第 3 編　ネットワークインタフェース

14 イーサネット 149
14.1 イーサネット共通の解説 150
14.1.1 ネットワーク構成例 150
14.1.2 物理インタフェース 150
14.1.3 MAC および LLC 副層制御 150
14.1.4 本装置の MAC アドレス 152
14.1.5 イーサネットフレームの順序について 153
14.2 イーサネット共通のコンフィグレーション 154
14.2.1 コンフィグレーションコマンド一覧 154

14.2.2 イーサネットインタフェースのポートの設定 【S2200】【S2100】 154
14.2.3 イーサネットインタフェースのポートの設定【SS1250】【SS1240】 155
14.2.4 複数ポートの一括設定 155
14.2.5 ポートのシャットダウン 155
14.2.6 リンクダウン検出タイマの設定 156
14.2.7 フローコントロールの設定 156
14.2.8 自動 MDIX の設定 157
14.2.9 ジャンボフレームの設定 157
14.3 イーサネット共通のオペレーション 159
14.3.1 運用コマンド一覧 159
14.3.2 イーサネットの動作状態を確認する 159
14.4 Fastethernet の解説【SS1250】【SS1240】 160
14.4.1 機能一覧 160
14.5 Fastethernet のコンフィグレーション【SS1250】【SS1240】 165
14.5.1 ポートの設定 165
14.5.2 フローコントロールの設定 166
14.5.3 自動 MDIX の設定 166
14.5.4 ジャンボフレームの設定 166
14.6 Gigabitethernet（RJ45）の解説 167
14.6.1 機能一覧 167
14.6.2 SFP 自動認識機能 (メディアタイプの選択)【SS1250】【SS1240】 173
14.7 Gigabitethernet（RJ45）のコンフィグレーション 174
14.7.1 ポートの設定 174
14.7.2 フローコントロールの設定 175
14.7.3 自動 MDIX の設定 175
14.7.4 ジャンボフレームの設定 175
14.7.5 メディアタイプの設定【SS1250】【SS1240】 175
14.8 Gigabitethernet（SFP）の解説 177
14.8.1 機能一覧 177
14.8.2 SFP 使用時の注意事項 182
14.9 Gigabitethernet（SFP）のコンフィグレーション 184
14.9.1 100BASE-FX のポート設定【SS1250】 184
14.9.2 1000BASE-X のポート設定 184
14.9.3 フローコントロールの設定 185
14.9.4 ジャンボフレームの設定 185
14.9.5 メディアタイプの設定【SS1250】【SS1240】 185
14.10 PoE の解説【S2200】【S2100】【SS1240】 186
14.10.1 PoE の概要 186
14.10.2 PoE の供給電力割り当て【S2200】 186
14.10.3 PoE の供給電力割り当て【S2100】【SS1240】 188
14.10.4 最大電力供給超過時の動作設定 190
14.10.5 電力給電再開・停止とポート状態 192

14.10.6 PoE 使用時の注意事項 194
14.11 PoE のコンフィグレーション【S2200】【S2100】【SS1240】 196
14.11.1 コンフィグレーションコマンド一覧 196
14.11.2 系統 1 で供給可能な最大電力量の設定【S2200】 196
14.11.3 ポート優先度の設定 197
14.11.4 既給電ポート優先の設定 197
14.11.5 ポート単位の供給電力割り当て設定 198
14.12 PoE のオペレーション【S2200】【S2100】【SS1240】 199
14.12.1 運用コマンド一覧 199
14.12.2 PoE の確認 199

15 リンクアグリゲーション 201
15.1 リンクアグリゲーション基本機能の解説 202
15.1.1 概要 202
15.1.2 リンクアグリゲーションの構成 202
15.1.3 サポート仕様 202
15.1.4 チャネルグループの MAC アドレス 203
15.1.5 フレーム送信時のポート振り分け 203
15.1.6 リンクアグリゲーション使用時の注意事項 203
15.2 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 205
15.2.1 コンフィグレーションコマンド一覧 205
15.2.2 スタティックリンクアグリゲーションの設定 205
15.2.3 LACP リンクアグリゲーションの設定 205
15.2.4 ポートチャネルインタフェースの設定 207
15.2.5 チャネルグループの削除 210
15.3 リンクアグリゲーション拡張機能の解説 211
15.3.1 スタンバイリンク機能 211
15.4 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 213
15.4.1 コンフィグレーションコマンド一覧 213
15.4.2 スタンバイリンク機能のコンフィグレーション 213
15.5 リンクアグリゲーションのオペレーション 214
15.5.1 運用コマンド一覧 214
15.5.2 リンクアグリゲーションの状態の確認 214

第 4 編 レイヤ 2 スイッチ

16 レイヤ 2 スイッチ概説 217
16.1 概要 218
16.1.1 MAC アドレス学習 218

16.1.2 VLAN 218
16.2 サポート機能 219
16.3 レイヤ 2 スイッチ機能と他機能の共存について 220

17 MAC アドレス学習 223
17.1 MAC アドレス学習の解説 224
17.1.1 送信元 MAC アドレス学習 224
17.1.2 学習 MAC アドレスのエージング 224
17.1.3 MAC アドレスによるレイヤ 2 スイッチング 224
17.1.4 スタティックエントリの登録 225
17.1.5 MAC アドレステーブルのクリア 225
17.1.6 注意事項 226
17.2 MAC アドレス学習のコンフィグレーション 228
17.2.1 コンフィグレーションコマンド一覧 228
17.2.2 エージング時間の設定 228
17.2.3 スタティックエントリの設定 228
17.3 MAC アドレス学習のオペレーション 230
17.3.1 運用コマンド一覧 230
17.3.2 MAC アドレス学習の状態の確認 230
17.3.3 MAC アドレス学習数の確認 230

18 VLAN 233
18.1 VLAN 基本機能の解説 234
18.1.1 VLAN の種類 234
18.1.2 ポートの種類 234
18.1.3 デフォルト VLAN 235
18.1.4 VLAN の優先順位 235
18.1.5 VLAN Tag 237
18.1.6 VLAN 使用時の注意事項 238
18.2 VLAN 基本機能のコンフィグレーション 240
18.2.1 コンフィグレーションコマンド一覧 240
18.2.2 VLAN の設定 240
18.2.3 ポートの設定 241
18.2.4 トランクポートの設定 241
18.3 ポート VLAN の解説 243
18.3.1 アクセスポートとトランクポート 243
18.3.2 ネイティブ VLAN 243
18.3.3 ポート VLAN 使用時の注意事項 244
18.4 ポート VLAN のコンフィグレーション 245
18.4.1 コンフィグレーションコマンド一覧 245
18.4.2 ポート VLAN の設定 245

18.4.3 トランクポートのネイティブ VLAN の設定 247
18.5 プロトコル VLAN の解説 248
18.5.1 概要 248
18.5.2 プロトコルの識別 248
18.5.3 プロトコルポートとトランクポート 249
18.5.4 プロトコルポートのネイティブ VLAN 249
18.6 プロトコル VLAN のコンフィグレーション 250
18.6.1 コンフィグレーションコマンド一覧 250
18.6.2 プロトコル VLAN の作成 250
18.6.3 プロトコルポートのネイティブ VLAN の設定 253
18.7 MAC VLAN の解説 254
18.7.1 概要 254
18.7.2 装置間の接続と MAC アドレス設定 254
18.7.3 レイヤ 2 認証機能との連携について 255
18.7.4 MAC ポートのオプション機能 256
18.8 MAC VLAN のコンフィグレーション 258
18.8.1 コンフィグレーションコマンド一覧 258
18.8.2 MAC VLAN の設定 258
18.8.3 MAC ポートのネイティブ VLAN の設定 261
18.8.4 MAC ポートでの Tagged フレーム中継の設定 261
18.9 VLAN のオペレーション 264
18.9.1 運用コマンド一覧 264
18.9.2 VLAN の状態の確認 264

19 VLAN 拡張機能 269
19.1 L2 プロトコルフレーム透過機能の解説 270
19.1.1 概要 270
19.2 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 271
19.2.1 コンフィグレーションコマンド一覧 271
19.2.2 L2 プロトコルフレーム透過機能の設定 271
19.3 ポート間中継遮断機能の解説 272
19.3.1 概要 272
19.3.2 ポート間中継遮断機能使用時の注意事項 272
19.4 ポート間中継遮断機能のコンフィグレーション 274
19.4.1 コンフィグレーションコマンド一覧 274
19.4.2 ポート間中継遮断機能の設定 274
19.4.3 遮断するポートの変更 275
19.5 VLAN 拡張機能のオペレーション 276
19.5.1 運用コマンド一覧 276
19.5.2 VLAN 拡張機能の確認 276

20 スパニングツリー 279
20.1 スパニングツリーの概説 280
20.1.1 概要 280
20.1.2 スパニングツリーの種類 280
20.1.3 スパニングツリーと高速スパニングツリー 281
20.1.4 スパニングツリートポロジーの構成要素 282
20.1.5 スパニングツリーのトポロジー設計 284
20.1.6 STP 互換モード 286
20.1.7 スパニングツリー共通の注意事項 287
20.2 スパニングツリー動作モードのコンフィグレーション 288
20.2.1 コンフィグレーションコマンド一覧 288
20.2.2 動作モードの設定 288
20.3 PVST+ 解説 291
20.3.1 PVST+ によるロードバランシング 291
20.3.2 アクセスポートの PVST+ 292
20.3.3 PVST+ 使用時の注意事項 293
20.4 PVST+ のコンフィグレーション 294
20.4.1 コンフィグレーションコマンド一覧 294
20.4.2 PVST+ の設定 294
20.4.3 PVST+ のトポロジー設定 295
20.4.4 PVST+ のパラメータ設定 296
20.5 PVST+ のオペレーション 299
20.5.1 運用コマンド一覧 299
20.5.2 PVST+ の状態の確認 299
20.6 シングルスパニングツリー解説 300
20.6.1 概要 300
20.6.2 PVST+ との併用 300
20.6.3 シングルスパニングツリー使用時の注意事項 301
20.7 シングルスパニングツリーのコンフィグレーション 302
20.7.1 コンフィグレーションコマンド一覧 302
20.7.2 シングルスパニングツリーの設定 302
20.7.3 シングルスパニングツリーのトポロジー設定 303
20.7.4 シングルスパニングツリーのパラメータ設定 304
20.8 シングルスパニングツリーのオペレーション 307
20.8.1 運用コマンド一覧 307
20.8.2 シングルスパニングツリーの状態の確認 307
20.9 マルチプルスパニングツリー解説 308
20.9.1 概要 308
20.9.2 マルチプルスパニングツリーのネットワーク設計 310
20.9.3 ほかのスパニングツリーとの互換性 312
20.9.4 マルチプルスパニングツリー使用時の注意事項 313

20.10 マルチプルスパニングツリーのコンフィグレーション 314
20.10.1 コンフィグレーションコマンド一覧 314
20.10.2 マルチプルスパニングツリーの設定 314
20.10.3 マルチプルスパニングツリーのトポロジー設定 315
20.10.4 マルチプルスパニングツリーのパラメータ設定 317
20.11 マルチプルスパニングツリーのオペレーション 320
20.11.1 運用コマンド一覧 320
20.11.2 マルチプルスパニングツリーの状態の確認 320
20.12 スパニングツリー共通機能解説 321
20.12.1 PortFast 321
20.12.2 BPDU フィルタ 322
20.12.3 ループガード 323
20.12.4 ルートガード 325
20.13 スパニングツリー共通機能のコンフィグレーション 327
20.13.1 コンフィグレーションコマンド一覧 327
20.13.2 PortFast の設定 327
20.13.3 BPDU フィルタの設定 328
20.13.4 ループガードの設定 329
20.13.5 ルートガードの設定 329
20.13.6 リンクタイプの設定 330
20.14 スパニングツリー共通機能のオペレーション 331
20.14.1 運用コマンド一覧 331
20.14.2 スパニングツリー共通機能の状態の確認 331

21 Ring Protocol の解説【S2200】【SS1250】【SS1240】 333
21.1 Ring Protocol の概要 334
21.1.1 概要 334
21.1.2 特長 335
21.1.3 サポート仕様 337
21.2 Ring Protocol の基本原理 338
21.2.1 ネットワーク構成 338
21.2.2 制御 VLAN 340
21.2.3 障害監視方法 340
21.2.4 通信経路の切り替え 340
21.3 シングルリングの動作概要 341
21.3.1 リング正常時の動作 341
21.3.2 障害検出時の動作 341
21.3.3 復旧検出時の動作 343
21.4 マルチリングの動作概要 345
21.4.1 リング正常時の動作 345
21.4.2 共有リンク障害・復旧時の動作 347

21.4.3 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 349
21.4.4 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 351
21.5 Ring Protocol の多重障害監視機能 354
21.5.1 概要 354
21.5.2 多重障害監視機能の基本構成 355
21.5.3 多重障害監視の動作概要 356
21.5.4 多重障害発生時の動作 357
21.5.5 多重障害復旧時の動作 359
21.6 Ring Protocol のネットワーク設計 362
21.6.1 VLAN マッピングの使用方法 362
21.6.2 制御 VLAN の forwarding-delay-time の使用方法 362
21.6.3 Ring Protocol の禁止構成 363
21.6.4 多重障害監視機能の禁止構成 363
21.7 Ring Protocol 使用時の注意事項 364

22 Ring Protocol の設定と運用【S2200】【SS1250】【SS1240】 367
22.1 コンフィグレーション 368
22.1.1 コンフィグレーションコマンド一覧 368
22.1.2 Ring Protocol 設定の流れ 368
22.1.3 リング ID の設定 369
22.1.4 制御 VLAN の設定 369
22.1.5 VLAN マッピングの設定 370
22.1.6 VLAN グループの設定 371
22.1.7 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） 371
22.1.8 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） 372
22.1.9 各種パラメータの設定 375
22.1.10 多重障害監視機能の設定 376
22.2 オペレーション 377
22.2.1 運用コマンド一覧 377
22.2.2 Ring Protocol の状態確認 377

23 Ring Protocol とスパニングツリー /GSRP の併用【S2200】【SS1250】【SS1240】 379
23.1 Ring Protocol とスパニングツリーとの併用 380
23.1.1 概要 380
23.2 Ring Protocol と GSRP との併用 382
23.2.1 動作概要 382

24 IGMP snooping/MLD snooping の解説 385
24.1 IGMP snooping/MLD snooping の概要 386
24.1.1 マルチキャスト概要 386

24.1.2 IGMP snooping および MLD snooping 概要 387
24.2 IGMP snooping/MLD snooping サポート機能 388
24.3 IGMP snooping 389
24.3.1 MAC アドレス制御方式 389
24.3.2 マルチキャストルータとの接続 390
24.3.3 IGMP クエリア機能 391
24.3.4 IGMP 即時離脱機能 391
24.4 MLD snooping 392
24.4.1 MAC アドレス制御方式 392
24.4.2 マルチキャストルータとの接続 393
24.4.3 MLD クエリア機能 394
24.5 IGMP snooping/MLD snooping 使用時の注意事項 395

25 IGMP snooping/MLD snooping の設定と運用 399
25.1 IGMP snooping のコンフィグレーション 400
25.1.1 コンフィグレーションコマンド一覧 400
25.1.2 IGMP snooping の設定 400
25.1.3 IGMP クエリア機能の設定 400
25.1.4 マルチキャストルータポートの設定 401
25.2 IGMP snooping のオペレーション 402
25.2.1 運用コマンド一覧 402
25.2.2 IGMP snooping の確認 402
25.3 MLD snooping のコンフィグレーション 404
25.3.1 コンフィグレーションコマンド一覧 404
25.3.2 MLD snooping の設定 404
25.3.3 MLD クエリア機能の設定 404
25.3.4 マルチキャストルータポートの設定 405
25.3.5 MLD Query メッセージ送信元 IP アドレスの設定 405
25.4 MLD snooping のオペレーション 406
25.4.1 運用コマンド一覧 406
25.4.2 MLD snooping の確認 406

付録 409
付録 A 準拠規格 410
付録 A.1 TELNET/FTP 410
付録 A.2 RADIUS 410
付録 A.3 NTP 410
付録 A.4 イーサネット 410
付録 A.5 リンクアグリゲーション 411
付録 A.6 VLAN 411
付録 A.7 スパニングツリー 411

付録 A.8　IGMP snooping/MLD snooping　411
付録 A.9　IPv4 インタフェース　411

索引　413

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 本装置の概要
1.2 本装置の特長

1.1 本装置の概要

企業内のネットワークは，IP 電話，インターネット接続，基幹業務などに使われ，PC は一人に 1 台が配布されるなど企業内の通信トラフィックは増大し続ける一方です。

また，ネットワークに流れるデータは企業の利益を左右するミッションクリティカルな重要データが流れています。ミッションクリティカルな市場は，ISP やネットワーク事業者が中心でしたが，今後は企業や公共の構内網に拡大されていく傾向にあります。

本装置は，ミッションクリティカルの分野に適用可能な製品にすることによって，信頼性・可用性・拡張性の高い情報ネットワーク基盤を柔軟に構築するスイッチ製品です。

製品コンセプト

IP8800/S2200 シリーズ，IP8800/S2100 シリーズ，IP8800/SS1250 シリーズ，および IP8800/SS1240 シリーズは，充実した認証機能を含む各種機能を備えた，フロアやワークグループ LAN を実現するための，小型 LAN スイッチです。

IP8800/S2200 シリーズ，および IP8800/S2100 シリーズは，ギガビットイーサネット対応のレイヤ 2 スイッチです。

IP8800/SS1250 シリーズ，および IP8800/SS1240 シリーズは，ファーストイーサネット対応のレイヤ 2 スイッチです。

本装置は次の機能を実現します。

- さまざまなネットワーク冗長機能をサポートし，高信頼・高可用なネットワークを実現
- リンクアグリゲーションを用意し，トラフィック増大に対して余裕を持ったネットワークを実現
- 企業内で扱われるさまざまなトラフィック（基幹業務データ，VoIP 電話データ，テレビ会議，ストリーミング配信，CAD データなど）を QoS 技術などで保護するギャランティ型ネットワークを実現
- 高機能フィルタ，ユーザ認証などのセキュリティ機能で安全なネットワークを実現
- フルワイヤーレートでのパケットフォワーディングを実現
- IEEE802.3af/IEEE802.3at 準拠の PoE 対応によって，電源コンセントの位置に依存しない機器設置を実現【S2200】【S2100】【SS1240】
- ネットワークの設計・構築・運用のトータルコストを削減する OAN への対応

1.2 本装置の特長

(1) 統一ラインナップの実現

● ローエンドスイッチの提供

- ローエンドのイーサネットレイヤ 2 スイッチとしてエッジの部分をカバーし，IP8800 シリーズとしての一貫した接続性，操作性，相互運用性を維持
  ギガビットイーサネットレイヤ 2 スイッチ【S2200】【S2100】
  ファーストイーサネットレイヤ 2 スイッチ【SS1250】【SS1240】

(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（IEEE 802.1D），高速スパニングツリー（IEEE 802.1w），PVST+，マルチプルスパニングツリー（IEEE 802.1s）を実装

(3) 強固なセキュリティ機能

● 認証・検疫ソリューション

- レイヤ 2 認証機能（IEEE802.1X，Web 認証※ 1，MAC 認証）によって，エッジの物理構成の自由度を保ちつつ，PC1 台 1 台を認証し，VLAN に加入させることが可能
- IEEE802.1X ポート単位認証（静的）は，状態監視によって通信可能なパケットを制限，および解放することで，セキュリティポリシーに合致した端末だけにフルアクセスの通信を許可
- セキュア Wake on LAN により，自宅や出張などの外出先から，社内ネットワーク経由で本装置に Web ブラウザでアクセスし，社内自席 PC の電源を投入可能※ 2
- RSA SecurID システムと連携したワンタイムパスワード認証機能を使用して Web 認証やログイン認証を実施し，ネットワークアクセスに対するセキュリティを向上させることが可能。また New PIN モードや，Next token モードなどにも対応※ 2
- 「正規端末を使用するユーザだけにユーザ認証の機会を与える」ことを目的としたマルチステップ認証に対応※ 3

注※ 1
IP8800/S2100 シリーズは Web 認証未サポートです。

注※ 2
本機能はソフトウェアオプションライセンスを別途購入する必要があります。なお，IP8800/S2100 シリーズはオプションライセンスおよびライセンスに伴う機能は未サポートです。

注※ 3
端末認証 (MAC 認証または IEEE802.1X) が完了後に，ユーザ認証（IEEE802.1X または Web 認証）を実施する 2 段階の認証を実施します。

● 不正な DHCP サーバ / 固定 IP アドレス端末の排除

- DHCP snooping 機能により，不正な DHCP サーバや固定 IP アドレス端末を排除するなど，強固なセキュリティ対策が可能

● 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

● RADIUS による装置へのログイン・パスワード認証を設定可能

(4) ハードウェアによる強力な QoS をイーサネットで実現

● 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 ヘッダの一部）指定で，高い精度の QoS 制御が可能

● 多様な QoS 制御機能

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

注※
マーカー機能だけサポートしています。

● 音声・データ統合ネットワークでさまざまなシェーパ機能

- VoIP パケットを優先し，クリアな音声を提供可能。

(5) ミッションクリティカル対応のネットワークを実現する高信頼性

● 高い装置品質

- 厳選した部品と厳しい設計・検査基準による装置の高い信頼性

● 多様な冗長ネットワーク構築

- 高速な経路切り替え
  リンクアグリゲーション（IEEE 802.3ad），高速スパニングツリー（IEEE 802.1w，IEEE 802.1s）などの標準機能，GSRP-aware や Autonomous Extensible Ring Protocol※（以降，Ring Protocol と呼びます。）などの独自機能で冗長化した高信頼ネットワークを構築可能。また，スパニングツリーを使用しない冗長構成が可能なアップリンク・リダンダントに対応

注※
本装置はトランジットノードだけサポートしています。Ring Protocol の詳細については，「21 Ring Protocol の解説【S2200】【SS1250】【SS1240】」を参照してください。なお，IP8800/S2100 シリーズは Ring Protocol 未サポートです。

● L2 ループ回避

- UDLD 機能によりスパニングツリーでのループ発生や，リンクアグリゲーションでのフレーム紛失などを未然に防ぐことが可能
- L2 ループ検知機能により，ネットワーク上の装置の誤接続を検知し，ループの発生を防ぐことが可能

(6) 優れたネットワーク管理，保守・運用

● CFM(Connectivity Fault Management)（Ether OAM）
Continuity Check（CC），Loopback，Linktrace による，レイヤ 2 レベルでの接続性監視や障害管理が可能

● 基本的な MIB-II に加え，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

● SD メモリカード※採用

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

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

● MC 運用モード機能【S2100】
MC へのソフトウェアと装置情報の一括保存，MC に保存したソフトウェアと装置情報からの起動が容易に実行可能

● 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

● 安定運用に適した装置冷却方式
装置前面吸気・背面排気（IP8800/S2200,IP8800/S2100），装置側面吸気・背面排気（IP8800/SS1240）の採用により，ラック搭載時に他装置の排熱の影響を受けにくく，安定した運用が可能

（7）FAN レス設計（IP8800/S2230-24T，IP8800/S2130-24T，IP8800/SS1250-24T2C，IP8800/SS1240-24T2C）

- 機器内に吸い込まれる埃によるトラブルの発生を軽減するとともに，騒音のない静かなオフィス環境を実現

（8）PoE 対応

● IP 電話機 , 無線 LAN AP などの PD（受電装置）を収容 (IP8800/S2230-24P，IP8800/S2130-24P，IP8800/SS1240-24P2C)

- 電力線配線工事をなくし , ケーブル増による煩わしさを減らすと同時に電力線配線コストを削減 , 工事期間の短縮を実現
- 最大供給電力 370.0W
- IEEE802.3af のフル給電（Class 3：15.4W）で，24 ポート同時給電可能
- IEEE802.3at（Class 4：30.0W）に対応し，Class 1 ～ Class 3 と任意に混在可能
- ポート 0/1 ～ 0/4 は 60W 給電機能に対応【S2200】

（9）コンパクト・環境負荷低減

● コンパクトな筐体

- 高さ 1 U サイズのコンパクトな筐体
- 10BASE-T/100BASE-TX を最大 48 ポート収容可能な高ポート密度

● RoHS 対応の環境負荷低減を実現

（10）省電力

● スケジュール機能

- 長期連休や土日，祝祭日，夜間などのスケジュール設定に従い，装置本体をスリープ状態に移行，およびスリープ状態からの復帰を自動で実施【SS1250】【SS1240】
- スケジュール設定で下記の LED 動作やポート省電力を組み合わせることが可能

● LED の動作を制御

- LED の動作を通常輝度，消灯の 2 段階で制御【S2200】【S2100】
- LED の動作を通常輝度，省電力輝度（通常輝度に対して減光状態で動作），消灯の 3 段階で制御【SS1250】【SS1240】
- 本装置にコンソール接続，ポートのリンクアップおよび，SD メモリカードの挿入時に LED を通常輝度で点灯および点滅させ，これらの操作終了後に自動で消灯に変更することも実現

● ポート省電力

- リンクダウンを検出したポートおよびポート閉塞（コンフィグレーションコマンドで shutdown に設

定）したポートを電力ダウンさせることで，省電力化を実現※

注※

SFP ポートは，ポート閉塞によるポート省電力だけをサポートします。

（11）OAN（Open Autonomic Networking）※への対応

● IT システムとの連携およびネットワーク運用・管理の自動化によって，運用効率向上を実現

- AX-Config-Master

  各装置のコンフィグレーションが不要になる自動コンフィグレーション。
  ネットワーク全体でのコンフィグレーションの整合性チェック。
  装置のコンフィグレーションの収集および配信のセキュリティ確保。

- AX-ON-API

  CLI，SNMP に代わる新しい装置制御手段。
  XML（Extensible Markup Language），SOAP（Simple Object Access Protocol），Netconf など，IT システムの標準技術をエンタプライズ向けネットワーク装置に導入。
  VLAN，インタフェース，リンクアグリゲーションなどの設定が可能。

注※

詳細は，マニュアル「OAN ユーザーズガイド　AX-Config-Master 編」を参照してください。

2 装置構成

この章では，本装置の各モデル構成要素や外観など，各装置本体について説明します。

2.1 **本装置のモデル**

2.2 **装置の構成要素**

2.1 本装置のモデル

本装置は高さを 1U に抑えたボックス型イーサネットスイッチで，IP8800/S2200，IP8800/S2100 では 10BASE-T/100BASE-TX/1000BASE-T を最大 24 ポート，IP8800/SS1250 では 10BASE-T/100BASE-TX を最大 24 ポート，IP8800/SS1240 では 10BASE-T/100BASE-TX ポートを最大 48 ポート装備します。

また，IP8800/SS1250 シリーズは，IP8800/SS1240 シリーズの機能を継承し，高信頼・耐環境強化（動作環境 50 ℃）をコンセプトにしています。

IP8800/S2200，IP8800/S2100，IP8800/SS1250，および IP8800/SS1240 は，リンクアグリゲーション，VLAN，スパニングツリー，DHCP snooping，IGMP/MLD snooping，レイヤ 2 認証機能を備えています。また，高度なフィルタ／ QoS 機能をサポートし，ワイヤレート／ノンブロッキングのスイッチングに対応します。

最大ポート数ごとの対応モデルを次の表に示します。

表 2-1 最大ポート数ごとの対応モデル

最大ポート数による分類※		対応モデル
10BASE-T/100BASE-TX/1000BASE-T 1000BASE-X	24 ポート 4 ポート	IP8800/S2230-24T
10BASE-T/100BASE-TX/1000BASE-T（PoE/PoE Plus） 10BASE-T/100BASE-TX/1000BASE-T（PoE/PoE Plus/60W 給電機能） 1000BASE-X	20 ポート 4 ポート 4 ポート	IP8800/S2230-24P
10BASE-T/100BASE-TX/1000BASE-T 1000BASE-X	24 ポート 4 ポート	IP8800/S2130-24T
10BASE-T/100BASE-TX/1000BASE-T（PoE/PoE Plus） 1000BASE-X	24 ポート 4 ポート	IP8800/S2130-24P
10BASE-T/100BASE-TX 10BASE-T/100BASE-TX/1000BASE-T または 1000BASE-X	24 ポート 2 ポート	IP8800/SS1250-24T2C IP8800/SS1240-24T2C
10BASE-T/100BASE-TX 10BASE-T/100BASE-TX/1000BASE-T または 1000BASE-X	48 ポート 2 ポート	IP8800/SS1240-48T2C
10BASE-T/100BASE-TX（PoE/PoE Plus） 10BASE-T/100BASE-TX/1000BASE-T または 1000BASE-X	24 ポート 2 ポート	IP8800/SS1240-24P2C

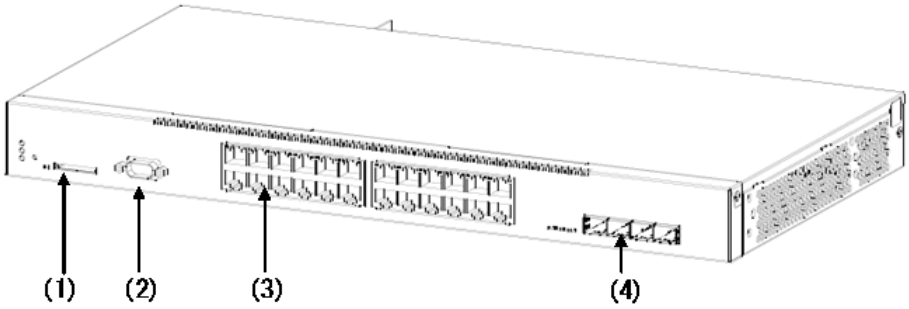
注※
同時に使用できる最大ポート数については，「3.1 搭載条件」を参照してください。

2.1.1 装置の外観

装置外観図を次の図に示します。各部位の詳細は，「ハードウェア取扱説明書」を参照してください。

（1） IP8800/S2200 シリーズ

図 2-1　IP8800/S2230-24T **モデル**



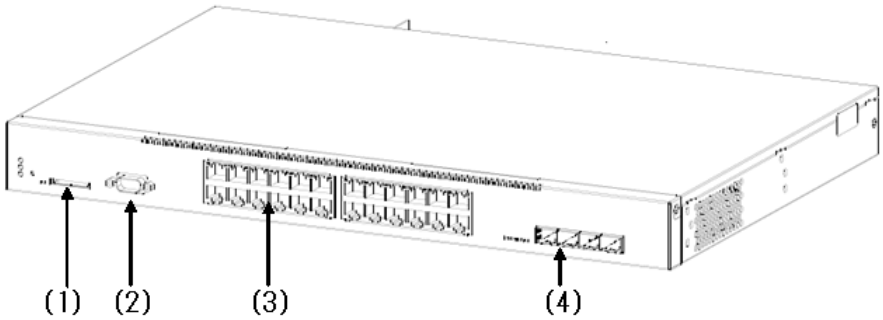
(1)　メモリカードスロット

(2)　CONSOLE ポート

(3)　10BASE-T/100BASE-TX/1000BASE-T イーサネットポート

(4)　SFP スロット

図 2-2　IP8800/S2230-24P **モデル**



(1)　メモリカードスロット

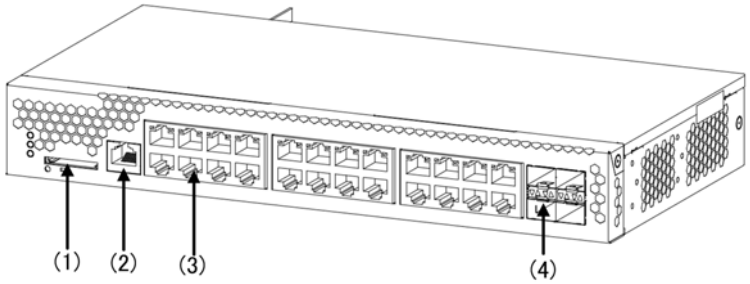
(2)　CONSOLE ポート

(3)　10BASE-T/100BASE-TX/1000BASE-T イーサネットポート

(4)　SFP スロット

（2）IP8800/S2100 シリーズ

図 2-3　IP8800/S2130-24T **モデル**



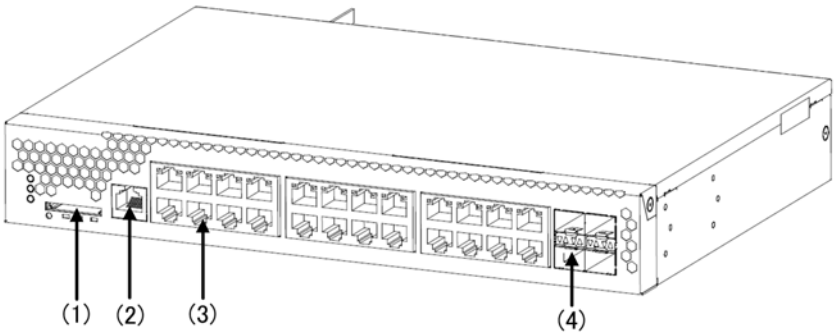
(1)　メモリカードスロット

(2)　CONSOLE ポート

(3)　10BASE-T/100BASE-TX/1000BASE-T イーサネットポート

(4)　SFP スロット

図 2-4　IP8800/S2130-24P **モデル**



(1)　メモリカードスロット

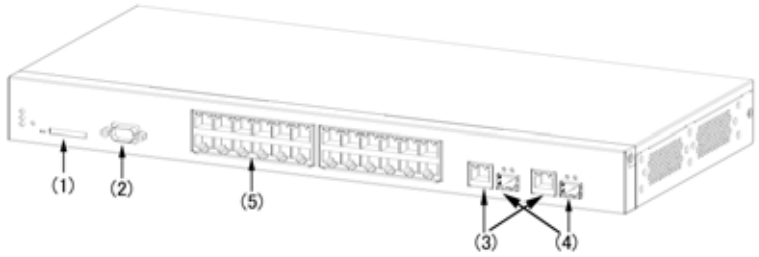
(2)　CONSOLE ポート

(3)　10BASE-T/100BASE-TX/1000BASE-T イーサネットポート

(4)　SFP スロット

（3）IP8800/SS1250 シリーズ

図 2-5　IP8800/SS1250-24T2C **モデル**



(1)　メモリカードスロット

(2)　CONSOLE ポート

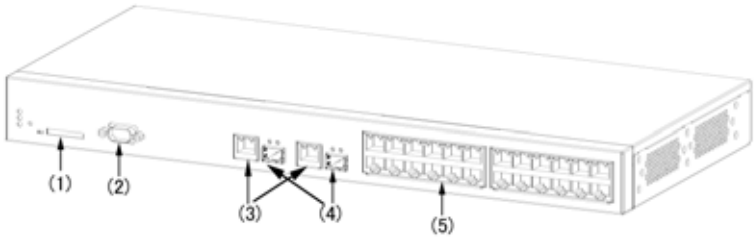
(3)　10BASE-T/100BASE-TX/1000BASE-T イーサネットポート

(4)　SFP スロット

(5)　10BASE-T/100BASE-TX イーサネットポート

（4）IP8800/SS1240 シリーズ

図 2-6　IP8800/SS1240-24T2C **モデル**



(1)　メモリカードスロット

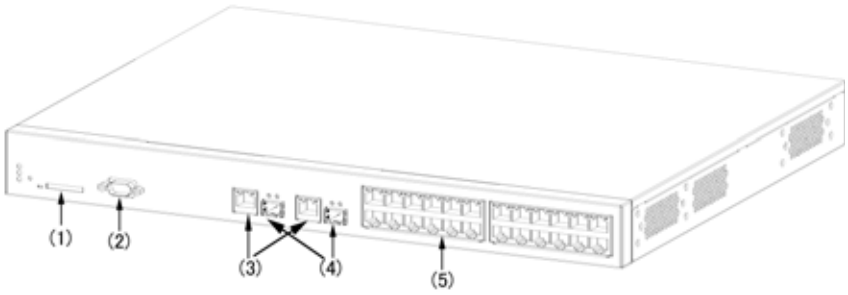
(2)　CONSOLE ポート

(3)　10BASE-T/100BASE-TX/1000BASE-T イーサネットポート

(4)　SFP スロット

(5)　10BASE-T/100BASE-TX イーサネットポート

図 2-7　IP8800/SS1240-24P2C **モデル**



(1)　メモリカードスロット

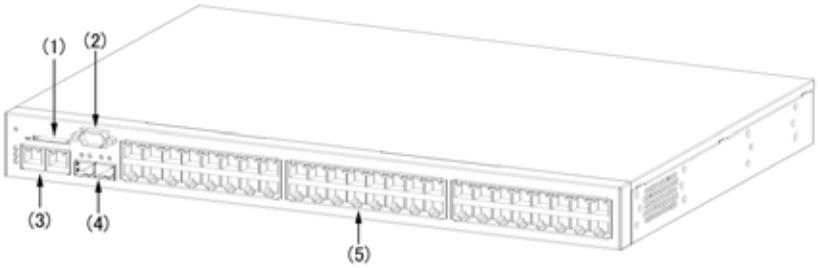
(2)　CONSOLE ポート

(3)　10BASE-T/100BASE-TX/1000BASE-T イーサネットポート

(4)　SFP スロット

(5)　10BASE-T/100BASE-TX イーサネットポート

図 2-8　IP8800/SS1240-48T2C **モデル**



(1)　メモリカードスロット

(2)　CONSOLE ポート

(3)　10BASE-T/100BASE-TX/1000BASE-T イーサネットポート

(4)　SFP スロット

(5)　10BASE-T/100BASE-TX イーサネットポート

2.2 装置の構成要素

2.2.1 ハードウェア

本装置の各モデルは，統一したアーキテクチャで設計しています。

ハードウェアの構成を次の図に示します。

(1) IP8800/S2200 シリーズ

図 2-9 ハードウェアの構成（IP8800/S2230-24T モデル）

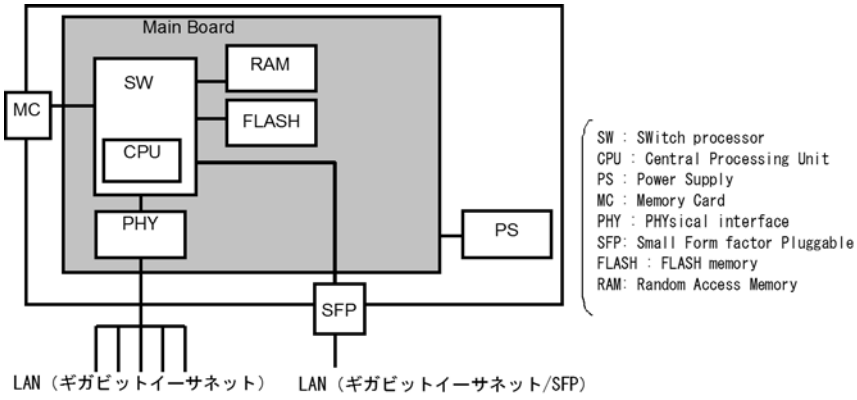
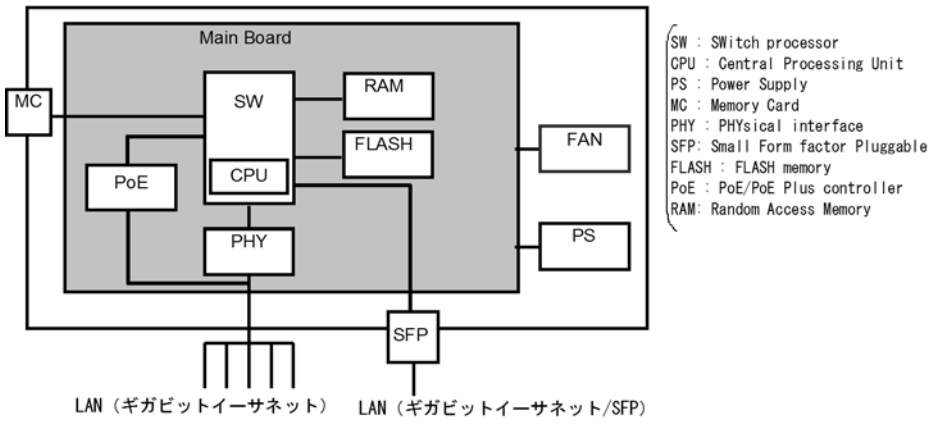


図 2-10 ハードウェアの構成（IP8800/S2230-24P モデル）



装置筐体には，メインボード，PS，FAN が含まれています。

(a) メインボード

メインボードは CPU 部，SW 部，MC，FLASH 部，PHY 部，PoE 部から構成されます。

- CPU 部（Central Processing Unit）
  装置全体の管理，PHY 部の制御 , 各種プロトコル処理をソフトウェアで行います。
  ソフトウェアは FLASH 部に搭載される内蔵フラッシュメモリに格納されます。
- SW（Switch processor）
  L2 フレームのスイッチングを行います。SW 部はハードウェアによる MAC アドレス学習 / エージング，リンクアグリゲーション，フィルタ /QoS テーブル検索，自宛 / 自発フレームの DMA 転送を行い

ます。これによって高速なフレームのスイッチングを実現します。

- MC（Memory Card）
  MC スロットです。
  MC には SD カードを使用しており，コンフィグレーションファイルの格納，障害情報の保存に用います。
- FLASH 部（FLASH memory）
  ソフトウェア／コンフィグレーションファイル／ログ情報が格納されます。
- PHY 部（Physical Interface）
  各種メディア対応のインタフェース部です。
- PoE/PoE Plus/PoE(60W 給電機能) 部（IP8800/S2230-24P モデル）
  ギガビットイーサネットポートで，受電装置に最大 60W/ ポート (ポート 0/1 ～ 0/4)，最大 30W/ ポート (ポート 0/5 ～ 0/24) の電力を給電します。

(b) PS（Power Supply）

PS は外部供給電源から本装置内で使用する直流電源を生成します。PS を交換する場合は，本装置を停止させ，本装置自体を交換する必要があります。

(c) FAN（IP8800/S2230-24P モデル）

本装置は装置内部を冷却するための FAN を装備します。

(2) IP8800/S2100 シリーズ

図 2-11 ハードウェアの構成（IP8800/S2130-24T モデル）

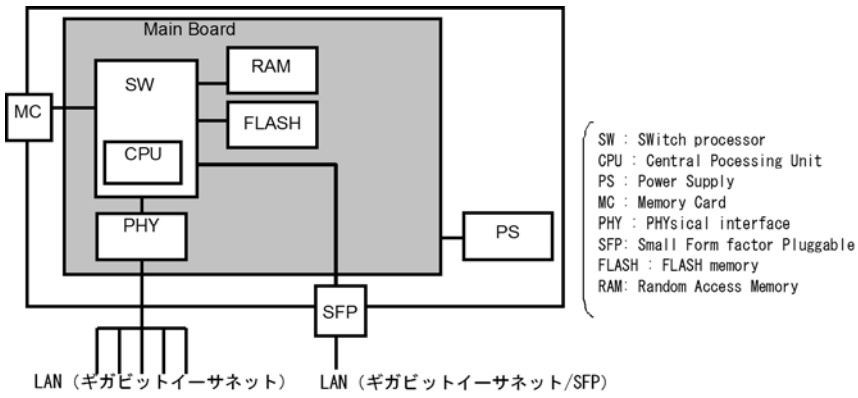
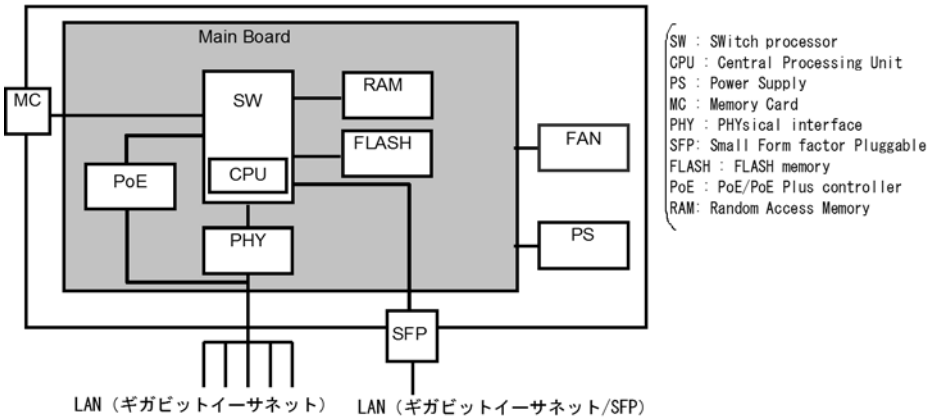


図 2-12 ハードウェアの構成（IP8800/S2130-24P モデル）



装置筐体には，メインボード，PS，FAN が含まれています。

(a) メインボード

メインボードは CPU 部，SW 部，MC，FLASH 部，PHY 部，PoE 部から構成されます。

- CPU 部（Central Processing Unit）
  装置全体の管理，PHY 部の制御 , 各種プロトコル処理をソフトウェアで行います。
  ソフトウェアは FLASH 部に搭載される内蔵フラッシュメモリに格納されます。
- SW（Switch processor）
  L2 フレームのスイッチングを行います。SW 部はハードウェアによる MAC アドレス学習 / エージング，リンクアグリゲーション，フィルタ /QoS テーブル検索，自宛 / 自発フレームの DMA 転送を行います。これによって高速なフレームのスイッチングを実現します。
- MC（Memory Card）
  MC スロットです。
  MC には SD カードを使用しており，コンフィグレーションファイルの格納，障害情報の保存に用います。
- FLASH 部（FLASH memory）
  ソフトウェア／コンフィグレーションファイル／ログ情報が格納されます。
- PHY 部（Physical Interface）
  各種メディア対応のインタフェース部です。
- PoE/PoE Plus 部（IP8800/S2130-24P モデル）
  ギガビットイーサネットポートで，受電装置に最大 30W/ ポート (ポート 0/1 ～ 0/24) の電力を給電します。

(b) PS（Power Supply）

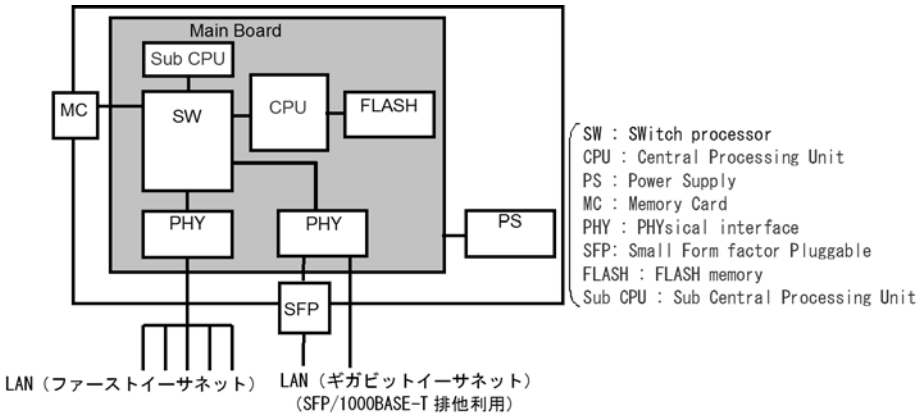
PS は外部供給電源から本装置内で使用する直流電源を生成します。PS を交換する場合は，本装置を停止させ，本装置自体を交換する必要があります。

(c) FAN（IP8800/S2130-24P モデル）

本装置は装置内部を冷却するための FAN を装備します。

(3) IP8800/SS1250 シリーズ

図 2-13　ハードウェアの構成（IP8800/SS1250-24T2C モデル）



装置筐体には，メインボード，PS が含まれています。

(a) メインボード

メインボードは CPU 部，SW 部，MC，FLASH 部，PHY 部，Sub CPU 部から構成されます。

- CPU 部（Central Processing Unit）
  装置全体の管理，PHY 部の制御 , 各種プロトコル処理をソフトウェアで行います。
  ソフトウェアは FLASH 部に搭載される内蔵フラッシュメモリに格納されます。
- SW（Switch processor）
  L2 フレームのスイッチングを行います。SW 部はハードウェアによる MAC アドレス学習 / エージング，リンクアグリゲーション，フィルタ /QoS テーブル検索，自宛 / 自発フレームの DMA 転送を行います。これによって高速なフレームのスイッチングを実現します。
- MC（Memory Card）
  MC スロットです。
  MC には SD カードを使用しており，コンフィグレーションファイルの格納，障害情報の保存に用います。
- FLASH 部（FLASH memory）
  ソフトウェア／コンフィグレーションファイル／ログ情報が格納されます。
- PHY 部（Physical Interface）
  各種メディア対応のインタフェース部です。
- Sub CPU 部（Sub Central Processing Unit）
  温度センサ監視を行います。

(b) PS（Power Supply）

PS は外部供給電源から本装置内で使用する直流電源を生成します。PS を交換する場合は，本装置を停止させ，本装置自体を交換する必要があります。

(4) IP8800/SS1240 シリーズ

図 2-14　ハードウェアの構成（IP8800/SS1240-24T2C モデル）

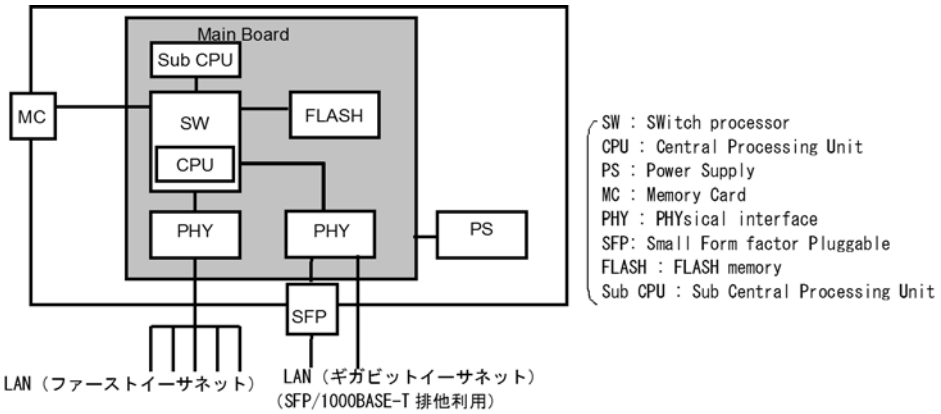


図 2-15 ハードウェアの構成（IP8800/SS1240-24P2C モデル）

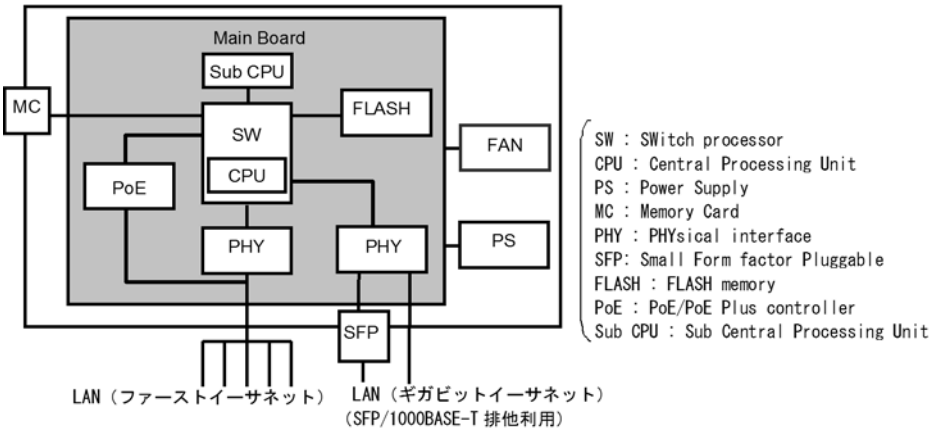
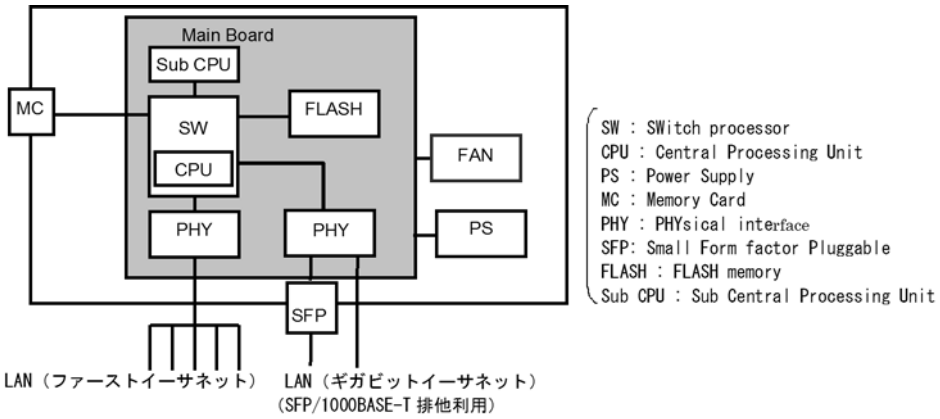


図 2-16 ハードウェアの構成（IP8800/SS1240-48T2C モデル）



装置筐体には，メインボード，PS，FAN が含まれています。

(a) メインボード

メインボードは SW 部，MC，FLASH 部，PHY 部，Sub CPU 部，PoE 部から構成されます。

- CPU 部（Central Processing Unit）
  装置全体の管理，PHY 部の制御 , 各種プロトコル処理をソフトウェアで行います。
  ソフトウェアは FLASH 部に搭載される内蔵フラッシュメモリに格納されます。
- SW（Switch processor）
  L2 フレームのスイッチングを行います。SW 部はハードウェアによる MAC アドレス学習 / エージング，リンクアグリゲーション，フィルタ /QoS テーブル検索，自宛 / 自発フレームの DMA 転送を行います。これによって高速なフレームのスイッチングを実現します。
- MC（Memory Card）
  MC スロットです。MC には SD カードを使用しており，コンフィグレーションファイルの格納，障害情報の保存に用います。
- FLASH 部（FLASH memory）
  ソフトウェア／コンフィグレーションファイル／ログ情報が格納されます。
- PHY 部（Physical Interface）
  各種メディア対応のインタフェース部です。
- Sub CPU 部（Sub Central Processing Unit）
  温度センサ監視を行います。

- PoE/PoE Plus 部（IP8800/SS1240-24P2C モデル）
  ファーストイーサネットポート，受電装置に最大 30W/ ポートの電力を供給します。

(b) PS（Power Supply）

PS は外部供給電源から本装置内で使用する直流電源を生成します。PS を交換する場合は，本装置を停止させ，本装置自体を交換する必要があります。

(c) FAN（IP8800/SS1240-24P2C，IP8800/SS1240-48T2C モデル）

本装置は装置内部を冷却するための FAN を装備します。

2.2.2 ソフトウェア

本装置のモデルとソフトウェアの対応を次の表に示します。

表 2-2 本装置のモデルとソフトウェアの対応

モデル	ソフトウェア略称	内容
IP8800/S2200	OS-LT4	IP8800/S2200 用ソフトウェア L2 スイッチ中継，VLAN，スパニングツリー，SNMP，LLDP ほか
IP8800/S2100	OS-LT5	IP8800/S2100 用ソフトウェア L2 スイッチ中継，VLAN，スパニングツリー，SNMP，LLDP ほか
IP8800/SS1250	OS-LT3	IP8800/SS1250 用ソフトウェア L2 スイッチ中継，VLAN，スパニングツリー，SNMP，LLDP ほか
IP8800/SS1240	OS-LT2	IP8800/SS1240 用ソフトウェア L2 スイッチ中継，VLAN，スパニングツリー，SNMP，LLDP ほか

本装置のオプションライセンスを次の表に示します。オプションライセンスは IP8800/S2200，IP8800/SS1250 および IP8800/SS1240 共通です。（IP8800/S2100 はオプションライセンス未サポートです。）

表 2-3 本装置のオプションライセンス一覧

オプションライセンス略称	内容
OP-WOL	セキュア Wake on LAN
OP-OTP	ワンタイムパスワード認証

3 収容条件

この章では，収容条件について説明します。

3.1 **搭載条件**

3.2 **収容条件**

3.1 搭載条件

3.1.1 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 3-1 最大収容可能回線数

モデル	イーサネット						
	10/100BASE-TX	10/100BASE-TX	10/100/1000BASE-T			100BASE-FX 1000BASE-X	1000BASE-X
	UTP	PoE/PoE Plus	UTP	PoE/PoE Plus	PoE/PoE Plus/60W 給電機能	SFP	SFP
IP8800/S2230-24T	―	―	24	―	―	―	4
IP8800/S2230-24P	―	―	―	20	4	―	4
IP8800/S2130-24T	―	―	24	―	―	―	4
IP8800/S2130-24P	―	―	―	24	―	―	4
IP8800/SS1250-24T2C	24	―	2※	―	―	2※	―
IP8800/SS1240-24T2C	24	―	2※	―	―	―	2※
IP8800/SS1240-24P2C	―	24	2※	―	―	―	2※
IP8800/SS1240-48T2C	48	―	2※	―	―	―	2※

（凡例）―：該当なし。

注※

排他使用（同時使用不可）です。

10BASE-T/100BASE-TX/1000BASE-T を使用した場合は，その使用回線数をマイナスした値が SFP の収容回線数になります。

3.1.2 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 3-2　メインボード搭載メモリ量と内蔵フラッシュメモリ・MC 容量

項目	IP8800/S2200 シリーズ	IP8800/S2100 シリーズ	IP8800/SS1250 シリーズ	IP8800/SS1240 シリーズ
メインボード搭載メモリ量 (RAMDISK 含む)	128MB（内，RAMDISK は 12MB）	128MB（内，RAMDISK は 12MB）	128MB（内，RAMDISK は 12MB）	128MB（内，RAMDISK は 12MB）
内蔵フラッシュメモリ容量	16MB	16MB	16MB	16MB

（1） RAMDISK について

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

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

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

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

なお，本装置を再起動すると，RAMDISK 上のファイルは削除されます。

3.2 収容条件

3.2.1 ログインセキュリティと RADIUS

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

表 3-3 リモート運用端末から本装置への最大ログイン数

モデル	telnet	ftp
全モデル共通	2	1

表 3-4 RADIUS サーバ情報登録数

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

（凡例）－：未サポート

3.2.2 リンクアグリゲーション

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

表 3-5 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	8

3.2.3 レイヤ 2 スイッチ機能

(1) MAC アドレステーブル

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

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

表 3-6 MAC アドレステーブルに登録できる MAC アドレスのエントリ数

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	16384※	256

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

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

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

（2）VLAN

コンフィグレーションによって設定できる VLAN の数を次の表に示します。

表 3-7　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
IP8800/S2230-24T IP8800/S2230-24P IP8800/S2130-24T IP8800/S2130-24P	256	256	7168
IP8800/SS1250-24T2C IP8800/SS1240-24T2C IP8800/SS1240-24P2C	256	256	6656
IP8800/SS1240-48T2C	256	256	12800

注
推奨する VLAN 数は 256 以下です。
ポートごと VLAN 数の装置での合計は，ポートに設定している VLAN の数を，装置の全ポートで合計した値です。例えば，24 ポートの装置で，ポート 1 からポート 10 では設定している VLAN 数が 200，ポート 11 からポート 24 では設定している VLAN 数が 1 の場合，ポートごと VLAN 数の装置での合計は 2014 となります。ポートごと VLAN 数の装置での合計が収容条件を超えた場合，CPU の利用率が高くなり，コンフィグレーションコマンドや運用コマンドのレスポンスが遅くなったり，実行できなくなったりすることがあります。

本装置で設定できる最大 VLAN 数は 256 ですが，そのうち IP アドレスを設定できる VLAN（VLAN インタフェース）数は最大 128 です。

(a) プロトコル VLAN

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

表 3-8　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 3-9　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 数です。プロトコルポートに設定できるプロトコル VLAN 数は 16 です。

(b) MAC VLAN

MAC VLAN の収容条件を次の表に示します。

表 3-10 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	64	256※	320

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

(3) スパニングツリー

スパニングツリーの収容条件を種類ごとに次の表に示します。

表 3-11 PVST+ の収容条件

モデル	対象 VLAN 数	VLAN ポート数※1
全モデル共通	250	256※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 3-12 シングルスパニングツリーの収容条件

モデル	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	256※3	1024	256

注※ 1
スパニングツリー対象となる各 VLAN に設定するポート数の合計（VLAN 数とポート数の積）。
例えば，100 個の VLAN を設定し，それぞれの VLAN に 2 回線が所属している場合，ポート数は 100 × 2 ＝ 200 となります。

注※ 2
PVST+ の対象ポートを含む合計の最大値が 256 となります。

注※ 3
PVST+ 同時動作時は PVST+ 対象 VLAN 数を引いた値となります。

表 3-13 マルチプルスパニングツリーの収容条件

モデル	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	256	1024	16	200

注※ 1

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

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

注※ 2

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

（4） Ring Protocol【S2200】【SS1250】【SS1240】

（a） Ring Protocol

Ring Protocol の収容条件を次の表に示します。

表 3-14 Ring Protocol の収容条件

項目	リング当たり	装置当たり
リング数	－	4
VLAN マッピング数	－	128
VLAN グループ数	2	8
VLAN グループの VLAN 数	255※1※3	255※1※3
リングポート数※2	2	8

（凡例）－：該当なし

注※ 1

装置として推奨する VLAN の最大数です。

本装置の VLAN 数は最大 256 ですが，リング当たりに制御 VLAN 用として VLAN を一つ消費するため，VLAN グループに使用できる VLAN の最大数は 255 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。

注※ 3

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

（b） 仮想リンク

本装置は仮想リンク設定をサポートしていません。（仮想リンク制御フレームの中継およびフラッシュ制御フレームの受信だけをサポートします。）

（c） 多重障害監視機能

多重障害監視機能の収容条件を次の表に示します。

表 3-15 多重障害監視機能の収容条件

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

（5） IGMP snooping ／ MLD snooping

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

表 3-16 IGMP/MLD snooping の収容条件

項目	最大数
設定 VLAN 数※1※3	32
登録エントリ数※2※3	500

注※1
IGMP/MLD snooping が動作するポート数（IGMP/MLD snooping を設定した VLAN に収容されるポートの総和）は装置全体で最大 512 です。例えば，各々 10 ポート収容している 16 個の VLAN で IGMP/MLD snooping を動作させる場合，IGMP/MLD snooping 動作ポート数は 160 となります。

注※2
各 VLAN で学習したマルチキャスト MAC アドレスの総和です。

注※3
各エントリ数は IGMP/MLD snooping で使用するエントリの合計値となります。同一 VLAN で IGMP/MLD snooping の両方を設定した場合，設定 VLAN 数は 2 となります。

3.2.4 IP インタフェース

本装置では VLAN に対して IP アドレスを設定します。ここでは，IP アドレスを設定できる VLAN インタフェースの最大数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。

（1） 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。

表 3-17 最大インタフェース数

モデル	最大インタフェース数（装置当たり）
全モデル共通	128

（2） マルチホームの最大サブネット数

本装置はマルチホームをサポートしていません。

（3） IP アドレス最大設定数

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

表 3-18 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	コンフィグレーションで設定可能な IPv4 アドレス最大数（装置当たり）
全モデル共通	128

(4) 最大相手装置数

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

(a) ARP エントリ数

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

表 3-19 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	2048	2048

(5) ダイナミックエントリ，スタティックエントリの最大エントリ数

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

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

表 3-20 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	128※	－	128※

（凡例）－：未サポート
注※ ダイレクト経路は含みません。

3.2.5 フィルタ・QoS

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

フィルタ・QoS の検出条件によるリソース配分を決定するために，フィルタおよび QoS 共通モードであるフロー検出モードを選択します。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。フィルタおよび QoS は，受信側でだけ設定できます。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。

(1) 受信側フィルタエントリ数

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

エントリ数を次の表に示します。フロー検出条件は選択するモードによって決まり，layer2-1 の場合は MAC 条件を，layer2-2 の場合は IPv4 条件を使用できます。

表 3-21　モード layer2-1，layer2-2 の受信側フィルタ最大エントリ数

モデル	受信側フィルタ最大エントリ数※		
	インタフェース種別	インタフェースあたり	装置あたり
全モデル共通	イーサネット	128	128
	VLAN	128	128

注※

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

（例 1）

エントリ条件 ：イーサネットインタフェース 0/1 に 1 エントリ設定

エントリ数　：設定エントリ (1) とイーサネットインタフェース 0/1 の廃棄エントリ (1) の合計 2 エントリを使用する

残エントリ数 ：126 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：121 エントリ使用可能

(2) 受信側 QoS エントリ数

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

表 3-22　モード layer2-1，layer2-2 の受信側 QoS 最大エントリ数

モデル	受信側 QoS 最大エントリ数		
	インタフェース種別	インタフェースあたり	装置あたり
全モデル共通	イーサネット	64	64
	VLAN	64	64

3.2.6 レイヤ 2 認証機能

(1) レイヤ 2 認証共通

装置全体の認証端末数を次の表に示します。

表 3-23 装置全体の認証端末数※

認証モード	認証機能	認証機能ごとの端末数	装置全体
固定 VLAN モード	IEEE802.1X	256	
	Web 認証	1024	
	MAC 認証	1024	
	固定 VLAN モード全体での最大認証端末数		1024
ダイナミック VLAN モード レガシーモード	IEEE802.1X	256	
	Web 認証	256	
	MAC 認証	256	
	ダイナミック VLAN モード・レガシーモード全体での最大認証端末数		256
装置全体での全認証機能／認証モードの合計最大端末数			1280

注※
DHCP snooping 機能を併用している場合は，最大 246 に制限されます。

表 3-24 その他のレイヤ２認証共通機能収容条件

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

注※ 1
ログインセキュリティ機能を含む装置全体での登録数です。

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

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

(2) IEEE802.1X

IEEE802.1X の収容条件を次の表に示します。

表 3-25 IEEE802.1X の最大認証端末数※1

認証モード		ポート単位		VLAN 単位		装置全体	
		最大端末数	認証数制限の設定※2	最大端末数	認証数制限の設定※2	最大端末数	認証数制限の設定※2
ポート単位認証	(静的)	64	不可			256	不可
	(動的)	64	不可			256	不可
VLAN 単位認証	(動的)			256	不可	256	不可
IEEE802.1X 認証全体での最大端末数 (ポート単位／ VLAN 単位認証合計)						256	不可

注※1

DHCP snooping 機能を併用している場合は，最大 246 に制限されます。

注※2

IEEE802.1X では，認証数制限を設定できません。

表 3-26 IEEE802.1X の収容条件

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

注※1

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

注※2

MAC アドレステーブルのスタティックエントリ数です。

注※3

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

(3) Web 認証【S2200】【SS1250】【SS1240】

Web 認証の収容条件を次の表に示します。

表 3-27 Web 認証の最大ユーザ数※1

認証モード	ポート単位		VLAN 単位		装置全体	
	最大ユーザ数	認証数制限の設定	最大ユーザ数	認証数制限の設定	最大ユーザ数	認証数制限の設定
固定 VLAN モード	1024	可			1024	可
ダイナミック VLAN モード	256	可			256	可
レガシーモード			256	不可	256	可
Web 認証全体での最大ユーザ数（固定 VLAN モード・ダイナミック VLAN モード・レガシーモード合計）					1280	不可※2

注※ 1

DHCP snooping 機能を併用している場合は，最大 246 に制限されます。

注※ 2

各認証モードを合計した Web 認証全体の認証数制限は設定できません。

表 3-28 Web 認証の収容条件

項目		最大数
認証方式グループ登録数	装置デフォルト	1
	認証方式リスト	4
Web 認証専用 RADIUS サーバ登録数※1		4
内蔵 Web 認証 DB 登録ユーザ数		300※2
Web 認証画面入れ替えで指定できるファイルの合計サイズ		256kB ／装置※3
	Web 認証画面のカスタムファイルセット※4 登録数	5 ／装置 内訳 • 基本 Web 認証画面：1 • 個別 Web 認証画面：4
	1 ファイルセットあたりのファイル数	64
DHCP サーバ機能	アドレスプール数 (network)	32
	アドレスプール数 (host/mac)	×（未サポート）
	配布可能 IP アドレス数	512
	配布除外アドレス数	64

注※ 1

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

注※ 2

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

注※ 3
基本 Web 認証画面および個別 Web 認証画面すべての合計です。なお，ファイル領域には管理領域も含んでいますので，実動上は 240kB となります。また，ファイルサイズによってはさらに少ない領域となる場合があります。

注※ 4
カスタムファイルセットについては，「コンフィグレーションガイド Vol.2 8 Web 認証の解説」を参照してください。

(4) MAC 認証

MAC 認証の収容条件を次の表に示します。

表 3-29 MAC 認証の最大認証端末数※ 1

認証モード	ポート単位		VLAN 単位		装置全体	
	最大端末数	認証数制限の設定	最大端末数	認証数制限の設定	最大端末数	認証数制限の設定
固定 VLAN モード	1024	可			1024	可
ダイナミック VLAN モード	256	可			256	可
レガシーモード			256	不可	256	可
MAC 認証全体での最大端末数（固定 VLAN モード・ダイナミック VLAN モード・レガシーモード合計）					1280	不可※ 2

注※ 1
DHCP snooping 機能を併用している場合は，最大 246 に制限されます。

注※ 2
各認証モードを合計した MAC 認証全体の認証数制限は設定できません。

表 3-30 MAC 認証の収容条件

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

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

(5) セキュア Wake on LAN【OP-WOL】

セキュア Wake on LAN の収容条件を次の表に示します。

表 3-31 セキュア Wake on LAN の収容条件

項目	最大数
同時使用可能ユーザ数	32※ 1
起動コマンド送信端末登録用内蔵 DB の登録可能端末数	300

項目	最大数
ユーザ認証用内蔵 DB の登録可能端末数	300
ユーザと端末の組み合わせ数	300※2

注※ 1

セキュア Wake on LAN 機能のユーザ認証から端末起動確認完了までを，1 ユーザとして管理します。
このため，起動コマンド送信端末登録用内蔵 DB の起動確認タイムアウト値が長いときに，同時使用者数の管理エントリが飽和してセキュア Wake on LAN 機能を使用できなくなる可能性があります。

注※ 2

ユーザと端末の組み合わせ数は最大 300 です。例えば，1 ユーザに 300 端末のアクセス権を設定した場合，その他ユーザへの端末アクセス権を設定できません。なお，"any" と "manual" 設定は本制限から除外されます。

3.2.7 セキュリティ

（1） DHCP snooping

DHCP snooping の収容条件を次の表に示します。

表 3-32 DHCP snooping の収容条件

項目	最大数
設定 VLAN 数	32
バインディングデータベースエントリ総数	246
バインディングデータベーススタティックエントリ数※	64

注※

スタティックエントリ数は，バインディングデータベースエントリ総数に含まれます。

3.2.8 冗長化構成による高信頼化機能

（1） アップリンク・リダンダント

アップリンク・リダンダントの収容条件を次の表に示します。

表 3-33 アップリンク・リダンダントの収容条件

モデル	アップリンクポート数	アップリンクポート当たりの収容インタフェース数
IP8800/S2230-24T IP8800/S2230-24P IP8800/S2130-24T IP8800/S2130-24P	14	2
IP8800/SS1250-24T2C IP8800/SS1240-24T2C IP8800/SS1240-24P2C	13	2
IP8800/SS1240-48T2C	25	2

表 3-34 MAC アドレスアップデート機能の収容条件

モデル	最大送信 MAC アドレスエントリ数
全モデル共通	1024

3.2.9 ネットワークの障害検出による高信頼化機能

（1） IEEE802.3ah/UDLD

IEEE802.3ah/UDLD の収容条件を次の表に示します。

表 3-35 IEEE802.3ah/UDLD の収容条件

モデル	最大リンク監視情報数
全モデル共通	装置の最大物理ポート数

（2） L2 ループ検知

L2 ループ検知フレーム送信レートを次の表に示します。

表 3-36 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送信レート（装置当たり）
全モデル共通	20（packet/ 秒）※ 1

L2 ループ検知フレームを送信可能なポート数および VLAN 数の算出式

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

注※ 1

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

注※ 2

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

（3） CFM

CFM の収容条件を次の表に示します。

表 3-37 CFM の収容条件

モデル	ドメイン数	MA 数	MEP 数	MIP 数	CFM ポート総数※ 1 ※ 2	リモート MEP 総数※ 2 ※ 3
全モデル共通	8 ／装置	32 ／装置	32 ／装置	32 ／装置	256 ／装置	2016 ／装置

注※ 1

CFM ポート総数とは，MA のプライマリ VLAN のうち，CFM のフレームを送信する VLAN ポートの総数です。

Down MEP だけの MA の場合

Down MEP の VLAN ポートの総数

Up MEP を含む MA の場合

プライマリ VLAN の全 VLAN ポートの総数

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。なお，CFM ポート総数は運用コマンド show cfm summary で確認できます。

注※ 2

CFM ポート総数およびリモート MEP 総数は，CCM 送信間隔がデフォルト値のときの収容条件です。CCM 送信間隔を変更すると，CFM ポート総およびリモート MEP 総数の収容条件が変わります。CCM 送信間隔による CFM ポート総数およびリモート MEP 総数の収容条件を次の表に示します。

表 3-38　CCM 送信間隔による収容条件

モデル	CCM 送信間隔	CFM ポート総数	リモート MEP 総数
全モデル共通	1 分以上	256 ／装置	2016 ／装置
	10 秒	100 ／装置	640 ／装置
	1 秒	50 ／装置	64 ／装置

注※ 3

リモート MEP 総数とは，自装置以外の MEP の総数です。MEP からの CCM 受信性能に影響します。リモート MEP 総数は運用コマンド show cfm remote-mep で確認できます。

表 3-39　CFM の物理ポートおよびチャネルグループの収容条件

モデル	MEP・MIP を設定可能な物理ポートおよびチャネルグループの総数※
全モデル共通	8 ／装置

注※

MEP・MIP は同一ポートに対して複数設定できます。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。

表 3-40　CFM のデータベース収容条件

モデル	MEP CCM データベースエントリ数	MIP CCM データベースエントリ数	Linktrace データベースエントリ数※
全モデル共通	63 ／ MEP	2048 ／装置	1024 ／装置 256 ／ルート

注※

1 ルート当たり最大 256 装置分の情報を保持します。1 ルート当たり 256 装置の情報を保持する場合は，最大で 4 ルート分を保持します（1024 ÷ 256 装置＝ 4 ルート）。

3.2.10　隣接装置情報（LLDP）

隣接装置情報（LLDP）の収容条件を次の表に示します。

表 3-41　隣接装置情報（LLDP）の収容条件

モデル	項目	最大収容数
IP8800/S2230-24T IP8800/S2230-24P IP8800/S2130-24T IP8800/S2130-24P	LLDP 隣接装置情報	28
IP8800/SS1250-24T2C IP8800/SS1240-24T2C IP8800/SS1240-24P2C IP8800/SS1240-48T2C	LLDP 隣接装置情報	50

4 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。

4.1 **運用端末による管理**

4.2 **装置起動**

4.3 **ログイン・ログアウト**

4.1 運用端末による管理

4.1.1 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 RS-232C に接続する端末，リモート運用端末は IP ネットワーク経由で接続する端末です。また，本装置は IP ネットワーク経由で SNMP マネージャによるネットワーク管理にも対応しています。運用端末の接続形態を「図 4-1　運用端末の接続形態」に，運用端末の条件を「表 4-1　運用端末の条件」に示します。

図 4-1　運用端末の接続形態

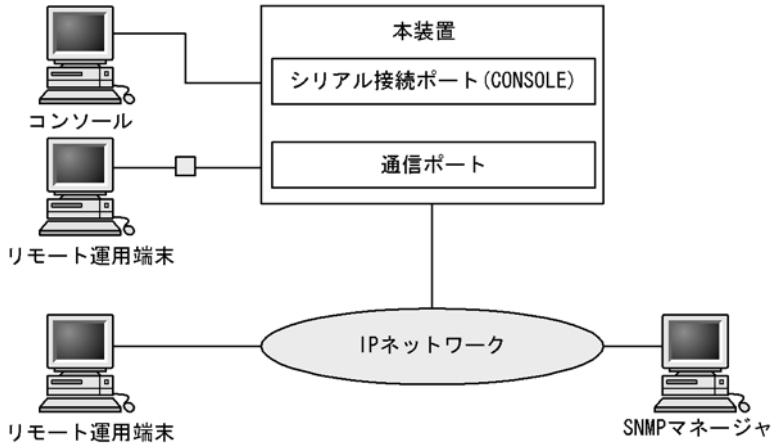


表 4-1　運用端末の条件

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

! 注意事項

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

(1) コンソール

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

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

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

図 4-2　コンソールの通信速度の設定例

```
> line console speed 19200 save
Do you wish to continue? (y/n): y
```

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 VT100 の制御文字を使用して画面サイズを取得・設定します。VT100 に対応していないコンソール端末では，不正な文字列を表示したり，最初の CLI プロンプトをずれて表示したりして，画面サイズを取得・設定できません。コンソール端末は，端末運用モード：VT100 でご使用ください。
また，ログインと同時にキー入力した場合，VT100 の制御文字の表示結果が正常に取得できないため同様の現象となりますのでご注意ください。この場合は，再度ログインし直してください。

(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すべてリモート運用端末として使用できます。

注意事項

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

4.1.2 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 4-2　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	なし	ftp
IP 通信	不可	IPv4
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。

4.1.3 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 4-3 運用管理の種類

運用機能	概要
コマンド入力機能	コマンドラインによる入力を受け付けます。
ログイン制御機能	不正アクセス防止，パスワードチェックを行います。
コンフィグレーション編集機能	運用のためのコンフィグレーションを設定します。設定された情報はすぐ運用に反映されます。
ネットワークコマンド機能	Telnet ログインによるリモート操作をサポートします。
ログ・統計情報	過去に発生した障害情報およびパケットカウンタなどの統計情報を表示します。
LED および障害部位の表示	LED によって本装置の状態を表示します。
MIB 情報収集	SNMP マネージャによるネットワーク管理を行います。
装置保守機能	装置を保守するための状態表示，装置とネットワークの障害を切り分けるための回線診断などのコマンドを持ちます。
MC 保守機能	MC のフォーマットなどを行います。

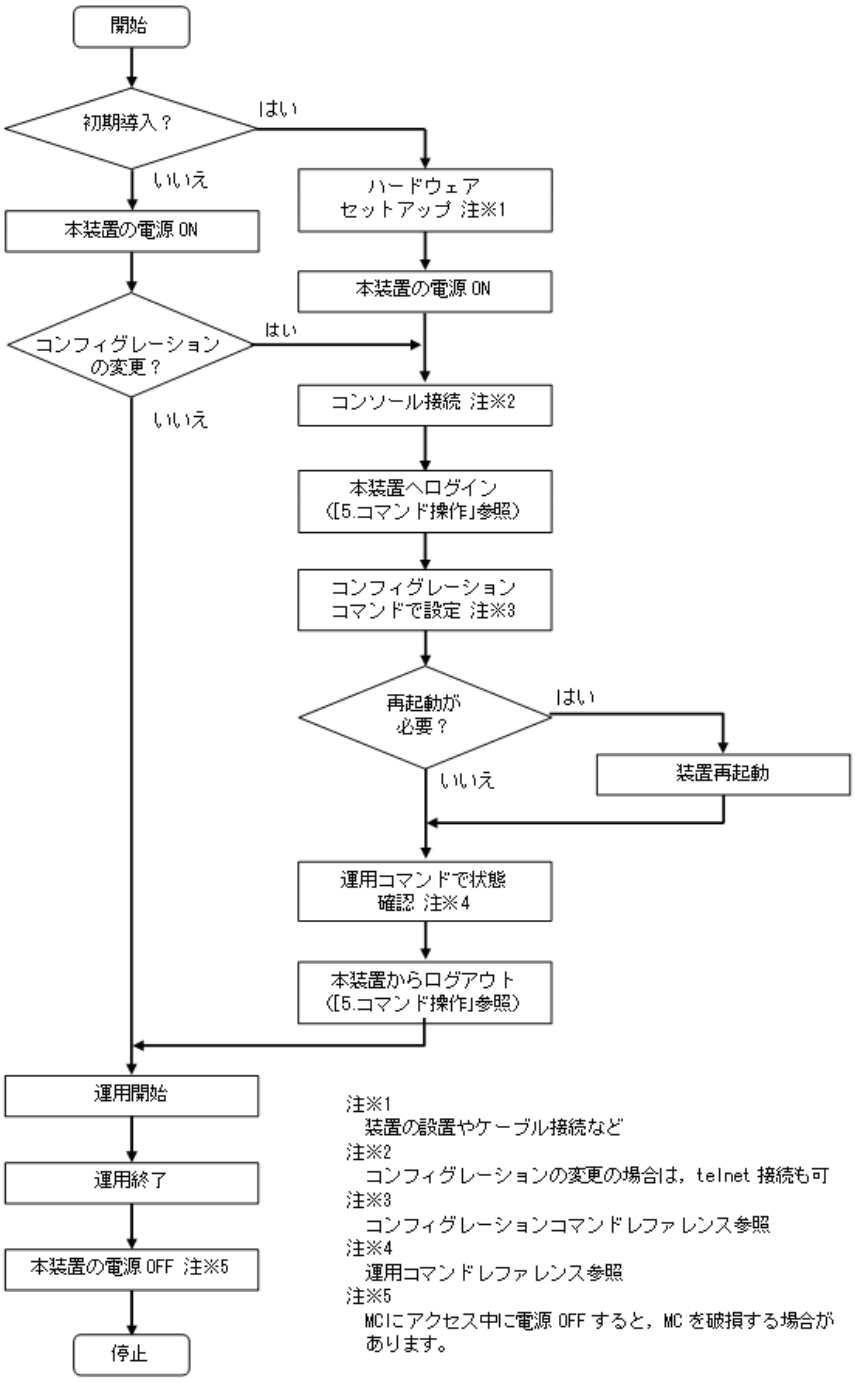
4.2　装置起動

この節では，装置の起動と停止について説明します。

4.2.1　本装置の起動から停止までの概略

本装置の起動から停止までの概略フローを次の図に示します。ハードウェアセットアップの内容についてはマニュアル「ハードウェア取扱説明書」を参照してください。

図 4-3　本装置の起動から停止までの概略フロー



4.2.2 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 4-4 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。	本体の電源を ON にします（電源スイッチのない装置は電源ケーブルを取り付けることで電源を 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。	運用コマンド reload を実行します。

本装置を起動，再起動したときに ST1 LED が赤点灯となった場合は，マニュアル「トラブルシューティングガイド」を参照してください。また，LED 表示内容の詳細は，マニュアル「ハードウェア取扱説明書」を参照してください。

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

4.2.3 装置の停止

本装置の電源を OFF にする場合は，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。電源スイッチのない装置は，本装置から電源ケーブルを取り外すことで電源を OFF にすることができます。

4.3 ログイン・ログアウト

この節では，ログインとログアウトについて説明します。

(1) ログイン

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

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

図 4-4 ログイン画面

```
login: operator
Password:                                                    …1

Copyright (c) 2006-20XX ALAXALA Networks Corporation. All rights reserved.

>                                                            …2
```

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

(2) ログアウト

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

図 4-5 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：30 分）内にキーの入力がなかった場合，自動的にログアウトします。なお，自動ログアウト時間は運用コマンド set exec-timeout で変更できます。

5 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。

5.1 **コマンド入力モード**

5.2 CLI **での操作**

5.3 CLI **の注意事項**

5.1 コマンド入力モード

5.1.1 運用コマンド一覧

コマンド入力モードの切り換えに関する運用コマンド一覧を次の表に示します。

表 5-1 運用コマンド一覧

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

5.1.2 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。

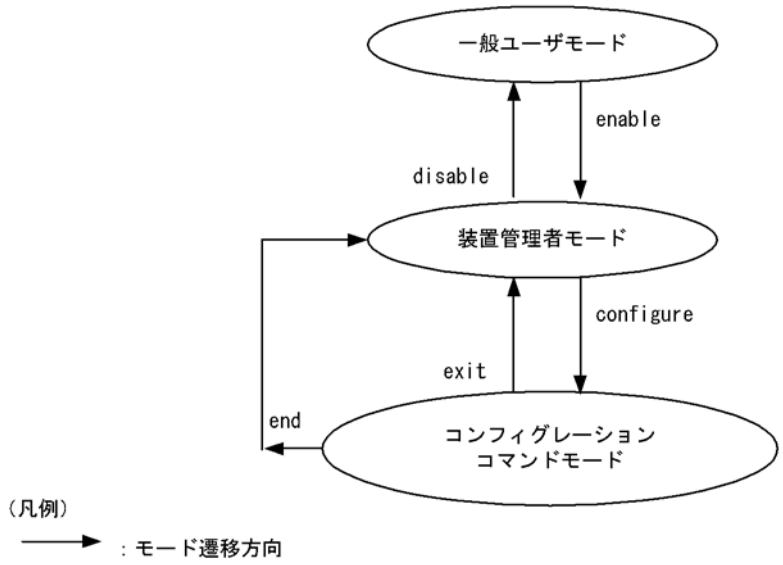
コマンド入力モードとプロンプトの対応を次の表に示します。

表 5-2 コマンド入力モードとプロンプトの対応

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

モード遷移の概要を次の図に示します。

図 5-1　モード遷移の概要



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

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

注意

以下のような操作だけを行い，ランニングコンフィグレーションに変更が生じない場合でもプロンプトの先頭に「！」が付きます。

- コンフィグレーションコマンドモードへ遷移し，コマンドモードを変更する。
- ランニングコンフィグレーションと同じ内容で，コンフィグレーションコマンドを設定（上書き）する。

1. ～ 2. のプロンプト表示例を次の図に示します。

図 5-2　プロンプト表示例

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

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

図 5-3　プロンプト表示例（@を表示する例）

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

5.2 CLI での操作

5.2.1 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パラメータ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 5-4 補完機能を使用したコマンド入力の簡略化

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

[Tab]押下で使用できるコマンドやパラメータの一覧を表示します。

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

注意

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

5.2.2 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 5-5 ［?］入力時の表示例

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

 <cr>
> show vlan
```

注意

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

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

5.2.3 入力エラー指摘機能

コマンドまたはパラメータを不正に入力した際，次行にエラーメッセージ（マニュアル「コンフィグレーションコマンドレファレンス　37　コンフィグレーション編集時のエラーメッセージ」を参照）を表示します。［Tab］入力時と［?］入力時も同様となります。

エラーメッセージの説明によって，コマンドまたはパラメータを見直して再度入力してください。入力エラー指摘の表示例を「図 5-6　入力エラーをしたときの表示例 (fastethernet のスペルミス)」および「図

5-7　パラメータ入力途中の表示例 (duplex のパラメータ指定なし)」に示します。

図 5-6　入力エラーをしたときの表示例 (fastethernet のスペルミス)

```
(config)# interface fastehternet 0/1 [Enter]
                    ^
Error: Invalid parameter.
(config)#
```

図 5-7　パラメータ入力途中の表示例 (duplex のパラメータ指定なし)

```
(config)# interface fastethernet 0/1
(config-if)# duplex [Enter]
              ^
Error: Missing parameter.
(config-if)#
```

5.2.4　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 5-8　短縮入力のコマンド実行例（show ip arp の短縮入力）

```
> sh ip ar [Enter]

Date 20XX/11/14 20:04:23 UTC
Total: 2
IP Address      Linklayer Address  Interface  Expire     Type
10.0.0.55       0013.20ad.0155     VLAN2048   20min      arpa
10.0.0.56       0013.20ad.0156     VLAN2048   20min      arpa

>
```

5.2.5　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 5-9　ヒストリ機能を使用したコマンド入力の簡略化

```
> ping -n 1 192.168.0.1                                    …1
Pinging 192.168.0.1 with 46 bytes of data:
Reply from 192.168.0.1: count=1. bytes=46

  ---- 192.168.0.1 Ping Statistics ----
  Packet: sent 1, received 1, lost 0 (0% loss)
>                                                          …2
> ping -n 1 192.168.0.1                                    …3
Pinging 192.168.0.1 with 46 bytes of data:
Reply from 192.168.0.1: count=1. bytes=46

  ---- 192.168.0.1 Ping Statistics ----
  Packet: sent 1, received 1, lost 0 (0% loss)
>                                                          …4
> ping -n 1 192.168.0.2                                    …5
Pinging 192.168.0.2 with 46 bytes of data:
Reply from 192.168.0.2: count=1. bytes=46

  ---- 192.168.0.2 Ping Statistics ----
  Packet: sent 1, received 1, lost 0 (0% loss)
>
```

1. 192.168.0.1 に対して運用コマンド ping 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 -n 1 192.168.0.1」を表示するので，［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 に対して運用コマンド ping 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 -n 1 192.168.0.1」を表示するので，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 に対して運用コマンド ping を実行します。

注意

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

5.2.6 ページング

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

5.2.7 キーボードコマンド機能

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

表 5-3 推奨キーボードコマンド

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

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

5.3 CLI の注意事項

(1) ログイン後の制限

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

(2) 補完機能，ヘルプ機能の表示制限

一部のコマンドにはパラメータの補完，ヘルプ表示に制限があります。

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

本項ではパラメータの説明として，下記の表記を使用します。

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

(a) 可変値パラメータの後ろに固定文字列キーワードがある場合

入力形式：コマンド ＜可変値＞ 固定文字列キーワード

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

図 5-10 入力後に，入力不可能な固定文字列キーワードを表示する例

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

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

(b) 固定文字列キーワードなしのパラメータが複数ある場合

入力形式：コマンド [＜可変値＞] [＜可変値＞] ・・・

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

図 5-11 [ ] で囲まれた固定文字列キーワードを付けないパラメータが複数ある例

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

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

(c) 可変値パラメータと固定文字列キーワードが同じ入力順にある場合

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

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

図 5-12 可変値パラメータを固定文字列キーワードとして補完する例

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

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

図 5-13 可変値パラメータとして認識する例

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

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

(d) ヘルプのコマンドやパラメータの表示文字数制限

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

図 5-14 ヘルプの表示文字数が制限された例

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

上記の例では，switchport-backup のヘルプ "startup-active-port-selection" が 24 文字以上のため，

"startup-active-port-sel" まで表示し，以降を表示しません。

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

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

- ヘルプ表示にコマンドの入力形式を表示
  パラメータ <Src IPv4>，または <Src MAC> を指定すると，以降のパラメータのヘルプ表示はすべて次の図に示すように該当コマンドの入力形式を表示します。

図 5-15 ヘルプ表示に入力形式を表示する例（ip access-list extended の例）

```
(config-ext-nacl)# permit
 <protocol>              - 0-255,ah,esp,gre,icmp,igmp,ip,ipinip,ospf,pcp,pim,sct
                           p,tcp,tunnel,udp,vrrp
(config-ext-nacl)# permit ip
<PARAMs:input format>    - [<Seq>] permit <Protocol> {<Src IPv4> <Src IPv4 wildc
                           ard> | host <Src IPv4> | any} [*1] {<Dst IPv4> <Dst I
                           Pv4 wildcard> | host <Dst IPv4> | any} [*2] [*3] {[to
                           s <TOS>] [precedence <Precedence>] | dscp <DSCP>} [vl
                           an <VLAN ID>] [user-priority <Priority>]        NOTE:
                            *1:for TCP/UDP - eq <Src port>  *2:for TCP/UDP - eq
                            <Dst port>  *3:for TCP - [ack] [fin] [psh] [rst] [sy
                           n] [urg]
```

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

図 5-16 コマンド不完全で <cr> が表示される例（ip access-list extended の例）

```
(config-ext-nacl)# permit ip any host
<PARAMs:input format>    - [<Seq>] permit <Protocol> {<Src IPv4> <Src IPv4 wildc
                           ard> | host <Src IPv4> | any} [*1] {<Dst IPv4> <Dst I
                           Pv4 wildcard> | host <Dst IPv4> | any} [*2] [*3] {[to
                           s <TOS>] [precedence <Precedence>] | dscp <DSCP>} [vl
                           an <VLAN ID>] [user-priority <Priority>]        NOTE:
                            *1:for TCP/UDP - eq <Src port>  *2:for TCP/UDP - eq
                            <Dst port>  *3:for TCP - [ack] [fin] [psh] [rst] [sy
                           n] [urg]

 <cr>
```

- 補完機能の制限
  パラメータ <Src IPv4>，および <Src MAC> 以降は補完できません。

図 5-17　補完不可の例（ip access-list extended の例）

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

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

(f)　コンフィグレーションの削除で省略可能パラメータを指定した場合の制限

入力形式　コマンド < パラメータ > [省略可能パラメータ]

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

図 5-18　入力不可能なパラメータを表示する例

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

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

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

(g)　no の補完，ヘルプについて

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

(3)　コンフィグレーションモードでの入力について

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

(4)　コンソール (RS-232C) の設定について

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

6 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。

6.1 **コンフィグレーション**

6.2 **ランニングコンフィグレーションの編集概要**

6.3 **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**

6.4 **コンフィグレーションの編集方法**

6.5 **コンフィグレーションの操作**

6.1 コンフィグレーション

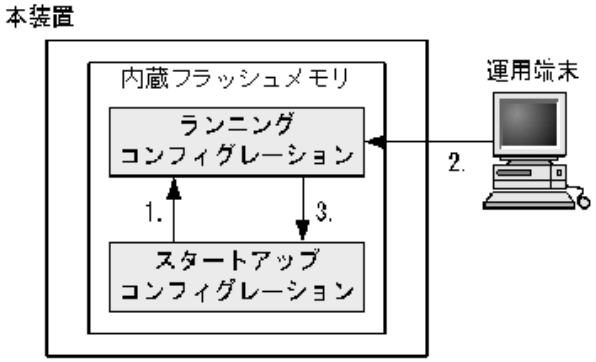
運用開始時または運用中，ネットワークの運用環境に合わせて，本装置に接続するネットワークの構成および動作条件などのコンフィグレーションを設定する必要があります。初期導入時，コンフィグレーションは設定されていません。

6.1.1 起動時のコンフィグレーション

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

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

図 6-1 起動時，および運用中のコンフィグレーションの概要



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

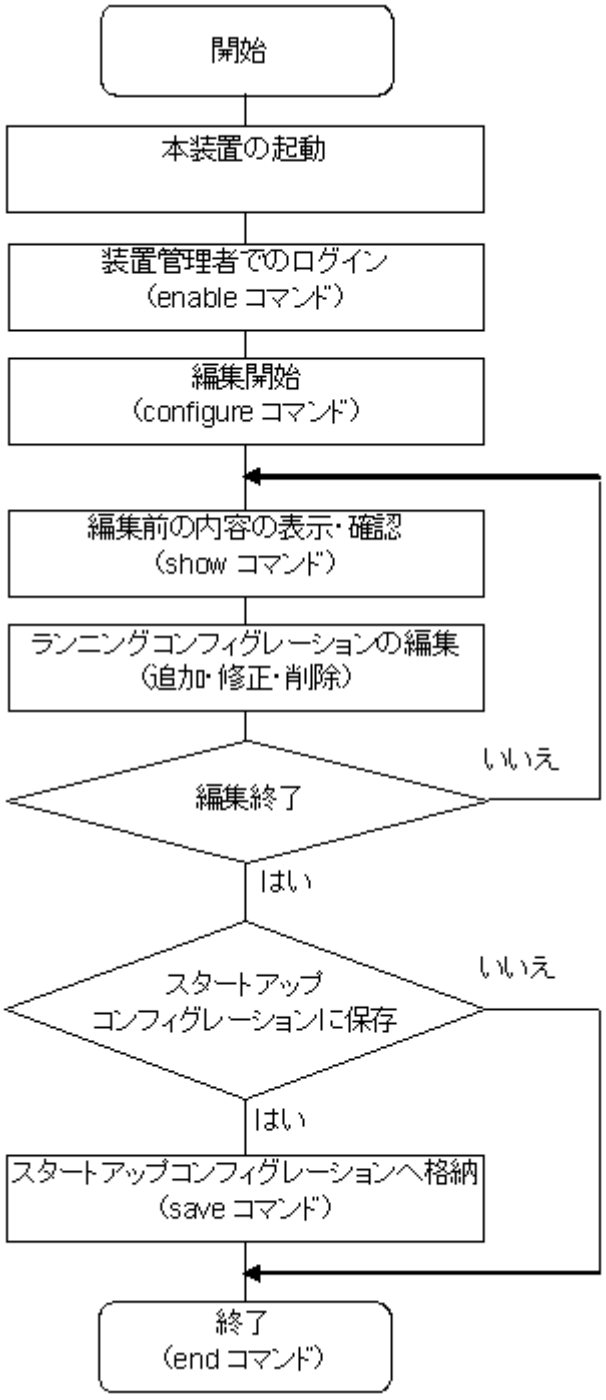
6.1.2 運用中のコンフィグレーション

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

6.2 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，「6.4 コンフィグレーションの編集方法」を参照してください。

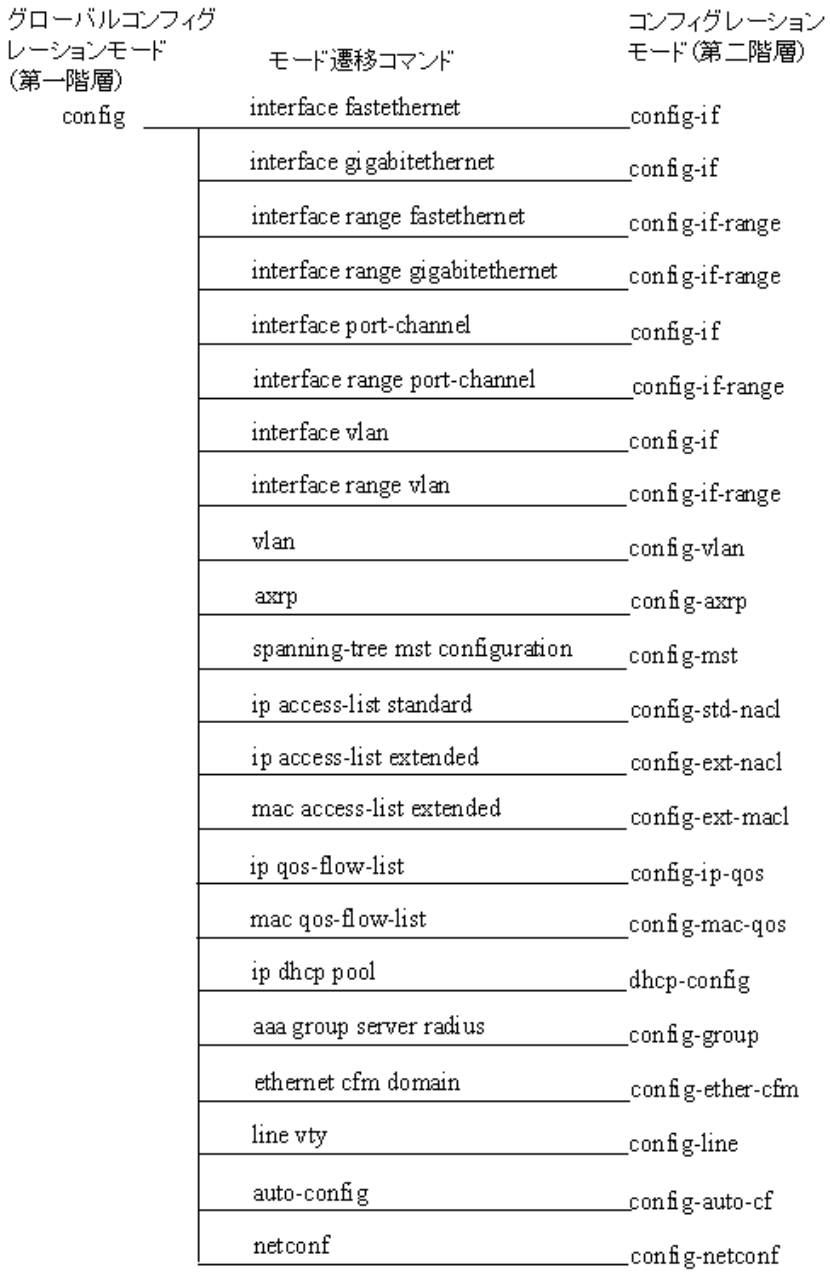
図 6-2 ランニングコンフィグレーションの編集の流れ



6.3 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 6-3 コンフィグレーションのモード遷移の概要



6.4 コンフィグレーションの編集方法

6.4.1 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 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
end	コンフィグレーションコマンドモードを終了して装置管理者モードに戻ります。
exit	モードを一つ戻ります。グローバルコンフィグレーションモードで編集中の場合は，コンフィグレーションコマンドモードを終了して装置管理者モードに戻ります。
save(write)	編集したコンフィグレーションをスタートアップコンフィグレーションファイルに保存します。
show	編集中のコンフィグレーションを表示します。
top	コンフィグレーションコマンドモード移行後は，本コマンド入力でグローバルコンフィグレーションモード（第一階層）に戻ります。

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

表 6-2 運用コマンド一覧

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

6.4.2 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 6-4 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。

6.4.3 コンフィグレーションの表示・確認（show コマンド）

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

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

図 6-5 ランニングコンフィグレーションの表示例

```
# show running-config                    …1
#configuration list for XXXXXXX-XXXXX
!
vlan 1
  name "VLAN0001"
!
vlan 100
  state active
!
vlan 200
  state active
!
spanning-tree mode pvst
!
interface fastethernet 0/1
  switchport mode access
  switchport access vlan 100
!
interface fastethernet 0/2
  switchport mode access
  switchport access vlan 200
!
       :
       :
#
```

1. ランニングコンフィグレーションを表示します。

(2) コンフィグレーションの表示・確認

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

[注意事項]

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

図 6-6 コンフィグレーションの内容をすべて表示

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

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

図 6-7 fastethernet インタフェース情報を表示

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

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

図 6-8 指定のインタフェース情報を表示

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

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

図 6-9 インタフェースモードで指定のインタフェース情報を表示

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

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

6.4.4 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 6-10 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 6-11 機能の抑止および解除の編集例」に示します。

図 6-10 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 fastethernet 0/1             …3
!(config-if)# switchport mode access              …4
!(config-if)# switchport access vlan 100          …5
!(config-if)# exit
!(config)# vlan 100                               …6
!(config-vlan)# state suspend                     …7
!(config-vlan)# exit
!(config)# interface fastethernet 0/1             …8
!(config-if)# no switchport access vlan           …9
!(config-if)# exit
!(config)#
```

1. VLAN 100 をポート VLAN として設定します。
2. VLAN 100 を有効にします。
3. イーサネットインタフェース 0/1 にモードを遷移します。
4. イーサネットインタフェース 0/1 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 6-11 機能の抑止および解除の編集例

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

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

（2）入力コマンドのチェック

コンフィグレーションコマンドを入力すると，入力されたコンフィグレーションに誤りがないかすぐにチェックされます。エラーがない場合は「図 6-12 正常入力時の出力」に示すようにプロンプトを表示して，コマンドの入力待ちになります。ランニングコンフィグレーションの編集中の場合は，変更した内容がすぐに運用に使用されます。

エラーがある場合は「図 6-13 異常入力時のエラーメッセージ出力」に示すように，入力したコマンドの行の下にエラーの内容を示したエラーメッセージを表示します。この場合，入力したコンフィグレーションは反映されないので，入力の誤りを修正してから再度入力してください。

図 6-12 正常入力時の出力

```
(config)# interface fastethernet 0/1
!(config-if)# description TokyoOsaka
!(config-if)#
```

図 6-13 異常入力時のエラーメッセージ出力

```
(config)# interface fastethernet 0/1
!(config-if)# description
                          ^
Error: Missing parameter.
!(config-if)#
```

6.4.5 コンフィグレーションのファイルへの保存

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

図 6-14 コンフィグレーションの保存例（save コマンド）

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

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

図 6-15 コンフィグレーションの保存例（copy コマンド）

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

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

6.4.6 コンフィグレーションの編集終了（exit コマンド）

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

6.4.7 コンフィグレーションの編集時の注意事項

（1）設定できるコンフィグレーションのコマンド数に関する注意事項

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

（2）コンフィグレーションをコピー＆ペーストで入力する際の注意事項

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

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

6.5 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。

6.5.1 ftp を使用したファイル転送

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

(1) バックアップコンフィグレーションファイルを本装置に転送する場合

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

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

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

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

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

図 6-16 コマンドプロンプト画面での操作：バックアップコンフィグレーションファイルの本装置へのファイル転送例

```
C:\TEMP>ftp 192.168.0.1
Connected to 192.168.0.1
220 AX1200 FTP server ready
User (192.168.0.1:(none)): operator
331 Password required
Password:
230 User logged in
ftp> asc
200 Type set to A, ASCII mode
ftp>
ftp> put backup.cnf
200 Port set okay
150 Opening ASCII mode data connection
226 Transfer complete
ftp:xxxxxx bytes sent in xx.x Seconds (xx.xx Kbytes/sec)
ftp> bye
221 Bye…see you later
C:\TEMP>
```

コンソールログインし，運用コマンド copy で RAMDISK に転送したファイルをスタートアップコンフィグレーションファイルにコピーします。

図 6-17 コンソール画面での操作：転送したファイルを本装置へ反映（copy コマンド）

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

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

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

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

RAMDISK にコピーします。

図 6-18 コンソール画面での操作：スタートアップコンフィグレーションファイルを RAMDISK へコピー（copy コマンド）

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

PC でコマンドプロンプト画面を開きます。

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

図 6-19 コマンドプロンプト画面での操作：バックアップコンフィグレーションファイルの本装置へのファイル転送例

```
C:\TEMP>ftp 192.168.0.1
Connected to 192.168.0.1
220 AX1200 FTP server ready
User (192.168.0.1:(none)): operator
331 Password required
Password:
230 User logged in
ftp> asc
200 Type set to A, ASCII mode
ftp>
ftp> get backup.cnf
200 Port set okay
150 Opening ASCII mode data connection
226 Transfer complete
ftp:xxxxxx bytes sent in xx.x Seconds (xx.xx Kbytes/sec)
ftp> bye
221 Bye…see you later
C:\TEMP>
```

6.5.2 MC を使用したファイル転送

MC にファイル転送をするときは運用コマンド copy を使用します。

（1）バックアップコンフィグレーションファイルを本装置に転送する場合

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

図 6-20 バックアップコンフィグレーションファイルの MC から本装置へのファイル転送例（copy コマンド）

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

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

（2）バックアップコンフィグレーションファイルを MC に転送する場合

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

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

図 6-21　バックアップコンフィグレーションファイルを本装置から MC へコピー（copy コマンド）

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

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

6.5.3　バックアップコンフィグレーションファイル反映時の注意事項

運用コマンド copy を使用して，バックアップコンフィグレーションファイルをスタートアップコンフィグレーションファイルにコピーした場合，そのままではランニングコンフィグレーションに反映されません。必ず装置の電源を OFF/ON するか，運用コマンド reload により，装置の再起動が必要となりますので，リモートからログインしている場合は注意してください。

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

7 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。

7.1 **解説**

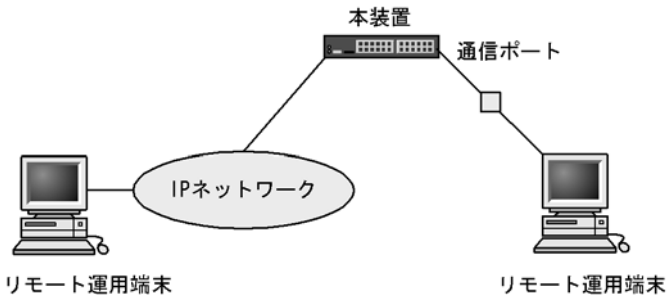
7.2 **コンフィグレーション**

7.3 **オペレーション**

7.1 解説

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，初期導入時には，VLAN や IP アドレスなどの設定が行われていません。そのため，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する必要があります。

図 7-1 リモート運用端末からの本装置へのログイン



7.2 コンフィグレーション

7.2.1 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 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
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 vty	装置への telnet リモートアクセスを許可します。
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。

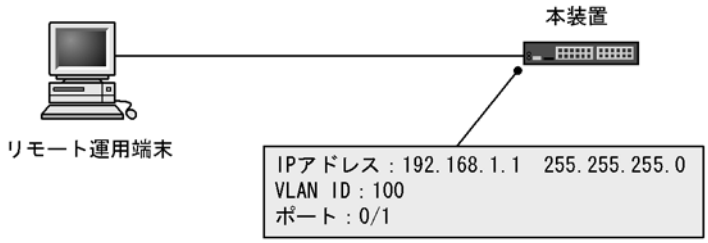
VLAN の設定，および IPv4 インタフェースの設定に関するコンフィグレーションコマンドについては，「18 VLAN」，「25 IPv4 インタフェース」を参照してください。

7.2.2 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，あらかじめ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。

図 7-2 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 を作成します。

2. **(config)# interface fastethernet 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レーションモードに移行します。VLAN ID 100 に IPv4 アドレス 192.168.1.1，サブネットマスク 255.255.255.0 を設定します。

7.2.3 telnet によるログインを許可する

[設定のポイント]

あらかじめ，IP アドレスを設定しておく必要があります。

リモート運用端末から本装置に telnet プロトコルによるリモートログインを許可するコンフィグレーションを実施します。

このコンフィグレーションが設定されていない場合，コンソールからだけ本装置にログインできます。

[コマンドによる設定]

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

リモート運用端末から本装置への telnet プロトコルによるリモートアクセスを許可します。本装置に同時にリモートログインできるユーザ数を最大２に設定します。

7.2.4 ftp によるログインを許可する

[設定のポイント]

あらかじめ，IP アドレスを設定しておく必要があります。

リモート運用端末から本装置に ftp プロトコルによるリモートアクセスを許可するコンフィグレーションを実施します。

このコンフィグレーションを実施していない場合，ftp プロトコルを用いた本装置へのアクセスはできません。

[コマンドによる設定]

1.
```
(config)# ftp-server
```

リモート運用端末から本装置への ftp プロトコルによるリモートアクセスを許可します。

7.3 オペレーション

7.3.1 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 7-2 運用コマンド一覧

コマンド名	説明
set exec-timeout	自動ログアウトが実行されるまでの時間を設定します。
set terminal pager	ページングの実施／未実施を設定します。
telnet	指定された IP アドレスのリモートホストへ telnet で接続します。
ftp	本装置と TCP ／ IP で接続されているリモート運用端末との間でファイル転送をします。
line console speed	コンソール（RS-232C) の通信速度を変更します。
trace-monitor	運用ログのモニタ表示実施／未実施を設定します。

7.3.2 リモート運用端末と本装置との通信の確認

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

8 ログインセキュリティと RADIUS

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

8.1 **ログインセキュリティの設定**

8.2 RADIUS **の解説**

8.3 RADIUS **のコンフィグレーション**

8.4 RADIUS **のオペレーション**

8.1 ログインセキュリティの設定

8.1.1 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 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
aaa authentication login	リモートログイン時に使用する認証方式を指定します。
aaa authentication login end-by-reject	ログイン時の認証で，否認された場合に認証を終了します。通信不可（RADIUS サーバ無応答など）による認証失敗時は，コンフィグレーションコマンド aaa authentication login で次に指定されている認証方式で認証します。
ip access-group	本装置へリモートログインを許可または拒否するリモート運用端末の IPv4 アドレスを指定したアクセスリストを設定します。

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 8-2 運用コマンド一覧

コマンド名	説明
password	ログインユーザのパスワードを指定します。
clear password	ログインユーザのパスワードを削除します。
rename user	初期状態のユーザ ID “operator” を任意の名前に変更します。
show sessions(who)	本装置にログインしているユーザを表示します。

8.1.2 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 ネットワーク経由のリモートログイン機能（telnet）があります。

本装置ではログイン時およびログイン中に次に示す制御を行っています。

1. ログイン時に不正アクセスを防止するため，ユーザ ID とパスワードによるチェックを設けています。
2. ローカルとリモートの運用端末から同時にログインできます。
3. 本装置にログインできるリモートユーザ数は最大２ユーザです。なお，コンフィグレーションコマンド line vty でログインできるユーザ数を制限できます。
4. 本装置にアクセスできる IPv4 アドレスをコンフィグレーションコマンド ip access-list standard，ip access-group 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。
7. 一定時間（デフォルト：30 分）内にキーの入力がなかった場合，自動的にログアウトします。なお，自動ログアウト時間は運用コマンド set exec-timeout で変更できます。
8. リモート運用端末（telnet）のログインでは，RSA SecurID システムと連携してワンタイムパスワード認証も可能です。ワンタイムパスワード認証については，「コンフィグレーションガイド Vol.2 14 ワンタイムパスワード認証【OP-OTP】」を参照してください。

8.1.3 ログインユーザの変更

運用コマンド rename user を用いて本装置にログインできるユーザ ID を変更できます。ログインユーザの変更例を次の図に示します。

図 8-1 ユーザ operator を変更

```
> enable
# rename user
Changing username.
Old username:operator                    … 1
New username:ax12-01                     … 2
# exit
>
```

1. 現在のユーザ ID を入力します。
2. 新しいユーザ ID を入力します（最大８文字まで指定可能です)。

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に変更することをお勧めします。

変更したユーザ ID は忘れないようにしてください。

8.1.4 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 8-2 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:
#
```

8.1.5 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 8-3 リモート運用端末からのログインを許可する設定例

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

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

図 8-4 ftp プロトコルによるアクセス許可の設定例

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

8.1.6 同時にログインできるユーザ数の設定

コンフィグレーションコマンド line vty を設定することで，リモート運用端末から本装置へログインできるようになります。コンフィグレーションコマンド line vty の <End allocation> パラメータで，リモートログインできるユーザ数が制限されます。なお，この設定にかかわらず，コンソールからは常にログインできます。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 8-5 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)# exit
```

同時ログインに関する動作概要を次に示します。

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

8.1.7 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，ip access-group 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は，最大 16 個の ip access-group で登録できます。このコンフィグレーションを実施していない場合，すべてのリモート運用端末から本装置へのアクセスが可能となります。

[コマンドによる設定]

1.
```
(config)# ip access-list standard REMOTE
(config-std-nacl)# deny host 192.168.0.254
(config-std-nacl)# permit 192.168.0.0 0.0.0.255
(config-std-nacl)# exit
```
ネットワーク（192.168.0.0/24）からだけログインを許可し，そのうち 192.168.0.254 の IP アドレスからのログインを拒否する，アクセスリスト情報 REMOTE を設定します。

2.
```
(config)# line vty 0 1
(config-line)# ip access-group REMOTE in
(config-line)# exit
```
line モードに遷移し，アクセスリスト情報 REMOTE を適用し，ネットワーク（192.168.0.0/24）にあるリモート運用端末からだけログインを許可します。

[注意事項]

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

(2) RADIUS 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 を使用した認証が可能です。

8.2 RADIUS の解説

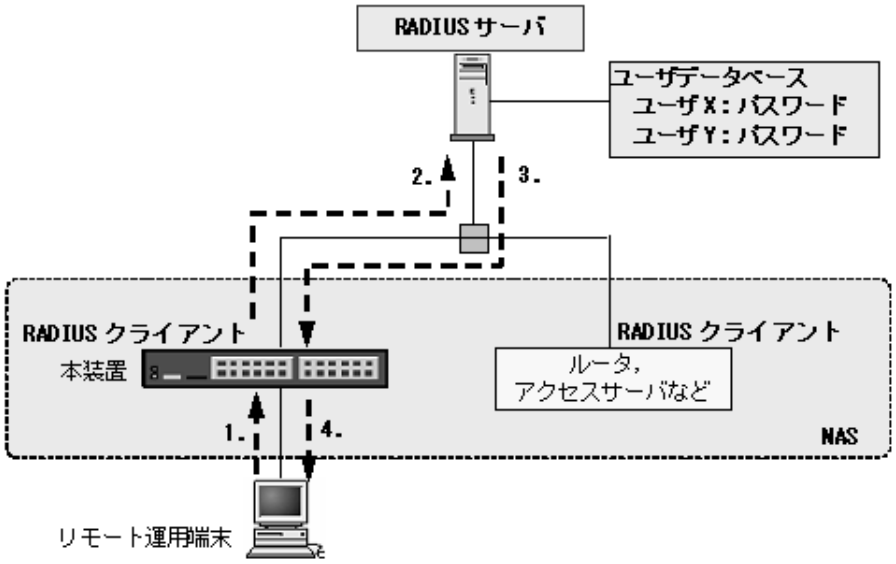
8.2.1 RADIUS の概要

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

RADIUS を使用すると 1 台の RADIUS サーバだけで，複数 NAS でのユーザパスワードなどの認証情報やアカウンティング情報を一元管理できるようになります。本装置では，RADIUS サーバに対してユーザ認証やアカウンティングを要求できます。

RADIUS 認証の流れを次の図に示します。

図 8-6　RADIUS 認証の流れ



8.2.2 RADIUS 認証の適用機能および範囲

本装置で RADIUS 認証を適用する機能を次に示します。

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

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

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

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

（1） RADIUS 認証の適用範囲

RADIUS 認証を適用できる操作を次に示します。

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

次に示す操作は RADIUS 認証を適用できません。

- コンソール（RS-232C）からのログイン

（2） RADIUS サーバのサポート範囲

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

表 8-3　RADIUS のサポート範囲

分類	内容
文書全体	NAS に関する記述だけを対象にします。
パケットタイプ	ログイン認証で使用する次のタイプ • Access-Request (送信) • Access-Accept (受信) • Access-Reject (受信) • Access-Challenge(受信)
属性	ログイン認証で使用する次の属性 • User-Name • User-Password • Service-Type • NAS-IP-Address • Reply-Message • State • NAS-Identifier

（a） 使用する RADIUS 属性の内容

使用する RADIUS 属性の内容を次の表に示します。

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

表 8-4　使用する RADIUS 属性の内容

属性名	属性値	パケットタイプ	内容
User-Name	1	Access-Request	認証するユーザの名前。
User-Password	2	Access-Request	認証ユーザのパスワード。送信時には暗号化されます。

属性名	属性値	パケットタイプ	内容
Service-Type	6	Access-Request	Login(値 =1)。Access-Accept および Access-Reject に添付された場合は無視します。
NAS-IP-Address	4	Access-Request	本装置の IP アドレス。IP アドレスが登録されている VLAN インタフェースのうち，最も小さい VLAN ID の IP アドレスを使用します。
Reply-Message	18	Access-Challenge Access-Accept ※1 Access-Reject ※1	テキスト文字列。 ワンタイムパスワード認証※2 で使用するメッセージを telnet 画面に表示します。
State	24	Access-Challenge Access-Request	テキスト文字列。 ワンタイムパスワード認証※2 で使用する Access-Challenge で State 有のとき，本装置で State 情報を保持します。 Access-Challenge に対応する Access-Request のときに，本装置で保持していた State 情報を付加します。
NAS-Identifier	32	Access-Request	本装置の装置名。装置名が設定されていない場合は添付されません。

注※ 1

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

注※ 2

ワンタイムパスワード認証については，「コンフィグレーションガイド Vol.2　14　ワンタイムパスワード認証【OP-OTP】」を参照してください。

8.2.3 RADIUS を使用した認証

本項ではログイン認証で使用する RADIUS 認証について説明します。

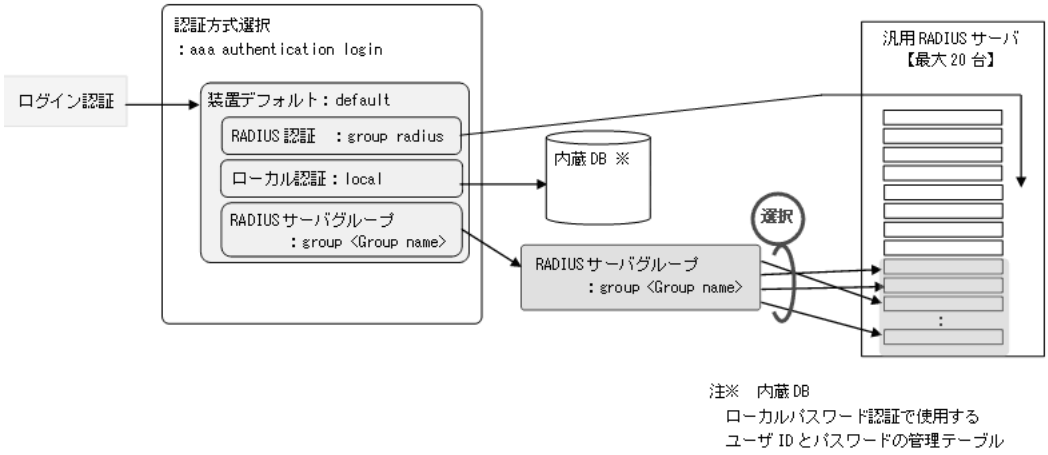
なお，後述の RADIUS サーバの選択や自動復旧機能は，レイヤ 2 認証でも同様に使用します。詳細は，「コンフィグレーションガイド Vol.2　5　レイヤ 2 認証機能の概説」を参照してください。

(1) ログイン認証サービスの選択

ログイン認証に使用するサービスは複数指定できます。指定できるサービスは RADIUS 認証（汎用 RADIUS サーバ認証，または RADIUS サーバグループ認証）および password コマンドによる本装置単体でのローカルパスワード認証機能です。

認証方式設定の相関図を次の図に示します。

図 8-7 認証方式設定の相関図



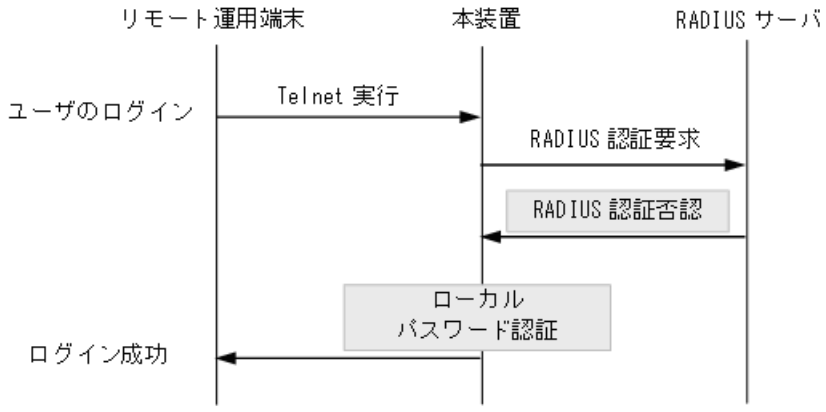
これらの認証方式は単独でも同時でも指定でき，同時に指定された場合は先に指定された方式で認証に失敗した場合に，次に指定された方式で認証できます。また，同時に指定された場合に先に指定された方式で認証に失敗したときの認証サービスの選択動作を，コンフィグレーションコマンド aaa authentication login end-by-reject で変更できます。

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

(a) end-by-reject 未設定時

end-by-reject 未設定時の認証サービスの選択について説明します。end-by-reject 未設定時は，先に指定された方式で認証に失敗した場合に，その失敗の理由に関係なく，次に指定された方式で認証できます。例として，コンフィグレーション認証方式に RADIUS 認証，単体でのローカルパスワード認証の順番で指定し，それぞれの認証結果が RADIUS サーバ認証否認，ローカルパスワード認証成功となる場合の認証方式シーケンスを次の図に示します。

図 8-8 認証方式シーケンス (end-by-reject **未設定時**)



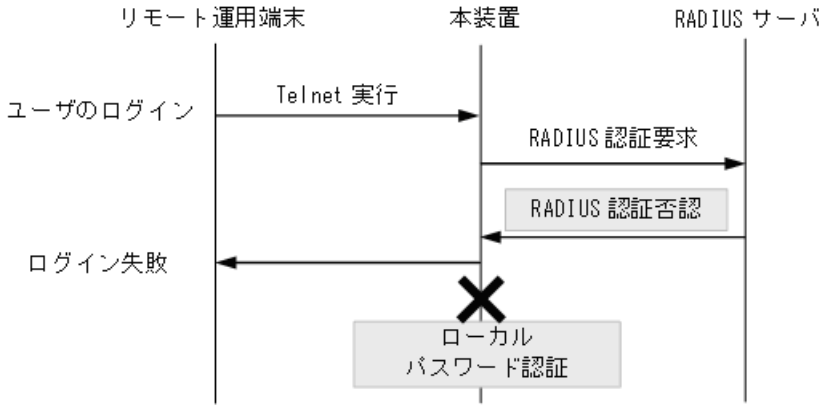
この図で端末からユーザが本装置に telnet を実行すると，RADIUS サーバに対し本装置から RADIUS 認証を要求します。RADIUS サーバとの認証否認によって RADIUS サーバでの認証に失敗すると，次に本装置のローカルパスワード認証での認証を実行します。ここで認証に成功し，ユーザは本装置へのログインに成功します。

(b) end-by-reject 設定時

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

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

図 8-9 認証方式シーケンス (end-by-reject **設定時**)



この図で端末からユーザが本装置に telnet を実行すると，RADIUS サーバに対し本装置から RADIUS 認証を要求します。RADIUS サーバでの認証否認によって RADIUS サーバでの認証に失敗すると，この時点で一連の認証が失敗となり，認証を終了します。次に指定されている本装置のローカルパスワード認証は行いません。その結果，ユーザは本装置へのログインに失敗します。

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

リモートログインの RADIUS 認証で使用する汎用 RADIUS サーバは最大 20 台まで指定できます。一つのサーバと通信できず，認証サービスが受けられない場合は，順次これらのサーバへの接続を試行します。

- RADIUS サーバの選択（通信不可を判断するまでの最大時間）
  RADIUS サーバと通信不可を判断する応答タイムアウト時間を設定できます。デフォルト値は 5 秒です。また，各 RADIUS サーバでタイムアウトした場合は，再接続を試行します。この再試行回数も設定でき，デフォルト値は 3 回です。このため，ログイン方式として RADIUS サーバが使用できないと判断するまでの最大時間は，応答タイムアウト時間×（最初の 1 回＋再送回数）× RADIUS サーバ設定数になります。
- 自動復旧（dead-interval）機能
  本装置の RADIUS 認証では，認証対象端末からのフレーム受信による RADIUS 認証要求を契機に有効な RADIUS サーバを検出し，以降の端末は常に有効な RADIUS サーバを使用します。この方式では，認証されるまでの時間は軽減されますが，RADIUS サーバを負荷分散構成などで使用時，RADIUS サーバに障害が発生すると負荷分散状態に自動的に復旧できません。本装置では，最初の有効な RADIUS サーバ（プライマリ RADIUS サーバ）への自動復旧手段として，監視タイマによる自動復旧（dead-interval）機能をサポートしています。監視タイマのデフォルトは 10 分です。

(3) RADIUS サーバに登録する情報

RADIUS 認証機能を使用するには，RADIUS サーバにユーザ ID およびパスワードを登録します。ユーザ ID は最大 8 文字，パスワードは最大 16 文字で RADIUS サーバへ登録してください。

8.2.4 RADIUS サーバとの接続

(1) RADIUS サーバでの本装置の識別

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

(2) RADIUS サーバのポート番号

RADIUS の認証サービスのポート番号は，RFC2865 で 1812 と規定されています。本装置では特に指定しないかぎり，RADIUS サーバへの要求に 1812 のポート番号を使用します。しかし，一部の RADIUS サーバで 1812 ではなく 1645 のポート番号を使用している場合があります。このときはコンフィグレーションコマンド radius-server host の auth-port パラメータで 1645 を指定してください。なお，auth-port パラメータでは 1 ～ 65535 の任意の値が指定できますので，RADIUS サーバが任意のポート番号で待ち受けできる場合にも対応できます。

(3) 本装置で設定する RADIUS サーバ情報

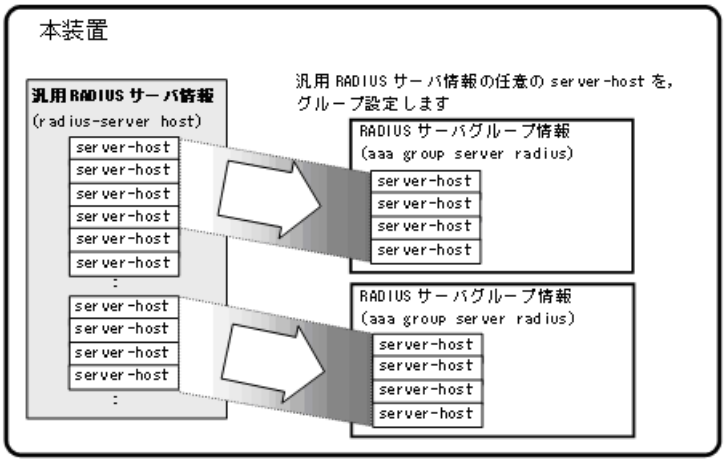
本装置では，以下の RADIUS サーバ情報を設定できます。

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

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

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

図 8-10　RADIUS サーバグループ情報と汎用 RADIUS サーバ情報の関係



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

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

RADIUS サーバグループの収容条件については，「3.2　収容条件」を参照してください。

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

8.3 RADIUS のコンフィグレーション

8.3.1 コンフィグレーションコマンド一覧

RADIUS に関するコンフィグレーションコマンド一覧を次の表に示します。

表 8-5 コンフィグレーションコマンド一覧（RADIUS）

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

注※

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

8.3.2 ログイン認証方式の設定

ログイン認証方式として，下記の設定例を示します。

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

（1）汎用 RADIUS サーバ認証とローカルパスワード認証の設定

[設定のポイント]

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

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

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

あらかじめ，通常のリモートアクセスに必要な設定を行っておく必要があります。

[コマンドによる設定]

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

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

ように設定します。

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

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

[注意事項]

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

(2) RADIUS サーバグループ認証とローカルパスワード認証の設定

[設定のポイント]

本例では，認証方式に RADIUS サーバグループ認証とローカルパスワード認証を設定します。通信不可（RADIUS サーバ無応答など）により RADIUS サーバグループ認証に失敗した場合は，本装置によるローカルパスワード認証を行うように設定します。
なお，RADIUS 認証否認によって認証に失敗した場合には，その時点で認証を終了し，ローカルパスワード認証を行いません。
また，RADIUS サーバグループ認証で使用する RADIUS サーバグループ情報については，「8.3.3 RADIUS サーバグループの設定」を参照してください。
あらかじめ，通常のリモートアクセスに必要な設定を行っておく必要があります。

[コマンドによる設定]

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

[注意事項]

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

8.3.3 RADIUS サーバグループの設定

[設定のポイント]

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

[コマンドによる設定]

1. **(config)# radius-server host 192.168.10.1 key "AAAA1234"**
   (config)# radius-server host 192.168.10.2 key "BBBB1234"
   (config)# radius-server host 192.168.10.3 key "CCCC1234"

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

汎用 RADIUS サーバの IP アドレスと共有鍵を設定します。

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

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

[注意事項]

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

8.4 RADIUS のオペレーション

8.4.1 運用コマンド一覧

RADIUS に関する運用コマンド一覧を次の表に示します。

表 8-6 運用コマンド一覧

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

8.4.2 有効 RADIUS サーバ情報の表示

(1) 有効 RADIUS サーバの表示

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

図 8-11 show radius-server の実行結果（有効 RADIUS サーバで動作中）

```
> show radius-server

Date 20XX/10/29 05:13:12 UTC
 <common>
   [Authentication]
      IP address        Port  Timeout  Retry  Remain
    * 192.168.0.251     1812        5      3       -
      192.168.0.252     1812        5      3       -
      192.168.0.253     1812        5      3       -
      192.168.0.254     1812        5      3       -
      192.168.11.1      1812       10      5       -
   [Accounting]
      IP address        Port  Timeout  Retry  Remain
    * 192.168.0.251     1813        5      3       -
      192.168.0.252     1813        5      3       -
      192.168.0.253     1813        5      3       -
      192.168.0.254     1813        5      3       -
      192.168.11.1      1813       10      5       -
 <dot1x>
   [Authentication]
      IP address        Port  Timeout  Retry  Remain
    * 192.168.11.1      1812       10      5       -
   [Accounting]
      IP address        Port  Timeout  Retry  Remain
    * 192.168.11.1      1813       10      5       -
 <mac-auth>
   [Authentication]
      IP address        Port  Timeout  Retry  Remain
      192.168.11.1      1812       10      5       -
    * hold down                                    8
   [Accounting]
      IP address        Port  Timeout  Retry  Remain
    * 192.168.11.1      1813       10      5       -
 <web-auth>
   [Authentication]
      IP address        Port  Timeout  Retry  Remain
    * 192.168.0.254     1812        5      3       -
   [Accounting]
```

```
      IP address        Port  Timeout  Retry  Remain
    * 192.168.0.254     1813        5      3       -
 <ra-group-1>
   [Authentication]
      IP address        Port  Timeout  Retry  Remain
      192.168.0.251     1812        5      3       -
      192.168.0.252     1812        5      3       -
      192.168.0.253     1812        5      3       -
    * 192.168.0.254     1812        5      3     541

>
```

「*」は現在使用中の RADIUS サーバの IP アドレスを示します。

(2) 有効 RADIUS サーバの統計情報表示

本装置に設定されている有効 RADIUS サーバの統計情報を表示します。

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

図 8-12 show radius-server statistics summary の実行結果

```
> show radius-server statistics summary

Date 20XX/10/29 04:49:05 UTC
  IP address:192.168.0.254 [Tx] Timeout:2 [Rx] Accept:10, Reject:2
  IP address:192.168.11.1 [Tx] Timeout:2 [Rx] Accept:12, Reject:2

>
```

図 8-13 show radius-server statistics の実行結果

```
> show radius-server statistics

Date 20XX/10/29 04:47:02 UTC
  IP address: 192.168.0.254
    [Authentication]     Current Request:          0
     [Tx] Request  :         12  Error  :          1
          Retry    :          2  Timeout:          2
     [Rx] Accept   :         10  Reject :          2  Challenge  :          0
          Malformed:          0  BadAuth:          0  UnknownType:          0
    [Accounting]         Current Request:          0
     [Tx] Request  :         19  Error  :          1
          Retry    :          0  Timeout:          0
     [Rx] Responses:         19
          Malformed:          0  BadAuth:          0  UnknownType:          0
  IP address: 192.168.11.1
    [Authentication]     Current Request:          0
     [Tx] Request  :         14  Error  :          1
          Retry    :          2  Timeout:          2
     [Rx] Accept   :         12  Reject :          2  Challenge  :          0
          Malformed:          0  BadAuth:          0  UnknownType:          0
    [Accounting]         Current Request:          0
     [Tx] Request  :         23  Error  :          1
          Retry    :          0  Timeout:          0
     [Rx] Responses:         23
          Malformed:          0  BadAuth:          0  UnknownType:          0

>
```

9 時刻の設定と NTP

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。

9.1 **時刻の設定と確認**

9.2 **コンフィグレーション**

9.3 **オペレーション**

9.1 時刻の設定と確認

9.1.1 サポート仕様

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

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

本装置でサポートしている NTP クライアント機能は下記のとおりです。

表 9-1 本装置でサポートする NTP クライアント機能

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

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

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

表 9-2 同時設定時の有効モード（○：設定あり，×：設定なし）

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

（1）指定した NTP サーバから定期時刻取得（Unicast モード）

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

NTP サーバアドレスは最大２個登録でき，最初に登録されたアドレスをプライマリ，後から登録さ

れたアドレスをセカンダリと呼びます。プライマリの NTP サーバアドレスに対して時刻取得に失敗した場合は，セカンダリの NTP サーバアドレスに対して時刻情報を要求します。

図 9-1 Unicast モードによる時刻情報取得図（プライマリ設定時）

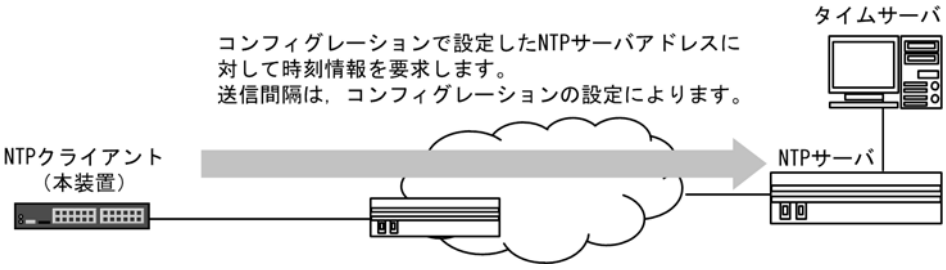
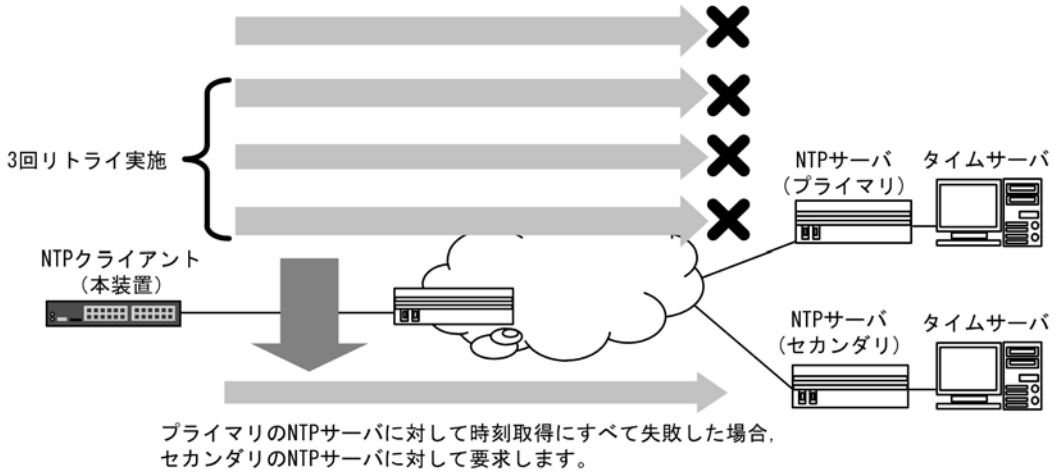


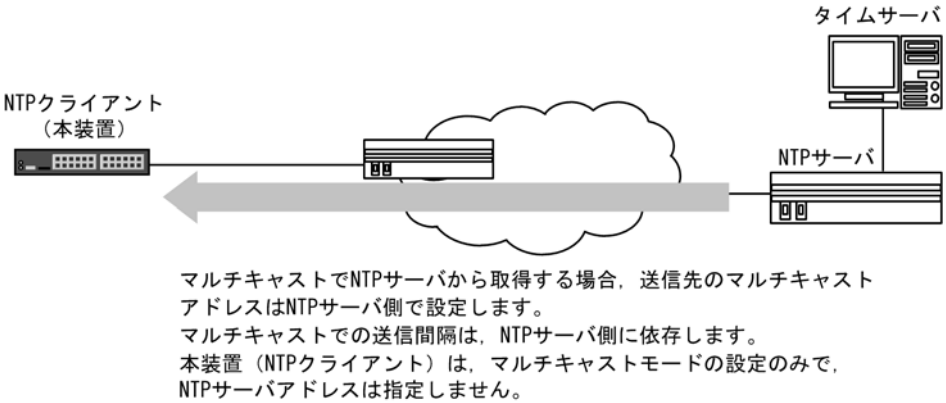
図 9-2 Unicast モードによる時刻情報取得図（プライマリ／セカンダリ設定時）



（2） マルチキャストで取得（Multicast モード）

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

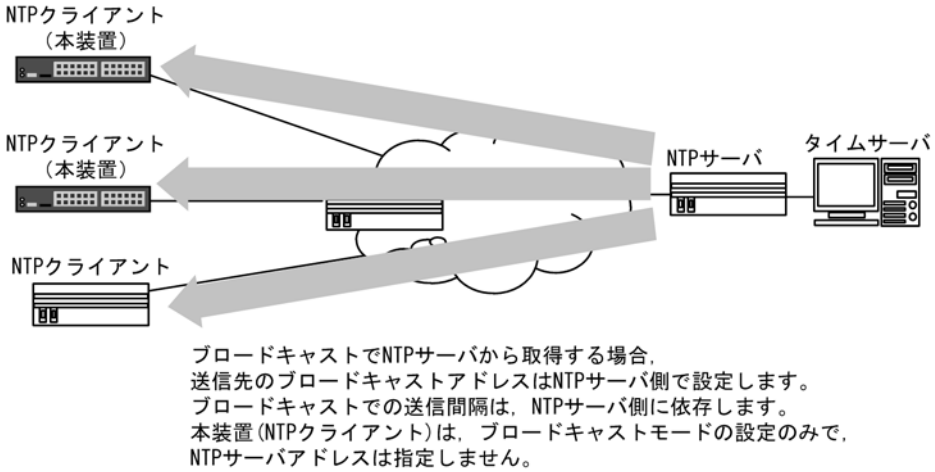
図 9-3 Multicast モードによる時刻情報取得図



（3） ブロードキャストで取得（Broadcast モード）

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

図 9-4 Broadcast モードによる時刻情報取得図



(4) 手動取得

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

9.1.2 時刻変更に関する注意事項

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

- 装置の再起動，または省電力機能のスケジューリングによる装置スリープ時
- コンフィグレーションコマンド clock timezone でタイムゾーンを変更した時
- 運用コマンド set clock，または NTP クライアントで時刻を変更した時（秒単位表示データだけクリア）

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

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 9-3 コンフィグレーションコマンド一覧

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

9.2.2 システムクロックの設定

[設定のポイント]

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

[コマンドによる設定]

1. **(config)# clock timezone JST +9**
   日本時間として，タイムゾーンに JST，UTC からのオフセットを +9 に設定します。
2. **(config)# exit**
   # copy running-config startup-config
   Do you wish to copy from running-config to startup-config? (y/n): y
   コンフィグレーションコマンドモードから装置管理者モードに移行し，保存します。
3. **# set clock 1102221530**
   Tue Feb 22 15:30:17 JST 2011
   #
   2011 年 2 月 22 日 15 時 30 分に時刻を設定します。

9.2.3 NTP サーバから定期的に時刻情報を取得する

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

[設定のポイント]

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

[コマンドによる設定]

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

9.3 オペレーション

9.3.1 運用コマンド一覧

時刻設定および NTP に関する運用コマンド一覧を次の表に示します。

表 9-4 運用コマンド一覧

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

9.3.2 時刻の確認

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

図 9-5 時刻の確認

```
> show clock
Tue Feb 22 15:30:24 JST 20XX
>
```

9.3.3 NTP クライアント情報の表示

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

図 9-6 NTP クライアント情報の表示

```
> show ntp-client

Date 20XX/02/23 11:38:05 UTC
 Last NTP Status
  NTP-Server : 192.168.7.1, Source-Address : ---
  Mode : Multicast, Lapsed time : 14(s), Offset : 1(s)

 Activate NTP Client
  NTP-Server : ---, Source-Address : ---
  Mode : Multicast

 NTP Execute History(Max 10 entry)
  NTP-Server      Source-Address  Mode      Set-NTP-Time          Status
  192.168.7.1     ---             Multicast 20XX/02/23 11:37:51        1
  192.168.7.1     ---             Multicast 20XX/02/23 11:36:51        1
  192.168.7.1     ---             Multicast 20XX/02/23 11:35:51        1
  192.168.7.2     ---             Command   20XX/02/23 11:35:24  Timeout
  192.168.7.1     ---             Multicast 20XX/02/23 11:34:51        1
  192.168.7.2     ---             Command   20XX/02/23 11:34:15  Timeout
  192.168.7.1     ---             Multicast 20XX/02/23 11:33:51        1
  192.168.7.1     ---             Multicast 20XX/02/23 11:32:51        1
  192.168.7.1     ---             Multicast 20XX/02/23 11:31:51        1
  192.168.7.1     ---             Multicast 20XX/02/23 11:30:51        0

>
```

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**

10.2 **装置情報のバックアップ・リストア**

10.3 **シリーズ間の互換性**

10.4 **障害時の復旧**

10.5 **内蔵フラッシュメモリへ保存時の注意事項**

10.1 装置の状態確認，および運用形態に関する設定

10.1.1 コンフィグレーション・運用コマンド一覧

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

表 10-1 コンフィグレーションコマンド一覧

コマンド名	説明
system fan mode	装置 FAN の運転モードを設定します。
system function 【SS1250】 【SS1240】	装置のシステムファンクションリソース配分を設定します。
system l2-table mode	レイヤ 2 ハードウェアテーブルの検索方式を設定します。
system recovery	no system recovery コマンドを設定すると，装置の障害が発生したときに，本装置を再起動しないで障害状態のままにします。
system temperature-warning-level	装置の入気温度が指定温度を超過した場合に運用メッセージを出力します。
system temperature-warning-level average	指定期間の装置の平均温度が，指定温度を超えた場合に運用メッセージを出力します。

表 10-2 運用コマンド一覧（ソフトウェアバージョンと装置状態の確認）

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

表 10-3 運用コマンド一覧（MC および RAMDISK の確認）

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

表 10-4 運用コマンド一覧（ログ情報の確認）

コマンド名	説明
show logging	運用ログの採取時間・メッセージだけを一覧表示します。
clear logging	本装置で収集している運用ログを消去します。

コマンド名	説明
show critical-logging	装置障害ログの詳細情報をログレコード単位で表示します。
clear critical-logging	本装置で収集している装置障害ログを消去します。

表 10-5 運用コマンド一覧（リソース情報の確認）

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

10.1.2 ソフトウェアバージョンの確認

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

図 10-1 ソフトウェア情報の確認

```
> show version

Date 20XX/11/30 16:31:29 UTC
Model: AX1240S-24P2C
S/W: OS-LT2 Ver. 2.5 (Build:yy)
H/W: AX-1240-24P2C [sssssssssssssssssssss:R]

>
```

10.1.3 装置の状態確認

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

図 10-2 装置の状態確認

```
> show system

Date 20XX/02/12 13:54:34 UTC
System: AX2130S-24T Ver. 2.7 (Build:yy)
    Name          : -
    Contact       : -
    Locate        : -
    Machine ID    : 0012.e225.eb06
    Boot Date     : 20XX/02/08 19:14:32
    Elapsed time : 3 days 18:40:02
    LED
       ST1 LED    : Green
       Brightness mode : normal
    MC configuration mode : disabled

Environment
    Fan           : -
    Temperature   : normal
    Accumulated running time
       total      : 18 days and 6 hours
       critical   : 2 days and 15 hours

File System
    < RAMDISK information >
       used         67,584 byte
       free     12,515,328 byte
       total    12,582,912 byte
    < RAMDISK files >
    File Date                Size Name
    20XX/02/12 13:54        1,135 showtech.txt
```

```
    < MC information >
    MC : not connect

System Setting
    set terminal pager : disabled  (save: disabled)
    line console speed : 9600      (save: 9600)
    trace-monitor      : enabled   (save: enabled)
    set exec-timeout   : 0         (save: 0)

Device Resources
    IP Routing Entry(static)     :    5(max entry=128)
    IP Routing Entry(connected) :    4(max entry=128)
    IP Interface Entry          :    4(max entry=128)
    IP ARP Entry                :    3(max entry=2048)
    MAC-address Table Entry     :   16(max entry=16384)

    System Layer2 Table Mode  : 1
    Flow detection mode : layer2-2
      Used resources for filter(Used/Max)
                              MAC      IPv4
        Port 0/1-28    :       -     0/128
        VLAN           :       -     0/128
      Used resources for QoS(Used/Max)
                              MAC      IPv4
        Port 0/1-28    :       -      0/64
        VLAN           :       -      0/64

>
```

運用コマンド show environment で FAN，電源，温度の状態，累積稼働時間を確認できます。FAN の運転モードはコンフィグレーションコマンド system fan mode で設定できます。次の図に例を示します。

図 10-3　装置の環境状態の確認

```
> show environment

Date 20XX/07/06 10:10:45 UTC
Fan environment
    Fan   : active
    Mode  : 1 (silent)

Temperature environment
    Main          : 30  degrees C
    Warning level : normal

    Temperature-warning-level current status : 30/40 degrees C
    Temperature-warning-level average status : 27/35 degrees C period 30 day(s)

Accumulated running time
    total    : 808 days and 0 hours
    critical : 0 days and 0 hours

>
```

運用コマンド show environment のパラメータ temperature-logging で温度履歴情報を確認できます。次の図に例を示します。

図 10-4 温度履歴情報の確認

```
> show environment temperature-logging

Date 20XX/02/16 21:54:23 UTC
Date          0:00  6:00 12:00 18:00
20XX/02/16   30.0  30.3  28.0  27.8
20XX/02/15   31.0  32.0  29.8  31.1
20XX/02/14      -     -  29.2  30.0
20XX/02/13   29.0  30.2  28.0  15.0
20XX/02/12   28.8  30.0  30.0  28.0
20XX/02/11   31.6  32.0  28.0  28.0
20XX/02/10   31.0  30.1  28.9  29.8
20XX/02/09      -     -     -  30.1

>
```

(1) 温度監視対応時の留意事項

温度監視対応で，コンフィグレーションコマンド system temperature-warning-level を設定する場合や，温度履歴情報で温度情報を確認する場合は，以下に留意してご使用ください。

1. コンフィグレーションコマンド system temperature-warning-level で指定する温度は，装置の入気に相当する温度を指定します。これに伴い，装置内温度を入気温度に換算しますが，装置の設定環境や，使用するポート数・SFP 種別などにより，誤差が発生する場合があります。
2. 温度監視対応の機能は，装置起動後にコンフィグレーションがすべて展開されてから 60 分後に監視動作を開始します。

10.1.4 運用ログのモニタ表示実施と停止

運用コマンド trace-monitor を設定することで，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ログとして運用端末（コンソール）にモニタ表示します。例えば，通信可能状態になった場合は通信可能状態になった運用ログを，通信停止状態になった場合は通信停止状態になった運用ログを表示します。

図 10-5 運用ログのモニタ表示の実施

```
> trace-monitor enable save
>
```

save オプションを入力すると，装置を再起動してもモニタ表示を実施します。

図 10-6 運用ログのモニタ表示の停止

```
> trace-monitor disable save
>
```

注意

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

10.1.5 運用ログ情報の確認

運用ログ情報は運用端末（コンソール）にモニタ表示するほかに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，運用ログのモニタ表示と同様の内容が格納されます。運用ログとして格納する情報には次に示すものがあります。

- ユーザのコマンド操作と応答メッセージ（モニタ表示はしません）
- 装置が出力する動作情報
- 装置障害ログ情報

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，装置障害ログ情報は，運用コマンド show critical-logging でも確認できます。

10.1.6 システムファンクションリソースを使用する機能【SS1250】【SS1240】

IP8800/SS1250・IP8800/SS1240 は，コンフィグレーションコマンド system function 未設定でも全機能を使用可能です。IP8800/SS1230 とのコンフィグレーション互換のために，IP8800/SS1250・IP8800/SS1240 でコンフィグレーションコマンド system function を入力可能にしています。

10.2 装置情報のバックアップ・リストア

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

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

10.2.1 運用コマンド一覧

バックアップ・リストアに使用する運用コマンド一覧を次の表に示します。

表 10-6 運用コマンド一覧

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

10.2.2 バックアップおよびリストア実行時の対象情報

(1) 情報のバックアップ

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

これらの情報を更新したときは，バックアップファイルの作成をお勧めします。

表 10-7 バックアップファイルに保存される装置情報

装置情報種別	備考
稼働中のソフトウェア	
スタートアップコンフィグレーションファイル	
ログイン認証ユーザ ID ／ログイン認証パスワード	運用コマンド rename user 運用コマンド password
装置管理者モードパスワード	運用コマンド password enable-mode
自動ログアウト設定	運用コマンド set exec-timeout
ページング設定	運用コマンド set terminal pager
CONSOLE ポート速度設定	運用コマンド line console speed
運用ログのモニタ表示設定	運用コマンド trace-monitor
装置の障害ログ情報	運用コマンド show critical-logging
Web 認証データベース	内蔵 Web 認証 DB
Web 認証用に登録された認証画面ファイル （登録された認証画面カスタムファイルセット）	基本 Web 認証画面カスタムファイルセット 個別 Web 認証画面カスタムファイルセット
Web 認証証明書ファイル	
MAC 認証データベース	内蔵 MAC 認証 DB

装置情報種別	備考
DHCP snooping バインディングデータベース	
オプションライセンス情報	
セキュア Wake on LAN 端末情報データベース【OP-WOL】	WOL 端末情報 DB
セキュア Wake on LAN ユーザ認証データベース【OP-WOL】	WOL ユーザ認証 DB
特定端末への Web 通信不可表示機能用に登録された Web 通信不可表示画面ファイル【S2100】	
MC 運用モード【S2100】	運用コマンド set mc-configuration

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

- 運用コマンド show logging で表示される運用ログ

(2) 情報のリストア

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

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

運用コマンド restore では次に示す情報は復旧されないので注意してください。

- 運用コマンド show critical-logging で表示される障害情報

(a) バージョン変更時のカスタムファイルセットについて

本装置を Ver.2.2 以降から Ver.2.2 より前のバージョンに変更したとき，または Ver.2.2 以降でバックアップしたファイルを Ver.2.2 より前のバージョンの装置にリストアしたときは，登録したカスタムファイルセットをすべて削除します。従って，基本 Web 認証画面カスタムファイルセットおよび個別 Web 認証画面カスタムファイルセットはすべて削除し，デフォルトファイルセットに戻します。

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

10.3 シリーズ間の互換性

次の表に示す一部の装置情報はシリーズ間で互換性があります。

表 10-8 シリーズ間で互換性のある装置情報

装置情報種別	備考
Web 認証データベース	IP8800/S2100 は未サポート
Web 認証用に登録された認証画面ファイル （登録された認証画面カスタムファイルセット）	IP8800/S2100 は未サポート
MAC 認証データベース	
セキュア Wake on LAN 端末情報データベース【OP-WOL】	IP8800/S2100 は未サポート
セキュア Wake on LAN ユーザ認証データベース【OP-WOL】	IP8800/S2100 は未サポート

10.3.1 IP8800/SS1250・IP8800/SS1240 と IP8800/SS1230 の入力コマンドの互換性

(1) コンフィグレーションコマンド

下記のコンフィグレーションコマンドは，IP8800/SS1250・IP8800/SS1240 シリーズで入力形式などを変更しています。

IP8800/SS1230 形式で IP8800/SS1250・IP8800/SS1240 に入力可能ですが，IP8800/SS1250・IP8800/SS1240 の対応は以下となります。

- IP8800/SS1230 形式のヘルプや補完，および短縮入力は対応しません。
- IP8800/SS1230 形式で入力すると装置内部で IP8800/SS1250・IP8800/SS1240 形式に自動変換します。
- コンフィグレーションの表示および保存は IP8800/SS1250・IP8800/SS1240 形式となります。

表 10-9 コンフィグレーションコマンド

IP8800/SS1250・IP8800/SS1240 のコマンド	IP8800/SS1230 からの変更内容
system function	コマンド省略時の動作変更※
deny (ip access-list extended) deny (ip access-list standard) deny (mac access-list extended) permit (ip access-list extended) permit (ip access-list standard) permit (mac access-list extended) qos(ip qos-flow-list) qos(mac qos-flow-list) monitor session	入力形式の変更
ip qos-flow-list mac qos-flow-list	コマンドの変更
ip qos-flow-list resequence mac qos-flow-list resequence	入力モードの変更

注※

IP8800/SS1230 の system function 設定済みコンフィグレーションファイルを，本装置で復元したときは設定値を引き継ぎます。system function 未設定の場合は IP8800/SS1250・IP8800/SS1240 のデフォルト値で動作します。

詳細は「10.1.6 システムファンクションリソースを使用する機能【SS1250】【SS1240】」を参照してください。
各コマンドの詳細は，「コンフィグレーションコマンドレファレンス」を参照してください。

(2) 運用コマンド

下記の運用コマンドは，IP8800/SS1250・IP8800/SS1240 シリーズでコマンド名や入力形式などを変更しています。表示内容および動作上の変更はありません。

表 10-10 運用コマンド

IP8800/SS1250・IP8800/SS1240 のコマンド	IP8800/SS1230 からの変更内容
show logging	show event-trace を show logging に変更 show event-trace additional は廃止
clear logging	clear event-trace を clear logging に変更
show critical-logging	show log を show critical-logging に変更
clear critical-logging	clear log を clear critical-logging に変更
set clock show vlan mac-vlan show access-filter show qos-flow show qos queueing clear mac-authentication auth-state	入力形式の変更

各コマンドの詳細は，「運用コマンドレファレンス」を参照してください。

10.3.2 IP8800/SS1250 と IP8800/SS1240 の装置情報の互換性

IP8800/SS1250 と IP8800/SS1240 間の装置情報の互換性を次の表に示します。

- 矢印の左辺はバックアップファイルを作成した装置を示します。
- 矢印の右辺はファイルを復元する装置を示します。

表 10-11 IP8800/SS1250 と IP8800/SS1240 の装置情報の互換性

装置情報種別	IP8800/SS1240 → IP8800/SS1250	IP8800/SS1250 → IP8800/SS1240
稼働中のソフトウェア	×	×
スタートアップコンフィグレーションファイル	△※1	○
ログイン認証ユーザ ID ／ログイン認証パスワード	○	○
装置管理者モードパスワード	○	○
自動ログアウト設定	○	○
ページング設定	○	○
CONSOLE ポート速度設定	○	○
運用ログのモニタ表示設定	○	○
装置の障害ログ情報	×※2	×※2
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 （登録された認証画面カスタムファイルセット）	○	○
Web 認証証明書ファイル	○	○
MAC 認証データベース	○	○

装置情報種別	IP8800/SS1240 → IP8800/SS1250	IP8800/SS1250 → IP8800/SS1240
DHCP snooping バインディングデータベース	○	○
オプションライセンス有無	○	○
セキュア Wake on LAN 端末情報データベース【OP-WOL】	○	○
セキュア Wake on LAN ユーザ認証データベース【OP-WOL】	○	○

（凡例）
○：互換性あり
×：互換性なし
△：制限あり
→：作成したファイルの復元先

注※ 1
IP8800/SS1250 で未サポートのコマンドは読み込み不可です。

注※ 2
運用コマンド restore では復旧されません。

10.3.3 IP8800/SS1250・IP8800/SS1240 と IP8800/SS1230 の装置情報の互換性

IP8800/SS1250・IP8800/SS1240 と IP8800/SS1230 間の装置情報の互換性を次の表に示します。

IP8800/SS1250・IP8800/SS1240 の装置情報 (ソフトウェア以外）を IP8800/SS1230 で復元するときは，運用コマンド backup で "AX1230" オプションを指定し，バックアップファイルを作成してください。（"AX1230" オプションを指定しないで作成したバックアップファイルは，IP8800/SS1230 で復元できません。）

- 矢印の左辺はバックアップファイルを作成した装置を示します。
- 矢印の右辺はファイルを復元する装置を示します。

表 10-12 IP8800/SS1250・IP8800/SS1240 と IP8800/SS1230 の装置情報の互換性

装置情報種別	IP8800/SS1230 → IP8800/SS1250・IP8800/SS1240	IP8800/SS1250・IP8800/SS1240 → IP8800/SS1230
稼働中のソフトウェア	×	×
スタートアップコンフィグレーションファイル	○	△※1
ログイン認証ユーザ ID ／ログイン認証パスワード	○	○
装置管理者モードパスワード	○	○
自動ログアウト設定	○	○
ページング設定	○	○
CONSOLE ポート速度設定	○	○
運用ログのモニタ表示設定	○	○
装置の障害ログ情報	×※2	×※2
Web 認証データベース	○	△※4※5
Web 認証用に登録された認証画面ファイル（登録された認証画面カスタムファイルセット）	△※3	△※6

装置情報種別	IP8800/SS1230 → IP8800/SS1250・IP8800/SS1240	IP8800/SS1250・IP8800/SS1240 → IP8800/SS1230
Web 認証証明書ファイル	○	△※4
MAC 認証データベース	○	△※4
DHCP snooping バインディングデータベース	○	△※4
オプションライセンス有無	－	×
セキュア Wake on LAN 端末情報データベース【OP-WOL】	－	×
セキュア Wake on LAN ユーザ認証データベース【OP-WOL】	－	×

（凡例）
○：互換性あり
×：互換性なし
△：制限あり
－：未サポートのため，バックアップファイルに含まれない
→：作成したファイルの復元先

注※ 1
IP8800/SS1230 で未サポートのコマンドは読み込み不可です。

注※ 2
運用コマンド restore では復旧されません。

注※ 3
IP8800/SS1230 のソフトウェアバージョンによっては，Web 認証入れ替え画面ファイルに Web 認証固有タグの追加設定が必要です。

表 10-13　Web 認証入れ替え画面ファイルの Web 認証固有タグの追加設定

IP8800/SS1230 のバージョン	Web 認証固有タグの追加設定
Ver.1.2 ～ 1.2.x	自動 URL 表示用の Web 認証固有タグ（"<!-- Redirect_URL -->"）と，ログイン成功後に表示する URL と URL へ移動するまでの時間（コンフィグレーションコマンド web-authentication jump-url の設定内容）を記述します。
Ver.1.3 ～ 1.3.x	自動 URL 表示用の Web 認証固有タグ（"<!-- Redirect_URL -->"）に，指定 URL へ移動するまでの時間を記述してください。時間はコンフィグレーションコマンド web-authentication jump-url のパラメータ delay に合わせてください。
Ver.1.4 以降	追加不要です。

なお，ワンタイムパスワード認証を使用するときは，Web 認証入れ替え画面ファイルと Web 認証固有タグが追加になります。詳細は，「コンフィグレーションガイド Vol.2　14　ワンタイムパスワード認証【OP-OTP】」を参照してください。

注※ 4
IP8800/SS1230 のソフトウェアバージョン 1.3 以降のときに復旧できます。

注※ 5
内蔵 Web 認証 DB を IP8800/SS1230 で復旧するときは，下記に注意してください。運用コマンド store web-authentication で作成したバックアップファイルも同様です。

1. ユーザ ID が 17 文字以上のエントリを含んでいるときは，内蔵 Web 認証 DB を IP8800/SS1230 に読み込みません。
2. 全エントリのユーザ ID が 16 文字以下のときは，内蔵 Web 認証 DB を IP8800/SS1230 に読み込みます。た

だし，パスワードが 17 文字以上のエントリに該当するユーザは認証できません。

注※ 6

Ver.2.2 以降のカスタムファイルセット（基本 Web 認証画面，個別 Web 認証画面）形式は，IP8800/SS1230 で未サポートのため削除され，初期状態のデフォルトファイルセットに戻ります。

10.4 障害時の復旧

10.4.1 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 10-14 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	IP8800/S2200 IP8800/S2100 IP8800/SS1250 IP8800/SS1240
メインボード	装置再起動により，復旧を試みます。	装置を再起動します。※	装置内の全ポートを介する通信が中断されます。	○
SW チップ	内蔵メモリのパリティエラー発生時，自動復旧を実施します。復旧後，障害が継続する場合，装置再起動による復旧を実施します。	発生箇所を正常状態に設定します。※	通信に影響があります。	○
ポート障害	実施しません。	自動復旧はありません。	該当するポートを介する通信に影響する場合があります。	－
電源異常	装置の運用に必要な電力が供給されなくなると装置再起動します。	装置を再起動します。	装置内の全ポートを介する通信が中断されます。	○
FAN	実施しません。	自動復旧はありません。	影響はありません。	－

（凡例）
○：自動復旧あり
－：自動復旧なし

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

(1) 自動復旧停止状態について

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

なお，本装置が自動復旧停止状態中は，下記に注意してください。

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

(a) 自動復旧停止状態中の装置状態情報の採取

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

自動復旧停止状態中の運用コマンド show tech-support の実行では，コンソール画面への表示だけが許可

されます。従って，本コマンドの実行では "ramdisk" や "page" オプションを指定しないでください。また，本コマンドの実行でコンソール画面に表示される情報は，端末のキャプチャ機能などを利用して，採取してください。また，自動復旧停止状態で本コマンド実行中は Ctrl+C を入力しないでください。

(b) 本装置の復旧

本装置の自動復旧停止状態は，下記により復旧します。

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

(c) 自動復旧停止状態中の省電力機能について

スケジューリングによる省電力機能を設定している場合は，スケジューリングを停止し，設定した省電力機能（LED 動作やポート省電力，または装置スリープ）の実行を抑止します。

10.5 内蔵フラッシュメモリへ保存時の注意事項

本装置はソフトウェア，コンフィグレーション，ログ情報など装置情報の保存先として内蔵フラッシュメモリを使用しています。

内蔵フラッシュメモリはデバイスの一般的な特性上，書き換え可能な回数に上限があり，これを上回る書き換えが発生した場合には，内蔵フラッシュメモリの故障に至る可能性があります。

本装置の内蔵フラッシュメモリへの書き込み契機は，コンフィグレーションの保存や，装置への一部の運用コマンドの実行により発生し，この操作を 30 分周期で継続して行うと，6 年程度で書き込み上限値に到達する可能性があります。

(1) コンフィグレーションコマンド

内蔵フラッシュメモリへの書き込み契機となる主なコンフィグレーションコマンドを，次に示します。

- save（write）
- ip dhcp snooping database url flash

(2) 運用コマンド

内蔵フラッシュメモリへの書き込み契機になる主な運用コマンドを，次の表に示します。

表 10-15 内蔵フラッシュメモリへの書き込み契機になる主な運用コマンド

分類	運用コマンド
運用端末とリモート操作	set terminal pager save※，set exec-timeout save※，line console speed save，trace-monitor save
コンフィグレーションとファイルの操作	copy，erase startup-config
ログインセキュリティと RADIUS	password，clear password，rename user
装置の管理	restore，reload
MC 運用モード機能【S2100】	set mc-configuration
ログ	clear logging，clear critical-logging
ソフトウェアの管理	ppupdate，set license，erase license
リソース情報	format flash
Web 認証	commit web-authentication，load web-authentication， set web-authentication html-files，clear web-authentication html-files
MAC 認証	commit mac-authentication，load mac-authentication
セキュア Wake on LAN	commit wol-device，load wol-device，commit wol-authentication，load wol-authentication
特定端末への Web 通信不可表示機能	set access-redirect html-file，clear access-redirect html-file

本装置では，ログイン・ログアウトによる内蔵フラッシュメモリへの書き込みはありません。

11 MC 運用モード機能【S2100】

この章では，MC 運用モード機能について説明します。

11.1 MC 運用モード機能の解説

11.2 MC 運用モード機能のコンフィグレーション

11.3 MC 運用モード機能のオペレーション

11.1 MC 運用モード機能の解説

11.1.1 概要

本装置は通常内蔵フラッシュメモリのソフトウェアと装置情報で起動されますが，MC 運用モード機能を使用することで，以下の動作が可能です。

装置起動時：

ソフトウェアと装置情報をあらかじめ格納した MC を挿入し，本装置を起動すると，MC 内のソフトウェアと装置情報で起動されます。内蔵フラッシュメモリと MC 内の情報に差分がある場合は内蔵フラッシュメモリが更新されます。

運用中の MC 挿入時：

運用中に MC を挿入することで，自動的にソフトウェアと装置情報が一括で MC に保存されます。

MC 出力コマンド実行時：

運用コマンド update mc-configuration を実行することで，ソフトウェアと装置情報が一括で MC に保存されます。

MC 運用モードが有効の場合は，以下に示すコマンド実行時に該当コマンドの動作に加えて運用コマンド update mc-configuration の処理も自動的に実行されます。

- コンフィグレーションを save コマンドで保存時
- 運用コマンド copy でコピー先にスタートアップコンフィグレーションファイルを指定時
- 運用コマンド ppupdate 実行時

11.1.2 MC に保存されるファイル

本機能を使用時に MC に保存されるファイルを次に示します。

表 11-1 MC に保存されるファイル

項目	内容	MC に保存される名称
ソフトウェア	稼働中のソフトウェア	k.img
装置情報	運用コマンド backup 相当の装置情報※ ただし，DHCP snooping バインディングデータベースは対象外です。	axsroot/

注※

対象の装置情報については「10.2.2 バックアップおよびリストア実行時の対象情報」を参照してください。

11.1.3 本機能を使用した運用手順

本機能はシステム導入，構成変更，装置交換など，装置メンテナンス作業で利用できます。その際は，以下に示す手順で実施してください。

＜システム導入時＞

1. MC をフォーマットしてください。

   本装置に MC を挿入し，運用コマンド format mc を実行してください。

2. MC 運用モードを設定してください。
   運用コマンド set mc-configuration を実行してください。
3. システム構築後，各装置のソフトウェアと装置情報を MC に保存してください。
   運用コマンド update mc-configuration を実行してください。
4. MC を挿入したまま運用してください。

＜システム構成変更時＞

1. システム再構築後，各装置のソフトウェアと装置情報を MC に保存してください。
   運用コマンド update mc-configuration を実行してください。

＜装置交換時＞

1. 新しい装置を用意します。
2. 新しい装置の装置情報をクリアしてください。
   運用コマンド format flash を実行してください。
3. 新しい装置に MC 運用モードを設定してください。
   運用コマンド set mc-configuration を実行してください。
4. 新しい装置を電源 OFF してください。
5. 新しい装置に MC を挿入してください。（交換前の装置のソフトウェアと装置情報を保存した MC）
6. 新しい装置を電源 ON してください。

＜予備の MC を作成する場合＞

1. 新しい MC を用意します。
2. 該当装置に MC を挿入してください。
   または運用コマンド update mc-configuration を実行してください。
   装置のソフトウェアと装置情報が一括で MC に保存されます。

11.1.4 障害時の動作

MC 運用モード時に MC 障害を検出した場合の動作を次の表に示します。

表 11-2 MC 運用モードで MC 障害検出時の動作

イベント契機	障害要因	動作
装置起動時	MC 未搭載	内蔵フラッシュメモリのソフトウェアおよび装置情報で起動されます。 また，MC 内の情報の読み込みに失敗したことを示す運用ログが採取されます。
	MC 読み込み失敗	
MC 挿入時	MC 書き込み失敗	MC 出力失敗を示す運用ログが採取されます。 また，MC アクセス LED（ACC LED）を 1 秒間隔で緑点滅します。※3
	MC ライトプロテクト	
	MC 空き容量不足	
MC 出力コマンド※1 実行時	MC 未搭載	コマンド実行エラーメッセージが表示されます。 運用ログは採取されません。 MC アクセス LED（ACC LED）は緑点滅しません。
	MC 書き込み失敗	
	MC ライトプロテクト	
	MC 空き容量不足	

イベント契機	障害要因	動作
上記以外のコマンド※2 実行時	MC 未搭載	MC 出力失敗を示す運用ログが採取されます。 MC アクセス LED（ACC LED）は緑点滅しません。
	MC 書き込み失敗	
	MC ライトプロテクト	
	MC 空き容量不足	

注※ 1

運用コマンド update mc-configuration

注※ 2

- コンフィグレーションを save コマンドで保存時
- 運用コマンド copy でコピー先にスタートアップコンフィグレーションファイルを指定時
- 運用コマンド ppupdate 実行時

注※ 3

ACC LED が緑点滅の時は，MC を取り出して運用ログを確認してください。

11.1.5 他機能との共存

本機能で動作中は，コマンドレス保守機能※を使用できません。

注※

コマンドレス保守機能は初期状態で有効ですが，MC 運用モードが有効の場合は，コマンドレス保守機能は動作しません。

11.1.6 MC 運用モード機能使用時の注意事項

(1) MC に保存されたディレクトリ・ファイルについて

運用コマンド update mc-configuration，または MC 挿入によって，「表 11-1　MC に保存されるファイル」に示す名称で MC 内に保存されたソフトウェアや装置情報は，追加・変更・削除を行わないでください。また，名称も変更しないでください。

(2) MC の抜き挿しについて

- 装置起動時は，MC 内のソフトウェアと装置情報で起動し，かつ内蔵フラッシュメモリにソフトウェアと装置情報を保存するため MC にアクセスしています。MC アクセス LED（ACC LED）が点灯している間は MC を抜かないでください。
- MC を挿入した場合は，内蔵フラッシュメモリのソフトウェアと装置情報を MC に書き込んでいます。MC アクセス LED（ACC LED）が点灯している間は MC を抜かないでください。
- MC にアクセスする運用コマンドの実行中に，MC の抜き挿しを行わないでください。MC の抜き挿しを正しく検出できない場合があります。

11.2 MC 運用モード機能のコンフィグレーション

11.2.1 コンフィグレーションコマンド一覧

MC 運用モード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 11-3 コンフィグレーションコマンド一覧

コマンド名	説明
save(write) ※	編集したコンフィグレーションの内容を，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ます。MC 運用モードが有効の場合は，運用コマンド update mc-configuration の処理も自動的に実行されます。

注※

「コンフィグレーションコマンドレファレンス 3 コンフィグレーションの編集と操作」を参照してください。

11.3 MC 運用モード機能のオペレーション

11.3.1 運用コマンド一覧

MC 運用モード機能の運用コマンド一覧を次の表に示します。

表 11-4 運用コマンド一覧

コマンド名	説明
set mc-configuration	MC 運用モード機能を設定します。
update mc-configuration	稼働中のソフトウェアおよび装置の情報を，MC に出力します。
copy ※1	指定したファイルまたはディレクトリをコピーします。MC 運用モードが有効の場合は，コピー先がスタートアップコンフィグレーションファイルのときに，運用コマンド update mc-configuration の処理も自動的に実行されます。
ppupdate ※2	MC から RAMDISK にコピーした新しいソフトウェア，または ftp 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。MC 運用モードが有効の場合は，運用コマンド update mc-configuration の処理も自動的に実行されます。

注※1

「運用コマンドレファレンス 4 コンフィグレーションとファイルの操作」を参照してください。

注※2

「運用コマンドレファレンス 12 ソフトウェアの管理」を参照してください。

12 省電力機能

この章では，省電力を目的とした機能と本装置の設定について説明します。

12.1 **省電力機能の解説**

12.2 **省電力機能のコンフィグレーション**

12.3 **省電力機能のオペレーション**

12.1 省電力機能の解説

本装置は，省電力機能で夜間や長期連休時などに計画的に装置スリープ状態とすることで，装置の消費電力を抑えることができます。

12.1.1 サポートする省電力機能

本装置でサポートしている省電力機能は，常時省電力で動作させることも，スケジューリングによって省電力で動作させる時間帯を限定することもできます。通常時間帯に動作する省電力機能とスケジュール時間帯に動作する省電力機能を次の表に示します。

なお，省電力のスケジュールを設定している時間帯を「スケジュール時間帯」，スケジュールを設定していない時間帯を「通常時間帯」と呼びます。

表 12-1 省電力機能サポート一覧

機能	内容	通常時間帯の設定	スケジュール時間帯専用の設定	IP8800/S2200 IP8800/S2100	IP8800/SS1250 IP8800/SS1240
LED 動作	通常輝度，省電力輝度，消灯	○	○	○※3	○
	自動動作の契機	○	×	○※3	○
ポート省電力	リンクダウンポートの省電力機能※1	○	○	○	○
	Gigabitethernet ポートの拡張省電力機能※1	○	○	×	○
	ポート閉塞（ポート未使用設定）	○	○	○	○
装置スリープ	本装置の電源 OFF，自動 ON	×	○	×	○
冷却 FAN 制御機能（準 FAN レス動作）※2	温度変化による冷却 FAN の OFF/ON	○	×	×	○

（凡例）

○：サポート

×：未サポート

注※ 1

Fastethernet ポートおよび Gigabitethernet ポートが対象です。SFP ポートは対象外です。

注※ 2

対象は IP8800/SS1240-48T2C だけです。

注※ 3

通常輝度，消灯をサポートします。省電力輝度は未サポートです。

本章では各ポートを以下で表記します。

- 10BASE-T/100BASE-TX ポート：Fastethernet ポート
- 10BASE-T/100BASE-TX/1000BASE-T ポート：Gigabitethernet ポート
- 100BASE-FX【SS1250】/1000BASE-X ポート：SFP ポート

12.1.2 LED 動作

本機能ではコンフィグレーションにより LED の動作を，IP8800/S2200・IP8800/S2100 は２段階，IP8800/SS1250・IP8800/SS1240 は３段階で制御します。また，コンフィグレーションで自動動作の契機を設定することで，LED 動作を自動変更することも可能です。

(1) LED 動作内容

コンフィグレーションコマンド system port-led により，以下の LED 動作のいずれかを設定します。

- 通常輝度：使用中の LED 点灯および点滅は，通常輝度で動作します。
- 省電力輝度：使用中の LED 点灯および点滅は，通常輝度に対して減光状態で動作します。
- 消灯：全ポートの LED を消灯します。（ST1/ACC は減光状態もあります。）

コンフィグレーションによる制御対象は下記の LED です。PWR LED は制御対象外で , 点灯時は常に「通常輝度」で動作します。LED の説明については，「ハードウェア取扱説明書」を参照してください。

- ST1
- ACC
- LINK
- T/R
- 1 ～ 24：IP8800/SS1240-48T2C 以外の全モデル
- 1 ～ 48：IP8800/SS1240-48T2C

コンフィグレーションコマンド system port-led の LED 動作設定による，各種 LED の状態を次の表に示します。

表 12-2 コンフィグレーションの LED 動作設定別の各種 LED 状態【S2200】【S2100】

LED 種別	装置状態	コンフィグレーションコマンド system port-led の LED 動作設定			
		通常輝度（enable）		消灯（disable）	
		LED 状態	輝度状態	LED 状態	輝度状態
ST1	動作可能	緑点灯	通常	長い間隔の緑点滅	通常
	準備中	緑点滅	通常	緑点滅	通常
	初期状態	橙点灯	通常	橙点灯	通常
	部分障害	赤点滅	通常	赤点滅	通常
	致命的障害	赤点灯	通常	赤点灯	通常
	電源 OFF 電源異常	消灯	－	消灯	－
ACC	アクセス中	緑点灯	通常	緑点灯	通常
	アイドル中	消灯	－	消灯	－
LINK/ T/R ※1	リンク確立	緑点灯	通常	消灯	－
	送受信中	緑点滅	通常	消灯	－
	リンク未確立	消灯	－	消灯	－
	障害	消灯	－	消灯	－

LED 種別	装置状態	コンフィグレーションコマンド system port-led の LED 動作設定			
		通常輝度（enable）		消灯（disable）	
		LED 状態	輝度状態	LED 状態	輝度状態
1-24 ※2	リンク確立	緑点灯	通常	消灯	－
	送受信中	緑点滅	通常	消灯	－
	障害	消灯	－	消灯	－

注※1
SFP ポートです。

注※2
Gigabitethernet ポートです。

表 12-3　コンフィグレーションの LED 動作設定別の各種 LED 状態【SS1250】【SS1240】

LED 種別	装置状態	コンフィグレーションコマンド system port-led の LED 動作設定					
		通常輝度（enable）		省電力輝度（economy）		消灯（disable）	
		LED 状態	輝度状態	LED 状態	輝度状態	LED 状態	輝度状態
ST1	動作可能	緑点灯	通常	緑点灯	減光	長い間隔の緑点滅	減光
	準備中	緑点滅	通常	緑点滅	通常	緑点滅	通常
	初期状態	橙点灯	通常	橙点灯	通常	橙点灯	通常
	部分障害	赤点滅	通常	赤点滅	減光	赤点滅	減光
	致命的障害	赤点灯	通常	赤点灯	減光	赤点灯	減光
	電源 OFF 電源異常	消灯	－	消灯	－	消灯	－
ACC	アクセス中	緑点灯	通常	緑点灯	減光	緑点灯	減光
	アイドル中	消灯	－	消灯	－	消灯	－
LINK ※1	リンク確立	緑点灯	通常	緑点灯	減光	消灯	－
	リンク未確立	消灯	－	消灯	－	消灯	－
	障害	消灯	－	消灯	－	消灯	－
T/R ※1	送受信中	緑点滅	通常	緑点滅	減光	消灯	－
	障害	消灯	－	消灯	－	消灯	－
1-24 ※2 1-48 ※2	リンク確立	緑点灯	通常	緑点灯	減光	消灯	－
	送受信中	緑点滅	通常	緑点滅	減光	消灯	－
	障害	消灯	－	消灯	－	消灯	－

注※1
Gigabitethernet/SFP ポートです。

注※2
Fastethernet ポートです。

（2）LED 自動動作の契機

コンフィグレーションコマンド system port-led trigger で「表 12-4　自動動作の契機と動作内容」に示す

自動動作の契機を設定しておくことで，LED 動作を自動変更できます。コンフィグレーションコマンド system port-led は「通常輝度（enable)」を設定してください。

自動動作の契機と動作内容を次の表に示します。

表 12-4　自動動作の契機と動作内容

自動動作の契機	動作内容
コンソール （RS-232C）	コンソール接続による装置へのログインを契機に通常輝度で点灯します。 ログイン中はタイマ制御を停止し，通常輝度を継続します。 ログアウト後，タイマ制御により省電力輝度，消灯に遷移します。
MC	MC の挿抜を契機に通常輝度で点灯します。 タイマ制御により，省電力輝度，消灯に遷移します。
物理ポート	指定した物理ポートのリンクアップまたはリンクダウンを契機に通常輝度で点灯します。 タイマ制御により，省電力輝度，消灯に遷移します。

自動動作の契機は複数設定できます。

LED 自動動作の遷移を次の図に示します。

図 12-1　LED 自動動作の遷移【S2200】【S2100】

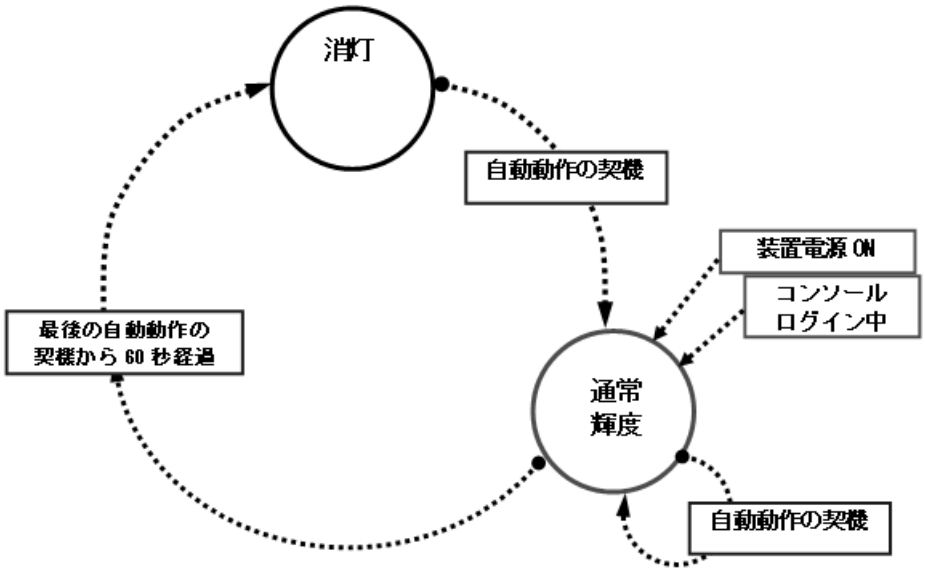
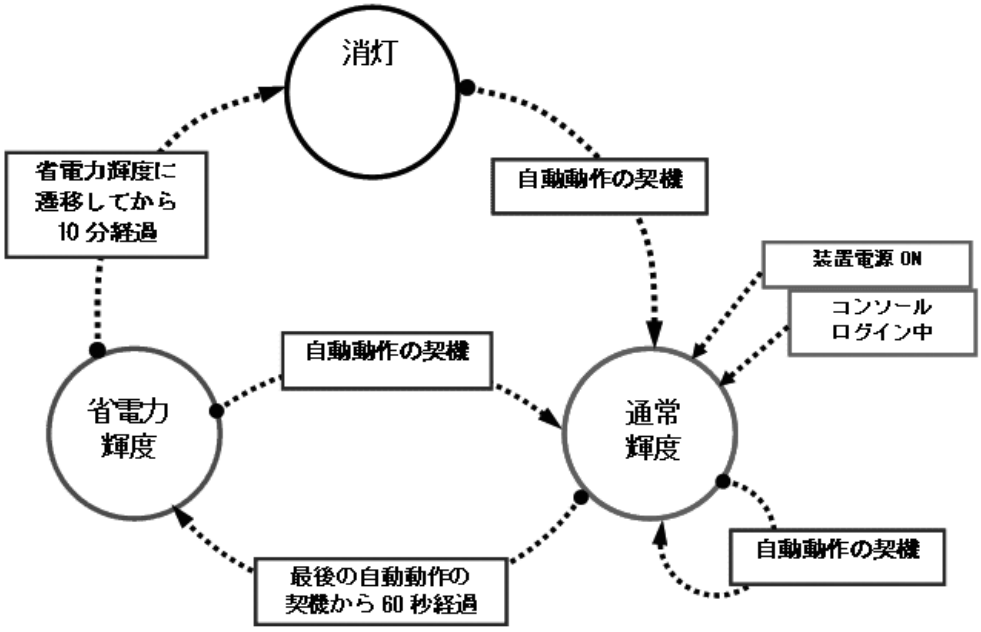


図 12-2　LED **自動動作の遷移**【SS1250】【SS1240】



自動動作の契機は,「表 12-4　自動動作の契機と動作内容」に従いますが，遷移条件は「自動動作の契機」と「タイマ制御」があります。

1. 通常輝度へ遷移する条件
   通常輝度への遷移は,「表 12-4　自動動作の契機と動作内容」のいずれかに従います。
2. 省電力輝度へ遷移する条件【SS1250】【SS1240】
   通常輝度から省電力輝度への遷移はタイマ制御で実施します。最後の自動動作の契機から 60 秒経過後に省電力輝度へ遷移します。
   継続的に通常輝度へ自動動作の契機が発生したときも，最後の自動動作の契機から 60 秒経過後に省電力輝度へ遷移します。
3. 消灯へ遷移する条件
   消灯への遷移はタイマ制御で実施します。最後に通常輝度へ遷移してから 60 秒経過後に消灯へ遷移します。【S2200】【S2100】
   消灯への遷移はタイマ制御で実施します。最後に省電力輝度へ遷移してから 10 分経過後に消灯へ遷移します。【SS1250】【SS1240】
   なお，通常輝度から消灯へは遷移しません。

自動動作の制御対象を次の表に示します。なお，PWR LED は制御対象外で , 点灯時は常に「通常輝度」で動作します。

表 12-5 自動動作の制御対象と動作範囲【S2200】【S2100】

LED 種別	LED 動作種別と自動動作の動作範囲		動作内容
	通常輝度	消灯	
ST1	○	－	常時通常輝度で点灯します。
ACC			
LINK/ T/R ※1		○	２段階の輝度制御によって，点灯状態が変化します。
1-24 ※2			

（凡例）
○：制御対象
－：制御対象外

注※ 1
SFP ポートの LED です。

注※ 2
Gigabitethernet ポートの LED です。

表 12-6 自動動作の制御対象と動作範囲【SS1250】【SS1240】

LED 種別	LED 動作種別と自動動作の動作範囲			動作内容
	通常輝度	省電力輝度	消灯	
ST1	○	○	－	省電力輝度，消灯のどちらの状態でも，省電力輝度で点灯します。
ACC				
LINK ※1			○	３段階の輝度制御によって，点灯状態が変化します。
T/R ※1				
1-24 ※2 1-48 ※2				

（凡例）
○：制御対象
－：制御対象外

注※ 1
Gigabitethernet/SFP ポートの LED です。

注※ 2
Fastethernet ポートの LED です。

12.1.3 ポート省電力

本機能は，イーサネットポートが非アクティブ状態のときに，ポートの電力ダウンを実施し，消費電力を削減します。

ポート省電力では以下の機能を実施できます。

- リンクダウンポートの省電力機能（Fastethernet ポート，Gigabitethernet ポート）
- Gigabitethernet ポートの拡張省電力機能（Gigabitethernet ポート）【SS1250】【SS1240】
- ポート閉塞（Fastethernet ポート，Gigabitethernet ポート，SFP ポート）

(1) リンクダウンポートの省電力機能

LAN ケーブルが未接続のポートや相手装置の電源断などでリンクがダウン状態のポートで，LAN ケーブルの電気信号を検出できないときに電気信号を検出するまでそのポートの消費電力を削減できます。本機能を使用すると，リンクダウン中のポートで消費電力を削減できますが，リンクアップまでの時間は長くなります。

本機能を使用するには，コンフィグレーションコマンド power-control port cool-standby でリンクダウンポートの消費電力を削減する設定をします。この設定は装置で一括の設定となり，ポート単位では設定できません。

また，リンクダウン時に消費電力が削減できるポートは Fastethernet ポート，Gigabitethernet ポートだけです。SFP ポートは，リンクダウンポート省電力機能の対象外です。

リンクダウンポートの省電力動作条件を次の表に示します。

表 12-7 リンクダウンポートの省電力動作条件

コンフィグレーション設定	shutdown ※		no shutdown	
	電気信号の検出		電気信号の検出	
	無	有	無	有
power-control port cool-standby	○ （リンクダウン）	○ （リンクダウン）	○ （リンクダウン）	－ （リンクアップ）
no power-control port cool-standby	○ （リンクダウン）	○ （リンクダウン）	－ （リンクダウン）	－ （リンクアップ）

（凡例）
○：リンクダウンポート省電力機能が有効で，省電力状態で運用します。
－：リンクダウンポート省電力機能が無効で，通常の消費電力で運用します。

注※
コンフィグレーションコマンド shutdown 設定，または SNMP マネージャからの SetRequest オペレーションによる ifAdminStatus の Set 実行が該当します。

(2) Gigabitethernet ポートの拡張省電力機能【SS1250】【SS1240】

本機能は，コンフィグレーションコマンド power-control port cool-standby 設定有無に関わらず，本装置の 2 つの Gigabitethernet ポートが shutdown 設定のときに有効となります。また，コンフィグレーションコマンド power-control port cool-standby 設定よりも，さらに消費電力を低減します。

また，拡張省電力機能で消費電力が削減できるポートは Gigabitethernet ポートだけです。SFP ポートは Gigabitethernet ポート拡張省電力機能の対象外です。

表 12-8 Gigabitethernet ポート拡張省電力機能の動作条件

Gigabitethernet ポート 0/25 ※の設定	Gigabitethernet ポート 0/26 ※の設定	
	shutdown	no shutdown
shutdown	○	－
no shutdown	－	－

（凡例）
○：Gigabitethernet ポート拡張省電力機能が有効で，省電力状態で運用します。

－：Gigabitethernet ポート拡張省電力機能が無効で，通常の電力消費で運用します。

注※
IP8800/SS1240-48T2C は，0/49 と 0/50 が対象です。

(3) ポート閉塞

コンフィグレーションコマンド shutdown 設定によりポートをシャットダウンしておくことで，未使用ポートや意図しない PoE 受電装置への給電を停止し，消費電力の削減を図ります。

前述の「(1) リンクダウンポートの省電力機能」や「(2) Gigabitethernet ポートの拡張省電力機能【SS1250】【SS1240】」と併用して，ポートの消費電力を削減できます。

12.1.4 装置スリープ【SS1250】【SS1240】

装置スリープは，省電力機能のスケジューリングにより実施します。スケジューリングの詳細は，後述の「12.1.6 省電力機能のスケジューリング」を参照してください。

装置スリープは，特定の時間帯に装置本体電源を OFF，設定した時間に自動電源 ON による起動を行います。スリープ中は，PWR LED が長い間隔の緑点滅状態となり，スイッチング機能（フレーム中継），リモートアクセスなどすべての機能を停止します。

装置スリープ機能には，スケジュール時間満了でスリープ解除による本装置の起動とは別に，管理者が意図的に本装置を起動する手段として強制スリープ解除があります。

(1) 強制スリープ解除

装置スリープ状態のときに，装置正面の RESET スイッチを正面の LED が全点灯するまで長押し（3秒以上）してください。装置スリープ状態を解除します。このときスケジュール抑止モードで本装置を起動します。

12.1.5 冷却 FAN 制御機能（準 FAN レス動作）【SS1240】

本機能は，装置内温度監視により設置環境が良好な場所で装置の強制冷却が不要のときは FAN を停止し，環境温度が高いときは FAN を動作して強制冷却します（準 FAN レス動作）。これにより，良好な設置環境での騒音防止と，消費電力の低減を図ることができます。

本機能は，コンフィグレーションコマンド system fan-control を設定することで有効となります（未設定のときは，FAN を常時動作します）。

コンフィグレーション設定時の FAN 動作・停止条件

- FAN 動作条件：装置内温度 47 ℃以上を検出時に動作
- FAN 停止条件：装置内温度 46 ℃以下を検出後，46 ℃以下の状態が 10 分経過後に停止

本機能は IP8800/SS1240-48T2C モデルだけが対象です。また，本機能設定状態で装置を起動したときでも，装置起動直後の約 10 分間は必ず冷却 FAN が動作しています。

なお，本機能と温度監視対応の FAN 運転モード（system fan mode）を同時設定した場合は，温度監視対応の FAN 運転モード (system fan mode) が優先されます。

次の表に本機能と FAN 運転モードを同時設定したときの FAN 動作状態を示します。

表 12-9 本機能と FAN 運転モードを同時設定したときの FAN 動作状態

準 FAN レス動作の設定（system fan-control）	FAN 運転モードの設定（system fan mode）	FAN 動作状態	備考
設定有	system fan mode 2	常時動作	冷却重視と同一動作（system fan-control は無効）
	system fan mode 1 または設定無	準 FAN レス動作	
設定無	system fan mode 2	常時動作	冷却重視と同一動作
	system fan mode 1 または設定無	常時動作	

12.1.6 省電力機能のスケジューリング

時間帯を指定して省電力機能を実行する場合はスケジューリングをします。スケジューリングは，実行する省電力機能の組み合わせと実施したい時間帯を指定します。これらの指定によって，開始時刻になると，自動的に省電力機能が実行されます。また，すでに実行中の省電力機能をある時間帯だけ無効にするスケジューリングもできます。なお，省電力のスケジュールを設定している時間帯をスケジュール時間帯，スケジュールを設定していない時間帯を通常時間帯と呼びます。

(1) スケジュールに指定できる省電力機能

スケジュールは，実行する省電力機能と時間帯で設定します。設定できる省電力機能を次に示します。スケジューリングの際には，これらの機能の中から目的に合わせて一つまたは複数選択し，同時に実行する機能の組み合わせを決めます。

なお，スケジュールで設定できる機能の組み合わせは，装置単位で 1 組だけです。

- LED 動作
- ポート省電力
- 装置スリープ【SS1250】【SS1240】

(a) スケジューリングによる LED 動作

スケジュール設定に従い，スケジュール時間帯に LED 動作を変更する機能です。

LED 動作は，通常時間帯とスケジュール時間帯で個別に設定できます。LED 自動動作の契機は，通常時間帯とスケジュール時間帯で共通の設定となります。

表 12-10 スケジュール時間帯の LED 動作設定と動作内容

	通常時間帯・スケジュール時間帯共通のコンフィグレーション	
スケジュール時間帯の LED 動作設定	LED 自動動作の契機　設定有	LED 自動動作の契機　設定無
コマンド未設定	自動動作	通常輝度
通常輝度	自動動作	通常輝度
省電力輝度	省電力輝度	省電力輝度
消灯	消灯	消灯

(b) スケジューリングによるポート省電力

スケジュール設定に従い，スケジュール時間帯にポート省電力を実施する機能です。

(c) 装置スリープ【SS1250】【SS1240】

スケジュール設定に従い，スケジュール時間帯になると装置スリープ状態にする機能です。通常時間帯になるとスリープ状態を解除して装置を起動します。長期連休や土日・祝日，夜間などの計画的な本装置の運用と停止ができます。

(2) スケジュール機能の起動モード

スケジュール機能の起動モードを運用コマンド set power-control schedule で，次の 2 種類から選択できます。

- スケジュール適用モード
  本モードは，「通常時間帯」設定および「スケジュール時間帯」設定の両方を適用します。運用中の時刻が「スケジュール時間帯」のときは「スケジュール時間帯」設定を適用し，スケジュール時間帯以外は「通常時間帯」設定を適用します。
  スケジュール時間満了による装置起動時は，スケジュール適用モードで動作します。
- スケジュール抑止モード
  本モードは，「通常時間帯」設定だけを適用します。運用中の時刻が「スケジュール時間帯」設定の実行時間であっても，「通常時間帯」設定を適用します。
  RESET スイッチ長押しによる強制スリープ解除時は，スケジュール抑止モードで動作します。

ただし，スケジュール抑止モードは，運用中の時刻が「通常時間帯」になると，自動的にスケジュール適用モードに変わります。

(3) スケジュールの時刻指定方法

省電力で運用する時間帯をスケジュール時間帯として，開始と終了の時刻で指定します。時間帯の指定方法を次に示します。

- 日時で時間帯を指定して省電力にする
- 曜日と時刻で時間帯を指定して省電力にする
- 毎日の時間帯を指定して省電力にする
- 特定日時を指定して省電力スケジュールを無効にする

スケジューリングの際には，これらの指定方法を組み合わせて設定できるため，さまざまな時間帯で省電力機能を有効にしたり，無効にしたりできます。

スケジュール時間帯は，コンフィグレーションコマンド schedule-power-control time-range で最大 50 件まで設定可能です。

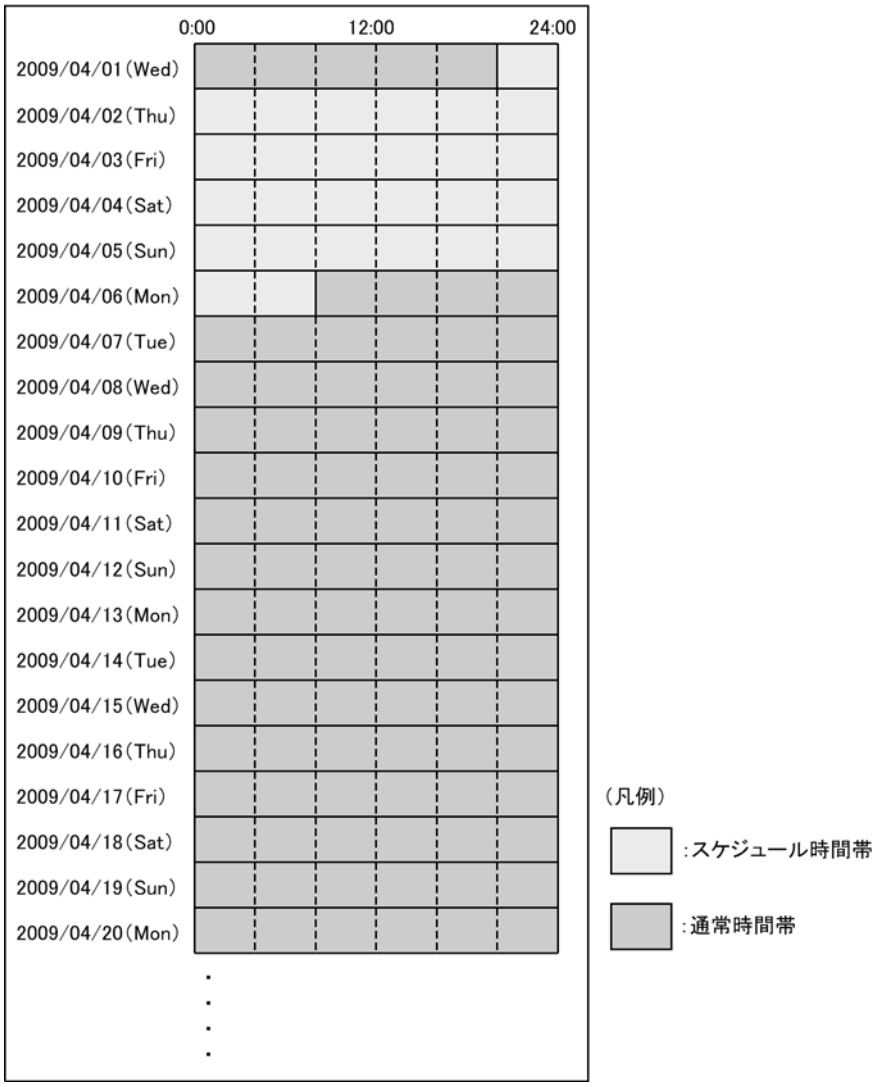
(a) 日時で時間帯を指定して省電力にする

省電力に設定したい，開始と終了の日付および時刻を指定します。

例：

2009 年 4 月 2 日から 5 日までは業務システムの稼動が低減します。稼動低減に合わせて，2009 年 4 月 1 日 20 時から 2009 年 4 月 6 日 8 時までを省電力にするスケジュールを指定します。動作スケジュールを次の図に示します。

図 12-3 省電力スケジュール（特定の日付）



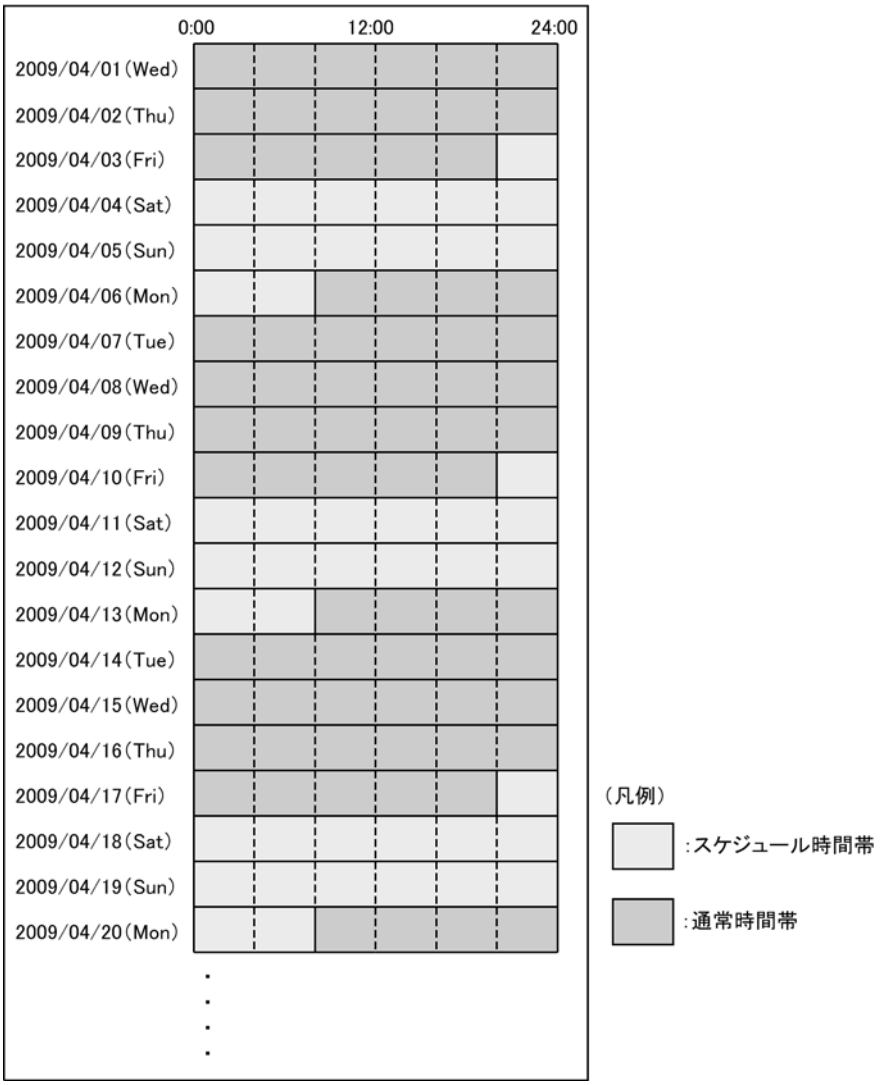
(b) 曜日と時刻で時間帯を指定して省電力にする

省電力に設定したい，開始と終了の曜日および時刻を指定します。

例：

毎週土曜日と日曜日は休日となっていて，その間は業務システムの稼動が低減します。稼動低減に合わせて，毎週金曜日 20 時から毎週月曜日 8 時までを省電力にするスケジュールを指定します。動作スケジュールを次の図に示します。

図 12-4 省電力スケジュール（特定の曜日）



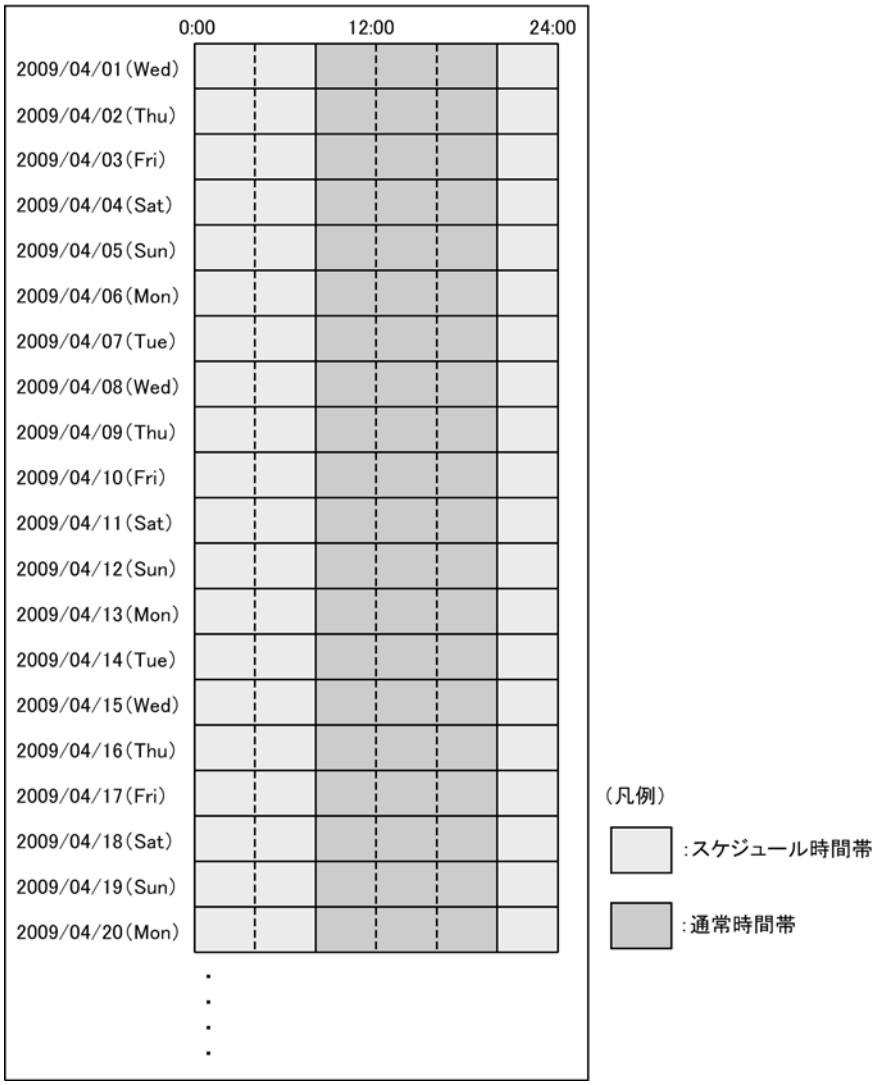
(c) 毎日の時間帯を指定して省電力にする

省電力に設定したい，開始と終了の時刻を指定します。

例：

通信業務は毎日 8 時 30 分から 17 時までとなっているため，業務システムを 8 時から 20 時まで通常の電力で運用します。毎日 20 時から翌日の 8 時までを省電力にするスケジュールを指定します。動作スケジュールを次の図に示します。

図 12-5 省電力スケジュール（毎日）



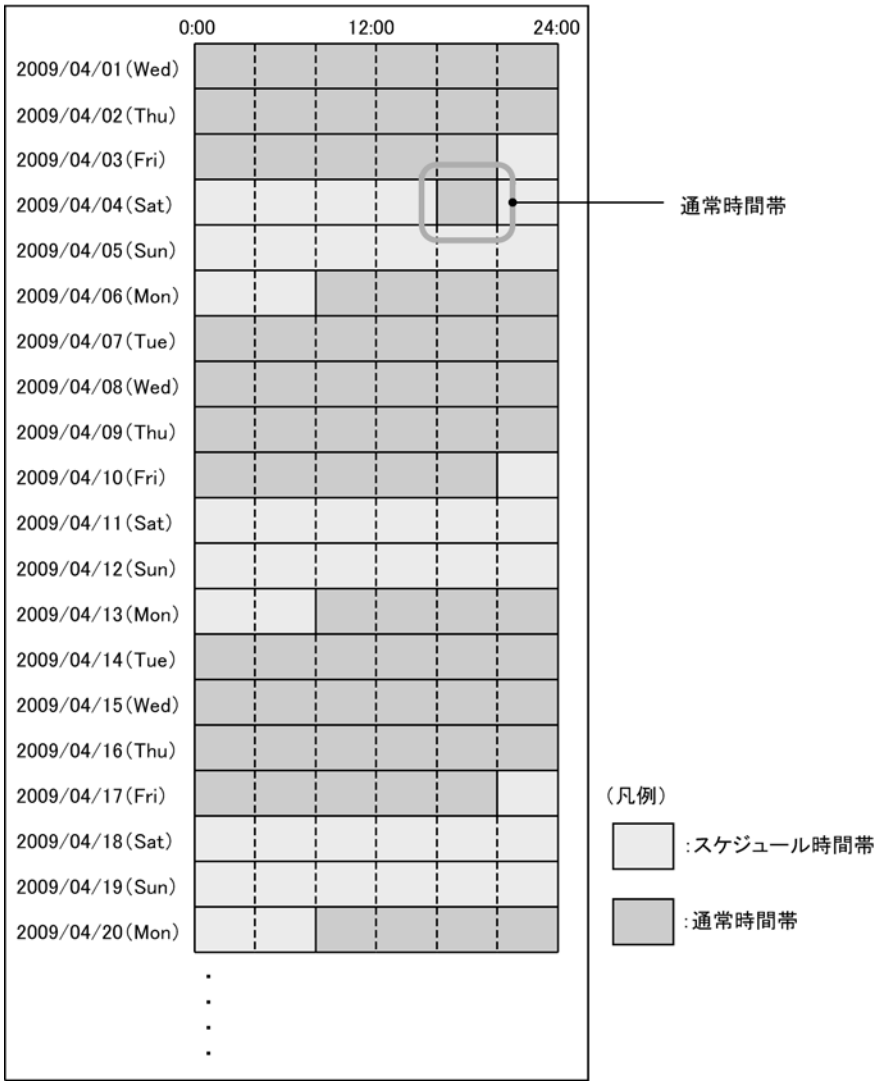
(d) 特定日時を指定して省電力スケジュールを無効にする

すでに省電力機能がスケジュールされている時間帯の，スケジュールの実行を無効にできます。実行を無効にしたい開始と終了の時刻を指定します。特定の日付，特定の曜日，および毎日の特定時間で無効にする時間帯を指定できます。

例：

毎週土曜日と日曜日は休日のため，毎週金曜日 20 時から毎週月曜日 8 時までを省電力にするスケジュールが指定してあります。ただし，業務システムのバッチ処理を行うために 2009 年 4 月 4 日 16 時から 20 時までを通常の電力で運用します。動作スケジュールを次の図に示します。

図 12-6　**省電力スケジュール（無効設定）**



12.1.7　省電力機能使用時の注意事項

(1) ポート省電力使用時【SS1250】【SS1240】

ポート省電力機能はリンクアップまでに多少の時間 (３～５秒程度) が必要となります。

(2) スケジューリングを使用した省電力機能に関する注意事項

通常時間帯とスケジュール時間帯で同じ省電力機能を使用する場合は，通常時間帯とスケジュール時間帯の両方にその設定をしてください。

例：

通常時間帯でポートの閉塞するために，コンフィグレーションコマンド shutdown を設定します。スケジュール時間帯でもポートを閉塞する場合は，コンフィグレーションコマンド schedule-power-control shutdown interface を設定してください。

(3) スケジュール時間帯の開始・終了時間の誤差に関する注意事項

スケジューリングではソフトウェアのタイマを使用しているため，CPU の負荷が高い場合などに，スケ

ジュール時間帯の開始または終了が設定した時間とずれるおそれがあります。このずれは，通常 1 分を超えることはありません。また，スケジューリングによってポートを閉塞していた場合，スケジュールが終了してから実際に通信できるまでネットワークの構成に応じた時間が必要です。省電力機能のスケジューリングでは余裕を持った時間を設定してください。

(4) 装置スリープを実行する場合【SS1250】【SS1240】

スケジュール機能で装置スリープを実行する場合は，下記にご注意ください。

1. コンフィグレーションコマンドモードで操作中にスケジュール実行時間帯になっても，スリープ状態に遷移しません。コンフィグレーションコマンドモードを終了後（装置管理者モードに遷移後），スリープ状態に遷移します。
2. ソフトウェアアップデートまたはリストア中にスケジュール実行時間帯になった場合は，スリープ状態に遷移しません。ソフトウェアアップデートまたはリストア終了後，スリープ状態に遷移します。
3. スリープ状態に遷移したとき保存されていないコンフィグレーションが消失します。このため，コンフィグレーションコマンドモードを終了すると，下記のメッセージを表示します。
   ```
   Unsaved changes would be lost when the machine goes to sleep!
   Do you exit "configure" without save ? (y/n):
   ```
   保存するときは "n" を入力して，save コマンドを実行してください。
4. 一定時間（デフォルト：30 分）キー入力操作を行わないと自動的にログアウトします。コンフィグレーションの編集中に自動ログアウトし，スリープ状態に遷移した場合，保存されていないコンフィグレーションは消失します。
5. スリープ状態が 20 日間を超過すると，20 日に一度自動でスリープ状態を解除し装置を起動します。装置起動後，再度スリープ状態となります。
6. スリープ期間終了後は，通常の起動処理時間がかかるので即時に通信運用再開にはなりません。スケジュール実行時間帯と通常運用の時間帯には余裕をもたせてください。
7. 装置スリープを設定した場合，スケジューリング時間帯になるとスリープ状態に移行するため，下記のコマンドは設定されていても適用されません。
   - schedule-power-control port-led
   - schedule-power-control port cool-standby
   - schedule-power-control shutdown interface

(5) 装置スリープ機能と DHCP snooping との共存【SS1250】【SS1240】

装置スリープ機能と DHCP snooping が共存する場合は，装置スリープ状態となる時間が DHCP サーバから配布する IP アドレスのリース時間より長くなるように設定してください。装置スリープ状態となる時間がリース時間より短いと，装置スリープ解除時にバインディングデータベースを復元できないために，DHCP クライアントから通信できなくなるおそれがあります。

通信できなくなった場合は，DHCP クライアント側で IP アドレスを解放および更新してください。例えば，Windows の場合，コマンドプロンプトから ipconfig/release を実行したあとに，ipconfig/renew を実行します。これによって，バインディングデータベースに端末情報が再登録され，DHCP クライアントから通信できるようになります。

12.2 省電力機能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

省電力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 12-11 コンフィグレーションコマンド一覧

コマンド名		説明
通常時間帯への設定コマンド	スケジュール時間帯への設定コマンド	
system port-led	schedule-power-control port-led	本装置の LED 動作を設定します。
system port-led trigger interface ※		指定した物理ポートのリンクアップ・リンクダウンを LED の自動動作の契機に追加します。
system port-led trigger console ※		コンソール（RS-232C）接続による装置へのログイン・ログアウトを LED の自動動作の契機に追加します。
system port-led trigger mc ※		MC の挿抜を LED の自動動作の契機に追加します。
power-control port cool-standby	schedule-power-control port cool-standby	リンクダウンポートの省電力機能を有効にします。
system fan-control ※ 【SS1240】		冷却 FAN 制御機能（準 FAN レス動作）を有効にします。
shutdown	schedule-power-control shutdown interface	ポート閉塞動作を設定します。
－	schedule-power-control system-sleep 【SS1250】【SS1240】	装置スリープ動作を設定します。
－	schedule-power-control time-range	省電力スケジュールの時間帯を設定します。

（凡例）

－：該当なし

注※

設定内容は，通常時間帯・スケジュール時間帯共通です。

12.2.2 LED 動作の設定

（1）LED 動作の設定

[設定のポイント]

本装置の LED 動作を省電力輝度に設定します。

[コマンドによる設定]

1. **(config)# system port-led economy**

LED 動作を省電力輝度に設定します。

[注意事項]

IP8800/S2200,IP8800/S2100 は省電力輝度未サポートです。通常輝度または消灯を設定してください。

(2) LED 自動動作の契機の設定

LED 設定に自動動作の契機を付加することで，LED 動作を自動変更できます。

[設定のポイント]

本装置の LED 自動動作の契機として，コンソールと物理ポート（リンクアップ・リンクダウン），および MC（挿抜）を設定します。

[コマンドによる設定]

1. **(config)# system port-led enable**
   LED 動作を通常輝度に設定します。
2. **(config)# system port-led trigger console**
   (config)# system port-led trigger interface 0/1,0/20
   (config)# system port-led trigger mc
   LED 自動動作の契機に，コンソールとポート 0/1 と 0/20（リンクアップ・リンクダウン），および MC（挿抜）を設定します。

12.2.3 リンクダウンポートの省電力機能の設定

[設定のポイント]

リンクダウンポートの省電力機能を設定します。

[コマンドによる設定]

1. **(config)# power-control port cool-standby**
   全ポートに対して，リンクダウン時の省電力機能を設定します。

12.2.4 冷却 FAN 制御機能（準 FAN レス動作）の設定【SS1240】

[設定のポイント]

装置内温度監視により，強制冷却が不要な環境温度のときに，冷却 FAN が停止するよう設定します。

[コマンドによる設定]

1. **(config)# system fan-control**
   強制冷却が不要な温度のときに，冷却 FAN が停止するよう設定します。

12.2.5 スケジューリングによる省電力の設定

装置スリープによる省電力，または装置スリープ以外の省電力設定で運用します。

- 装置スリープ（年末年始や長期休暇など）【SS1250】【SS1240】
- 装置スリープ以外の LED 動作やリンクダウンポートの省電力設定

(1) 年末年始の本装置スリープ設定【SS1250】【SS1240】

[設定のポイント]

年末年始に本装置をスリープに設定します。

[コマンドによる設定]

1. **(config)# schedule-power-control system-sleep**
   スケジュール時間帯に設定する省電力機能を設定します。ここでは，本装置の装置スリープを設定しま

す。

2. **(config)# schedule-power-control time-range 1 date start-time 091228 2300 end-time 100104 0600 action enable**
   2009 年 12 月 28 日 23 時から 2010 年 1 月 4 日 6 時まで動作するスケジュールを設定します。
3. **(config)# schedule-power-control time-range 2 date start-time 101228 2300 end-time 110104 0600 action enable**
   2010 年 12 月 28 日 23 時から 2011 年 1 月 4 日 6 時まで動作するスケジュールを設定します。
4. **(config)# schedule-power-control time-range 3 date start-time 111228 2300 end-time 120104 0600 action enable**
   2011 年 12 月 28 日 23 時から 2012 年 1 月 4 日 6 時まで動作するスケジュールを設定します。
5. **(config)# end**
   Unsaved changes would be lost when the machine goes to sleep!
   Do you exit "configure" without save ? (y/n):
   スケジュール実行対象に装置スリープを設定しているので，コンフィグレーションコマンドモードを終了するときに，上記のメッセージを表示します。
6. Do you exit "configure" without save ? (y/n): **n**
   (config)# save
   保存するときは "n" を入力して，save コマンドを実行してください。

[注意事項]

「12.1.7　省電力機能使用時の注意事項　(4) 装置スリープを実行する場合【SS1250】【SS1240】」を参照してください。

(2) スケジュール時間帯の LED 動作とリンクダウンポートの省電力を設定

[設定のポイント]

LED 動作の消灯，リンクダウンポートの省電力機能，未使用ポートの閉塞を設定します。
コンフィグレーション設定前の運用状態（通常時間帯）と，設定後の運用状態（スケジュール時間帯）を次の表に示します。

表 12-12　コンフィグレーション設定例

項目	通常時間帯	スケジュール時間帯
LED 動作	通常輝度	消灯
リンクダウンポートの省電力機能	全ポート通常運用	リンクダウンポートを省電力運用
ポート閉塞	全ポート no shutdown	未使用ポート 0/21 ～ 0/24 を閉塞（shutdown）

[コマンドによる設定]

1. **(config)# schedule-power-control port-led disable**
   (config)# schedule-power-control port cool-standby
   (config)# schedule-power-control shutdown interface 0/21-24
   スケジュール時間帯に設定する省電力機能を設定します。ここでは，LED 動作の消灯，リンクダウンポートの省電力機能，ポート閉塞を設定します。
2. **(config)# schedule-power-control time-range 1 weekly start-time fri 2000 end-time mon 0800 action enable**
   毎週金曜日 20 時から毎週月曜日 8 時まで動作するスケジュールを設定します。
3. **(config)# schedule-power-control time-range 2 date start-time 090404 1600**

end-time 090404 2000 action disable

2009 年 4 月 4 日 16 時から 20 時までの時間帯は，省電力スケジュールの実行を無効にする設定をします。

[注意事項]

1. スケジュール実行時間は複数設定できます。スケジュール実行時間帯になると，コンフィグレーションコマンド schedule power-control で設定された実行対象の動作をすべて実行します。実行時間ごとに実行対象を設定することはできません。
2. 異なる action パラメータで実行時間帯が重複しているときは，action disable 設定を優先します。

12.3 省電力機能のオペレーション

12.3.1 運用コマンド一覧

省電力機能の運用コマンド一覧を次の表に示します。

表 12-13 運用コマンド一覧

コマンド名	説明
show power-control port	ポート省電力制御状態を表示します。
show power-control schedule	スケジュール機能の運用状態を表示します。
set power-control schedule	スケジュール機能の起動モードを変更します。

12.3.2 LED 動作状態の表示

LED 動作の設定状態は，運用コマンド show system の「Brightness mode」で確認できます。詳細は，「10.1.3 装置の状態確認」を参照してください。

12.3.3 ポート省電力制御状態の表示

ポート省電力制御状態は，運用コマンド show power-control port で確認できます。

図 12-7 show power-control port の実行結果

```
> show power-control port

Date 20XX/03/24 22:55:17 UTC
Port  status  cool-standby
 0/1  up      -
 0/2  down    applied
 0/3  up      -
 0/4  up      -
 0/5  up      -
 0/6  up      -
 0/7  up      -
 0/8  up      -
 0/9  down    applied
 0/10 down    applied
       :
       :

>
```

12.3.4 冷却 FAN 制御状態の表示【SS1240】

冷却 FAN 制御の設定状態は，運用コマンド show system の「Fan」で確認できます。詳細は，「10.1.3 装置の状態確認」を参照してください。

12.3.5 スケジュール運用状態の表示

現在の省電力スケジュールの状態，省電力スケジュールが有効となる予定日時を，運用コマンド show power-control schedule で表示します。

図 12-8　show power-control schedule **の実行結果**

```
> show power-control schedule

Date 20XX/05/01(Fri) 18:36:57 UTC
Current Schedule Status : Disable
Schedule Power Control Date :
  20XX/05/01(Fri) 20:00 UTC  -  20XX/05/04(Mon) 06:00 UTC
  20XX/05/04(Mon) 20:00 UTC  -  20XX/05/05(Tue) 06:00 UTC
  20XX/05/05(Tue) 20:00 UTC  -  20XX/05/06(Wed) 06:00 UTC
  20XX/05/06(Wed) 20:00 UTC  -  20XX/05/07(Thu) 06:00 UTC
  20XX/05/07(Thu) 20:00 UTC  -  20XX/05/08(Fri) 06:00 UTC

>
```

13 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の概念，ソフトウェアのバックアップ・リストアについて説明します。実際のアップデート手順については，「ソフトウェアアップデートガイド」を参照してください。

13.1 **運用コマンド一覧**

13.2 **ソフトウェアのアップデート**

13.1 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 13-1 運用コマンド一覧

コマンド名	説明
ppupdate	MC から RAMDISK にコピーした新しいソフトウェア，または ftp 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。
set license	購入したライセンスを設定します。
show license	認証しているライセンスを表示します。
erase license	指定したライセンスを削除します。

13.2 ソフトウェアのアップデート

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

ソフトウェアのアップデートの概要を次の図に示します。

図 13-1 ソフトウェアのアップデートの概要 (MC)

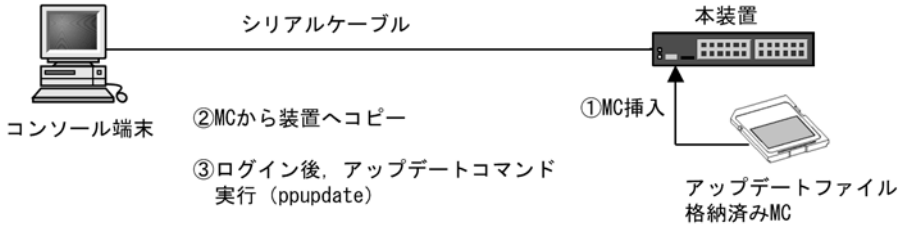
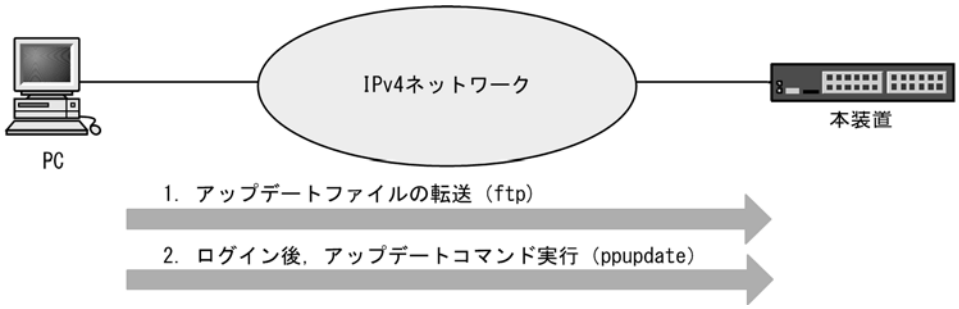


図 13-2 ソフトウェアのアップデートの概要 (ftp)



13.2.1 ソフトウェアのアップデートに関する注意事項

装置スリープ中にソフトウェアをアップデートする場合は，強制スリープ解除操作をして装置を再起動したあとアップデートしてください。【SS1250】【SS1240】

14 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。

14.1　**イーサネット共通の解説**

14.2　**イーサネット共通のコンフィグレーション**

14.3　**イーサネット共通のオペレーション**

14.4　Fastethernet **の解説**【SS1250】【SS1240】

14.5　Fastethernet **のコンフィグレーション**【SS1250】【SS1240】

14.6　Gigabitethernet（RJ45）**の解説**

14.7　Gigabitethernet（RJ45）**のコンフィグレーション**

14.8　Gigabitethernet（SFP）**の解説**

14.9　Gigabitethernet（SFP）**のコンフィグレーション**

14.10　PoE **の解説**【S2200】【S2100】【SS1240】

14.11　PoE **のコンフィグレーション**【S2200】【S2100】【SS1240】

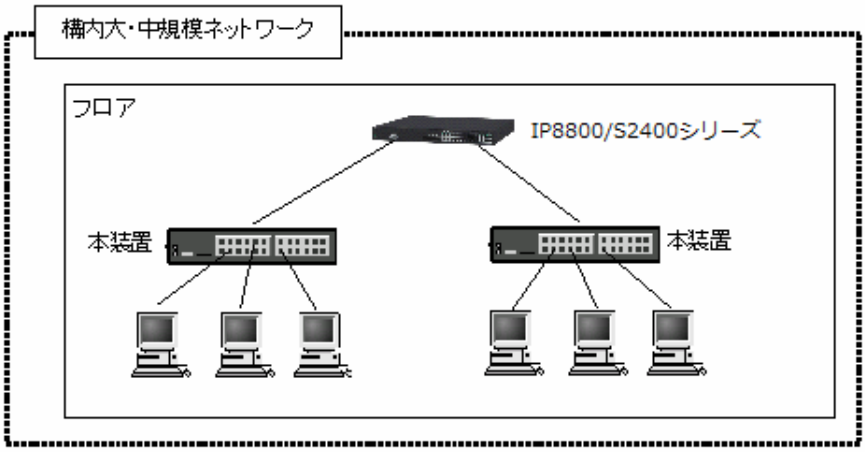
14.12　PoE **のオペレーション**【S2200】【S2100】【SS1240】

14.1 イーサネット共通の解説

14.1.1 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構成例を次の図に示します。IP8800/S2200,IP8800/S2100 はギガビットイーサネットを，IP8800/SS1250,IP8800/SS1240 はファーストイーサネットを収容していますので，フロア内の端末を接続して集線スイッチとして使用できます。

図 14-1 イーサネットの構成例



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

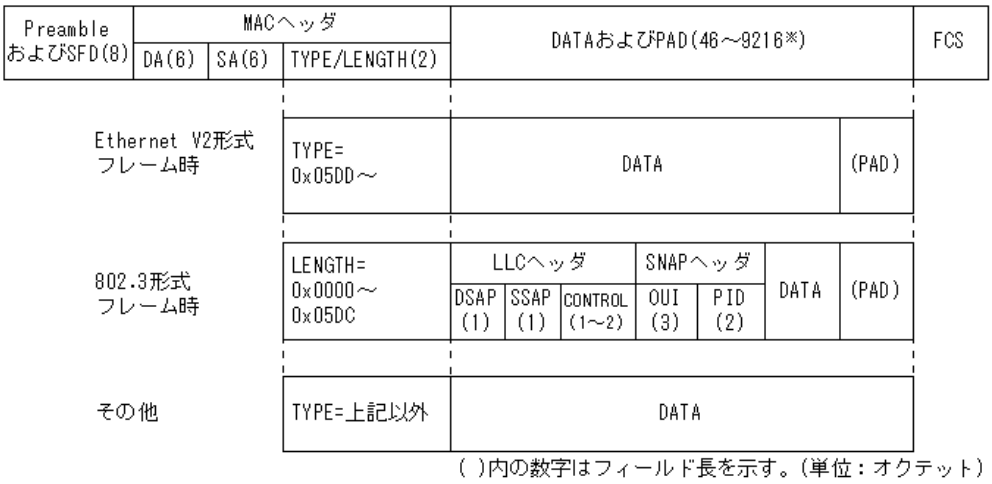
注※

IEEE802.3ah を含みます。

14.1.3 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 14-2 フレームフォーマット



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

(1) MAC 副層フレームフォーマット

(a) Preamble および SFD

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

(b) DA および SA

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

(c) TYPE ／ LENGTH

TYPE ／ LENGTH フィールドの扱いを次の表に示します。

表 14-1 TYPE ／ LENGTH フィールドの扱い

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

(d) FCS

32 ビットの CRC 演算を使用します。

(2) LLC 副層フレームフォーマット

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

(a) DSAP

LLC 情報部の宛先のサービスアクセス点を示します。

(b) SSAP

LLC 情報部を発信した特定のサービスアクセス点を示します。

(c) CONTROL

情報転送形式，監視形式，非番号制御形式の三つの形式を示します。

(d) OUI

SNAP 情報部を発信した組織コードフィールドを示します。

(e) PID

SNAP 情報部を発信したイーサネット・タイプ・フィールドを示します。

(3) 受信フレームの廃棄条件

次に示すどれかの条件によって受信したフレームを廃棄します。

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

(4) パッドの扱い

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

14.1.4 本装置の MAC アドレス

(1) 装置 MAC アドレス

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

(2) 装置 MAC アドレスを使用する機能

装置 MAC アドレスを使用する機能を次の表に示します。

表 14-2 装置 MAC アドレスを使用する機能

機能	用途
VLAN	VLAN インタフェースの MAC アドレス
リンクアグリゲーションの LACP	装置識別子
スパニングツリー	装置識別子
LLDP	装置識別子
IEEE802.3ah/UDLD	装置識別子
アップリンク・リダンダント（フラッシュ制御フレーム送信）	装置識別子

機能	用途
L2 ループ検知	装置識別子
CFM	装置識別子

14.1.5 イーサネットフレームの順序について

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

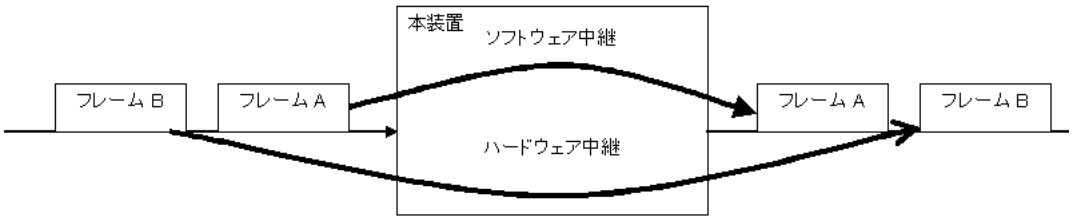
注※

CoS 値は，本装置内におけるフレームの優先度を表すインデックス値です。

(1) ソフトウェア中継による中継フレームの順番の入れ替わりについて

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

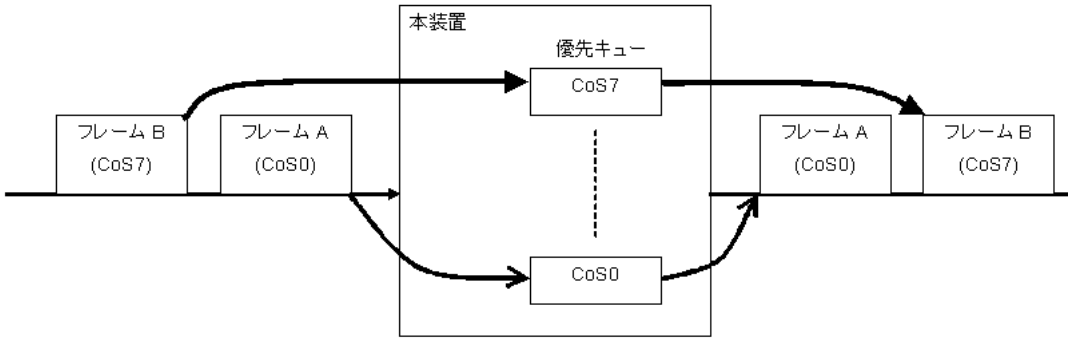
図 14-3 ソフトウェア中継によるフレームの入れ替わり



(2) 優先制御によるフレーム順番の入れ替わりについて

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

図 14-4 優先制御によるフレームの入れ替わり



14.2 イーサネット共通のコンフィグレーション

14.2.1 コンフィグレーションコマンド一覧

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 14-3 コンフィグレーションコマンド一覧

コマンド名	説明
bandwidth	ポートの帯域幅を設定します。
description	ポートの補足説明を設定します。
duplex	ポートの duplex を設定します。
flowcontrol	ポートのフローコントロールを設定します。
interface fastethernet 【SS1250】 【SS1240】	Fastethernet ポート（10BASE-T/100BASE-TX インタフェース）のコンフィグレーションを設定します。
interface gigabitethernet	Gigabitethernet ポート（10BASE-T/100BASE-TX/1000BASE-T, 100BASE-FX，1000BASE-X インタフェース）のコンフィグレーションを設定します。
link debounce	ポートの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を設定します。
linkscan-mode	本装置のリンク状態を監視する動作モードを設定します。
mdix auto	ポートの自動 MDIX 機能を設定します。
media-type 【SS1250】 【SS1240】	Gigabitethernet ポートの RJ45（10BASE-T/100BASE-TX/1000BASE-T インタフェース）と SFP（100BASE-FX/1000BASE-X インタフェース）を切り替え可能なポートで，使用するメディアタイプのポートを選択します。
mtu	ポートの MTU を設定します。
shutdown	ポートをシャットダウンします。
speed	ポートの速度を設定します。
system mtu	全ポート共通の MTU を設定します。

14.2.2 イーサネットインタフェースのポートの設定 【S2200】【S2100】

[設定のポイント]

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

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/1**
   (config-if)# exit
   Gigabitethernet のポート 0/1 への設定を指定します。

このマニュアルでは，以降の設定例は interface fastethernet を指定した形式で記載しますが，IP8800/S2200,IP8800/S2100 では interface gigabitethernet を指定する形式で設定してください。

14.2.3 イーサネットインタフェースのポートの設定【SS1250】【SS1240】

[設定のポイント]

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

[コマンドによる設定]

1. **(config)# interface fastethernet 0/1**
   (config-if)# exit
   Fastethernet のポート 0/1 への設定を指定します。

2. **(config)# interface gigabitethernet 0/25**
   (config-if)# exit
   Gigabitethernet のポート 0/25 への設定を指定します。

14.2.4 複数ポートの一括設定

[設定のポイント]

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

[コマンドによる設定]

1. **(config)# interface range fastethernet 0/1-10,0/15-20**
   ポート 0/1 から 0/10，0/15 から 0/20 への設定を指定します。

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

14.2.5 ポートのシャットダウン

[設定のポイント]

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

[コマンドによる設定]

1. **(config)# interface fastethernet 0/10**
   ポート 0/10 の設定を指定します。

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

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

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

[関連事項]

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

14.2.6 リンクダウン検出タイマの設定

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

[設定のポイント]

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

[コマンドによる設定]

1. **(config)# interface fastethernet 0/10**
   ポート 0/10 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。

14.2.7 フローコントロールの設定

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

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

[設定のポイント]

フローコントロールの設定内容は，相手装置と矛盾しないように決定してください。
Fastethernet ポートへの設定例を次に示します。

[コマンドによる設定]

1. **(config)# interface fastethernet 0/10**
   (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

[注意事項]

100BASE-FX の場合は，オートネゴシエーションが動作しないため，ネゴシエーションによるフローコントロールが動作しません。duplex を full に設定し，全二重固定設定として使用してください。

14.2.8 自動 MDIX の設定

本装置の Fastethernet および Gigabitethernet(RJ45) 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／クロスに合わせて自動的に MDI 設定が切り替わり通信が可能となります。また，本装置は MDI の固定機能を有しており MDI 固定時は MDI-X（HUB 仕様）となります。

(1) 固定 MDI の設定

[設定のポイント]

自動 MDIX を MDI-X に固定する場合に，固定したいポートに設定します。
Fastethernet ポートへの設定例を次に示します。

[コマンドによる設定]

1. **(config)# interface fastethernet 0/24**
   ポート 0/24 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。

14.2.9 ジャンボフレームの設定

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

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

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

(1) ポートの MTU の設定

[設定のポイント]

ポート 0/10 の MTU を 8192 オクテットに設定します。この設定によって，VLAN Tag の付かないフレームであれば 8206 オクテット，VLAN Tag の付いたフレームであれば 8210 オクテットまでのジャンボフレームを送受信できるようになります。
Fastethernet ポートへの設定例を次に示します。

[コマンドによる設定]

1. **(config)# interface fastethernet 0/10**
   (config-if)# shutdown
   (config-if)# mtu 8192
   ポート 0/10 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単位の MTU を設定していても，10BASE-T または 100BASE-TX 半二重で接続する場合（オートネゴシエーションの結果が 10BASE-T または 100BASE-TX 半二重になった場合も含みます）は，ポートの MTU は 1500 オクテットになります。

(2) 全ポート共通の MTU の設定

[設定のポイント]

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

[コマンドによる設定]

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

[注意事項]

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

14.3 イーサネット共通のオペレーション

14.3.1 運用コマンド一覧

イーサネット共通の運用コマンド一覧を次の表に示します。

表 14-4 運用コマンド一覧

コマンド名	説明
show interfaces	イーサネットの情報を表示します。
show port	イーサネットの情報を一覧で表示します。
clear counters	イーサネットの統計情報カウンタをクリアします。
inactivate	active 状態のイーサネットを inactive 状態にします。
activate	inactive 状態のイーサネットを active 状態にします。

14.3.2 イーサネットの動作状態を確認する

(1) 全イーサネットの動作状態を確認する

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

運用コマンド show port の実行結果を次の図に示します。

図 14-5 「本装置に実装している全イーサネットの状態」の表示例

```
> show port

Date 20XX/11/13 11:40:21 UTC
Port Counts: 26
Port  Name            Status  Speed           Duplex     FCtl FrLen  ChGr/Status
 0/1  fastether0/1    up      100BASE-TX      full(auto) off   1518  8/up
 0/2  fastether0/2    up      100BASE-TX      full(auto) off   1518  8/up
 0/3  fastether0/3    up      100BASE-TX      full(auto) off   1518  8/up
 0/4  fastether0/4    up      100BASE-TX      full(auto) off   1518  8/up
 0/5  fastether0/5    down    -               -          -        -  8/up
 0/6  fastether0/6    down    -               -          -        -  8/up
      :
      :
```

14.4 Fastethernet の解説【SS1250】【SS1240】

Fastethernet ポートでは，10BASE-T ／ 100BASE-TX のツイストペアケーブル（UTP）を使用します。本節では，10BASE-T ／ 100BASE-TX インタフェースについて説明します。

14.4.1 機能一覧

(1) 接続インタフェース：10BASE-T ／ 100BASE-TX

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

10BASE-T ／ 100BASE-TX 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
- 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 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。

表 14-5 伝送速度，全二重／半二重モードごとの接続仕様

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

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	
オートネゴシエーション	10BASE-T 半二重	10BASE-T 半二重	×	×	×	10BASE-T 半二重
	10BASE-T 全二重	×	×	×	×	10BASE-T 全二重
	10BASE-T 全二重および半二重	10BASE-T 半二重	×	×	×	10BASE-T 全二重
	100BASE-TX 半二重	×	×	100BASE-TX 半二重	×	100BASE-TX 半二重
	100BASE-TX 全二重	×	×	×	×	100BASE-TX 全二重
	100BASE-TX 全二重および半二重	×	×	100BASE-TX 半二重	×	100BASE-TX 全二重
	10/100BASE-TX 全二重および半二重	10BASE-T 半二重	×	100BASE-TX 半二重	×	100BASE-TX 全二重

(凡例) ×：接続できない

(2) オートネゴシエーション

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

本装置での接続仕様を，「表 14-5　伝送速度，全二重／半二重モードごとの接続仕様」に示します。

(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は，送信キュー溢れ（運用コマンド show qos queueing の HOL）の防止を目的とするものではありません。ポーズパケットの送信は中継先ポートの送信キューの使用状況とは連動しません。

また，48 ポートモデルの場合は，前半ポートと後半ポートの境界で受信バッファの積み替えが行われるため，24 ポートモデルとは異なる動作になります。

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 14-6　フローコントロールの送信動作」，「表 14-7 フローコントロールの受信動作」および「表 14-8　オートネゴシエーション時のフローコントロール動

作」に示します。

表 14-6　フローコントロールの送信動作

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

（凡例）

on：有効。

off：無効。desired と組み合わせた設定の場合，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 14-8　オートネゴシエーション時のフローコントロール動作」を参照してください。オートネゴシエーション以外の場合は，"on" 固定となります。

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 14-8　オートネゴシエーション時のフローコントロール動作」を参照してください。

表 14-7　フローコントロールの受信動作

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

（凡例）

on：有効。

off：無効。desired と組み合わせた設定の場合，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 14-8　オートネゴシエーション時のフローコントロール動作」を参照してください。オートネゴシエーション以外の場合は，"on" 固定となります。

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 14-8　オートネゴシエーション時のフローコントロール動作」を参照してください。

表 14-8　オートネゴシエーション時のフローコントロール動作

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

注※

"any" は，本装置（on/off/desired）と相手装置（有効 / 無効）がそれぞれどの設定でもよいことを示します。

(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 14-9　MDI ／ MDI-X のピンマッピング

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

(5) ジャンボフレーム

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

フレームについては，「14.1.3　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，「18.1.5　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）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 14-10　ジャンボフレームサポート機能

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

（凡例）
　○：サポート　×：未サポート

注※
　「14.1.3　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 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運用コマンド inactivate および activate を実行してください。
- 100BASE-TX を使用する場合，接続ケーブルはカテゴリ 5 以上のツイストペアケーブル（UTP）を使用してください。
- 全二重インタフェースはコリジョン検出とループバック機能を行わないことによって実現しています。このため，10BASE-T または 100BASE-TX を全二重インタフェース設定で使用する場合，相手接続インタフェースは必ず全二重インタフェースに設定して接続してください。

14.5 Fastethernet のコンフィグレーション【SS1250】【SS1240】

14.5.1 ポートの設定

(1) 速度と duplex の設定

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

(a) オートネゴシエーションに対応していない相手装置と接続する場合

[設定のポイント]

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

[コマンドによる設定]

1. **(config)# interface fastethernet 0/10**
   (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 fastethernet 0/10**
   (config-if)# shutdown
   (config-if)# speed auto 100
   相手装置とオートネゴシエーションで接続しても，100BASE-TX 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。

14.5.2 フローコントロールの設定

フローコントロールの設定については，「14.2.7　フローコントロールの設定」を参照してください。

14.5.3 自動 MDIX の設定

自動 MDIX の設定については，「14.2.8　自動 MDIX の設定」を参照してください。

14.5.4 ジャンボフレームの設定

ジャンボフレームの設定については，「14.2.9　ジャンボフレームの設定」を参照してください。

14.6 Gigabitethernet（RJ45）の解説

Gigabitethernet（RJ45）ポートでは，10BASE-T ／ 100BASE-TX ／ 1000BASE-T のツイストペアケーブル（UTP）を使用します。本節では，10BASE-T ／ 100BASE-TX ／ 1000BASE-T インタフェースについて説明します。

14.6.1 機能一覧

（1）接続インタフェース：10BASE-T ／ 100BASE-TX ／ 1000BASE-T

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

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

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

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

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

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

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

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

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

表 14-11 伝送速度，全二重／半二重モードごとの接続仕様

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

(凡例) ×：接続できない

(2) オートネゴシエーション

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

対向装置間でやりとりを行い，接続動作を決定する機能です。

本装置での接続仕様を，「表 14-11　伝送速度，全二重／半二重モードごとの接続仕様」に示します。また，本装置では，ネゴシエーションで解決できなかった場合，リンク接続されるまで接続動作を繰り返します。（本動作については，「14.6.1　機能一覧（6）ダウンシフト機能」を参照してください。）

(3) フローコントロール

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は，送信キュー溢れ（運用コマンド show qos queueing の HOL）の防止を目的とするものではありません。ポーズパケットの送信は中継先ポートの送信キューの使用状況とは連動しません。

また，48 ポートモデルの場合は，前半ポートと後半ポートの境界で受信バッファの積み替えが行われるため，24 ポートモデルとは異なる動作になります。

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 14-12　フローコントロールの送信動作」，「表 14-13　フローコントロールの受信動作」および「表 14-14　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 14-12　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 14-14　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 14-14　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 14-13　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 14-14　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 14-14　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 14-14　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	off	off	行わない	行わない
			desired	on	on	行う	行う
		無効	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
		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
off		有効	有効	on	on	行う	行う
			無効	off	on	行う	行わない
			desired	on	on	行う	行う
		無効	有効	on	on	行う	行う
			無効	off	off	行わない	行わない
			desired	on	on	行う	行う
		desired	有効	on	on	行う	行う
			無効	off	on	行う	行わない
			desired	on	on	行う	行う
desired	on	有効	有効	on	on	行う	行う
			無効	off	off	行わない	行わない
			desired	on	on	行う	行う
		無効	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
		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
	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

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
		無効	有効	on	off	行わない	行う
			無効	off	off	行わない	行わない
			desired	on	off	行わない	行う
		desired	有効	off	off	行わない	行わない
			無効	off	off	行わない	行わない
			desired	off	off	行わない	行わない
	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	行う	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 14-15　MDI ／ MDI-X のピンマッピング

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

注 1

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

注 2

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

す。（BI_Dx：双方向データ信号）

(5) ジャンボフレーム

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

フレームについては，「14.1.3　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，「18.1.5　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 14-16　ジャンボフレームサポート機能

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

（凡例）
○：サポート　×：未サポート

注※
「14.1.3　MAC および LLC 副層制御」のフレームフォーマットを参照してください。

(6) ダウンシフト機能

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

(a) 適用回線

本機能は 1000BASE-T でサポートします。

(b) 回線速度変更順序

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

表 14-17　回線速度変更順序

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

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

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

- 伝送速度，全二重／半二重モードが相手装置と不一致の場合，接続できないので注意してください。不一致の状態で通信を行うと，以降の通信が停止することがあります。この場合，当該ポートに対して運用コマンド inactivate および activate を実行してください。
- 100BASE-TX を使用する場合は接続ケーブルはカテゴリ 5 以上，1000BASE-T を使用する場合はエンハンストカテゴリ 5 以上のツイストペアケーブル（UTP）を使用してください。
- 全二重インタフェースはコリジョン検出とループバック機能を行わないことによって実現しています。このため，10BASE-T または 100BASE-TX を全二重インタフェース設定で使用する場合，相手接続インタフェースは必ず全二重インタフェースに設定して接続してください。
- 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。

14.6.2　SFP 自動認識機能 (メディアタイプの選択)【SS1250】【SS1240】

本装置の Gigabitethernet ポートは，RJ45（10BASE-T/100BASE-TX/1000BASE-T）ポートと SFP（100BASE-FX/1000BASE-X）ポートの排他使用となります。本装置の出荷時のデフォルトコンフィグレーションでは，メディアの自動検出となっており，SFP を検出した場合は SFP を使います。（1000BASE-X でリンクアップ時に SFP に切り替えます。）

メディア固定（SFP または RJ45 固定）で使う場合は，コンフィグレーションコマンド media-type で設定可能です。

14.7 Gigabitethernet（RJ45）のコンフィグレーション

14.7.1 ポートの設定

（1）速度と duplex の設定

本装置と相手装置の伝送速度と duplex を設定できます。デフォルトでは相手装置とオートネゴシエーションで，伝送速度と duplex を決定します。相手装置に合わせて回線速度と duplex を変更する場合，メディアタイプに rj45 を指定してから，変更してください。メディアタイプの設定については「14.7.5　メディアタイプの設定【SS1250】【SS1240】」を参照してください。

(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 0/25
(config-if)# shutdown
(config-if)# media-type rj45
(config-if)# speed 100
(config-if)# duplex half
```
相手装置と 100BASE-TX 半二重で接続する設定をします。

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

(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 0/25
(config-if)# shutdown
(config-if)# media-type rj45
(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。

14.7.2 フローコントロールの設定

フローコントロールの設定については，「14.2.7　フローコントロールの設定」を参照してください。

14.7.3 自動 MDIX の設定

自動 MDIX の設定については，「14.2.8　自動 MDIX の設定」を参照してください。

14.7.4 ジャンボフレームの設定

ジャンボフレームの設定については，「14.2.9　ジャンボフレームの設定」を参照してください。

14.7.5 メディアタイプの設定【SS1250】【SS1240】

1 ギガビットイーサネットでどのメディアを使うかは，そのポートに対して media-type コマンドで設定します。

(1) 自動メディア検出の設定

[設定のポイント]

1 ギガビットインタフェースの自動メディア検出機能を有効にします。

[コマンドによる設定]

1. **(config)# interface range gigabitethernet 0/25-26**
   (config-if-range)# shutdown
   (config-if-range)# media-type auto
   自動メディア検出機能を有効にします。

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

(2) RJ45 固定の設定

[設定のポイント]

10BASE-T/100BASE-TX/1000BASE-T インタフェースを使う場合に設定が必要です。

[コマンドによる設定]

1. **(config)# interface range gigabitethernet 0/25-26**
   (config-if-range)# shutdown
   (config-if-range)# media-type rj45
   自動メディア検出機能を無効にし，10BASE-T/100BASE-TX/1000BASE-T インタフェースを使うように設定します。
2. **(config-if-range)# no shutdown**

```
(config-if-range)# exit
```

(3) SFP 固定の設定

[設定のポイント]

SFP 固定で使う場合に設定が必要です。

[コマンドによる設定]

1.
```
(config)# interface range gigabitethernet 0/25-26
(config-if-range)# shutdown
(config-if-range)# media-type sfp
```
   - 自動メディア検出機能を無効にし，SFP 固定に設定します。

2.
```
(config-if-range)# no shutdown
(config-if-range)# exit
```

(4) メディアタイプ設定時の注意事項【SS1250】【SS1240】

1. media-type の設定を変更した場合，下記コンフィグレーションコマンドの設定はデフォルト値に戻ります。
   - duplex
   - mdix auto
   - speed
2. media-type auto を設定した場合，下記コンフィグレーションコマンドは設定できません。デフォルト値でご使用ください。
   - duplex
   - mdix auto
   - speed

14.8 Gigabitethernet（SFP）の解説

Gigabitethernet（SFP）ポートでは，100BASE-FX/1000BASE-X の光ファイバを使用します。本節では，100BASE-FX/1000BASE-X の光ファイバインタフェースについて説明します。

14.8.1 機能一覧

100BASE-FX /1000BASE-X 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：100BASE-FX【SS1250】

100BASE-FX をサポートしています。回線速度は 100Mbit/s，全二重固定です。オートネゴシエーションはサポートしていません。

100BASE-FX :

マルチモード光ファイバを使用して 2km の伝送距離を実現します。
（マルチモード，最大 2km）

コンフィグレーションでは次のモードを指定してしてください。

- 伝送速度　100 Mbit/s 固定，全二重固定
- メディアタイプ　sfp 固定

(a) 100BASE-FX 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，全二重／半二重モードの接続仕様を次の表に示します。なお，100BASE-FX の物理仕様については，マニュアル「ハードウェア取扱説明書」を参照してください。

表 14-18　伝送速度，全二重／半二重モードごとの接続仕様

接続装置側設定		本装置の設定
設定	インタフェース	固定
		100BASE-FX 全二重
固定	100BASE-FX 半二重	×
	100BASE-FX 全二重	100BASE-FX 全二重
オートネゴシエーション	100BASE-FX 半二重	×
	100BASE-FX 全二重	×

（凡例）　×：接続できない

(2) 接続インタフェース：1000BASE-X

1000BASE-SX，1000BASE-SX2，1000BASE-LX，1000BASE-LH，および 1000BASE-BX をサポートしています。回線速度は 1000Mbit/s 全二重固定です。

1000BASE-SX：
短距離間を接続するために使用します。
（マルチモード，最大 550m）

1000BASE-SX2：
マルチモード光ファイバを使用して 2km の伝送距離を実現します。
（マルチモード，最大 2km）

1000BASE-LX：
中距離間を接続するために使用します。
（シングルモード，最大 5km ／マルチモード，最大 550m）

1000BASE-LH：
長距離間を接続するために使用します。
（シングルモード，最大 70km）

1000BASE-BX：
送受信で波長の異なる光を使用することで，１芯の光ファイバを使い，光ファイバのコストを抑えることができます。
送受信で異なる波長の光を使用するため，アップ側とダウン側で１対となるトランシーバを使用します。
本装置では，IEEE802.3ah で規定されている 1000BASE-BX10-D/1000BASE-BX10-U と，独自規格の 1000BASE-BX40-D/1000BASE-BX40-U をサポートします。

1000BASE-BX10-D/1000BASE-BX10-U：
中距離間を接続するために使用します。
（シングルモード，最大 10km）

1000BASE-BX40-D/1000BASE-BX40-U：
長距離間を接続するために使用します。
（シングルモード，最大 40km）

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になります。

- オートネゴシエーション
- 1000BASE-X 全二重固定

(a) 1000BASE-X 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，全二重／半二重モードの接続仕様を次の表に示します。なお，1000BASE-X の物理仕様については，マニュアル「ハードウェア取扱説明書」を参照してください。

表 14-19　伝送速度，全二重／半二重モードごとの接続仕様

接続装置側設定		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
		1000BASE **全二重**	1000BASE **全二重**
固定	1000BASE 半二重	×	×
	1000BASE 全二重	1000BASE 全二重	×
オートネゴ シエーション	1000BASE 半二重	×	×
	1000BASE 全二重	×	1000BASE 全二重

（凡例）　×：接続できない

(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。

本装置での接続仕様を，「表 14-19　伝送速度，全二重／半二重モードごとの接続仕様」に示します。また，本装置では，ネゴシエーションで解決できなかった場合，リンク接続されるまで接続動作を繰り返します。

なお，100BASE-FX はオートネゴシエーション未サポートです。

(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，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は，送信キュー溢れ（運用コマンド show qos queueing の HOL）の防止を目的とするものではありません。ポーズパケットの送信は中継先ポートの送信キューの使用状況とは連動しません。

また，48 ポートモデルの場合は，前半ポートと後半ポートの境界で受信バッファの積み替えが行われるため，24 ポートモデルとは異なる動作になります。

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 14-20　フローコントロールの送信動作」，「表 14-21　フローコントロールの受信動作」および「表 14-22　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。

なお，100BASE-FX はオートネゴシエーション未サポートのため , オートネゴシエーション時のフローコントロール動作はありません。

表 14-20　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 14-22　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 14-22　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 14-21　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 14-22　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 14-22　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 14-22　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	off	off	行わない	行わない
			desired	on	on	行う	行う
		無効	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
		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
off		有効	有効	on	on	行う	行う
			無効	off	on	行う	行わない
			desired	on	on	行う	行う

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
		無効	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
		desired	有効	on	on	行う	行う
			無効	off	on	行う	行わない
			desired	on	on	行う	行う
desired	on	有効	有効	on	on	行う	行う
			無効	off	off	行わない	行わない
			desired	on	on	行う	行う
		無効	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
		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
	off	有効	有効	off	off	行わない	行わない
			無効	off	off	行わない	行わない
			desired	off	off	行わない	行わない
		無効	有効	on	off	行わない	行う
			無効	off	off	行わない	行わない
			desired	on	off	行わない	行う
		desired	有効	off	off	行わない	行わない
			無効	off	off	行わない	行わない
			desired	off	off	行わない	行わない
	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	行う	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。

フレームについては，「14.1.3　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，「18.1.5　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 14-23　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 ※	IEEE802.3 ※	
フレーム長（オクテット）	Tag 無 :1519 ～ 9234 Tag 付 :1523 ～ 9238	×	MAC ヘッダの DA ～データの長さ。 FCS は含みます。
受信機能	○	×	IEEE802.3 フレームは，LENGTH フィールド値が 0x05DD（1501 オクテット）以上の場合に廃棄します。
送信機能	○	×	IEEE802.3 フレームは送信しません。

（凡例）
　○：サポート　×：未サポート

注※
　「14.1.3　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) SFP 自動認識機能 (メディアタイプの選択)【SS1250】【SS1240】

「14.6.2　SFP 自動認識機能 (メディアタイプの選択)【SS1250】【SS1240】」参照してください。

自動メディア検出機能に制限がある SFP もありますので，後述の「14.8.2　SFP 使用時の注意事項」も合わせて参照してください。

14.8.2　SFP 使用時の注意事項

(1) 100BASE-FX の SFP 挿入時の注意事項【SS1250】

自動メディア検出機能が有効でも，100BASE-FX については自動認識しません。100BASE-FX の場合は，下記設定でご使用ください。

- 伝送速度：100Mbit/s 固定，全二重固定
- メディアタイプ：SFP 固定

(2) 100BASE-FX 使用後の注意事項【SS1250】

100BASE-FX を使用した後，10BASE-T/100BASE-TX/1000BASE-T，または 1000BASE-X を使用する場合，下記の順で設定変更を行ってからご使用ください。

1. 速度設定削除（no speed）
2. 全二重設定削除（no duplex）
3. メディアタイプ設定削除（no media-type）

(3) 1000BASE-X 接続時の注意事項

- 全二重のオートネゴシエーションおよび固定接続だけサポートします。
- 相手装置（スイッチングハブなど）をオートネゴシエーションまたは全二重固定に設定してください。
- マニュアル「ハードウェア取扱説明書」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。

（4） 1000BASE-SX2 での自動メディア検出動作および制限事項【SS1250】【SS1240】

自動メディア検出では 1000BASE-X を優先しており，1000BASE-X がリンクアップした場合には 10BASE-T/100BASE-TX/1000BASE-T(RJ45) 使用している場合でも，1000BASE-X に自動的に切り替わります。

しかし 1000BASE-SX2 の SFP の場合，RJ45 を使用している場合は 1000BASE-X がリンクアップしないため自動的に切り替わりません。

従って 1000BASE-SX2 の場合は，下記のいずれかでご使用ください。

1. 固定メディア設定で使用
2. 光ファイバケーブルと UTP（RJ45）ケーブルを同時に挿さない運用

（5） 1000BASE-BX ※の SFP 挿入時の注意事項【SS1250】【SS1240】

自動メディア検出機能が有効および，10BASE-T/100BASE-TX/1000BASE-T(RJ45) がリンクアップしている状態で，1000BASE-BX の SFP を挿入すると，10BASE-T/100BASE-TX/1000BASE-T で一時的にリンクダウンが発生しますのでご注意ください。

注※
1000BASE-BX10-D，1000BASE-BX10-U，1000BASE-BX40-D，1000BASE-BX40-U

RJ45 側の運用を優先する場合，1000BASE-BX の SFP の挿入は下記のいずれかで実施してください。

1. 固定メディア（RJ45）設定で SFP を挿入
2. 装置電源 ON 前に SFP を挿入

14.9 Gigabitethernet（SFP）のコンフィグレーション

14.9.1 100BASE-FX のポート設定【SS1250】

100BASE-FX を使用するポートでは，伝送速度，全二重とメディアタイプを設定します。

[設定のポイント]

伝送速度 100Mbit/s，全二重，メディアタイプを sfp に設定します

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/26**
   (config-if)# shutdown
   (config-if)# media-type sfp
   (config-if)# speed 100
   (config-if)# duplex full
   メディアタイプ sfp と相手装置と 100Mbit/s 全二重固定で接続する設定をします。

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

[注意事項]

100BASE-FX を使用するときは，必ず上記の設定でご使用ください。（duplex が未設定，または auto の場合，flowcontol は動作しません。）

14.9.2 1000BASE-X のポート設定

(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。相手装置に合わせて回線速度と duplex を変更する場合，メディアタイプに sfp を指定してから，変更してください。メディアタイプの設定については「14.7.5　メディアタイプの設定【SS1250】【SS1240】」を参照してください。【SS1250】【SS1240】

[設定のポイント]

通常は相手装置とオートネゴシエーションで接続します。本装置のデフォルトはオートネゴシエーションなので，速度と duplex を設定する必要はありません。オートネゴシエーションを使用しない場合は，速度を 1000Mbit/s に，duplex を全二重に設定します。

[コマンドによる設定]

1. **(config)# interface gigabitethernet 0/25**
   (config-if)# shutdown
   (config-if)# media-type sfp
   (config-if)# speed 1000
   (config-if)# duplex full
   メディアタイプ sfp で，相手装置と 1000Mbit/s 全二重で接続する設定をします。

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

[注意事項]

回線速度を 1000Mbit/s に設定する場合は，必ず duplex も full（全二重）に設定してください。
speed と duplex の両方が正しく設定されている場合以外は，オートネゴシエーションでの接続になります。

14.9.3 フローコントロールの設定

フローコントロールの設定については，「14.2.7　フローコントロールの設定」を参照してください。

14.9.4 ジャンボフレームの設定

ジャンボフレームの設定については，「14.2.9　ジャンボフレームの設定」を参照してください。

14.9.5 メディアタイプの設定【SS1250】【SS1240】

「14.7.5　メディアタイプの設定【SS1250】【SS1240】」を参照してください。

14.10 PoE の解説【S2200】【S2100】【SS1240】

14.10.1 PoE の概要

PoE(Power over Ethernet) とは，データ通信用の UTP ケーブルを使ってネットワーク機器に電力を供給する機能です。最大 30.0W の電力を供給できます。また，IP8800/S2200 シリーズは，最大 60.0W の電力を供給できます。

PoE は，電源を取りにくい場所に設置するネットワーク機器で使用します。電力の供給側を給電装置，需要側を受電装置と呼びます。

本装置は IEEE802.3af/IEEE802.3at 規格に準拠し，受電装置の検出（検出プロセス），受電装置が要求する電力クラスの分類（電力クラス分類プロセス），電力供給（電力供給プロセス）の三つのプロセスを自動的に実施する給電装置です。

(1) 検出プロセス

検出プロセスでは，接続装置が受電装置かどうかの検出を実施します。接続装置が IEEE802.3af 規格または IEEE802.3at 規格に準拠した受電装置である場合は，次の電力クラス分類プロセスへ移行します。ただし，PoE に対応していないネットワーク機器の場合は電力を供給しません。

(2) 電力クラス分類プロセス

電力クラス分類プロセスでは，IEEE802.3af/IEEE802.3at 規定の特別な電圧を用いて受電装置の電力クラスを判断します。受電装置は，本装置から特別な電圧で給電を受けることにより，電力クラス分類プロセスにあることを認識します。この時，受電装置は IEEE802.3af/IEEE802.3at 規定の電流を消費する動作をすることから，本装置は五つに分類されている電力クラスのどれに属しているかを知ることができます。なお，電力クラスの分類は IEEE802.3af 規格ではオプションとなっており，受電装置がこれら電力クラス分類に対応しているとは限りません。対応していない装置は Class 0 に分類します。

(3) 電力供給プロセス

電力供給プロセスでは，受電装置の需要にあわせて，「表 14-24　本装置の電力クラスと最大出力電力」に示す「最大出力電力」まで給電します。

表 14-24　本装置の電力クラスと最大出力電力

電力クラス	最大出力電力
Class 0	15.4W
Class 1	4.0W
Class 2	7.0W
Class 3	15.4W
Class 4	30.0W

14.10.2 PoE の供給電力割り当て【S2200】

IP8800/S2200 は，IEEE802.3af，IEEE802.3at に加え，60.0W 給電機能を搭載しています。IP8800/S2200 は，次の図に示すように，ポート 0/1 ～ 0/4 の系統 1 で 60.0W 給電機能をサポートします。また，ポート 0/5 ～ 0/24 の系統 2 では，最大 30.0W の給電機能をサポートします。

図 14-6　IP8800/S2200 の供給電力機能概要図

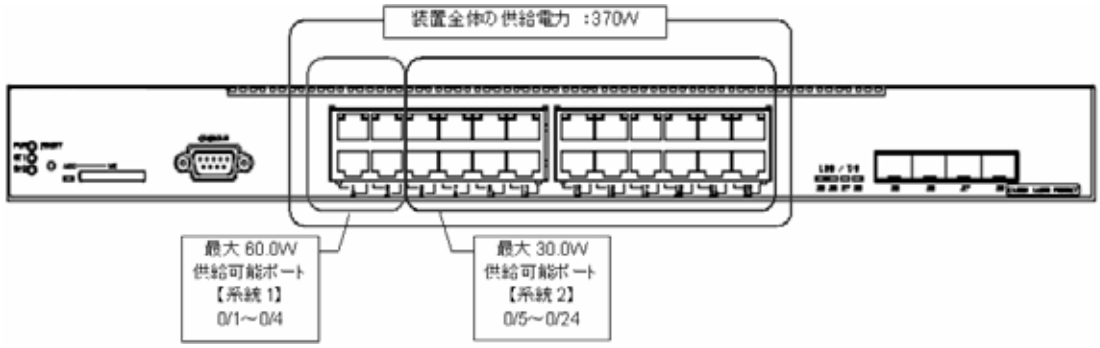


表 14-25　IP8800/S2200 の PoE 機能概要

機能		仕様		備考
モデル		IP8800/S2230-24P		
最大給電能力	装置全体 [W]		370.0	
	ポート単位 [W]	系統 1 ：0/1 ～ 0/4	60.0	コンフィグレーションによる手動設定
		系統 2 ：0/5 ～ 0/24	30.0	
	Class 別 [W]	Class 0	15.4	
		Class 1	4.0	
		Class 2	7.0	
		Class 3	15.4	
		Class 4	30.0	
Pre.STD		未サポート		
優先制御		系統 1 の範囲で動作		
		系統 2 の範囲で動作		

(1) 装置全体の電力管理

IP8800/S2200 は，装置全体給電能力に対して，ポート 0/1 ～ 0/4 を系統 1，ポート 0/5 ～ 0/24 を系統 2 とし，合計 2 系統の最大電力管理を行います。

各系統別の最大電力管理を「表 14-26　系統別電力管理」に示します。

系統 1 には，下記のコンフィグレーションコマンドで供給可能な最大電力量を設定できます。本コンフィグレーションコマンドの反映には，装置の再起動が必要です。

power inline system-allocation limit <Threshold>

表 14-26 系統別電力管理

系統	対象ポート	最大電力管理内容	備考
1	0/1 ～ 0/4	• 系統１に対して，コンフィグレーションで設定した最大供給電力を割り当て • 設定変更後は装置再起動が必要 • 優先制御は，系統１のポート範囲内で実施	系統１デフォルト 61.6[W] (=15.4[W] × 4 ポート)
2	0/5 ～ 0/24	• 装置全体の最大供給電力から，系統１で割り当てた最大供給電力を差し引いた値を割り当て • 系統２の最大供給電力は，系統１のコンフィグレーションに依存し，系統２の値をコンフィグレーションで設定不可 • 優先制御は，系統２のポート範囲内で実施	系統２デフォルト 308.4[W] (=370.0[W] － 61.6[W])

(2) PoE 供給電力の割り当て

系統１，および系統２ともに，電力割り当て設定は下記の２種類をサポートし，ポート単位で任意の電力割り当てを選択可能です。

- Class ベース設定
- 手動設定

(a) Class ベース設定

コンフィグレーションコマンド power inline allocation auto で，該当ポートの電力量割り当てを「Class ベース」設定とすることで，供給電力割り当てを Class ベースで計算します。Class ベースの供給電力割り当ての対応は，「表 14-24　本装置の電力クラスと最大出力電力」によります。

(b) 手動設定

コンフィグレーションコマンド power inline allocation limit で，該当ポートの電力量割り当てを「手動」設定することで，手動で供給電力量を割り当てます。

通常は Class ベースで運用しますが，実消費電力が Class ベースの割り当てよりも大幅に小さかった場合，手動設定することで無駄を省くことができます。

例えば，Class ベースでは Class ４（30.0W）に分類される受電装置を接続するときに，実際の消費電力が 18.0W の場合に手動で 20.0W を設定することで，他のポートの給電割り当てを増やすことができます。

また，系統 1 で 30.0W を超える受電装置を接続するときは，手動設定で割り当てが必要になります。

14.10.3 PoE の供給電力割り当て【S2100】【SS1240】

(1) 収容条件

本装置の PoE 供給電力，同時接続（電力供給）可能な受電装置の接続数を次の表に示します。

表 14-27 同時接続（電力供給）可能な受電装置の接続数

項目名	仕様
モデル	IP8800/S2130-24P IP8800/SS1240-24P2C
本装置の PoE 供給電力	370.0W

項目名		仕様
PoE 供給可能ポート※1	Class 0（15.4W）の場合	24 ポート※2
	Class 1（4.0W）の場合	24 ポート
	Class 2（7.0W）の場合	24 ポート
	Class 3（15.4W）の場合	24 ポート
	Class 4（30.0W）の場合	12 ポート※3

注※1
受電装置追加等により計算上供給電力をオーバーした場合は，優先度の低いポートから供給を遮断します。（ポート優先度が同じときは，ポート番号の大きいポートから電力供給を遮断します。）

注※2
ネゴシエーションできない受電装置は Class 0 として扱います。

注※3
30.0W を消費する受電装置の最大接続可能数は 12 ポートとなります。（30.0W × 12 ＝ 360.0W）

（2） PoE 供給電力の割り当て

受電装置への供給電力は，ポート単位で「Class ベース」または「手動設定」で算出できます。

(a) Class ベース設定

コンフィグレーションコマンド power inline allocation auto で，該当ポートの電力量割り当てを「Class ベース」設定とすることで，供給電力割当てを Class ベースで計算します。Class ベースの供給電力割当ての対応は「表 14-24　本装置の電力クラスと最大出力電力」によります。

(b) 手動設定

コンフィグレーションコマンド power inline allocation limit で，該当ポートの電力量割り当てを「手動」設定とすることで，手動で供給電力量を割り当てます。

通常は Class ベースで運用しますが，実消費電力が Class ベースの割り当てよりも大幅に小さかった場合，手動設定することで無駄を省くことができます。

例えば，Class ベースでは Class 4（30.0W）に分類される受電装置を接続するときに，実際の消費電力が 18.0W の場合に手動で 20.0W を設定することで，他のポートの給電割り当てを増やすことができます。

また，Class 0 で 30.0W を要する受電装置を接続するときは，手動設定で割り当てが必要になります。

(c) ポートに割り当てる電力の総和

PoE 供給電力（ポートに割り当てる電力の総和）は 370.0W 以下に設定してください。また，PoE 対応ポートに接続する受電装置は次の関係式を満たすように組み合わせてください。

ポートに割り当てる電力の総和（W）≧

Class 0 のポート数×出力電力（15.4W）＋

Class 1 のポート数×出力電力（4.0W）＋

Class 2 のポート数×出力電力（7.0W）＋

Class 3 のポート数×出力電力（15.4W）＋

Class 4 のポート数×出力電力（30.0W）＋

手動電力割り当て設定ポートの合計電力

14.10.4 最大電力供給超過時の動作設定

IP8800/S2200 は系統１，系統２ごとの最大供給電力を超過した場合，IP8800/S2100,IP8800/SS1240 は装置全体の最大供給電力を超過した場合に，どのポートへの供給を有効・無効とするかの優先度をコンフィグレーションで設定できます。

電力超過時の動作には下記の２種類があります。

- コンフィグレーションによるポート優先度設定
- 既給電ポートの優先

(1) コンフィグレーションによるポート優先度設定

各ポートそれぞれに対して電力供給の優先度を設定できます。本機能によって供給する電力が不足する場合，電力供給を保証するポートと停止させるポートを指定できます。コンフィグレーションの設定がない場合，デフォルトの優先度は「高」です。また，同一設定が複数あった場合はポート番号の小さいポートを優先します。

IP8800/S2200 は，ポートごとに設定した優先度に従い，系統１および系統２のそれぞれの範囲内で優先度の高いポートへの供給を優先します。

IP8800/S2100,IP8800/SS1240 は装置全体で，ポートごとに設定した優先度に従い，優先度の高いポートへの供給を優先します。

重要 (critical)

最重要ポートとして電力供給を保証する設定です。常時電力を供給する必要があるポートに設定してください。

高 (high)

電力供給の優先度を「高」で供給します。使用頻度が高いポートに設定してください。優先度の指定がない場合は，本設定になります。
「高」に設定したポートは，供給電力の不足時に「低」に設定されているポートよりもあとに電力供給が停止されます。また，「高」の設定が複数ポートに指定されている場合は，設定内でポート番号が大きいポートから電力供給が停止されます。

低 (low)

電力供給の優先度を「低」で供給します。使用頻度が低いポートに設定してください。「低」に設定したポートは，供給電力の不足時に「高」に設定されているポートよりも先に電力供給が停止されます。また，「低」の設定が複数ポートに指定されている場合は，設定内でポート番号が大きいポートから電力供給が停止されます。

停止 (never)

電力供給を停止して PoE 機能を無効にします。PoE 機能を使用しないポートに設定してください。
「停止」の設定をしたポートは，供給電力が余っていても電力が供給されません。

(2) 既給電ポートの優先

ポートごとに設定した優先度に依存せず，すでに接続されているポートへの給電を保持する機能です。

IP8800/S2200 は系統１および系統２のそれぞれの範囲内で既給電ポートを優先します。

IP8800/S2100,IP8800/SS1240 は装置全体で既給電ポートを優先します。

コンフィグレーションコマンド power inline priority-control disable で，既給電ポートを優先します。

既給電ポートを優先したときは先に接続された受電装置を優先して供給します。総消費電力が 370.0W を超えた状態では，優先度「重要」と設定してあるポートに受電装置が接続されても電力供給は実施しません。

このため，コンフィグレーションコマンド power inline による優先度設定は無効となり，単に電力を供給するポートとして認識します。コンフィグレーションコマンド power inline never を設定した場合は電力供給を実施しません。

既給電ポート優先にしたときも電力供給警告通知のトラップを発行します。

なお，コンフィグレーションコマンド power inline priority-control disable 設定は，装置の再起動後に有効となります。

（3） コンフィグレーションと既給電ポートの優先度の関係

コンフィグレーションによる優先度設定と既給電ポート優先の関係を次の表に示します。

表 14-28　コンフィグレーションと既給電ポートの優先度の関係

既給電ポート優先度 （power inline priority-control disable）	コンフィグレーションの優先度設定 （power inline）	ポートの動作
既給電ポート非優先 （power inline priority-control disable 設定なし）	critical	給電ポート：優先度「重要」
	high	給電ポート：優先度「高」
	low	給電ポート：優先度「低」
	never	給電しないポート：優先度「停止」
既給電ポート優先 （power inline priority-control disable 設定あり）	critical	給電ポート：「重要」「高」「低」の優先度は無視
	high	
	low	
	never	給電しないポート：優先度「停止」

（4） PoE の給電停止について

受電装置への供給電力の総和が 370.0W をオーバーする場合，ポートに設定した優先度に従い電力の供給を停止します。装置では以下の値が 370.0W を越えた場合に優先度の低い受電装置への給電を停止します。

給電状況判定値（370.0W）＜

Class 0 のポート数×出力電力（15.4W）＋

Class 1 のポート数×出力電力（4.0W）＋

Class 2 のポート数×出力電力（7.0W）＋

Class 3 のポート数×出力電力（15.4W）＋

Class 4 のポート数×出力電力（30.0W）＋

手動電力割り当て設定ポートの合計電力

ポート優先度が同じときは，ポート番号が大きいポートから電力供給を停止します。（ポート番号の小さいポートへの電力供給を優先します。）

また，既給電ポート優先の設定があるときは，ポート優先度の低いポートから電力供給を停止します。（既給電ポートへの電力供給を優先します。）

(5) 電力供給警告通知

装置の最大電力供給能力は 370.0W であるため，各ポートの消費電力合計が 370.0W を超える場合に優先制御を実施します。なお，電力供給警告通知トラップの閾値は 340.0W（約 90%）としています。

14.10.5 電力給電再開・停止とポート状態

(1) 運用コマンドによる電力給電再開・停止

本装置では，給電を停止したポートに対して運用コマンド activate power inline で給電を再開することができます。

ただし，ポートのコンフィグレーションや運用コマンドの実行，および省電力スケジュールの動作によっても給電制御に影響します。

次の表にコンフィグレーションコマンド，および省電力スケジュール動作と給電制御への影響を示します。

表 14-29 コンフィグレーションコマンドおよび省電力スケジュール動作と給電制御への影響

指定単位	コンフィグレーションコマンド	給電制御への影響			備考
		省電力スケジュール動作			
		無効	有効（通常時間帯）	有効（スケジュール時間帯）	
装置	未サポート	－	－	－	
ポート	shutdown	○	○	×	
	no shutdown	○	○	×	
	power inline never	○	○	○	強制給電停止
	schedule-power-control shutdown interface	×	×	○	
	no schedule-power-control shutdown interface	×	×	○	

（凡例）
○：影響あり (該当ポートの給電再開・停止が発生します)
×：影響なし
－：コマンド未サポートにより影響なし

また，運用コマンドと給電制御への影響は次の表のとおりです。省電力スケジュール動作の有効・無効は影響しません。

表 14-30 運用コマンドと給電制御への影響

指定単位	ポート設定	運用コマンド	給電制御への影響	備考
装置	なし	未サポート	－	
ポート	no shutdown power inline never 以外	inactivate interface	×	
		activate interface	×	
		inactivate power inline	○	給電停止によるリンクダウン
		activate power inline	○	給電再開によるリンクアップ

指定単位	ポート設定	運用コマンド	給電制御への影響	備考
	上記以外	inactivate interface	×	運用コマンド実行による影響はなく，コンフィグレーションに従います。（表 14-29 参照）
		activate interface	×	
		inactivate power inline	×	
		activate power inline	×	

（凡例）
○：影響あり
×：影響なし
－：コマンド未サポートにより影響なし

(2) ポート状態が遷移する契機

運用コマンド show power inline で表示するポート状態は，コンフィグレーション設定や運用コマンドの実行，または電力供給状態により遷移します。

- off：電力を供給していません。
- on：電力を供給しています。
- denied：十分な電力がなく，電力を供給していません。
- faulty：接続された装置に電力を供給できません。
- inact：運用コマンドで電力の供給を停止しています。

次の表にポート状態と状態遷移する契機を示します。

表 14-31 ポート状態と状態遷移の契機

ポートの状態	状態遷移の契機	遷移後のポート状態
off（受電装置未接続時）	受電装置を接続する（電力供給開始）	on
	運用コマンド inactivate power inline 実行	inact
off（shutdown 設定時）	コンフィグレーションコマンド no shutdown 設定	off（受電装置未接続時）
		on（受電装置接続時）
on	接続していた受電装置を外す（電力供給停止）	off
	コンフィグレーションコマンド shutdown 設定	
	運用コマンド inactivate power inline 実行	inact
	装置全体の電力不足を検出（電力供給停止）	denied
	オーバーロード検出	faulty
	PoE コントローラの温度異常検出	
	その他の異常検出	
denied	コンフィグレーションコマンド shutdown 設定	off
	接続していた受電装置を外す	
	装置全体の電力不足解決（電力供給開始）	on
	運用コマンド inactivate power inline 実行	inact

ポートの状態	状態遷移の契機	遷移後のポート状態
faulty	コンフィグレーションコマンド shutdown 設定	off
	運用コマンド activate power inline 実行	off（受電装置未接続時）
		on（受電装置接続時）
	運用コマンド inactivate power inline 実行	inact
	接続していた受電装置を外す	faulty
	受電装置を接続する	
inact	コンフィグレーションコマンド shutdown 設定	off
	運用コマンド activate power inline 実行	off（受電装置未接続時）
		on（受電装置接続時）
	接続していた受電装置を外す	inact
	受電装置を接続する	

(a) ポート状態 "faulty" の要因と対応

ポート状態が "faulty" を表示したときは，該当ポートの給電を停止します。「表 14-31　ポート状態と状態遷移の契機」に示すように，ポート状態が "faulty" となる主な要因としては，下記があります。

- オーバロード検出
- PoE コントローラの温度異常検出
- その他の PoE 異常検出

該当ポートの給電を再開するときは，運用コマンド activate power inline を実行してください。

(b) ポート状態 "denied" の要因と対応

ポート状態が "denied" を表示したときは，装置全体の供給電力が不足しているため，該当ポートの給電を停止しています。

運用コマンド show power inline で，装置全体の割り当て電力量と装置全体の総供給電力量を確認し，コンフィグレーションで適切な電力割り当て量を設定，または受電装置の接続構成を確認してください。

装置全体の供給電力不足が解消されると，ポート状態 "denied" は解消されます。

14.10.6　PoE 使用時の注意事項

(1) 手動による電力割り当て設定について

手動割り当て設定は，受電装置のマニュアルをよくご確認のうえ，お客様の責任において行ってください。

受電装置の最大消費電力に若干の余裕を持たせた値を設定してください。

受電装置が必要とする最低消費電力よりも小さな値を手動設定すると，オーバーロードを検出して受電装置への電力供給を停止する場合があります。回復するときは，運用コマンド activate power inline を実行してください。

(2) 既給電ポート優先で使用する場合

コンフィグレーションコマンド power inline priority-control disable を設定すると，コンフィグレーションコマンド power inline による優先度設定は無効となるため，装置を再起動したときは，再起動前と給電

ポートが変わる場合があります。

（3） 接続装置が Pre.STD の場合

IP8800/S2200,IP8800/S2100 では Pre.STD の接続をサポートしていません。

IP8800/SS1240 で Pre.STD 対応の受電装置を接続する場合は，ストレートケーブルを使用してください。クロスケーブルでは接続できません。

（4） 省電力スケジュールを併用している場合

PoE ポートに schedule-power-control shutdown interface を設定した場合，スケジュール時間帯への切り替えのタイミングで，コンソールが十数秒程度，無応答状態に見える場合があります。

14.11 PoE のコンフィグレーション【S2200】【S2100】【SS1240】

14.11.1 コンフィグレーションコマンド一覧

PoE のコンフィグレーションコマンド一覧を次の表に示します。

表 14-32 コンフィグレーションコマンド一覧

コマンド名	説明
power inline	ポート優先度を設定します。
power inline priority-control disable	既給電ポートを優先します。
power inline allocation	ポート単位の割り当て電力を Class ベースまたは手動で設定します。
power inline system-allocation【S2200】	系統 1 で供給可能な最大電力量を手動で設定します。

14.11.2 系統 1 で供給可能な最大電力量の設定【S2200】

IP8800/S2200 は系統 1 と系統 2 に分かれており，系統 1 全体で供給可能な最大電力量はコンフィグレーションで設定できます。

なお，装置全体 370.0W から系統 1 の設定値を差し引いた値が，系統 2 全体の電力割り当て量となります。

[設定のポイント]

系統 1 で 60.0W 給電を使用するために，最大 240.0W の供給電力量を割り当てます。

[コマンドによる設定]

1. **(config)# power inline system-allocation limit 240000**
   ```
   Please execute the reload command after save,
   because this command becomes effective after reboot.
   ```
   系統 1 全体で供給可能な最大電力量を 240.0W に設定します。設定の保存と装置再起動を促すメッセージを表示します。

2. **(config)# exit**
   # copy running-config startup-config
   ```
   Do you wish to copy from running-config to startup-config? (y/n): y
   ```
   コンフィグレーションコマンドモードから装置管理者モードに移行し，保存します。

3. **@# reload**
   ```
   Restart OK? (y/n): y
   ```
   コンフィグレーションの設定を保存すると，プロンプトに " @ " を表示しますので，運用コマンド reload で装置を再起動してください。

[注意事項]

本コマンドを設定および削除した場合は，装置再起動後に変更内容が反映されます。

14.11.3 ポート優先度の設定

本装置の PoE 機能は，３段階の電力供給優先度を設定できます。電力供給能力が不足した場合は，優先度の低いポートから電力供給を停止します。なお，本装置から電力を供給しない運用にしたい場合は，電力供給を停止するように設定できます。

[設定のポイント]

接続する装置が PoE 受電装置の場合で，本装置から電力を供給しない場合，もしくは接続する相手装置も PoE 給電装置の場合に電力供給の停止を設定します。
ここでは，ポート 0/10 で電力を供給しないように設定します。

[注意事項]

PoE ポートで接続する相手装置が給電装置の場合は，本装置で該当するポートに電力供給の停止を設定してください。相手装置が給電装置で，電力供給の停止を設定しない場合は，オーバーロードを検出してメッセージを出力する場合があります。相手装置で電力供給を停止できる場合は，相手装置でも電力供給を停止することを推奨します。

[コマンドによる設定]

1. **(config)# interface fastethernet 0/10**
   (config-if)# power inline never
   PoE 機能での電力を供給しないように設定します。

2. **(config-if)# exit**

14.11.4 既給電ポート優先の設定

ポート優先度を無効にし，既給電ポートを優先したときは先に接続された受電装置を優先して供給します。総消費電力が 370.0W を超えた状態では，優先度「重要」と設定してあるポートに受電装置が接続されても電力供給は実施しません。

[設定のポイント]

コンフィグレーションコマンド power inline によるポート優先度設定を無効にし，既給電ポートを優先にします。

[コマンドによる設定]

1. **(config)# power inline priority-control disable**
   ```
   Please execute the reload command after save,
   because this command becomes effective after reboot.
   ```
   ポート優先度設定を無効にし，既給電ポート優先を設定します。設定の保存と装置再起動を促すメッセージを表示します。

2. **(config)# exit**
   # copy running-config startup-config
   ```
   Do you wish to copy from running-config to startup-config? (y/n): y
   ```
   コンフィグレーションコマンドモードから装置管理者モードに移行し，保存します。

3. **@# reload**
   ```
   Restart OK? (y/n): y
   ```
   コンフィグレーションの設定を保存すると，プロンプトに " @ " を表示しますので，運用コマンド

reload で装置を再起動してください。

[注意事項]

本コマンドを設定および削除した場合は，装置再起動後に変更内容が反映されます。

14.11.5 ポート単位の供給電力割り当て設定

ポート単位の供給電力は，Class ベースまたは手動で設定できます。初期状態は Class ベースによる割り当て設定です。

[設定のポイント]

接続する装置が Class 4 の受電装置で，最大 30.0W より少ない消費電力の場合，受電装置の最大消費電力に若干の余裕を加えて供給電力値を設定します。
ここでは，ポート 0/20 に接続する供給電力を任意値に設定します。

[コマンドによる設定]

1. **(config)# interface fastethernet 0/20**
   (config-if)# power inline allocation limit 20000
   ポート 0/20 の供給電力を 20000mW（20W）に設定します。

2. **(config-if)# exit**

14.12 PoE のオペレーション【S2200】【S2100】【SS1240】

14.12.1 運用コマンド一覧

PoE の運用コマンド一覧を次の表に示します。

表 14-33 運用コマンド一覧

コマンド名	説明
show power inline	PoE 情報を表示します。
activate power inline	電力供給を手動で再開します。
inactivate power inline	電力供給を手動で停止します。

14.12.2 PoE の確認

PoE の電力供給状態を確認するには，運用コマンド show power inline を使用します。電力を供給している場合は，Status に「on」を表示し，Priority に電力供給の優先度，Class に IEEE802.3af/IEEE802.3at 準拠電力クラス，Power/Vol/Cur にポート単位の消費電力 / 電圧 / 電流状態を表示します。

運用コマンド show power inline の実行結果を次の図に示します。

図 14-7 PoE 電力供給状態の表示例【S2200】

```
> show power inline
Please wait a little.

Date 20XX/07/03 20:46:06 UTC
System Wattage       :   370.0
Priority Control     :  enable

                       < 0/1-4> <0/5-24>
Threshold(W)         :   240.0    130.0
Total Allocate(W)    :   240.0     60.8
Total Power(W)       :   210.3      2.0

Port Counts          :      24
 Port Status Priority Class  Alloc(mW) Power(mW) Vol(V) Cur(mA) Description
 0/1  on     low      manual     60000     54400   53.6    1014
 0/2  on     high     manual     60000     48600   53.7     900
 0/3  on     critical manual     60000     51200   53.9     949
 0/4  on     high     manual     60000     56100   53.9    1047
 0/5  on     critical manual     30000       700   53.9      14
 0/6  on     low      0          15400       700   53.9      14
 0/7  off    high     -              0         0    0.0       0
 0/8  off    high     -              0         0    0.0       0
 0/9  off    high     -              0         0    0.0       0
 0/10 off    high     -              0         0    0.0       0
 0/11 off    high     -              0         0    0.0       0
 0/12 off    high     -              0         0    0.0       0
 0/13 off    high     -              0         0    0.0       0
 0/14 off    high     -              0         0    0.0       0
 0/15 off    high     -              0         0    0.0       0
 0/16 off    high     -              0         0    0.0       0
 0/17 off    high     -              0         0    0.0       0
 0/18 off    high     -              0         0    0.0       0
 0/19 off    high     -              0         0    0.0       0
 0/20 off    high     -              0         0    0.0       0
 0/21 off    high     -              0         0    0.0       0
 0/22 off    high     -              0         0    0.0       0
```

```
 0/23 off    high     -              0         0    0.0       0
 0/24 on     high     0          15400       600   53.8      13

>
```

図 14-8　PoE 電力供給状態の表示例【S2100】【SS1240】

```
> show power inline
Please wait a little.

Date 20XX/11/07 14:18:40 UTC
System Wattage:                          …1.
Threshold(W)          :   370.0
Total Allocate(W)     :   146.6
Total Power(W)        :    87.1
Priority Control      :  enable
Port Counts           :      24
 Port Status Priority  Class  Alloc(mW) Power(mW) Vol(V) Cur(mA) Description
 0/1  on     high      0          15400      5400   51.3     107 IPphone(1001)
 0/2  on     high      0          15400      5200   51.1     102 IPphone(1002)
 0/3  on     high      0          15400      5100   50.9     101 IPphone(1003)
 0/4  inact  high      -              0         0    0.0       0 IPphone(1004)
 0/5  on     critical  4          30000     25900   50.9     510 PRINTER
 0/6  off    high      -              0         0    0.0       0
 0/7  off    never     -              0         0    0.0       0
 0/8  on     high      3          15400     12400   50.9     244
 0/9  on     low       1           4000      2100   51.0      43
 0/10 off    high      -              0         0    0.0       0
 0/11 on     critical  manual     30000     18000   51.1     353 wirelessAP
 0/12 off    high      -              0         0    0.0       0
 0/13 off    high      -              0         0    0.0       0
 0/14 on     high      2           7000      5900   51.0     117
 0/15 off    low       -              0         0    0.0       0
 0/16 off    high      -              0         0    0.0       0
 0/17 off    high      -              0         0    0.0       0
 0/18 off    never     -              0         0    0.0       0
 0/19 off    high      -              0         0    0.0       0
 0/20 on     high      2           7000      3800   51.1      76
 0/21 off    high      -              0         0    0.0       0
 0/22 off    high      -              0         0    0.0       0
 0/23 on     high      2           7000      3300   50.9      66
 0/24 off    high      -              0         0    0.0       0

>
```

1. IP8800/S2100 の場合は「System Wattage　: 370.0」を表示します。

15 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。

15.1 **リンクアグリゲーション基本機能の解説**

15.2 **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**

15.3 **リンクアグリゲーション拡張機能の解説**

15.4 **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**

15.5 **リンクアグリゲーションのオペレーション**

15.1 リンクアグリゲーション基本機能の解説

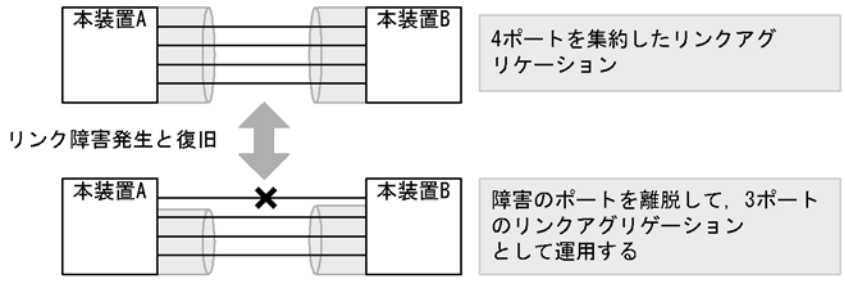
15.1.1 概要

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。

15.1.2 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 15-1 リンクアグリゲーションの構成例



15.1.3 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 15-1 リンクアグリゲーションのサポート仕様

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

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

(凡例)
－：該当しない

注※
その時点でリンクアップしている最高速度よりも遅い回線です。

15.1.4 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。

15.1.5 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 15-2 フレーム送信時のポート振り分け

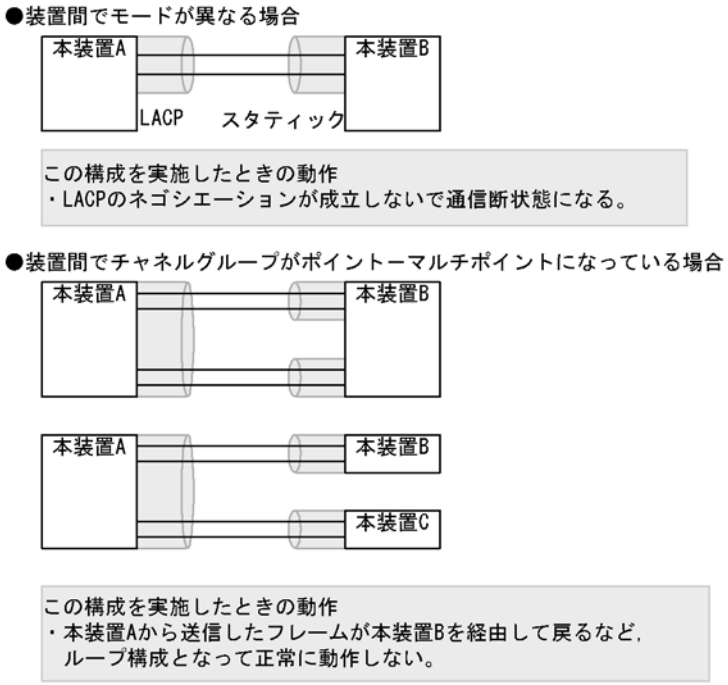
中継	フレームの種類	振り分けに使用する情報
レイヤ 2 中継	MAC アドレス未学習フレーム (ブロードキャスト，マルチキャスト含む)	宛先 MAC アドレス 送信元 MAC アドレス 受信ポート番号または受信チャネルグループ番号
	MAC アドレス学習済の IP フレーム	宛先 IP アドレス 送信元 IP アドレス 宛先 TCP/UDP ポート番号 送信元 TCP/UDP ポート番号
	MAC アドレス学習済の非 IP フレーム	宛先 MAC アドレス 送信元 MAC アドレス 受信 VLAN イーサタイプ

15.1.6 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 15-2 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。タイムアウト・一時的な通信断が頻発する場合は，CPU が過負荷状態となっている可能性があるため，LACPDU の送信間隔を長くするか，スタティックリンクアグリゲーションを使用してください。

15.2 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

15.2.1 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 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
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。

15.2.2 スタティックリンクアグリゲーションの設定

[設定のポイント]

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

[コマンドによる設定]

1. **(config)# interface range fastethernet 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 3 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 3 に登録します。

15.2.3 LACP リンクアグリゲーションの設定

(1) チャネルグループの設定

[設定のポイント]

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

[コマンドによる設定]

1. **(config)# interface range fastethernet 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 3 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 3 に登録します。LACP は active モードとして対向装置に関係なく LACPDU の送信を開始します。passive を指定した場合は，対向装置からの LACPDU を受信したときだけ LACPDU の送信を開始します。

(2) システム優先度の設定

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

[設定のポイント]

LACP システム優先度は値が小さいほど高い優先度となります。

[コマンドによる設定]

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

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

(3) ポート優先度の設定

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

[設定のポイント]

LACP ポート優先度は値が小さいほど高い優先度となります。

[コマンドによる設定]

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

[注意事項]

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

15.2.4 ポートチャネルインタフェースの設定

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

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

(1) ポートチャネルインタフェースとイーサネットインタフェースの関係

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

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

ポートチャネル関連コマンドを次の表に示します。

表 15-4 ポートチャネルインタフェースの関連コマンド

機能	コマンド
VLAN	switchport mode
	switchport access

機能	コマンド
	switchport protocol
	switchport trunk
	switchport mac
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
DHCP snooping	ip arp inspection limit rate
	ip arp inspection trust
	ip dhcp snooping limit rate
	ip dhcp snooping trust
	ip verify source
IEEE802.1X	dot1x port-control
	dot1x multiple-authentication
	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
	dot1x force-authorized
	dot1x force-authorized vlan
アップリンク・リダンダント	switchport backup interface
	switchport backup flush request transmit
L2 ループ検知	loop-detection

機能	コマンド
CFM	ethernet cfm enable
	ethernet cfm mep
	ethernet cfm mip
ポートミラーリング	switchport monitor dot1q tag

(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 fastethernet 0/1-2**
   (config-if-range)# channel-group 3 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 3 に登録します。また，チャネルグループ 3 のポートチャネルインタフェースが自動生成されます。

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

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

(3) ポートチャネルインタフェースの shutdown

[設定のポイント]

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

[コマンドによる設定]

1. **(config)# interface range fastethernet 0/1-2**
   (config-if-range)# channel-group 3 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 3 として登録します。

2. **(config)# interface port-channel 3**
   (config-if)# shutdown
   (config-if)# exit
   ポートチャネルインタフェースモードに移行して shutdown を設定します。ポート 0/1，0/2 の通信が停止し，チャネルグループ 3 は停止状態になります。

15.2.5 チャネルグループの削除

チャネルグループのポートやチャネルグループ全体を削除する場合は，削除する対象のポートをあらかじめイーサネットインタフェースコンフィグレーションモードで shutdown に設定して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 15-4　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 fastethernet 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コンフィグレーションコマンド channel-group mode が自動的に削除されます。ただし，各ポートには削除前に interface port-channel で設定した関連コマンド（表 15-4　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 fastethernet 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 3**
   チャネルグループ 3 を削除します。ポート 0/1，0/2 に設定されているコンフィグレーションコマンド channel-group mode も自動的に削除されます。

15.3 リンクアグリゲーション拡張機能の解説

15.3.1 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。

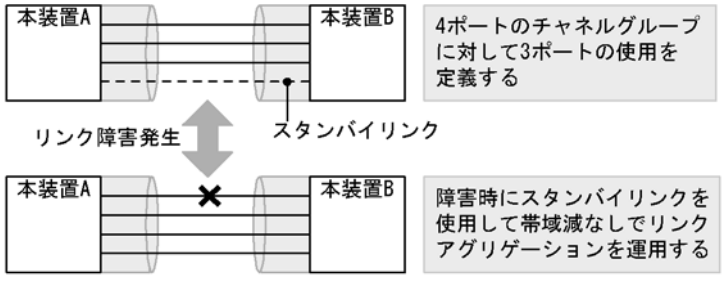
待機用ポートは，コンフィグレーションで設定するポート優先度，ポート番号から選択されます。待機用ポートは，次の表に示すように選択優先度の高い順に決定します。

表 15-5 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 15-3 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（待機用ポート）をリンクダウン状態にします。スタンバイリンク機能をサポートしていない対向装置も待機用ポートにすることができます。
- 非リンクダウンモード
  スタンバイリンク（待機用ポート）をリンクダウン状態にしないで，送信だけを停止します。リンクアップ状態のため，待機中のポートでも障害を監視できます。また，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。
- 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。

(4) リンクダウンモード使用時の注意事項

同一チャネルグループに Fastethernet ポートと Gigabitethernet ポートを混在した構成で，Gigabitethernet ポートを運用ポートとして使用するときは，Gigabitethernet ポートにコンフィグレーションコマンド lacp port-priority でポート優先度を高く設定してください。（ポート優先度は値が小さいほど，優先度が高くなります。）

15.4 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

15.4.1 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 15-6 コンフィグレーションコマンド一覧

コマンド名	説明
channel-group lacp system-priority	システム優先度をチャネルグループごとに設定します。
channel-group max-active-port	スタンバイリンク機能を設定し，最大ポート数を指定します。
lacp port-priority	ポート優先度を設定します。スタンバイリンクを選択するために使用します。
lacp system-priority	システム優先度のデフォルト値を設定します。

15.4.2 スタンバイリンク機能のコンフィグレーション

[設定のポイント]

チャネルグループにスタンバイリンク機能を設定して，同時に最大ポート数を設定します。また，リンクダウンモード，非リンクダウンモードのどちらかを設定します。スタンバイリンク機能は，スタティックリンクアグリゲーションだけで使用できます。

待機用ポートはポート優先度によって設定し，優先度が低いポートからスタンバイリンクに選択します。ポート優先度は値が小さいほど高い優先度になります。

[コマンドによる設定]

1. **(config)# interface port-channel 3**

   チャネルグループ 3 のポートチャネルインタフェースコンフィグレーションモードに移行します。

2. **(config-if)# channel-group max-active-port 3**

   チャネルグループ 3 にスタンバイリンク機能を設定して，最大ポート数を 3 に設定します。チャネルグループ 3 はリンクダウンモードで動作します。

3. **(config-if)# exit**

   グローバルコンフィグレーションモードに戻ります。

4. **(config)# interface port-channel 5**
   (config-if)# channel-group max-active-port 1 no-link-down
   (config-if)# exit

   チャネルグループ 5 のポートチャネルインタフェースコンフィグレーションモードに移行して，スタンバイリンク機能を設定します。最大ポート数を 1 とし，非リンクダウンモードを設定します。

5. **(config)# interface fastethernet 0/1**
   (config-if)# channel-group 5 mode on
   (config-if)# lacp port-priority 300
   (config-if)# exit

   チャネルグループ 5 にポート 0/1 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。

15.5 リンクアグリゲーションのオペレーション

15.5.1 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 15-7 運用コマンド一覧

コマンド名	説明
show channel-group	リンクアグリゲーションの情報を表示します。
show channel-group statistics	リンクアグリゲーションのデータパケット送受信統計情報を表示します。
show channel-group statistics lacp	LACPDU の送受信統計情報を表示します。
clear channel-group statistics lacp	LACPDU の送受信統計情報をクリアします。

15.5.2 リンクアグリゲーションの状態の確認

(1) リンクアグリゲーションの接続状態の確認

リンクアグリゲーションの情報を運用コマンド show channel-group で表示します。CH Status でチャネルグループの接続状態を確認できます。また，設定が正しいことを各項目で確認してください。

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

図 15-4 show channel-group の実行結果

```
> show channel-group 8

Date 20XX/11/13 10:54:25 UTC
ChGr: 8   Mode: LACP
  CH Status       : Up      Elapsed Time: 00:00:16
  Max Active Port: 8
  MAC address     : 0012.e231.0101  VLAN ID: 100
  Actor System    : Priority: 128    MAC: 00ed.f031.0001  Key: 8
  Partner System : Priority: 128    MAC: 0012.e214.ff99  Key: 8
  Port Information
    0/1   Up    State: Distributing
    0/2   Up    State: Distributing
    0/3   Up    State: Distributing
    0/4   Up    State: Distributing
    0/5   Down  State: Detached
    0/6   Down  State: Detached
    0/7   Down  State: Detached
    0/8   Down  State: Detached
  Uplink redundant
    Switchport backup pairs                          Preemption    Flush
    Primary    Status      Secondary  Status      Delay Limit   VLAN
    ChGr 8     Blocking    Port 0/24  Forwarding     60    43      -

>
```

(2) 各ポートの運用状態の確認

運用コマンド show channel-group detail で各ポートの詳細な状態を表示します。ポートの通信状態を Status で確認してください。

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

図 15-5　show channel-group detail の実行結果

```
> show channel-group 8 detail

Date 20XX/11/13 10:55:01 UTC
ChGr: 8   Mode: LACP
  CH Status       : Up      Elapsed Time: 00:00:52
  Max Active Port: 8
  MAC address     : 0012.e231.0101  VLAN ID: 100
  Actor System    : Priority: 128    MAC: 00ed.f031.0001  Key: 8
  Partner System : Priority: 128    MAC: 0012.e214.ff99  Key: 8
  Port Information
  Port: 0/1   Up
    State: Distributing  Speed: 100M   Duplex: Full
    Actor   Port  : Priority: 128
    Partner System: Priority: 128    MAC: 0012.e214.ff99  Key: 8
    Partner Port  : Priority: 128    Number: 22
  Port: 0/2   Up
    State: Distributing  Speed: 100M   Duplex: Full
    Actor   Port  : Priority: 128
    Partner System: Priority: 128    MAC: 0012.e214.ff99  Key: 8
    Partner Port  : Priority: 128    Number: 21
  Port: 0/3   Up
    State: Distributing  Speed: 100M   Duplex: Full
    Actor   Port  : Priority: 128
    Partner System: Priority: 128    MAC: 0012.e214.ff99  Key: 8
    Partner Port  : Priority: 128    Number: 24
  Port: 0/4   Up
    State: Distributing  Speed: 100M   Duplex: Full
    Actor   Port  : Priority: 128
    Partner System: Priority: 128    MAC: 0012.e214.ff99  Key: 8
    Partner Port  : Priority: 128    Number: 23
  Port: 0/5   Down
    State: Detached      Speed: -      Duplex: -
    Actor   Port  : Priority: 128
  Port: 0/6   Down
    State: Detached      Speed: -      Duplex: -
    Actor   Port  : Priority: 128
  Port: 0/7   Down
    State: Detached      Speed: -      Duplex: -
    Actor   Port  : Priority: 128
  Port: 0/8   Down
    State: Detached      Speed: -      Duplex: -
    Actor   Port  : Priority: 128
  Uplink redundant
    Switchport backup pairs                          Preemption    Flush
    Primary    Status      Secondary  Status      Delay Limit   VLAN
    ChGr 8     Blocking    Port 0/24  Forwarding     60     5      -

>
```

16 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。

16.1　概要

16.2　サポート機能

16.3　レイヤ 2 スイッチ機能と他機能の共存について

16.1 概要

16.1.1 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。

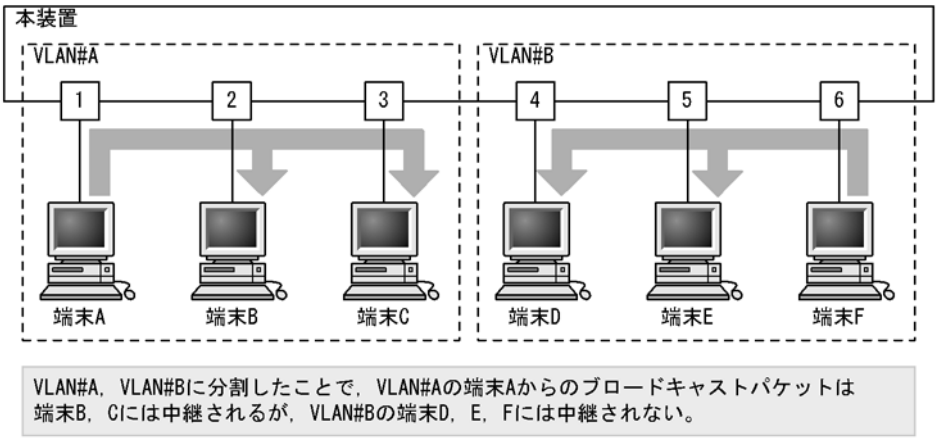
レイヤ 2 スイッチは，MAC アドレステーブルのエントリに従ってフレームを中継します。フレームの宛先 MAC アドレスに一致するエントリがあると，そのエントリのポートに中継します（エントリのポートが受信したポートである場合は中継しません）。一致するエントリがない場合，受信したポート以外のすべてのポートにフレームを中継します。この中継をフラッディングと呼びます。

16.1.2 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 16-1 VLAN の概要



16.2 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 16-1 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
	L2 プロトコルフレーム透過機能	レイヤ 2 のプロトコルのフレームを中継する機能 スパニングツリー (BPDU)，IEEE802.1X(EAP) を透過します。
スパニングツリー	PVST+	VLAN 単位のスイッチ間のループ防止機能
	シングルスパニングツリー	装置単位のスイッチ間のループ防止機能
	マルチプルスパニングツリー	MST インスタンス単位のスイッチ間のループ防止機能
Ring Protocol		リングトポロジーでのレイヤ 2 ネットワークの冗長化機能
IGMP snooping/MLD snooping		レイヤ 2 スイッチで VLAN 内のマルチキャストトラフィック制御機能
ポート間中継遮断機能		指定したポート間ですべての通信を遮断する機能

16.3 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 16-2 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	レイヤ 2 認証	一部制限あり※ 1
		ポートミラーリング (ミラーポート)	共存不可
	プロトコル VLAN	デフォルト VLAN	共存不可
		PVST+	
		レイヤ 2 認証	一部制限あり※ 1
		ポートミラーリング (ミラーポート)	共存不可
	MAC VLAN	デフォルト VLAN	共存不可
		PVST+	
		レイヤ 2 認証	一部制限あり※ 1
		ポートミラーリング (ミラーポート)	共存不可
デフォルト VLAN		プロトコル VLAN	共存不可
		MAC VLAN	
		IGMP snooping	
		MLD snooping	
		レイヤ 2 認証	一部制限あり※ 1
		ポートミラーリング (ミラーポート)	共存不可
VLAN 拡張機能	L2 プロトコルフレーム透過機能 (BPDU)	PVST+	共存不可
		シングルスパニングツリー	
		マルチプルスパニングツリー	
	L2 プロトコルフレーム透過機能 (EAP)	レイヤ 2 認証	一部制限あり※ 1
	ポート間中継遮断機能	スパニングツリー	一部制限あり※ 2
		DHCP snooping	
		IGMP snooping	
		MLD snooping	
		GSRP aware	
		CFM	

注※ 1

「コンフィグレーションガイド Vol.2 5 レイヤ 2 認証機能の概説」を参照してください。

注※ 2

「19.3.2 ポート間中継遮断機能使用時の注意事項」を参照してください。

表 16-3 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	
	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	
	Ring Protocol	
	レイヤ 2 認証	一部制限あり※1
	アップリンク・リダンダント	一部制限あり※2
シングルスパニングツリー	L2 プロトコルフレーム透過機能 (BPDU)	共存不可
	マルチプルスパニングツリー	
	Ring Protocol	
	レイヤ 2 認証	一部制限あり※1
	アップリンク・リダンダント	一部制限あり※2
マルチプルスパニングツリー	L2 プロトコルフレーム透過機能 (BPDU)	共存不可
	シングルスパニングツリー	
	PVST+	
	ループガード	
	Ring Protocol	
	レイヤ 2 認証	一部制限あり※1
	アップリンク・リダンダント	一部制限あり※2

注※ 1

「コンフィグレーションガイド Vol.2　5　レイヤ 2 認証機能の概説」を参照してください。

注※ 2

アップリンク・リダンダントのプライマリポート・セカンダリポートを設定したポートは，スパニングツリー強制 Disable となります。

表 16-4 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	PVST+	共存不可
	シングルスパニングツリー	
	マルチプルスパニングツリー	
	DHCP snooping（端末フィルタ機能）	一部制限あり※1
	レイヤ 2 認証	一部制限あり※2
	アップリンク・リダンダント	一部制限あり※3

注※ 1

DHCP snooping で端末フィルタを行うポートは，リングポート以外を設定してください。

注※ 2

認証を行うポートは，リングポート以外を設定してください。

注※ 3
アップリンク・リダンダントのプライマリポート・セカンダリポートは，リングポート以外を設定してください。

表 16-5 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
	レイヤ 2 認証	一部制限あり※
MLD snooping	デフォルト VLAN	共存不可

注※
「コンフィグレーションガイド Vol.2 5 レイヤ 2 認証機能の概説」を参照してください。

17 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。

17.1 MAC アドレス学習の解説

17.2 MAC アドレス学習のコンフィグレーション

17.3 MAC アドレス学習のオペレーション

17.1 MAC アドレス学習の解説

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

MAC アドレス学習では，チャネルグループを一つのポートとして扱います。

17.1.1 送信元 MAC アドレス学習

すべての受信フレームを MAC アドレス学習の対象とし，送信元 MAC アドレスを学習して MAC アドレステーブルに登録します。登録した MAC アドレスは，エージング処理で削除されるまで保持します。学習は VLAN 単位に行い，MAC アドレステーブルは MAC アドレスと VLAN のペアによって管理します。同一の MAC アドレスでも VLAN が異なる場合は登録します。

17.1.2 学習 MAC アドレスのエージング

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

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

学習したエントリを削除するまでに最大でエージング時間の 2 倍掛かることがあります。

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

17.1.3 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 17-1 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。

17.1.4 スタティックエントリの登録

受信フレームによるダイナミックな学習のほかに，ユーザ指定によってスタティックに MAC アドレスを登録できます。ユニキャスト MAC アドレスに対して一つのポートまたはチャネルグループを指定できます。

ユニキャスト MAC アドレスに対してスタティックに登録を行うと，そのアドレスについてダイナミックな学習は行いません。すでに学習済みのエントリは MAC アドレステーブルから削除してスタティックエントリを登録します。また，指定された MAC アドレスが送信元のフレームをポートまたはチャネルグループ以外から受信した場合は，そのフレームを廃棄します。スタティックエントリの指定パラメータを次の表に示します。

表 17-2 スタティックエントリの指定パラメータ

項番	指定パラメータ	説明
1	MAC アドレス	ユニキャスト MAC アドレスを指定できます。
2	VLAN	このエントリを登録する VLAN を指定します。
3	送信先ポート指定	一つのポートまたはチャネルグループを指定できます。

17.1.5 MAC アドレステーブルのクリア

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

表 17-3 MAC アドレステーブルをクリアする契機

契機	説明
ポートダウン※1	該当ポートから学習したエントリを削除します。
チャネルグループダウン※2	該当チャネルグループから学習したエントリを削除します。
運用コマンド clear mac-address-table の実行	パラメータに従って MAC アドレステーブルをクリアします。
スパニングツリーのトポロジー変更	[本装置でスパニングツリーを構成] トポロジー変更を検出した時に MAC アドレステーブルをクリアします。
	[スパニングツリーと Ring Protocol を併用しているネットワーク構成で，本装置がリングネットワークのトランジットノードとして動作] Ring Protocol と併用している装置がトポロジー変更を検出した時に送信するフラッシュ制御フレームを受信した場合，MAC アドレステーブルをクリアします。
GSRP のマスタ／バックアップ切り替え	[本装置が GSRP aware として動作] GSRP スイッチがマスタ状態になった時に送信される GSRP Flush request フレームを受信した場合，MAC アドレステーブルをクリアします。
	[GSRP と Ring Protocol を併用しているネットワーク構成で，本装置がリングネットワークのトランジットノードとして動作] Ring Protocol と併用している装置がマスタ状態になった時に送信するフラッシュ制御フレームを受信した場合，MAC アドレステーブルをクリアします。
Ring Protocol による経路の切り替え	[本装置がトランジットノードとして動作] 経路切り替え時にマスタノードから送信されるフラッシュ制御フレームを受信した場合，MAC アドレステーブルをクリアします。 フラッシュ制御フレーム受信待ち保護時間のタイムアウト時に MAC アドレステーブルをクリアします。

契機	説明
	多重障害監視機能適用時，バックアップリングの切り替え／切り戻しに伴い共有ノードから送信されるフラッシュ制御フレームを受信した場合，MAC アドレステーブルをクリアします。
アップリンク・リダンダント機能によるプライマリポートとセカンダリポートの切り替え	プライマリポートからセカンダリポートへの切り替え時，およびセカンダリポートからプライマリポートへの切り戻し時に送信されるフラッシュ制御フレームを受信した場合，MAC アドレステーブルをクリアします。

注※ 1

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

注※ 2

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

17.1.6 注意事項

(1) 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，PC などの端末がポート間を移動した場合，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，運用コマンド clear mac-address-table 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。

(2) 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。

(3) レイヤ 2 認証機能を使用時のエージング時間について

学習したエントリのエージング時間はコンフィグレーションで設定可能ですが，レイヤ 2 認証機能を使用時は，下記のエージング時間で動作します。

表 17-4 レイヤ 2 認証機能使用時のエージング時間

レイヤ 2 認証機能 設定状態	MAC アドレステーブル エージング時間設定状態	エージング動作	
		動作	エージング時間
下記認証機能のいずれかが動作中 1. IEEE802.1X •認証モード ポート単位認証（静的）または ポート単位認証（動的） •無通信監視機能有効 2. Web 認証 •認証モード 固定 VLAN モードまたは ダイナミック VLAN モード •無通信監視機能有効 3. MAC 認証 •認証モード 固定 VLAN モードまたは ダイナミック VLAN モード •無通信監視機能有効	エージング時間を 0 秒で設定	×	―
	エージング時間を 10 ～ 300 秒の範囲内で設定	○	300 秒
	エージング時間を 301 ～ 1000000 秒の範囲内で設定	○	設定時間
	未設定	○	300 秒
上記以外	エージング時間を 0 秒で設定	×	―
	エージング時間を 10 ～ 300 秒の範囲内で設定	○	設定時間
	エージング時間を 301 ～ 1000000 秒の範囲内で設定	○	設定時間
	未設定	○	300 秒

（凡例）
○：エージングする
×：エージングしない
―：該当なし

17.2 MAC アドレス学習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

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 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
mac-address-table aging-time	MAC アドレス学習のエージング時間を設定します。
mac-address-table static	スタティックエントリを設定します。

17.2.2 エージング時間の設定

[設定のポイント]

MAC アドレス学習のエージング時間を変更できます。設定は装置単位です。設定しない場合，エージング時間は 300 秒です。

[コマンドによる設定]

1. **(config)# mac-address-table aging-time 100**
   エージング時間を 100 秒に設定します。

[注意事項]

レイヤ 2 認証機能を併用しているときに，本コマンドで設定した 10 ～ 300 秒の範囲のエージング時間は 300 秒となります。詳細は，「17.1.6 注意事項 (3) レイヤ 2 認証機能を使用時のエージング時間について」を参照してください。

17.2.3 スタティックエントリの設定

スタティックエントリを登録すると，指定した MAC アドレスについて MAC アドレス学習をしないで，常に登録したエントリに従ってフレームを中継するため，MAC アドレスのエージングによるフラッディングを回避できます。本装置に直接接続したサーバなどのように，ポートの移動がなく，かつトラフィック量の多い端末などに有効な機能です。

スタティックエントリには，MAC アドレス，VLAN および出力先を指定します。出力先はポート，チャネルグループのどちらかを指定します。

(1) 出力先にポートを指定するスタティックエントリ

[設定のポイント]

出力先にポートを指定した例を示します。

[コマンドによる設定]

1. **(config)# mac-address-table static 0012.e200.1122 vlan 10 interface fastethernet 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]

1. 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. 指定 VLAN が，レイヤ 2 認証機能でポートに自動割り当てされた VLAN と一致したときは，設定できません。

(2) 出力先にリンクアグリゲーションを指定するスタティックエントリ

[設定のポイント]

出力先にリンクアグリゲーションを指定した例を示します。

[コマンドによる設定]

1. **(config)# mac-address-table static 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。

17.3 MAC アドレス学習のオペレーション

17.3.1 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 17-6 運用コマンド一覧

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

17.3.2 MAC アドレス学習の状態の確認

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

運用コマンド show mac-address-table では，MAC アドレス学習によって登録したエントリ，スタティックエントリ，レイヤ 2 認証機能，IGMP snooping および MLD snooping によって登録したエントリを表示します。

図 17-1 show mac-address-table の実行結果

```
> show mac-address-table

Date 20XX/03/16 23:24:47 UTC
Aging time : 300
MAC address         VLAN    Type      Port-list
0000.0088.7701         2    Dynamic   0/49-50
000b.972f.e22b         2    Dot1x     0/35
0000.ef01.34f4      1000    Static    0/30
0000.ef01.3d17      1000    Static    0/30
000b.9727.ee41      1024    WebAuth   0/28
0010.c6ce.e1c6      1024    MacAuth   0/29
0012.e284.c703      1024    Dynamic   0/49-50
001b.7887.a492      1024    Dynamic   0/49-50
0100.5e00.00fc      1024    Snoop     0/49-50

>
```

17.3.3 MAC アドレス学習数の確認

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

図 17-2 show mac-address-table（learning-counter パラメータ指定）の実行結果

```
> show mac-address-table learning-counter

Date 20XX/11/17 15:02:38 UTC
 Port           Count
 0/1                7
 0/2                0
 0/3                0
 0/4              124
 0/5                0
 0/6                2
 0/7                0
 0/8                0
 0/9                0
 0/10               0

>
```

18 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。

18.1 VLAN **基本機能の解説**

18.2 VLAN **基本機能のコンフィグレーション**

18.3 **ポート** VLAN **の解説**

18.4 **ポート** VLAN **のコンフィグレーション**

18.5 **プロトコル** VLAN **の解説**

18.6 **プロトコル** VLAN **のコンフィグレーション**

18.7 MAC VLAN **の解説**

18.8 MAC VLAN **のコンフィグレーション**

18.9 VLAN **のオペレーション**

18.1 VLAN 基本機能の解説

この節では，VLAN の概要を説明します。

18.1.1 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 18-1 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。

18.1.2 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 18-2 ポートの種類

ポートの種類	概要	使用する VLAN
アクセスポート	ポート VLAN として Untagged フレームを扱います。 このポートでは，すべての Untagged フレームを一つのポート VLAN で扱います。	ポート VLAN MAC VLAN
プロトコルポート	プロトコル VLAN として Untagged フレームを扱います。 このポートでは，フレームのプロトコルによって VLAN を決定します。 Tagged フレームを受信したときは廃棄します。	プロトコル VLAN ポート VLAN
MAC ポート	MAC VLAN として Untagged フレームを扱います。 このポートでは，フレームの送信元 MAC アドレスによって VLAN を決定します。 Tagged フレームを受信したときは，コンフィグレーションの設定に従います。詳細は「18.7.4 MAC ポートのオプション機能」を参照してください。	MAC VLAN ポート VLAN
トランクポート	すべての種類の VLAN で Tagged フレームを扱います。 このポートでは，VLAN Tag によって VLAN を決定します。 Untagged フレームを受信したときは，ネイティブ VLAN で扱います。	ポート VLAN プロトコル VLAN MAC VLAN

ポートの種類ごとの，使用できる VLAN の種類を次の表に示します。VLAN Tag を扱うトランクポートはすべての VLAN で同じポートを使用できます。

表 18-3 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	○	○	×

ポートの種類	VLAN の種類		
	ポート VLAN	プロトコル VLAN	MAC VLAN
MAC ポート	○	×	○
トランクポート	○	○	○

(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。

18.1.3 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
- 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）は自動的に VLAN に所属することはありません。

18.1.4 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。

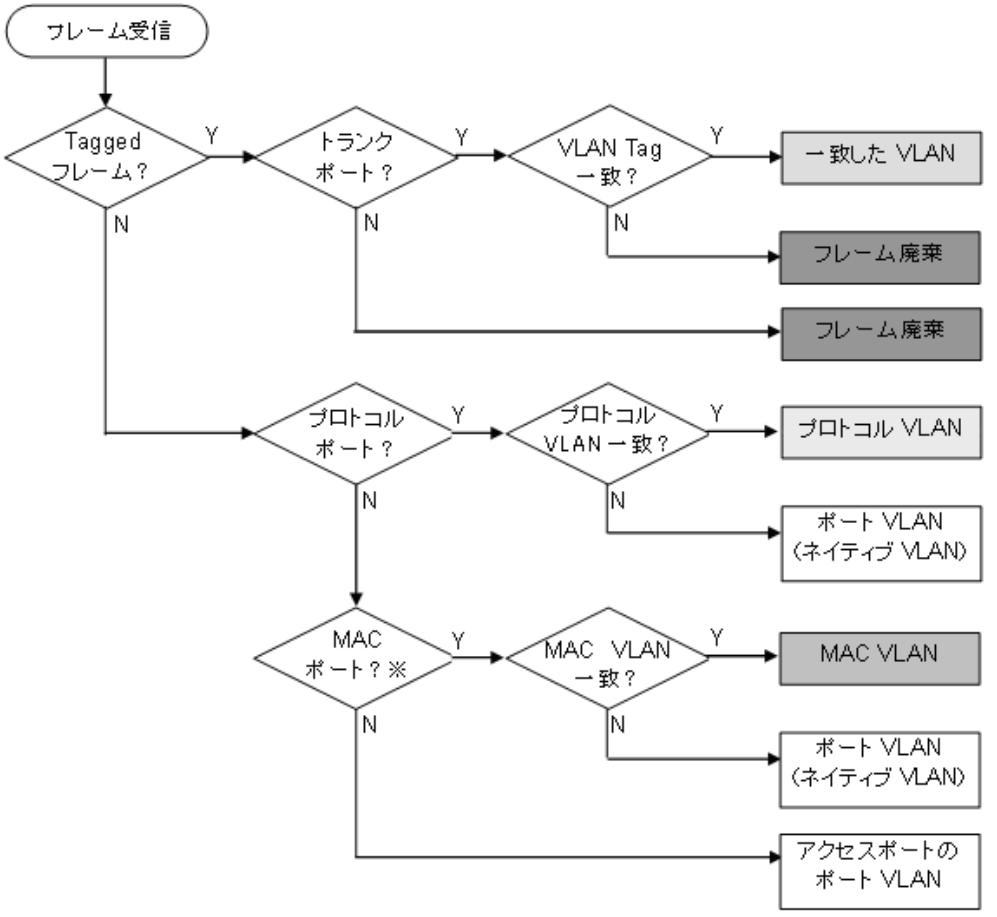
表 18-4　VLAN 判定の優先順位

ポートの種類	VLAN 判定の優先順位
アクセスポート	ポート VLAN
プロトコルポート	プロトコル VLAN ＞ポート VLAN（ネイティブ VLAN）
MAC ポート	VLAN Tag※＞ MAC VLAN ＞ポート VLAN（ネイティブ VLAN）
トランクポート	VLAN Tag ＞ポート VLAN（ネイティブ VLAN）

注※
コンフィグレーションにより Tagged フレームも扱えます。詳細は「18.7.4　MAC ポートのオプション機能」を参照してください。

VLAN 判定のアルゴリズムを次の図に示します。

図 18-1　VLAN 判定のアルゴリズム



注※
コンフィグレーション設定により Tagged フレームも扱えます。

18.1.5 VLAN Tag

(1) 概要

IEEE 802.1Q 規定による VLAN Tag（イーサネットフレーム中に Tag と呼ばれる識別子を挿入する方法）を使用して，一つのポートに複数の VLAN を構築できます。

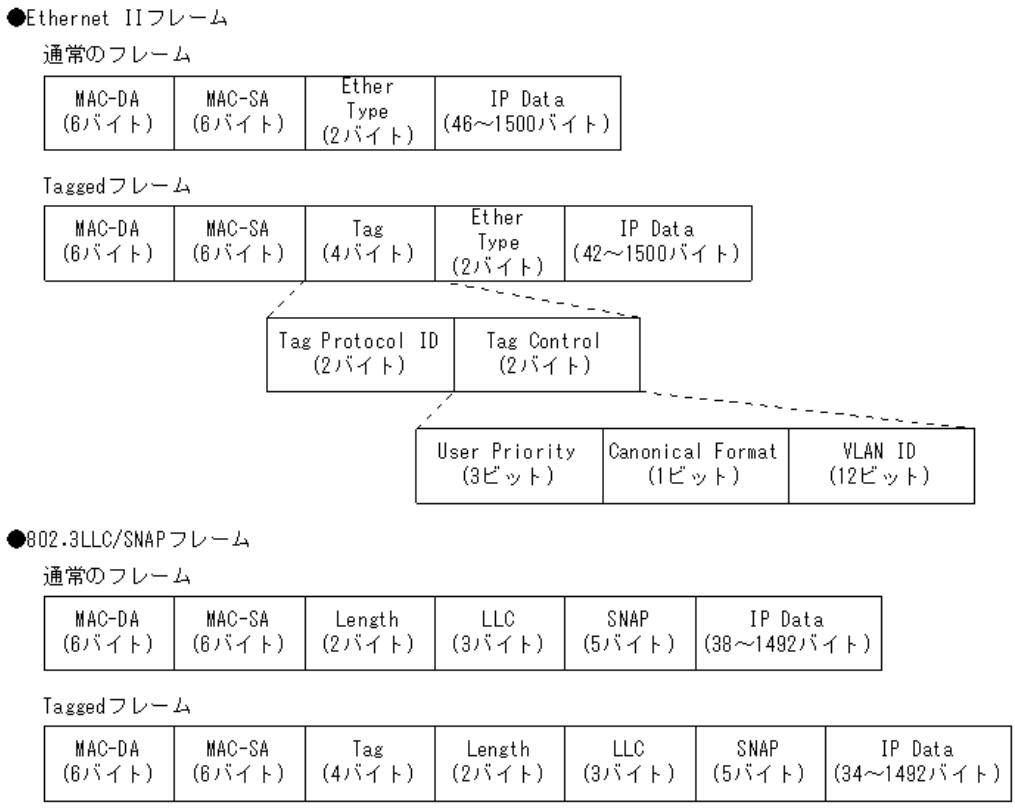
VLAN Tag はトランクポート，MAC ポートで使用します。トランクポート，MAC ポートはその対向装置も VLAN Tag を認識できなければなりません。

(2) プロトコル仕様

VLAN Tag はイーサネットフレームに Tag と呼ばれる識別子を埋め込むことで，VLAN 情報（=VLAN ID）を離れたセグメントへと伝えることができます。

Tagged フレームのフォーマットを次の図に示します。VLAN Tag を挿入するイーサネットフレームのフォーマットは，Ethernet V2 フォーマットと 802.3 フォーマットの 2 種類があります。

図 18-2 Tagged フレームのフォーマット



VLAN Tag のフィールドの説明を次の表に示します。

表 18-5 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。	本装置は TPID 設定は未サポートのため，0x8100 固定で動作します。
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。

フィールド	説明	本装置の条件
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。

本装置が中継するフレームの User Priority は，受信したフレームの User Priority と同じです。また，User Priority のデフォルト値は下記のとおりです。

- 受信したフレームが中継フレームの場合：User Priority のデフォルト値は 3
- 自発送信フレームの場合：User Priority のデフォルト値は 7

なお，送信するフレームの User Priority はコンフィグレーションで変更することができます。User Priority の変更については，下記を参照してください。

- 中継フレーム：「コンフィグレーションガイド Vol.2 3.4 マーカー解説」
- 自発送信フレーム：「コンフィグレーションガイド Vol.2 3.10 自発フレームのユーザ優先度の解説」

18.1.6 VLAN 使用時の注意事項

(1) 他機能との共存

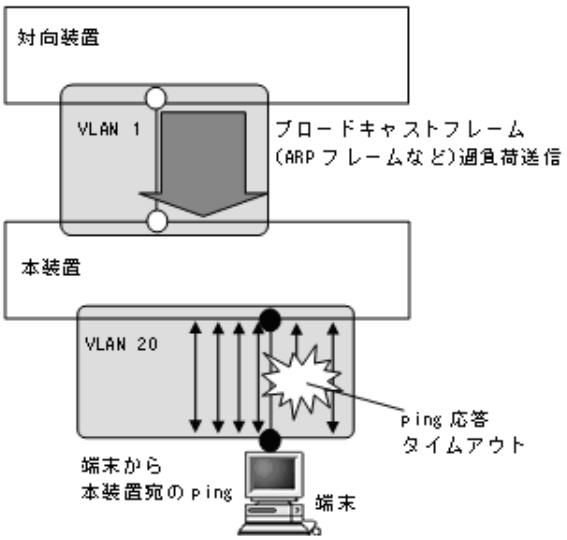
「16.3 レイヤ 2 スイッチ機能と他機能の共存について」を参照してください。

(2) VLAN1 の使用について

本装置の VLAN1 でブロードキャスト過負荷受信が発生すると，他 VLAN の ping 応答などに影響する可能性があります。

VLAN1 のブロードキャスト過負荷の例を次の図に示します。

図 18-3 VLAN1 でブロードキャスト過負荷による影響の例



- 本装置の VLAN1 は対向装置からブロードキャストフレーム（ARP フレームなど）を受信します。本装置の別 VLAN（図内の VLAN20）は，端末から本装置宛 ping を受信しています。

- VLAN1 でブロードキャスト過負荷状態が発生したとき，本装置の別 VLAN で実施している，端末から本装置宛 ping を取りこぼす（ping 応答タイムアウト）可能性があります。このような状態が発生したときは，VLAN1 以外をご使用ください。

18.2 VLAN 基本機能のコンフィグレーション

18.2.1 コンフィグレーションコマンド一覧

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 18-6 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 mac	MAC VLAN ポートの情報を設定します。
switchport mode	ポートの種類（アクセス，プロトコル，MAC，トランク）を設定します。
switchport protocol	プロトコルポートの VLAN を設定します。
switchport trunk	トランクポートの VLAN を設定します。
vlan	VLAN を作成します。また，VLAN コンフィグレーションモードで VLAN に関する項目を設定します。

18.2.2 VLAN の設定

[設定のポイント]

VLAN を作成します。新規に VLAN を作成するためには，VLAN ID と VLAN の種類を指定します。VLAN の種類を省略した場合はポート VLAN を作成します。VLAN ID リストによって複数の VLAN を一括して設定することもできます。

コンフィグレーションコマンド vlan によって，VLAN コンフィグレーションモードに移行します。作成済みの VLAN を指定した場合は，モードの移行だけとなります。VLAN コンフィグレーションモードでは VLAN のパラメータを設定できます。

なお，ここでは VLAN の種類によらない共通した設定について説明します。ポート VLAN，プロトコル VLAN，MAC VLAN のそれぞれについては次節以降を参照してください。

[コマンドによる設定]

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

   VLAN ID 10 のポート VLAN を作成し，VLAN 10 の VLAN コンフィグレーションモードに移行します。

2. **(config-vlan)# name "PORT BASED VLAN 10"**
   (config-vlan)# exit

   作成したポート VLAN 10 の名称を”PORT BASED VLAN 10”に設定します。

3. **(config)# vlan 100-200**

   VLAN ID 100 ～ 200 のポート VLAN を一括して作成します。また，VLAN 100 ～ 200 の VLAN コンフィグレーションモードに移行します。

4. **(config-vlan)# state suspend**
   (config-vlan)# exit

作成した VLAN ID 100 ～ 200 のポート VLAN を一括して停止状態にします。

18.2.3 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 fastethernet 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 3**

   チャネルグループ 3 のポートチャネルインタフェースコンフィグレーションモードに移行します。

4. **(config-if)# switchport mode trunk**
   (config-if)# exit

   チャネルグループ 3 をトランクポートに設定します。ポートチャネル 3 は Tagged フレームを扱うポートになります。

18.2.4 トランクポートの設定

[設定のポイント]

トランクポートは VLAN の種類に関係なく，すべての VLAN で使用でき，Tagged フレームを扱います。また，イーサネットインタフェースおよびポートチャネルインタフェースで使用できます。

トランクポートは，コンフィグレーションコマンド switchport mode を設定しただけではどの VLAN にも所属していません。このポートで扱う VLAN はコンフィグレーションコマンド switchport trunk allowed vlan によって設定します。

VLAN の追加と削除は，コンフィグレーションコマンド switchport trunk vlan add および switchport trunk vlan remove によって行います。すでにコンフィグレーションコマンド switchport trunk allowed vlan を設定した状態でもう一度コンフィグレーションコマンド switchport trunk allowed vlan を実行すると，指定した VLAN ID リストに置き換わります。

[コマンドによる設定]

1. **(config)# vlan 10-20,100,200-300**
   (config-vlan)# exit
   (config)# interface fastethernet 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，「18.4.3　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。

18.3 ポート VLAN の解説

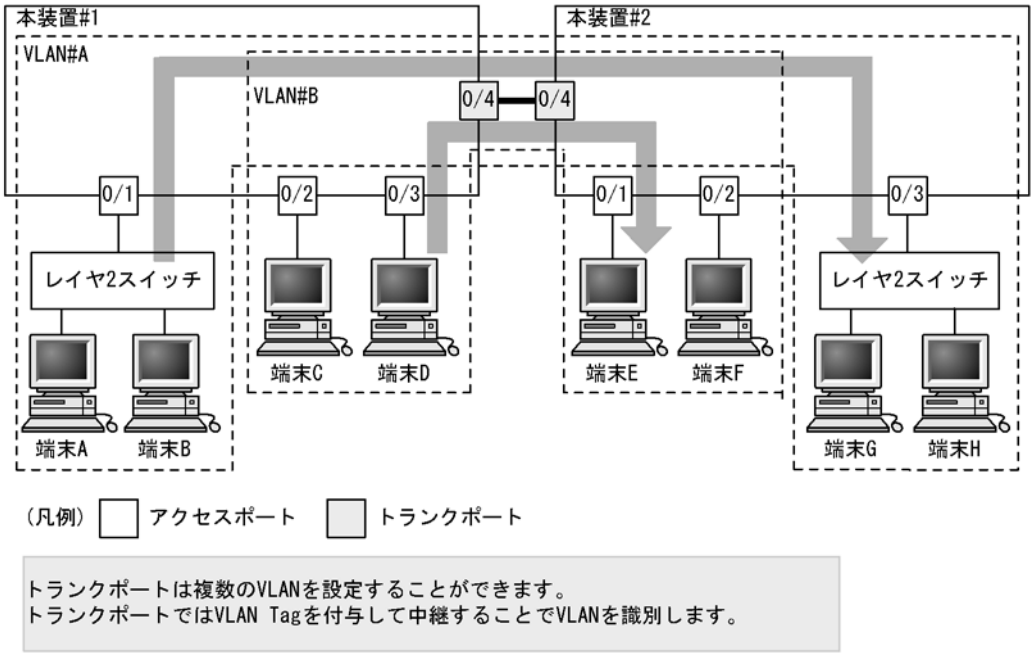
ポート単位に VLAN のグループ分けを行います。

18.3.1 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。2 台の本装置の間はトランクポート (ポート 0/4) で接続します。そのとき，VLAN Tag を使います。

図 18-4 ポート VLAN の構成例



18.3.2 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 18-4　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。

18.3.3 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。

18.4 ポート VLAN 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

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 18-7 コンフィグレーションコマンド一覧

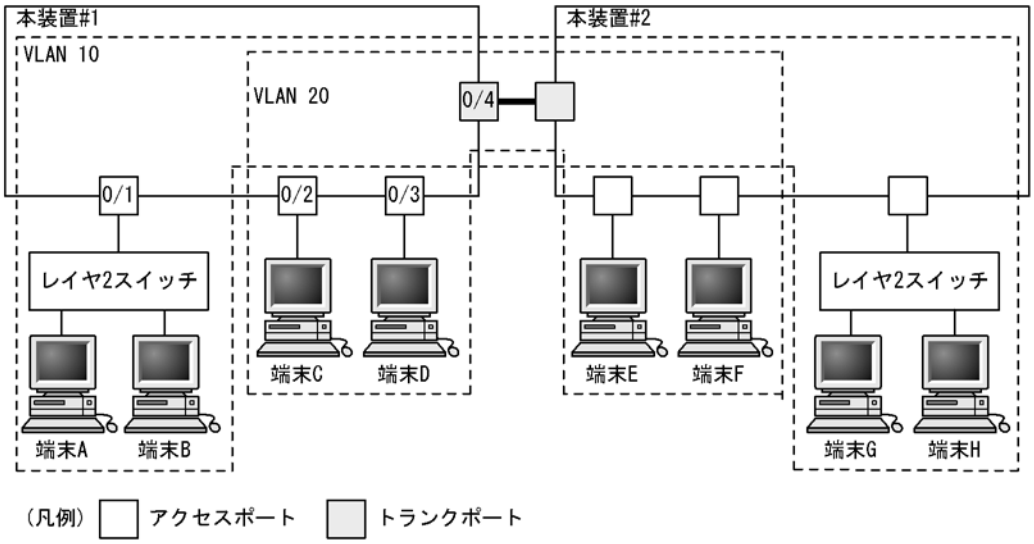
コマンド名	説明
switchport access	アクセスポートの VLAN を設定します。
switchport mode	ポートの種類（アクセス，トランク）を設定します。
switchport trunk	トランクポートの VLAN を設定します。
vlan	ポート VLAN を作成します。また，VLAN コンフィグレーションモードで VLAN に関する項目を設定します。

18.4.2 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 18-5 ポート VLAN の設定例



（1）ポート VLAN の作成

[設定のポイント]

ポート VLAN を作成します。VLAN を作成する際に VLAN ID だけを指定して VLAN の種類を指定しないで作成するとポート VLAN となります。

[コマンドによる設定]

1. **(config)# vlan 10,20**
   (config-vlan)# exit

VLAN ID 10，VLAN ID 20 をポート VLAN として作成します。

(2) アクセスポートの設定

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

[設定のポイント]

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

[コマンドによる設定]

1. **(config)# interface fastethernet 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 fastethernet 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 fastethernet 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。

18.4.3 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 をコンフィグレーションコマンド switchport trunk allowed vlan で指定すると，トランクポートで Untagged フレームを扱う VLAN となります。ネイティブ VLAN は，コンフィグレーションで明示して指定しない場合は VLAN 1（デフォルト VLAN）です。

トランクポート上で，デフォルト VLAN で Tagged フレーム（VLAN ID 1 の VLAN Tag）を扱いたい場合は，ネイティブ VLAN をほかの VLAN に変更してください。

[コマンドによる設定]

1. **(config)# vlan 10,20**
   (config-vlan)# exit
   VLAN ID 10，VLAN ID 20 をポート VLAN として作成します。

2. **(config)# interface fastethernet 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 allowed vlan 1,10,20**
   (config-if)# switchport trunk native vlan 10
   (config-if)# exit
   トランクポート 0/1 に allowed vlan に VLAN1，10，20 を設定します。また，ネイティブ VLAN に VLAN 10 を設定します。VLAN 1（デフォルト VLAN），VLAN 20 は Tagged フレームを扱い，ネイティブ VLAN である VLAN10 は Untagged フレームを扱います。

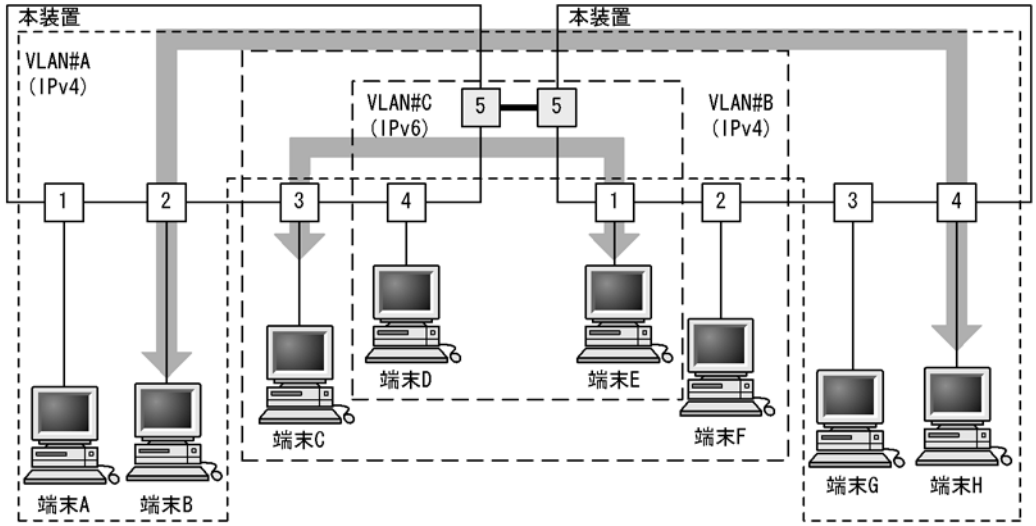
18.5 プロトコル VLAN の解説

18.5.1 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 18-6 プロトコル VLAN の構成例



18.5.2 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 18-8 プロトコルを識別する値

識別する値	概要
EtherType 値	EthernetV2 形式フレームの EtherType 値によってプロトコルを識別します。
LLC 値	802.3 形式フレームの LLC 値 (DSAP,SSAP) によってプロトコルを識別します。
SNAP EtherType 値	802.3 形式フレームの EtherType 値によってプロトコルを識別します。フレームの LLC 値が AA AA 03 であるフレームだけが対象となります。

プロトコルは，コンフィグレーションによってプロトコルを作成し VLAN に対応付けます。一つのプロトコル VLAN に複数のプロトコルを対応付けることもできます。

18.5.3 プロトコルポートとトランクポート

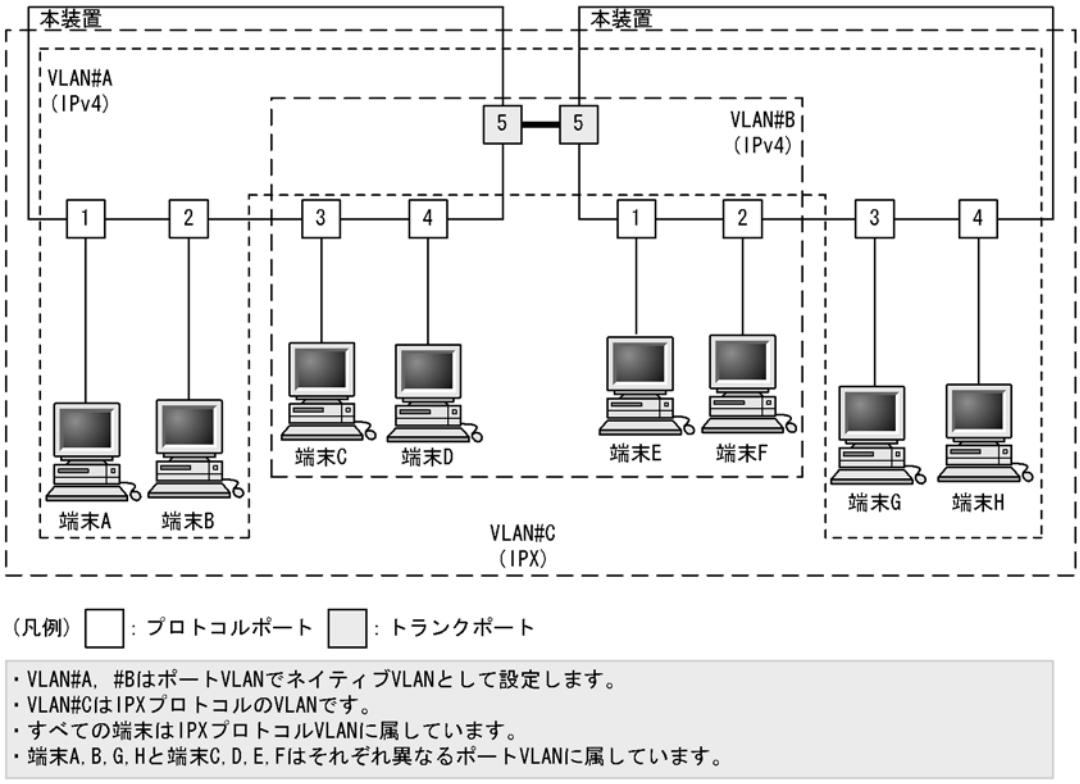
プロトコルポートは Untagged フレームのプロトコルを識別します。プロトコル VLAN として使用するポートはプロトコルポートを設定します。プロトコルポートには複数のプロトコルで異なる VLAN を割り当てることもできます。複数のプロトコル VLAN をほかの LAN スイッチなどに接続するためにはトランクポートを使用します。なお，トランクポートは VLAN Tag によって VLAN を識別するため，プロトコルによる識別は行いません。

18.5.4 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 18-7 プロトコルポートでネイティブ VLAN を使用する構成例



18.6 プロトコル VLAN のコンフィグレーション

18.6.1 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 18-9 コンフィグレーションコマンド一覧

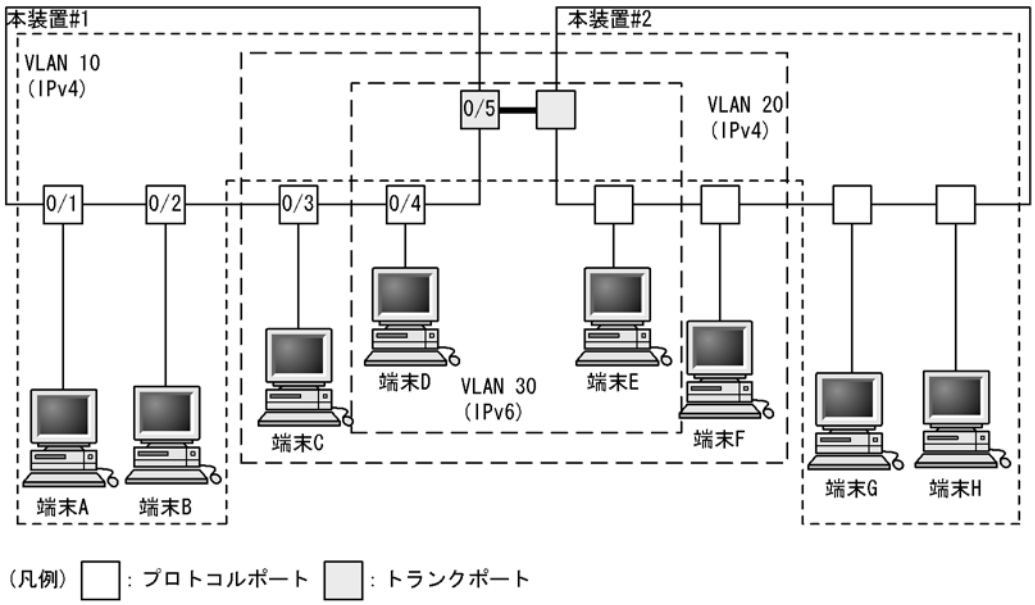
コマンド名	説明
protocol	プロトコル VLAN で VLAN を識別するプロトコルを設定します。
switchport mode	ポートの種類（プロトコル，トランク）を設定します。
switchport protocol	プロトコルポートの VLAN を設定します。
switchport trunk	トランクポートの VLAN を設定します。
vlan-protocol	プロトコル VLAN 用のプロトコル名称とプロトコル値を設定します。
vlan protocol-based	プロトコル VLAN を作成します。また，VLAN コンフィグレーションモードで VLAN に関する項目を設定します。

18.6.2 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 0/1，0/2 は IPv4 プロトコル VLAN 10 を設定します。ポート 0/3，0/4 は IPv4 プロトコル VLAN 20 を設定します。ポート 0/4 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 0/5 はトランクポートであり，すべての VLAN を設定します。

図 18-8 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コンフィグレーションコマンド vlan-protocol で設定します。プロトコルは，プロトコル名称とプロトコル値を設定します。一つの名称に複数のプロトコル値を関連づけることもできます。

IPv4 プロトコルは，IPv4 の EtherType 値と同時に ARP の EtherType 値も指定する必要があるため，IPv4 には二つのプロトコル値を関連づけます。

[コマンドによる設定]

1. **(config)# vlan-protocol IPV4 ethertype 0800,0806**

   名称 IPV4 のプロトコルを作成します。プロトコル値として，IPv4 の EtherType 値 0800 と ARP の EtherType 値 0806 を関連づけます。

   なお，この設定でのプロトコル判定は EthernetV2 形式のフレームだけとなります。

2. **(config)# vlan-protocol IPV6 ethertype 86dd**

   名称 IPV6 のプロトコルを作成します。プロトコル値として IPv6 の EtherType 値 86DD を関連づけます。

[注意事項]

EtherType 値は，05FF 以下の値の場合，0000 で動作します。

(2) プロトコル VLAN の作成

[設定のポイント]

プロトコル VLAN を作成します。VLAN を作成する際に VLAN ID と protocol-based パラメータを指定します。また，VLAN を識別するプロトコルとして，作成したプロトコルを指定します。

[コマンドによる設定]

1. **(config)# vlan 10,20 protocol-based**

   VLAN 10，20 をプロトコル VLAN として作成します。VLAN 10，20 は同じ IPv4 プロトコル VLAN とするため一括して設定します。本コマンドで VLAN コンフィグレーションモードに移行します。

2. **(config-vlan)# protocol IPV4**
   (config-vlan)# exit

   VLAN 10，20 を識別するプロトコルとして，作成した IPv4 プロトコルを設定します。

3. **(config)# vlan 30 protocol-based**
   (config-vlan)# protocol IPV6
   (config-vlan)# exit

   VLAN 30 をプロトコル VLAN として作成します。また，VLAN 30 を識別するプロトコルとして，作成した IPv6 プロトコルを設定します。

(3) プロトコルポートの設定

[設定のポイント]

プロトコル VLAN でプロトコルによって VLAN を識別するポートは，プロトコルポートを設定します。このポートでは Untagged フレームを扱います。

[コマンドによる設定]

1. **(config)# interface range fastethernet 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 は同じコンフィグレーションとなるため一括して指定します。

2. **(config-if-range)# switchport mode protocol-vlan**
   (config-if-range)# switchport protocol vlan 10
   (config-if-range)# exit
   ポート 0/1，0/2 をプロトコルポートに設定します。また，VLAN 10 を設定します。

3. **(config)# interface range fastethernet 0/3-4**
   (config-if-range)# switchport mode protocol-vlan
   (config-if-range)# switchport protocol vlan 20
   (config-if-range)# exit
   ポート 0/3，0/4 をプロトコルポートに設定します。また，VLAN 20 を設定します。

4. **(config)# interface fastethernet 0/4**
   (config-if)# switchport protocol vlan add 30
   (config-if)# exit
   ポート 0/4 に VLAN 30 を追加します。ポート 0/4 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]

コンフィグレーションコマンド switchport protocol vlan は，それ以前のコンフィグレーションに追加するコマンドではなく指定した <VLAN ID list> に設定を置き換えます。すでにプロトコル VLAN を運用中のポートで VLAN の追加や削除を行う場合は，コンフィグレーションコマンド switchport protocol vlan add および switchport protocol vlan remove 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 fastethernet 0/5**
   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。

18.6.3 プロトコルポートのネイティブ VLAN の設定

[設定のポイント]

プロトコルポートで設定したプロトコルに一致しない Untagged フレームを扱いたい場合，そのフレームを扱う VLAN としてネイティブ VLAN を設定します。ネイティブ VLAN はポート VLAN だけが設定できます。

ネイティブ VLAN の VLAN ID をコンフィグレーションコマンド switchport protocol native vlan で設定すると，プロトコルポート上で設定したプロトコルに一致しない Untagged フレームを扱う VLAN となります。ネイティブ VLAN は，コンフィグレーションで明示して設定しない場合は VLAN 1（デフォルト VLAN）です。

ネイティブ VLAN に status suspend が設定されている場合は，設定したプロトコルと一致しないフレームが中継されません。

[コマンドによる設定]

1. **(config)# vlan 10,20 protocol-based**
   (config-vlan)# exit
   (config)# vlan 30
   (config-vlan)# exit
   VLAN 10，20 をプロトコル VLAN として作成します。また，VLAN 30 をポート VLAN として作成します。

2. **(config)# interface fastethernet 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。

18.7 MAC VLAN の解説

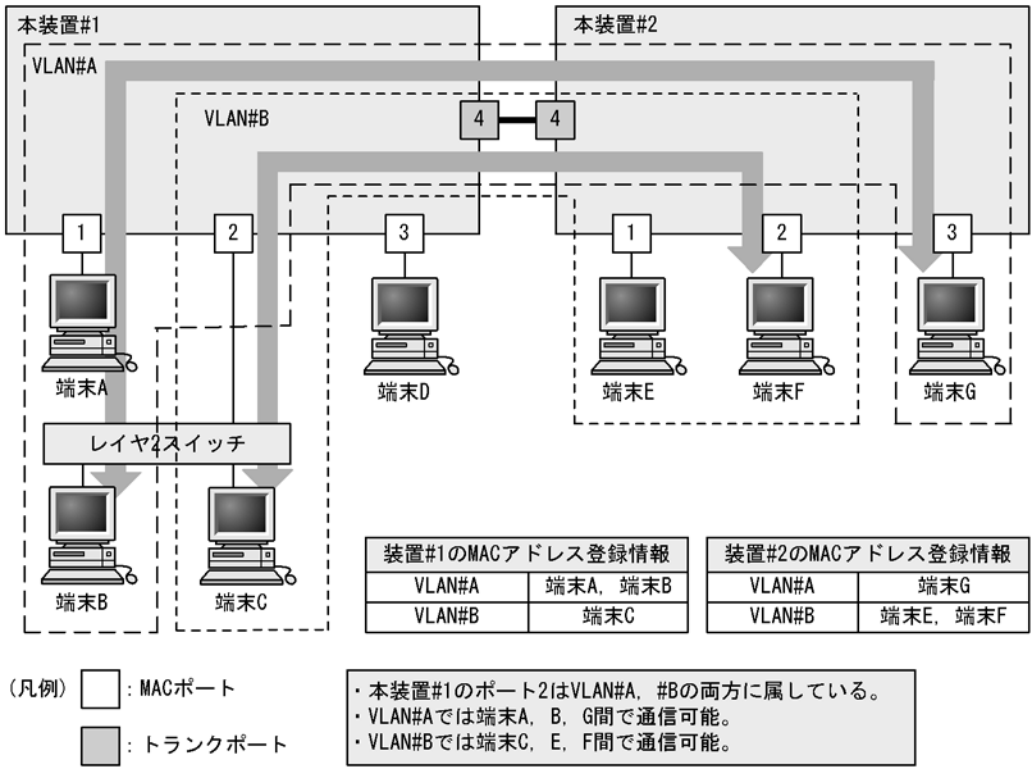
18.7.1 概要

送信元の MAC アドレス単位に VLAN のグループ分けを行います。VLAN への MAC アドレスの登録は，コンフィグレーションによる登録と，レイヤ 2 認証機能による動的な登録ができます。

MAC VLAN は，許可した端末の MAC アドレスをコンフィグレーションで登録するか，レイヤ 2 認証機能で認証された MAC アドレスを登録することによって，接続を許可された端末とだけ通信できるように設定できます。

MAC VLAN の構成例を次の図に示します。VLAN を構成する装置間にトランクポートを設定している場合は，送信元 MAC アドレスに関係なく VLAN Tag によって VLAN を決定します。そのため，すべての装置に同じ MAC アドレスの設定をする必要はありません。装置ごとに MAC ポートに接続した端末の MAC アドレスを設定します。

図 18-9 MAC VLAN の構成例



18.7.2 装置間の接続と MAC アドレス設定

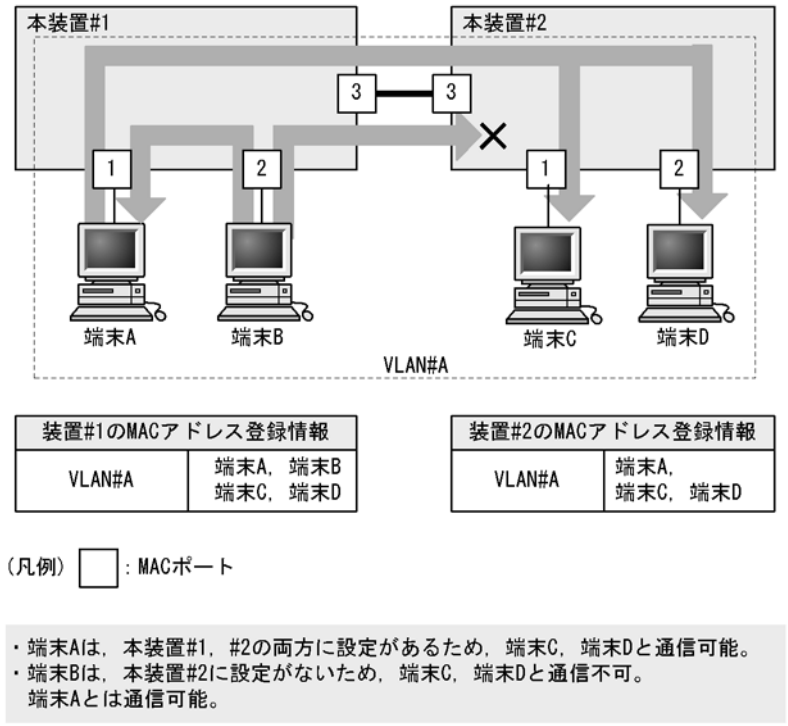
複数の装置で MAC VLAN を構成する場合，装置間の接続はトランクポートをお勧めします。トランクポートで受信したフレームの VLAN 判定は VLAN Tag で行います。そのため，送信元 MAC アドレスが VLAN に設定されていなくても，MAC VLAN で通信できます。トランクポートで装置間を接続した場合については，「図 18-9 MAC VLAN の構成例」を参照してください。

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 18-10　装置間を MAC ポートで接続した場合



18.7.3　レイヤ 2 認証機能との連携について

（1）MAC VLAN に MAC アドレスを動的登録

MAC VLAN は，レイヤ 2 認証機能と連携して，VLAN への MAC アドレスを動的に登録できます。連携するレイヤ 2 認証機能を次に示します。

- IEEE802.1X：ポート単位認証（動的），VLAN 単位認証（動的）
- Web 認証：ダイナミック VLAN モード，レガシーモード
- MAC 認証：ダイナミック VLAN モード，レガシーモード

コンフィグレーションとレイヤ 2 認証機能で同じ MAC アドレスを設定した場合，コンフィグレーションの MAC アドレスを MAC VLAN に登録します。

プリンタやサーバなどの Untagged フレームの装置を，レイヤ 2 認証させずに MAC ポートで意図した VLAN に収容したい場合は，コンフィグレーションコマンド mac-address で対象装置の MAC アドレスを MAC VLAN に登録します。

IEEE802.1X ポート単位認証（動的），Web 認証 /MAC 認証のダイナミック VLAN モードの場合は，コンフィグレーションコマンド mac-address-table static で MAC アドレステーブルにも対象装置の MAC アドレスを登録してください。

また，MAC ポートではコンフィグレーションコマンド switchport mac dot1q vlan を指定した VLAN で，Tagged フレームを中継することが可能です。この機能とレイヤ 2 認証機能については後述の「18.7.4

MAC ポートのオプション機能」を参照してください。

レイヤ 2 認証機能については,「コンフィグレーションガイド Vol.2　5　レイヤ 2 認証機能の概説」および各認証機能の解説編を参照してください。

(2) MAC ポートに対する自動 VLAN 割当

MAC ポートに VLAN を設定するときは，コンフィグレーションコマンド switchport mac vlan で設定，またはレイヤ 2 認証機能による自動割当が可能です。

自動 VLAN 割当が動作するレイヤ 2 認証機能を次に示します。

- IEEE802.1X：ポート単位認証（動的）
- Web 認証：ダイナミック VLAN モード
- MAC 認証：ダイナミック VLAN モード

コンフィグレーションコマンド switchport mac vlan で，自動で割り当てた VLAN と同じ VLAN をポートに設定したときは，自動で割り当てた VLAN は解除します。ただし，認証済みの端末は設定したコンフィグレーションに従いますので，認証は解除しません。

レイヤ 2 認証機能の自動 VLAN 割当については,「コンフィグレーションガイド Vol.2　5.4　レイヤ 2 認証の共通機能」を参照してください。

18.7.4 MAC ポートのオプション機能

MAC ポートのオプション機能として，MAC ポートで任意の VLAN ID の Tagged フレームを中継させることができます。

本オプションは，コンフィグレーションコマンド switchport mac dot1q vlan を設定します。コンフィグレーションコマンド switchport mac dot1q vlan で指定できる VLAN は，ポート VLAN または MAC VLAN です。

本オプションの VLAN に収容する Tagged フレームの装置は，フレーム内の VLAN Tag によって収容されるため，コンフィグレーションで MAC アドレスを登録する必要はありません。

(1) 受信フレームの動作

コンフィグレーションコマンド switchport mac dot1q vlan で設定した VLAN ID を持つ Tagged フレームは，当該 VLAN に中継されます。なお，本コマンドを設定した場合,「表 18-11　コンフィグレーションコマンドと VLAN 種別」で設定した VLAN ID を持つ Tagged フレームを中継します。

(2) 送信フレームの動作

コンフィグレーションコマンド switchport mac dot1q vlan で設定した VLAN の Tagged フレームの中継先により Tag の有無が異なります。

表 18-10　中継先と Tagged フレームの処理

中継先	Tagged フレームの処理
アクセスポート	Tag を外して Untagged フレームを送信
トランクポートのネイティブ VLAN	Tag を外して Untagged フレームを送信
トランクポートのネイティブ VLAN 以外	Tagged フレームを送信

中継先	Tagged フレームの処理
プロトコルポートのネイティブ VLAN	Tag を外して Untagged フレームを送信
MAC ポートの MAC VLAN	Tag を外して Untagged フレームを送信
MAC ポートの dot1q vlan で指定した VLAN	Tagged フレームを送信

(3) オプション機能使用時の注意事項

(a) VLAN の排他について

下記のコンフィグレーションコマンドで指定する VLAN は，すべて排他設定となります。いずれかに設定した VLAN ID を，その他のコマンドで設定することはできません。

表 18-11 コンフィグレーションコマンドと VLAN 種別

コンフィグレーションコマンド	指定可能な VLAN 種別
switchport mac dot1q vlan	ポート VLAN，MAC VLAN
switchport mac vlan	MAC VLAN
switchport mac native vlan	ポート VLAN

(b) コンフィグレーションコマンド switchport mac dot1q vlan について

本コマンドは，コンフィグレーションコマンド switchport mode mac-vlan 設定時に有効となります。

(c) レイヤ２認証機能との併用について

MAC ポートでコンフィグレーションコマンド switchport mac dot1q vlan を設定した場合，当該 VLAN での Untagged フレームおよび Tagged フレームとレイヤ２認証は下記の動作となります。

- Untagged フレームとレイヤ２認証
  「18.7.3　レイヤ 2 認証機能との連携について」と同様に使用可能です。
- Tagged フレームとレイヤ２認証
  当該 VLAN を収容したインタフェースポートに，Web 認証 /MAC 認証の固定 VLAN モードが設定されている場合，「表 18-11　コンフィグレーションコマンドと VLAN 種別」で設定した VLAN ID を持つ Tagged フレームは固定 VLAN モードの認証対象となります。
  固定 VLAN モードで認証させない場合は，コンフィグレーションコマンド mac-address-table static で対象 MAC アドレスと VLAN ID※を登録します。
  注※ : コンフィグレーションコマンド switchport mac dot1q vlan で設定した VLAN ID を指定してください。

18.8 MAC VLAN のコンフィグレーション

18.8.1 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 18-12 コンフィグレーションコマンド一覧

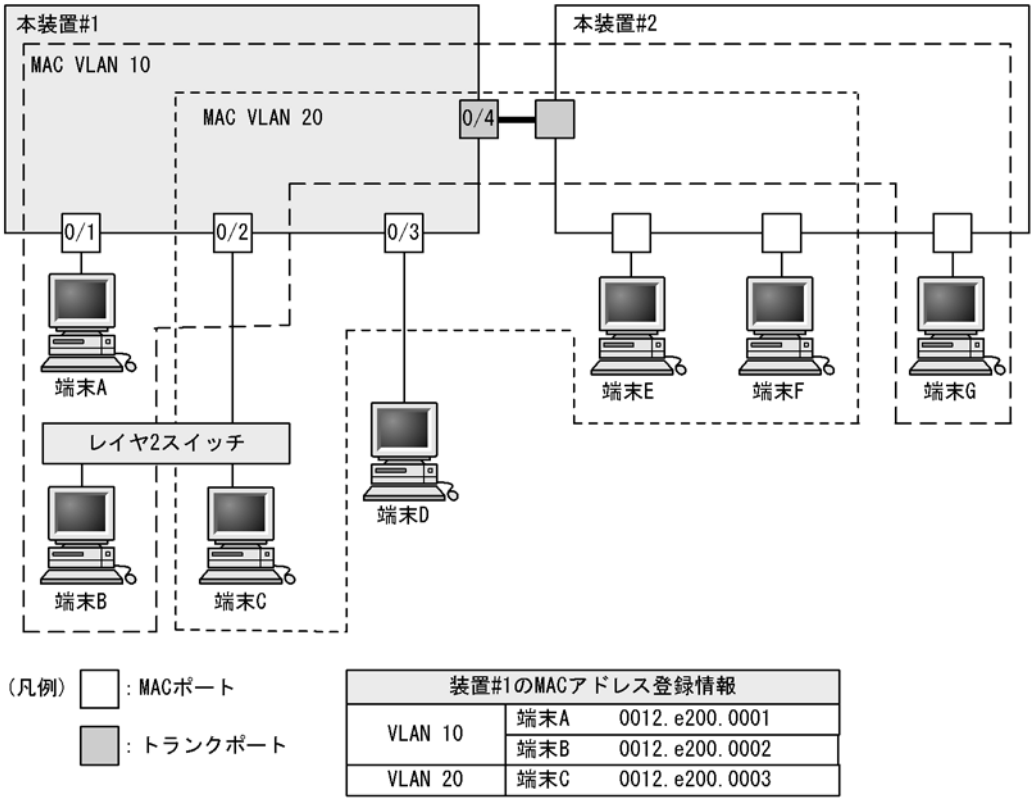
コマンド名	説明
mac-address	MAC VLAN で VLAN に所属する端末の MAC アドレスをコンフィグレーションによって設定します。
switchport mac-vlan	MAC ポートの VLAN を設定します。
switchport mode	ポートの種類（MAC，トランク）を設定します。
switchport trunk	トランクポートの VLAN を設定します。
vlan mac-based	MAC VLAN を作成します。また，VLAN コンフィグレーションモードで VLAN に関する項目を設定します。

18.8.2 MAC VLAN の設定

MAC VLAN を設定する手順を以下に示します。ここでは，MAC VLAN と VLAN に所属する MAC アドレスをコンフィグレーションで設定する場合の例を示します。レイヤ 2 認証機能との連携については，マニュアル「コンフィグレーションガイド Vol.2」の各認証機能の「設定と運用」を参照してください。

次の図に示す本装置 #1 の設定例を示します。ポート 0/1 は MAC VLAN 10 を設定します。ポート 0/2 は MAC VLAN 10 および 20，0/3 は MAC VLAN 20 を設定します。ただし，ポート 0/3 には MAC アドレスを登録していない端末 D を接続しています。

図 18-11　MAC VLAN **の設定例**



（1） MAC VLAN **の作成と** MAC **アドレスの登録**

[設定のポイント]

MAC VLAN を作成します。VLAN を作成する際に VLAN ID と mac-based パラメータを指定します。

また，VLAN に所属する MAC アドレスを設定します。構成例の端末 A ～ C をそれぞれの VLAN に登録します。端末 D は MAC VLAN での通信を許可しないので登録しません。

[コマンドによる設定]

1. **(config)# vlan 10 mac-based**

   VLAN 10 を MAC VLAN として作成します。本コマンドで VLAN コンフィグレーションモードに移行します。

2. **(config-vlan)# mac-address 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 fastethernet 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 fastethernet 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，コンフィグレーションコマンド switchport mac vlan add 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。

[注意事項]

コンフィグレーションコマンド switchport mac vlan は，それ以前のコンフィグレーションに追加するコマンドではなく指定した <VLAN ID list> に設定を置き換えます。すでに MAC VLAN を運用中のポートで VLAN の追加や削除を行う場合は，コンフィグレーションコマンド switchport mac vlan add および switchport mac vlan remove を使用してください。

(3) トランクポートの設定

[設定のポイント]

MAC VLAN においても，Tagged フレームを扱うポートはトランクポートとして設定し，そのトランクポートに VLAN を設定します。

[コマンドによる設定]

1. **(config)# interface fastethernet 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。

18.8.3 MAC ポートのネイティブ VLAN の設定

[設定のポイント]

MAC ポートで MAC VLAN に登録した MAC アドレスに一致しない Untagged フレームを扱いたい場合，そのフレームを扱う VLAN としてネイティブ VLAN を設定します。ネイティブ VLAN はポート VLAN だけが設定できます。

ネイティブ VLAN の VLAN ID をコンフィグレーションコマンド switchport mac native vlan で指定すると，MAC ポート上で登録した MAC アドレスに一致しない Untagged フレームを扱う VLAN となります。ネイティブ VLAN は，コンフィグレーションで明示して指定しない場合は VLAN 1（デフォルト VLAN）です。

ネイティブ VLAN に status suspend が設定されていた場合は，登録した MAC アドレスに一致しないフレームが中継されません。

[コマンドによる設定]

1. **(config)# vlan 10,20 mac-based**
   (config-vlan)# exit
   (config)# vlan 30
   (config-vlan)# exit
   VLAN 10,20 を MAC VLAN として作成します。また，VLAN 30 をポート VLAN として作成します。

2. **(config)# interface fastethernet 0/1**
   (config-if)# switchport mode mac-vlan
   ポート 0/1 のイーサネットインタフェースコンフィグレーションモードに移行します。また，MAC ポートとして設定します。

3. **(config-if)# switchport mac vlan 10,20**
   ポート 0/1 に MAC VLAN 10，20 を設定します。
   この状態で，ポート 0/1 は MAC VLAN 10，20 だけ通信を許可するポートとなります。登録されていない MAC アドレスは通信することはできません。登録されていない MAC アドレスから通信するためには，ネイティブ VLAN が通信可能となるように設定します。

4. **(config-if)# switchport mac native vlan 30**
   (config-if)# exit
   ポート 0/1 にポート VLAN30 をネイティブ VLAN として設定します。VLAN 30 はポート 0/1 で登録されていない MAC アドレスからの Untagged フレームを扱う VLAN となります。

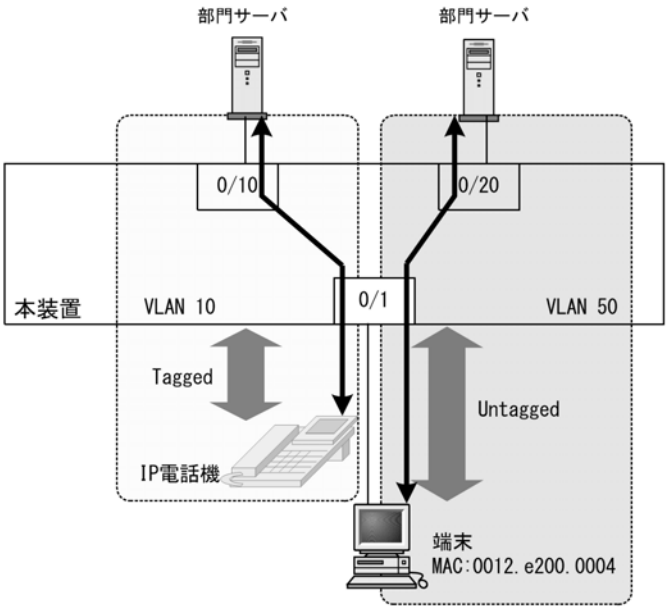
18.8.4 MAC ポートでの Tagged フレーム中継の設定

下記構成図のように，同一ポートで IP 電話機からは Tagged フレーム，IP 電話機配下の端末からは Untagged フレームを受信して通信する場合は，MAC ポートのオプション機能を使用します。

オプション機能は，コンフィグレーションコマンド switchport mac dot1q vlan で，Tagged フレーム中継用の VLAN ID を指定することにより，同一 MAC ポートで Tagged フレーム／ Untagged フレームの中継が可能となります。

IP 電話機および端末をレイヤ 2 認証機能で認証する設定については，マニュアル「コンフィグレーションガイド Vol.2」を参照してください。

図 18-12　MAC ポートでの Tagged フレーム中継の設定例



[設定のポイント]

MAC ポートを設定し，同一 MAC ポートで Tagged フレームと Untagged フレームを扱うポートとして設定します。また，MAC VLAN には端末の MAC アドレスを設定します。

- VLAN 10：ポート VLAN で Tagged フレームを扱います。
- VLAN 50：MAC VLAN で Untagged フレームを扱います。

[コマンドによる設定]

1. **(config)# vlan 10**
   (config-vlan)# exit
   VLAN 10 をポート VLAN として作成します。

2. **(config)# vlan 50 mac-based**
   (config-vlan)# mac-address 0012.e200.0004
   (config-vlan)# exit
   VLAN 50 を MAC VLAN として作成し，VLAN 50 に所属する端末の MAC アドレス（0012.e200.0004）を設定します。

3. **(config)# interface fastethernet 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。

4. **(config-if)# switchport mode mac-vlan**
   ポート 0/1 を MAC ポートとして設定します。

5. **(config-if)# switchport mac dot1q vlan 10**
   MAC ポートで Tagged フレームを扱う VLAN として，VLAN 10 を設定します。

6. **(config-if)# switchport mac vlan 50**
   (config-if)# exit

MAC ポートで Untagged フレームを扱う VLAN として，VLAN50 を設定します。

[注意事項]

1. コンフィグレーションコマンド switchport mac dot1q vlan の設定については，下記にご注意ください。
   - 指定可能な VLAN はポート VLAN または MAC VLAN です。コンフィグレーションコマンド switchport mac vlan および switchport mac native vlan で指定した VLAN は指定できません。
   - 本設定は，switchport mode mac-vlan 設定時に有効となります。
2. Tagged フレーム中継を設定したポートには，BPDU を送信する装置を接続しないでください。（接続する場合は，スパニングツリーを Disable に設定してください。）

18.9 VLAN のオペレーション

18.9.1 運用コマンド一覧

VLAN の運用コマンド一覧を次の表に示します。

表 18-13 運用コマンド一覧

コマンド名	説明
show vlan	VLAN の各種情報を表示します。
show vlan mac-vlan	MAC VLAN に登録されている MAC アドレスを表示します。

18.9.2 VLAN の状態の確認

(1) VLAN の設定状態の確認

VLAN の情報は運用コマンド show vlan で確認できます。VLAN ID，Type，IP Address などによって VLAN に関する設定が正しいことを確認してください。また，Untagged はその VLAN で Untagged フレームを扱うポート，Tagged はその VLAN で Tagged フレームを扱うポートになります。VLAN に設定されているポートの設定が正しいことを確認してください。

図 18-13 show vlan の実行結果

```
> show vlan

Date 20XX/10/28 16:32:45 UTC
VLAN counts: 5
VLAN ID: 7     Type: Port based  Status: Up
  Learning: On
  BPDU Forwarding:        EAPOL Forwarding:
  Router Interface Name: VLAN0007
  IP Address:
  Source MAC address: 0012.e294.aadc(System)
  Description: VLAN0007
  Spanning Tree: None(-)
  AXRP RING ID:200    AXRP VLAN group:1
  IGMP snooping:      MLD snooping:
  Untagged(0)    :
  Tagged(10)     : 0/1,0/17-25
VLAN ID: 10    Type: Port based  Status: Up
  Learning: On
  BPDU Forwarding:        EAPOL Forwarding:
  Router Interface Name: VLAN0010
  IP Address:
  Source MAC address: 0012.e294.aadc(System)
  Description: VLAN0010
  Spanning Tree: None(-)
  AXRP RING ID:200    AXRP VLAN group:Control-VLAN
  IGMP snooping:      MLD snooping:
  Untagged(0)    :
  Tagged(9)      : 0/17-25
VLAN ID: 30    Type: Protocol based  Status: Down
  Protocol VLAN Information  Name: "IPV4"
  EtherType: 0800,0806 LLC:  Snap-EtherType:
  Learning: On
  BPDU Forwarding:        EAPOL Forwarding:
  Router Interface Name: VLAN0030
  IP Address:
  Source MAC address: 0012.e294.aadc(System)
  Description: PROT-VLAN0030
  Spanning Tree: None(-)
  AXRP RING ID:       AXRP VLAN group:
```

```
  IGMP snooping:      MLD snooping:
  Untagged(0)    :
  Tagged(0)      :
VLAN ID: 51    Type: MAC based  Status: Up
  Learning: On
  BPDU Forwarding:        EAPOL Forwarding:
  Router Interface Name: VLAN0051
  IP Address:
  Source MAC address: 0012.e294.aadc(System)
  Description: VLAN0051
  Spanning Tree: None(-)
  AXRP RING ID:       AXRP VLAN group:
  IGMP snooping:      MLD snooping:
  Untagged(1)    : 0/11
  Tagged(0)      :
VLAN ID: 4094  Type: Port based  Status: Up
  Learning: On
  BPDU Forwarding:        EAPOL Forwarding:
  Router Interface Name: VLAN4094
  IP Address: 192.168.0.150/24
  Source MAC address: 0012.e294.aadc(System)
  Description: VLAN4094
  Spanning Tree: None(-)
  AXRP RING ID:200    AXRP VLAN group:2
  IGMP snooping:      MLD snooping:
  Untagged(1)    : 0/14
  Tagged(10)     : 0/1,0/17-25

>
```

（2）VLAN の通信状態の確認

VLAN の通信状態は運用コマンド show vlan detail で確認できます。Port Information でポートの Up/Down，Forwarding/Blocking を確認してください。Blocking 状態の場合，括弧内に Blocking の要因が示されています。

図 18-14　show vlan detail の実行結果

```
> show vlan 10,4094 detail

Date 20XX/10/28 16:32:49 UTC
VLAN counts: 2
VLAN ID: 10    Type: Port based  Status: Up
  Learning: On
  BPDU Forwarding:        EAPOL Forwarding:
  Router Interface Name: VLAN0010
  IP Address:
  Source MAC address: 0012.e294.aadc(System)
  Description: VLAN0010
  Spanning Tree: None(-)
  AXRP RING ID:200    AXRP VLAN group:Control-VLAN
  IGMP snooping:      MLD snooping:
  Port Information
   0/17(ChGr:8)  Down -               Tagged
   0/18(ChGr:8)  Down -               Tagged
   0/19(ChGr:8)  Down -               Tagged
   0/20(ChGr:8)  Down -               Tagged
   0/21(ChGr:8)  Down -               Tagged
   0/22(ChGr:8)  Down -               Tagged
   0/23(ChGr:8)  Down -               Tagged
   0/24(ChGr:8)  Up   Forwarding      Tagged
   0/25          Up   Forwarding      Tagged
VLAN ID: 4094  Type: Port based  Status: Up
  Learning: On
  BPDU Forwarding:        EAPOL Forwarding:
  Router Interface Name: VLAN4094
  IP Address: 192.168.0.150/24
  Source MAC address: 0012.e294.aadc(System)
  Description: VLAN4094
  Spanning Tree: None(-)
  AXRP RING ID:200    AXRP VLAN group:2
```

```
  IGMP snooping:      MLD snooping:
  Port Information
   0/1           Up   Forwarding      Tagged
   0/14          Down -               Untagged
   0/17(ChGr:8)  Down -               Tagged
   0/18(ChGr:8)  Down -               Tagged
   0/19(ChGr:8)  Down -               Tagged
   0/20(ChGr:8)  Down -               Tagged
   0/21(ChGr:8)  Down -               Tagged
   0/22(ChGr:8)  Down -               Tagged
   0/23(ChGr:8)  Down -               Tagged
   0/24(ChGr:8)  Up   Forwarding      Tagged
   0/25          Up   Forwarding      Tagged

>
```

(3) VLAN ID 一覧の確認

運用コマンド show vlan summary で，設定した VLAN の種類とその数，VLAN ID を確認できます。

図 18-15 show vlan summary の実行結果

```
>show vlan summary

Date 20XX/10/28 16:32:16 UTC
Total(5)            : 7,10,30,51,4094
Port based(3)       : 7,10,4094
Protocol based(1)   : 30
MAC based(1)        : 51

>
```

(4) VLAN のリスト表示による確認

運用コマンド show vlan list は VLAN の設定状態の概要を 1 行に表示します。本コマンドによって，VLAN の設定状態やレイヤ 2 冗長機能，IP アドレスの設定状態を一覧で確認できます。また，VLAN，ポートまたはチャネルグループをパラメータとして指定することで，指定したパラメータの VLAN の状態だけを一覧で確認できます。

図 18-16 show vlan list の実行結果

```
> show vlan list

Date 20XX/10/28 16:31:47 UTC
VLAN counts: 5
  ID Status   Fwd/Up /Cfg Name             Type  Protocol       Ext. IP
   7 Up         3/  3/ 10 VLAN0007         Port  AXRP (-)       -    -
  10 Up         2/  2/  9 VLAN0010         Port  AXRP (C)       -    -
  30 Down       0/  0/  0 PROT-VLAN0030    Proto -              -    -
  51 Up         1/  1/  1 VLAN0051         MAC   -              -    -
4094 Up         3/  3/ 11 VLAN4094         Port  AXRP (-)       -    4
     AXRP (C:Control-VLAN)
     S:IGMP/MLD snooping
     4:IPv4 address configured

>
```

(5) MAC VLAN の登録 MAC アドレスの確認

MAC VLAN に登録されている MAC アドレスを，運用コマンド show vlan mac-vlan で確認できます。

括弧内は MAC アドレスを登録した機能を示しています。

- 「static」はコンフィグレーションで登録した MAC アドレス

- 「dot1x」「web-auth」「mac-auth」はレイヤ 2 認証機能で登録した MAC アドレス

図 18-17　show vlan mac-vlan の実行結果

```
> show vlan mac-vlan

Date 20XX/11/17 06:12:04 UTC
VLAN counts: 1    Total MAC Counts: 3
VLAN ID: 100         MAC Counts: 3
   0000.e22b.ffdd(mac-auth)   000b.972f.e22b(mac-auth)
   0050.daba.4fc8(mac-auth)

>
```

19 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。

19.1 L2 プロトコルフレーム透過機能の解説

19.2 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

19.3 ポート間中継遮断機能の解説

19.4 ポート間中継遮断機能のコンフィグレーション

19.5 VLAN 拡張機能のオペレーション

19.1 L2 プロトコルフレーム透過機能の解説

19.1.1 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。

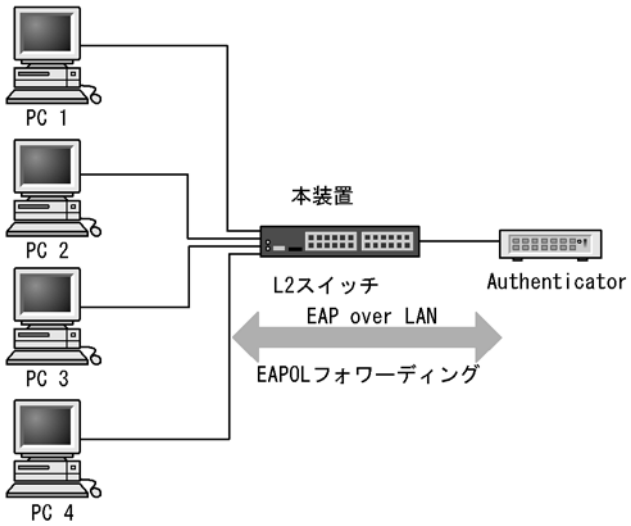
(1) BPDU フォワーディング機能

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。

(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 19-1 EAPOL フォワーディング機能の適用例



19.2 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

19.2.1 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 19-1 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。

19.2.2 L2 プロトコルフレーム透過機能の設定

(1) BPDU フォワーディング機能の設定

[設定のポイント]

本機能の設定は装置単位で有効になります。設定すると，BPDU をすべての VLAN で中継します。BPDU フォワーディング機能は，本装置のスパニングツリーを停止してから設定する必要があります。

[コマンドによる設定]

1. **(config)# spanning-tree disable**
   (config)# l2protocol-tunnel stp
   BPDU フォワーディング機能を設定します。事前にスパニングツリーを停止し，BPDU フォワーディング機能を設定します。本装置は BPDU をプロトコルフレームとして扱わないで中継します。

(2) EAPOL フォワーディング機能の設定

[設定のポイント]

本機能の設定は装置単位で有効になります。設定すると，EAPOL をすべての VLAN で中継します。EAPOL フォワーディング機能と IEEE802.1X 機能は同時に使用することはできません。

[コマンドによる設定]

1. **(config)# l2protocol-tunnel eap**
   EAPOL フォワーディング機能を設定します。本装置は EAPOL をプロトコルフレームとして扱わないで中継します。

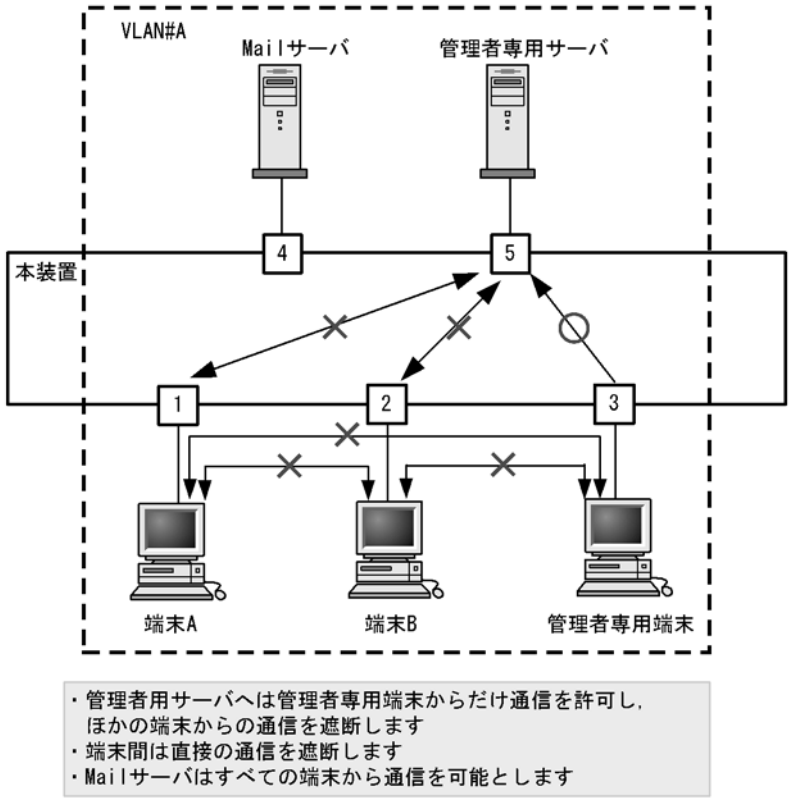
19.3 ポート間中継遮断機能の解説

19.3.1 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 19-2 ポート間中継遮断機能の適用例



19.3.2 ポート間中継遮断機能使用時の注意事項

(1) 遮断するポートについて

ポート間中継遮断機能は，チャネルグループに登録されていないポートで動作します。

(2) 他機能との共存

ポート間中継遮断機能と下記に示す機能を同時に使用したときの動作を，次の表に示します。

表 19-2　ポート間中継遮断機能と他機能の同時使用について

機能	動作
スパニングツリー	通信を遮断したポートでスパニングツリーを運用すると，トポロジーによって通信できなくなる場合があります。
DHCP snooping	通信を遮断したポートで DHCP snooping を運用すると，DHCP フレーム（ダイナミック ARP 検査有効時は ARP フレームも対象）に対してポート間中継遮断機能が無効になり，中継してしまいます。
IGMP snooping	通信を遮断したポートで IGMP snooping を運用すると，IGMP フレームに対してポート間中継遮断機能が無効になり，中継してしまいます。
MLD snooping	通信を遮断したポートで MLD snooping を運用すると，MLD フレームに対してポート間中継遮断機能が無効になり，中継してしまいます。
GSRP aware	通信を遮断したポートで GSRP を運用すると GSRP aware フレームに対してポート間中継遮断機能が無効になり，中継してしまいます。
CFM	通信を遮断したポートで CFM を運用すると，CFM フレームに対してポート間中継遮断機能が無効になり，中継してしまいます。

19.4 ポート間中継遮断機能のコンフィグレーション

19.4.1 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 19-3 コンフィグレーションコマンド一覧

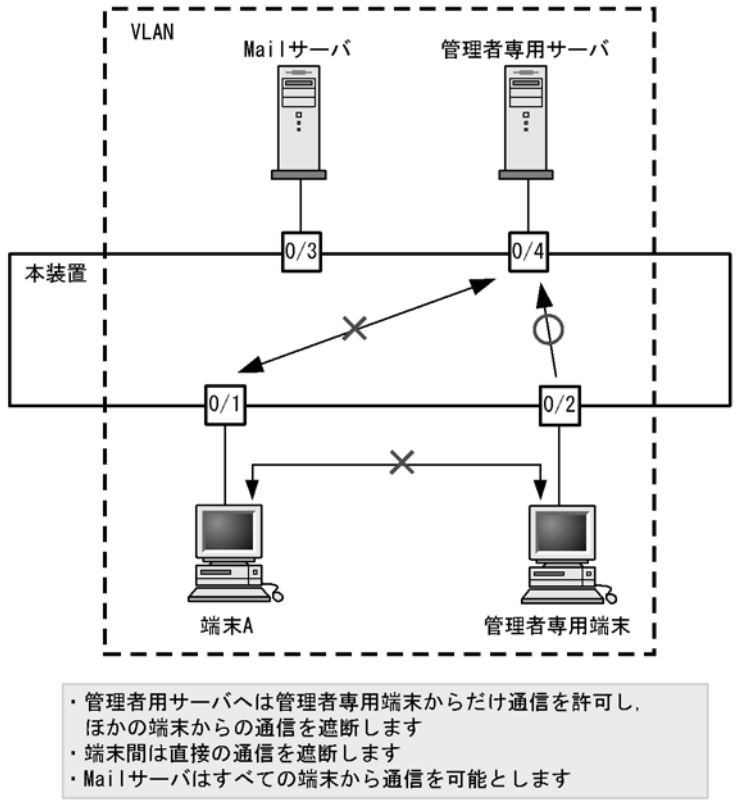
コマンド名	説明
switchport isolation	指定したポートへの中継を遮断します。

19.4.2 ポート間中継遮断機能の設定

ポート間中継遮断機能を設定する手順を次に示します。ここでは，図に示す構成の設定例を示します。

構成例では，ポート 0/1 とポート 0/4 間の通信を遮断します。また，ポート 0/1，0/2 間の通信を遮断します。ポート 0/3 はどのポートとも通信が可能です。

図 19-3 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 fastethernet 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 fastethernet 0/2,0/4**
   (config-if)# exit
   ポート 0/1 でポート 0/2，0/4 からの中継を遮断します。この設定で，ポート 0/1 へ発信する片方向の中継を遮断します。

3. **(config)# interface fastethernet 0/2**
   (config-if)# switchport isolation interface fastethernet 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 fastethernet 0/4**
   (config-if)# switchport isolation interface fastethernet 0/1
   (config-if)# exit
   ポート 0/4 のイーサネットインタフェースコンフィグレーションモードに移行し，ポート 0/4 でポート 0/1 からの中継を遮断します。この設定によって，ポート 0/1，0/4 間は双方向で通信を遮断します。

19.4.3 遮断するポートの変更

[設定のポイント]

コンフィグレーションコマンド switchport isolation add および switchport isolation remove でポート間中継遮断機能で遮断するポートを変更します。すでに設定したポートでコンフィグレーションコマンド switchport isolation interface fastethernet <IF#> または switchport isolation interface gigabitethernet <IF#> 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 fastethernet 0/1**
   (config-if)# switchport isolation interface fastethernet 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 0/2 ～ 0/10 からポート 0/1 への中継を遮断します。

2. **(config-if)# switchport isolation interface add fastethernet 0/11**
   (config-if)# switchport isolation interface remove fastethernet 0/5
   ポート 0/11 を追加します。また，ポート 0/5 の設定を解除します。この状態で，ポート 0/2 ～ 0/4，0/6 ～ 0/11 からポート 0/1 への通信を遮断します。

3. **(config-if)# switchport isolation interface fastethernet 0/3-4**
   (config-if)# exit
   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 からポート 0/1 への中継だけ遮断しそのほかのポートは通信を可能とします。

19.5 VLAN 拡張機能のオペレーション

19.5.1 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 19-4 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。

19.5.2 VLAN 拡張機能の確認

(1) VLAN の通信状態の確認

VLAN 拡張機能の設定状態を運用コマンド show vlan detail で確認できます。運用コマンド show vlan detail による VLAN 拡張機能の確認方法を次の表に示します。

表 19-5 show vlan detail による VLAN 拡張機能の確認方法

機能	確認方法
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 19-4 show vlan detail の実行結果

```
> show vlan 10,4094 detail

Date 20XX/10/28 16:32:49 UTC
VLAN counts: 2
VLAN ID: 10    Type: Port based  Status: Up
  Learning: On
  BPDU Forwarding:         EAPOL Forwarding:
  Router Interface Name: VLAN0010
  IP Address:
  Source MAC address: 0012.e294.aadc(System)
  Description: VLAN0010
  Spanning Tree: None(-)
  AXRP RING ID:200    AXRP VLAN group:Control-VLAN
  IGMP snooping:      MLD snooping:
  Port Information
   0/17(ChGr:8)  Down -               Tagged
   0/18(ChGr:8)  Down -               Tagged
   0/19(ChGr:8)  Down -               Tagged
   0/20(ChGr:8)  Down -               Tagged
   0/21(ChGr:8)  Down -               Tagged
   0/22(ChGr:8)  Down -               Tagged
   0/23(ChGr:8)  Down -               Tagged
   0/24(ChGr:8)  Up   Forwarding      Tagged
   0/25          Up   Forwarding      Tagged
VLAN ID: 4094  Type: Port based  Status: Up
  Learning: On
  BPDU Forwarding:         EAPOL Forwarding:
  Router Interface Name: VLAN4094
  IP Address: 192.168.0.150/24
  Source MAC address: 0012.e294.aadc(System)
  Description: VLAN4094
  Spanning Tree: None(-)
  AXRP RING ID:200    AXRP VLAN group:2
  IGMP snooping:      MLD snooping:
  Port Information
   0/1           Up   Forwarding      Tagged
```

```
   0/14           Down -               Untagged
   0/17(ChGr:8)   Down -               Tagged
   0/18(ChGr:8)   Down -               Tagged
   0/19(ChGr:8)   Down -               Tagged
   0/20(ChGr:8)   Down -               Tagged
   0/21(ChGr:8)   Down -               Tagged
   0/22(ChGr:8)   Down -               Tagged
   0/23(ChGr:8)   Down -               Tagged
   0/24(ChGr:8)   Up   Forwarding      Tagged
   0/25           Up   Forwarding      Tagged

>
```

20 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。

20.1 **スパニングツリーの概説**

20.2 **スパニングツリー動作モードのコンフィグレーション**

20.3 PVST+ **解説**

20.4 PVST+ **のコンフィグレーション**

20.5 PVST+ **のオペレーション**

20.6 **シングルスパニングツリー解説**

20.7 **シングルスパニングツリーのコンフィグレーション**

20.8 **シングルスパニングツリーのオペレーション**

20.9 **マルチプルスパニングツリー解説**

20.10 **マルチプルスパニングツリーのコンフィグレーション**

20.11 **マルチプルスパニングツリーのオペレーション**

20.12 **スパニングツリー共通機能解説**

20.13 **スパニングツリー共通機能のコンフィグレーション**

20.14 **スパニングツリー共通機能のオペレーション**

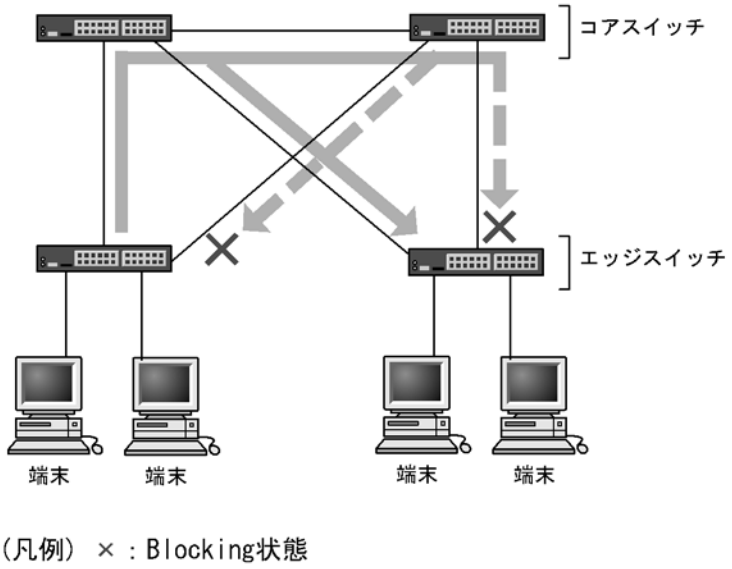
20.1 スパニングツリーの概説

20.1.1 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 20-1 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。

20.1.2 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 20-1 スパニングツリーの種類

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

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

表 20-2 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。

20.1.3 スパニングツリーと高速スパニングツリー

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

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

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

表 20-3 PVST+，STP(シングルスパニングツリー) の状態遷移

状態	状態の概要	次の状態への遷移
Disable	ポートが使用できない状態です。使用可能となるとすぐに Blocking に遷移します。	－
Blocking	通信不可の状態で，MAC アドレス学習も行いません。リンクアップ直後またはトポロジーが安定して Blocking になるポートもこの状態になります。	20 秒 (変更可能) または BPDU を受信
Listening	通信不可の状態で，MAC アドレス学習も行いません。該当ポートが Learning になる前に，トポロジーが安定するまで待つ期間です。	15 秒 (変更可能)
Learning	通信不可の状態です。しかし，MAC アドレス学習は行います。該当ポートが Forwarding になる前に，事前に MAC アドレス学習を行う期間です。	15 秒 (変更可能)
Forwarding	通信可能の状態です。トポロジーが安定した状態です。	－

（凡例）－：該当なし

表 20-4 Rapid PVST+，Rapid STP(シングルスパニングツリー) の状態遷移

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

（凡例）－：該当なし

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

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

- トポロジーの全体を同じプロトコル（Rapid PVST+ または Rapid STP）で構築する（Rapid PVST+ と Rapid STP の相互接続は「20.3.2 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。

20.1.4 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 20-5 ブリッジの役割

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

(2) ポートの役割

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

表 20-6 ポートの役割

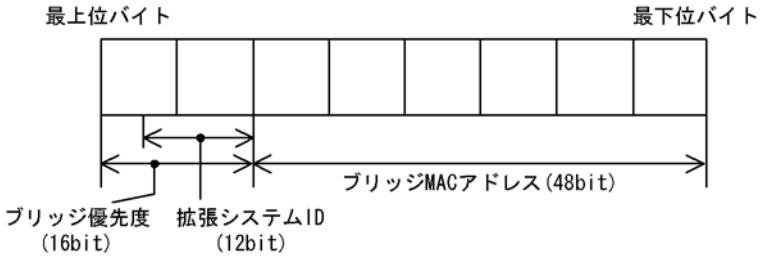
ポートの役割	概要
ルートポート	指定ブリッジからルートブリッジへ向かう通信経路のポートです。通信可能なポートとなります。
指定ポート	ルートポート以外の通信可能なポートです。ルートブリッジからの通信経路でトポロジーの下流へ接続するポートです。
非指定ポート	ルートポート，指定ポート以外のポートで，通信不可の状態のポートです。障害が発生した際に通信可能になり代替経路として使用します。

(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 20-2 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

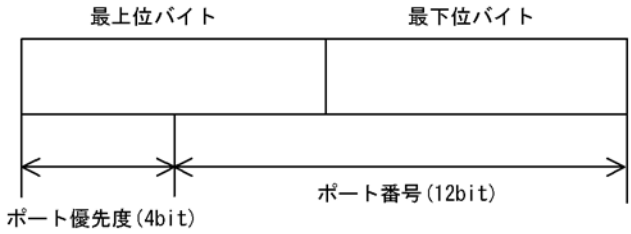
トの速度に応じた値となっていて，コンフィグレーションで変更することもできます。

(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。

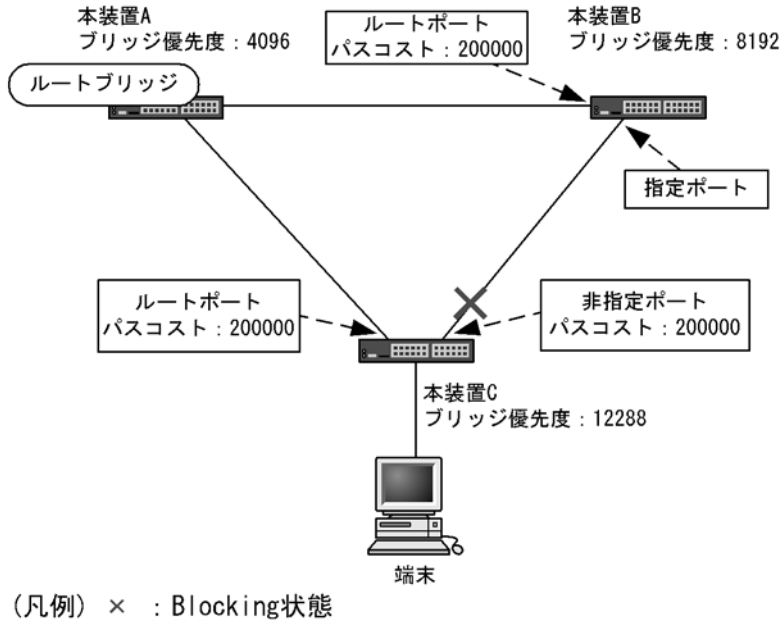
図 20-3 ポート識別子



20.1.5 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 20-4 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，本装置 A がルートブリッジになるように設定します。本装置 B，本装置 C は指定ブリッジとなります。

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

スパニングツリーのトポロジー設計では，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

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

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

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

(b) 指定ポート，非指定ポートの選出

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

指定ポート，非指定ポートは次のように選出します。

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

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

20.1.6 STP 互換モード

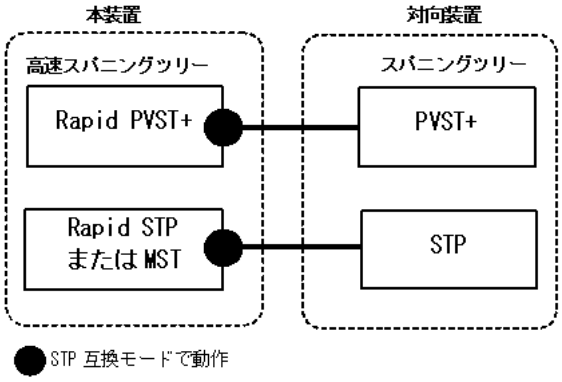
(1) 概要

本装置が高速スパニングツリーで，対向装置がスパニングツリーの場合，本装置の該当するポートは STP 互換モードで動作します。

STP 互換モードで動作中，本装置の該当ポートは対向装置に合わせているため，高速遷移を行いません。

STP 互換モードで動作可能な組み合わせを次の図に示します。

図 20-5 STP 互換モード動作関係図



STP 互換モードで動作していると，該当するポートで高速遷移が行われなくなり，通信復旧に時間が掛かるようになります。

本装置では，高速スパニングツリーへの復旧機能として自動復旧機能と強制復旧機能をサポートしています。

(2) 復旧機能

(a) 自動復旧機能

自動復旧機能は，STP 互換モードで動作中に，対向装置が高速スパニングツリーに変更された場合，STP 互換モードから自動復旧し，再び高速スパニングツリーで動作できるようになります。

- 該当するポートのリンクタイプが point-to-point の場合，STP 互換モード自動復旧機能が動作します。
- 該当するポートが非指定ポート※で STP 互換モードで動作した場合，該当するポートから RST BPDU または MST BPDU を送信することで STP 互換モードを解除します。

  注※
  非指定ポートについては，「20.1.4 スパニングツリートポロジーの構成要素（2）ポートの役割 表 20-6 ポートの役割」を参照してください。
- 該当するポートのリンクタイプが shared の場合，自動復旧モードが正しく動作できないため，自動復旧機能は動作しません。

また，復旧のタイミングによっては，該当するポートと対向装置が STP 互換モードで動作し続ける場合があります。

(b) 強制復旧機能

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

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

20.1.7 スパニングツリー共通の注意事項

（1） CPU の過負荷について

CPU が過負荷な状態になった場合，本装置が送受信する BPDU の廃棄が発生して，タイムアウトのメッセージ出力，トポロジー変更，一時的な通信断となることがあります。

（2） VLAN のダウンを伴うコンフィグレーションコマンドの設定について

コンフィグレーションコマンド no spanning-tree disable 設定により，本装置にスパニングツリー機能を適用させると，全 VLAN が一時的にダウンします。

20.2 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。

20.2.1 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 20-7 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。

20.2.2 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 20-8 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。

20.3 PVST+ 解説

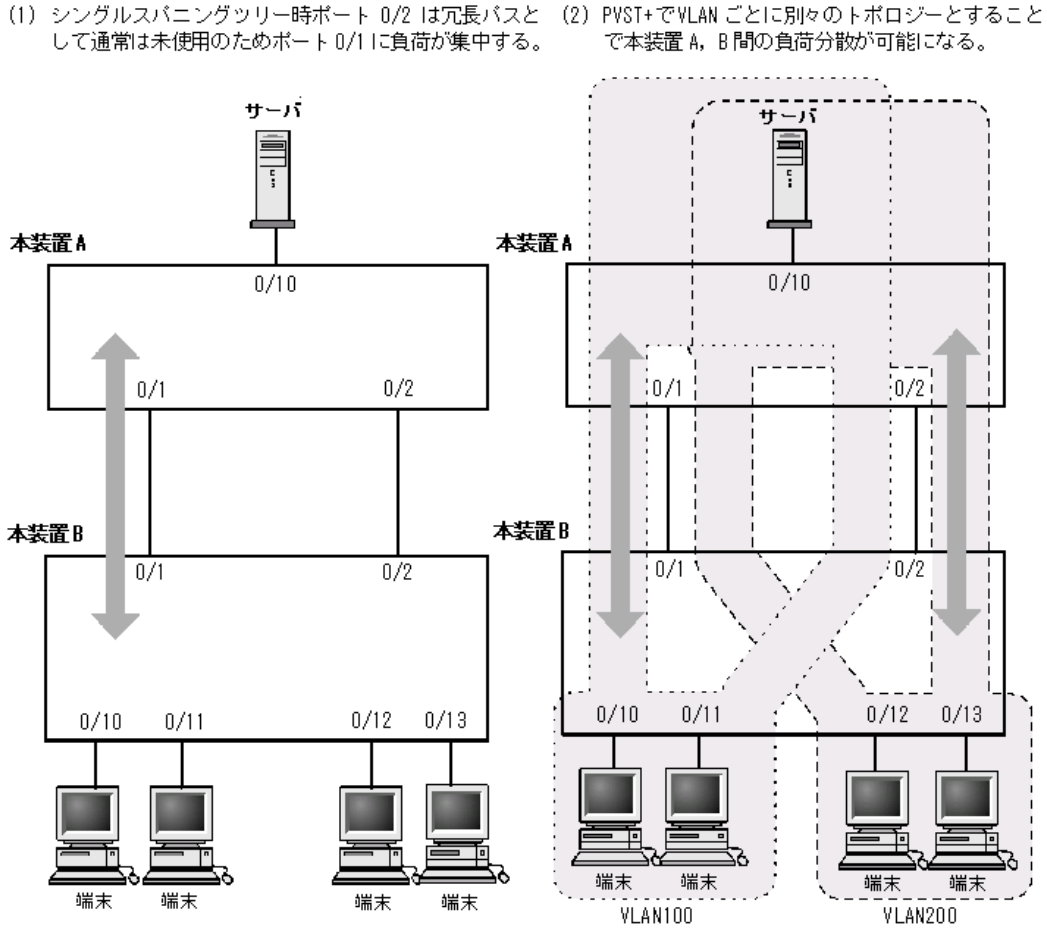
PVST+ は，VLAN 単位にツリーを構築します。VLAN 単位にツリーを構築できるため，ロードバランシングが可能です。また，アクセスポートでは，シングルスパニングツリーで動作しているスイッチと接続できます。

20.3.1 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 20-6 PVST+ によるロードバランシング



20.3.2 アクセスポートの PVST+

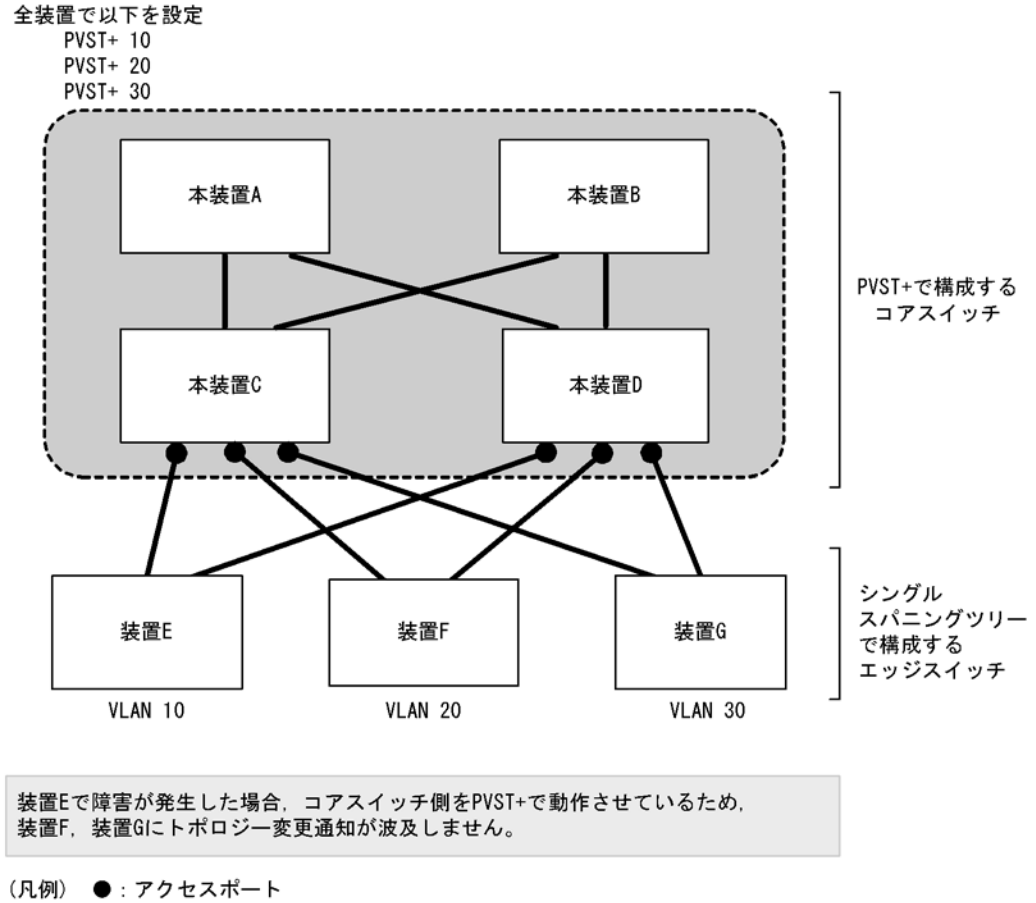
(1) 解説

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 20-7 シングルスパニングツリーとの接続



(2) アクセスポートでシングルスパニングツリーを混在させた場合

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

(3) 構成不一致検出機能

同一 VLAN で接続しているポートについて，本装置でアクセスポート，プロトコルポート，MAC ポートのどれかを設定（Untagged フレームを使用）し，対向装置ではトランクポートを設定（Tagged フレームを使用）した場合，該当 VLAN では通信できないポートとなります。このようなポートを構成不一致として検出します。検出する条件は，本装置がアクセスポートで，対向装置でトランクポートを設定（Tagged フレームを使用）した場合です。この場合，該当するポートを停止状態（Disable）にします。対向装置でトランクポートの設定（Tagged フレームを使用）を削除すれば，hello-time 値× 3 秒（デフォルトは 6 秒）後に，自動的に停止状態を解除します。

20.3.3 PVST+ 使用時の注意事項

(1) 他機能との共存

「16.3 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

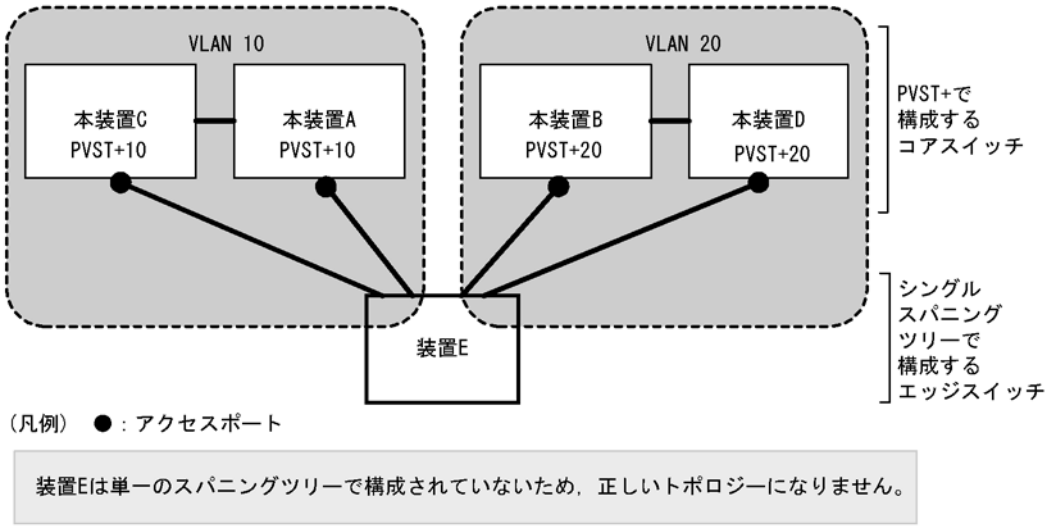
シングルスパニングツリーと VLAN 1 の PVST+ を同時に動作させることはできません。シングルスパニングツリーを動作させると VLAN 1 の PVST+ は停止します。

(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 20-8 シングルスパニングツリーとの禁止構成例



装置Eは単一のスパニングツリーで構成されていないため，正しいトポロジーになりません。

20.4 PVST+ のコンフィグレーション

20.4.1 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 20-9 コンフィグレーションコマンド一覧

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

20.4.2 PVST+ の設定

[設定のポイント]

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

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

[コマンドによる設定]

1. **(config)# no spanning-tree vlan 20**
   VLAN 20 の PVST+ の動作を停止します。

2. **(config)# spanning-tree vlan 20**
   停止した VLAN 20 の PVST+ を動作させます。

[注意事項]

- PVST+ はコンフィグレーションに表示がないときは自動的に動作しています。コンフィグレーションコマンド no spanning-tree vlan で停止すると，停止状態であることがコンフィグレーションで確認できます。
- PVST+ は最大 250 個のポート VLAN まで動作します。それ以上のポート VLAN を作成しても自動的には動作しません。

20.4.3 PVST+ のトポロジー設定

(1) ブリッジ優先度の設定

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

[設定のポイント]

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

[コマンドによる設定]

1. **(config)# spanning-tree vlan 10 priority 4096**
   VLAN 10 の PVST+ のブリッジ優先度を 4096 に設定します。

(2) パスコストの設定

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

[設定のポイント]

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

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

パスコスト値には short（16bit 値），long（32bit 値）の 2 種類があり，トポロジーの全体で合わせる必要があります。デフォルトでは short（16bit 値）で動作します。イーサネットインタフェースの速度による自動的な設定は，short（16bit 値）か long（32bit 値）かで設定内容が異なります。パスコストのデフォルト値を次の表に示します。

表 20-10 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

[コマンドによる設定]

1. **(config)# interface fastethernet 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 fastethernet 0/1
   (config-if)# spanning-tree vlan 10 cost 200000
   (config-if)# exit
   long（32bit 値）のパスコストを使用するように設定した後に，ポート 0/1 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。

(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 fastethernet 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 fastethernet 0/1**
   (config-if)# spanning-tree vlan 10 port-priority 144
   (config-if)# exit
   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。

20.4.4 PVST+ のパラメータ設定

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

(1) BPDU の送信間隔の設定

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

の負荷を軽減できます。

[設定のポイント]

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

[コマンドによる設定]

1. **(config)# spanning-tree vlan 10 hello-time 3**
   VLAN 10 の PVST+ の BPDU 送信間隔を 3 秒に設定します。

[注意事項]

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

(2) 送信する最大 BPDU 数の設定

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

[設定のポイント]

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

[コマンドによる設定]

1. **(config)# spanning-tree vlan 10 transmission-limit 5**
   VLAN 10 の Rapid PVST+ の hello-time 当たりの最大送信 BPDU 数を 5 に設定します。

(3) BPDU の最大有効時間の設定

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

[設定のポイント]

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

[コマンドによる設定]

1. **(config)# spanning-tree vlan 10 max-age 25**
   VLAN 10 の PVST+ の BPDU の最大有効時間を 25 秒に設定します。

(4) 状態遷移時間の設定

PVST+ モードまたは Rapid PVST+ モードでタイマによる動作となる場合，ポートの状態が一定時間ごとに遷移します。PVST+ モードの場合は Blocking から Listening，Learning，Forwarding と遷移し，

Rapid PVST+ モードの場合は Discarding から Learning，Forwarding と遷移します。この状態遷移に必要な時間を設定できます。小さい値を設定すると，より早く Forwarding 状態に遷移できます。

［設定のポイント］

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

［コマンドによる設定］

1. **(config)# spanning-tree vlan 10 forward-time 10**
   VLAN 10 の PVST+ の状態遷移時間を 10 秒に設定します。

20.5 PVST+ のオペレーション

20.5.1 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 20-11 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。

20.5.2 PVST+ の状態の確認

PVST+ の情報は運用コマンド show spanning-tree の実行結果で示されます。Mode で PVST+，Rapid PVST+ の動作モードを確認できます。トポロジーが正しく構築されていることを確認するためには，Root Bridge ID の内容が正しいこと，Port Information の Status，Role が正しいことを確認してください。

図 20-9 show spanning-tree の実行結果

```
> show spanning-tree vlan 4094

Date 20XX/11/14 11:22:22 UTC
VLAN 4094  PVST+ Spanning Tree:Enabled   Mode:PVST+
  Bridge ID       Priority: 36862     MAC Address: 00ed.f010.0001
    Bridge Status: Designated
  Root Bridge ID  Priority: 36862     MAC Address: 0012.e2c4.2772
    Root Cost: 19
    Root Port: 0/20
  Port Information
    0/17      Down Status:Disabled    Role:-            LoopGuard
    0/18      Down Status:Disabled    Role:-            LoopGuard
    0/19      Down Status:Disabled    Role:-            LoopGuard
    0/20      Up   Status:Forwarding  Role:Root         PortFast
    0/21      Down Status:Disabled    Role:-            -
    0/22      Up   Status:Blocking    Role:Alternate    -
    ChGr:8    Down Status:Disabled    Role:-            RootGuard

>
```

20.6 シングルスパニングツリー解説

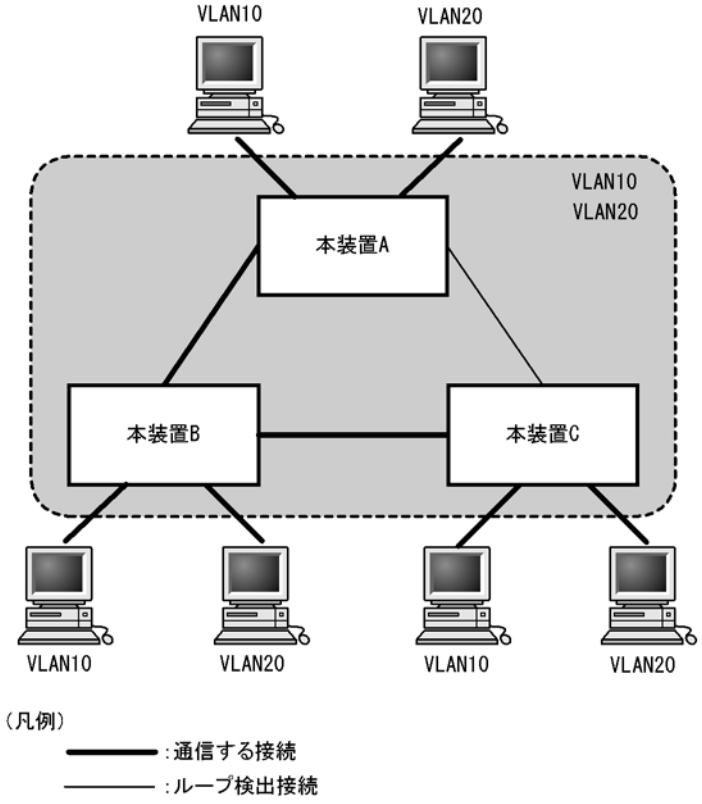
シングルスパニングツリーは装置全体を対象としトポロジーを構築します。

20.6.1 概要

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

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

図 20-10 シングルスパニングツリーによるネットワーク構成



20.6.2 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 20-12 シングルスパニングツリー対象の VLAN

項目	VLAN
PVST+ 対象の VLAN	PVST+ が動作している VLAN。 最大 250 個のポート VLAN は自動的に PVST+ が動作します。
シングルスパニングツリー対象の VLAN	251 個目以上のポート VLAN。
	PVST+ を停止（コンフィグレーションコマンド no spanning-tree vlan で指定）している VLAN。
	デフォルト VLAN（VLAN ID 1 のポート VLAN）。
	プロトコル VLAN。
	MAC VLAN。

20.6.3 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

「16.3 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。

20.7 シングルスパニングツリーのコンフィグレーション

20.7.1 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 20-13 コンフィグレーションコマンド一覧

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

20.7.2 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。

20.7.3 シングルスパニングツリーのトポロジー設定

(1) ブリッジ優先度の設定

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

[設定のポイント]

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

[コマンドによる設定]

1. **(config)# spanning-tree single priority 4096**
   シングルスパニングツリーのブリッジ優先度を 4096 に設定します。

(2) パスコストの設定

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

[設定のポイント]

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

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

パスコスト値には short（16bit 値），long（32bit 値）の 2 種類があり，トポロジーの全体で合わせる必要があります。デフォルトでは short（16bit 値）で動作します。イーサネットインタフェースの速度による自動的な設定は，short（16bit 値）か long（32bit 値）かで設定内容が異なります。パスコストのデフォルト値を次の表に示します。

表 20-14 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

[コマンドによる設定]

1. **(config)# interface fastethernet 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 fastethernet 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。

(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 fastethernet 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 fastethernet 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。

20.7.4 シングルスパニングツリーのパラメータ設定

各パラメータは「2 × (forward-time − 1) ≧ max-age ≧ 2 × (hello-time + 1)」という関係が成立するように設定する必要があります。パラメータを変える場合はトポロジー全体でパラメータを合わせる必要があります。

(1) BPDU の送信間隔の設定

BPDU の送信間隔は，短くした場合はトポロジー変更を検知しやすくなります。長くした場合はトポロ

ジー変更の検知までに時間が掛かるようになる一方で，BPDU トラフィックや本装置のスパニングツリーの負荷を軽減できます。

[設定のポイント]

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

[コマンドによる設定]

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

[注意事項]

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

(2) 送信する最大 BPDU 数の設定

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

[設定のポイント]

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

[コマンドによる設定]

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

(3) BPDU の最大有効時間

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

[設定のポイント]

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

[コマンドによる設定]

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

(4) 状態遷移時間の設定

STP モードまたは Rapid STP モードでタイマによる動作となる場合，ポートの状態が一定時間ごとに遷

移します。STP モードの場合は Blocking から Listening，Learning，Forwarding と遷移し，Rapid STP モードの場合は Discarding から Learning，Forwarding と遷移します。この状態遷移に必要な時間を設定できます。小さい値を設定すると，より早く Forwarding 状態に遷移できます。

［設定のポイント］

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

［コマンドによる設定］

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

20.8 シングルスパニングツリーのオペレーション

20.8.1 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 20-15 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。

20.8.2 シングルスパニングツリーの状態の確認

シングルスパニングツリーの情報は運用コマンド show spanning-tree で確認してください。Mode で STP，Rapid STP の動作モードを確認できます。トポロジーが正しく構築されていることを確認するためには，Root Bridge ID の内容が正しいこと，Port Information の Status，Role が正しいことを確認してください。

図 20-11 シングルスパニングツリーの情報

```
> show spanning-tree single

Date 20XX/11/14 11:38:40 UTC
Single Spanning Tree:Enabled   Mode:STP
  Bridge ID       Priority: 32768     MAC Address: 00ed.f010.0001
    Bridge Status: Root
  Root Bridge ID  Priority: 32768     MAC Address: 00ed.f010.0001
    Root Cost: 0
    Root Port: -
  Port Information
    0/1       Up   Status:Learning    Role:Designated   RootGuard
    0/2       Down Status:Disabled    Role:-            RootGuard
    0/3       Down Status:Disabled    Role:-            -
    0/4       Down Status:Disabled    Role:-            -
    0/5       Down Status:Disabled    Role:-            -
    0/6       Down Status:Disabled    Role:-            -
    0/7       Down Status:Disabled    Role:-            RootGuard
    0/8       Down Status:Disabled    Role:-            RootGuard
    0/11      Down Status:Disabled    Role:-            LoopGuard
    0/12      Up   Status:Blocking    Role:Alternate    LoopGuard
    0/14      Down Status:Disabled    Role:-            PortFast
    0/16      Down Status:Disabled    Role:-            PortFast
    0/17      Down Status:Disabled    Role:-            LoopGuard
    0/18      Down Status:Disabled    Role:-            LoopGuard
    0/19      Down Status:Disabled    Role:-            LoopGuard
    0/20      Up   Status:Forwarding  Role:Designated   PortFast
    0/21      Down Status:Disabled    Role:-            -
    0/22      Up   Status:Learning    Role:Designated   -
    0/23      Down Status:Disabled    Role:-            -
    0/24      Up   Status:Learning    Role:Designated   -
    0/25      Down Status:Disabled    Role:-            LoopGuard
    0/26      Down Status:Disabled    Role:-            LoopGuard
    ChGr:1    Up   Status:Learning    Role:Designated   RootGuard
    ChGr:8    Down Status:Disabled    Role:-            RootGuard

>
```

20.9 マルチプルスパニングツリー解説

20.9.1 概要

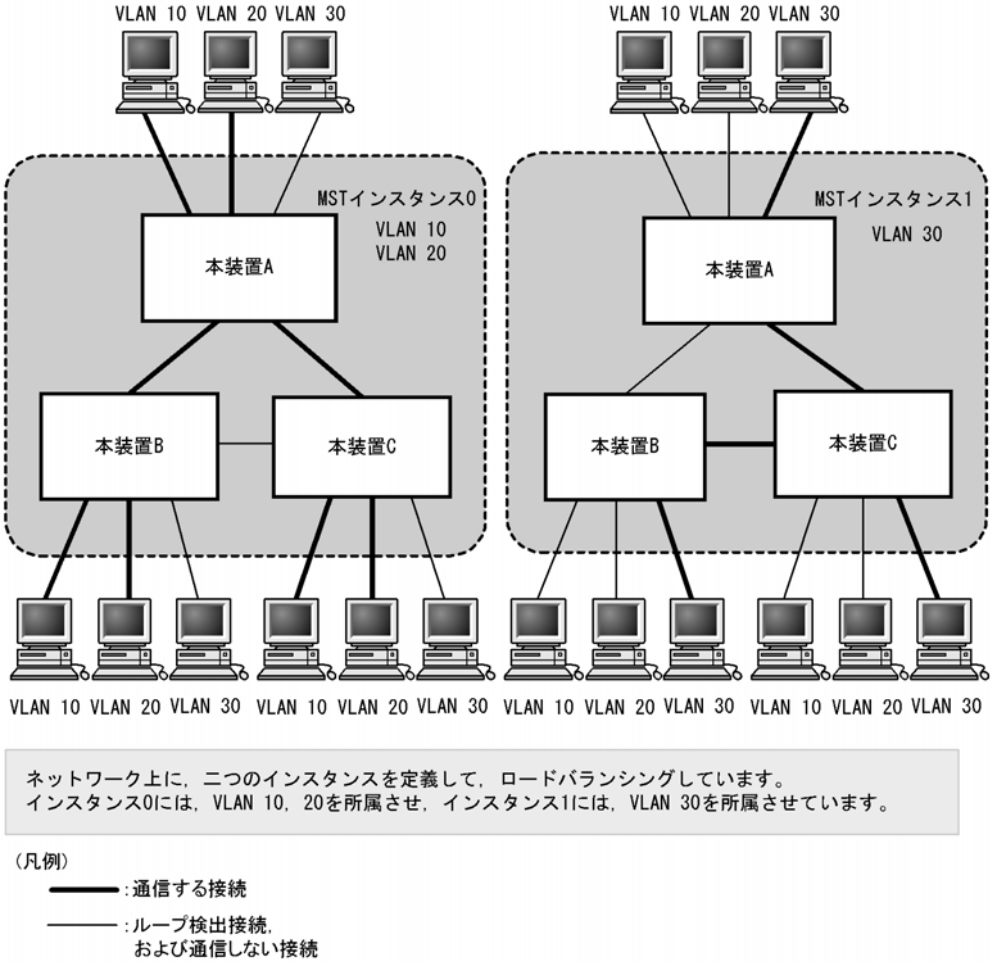
マルチプルスパニングツリーには，次の特長があります。MST インスタンスによってロードバランシングを可能にしています。また，MST リージョンによって，大規模なネットワーク構成を中小構成に分割することでネットワーク設計が容易になります。以降，これらを実現するためのマルチプルスパニングツリーの機能概要を説明します。

(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 20-12 MST インスタンスイメージ



(2) MST リージョン

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

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

● CST

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

● IST

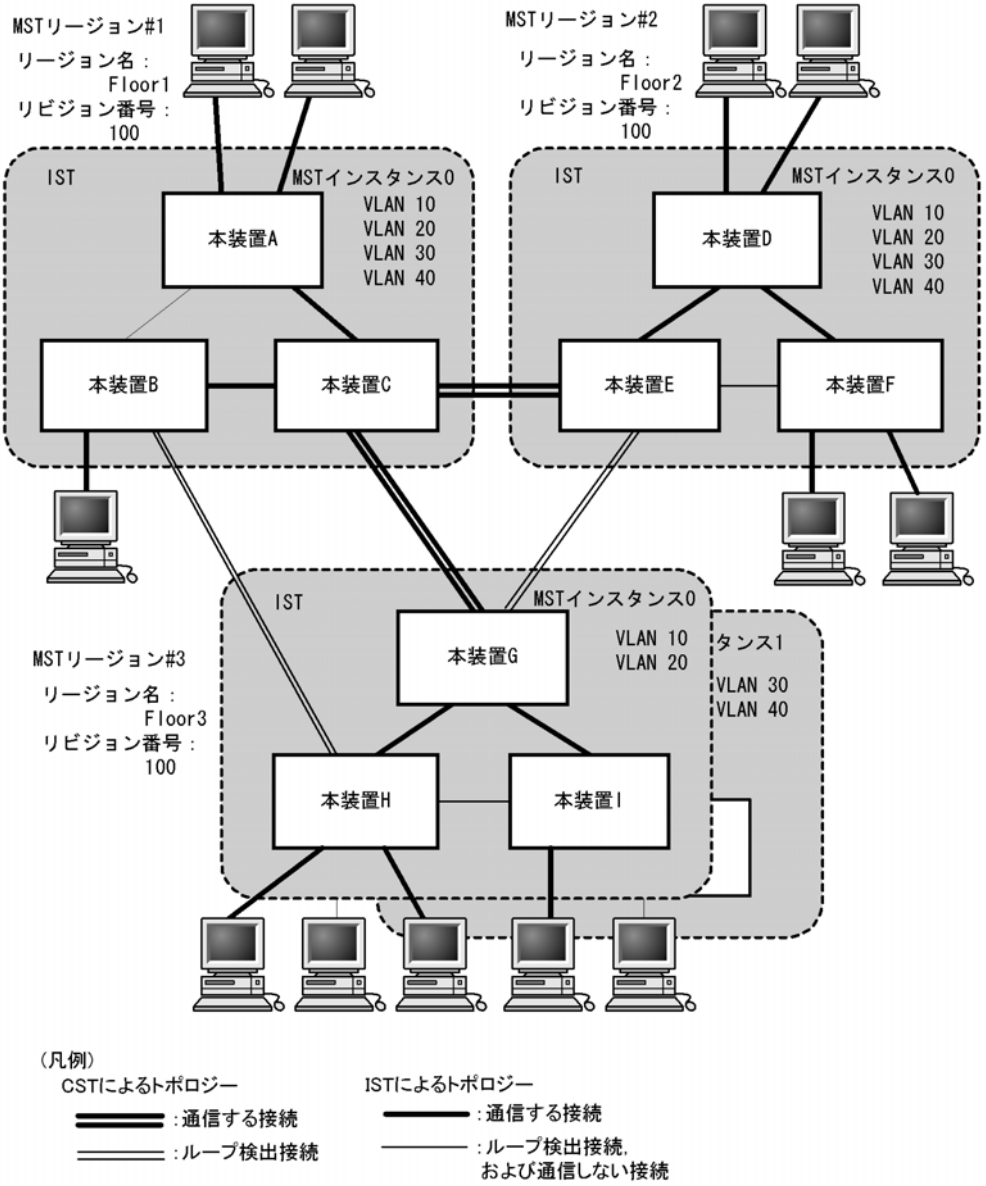
IST（Internal Spanning Tree）は，MST リージョン外と接続するために，MST リージョン内で Default 動作するトポロジーのことを指し，MST インスタンス ID0 が割り当てられます。MST リージョン外と接続しているポートを境界ポートと呼びます。また，リージョン内，リージョン間で MST BPDU を送受信する唯一の MST インスタンスとなります。全 MST インスタンスのトポロジー情報は，MST BPDU にカプセル化し通知します。

● CIST

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

マルチプルスパニングツリー概要を次の図に示します。

図 20-13 マルチプルスパニングツリー概要

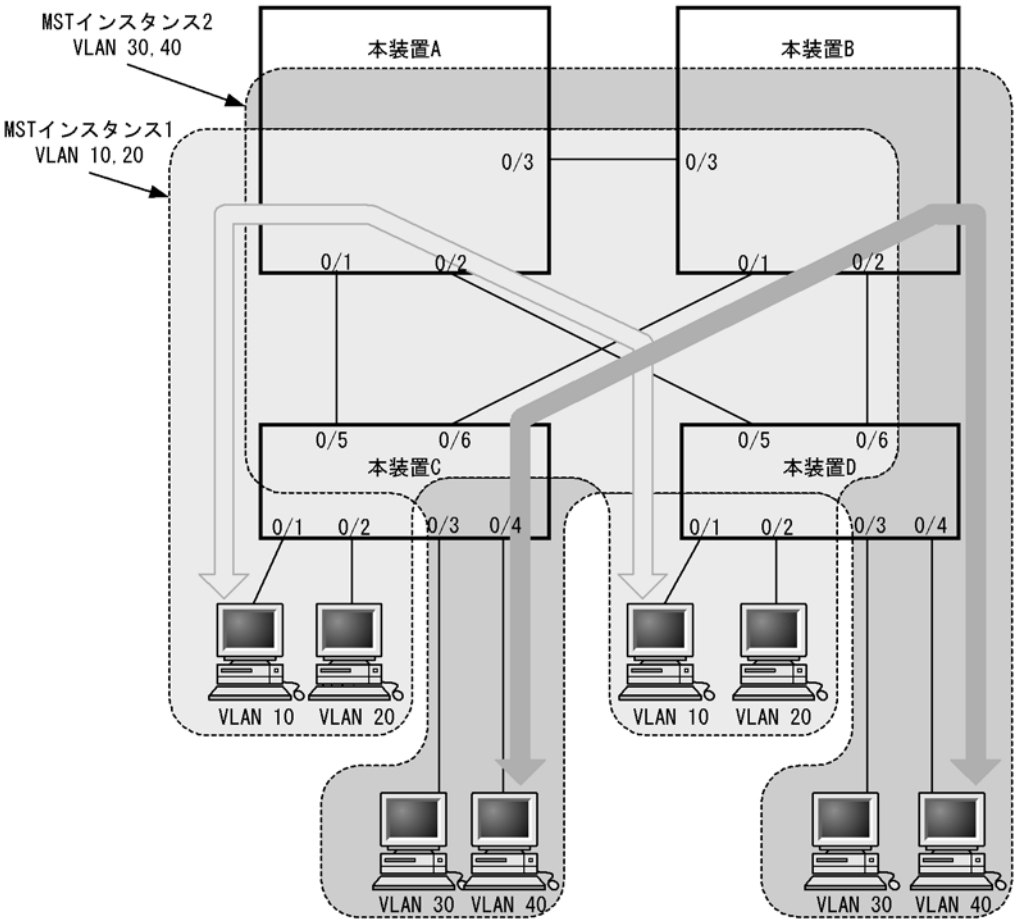


20.9.2 マルチプルスパニングツリーのネットワーク設計

(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 20-14 マルチプルスパニングツリーのロードバランシング構成

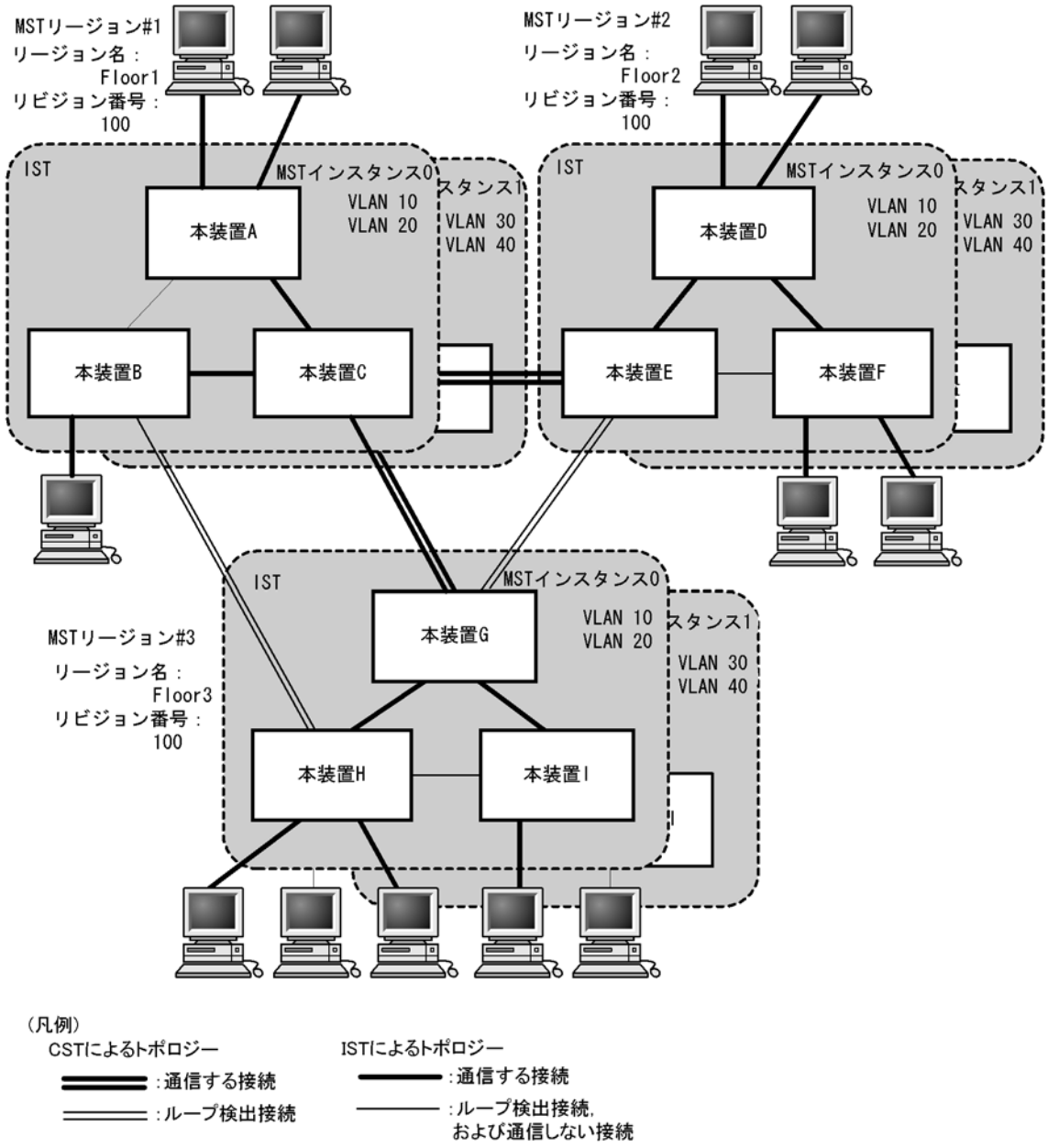


(2) MST リージョンによるネットワーク設計

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

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

図 20-15　MST リージョンによるネットワーク構成



20.9.3　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。

20.9.4 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

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

(2) MST リージョンについて

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

(3) トポロジーの収束に時間が掛かる場合について

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

表 20-16 ルートブリッジでのイベント発生

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

20.10 マルチプルスパニングツリーのコンフィグレーション

20.10.1 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 20-17 コンフィグレーションコマンド一覧

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

20.10.2 マルチプルスパニングツリーの設定

(1) マルチプルスパニングツリーの設定

[設定のポイント]

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

[コマンドによる設定]

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

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

[注意事項]

コンフィグレーションコマンド no spanning-tree mode でマルチプルスパニングツリーの動作モード

設定を削除すると，デフォルトの動作モードである pvst になります。その際，ポート VLAN で自動的に PVST+ が動作を開始します。

(2) リージョン，インスタンスの設定

[設定のポイント]

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

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

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

[コマンドによる設定]

1. **(config)# spanning-tree mst configuration**
   (config-mst)# name "REGION TOKYO"
   (config-mst)# revision 1
   マルチプルスパニングツリーコンフィグレーションモードに移り，name（リージョン名），revision（リビジョン番号）の設定を行います。

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

20.10.3 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 20-18 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

[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 fastethernet 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。

(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 fastethernet 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 fastethernet 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。

20.10.4 マルチプルスパニングツリーのパラメータ設定

各パラメータは「2 × (forward-time − 1) ≧ max-age ≧ 2 × (hello-time + 1)」という関係が成立するように設定する必要があります。パラメータを変える場合はトポロジー全体でパラメータを合わせる必要があります。

(1) BPDU の送信間隔の設定

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

[設定のポイント]

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

[コマンドによる設定]

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

[注意事項]

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

(2) 送信する最大 BPDU 数の設定

スパニングツリーでは，CPU 負荷の増大を抑えるために，hello-time（BPDU 送信間隔）当たりに送信す

る最大 BPDU 数を決めることができます。トポロジー変更が連続的に発生すると，トポロジー変更を通知，収束するために大量の BPDU が送信され，BPDU トラフィックの増加，CPU 負荷の増大につながります。送信する BPDU の最大数を制限することによりこれらを抑えます。

[設定のポイント]

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

[コマンドによる設定]

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

(3) 最大ホップ数の設定

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

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

[設定のポイント]

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

[コマンドによる設定]

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

(4) BPDU の最大有効時間の設定

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

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

[設定のポイント]

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

[コマンドによる設定]

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

(5) 状態遷移時間の設定

タイマによる動作となる場合，ポートの状態が Discarding から Learning，Forwarding へ一定時間ごと

に遷移します。この状態遷移に必要な時間を設定できます。小さい値を設定すると，より早く Forwarding 状態に遷移できます。

[設定のポイント]

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

[コマンドによる設定]

1. **(config)# spanning-tree mst forward-time 10**
   マルチプルスパニングツリーの状態遷移時間を 10 秒に設定します。

20.11 マルチプルスパニングツリーのオペレーション

20.11.1 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 20-19 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。

20.11.2 マルチプルスパニングツリーの状態の確認

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

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

show spanning-tree の実行結果を次の図に示します。

図 20-16 show spanning-tree の実行結果

```
> show spanning-tree mst instance 4095

Date 20XX/11/14 13:04:05 UTC
Multiple Spanning Tree: Enabled
Revision Level: 0      Configuration Name:
MST Instance 4095
  VLAN Mapped: 4094
  Regional Root  Priority: 36863       MAC      : 00ed.f010.0001
  Internal Root Cost     : 0           Root Port: -
  Bridge ID      Priority: 36863       MAC      : 00ed.f010.0001
  Regional Bridge Status : Root
  Port Information
    0/17      Down Status:Disabled    Role:-            -
    0/18      Down Status:Disabled    Role:-            -
    0/19      Down Status:Disabled    Role:-            -
    0/20      Up   Status:Forwarding  Role:Designated   PortFast
    0/21      Down Status:Disabled    Role:-            -
    0/22      Up   Status:Forwarding  Role:Designated   -
    ChGr:8    Down Status:Disabled    Role:-            RootGuard

>
```

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。

20.12 スパニングツリー共通機能解説

20.12.1 PortFast

(1) 概要

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

PortFast 機能は，PortFast の設定とポートの種類に従って動作します。PortFast 機能の動作条件を次の表に示します。

表 20-20 PortFast 機能の動作条件

コンフィグレーションの設定		ポートの種類	
ポート単位の設定 (spanning-tree portfast)	装置単位の設定 (spanning-tree portfast default)	アクセスポート プロトコルポート MAC ポート	トランクポート
PortFast 設定（trunk）	（ポート単位の設定を優先）	○	○
PortFast 無効（disable）		×	×
パラメータ省略時		○	×
コマンド未設定	コマンド設定	○	×
	コマンド未設定	×	×

（凡例）
○：動作可，×：動作不可

(2) PortFast 適用時の BPDU 受信

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

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

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

(3) PortFast 適用時の BPDU 送信

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

ただし，PortFast を設定したポート同士を誤って接続した状態を検出するために，PortFast 機能によって即時に通信可状態になった時点から 10 フレームだけ BPDU の送信を行います。

(4) BPDU ガード

PortFast に適用する機能として，BPDU ガード機能があります。BPDU ガード機能を適用したポートで

は，BPDU 受信時に，スパニングツリー対象のポートとして動作するのではなくポートを inactive 状態にします。

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

20.12.2 BPDU フィルタ

(1) 概要

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

(2) BPDU フィルタに関する注意事項

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

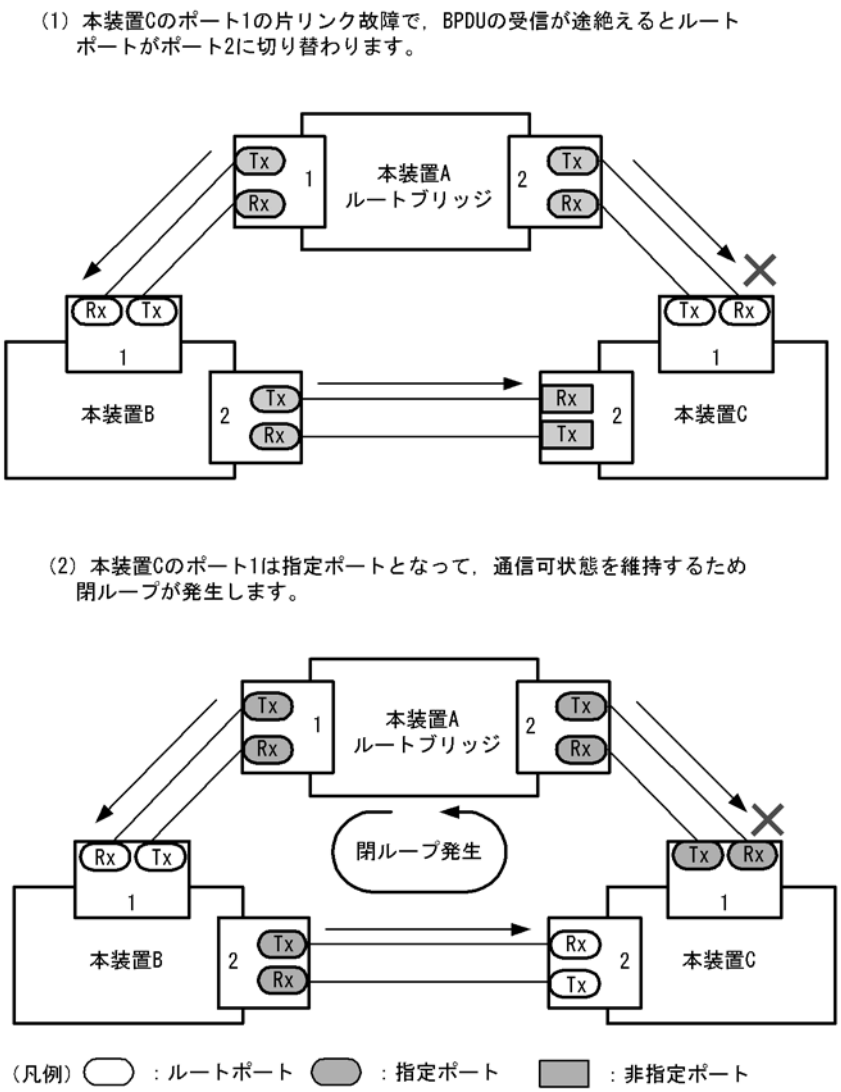
20.12.3 ループガード

(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 20-17 単一方向のリンク障害時の問題点



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

ループガード機能は，装置またはポート単位で PortFast 機能を設定している場合，またはルートガード機能を設定したポートでは動作しません。

ループガードの動作条件を次の表に示します。

表 20-21 ループガードの動作条件

PortFast 機能	コンフィグレーションの設定		ループガードの動作
	ポート単位の設定 (spanning-tree guard)	装置単位の設定 (spanning-tree loopguard default)	
有効	ループガード設定（loop）	（ポート単位の設定を優先）	×
	ガード無効設定（none）		×
	ルートガード設定（root）		×
	コマンド未設定	コマンド設定	×
		コマンド未設定	×
無効	ループガード設定（loop）	（ポート単位の設定を優先）	○
	ガード無効設定（none）		×
	ルートガード設定（root）		×
	コマンド未設定	コマンド設定	○
		コマンド未設定	×

（凡例）
○：動作可，×：動作不可

(2) ループガードに関する注意事項

ループガードはマルチプルスパニングツリーでは使用できません。

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

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

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

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

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

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

20.12.4 ルートガード

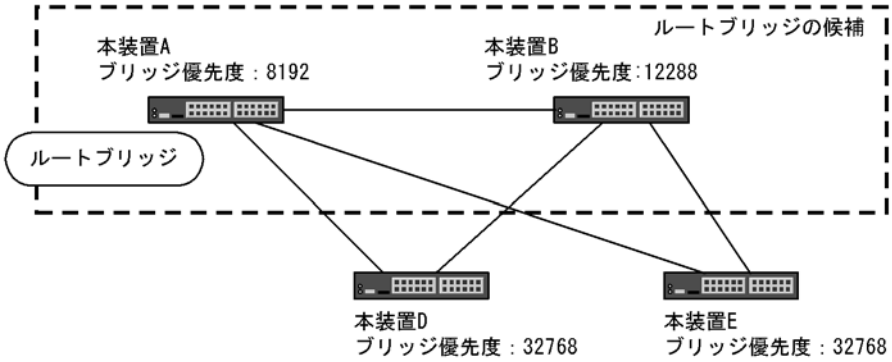
(1) 概要

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。

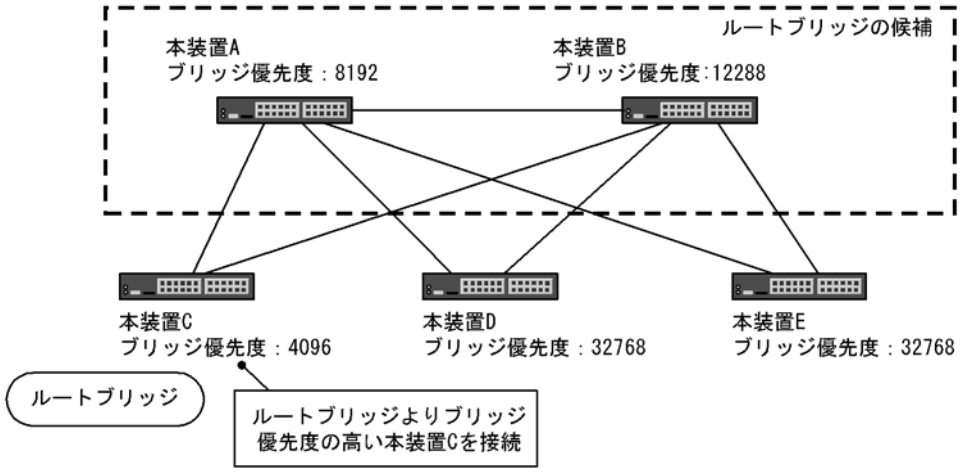
● 本装置 A，本装置 B をルートブリッジの候補として運用

図 20-18 本装置 A，本装置 B をルートブリッジの候補として運用



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

図 20-19 本装置 A，本装置 B よりブリッジ優先度の高い本装置 C を接続



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

ルートガードの動作条件を次の表に示します。

表 20-22 ルートガードの動作条件

コンフィグレーションの設定		ルートガードの動作
ポート単位の設定 (spanning-tree guard)	**装置単位の設定** (spanning-tree loopguard default)	
ループガード設定（loop）	（ポート単位の設定を優先）	×
ガード無効設定（none）		×
ルートガード設定（root）		○
コマンド未設定	コマンド設定	×
	コマンド未設定	×

（凡例）
○：動作可，×：動作不可

20.13 スパニングツリー共通機能のコンフィグレーション

20.13.1 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 20-23 コンフィグレーションコマンド一覧

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

20.13.2 PortFast の設定

(1) PortFast の設定

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

[設定のポイント]

コンフィグレーションコマンド spanning-tree portfast default を設定すると，アクセスポート，プロトコルポート，MAC ポートにデフォルトで PortFast 機能を適用します。デフォルトで適用してポートごとに無効にしたい場合は，コンフィグレーションコマンド spanning-tree portfast disable を設定します。
トランクポートでは，ポートごとの指定で適用できます。

[コマンドによる設定]

1. **(config)# spanning-tree portfast default**
   すべてのアクセスポート，プロトコルポート，MAC ポートに対して PortFast 機能を適用するように設定します。

2. **(config)# interface fastethernet 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 fastethernet 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。コンフィグレーションコマンド spanning-tree portfast bpduguard default は PortFast 機能を適用しているすべてのポートにデフォルトで BPDU ガードを適用します。デフォルトで適用するときに BPDU ガード機能を無効にしたい場合は，コンフィグレーションコマンド spanning-tree bpduguard disable を設定します。

[コマンドによる設定]

1.
```
(config)# spanning-tree portfast default
(config)# spanning-tree portfast bpduguard default
```
すべてのアクセスポート，プロトコルポート，MAC ポートに対して PortFast 機能を設定します。また，PortFast 機能を適用したすべてのポートに対し BPDU ガード機能を設定します。

2.
```
(config)# interface fastethernet 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 fastethernet 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，コンフィグレーションコマンド spanning-tree bpduguard enable で設定します。

20.13.3 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 fastethernet 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。

20.13.4 ループガードの設定

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

[設定のポイント]

ループガードは，PortFast 機能を設定していないポートで動作します。
コンフィグレーションコマンド spanning-tree loopguard default 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コンフィグレーションコマンド spanning-tree guard none を設定します。

[コマンドによる設定]

1. **(config)# spanning-tree loopguard default**
   PortFast を設定したポート以外のすべてのポートに対してループガード機能を適用するように設定します。

2. **(config)# interface fastethernet 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 fastethernet 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。

20.13.5 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 fastethernet 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。

20.13.6 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 fastethernet 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。

20.14 スパニングツリー共通機能のオペレーション

20.14.1 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 20-24 運用コマンド一覧

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

20.14.2 スパニングツリー共通機能の状態の確認

スパニングツリーの情報は運用コマンド show spanning-tree detail で確認してください。VLAN 4094 の PVST+ の例を次の図に示します。

- PortFast はポート 0/20 に設定していることを PortFast の項目で確認できます。
- ループガードはポート 0/17 に設定していることを Loop Guard の項目で確認できます。
- ルートガードは RootGuard，BPDU フィルタは BPDUFilter の項目で確認できます。（本例では，どちらも OFF を表示しているので未設定を示しています。）
- リンクタイプは各ポートの Link Type の項目で確認できます。（本例は，PVST+ のため " － " を表示します。）

図 20-20 スパニングツリーの情報

```
> show spanning-tree vlan 4094 detail

Date 20XX/11/14 11:26:46 UTC
VLAN 4094  PVST+ Spanning Tree:Enabled   Mode:PVST+
  Bridge ID
    Priority:36862                 MAC Address:00ed.f010.0001
    Bridge Status:Designated       Path Cost Method:Short
    Max Age:20                     Hello Time:2
    Forward Delay:15
  Root Bridge ID
    Priority:36862                 MAC Address:0012.e2c4.2772
    Root Cost:19
    Root Port:0/20
    Max Age:20                     Hello Time:2
    Forward Delay:15
  Port Information
  Port:0/17 Down
    Status:Disabled                Role:-
    Priority:128                   Cost:-
    Link Type:-                    Compatible Mode:-
    Loop Guard:ON(Blocking)        PortFast:OFF
    BPDUFilter:OFF                 RootGuard:OFF
  Port:0/20 Up
    Status:Forwarding              Role:Root
    Priority:128                   Cost:19
    Link Type:-                    Compatible Mode:-
    Loop Guard:OFF                 PortFast:ON(BPDU received)
    BPDUFilter:OFF                 RootGuard:OFF
    BPDU Parameters(20XX/11/14 11:26:47):
      Designated Root
        Priority:36862             MAC address:0012.e2c4.2772
      Designated Bridge
        Priority:36862             MAC address:0012.e2c4.2772
        Root Cost:0
      Port ID
        Priority:128               Number:20
      Message Age Timer:2(0)/20
```

>

21 Ring Protocol の解説【S2200】【SS1250】【SS1240】

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。

21.1 Ring Protocol の概要

21.2 Ring Protocol の基本原理

21.3 シングルリングの動作概要

21.4 マルチリングの動作概要

21.5 Ring Protocol の多重障害監視機能

21.6 Ring Protocol のネットワーク設計

21.7 Ring Protocol 使用時の注意事項

21.1 Ring Protocol の概要

21.1.1 概要

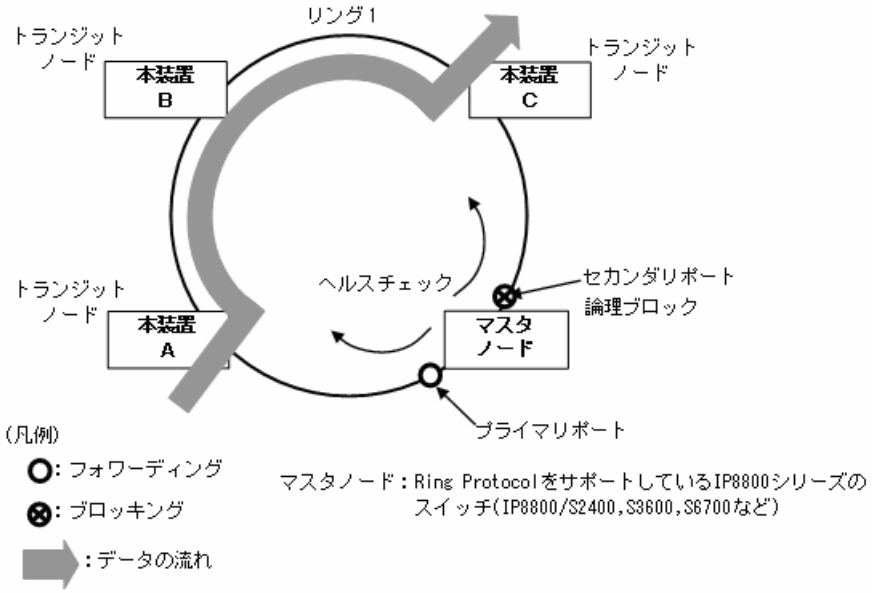
Ring Protocol とは，スイッチをリング状に接続したネットワークでの障害の検出と，それに伴う経路切り替えを高速に行うレイヤ 2 ネットワークの冗長化プロトコルです。

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

Ring Protocol を構成するスイッチにはマスタノードとトランジットノードがありますが，本装置はトランジットノードだけサポートしています。本マニュアルでは本装置のトランジットノードについて説明します。マスタノードの詳細については，マスタノードをサポートしている IP8800 シリーズのマニュアルを参照してください。

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 21-1 Ring Protocol の概要



リングを構成するノードのうち一つをマスタノードとして，ほかのリング構成ノードをトランジットノードとします。各ノード間を接続する二つのポートをリングポートと呼び，マスタノードのリングポートにはプライマリポートとセカンダリポートがあります。マスタノードはセカンダリポートを論理ブロックすることでリング構成を分断します。これによって，データフレームのループを防止しています。マスタノードはリング内の状態監視を目的とした制御フレーム（ヘルスチェックフレーム）を定期的に送信します。マスタノードは，巡回したヘルスチェックフレームの受信，未受信によって，リング内で障害が発生していないかどうかを判断します。障害または障害復旧を検出したマスタノードは，セカンダリポートの論理ブロックを設定または解除することで経路を切り替え，通信を復旧させます。

21.1.2　特長

（1）イーサネットベースのリングネットワーク

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

Ring Protocol の適用例を次の図に示します。

図 21-2　Ring Protocol **の適用例（その** 1**）**

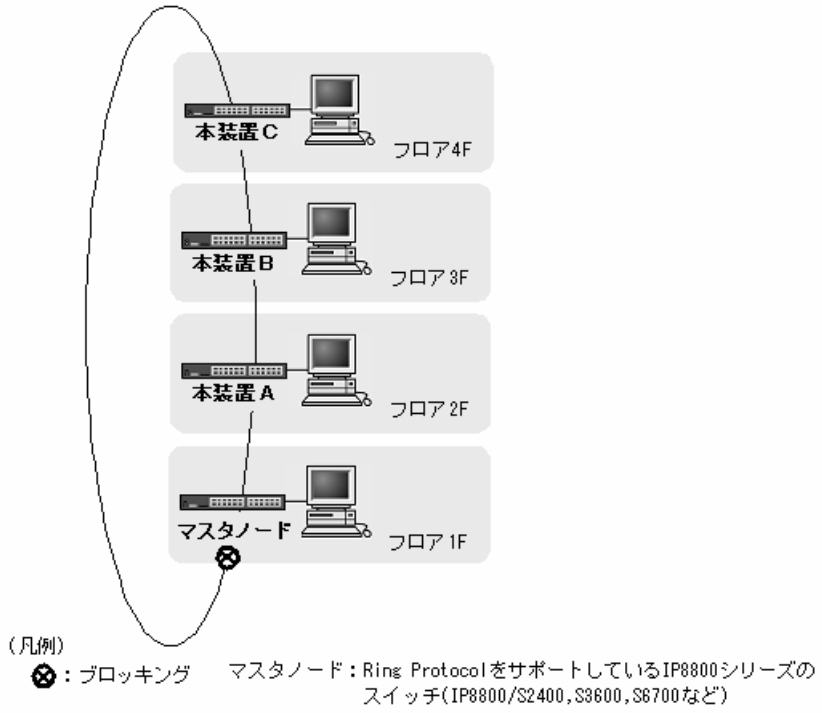
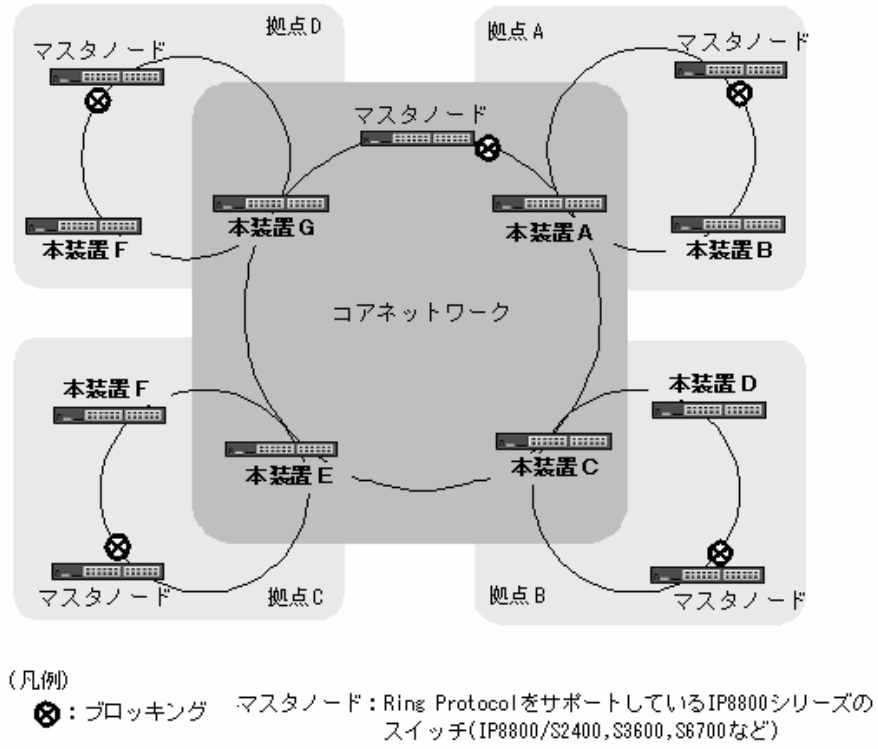


図 21-3 Ring Protocol の適用例（その 2）



(2) シンプルな動作方式

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

(3) 制御フレーム

Ring Protocol では，本プロトコル独自の制御フレームを使用します。制御フレームは，マスタノードによるリング状態の監視やマスタノードからトランジットノードへの経路の切り替え指示に使われます。制御フレームの送受信は，専用の VLAN 上で行われるため，通常のスパニングツリーのようにデータフレームと制御フレームが同じ VLAN 内に流れることはありません。また，制御フレームは優先的に処理されるため，データトラフィックが増大しても制御フレームに影響を与えません。

(4) 負荷分散方式

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

21.1.3 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 21-1 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）
ノード	マスタノード	×
	トランジットノード	○
	共有ノード	×
装置当たりのリング ID 最大数		4
リングポート（1 リング ID 当たりのポート数）		2（物理ポートまたはリンクアグリゲーション）
VLAN 数	1 リング ID 当たりの制御 VLAN 数	1（デフォルト VLAN の設定は不可）
	1 リング ID 当たりのデータ転送用 VLAN グループ最大数	2
	1 データ転送用 VLAN グループ当たりの VLAN マッピング最大数	128
	1VLAN マッピング当たりの VLAN 最大数	255
ヘルスチェックフレーム送信間隔		マスタノードに依存
障害監視時間		マスタノードに依存
負荷分散方式		マスタノードに依存
多重障害監視機能	装置当たりの多重障害監視可能リング数	4
	1 リング ID 当たりの多重障害監視 VLAN 数	1（デフォルト VLAN の設定は不可）
	多重障害監視フレーム送信間隔	マスタノードに依存
	多重障害監視時間	マスタノードに依存

（凡例） ○：サポート ×：未サポート

21.2 Ring Protocol の基本原理

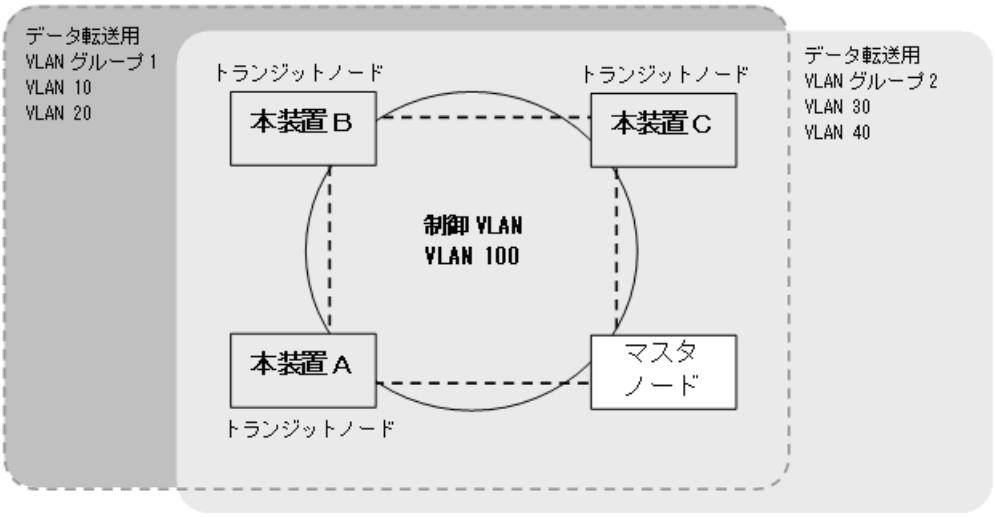
21.2.1 ネットワーク構成

Ring Protocol を使用する基本的なネットワーク構成と，本装置の位置づけを次に示します。

(1) シングルリング構成

シングルリング構成と，本装置の位置づけを次の図に示します。

図 21-4 シングルリング構成



マスタノード：Ring Protocolをサポートしている IP8800シリーズのスイッチ
（IP8800/S2400, S3600, S6700シリーズなど）

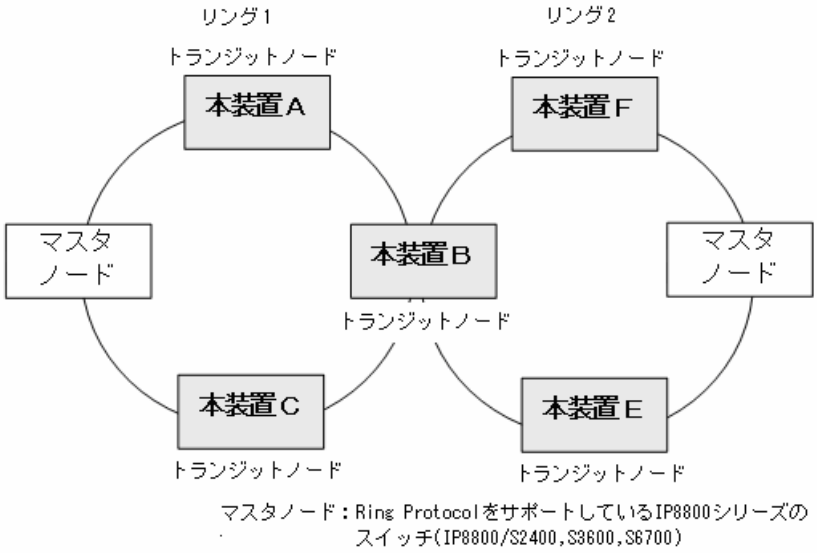
マスタノード 1 台とトランジットノード数台から成る一つのリング構成をシングルリング構成と呼びます。リングを構成するノード間は，リングポートとして，物理ポートまたはリンクアグリゲーションで接続されます。また，リングを構成するすべてのノードに，制御 VLAN として同一の VLAN，およびデータフレームの転送用として共通の VLAN を使用する必要があります。マスタノードから送信した制御フレームは，制御 VLAN 内を巡回します。データフレームの送受信に使用する VLAN は，VLAN グループと呼ばれる一つの論理的なグループに束ねて使用します。VLAN グループは複数の VLAN をまとめるこ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

マルチリング構成と，本装置の位置づけを次の図に示します。

マルチリング構成については，隣接するリングの接点となるノードが一つの場合を示しています。

図 21-5 マルチリング構成



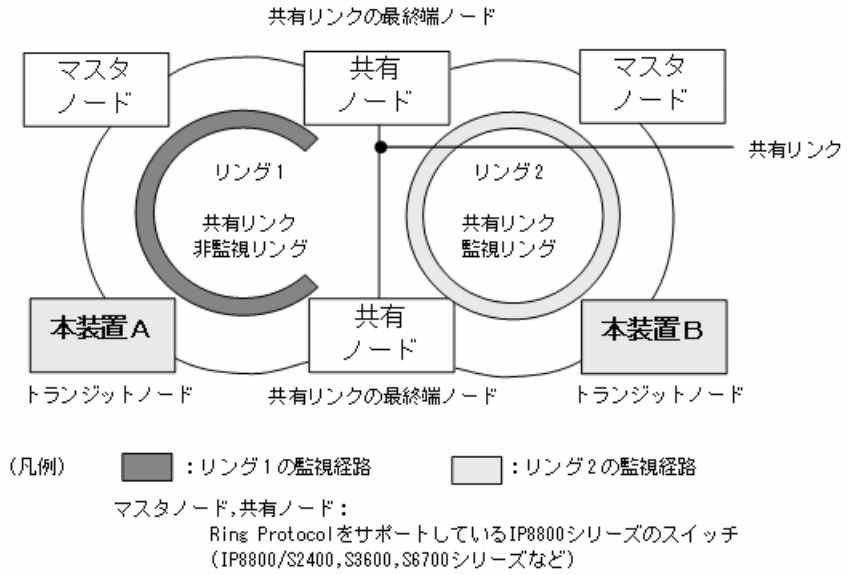
それぞれのリングを構成しているノードは独立したシングルリングとして動作します。このため，リング障害の検出および復旧の検出はそれぞれのリングで独立して行われます。

(3) 共有リンクありのマルチリング構成

共有リンクありのマルチリング構成と，本装置の位置づけを次の図に示します。

マルチリング構成については，隣接するリングの接点となるノードが二つ以上の場合を示しています。

図 21-6 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。

21.2.2 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。

21.2.3 障害監視方法

Ring Protocol のリング障害の監視は，マスタノードで実施します。詳細はマスタノード側のマニュアルを参照してください。

21.2.4 通信経路の切り替え

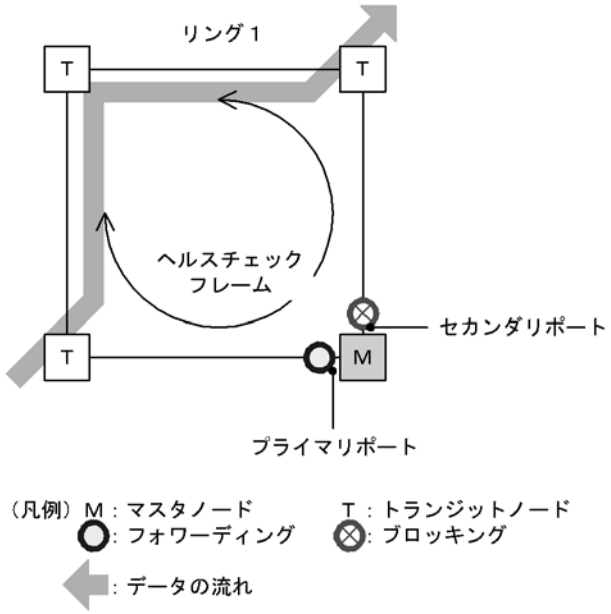
マスタノードがリングの障害を検出すると，同一の制御 VLAN を持つトランジットノードに対して MAC アドレステーブルエントリのクリアを要求するために，フラッシュ制御フレームと呼ぶ制御フレームを送信します。トランジットノードである本装置では，このフラッシュ制御フレームを受信すると，リングポートでの MAC アドレステーブルエントリのクリアを行います。これによって，MAC アドレスの学習が行われるまでフラッディングを行います。新しい経路でのフレームの送受信によって MAC アドレス学習が行われ，通信経路の切り替えが完了します。

21.3 シングルリングの動作概要

21.3.1 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 21-7 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。

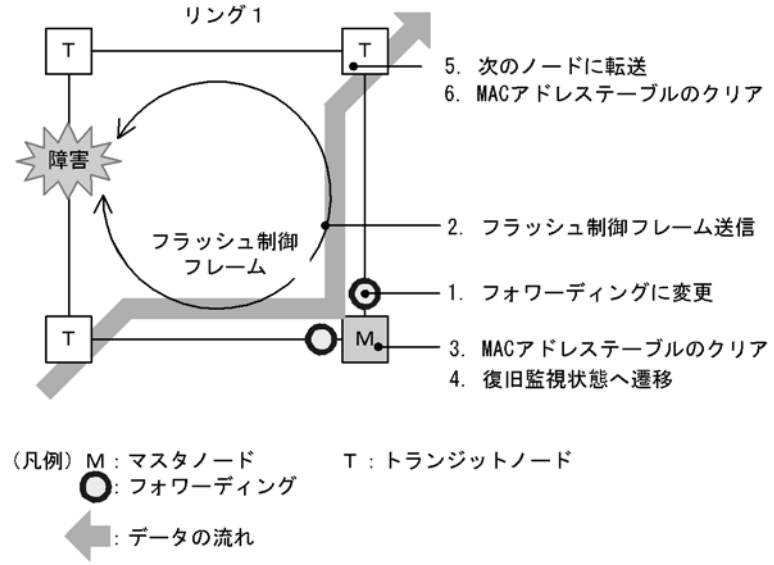
(2) トランジットノード動作

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。

21.3.2 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 21-8 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 21-2 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。

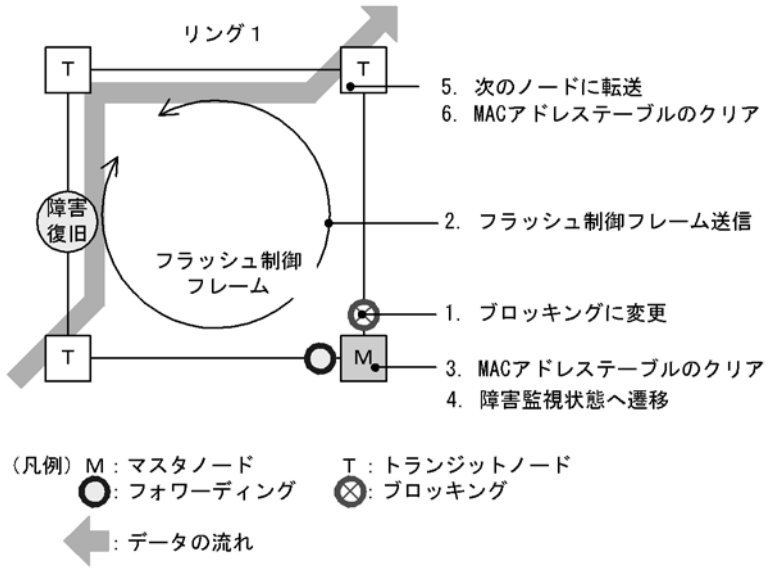
5. **フラッシュ制御フレームの転送**
   受信したフラッシュ制御フレームを次のノードに転送します。

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。

21.3.3 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 21-9 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 21-3 復旧検出時のデータ転送用リング VLAN 状態

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

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

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

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

(2) トランジットノード動作

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

5. **フラッシュ制御フレームの転送**
   受信したフラッシュ制御フレームを次のノードに転送します。

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

また，リンク障害が発生したトランジットノードでは，リンク障害が復旧した際のループの発生を防ぐため，リングポートのリング VLAN 状態はブロッキング状態となります。ブロッキング状態を解除する契機は，マスタノードが送信するフラッシュ制御フレームを受信したとき，またはトランジットノードでリングポートのフラッシュ制御フレーム受信待ち保護時間（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。

21.4　マルチリングの動作概要

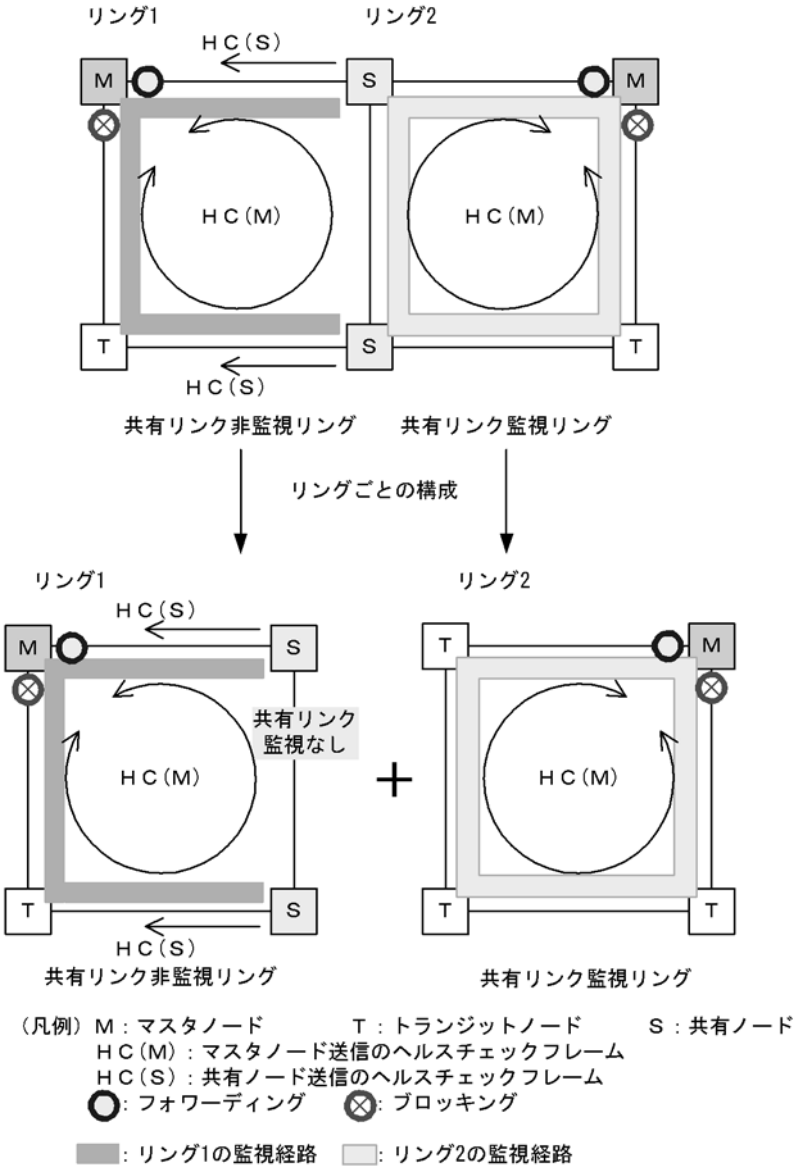
マルチリング構成のうち，共有リンクありのマルチリング構成について説明します。共有リンクなしのマルチリング構成については，シングルリング時の動作と同様ですので，「21.3　シングルリングの動作概要」を参照してください。

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。

21.4.1　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。

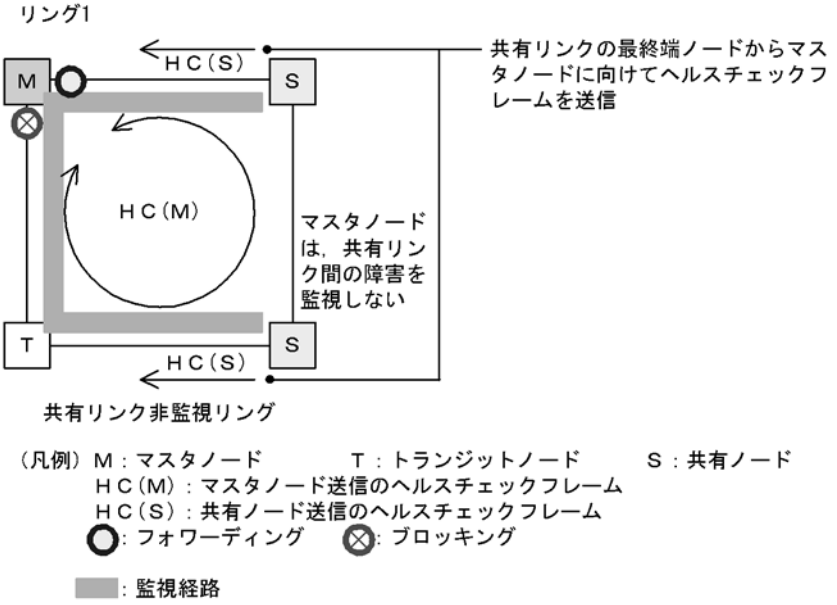
図 21-10　リング正常時の状態



(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 21-11　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。

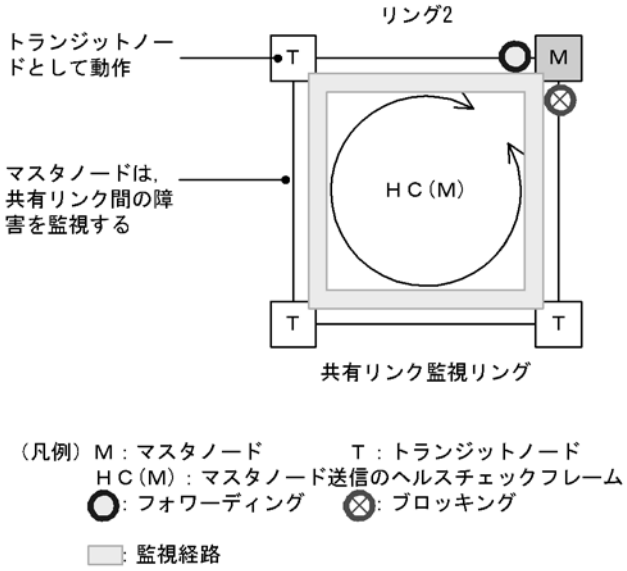
(c) 共有リンク非監視リングの最終端ノード動作

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 21-12 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。

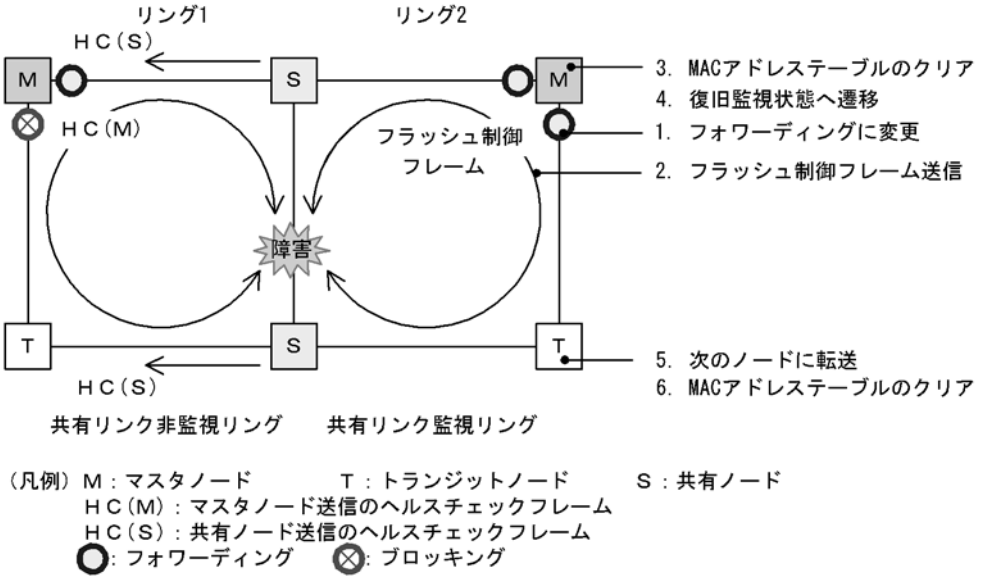
21.4.2 共有リンク障害・復旧時の動作

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 21-13 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

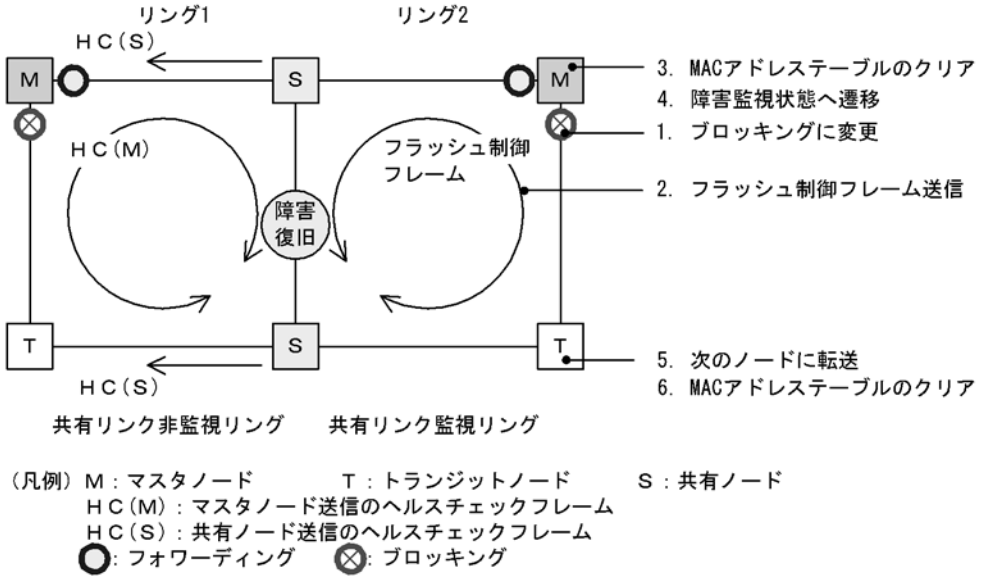
(c) 共有リンク非監視リングのマスタノードおよびトランジットノード動作

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 21-14 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。

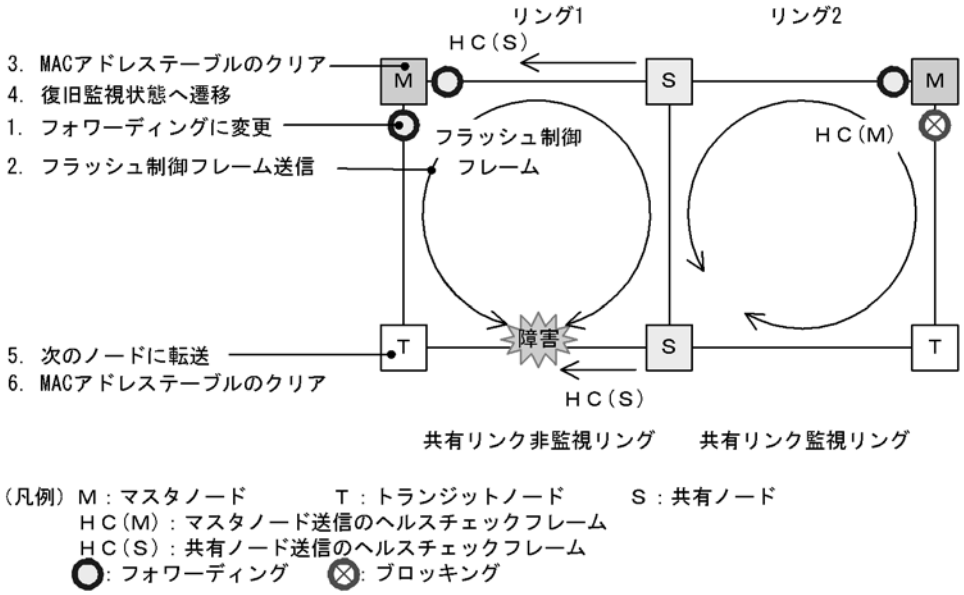
21.4.3 共有リンク非監視リングでの共有リンク以外の障害・復旧時の動作

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 21-15 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

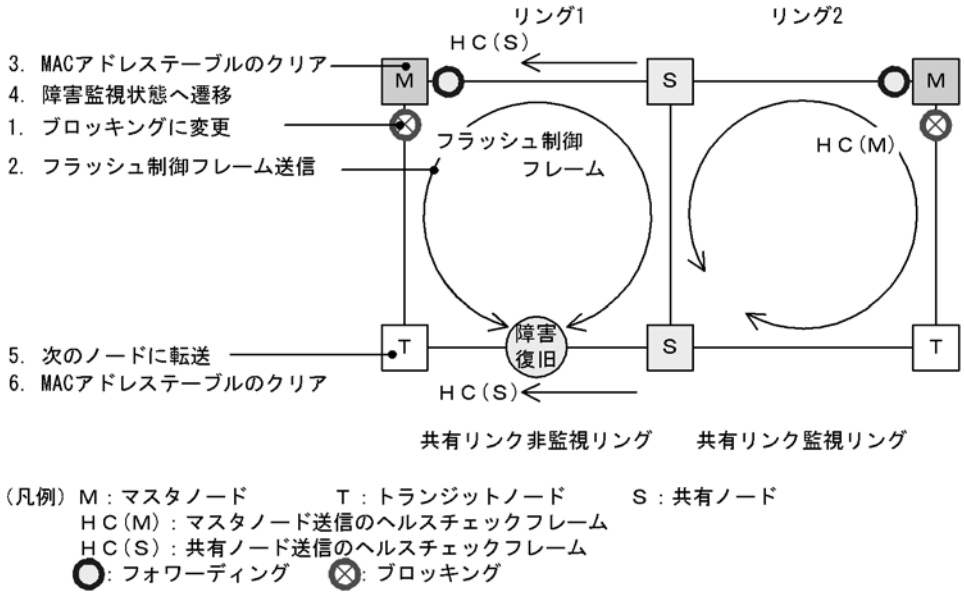
(c) 共有リンク監視リングのマスタノードおよびトランジットノード動作

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 21-16 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。

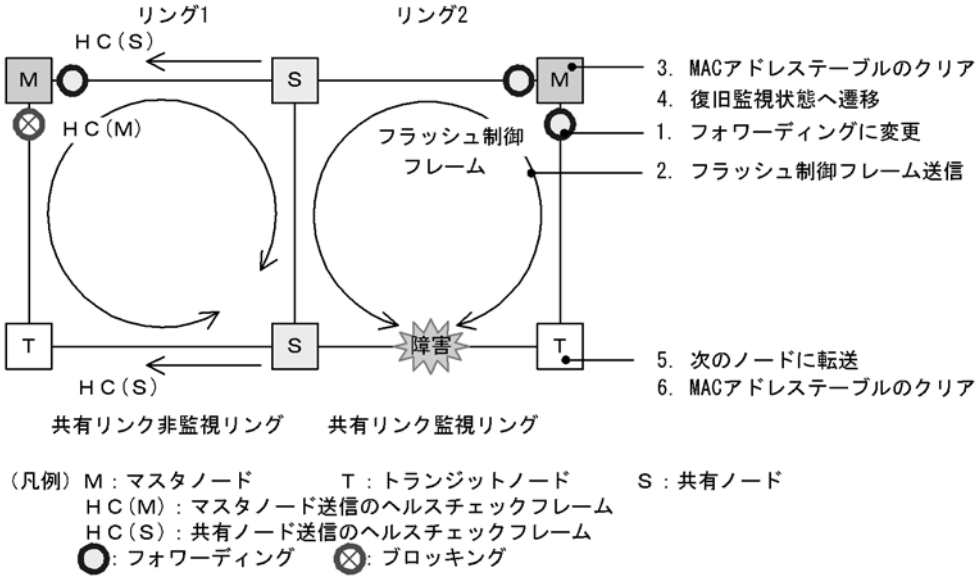
21.4.4 共有リンク監視リングでの共有リンク以外の障害・復旧時の動作

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 21-17　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

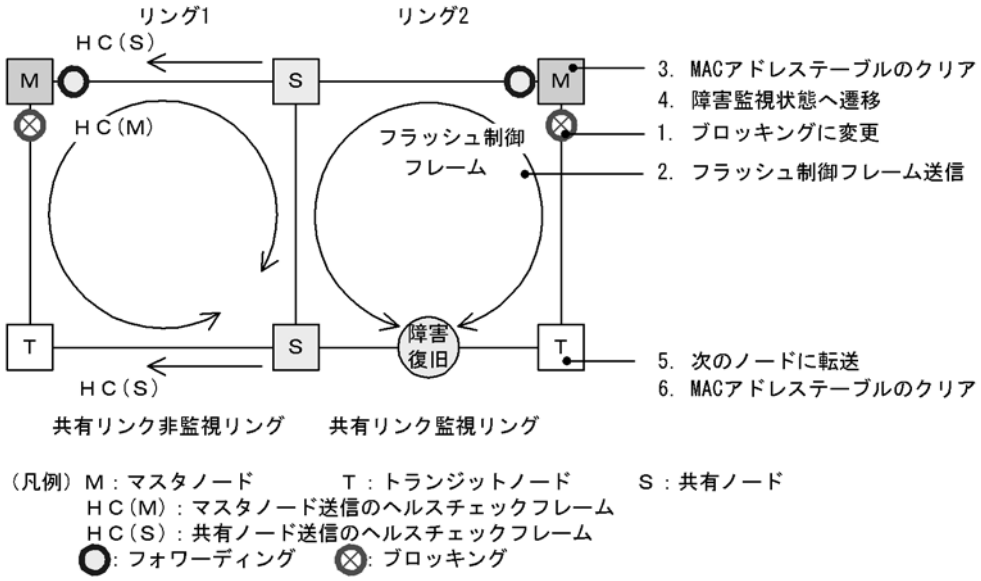
(c) 共有リンク非監視リングのマスタノードおよびトランジットノード（共有ノード）動作

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 21-18 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。

21.5 Ring Protocol の多重障害監視機能

21.5.1 概要

多重障害監視機能は，共有リンクありのマルチリング構成での共有リンク監視リングの多重障害を監視して，多重障害を検出した場合に共有リンク非監視リングに経路を切り替える機能です。このとき，経路の切り替えに使用する共有リンク非監視リングを**バックアップリング**と呼びます。

多重障害監視機能で検出の対象となるのは，共有リンク障害と，共有リンク監視リング内のその他のリンク障害およびリンク障害を伴う装置障害です。

共有リンク監視リングでの障害発生例と，多重障害監視機能で検出できる障害の組み合わせを次に示します。

なお，本装置はトランジットノード（最終端ノードを除く）だけサポートしています。

図 21-19 共有リンク監視リングでの障害発生例

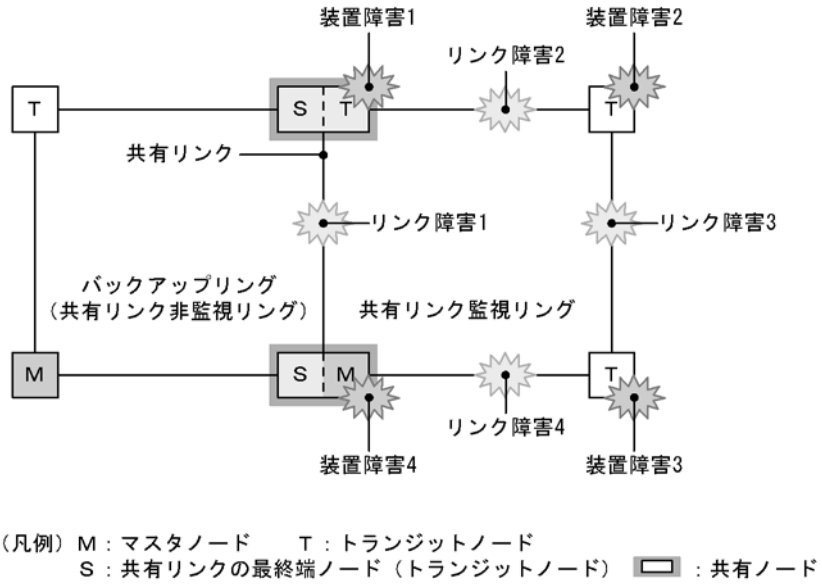


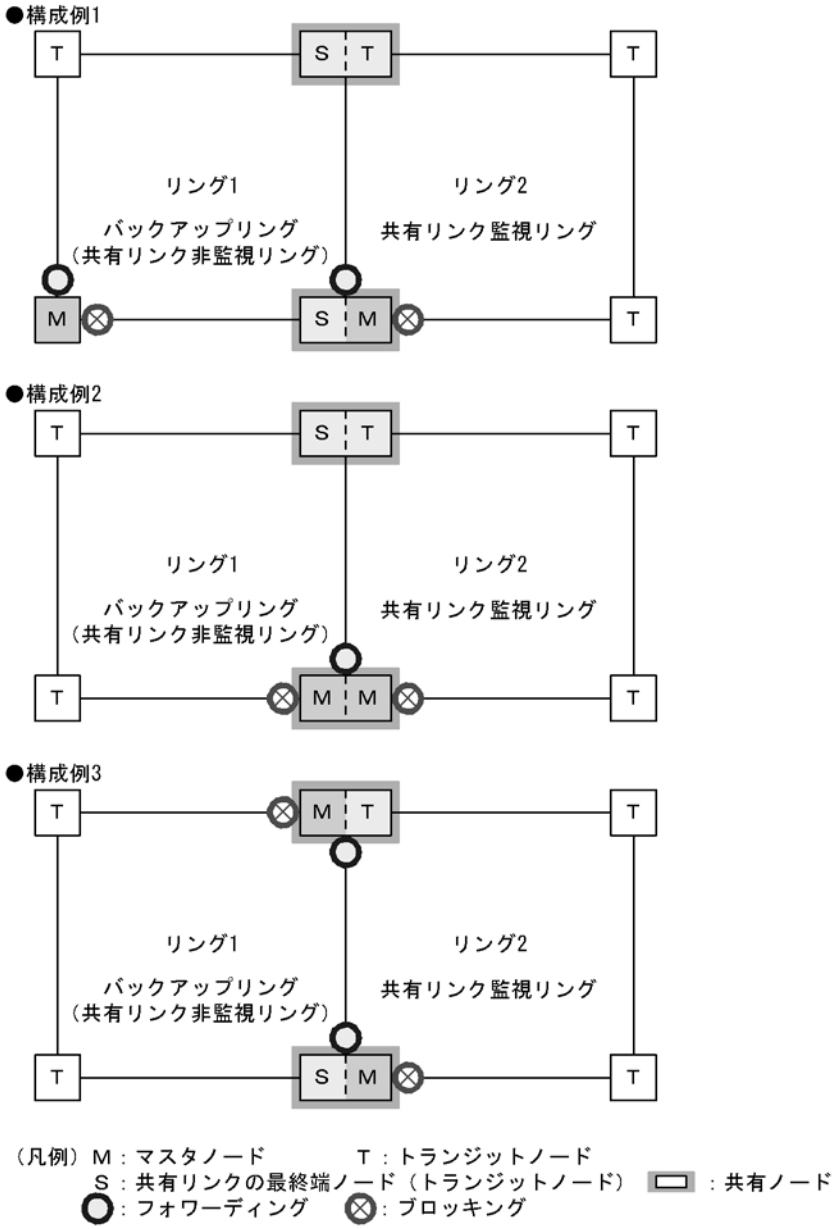
表 21-4 多重障害監視機能で検出できる障害の組み合わせ

障害種別	検出可能な組み合わせ	
リンク障害	リンク障害 1（共有リンク障害）	リンク障害 2（その他のリンク障害）
	リンク障害 1（共有リンク障害）	リンク障害 3（その他のリンク障害）
	リンク障害 1（共有リンク障害）	リンク障害 4（その他のリンク障害）
装置障害	装置障害 1（共有ノード障害）だけ	
	装置障害 4（共有ノード障害）だけ	
	装置障害 2（トランジットノード障害）	リンク障害 1（共有リンク障害）
	装置障害 3（トランジットノード障害）	リンク障害 1（共有リンク障害）

21.5.2　多重障害監視機能の基本構成

多重障害監視機能を適用できる共有リンクありのマルチリング構成は，共有リンク監視リングとバックアップリングとなる共有リンク非監視リングをそれぞれ 1 リングずつ対応づけた構成です。このとき，共有ノードを共有リンク監視リングのマスタノードとして設定します。多重障害監視機能の基本構成例を次の図に示します。

図 21-20　多重障害監視機能の基本構成例



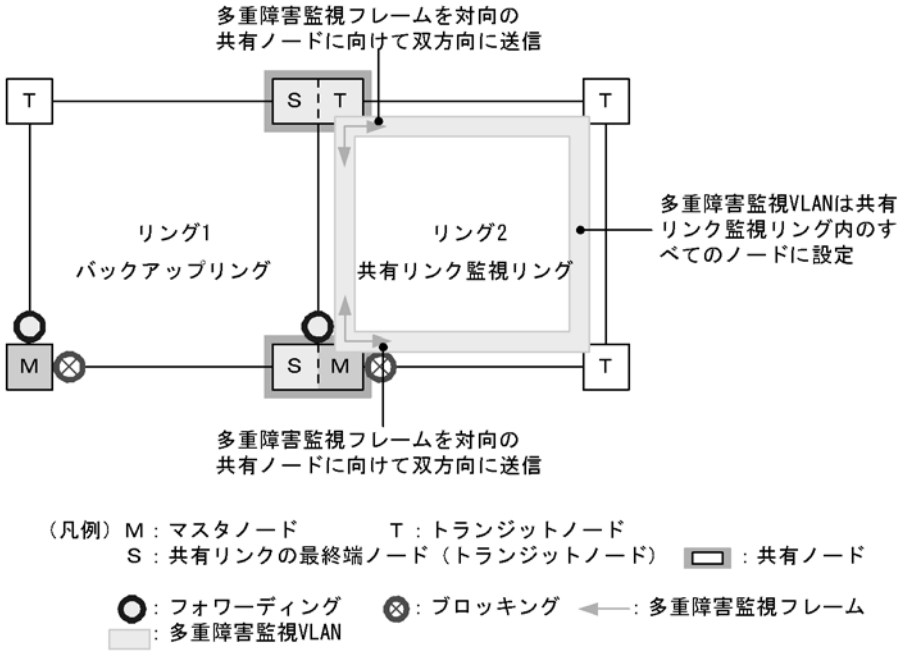
21.5.3 多重障害監視の動作概要

多重障害は，共有リンクありのマルチリング構成で共有リンクの両端に位置する共有ノードで監視します。共有ノードは，共有リンク監視リングの多重障害を監視するための制御フレーム（**多重障害監視フレーム**と呼びます）を送信します。対向の共有ノードでは，多重障害監視フレームの受信を監視します。なお，多重障害監視フレームは専用の VLAN（**多重障害監視** VLAN と呼びます）上に送信します。

本装置は多重障害監視フレームの受信・中継，および MAC アドレステーブルクリアをサポートします。

多重障害監視の動作概要を次の図に示します。

図 21-21 **多重障害監視の動作概要**



(1) 共有リンク監視リングの各ノードの動作

共有リンク監視リングのマスタノードおよびトランジットノードの動作は，マルチリング時の動作と同様ですので，「21.4.1　リング正常時の動作（2）共有リンク監視リング」を参照してください。

共有ノードでは，共有リンク監視リングの多重障害を監視します。共有ノードは，多重障害監視フレームを両リングポートから送信するとともに，対向の共有ノードが両リングポートから送信した多重障害監視フレームをあらかじめ設定した時間内に受信するかを監視します。

(2) バックアップリングの各ノードの動作

バックアップリングのマスタノードおよびトランジットノードの動作は，マルチリング時の動作と同様ですので，「21.4.1　リング正常時の動作（1）共有リンク非監視リング」を参照してください。

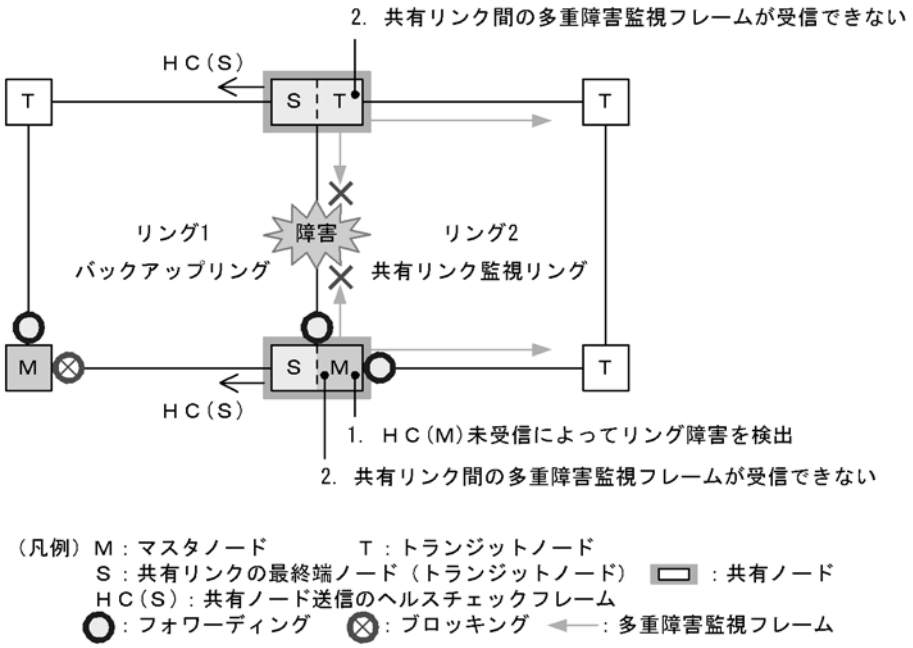
21.5.4 多重障害発生時の動作

共有リンク監視リングで，共有リンク障害とその他のリンク障害による多重障害が発生した場合の動作について説明します。

(1) 共有リンク障害時の動作

共有リンク監視リングでの共有リンク障害時の動作について，次の図に示します。

図 21-22 共有リンク障害時の動作



(a) 共有リンク監視リングの各ノードの動作

1. **HC(M) 未受信によってリング障害を検出**

   マスタノードは両方向の HC(M) を受信できなくなり，リング障害を検出します。リング障害検出時のマスタノードおよびトランジットノードの動作は，マルチリング時の動作と同様ですので，「21.4.2 共有リンク障害・復旧時の動作 (1) 障害検出時の動作」を参照してください。

2. **共有リンク間の多重障害監視フレームが受信できない**

   共有ノードは共有リンク間での多重障害監視フレームの受信ができなくなりますが，もう一方のリングポートでは受信できているため，多重障害の監視を継続します。

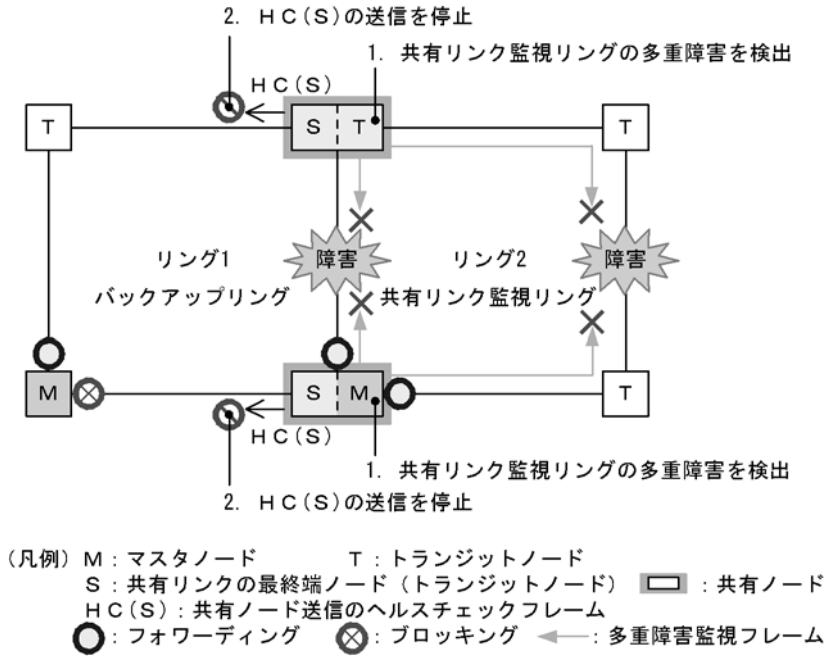
(b) バックアップリングの各ノードの動作

バックアップリングではマスタノードが送信した HC(M) の受信はできなくなりますが，共有ノードが送信した HC(S) は受信できているため，障害検出時の動作は行いません。

(2) 多重障害発生時の動作

共有リンク障害と共有リンク監視リング内のその他のリンク障害による多重障害発生時の動作について，次の図に示します。

図 21-23 多重障害発生時の動作



(a) 共有リンク監視リングの各ノードの動作

1. **共有リンク監視リングの多重障害を検出**

共有ノードは両リングポートで多重障害監視フレームを受信できなくなり，多重障害を検出します。

(b) バックアップリングの各ノードの動作

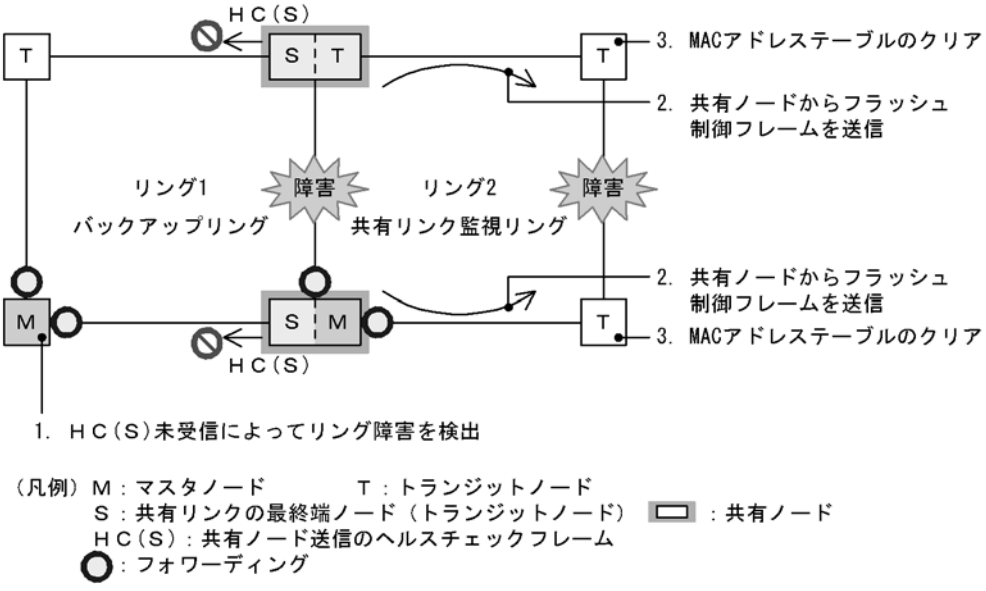
2. **HC(S) の送信を停止**

多重障害を検出した共有ノードは，バックアップリングの HC(S) の送信を停止します。

(3) バックアップリングへの切り替え動作

多重障害検出によるバックアップリングへの切り替え動作について，次の図に示します。

図 21-24 バックアップリングへの切り替え動作



(a) バックアップリングの各ノードの動作

1. HC(S) **未受信によってリング障害を検出**
   マスタノードは自身が送信した両方向の HC(M) と共有ノードが送信した HC(S) がどちらも未受信となり，リング障害を検出します。リング障害検出時のマスタノードおよびトランジットノードの動作は，マルチリング時の動作と同様ですので，「21.4.3　共有リンク非監視リングでの共有リンク以外の障害・復旧時の動作（1）障害検出時の動作」を参照してください。

(b) 共有リンク監視リングの各ノードの動作

2. **共有ノードからフラッシュ制御フレームを送信**
   バックアップリングのマスタノードから送信されたフラッシュ制御フレームを受信すると，共有ノードは共有リンク監視リングに向けて，MAC アドレステーブルのクリアだけをするフラッシュ制御フレームを送信します。

3. MAC **アドレステーブルのクリア**
   トランジットノードは共有ノードから送信されたフラッシュ制御フレームを受信して，MAC アドレステーブルをクリアします。

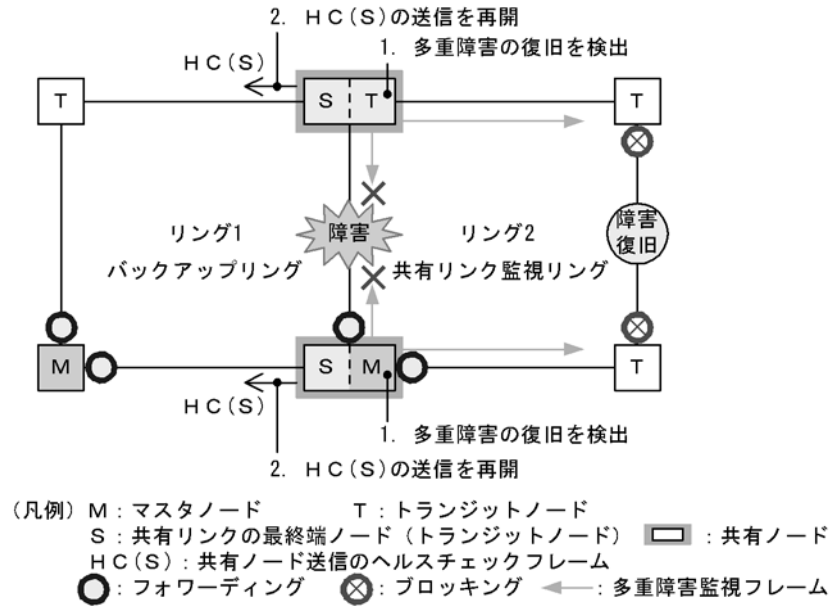
21.5.5　多重障害復旧時の動作

共有リンク監視リングでの多重障害が復旧した場合の動作について説明します。

(1) 多重障害からの一部復旧時の動作

共有リンク監視リングで多重障害からの一部復旧時の動作について，次の図に示します。

図 21-25　**多重障害からの一部復旧時の動作**



(a) 共有リンク監視リングの各ノードの動作

1. **多重障害の復旧を検出**
   共有ノードは対向の共有ノードが送信した多重障害監視フレームを受信して，多重障害の復旧を検出します。

(b) バックアップリングの各ノードの動作

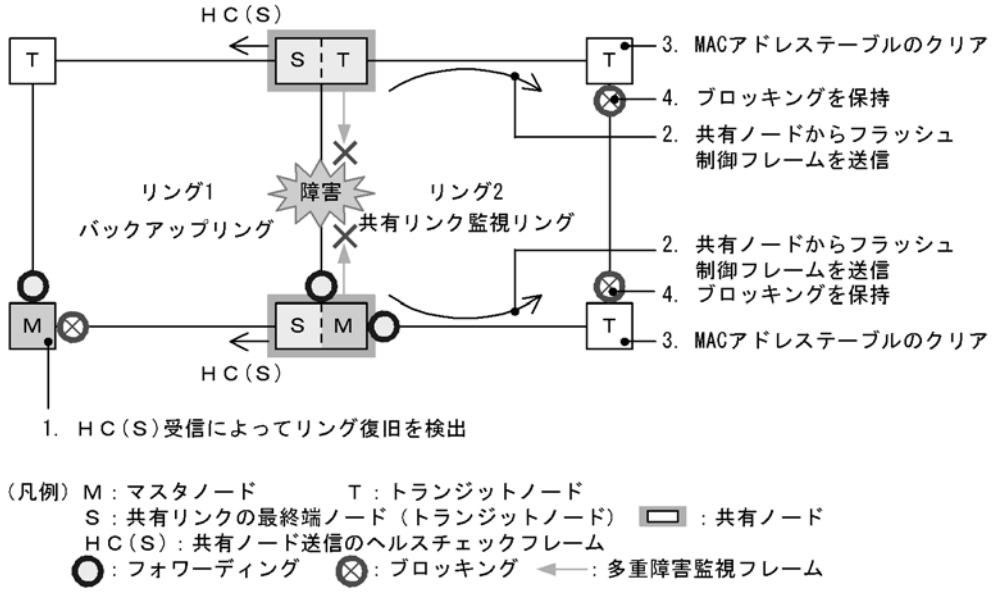
2. HC(S) の送信を再開

多重障害の復旧を検出した共有ノードは，バックアップリングの HC(S) の送信を再開します。

(2) バックアップリングからの切り戻し動作

バックアップリングからの切り戻し動作について，次の図に示します。

図 21-26 バックアップリングからの切り戻し動作



(a) バックアップリングの各ノードの動作

1. HC(S) 受信によってリング復旧を検出

マスタノードは共有ノードが送信した HC(S) を両方向から受信すると，リング障害が復旧したと判断して復旧動作を行います。復旧検出時のマスタノードおよびトランジットノードの動作は，マルチリング時の動作と同様ですので，「21.4.3　共有リンク非監視リングでの共有リンク以外の障害・復旧時の動作（2）復旧検出時の動作」を参照してください。

(b) 共有リンク監視リングの各ノードの動作

2. 共有ノードからフラッシュ制御フレームを送信

バックアップリングのマスタノードから送信されたフラッシュ制御フレームを受信すると，共有ノードは共有リンク監視リングに向けて，MAC アドレステーブルのクリアだけをするフラッシュ制御フレームを送信します。

3. MAC アドレステーブルのクリア

トランジットノードは共有ノードから送信されたフラッシュ制御フレームを受信して，MAC アドレステーブルをクリアします。

4. ブロッキングを保持

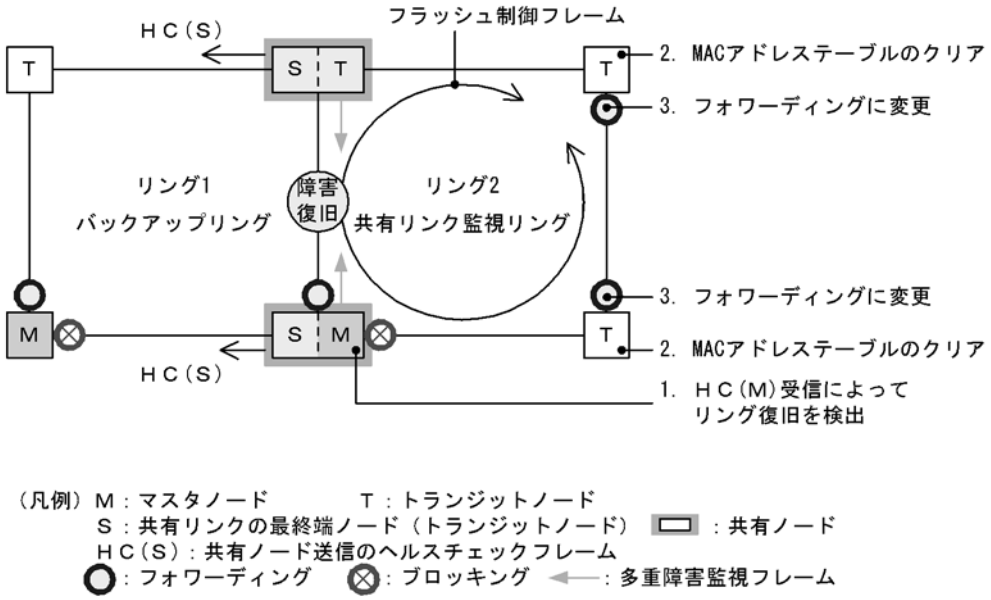
リンク障害から復旧したリングポートのリング VLAN 状態は，マスタノードがリング復旧を検出していないため，ブロッキングを保持します。

なお，ブロッキングの解除については「21.7　Ring Protocol 使用時の注意事項　(11) 多重障害の一部復旧時の通信について」を参照してください。

（3） 共有リンク障害復旧時の動作

共有リンク障害復旧時の動作について，次の図に示します。

図 21-27　共有リンク障害復旧時の動作



（a） 共有リンク監視リングの各ノードの動作

1. HC(M) **受信によってリング復旧を検出**

   マスタノードは自身が送信した HC(M) を受信すると，リング障害が復旧したと判断して復旧動作を行います。復旧検出時のマスタノードおよびトランジットノードの動作は，マルチリング時の動作と同様ですので，「21.4.2　共有リンク障害・復旧時の動作　（2）復旧検出時の動作」を参照してください。

2. MAC **アドレステーブルのクリア**

   トランジットノードはマスタノードから送信されたフラッシュ制御フレームを受信して，MAC アドレステーブルをクリアします。

3. **フォワーディングに変更**

   トランジットノードはマスタノードが送信したフラッシュ制御フレームの受信によって，リンク障害から復旧したリングポートのリング VLAN 状態をフォワーディングに変更します。

21.6 Ring Protocol のネットワーク設計

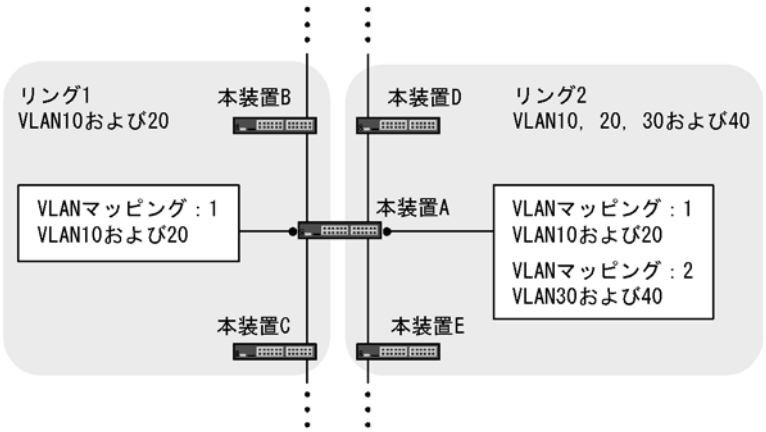
21.6.1 VLAN マッピングの使用方法

(1) VLAN マッピングとデータ転送用 VLAN

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

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

図 21-28 リングごとの VLAN マッピングの割り当て例



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

トランジットノードの装置起動で，Ring Protocol が初期状態から動作する場合，データ転送用 VLAN は論理ブロックされています。トランジットノードは，マスタノードが送信するフラッシュ制御フレームを受信することでこの論理ブロックを解除します。しかし，装置再起動時で，マスタノードの障害監視時間（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。

21.6.3 Ring Protocol の禁止構成

禁止構成については，マスタノード側のマニュアルを参照してください。

21.6.4 多重障害監視機能の禁止構成

禁止構成については，マスタノード側のマニュアルを参照してください。

21.7 Ring Protocol 使用時の注意事項

(1) 他機能との共存

「16.3 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。

なお，デフォルト VLAN（VLAN ID=1）は設定できません。

(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。従って，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，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. 制御 VLAN（コンフィグレーションコマンド control-vlan），およびデータ転送用 VLAN（コンフィグレーションコマンド axrp vlan-mapping，vlan-group）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。

(7) 相互運用

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

(8) ネットワーク内の多重障害時について

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

なお，多重障害監視機能を適用すると，障害の組み合わせによっては多重障害を検出できる場合があります。多重障害監視機能については，「21.5 Ring Protocol の多重障害監視機能」を参照してください。

(9) 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

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。

(10) 多重障害監視機能の監視開始タイミングについて

共有ノードでは，多重障害監視機能を適用したあと，対向の共有ノードが送信する多重障害監視フレームを最初に受信したときに多重障害の監視を開始します。このため，多重障害監視機能を設定するときにリングネットワークに障害が発生していると，多重障害の監視を開始できません。多重障害監視機能は，リングネットワークが正常な状態で設定してください。

(11) 多重障害の一部復旧時の通信について

多重障害の一部復旧時はマスタノードがリング復旧を検出しないため，トランジットノードのリングポートはフラッシュ制御フレームの受信待ち保護時間（forwarding-shift-time）が経過するまでの間，論理ブロック状態となります。論理ブロック状態を解除したい場合は，フラッシュ制御フレーム受信待ち保護時間（初期値：10 秒）を短くするか，残りのリンク障害を復旧してマスタノードにリング復旧を検出させてください。なお，フラッシュ制御フレームの受信待ち保護時間を設定するときは，マスタノードの多重障害監視フレームの送信間隔（コンフィグレーションコマンド multi-fault-detection interval）よりも大きい値を設定してください。小さい値を設定すると，一時的にループが発生するおそれがあります。

(12) リングポートに指定したリンクアグリゲーションのダウンについて

リングネットワークを構成するノード間をリンクアグリゲーション（スタティックモードまたは LACP モード）で接続していた場合，リンクアグリゲーションの該当チャネルグループをコンフィグレーションコマンド shutdown でダウン状態にするときは，あらかじめチャネルグループに属するすべての物理ポートをコンフィグレーションコマンド shutdown でダウン状態に設定してください。

なお，該当チャネルグループをコンフィグレーションコマンド no shutdown でアップ状態にするときは，あらかじめチャネルグループに属するすべての物理ポートをコンフィグレーションコマンド shutdown でダウン状態に設定してください。

22 Ring Protocol の設定と運用【S2200】【SS1250】【SS1240】

この章では，Ring Protocol の設定例について説明します。

22.1 コンフィグレーション

22.2 オペレーション

22.1 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。

22.1.1 コンフィグレーションコマンド一覧

本装置で設定する 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 22-1 コンフィグレーションコマンド一覧

コマンド名	説明
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-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。
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。
mode	リングでの動作モードを設定します。
multi-fault-detection mode	多重障害監視の監視モードを設定します。
multi-fault-detection vlan	多重障害監視 VLAN として使用する VLAN を設定します。
name	リングを識別するための名称を設定します。
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。

22.1.2 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してください。スパニングツリーの停止については，「20　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
- フラッシュ制御フレーム受信待ち保護時間

22.1.3 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。

22.1.4 制御 VLAN の設定

(1) 制御 VLAN の設定

[設定のポイント]

制御 VLAN として使用する VLAN を指定します。なお，下記に該当する VLAN は設定できません。

- データ転送用 VLAN に使用されている VLAN
- 異なるリングで使用されている VLAN ID と同じ値の VLAN ID
- デフォルト VLAN（VLAN=1）

[コマンドによる設定]

1. **(config)# axrp 1**
   リング ID 1 の axrp コンフィグレーションモードに移行します。

2. **(config-axrp)# control-vlan 2**
   (config-axrp)# exit
   制御 VLAN として VLAN2 を指定します。

(2) 制御 VLAN のフォワーディング遷移時間の設定

[設定のポイント]

Ring Protocol が初期状態の場合に，トランジットノードでの制御 VLAN のフォワーディング遷移時間を設定します。トランジットノードでの制御 VLAN のフォワーディング遷移時間（forwarding-delay-time パラメータでの設定値）は，マスタノードでのヘルスチェックフレームの保護時間（コンフィグレーションコマンド health-check holdtime 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（コンフィグレーションコマンド forwarding-shift-time 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。

22.1.5 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。

22.1.6 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。

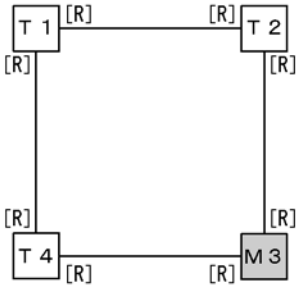
[コマンドによる設定]

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。

22.1.7 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）

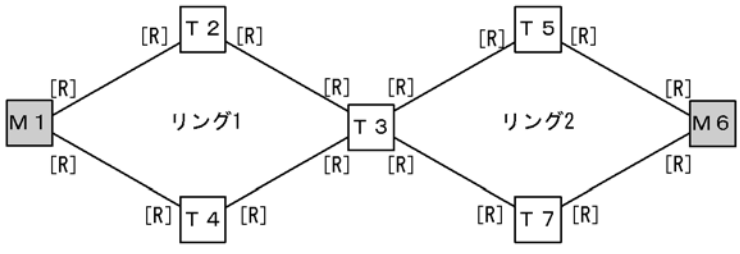
シングルリング構成を「図 22-1　シングルリング構成」に，共有リンクなしマルチリング構成を「図 22-2　共有リンクなしマルチリング構成」に示します。

図 22-1　シングルリング構成



（凡例）　M：マスタノード　　T：トランジットノード
[R]：リングポート

図 22-2　共有リンクなしマルチリング構成



（凡例）　M：マスタノード　　T：トランジットノード
[R]：リングポート

本装置はトランジットノードだけをサポートしており，本マニュアルでは本装置のトランジットノードについて説明します。マスタノードの詳細については，マスタノードをサポートしている IP8800 シリーズのマニュアルを参照してください。

(1) 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 22-1　シングルリング構成」では T1，T2 および T4 ノード，「図 22-2　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 fastethernet 0/1
(config-if)# axrp-ring-port 2
(config-if)# exit
(config)# interface fastethernet 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。

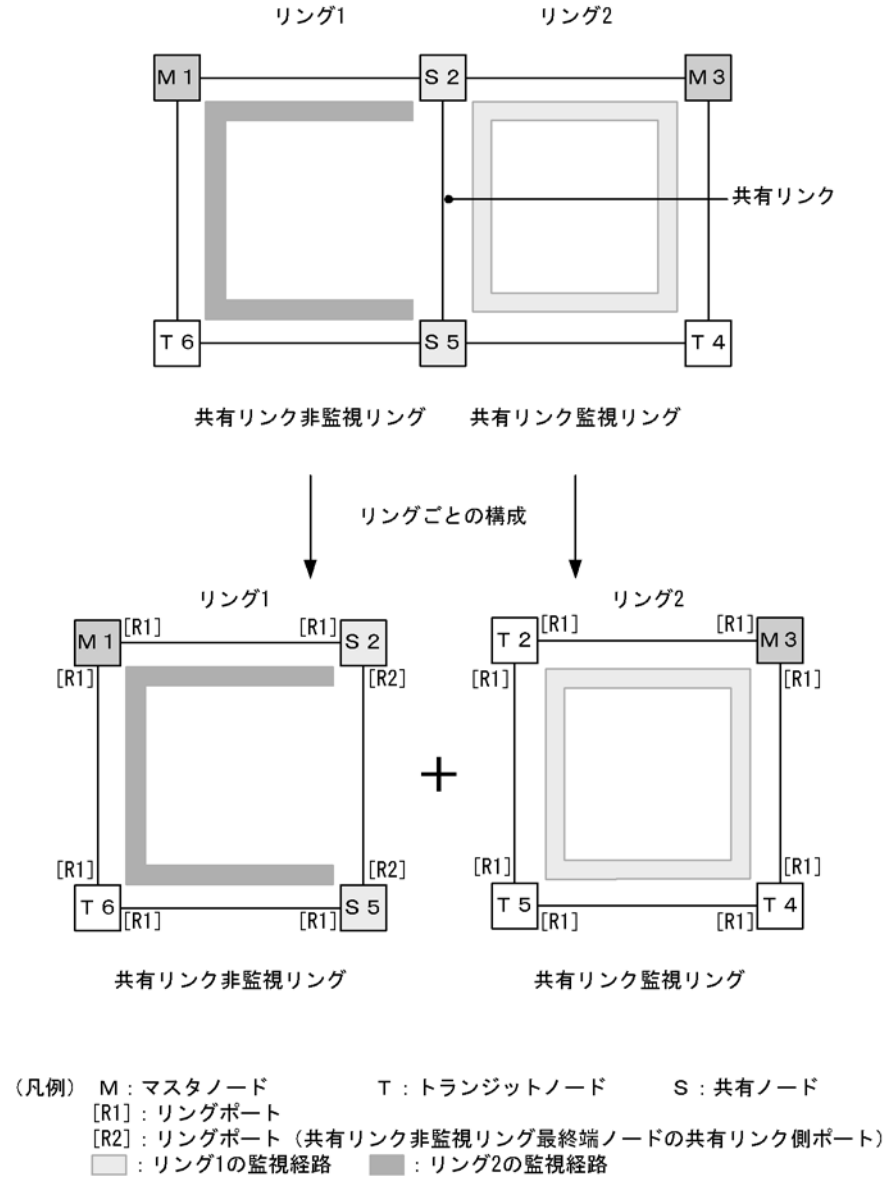
22.1.8 モードとリングポートに関する設定（共有リンクありマルチリング構成）

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 22-3　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。「22.1.7　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) トランジットノード」を参照してください。「図 22-3　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。

(b) 共有リンク非監視リングのトランジットノード

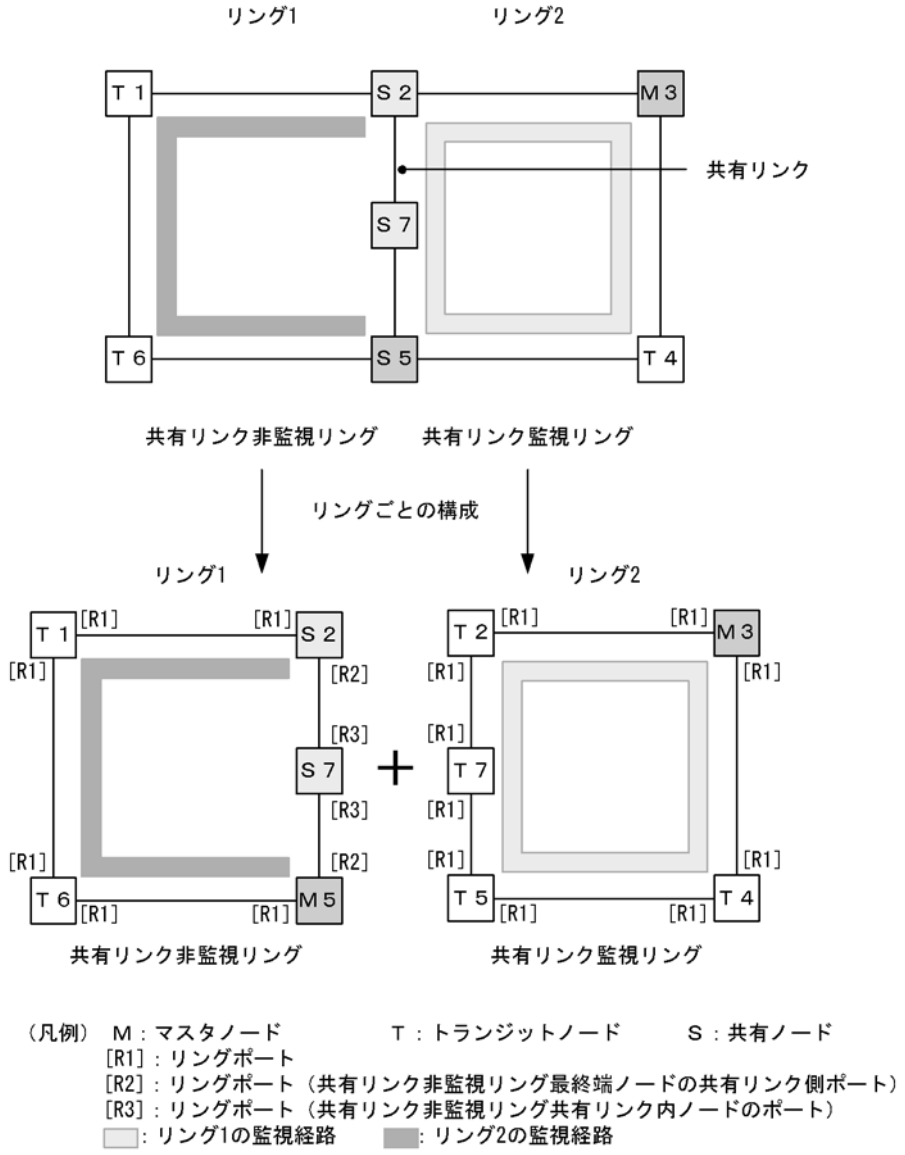
シングルリングのトランジットノード設定と同様です。「22.1.7　モードとリングポートに関する設定（シングルリングと共有リンクなしマルチリング構成）(1) トランジットノード」を参照してください。「図 22-3　共有リンクありマルチリング構成（基本構成）」では T6 ノードがこれに該当します。

(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 22-4　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 22-4　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 22-4　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 fastethernet 0/1
(config-if)# axrp-ring-port 1 shared
(config-if)# exit
(config)# interface fastethernet 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。

22.1.9 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) 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。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。

22.1.10 多重障害監視機能の設定

(1) 多重障害監視 VLAN の設定

[設定のポイント]

共有リンク監視リングの各ノードに多重障害監視 VLAN として使用する VLAN を設定します。なお，制御 VLAN とデータ転送用 VLAN に使われている VLAN は使用できません。また，異なるリングで使用されている多重障害監視 VLAN の VLAN ID と同じ値の VLAN ID は使用できません。

[コマンドによる設定]

1. **(config)# axrp 1**
   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)# multi-fault-detection vlan 20**
   (config-axrp)# exit
   多重障害監視 VLAN として VLAN 20 を設定します。

[注意事項]

多重障害監視 VLAN は多重障害監視機能を適用する共有リンク監視リングのすべてのノードに設定してください。

(2) 多重障害監視機能の監視モードの設定

[設定のポイント]

本装置の監視モードに transport-only を設定します。(本装置は transport-only だけをサポートしています。)

[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)# multi-fault-detection mode transport-only**
   (config-axrp)# exit
   多重障害監視の監視モードを transport-only に設定します。

22.2 オペレーション

22.2.1 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 22-2 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。
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。

22.2.2 Ring Protocol の状態確認

(1) コンフィグレーション設定と運用の状態確認

運用コマンド show axrp で Ring Protocol の設定と運用状態を確認できます。コンフィグレーションコマンドで設定した Ring Protocol の設定内容が正しく反映されているかどうかを確認してください。リング単位の状態情報確認には運用コマンド show axrp <Ring ID list> を使用できます。

表示される情報は，項目 "Oper State" の内容により異なります。"Oper State" に "enable" が表示されている場合は Ring Protocol 機能が動作しています。このとき，表示内容は全項目について運用の状態を示しています。"Oper State" に "-" が表示されている場合は必須であるコンフィグレーションコマンドが揃っていない状態です。また，"Oper State" に "Not Operating" が表示されている場合，コンフィグレーションに矛盾があるなどの理由で，Ring Protocol 機能が動作できていない状態です。"Oper State" の表示状態が "-"，または "Not Operating" 時には，コンフィグレーションを確認してください。

運用コマンド show axrp，運用コマンド show axrp detail の表示例を次に示します。

図 22-5 show axrp の実行結果

```
> show axrp

Date 20XX/09/01 15:34:11 UTC
Total Ring Counts:1

Ring ID:2
 Name:O-Ring
 Oper State:enable           Mode:Transit

 VLAN Group ID  Ring Port  Role/State            Ring Port  Role/State
 1              0/25       -/forwarding          0/26       -/forwarding
 2              -          -/-                   -          -/-

>
```

運用コマンド show axrp detail を使用すると，リング状態などについての詳細情報を確認できます。

図 22-6 show axrp detail の実行結果

```
> show axrp detail

Date 20XX/09/01 15:35:15 UTC
Total Ring Counts:1

Ring ID:2
 Name:O-Ring
 Oper State:enable           Mode:Transit
 Control VLAN ID:20
 Forwarding Shift Time (sec):15
 Last Forwarding:flush request receive

 VLAN Group ID:1
  VLAN ID:200
  Ring Port:0/25        Role:-            State:forwarding
  Ring Port:0/26        Role:-            State:forwarding

 VLAN Group ID:2
  VLAN ID:-
  Ring Port:-           Role:-            State:-
  Ring Port:-           Role:-            State:-

 Multi Fault Detection State:-
  Mode:transport
  Control VLAN ID:1000

>
```

23 Ring Protocol とスパニングツリー / GSRP の併用【S2200】【SS1250】【SS1240】

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。

23.1 Ring Protocol とスパニングツリーとの併用

23.2 Ring Protocol と GSRP との併用

23.1 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せん。ただし，リング構成にスパニングツリーと併用する装置（IP8800/S2400,IP8800/S3600,IP8800/S6700 シリーズなど）が存在する場合，本装置をトランジットノードとしてリング構成に含めることができます。

23.1.1 概要

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する装置が存在する構成に，本装置をトランジットノードとして含んだ例を次の図に示します。他装置 A － F － G 間，B － E － H 間，C － D － I 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，他装置 A ～ F では，Ring Protocol とスパニングツリーが同時に動作しています。本装置①および本装置②は Ring Protocol(トランジットノード) だけの装置です。

図 23-1 Ring Protocol とスパニングツリーの併用例と本装置の位置づけ（シングルリング構成）

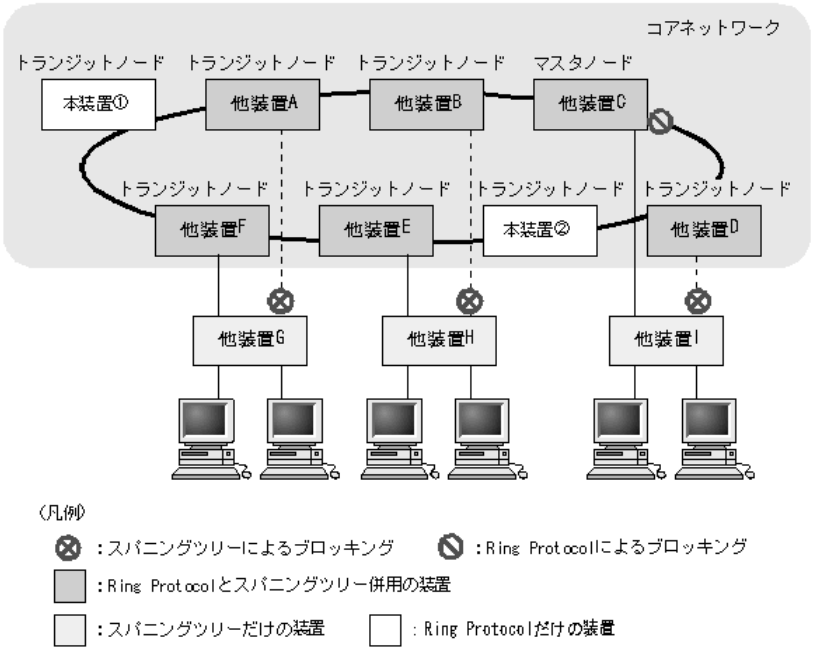
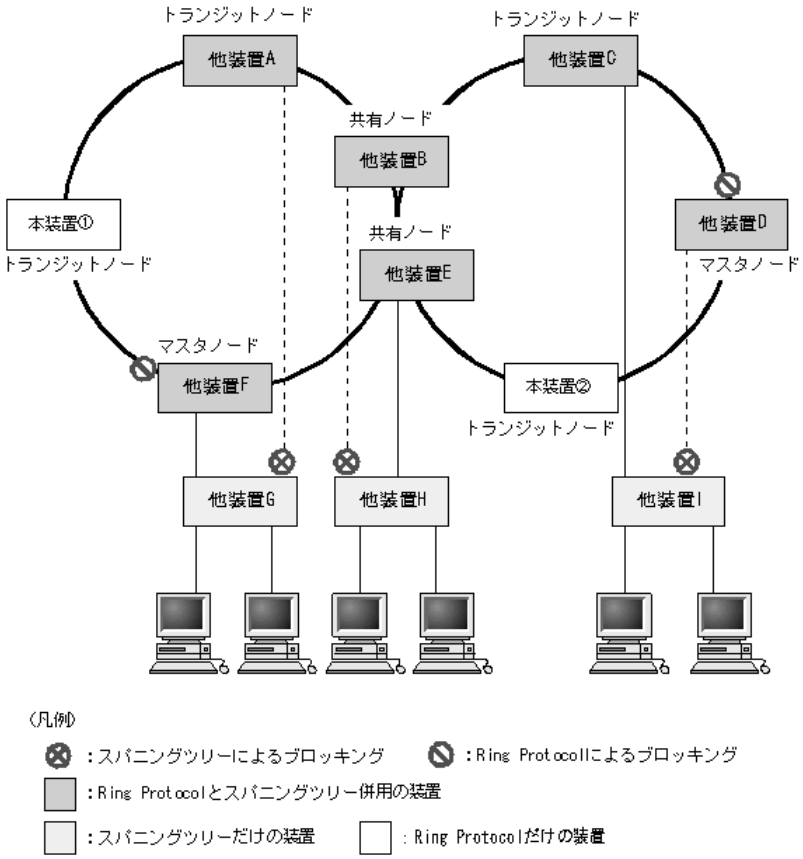


図 23-2 Ring Protocol とスパニングツリーの併用例と本装置の位置づけ（マルチリング構成）



本装置は，後述の仮想リンク制御フレームの中継と MAC アドレステーブルクリアだけを行います。Ring Protocol とスパニングツリーの併用動作および仮想リンクなどの詳細は，IP8800 シリーズのマニュアル (IP8800/S2400,IP8800/S3600,IP8800/S6700 など）を参照してください。

(1) スパニングツリーの仮想リンク制御フレームの中継

Ring Protocol とスパニングツリーを併用する装置では，二つの機能が共存している任意の 2 装置間を仮想リンクで接続されています。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。仮想リンク間の制御フレーム（仮想リンク制御フレーム）の送受信は，リングネットワーク上に設定された仮想 VLAN が使用されます。仮想 VLAN は，リングポートのデータ転送用 VLAN グループに所属する VLAN が使用されます。

リングネットワーク上に含まれる本装置は，仮想リンク制御フレームの中継だけを行います。

(2) 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は，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が仮想リンク VLAN を使用して送信されます。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。

リングネットワーク上に含まれる本装置も，フラッシュ制御フレームを受信すると，同様に MAC アドレステーブルエントリをクリアします。

23.2 Ring Protocol と GSRP との併用

本装置では，Ring Protocol と GSRP の併用ができません。ただし，リング構成に GSRP と併用する装置（IP8800/S2400,IP8800/S3600,IP8800/S6700 シリーズなど）が存在する場合，本装置をトランジットノードとしてリング構成に含めることができます。

23.2.1 動作概要

障害の監視や障害発生時の経路切り替えは，リングネットワークでは Ring Protocol で，GSRP ネットワークでは GSRP で，独立して実施します。ただし，GSRP ネットワークで経路の切り替え時にマスタに遷移した装置は，GSRP スイッチおよび aware/unaware 装置の MAC アドレステーブルをクリアします。同時に，リングネットワーク用のフラッシュ制御フレームを送信して，リングネットワークを構成する装置の MAC アドレステーブルもクリアします。

Ring Protocol と GSRP との併用例を次の図に示します。

図 23-3 Ring Protocol と GSRP の併用例と本装置の位置づけ（ダイレクトリンクをリングネットワークで使用する場合）

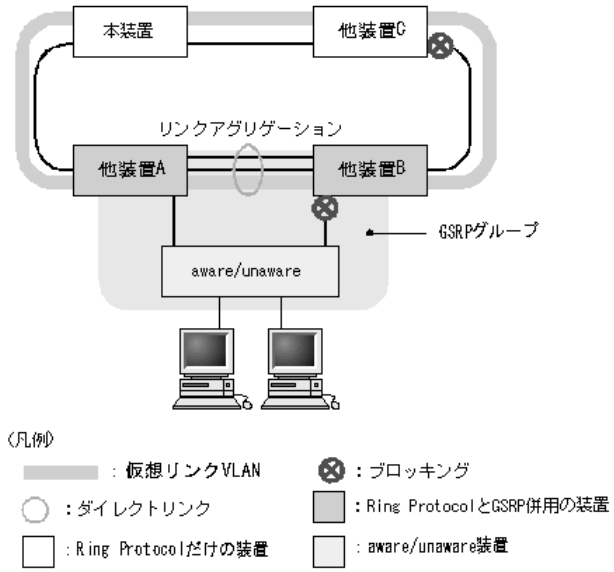
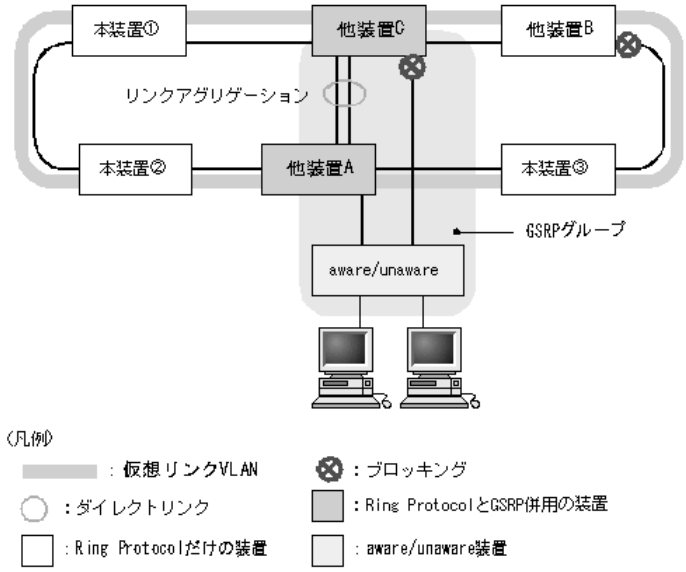


図 23-4 Ring Protocol と GSRP の併用例と本装置の位置づけ（ダイレクトリンクをリングネットワークで使用しない場合）



本装置は，後述の仮想リンク制御フレームの中継と MAC アドレステーブルクリアだけを行います。Ring Protocol と GSRP の併用動作および仮想リンクなどの詳細は，IP8800 シリーズのマニュアル (IP8800/S2400,IP8800/S3600,IP8800/S6700 など）を参照してください。

(1) GSRP の仮想リンク制御フレームの中継

Ring Protocol と GSRP を併用する装置では，前述の Ring Protocol とスパニングツリーの併用装置と同様に，2 装置間を仮想リンクで接続されています。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。仮想リンク制御フレームの送受信は，リングネットワーク上に設定された仮想 VLAN が使用されます。仮想 VLAN は，リングポートのデータ転送用 VLAN グループに所属する VLAN が使用されます。

リングネットワーク上に含まれる本装置は，仮想リンク制御フレームの中継だけを行います。

(2) GSRP ネットワーク切り替え時の MAC アドレステーブルクリア

GSRP ネットワークの経路切り替え時は，GSRP マスタからリングネットワークを構成する装置に対して，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が仮想リンク VLAN を使用して送信されます。これを受信したリングネットワーク内の各装置は，MAC アドレステーブルをクリアします。

リングネットワーク上に含まれる本装置も，フラッシュ制御フレームを受信すると，同様に MAC アドレステーブルエントリをクリアします。

24 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。

24.1 IGMP snooping/MLD snooping の概要

24.2 IGMP snooping/MLD snooping サポート機能

24.3 IGMP snooping

24.4 MLD snooping

24.5 IGMP snooping/MLD snooping 使用時の注意事項

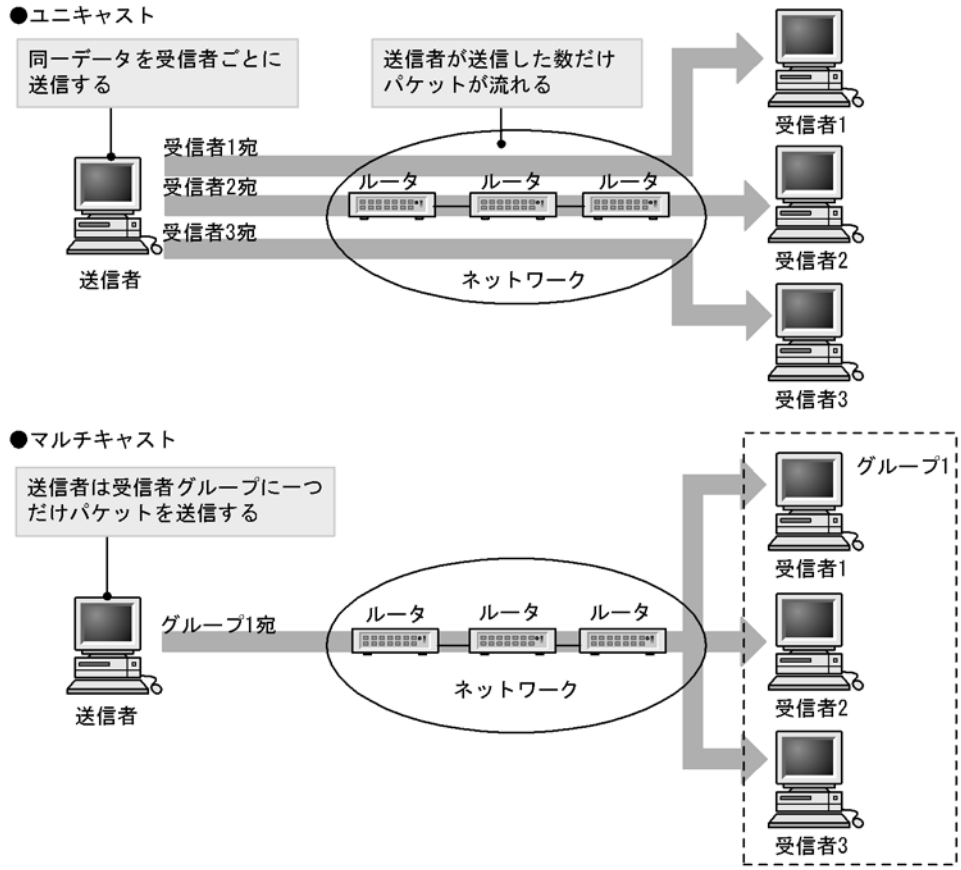
24.1 IGMP snooping/MLD snooping の概要

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。

24.1.1 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 24-1 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 24-1 マルチキャストグループアドレス

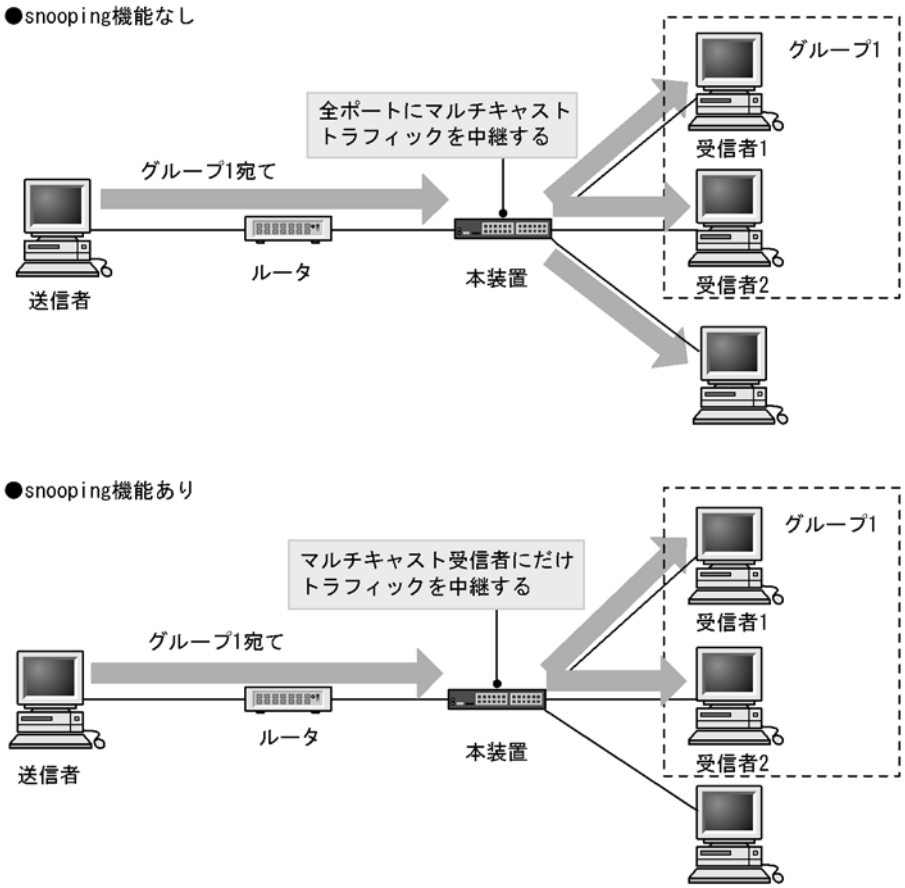
プロトコル	アドレス範囲
IPv4	224.0.0.0 ～ 239.255.255.255
IPv6	上位 8 ビットが ff(16 進数) となる IPv6 アドレス

24.1.2 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 24-2 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。

24.2 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 24-2 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 MLD: Version 1，2	－
この機能による学習 MAC アドレス範囲	IPv4	0100.5e00.0000 ～ 0100.5e7f.ffff	RFC1112 を参照
	IPv6	3333.0000.0000 ～ 3333.ffff.ffff	RFC2464 を参照
IGMP クエリア MLD クエリア		クエリア動作は IGMPv2，MLDv1，MLDv2 の仕様に従う	－
マルチキャストルータ接続ポートの設定		コンフィグレーションによる static 設定	－
IGMP 即時離脱機能		IGMPv2 Leave メッセージの受信による即時離脱	－

(凡例) －：該当なし

24.3 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。

IGMP snooping は MAC アドレス制御方式でマルチキャストトラフィックの中継制御を行います。

24.3.1 MAC アドレス制御方式

(1) MAC アドレスの学習

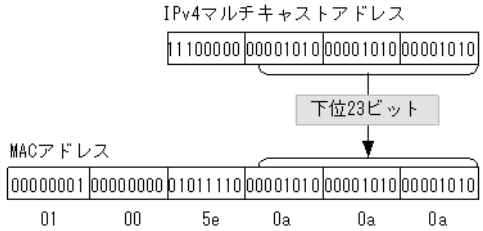
IGMP snooping が設定された VLAN で IGMP メッセージを受信することによってマルチキャスト MAC アドレスをダイナミックに学習します。学習したマルチキャスト MAC アドレスは MAC アドレステーブルに登録します。

(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 Report メッセージを受信したポートにだけマルチキャストグループ宛のトラフィックを転送するエントリを作成します。

IPv4 マルチキャストデータの宛先 MAC アドレスは IP アドレスの下位 23 ビットを MAC アドレスにコピーして生成します。そのため，下位 23 ビットが同じ IP アドレスは MAC アドレスが重複します。例えば，224.10.10.10 と 225.10.10.10 はどちらもマルチキャスト MAC アドレスは 0100.5E0A.0A0A となります。これらのアドレスについては，レイヤ 2 中継で同一 MAC アドレス宛のパケットとして取り扱います。IPv4 マルチキャストアドレスと MAC アドレスの対応を次の図に示します。

図 24-3 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 アドレスは次の二つ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。
  IGMP 即時離脱機能を使用している場合は，IGMPv2 Leave メッセージを受信すると，エントリから該当ポートをすぐに削除します。クエリアを設定していても，Group-Specific Query メッセージは送信しません。

- IGMPv1/IGMPv2 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 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。

(2) IPv4 マルチキャストパケットのレイヤ 2 中継

IPv4 マルチキャストパケットの受信 VLAN 内のレイヤ 2 中継は MAC アドレスベースで処理します。IGMP snooping の結果によってレイヤ 2 中継は，同一 MAC アドレスにマッピングされる IP マルチキャストアドレスの IGMP Report（加入要求）メッセージを受信したポートすべてに中継します。

「(1) MAC アドレスの学習 (a) エントリの登録」の例で述べた 224.10.10.10 と 225.10.10.10 のマルチキャスト MAC アドレスはどちらも 0100.5E0A.0A0A となるので，224.10.10.10 宛のマルチキャストデータをレイヤ 2 中継する際に，225.10.10.10 への IGMP Report（加入要求）メッセージを受信したポートへも中継します。

24.3.2 マルチキャストルータとの接続

マルチキャストパケットの中継先にはグループ加入済みホストだけでなく隣接するマルチキャストルータも対象とします。本装置とマルチキャストルータを接続して IGMP snooping を使用する場合，マルチキャストルータへマルチキャストパケットを中継するためにマルチキャストルータと接続するポート（以降，マルチキャストルータポートとします）をコンフィグレーションで指定します。

本装置は指定したマルチキャストルータポートへは全マルチキャストパケットを中継します。

また，IGMP はルータホスト間で送受信するプロトコルであるため，IGMP メッセージはルータおよびホストが受け取ります。本装置は IGMP メッセージを次の表に示すように中継します。

表 24-3 IGMP 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，他装置が代表クエリアの場合の中継動作です。自装置が代表クエリアの場合は，IGMPv2 Leave メッセージは中継しません。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/v2 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。

24.3.3 IGMP クエリア機能

IGMP クエリア機能は，VLAN 内にマルチキャストルータが存在せず，マルチキャストパケットの送信ホストと受信ホストだけが存在する環境で，本装置が IGMP Query メッセージを代理で受信ホストに対して送信する機能です。マルチキャストルータは定期的に IGMP Query メッセージを送信し，ホストからの応答を受け取ることでグループメンバーの存在有無を確認します。マルチキャストルータが存在しない場合，受信ホストからの応答がなくなるためにグループメンバーを監視することができなくなります。この機能によって，VLAN 内にマルチキャストルータが存在しない場合でも，IGMP snooping 機能を使用可能とします。本装置では IGMP Query メッセージを 125 秒間隔で送信します。

IGMP クエリア機能を利用するためには，IGMP snooping 機能を利用する VLAN に IP アドレスを設定する必要があります。

VLAN 内に IGMP Query メッセージを送信する装置が存在する場合，IGMP Query メッセージの送信元 IP アドレスの小さい方が代表クエリアとなって IGMP Query メッセージを送信します。VLAN 内のほかの装置が代表クエリアの場合，本装置は IGMP クエリア機能による Query メッセージの送信を停止します。

代表クエリアが障害などで停止すると新たに代表クエリアを選定します。VLAN 内の他装置が障害などで本装置が代表クエリアに決定すると Query メッセージの送信を開始します。本装置では代表クエリアの監視時間を 255 秒としています。

24.3.4 IGMP 即時離脱機能

IGMP 即時離脱機能は，IGMP2 Leave メッセージを受信した場合に，該当ポートへのマルチキャスト通信をすぐに停止する機能です。

24.4 MLD snooping

ここでは，MLD snooping の機能と動作について説明します。本装置が送受信する MLD メッセージのフォーマットおよび既定値は RFC2710 に従います。また，MLD バージョン 2（以降，MLDv2）メッセージのフォーマットおよび設定値は RFC3810 に従います。

MLD snooping は MAC アドレス制御方式でマルチキャストトラフィックの中継制御を行います。

24.4.1 MAC アドレス制御方式

(1) MAC アドレスの学習

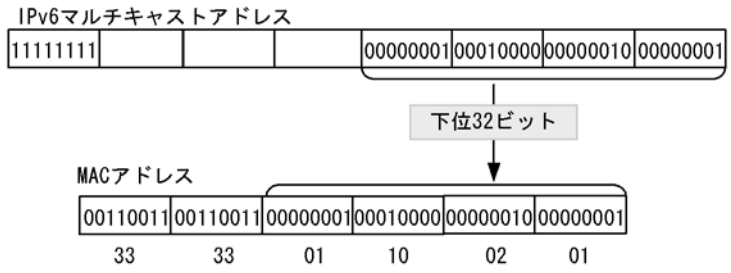
MLD snooping が設定された VLAN で MLD メッセージを受信することによってマルチキャスト MAC アドレスをダイナミックに学習します。学習したマルチキャスト MAC アドレスは MAC アドレステーブルに登録します。

(a) エントリの登録

MLDv1 Report メッセージおよび，MLDv2 Report（加入要求）メッセージを受信すると，メッセージに含まれるマルチキャストグループアドレスからマルチキャスト MAC アドレスを学習し，MLDv1/MLDv2 Report メッセージを受信したポートにだけマルチキャストグループ宛のトラフィックを転送するエントリを作成します。IPv6 マルチキャストデータの宛先 MAC アドレスは IP アドレスの下位 32 ビットを MAC アドレスにコピーして生成します。

IPv6 マルチキャストアドレスはマルチキャストグループを識別するグループ ID フィールドが 112 ビット長のフォーマットと 32 ビット長のフォーマットの 2 種類が規定されています。グループ ID フィールドが 112 ビット長のアドレスフォーマットを使用する場合は，IPv4 マルチキャストアドレスと同様に MAC アドレスの重複が発生します。IPv6 マルチキャストアドレスと MAC アドレスの対応を次の図に示します。

図 24-4 IPv6 マルチキャストアドレスと MAC アドレスの対応



(b) エントリの削除

学習したマルチキャスト MAC アドレスは次のどちらかの場合に，すべてのポートにグループメンバーが存在しなくなった時点で削除されます。

- MLDv1 Done メッセージを受信した場合
  MLDv1 Done メッセージを受信したポートに対して，本装置から Group-Specific Query メッセージを 1 秒間隔で 2 回送信します（Group-Specific Query メッセージの送信は，クエリア設定時だけです。未設定時は代表クエリアから送信されます）。応答がない場合にエントリからこのポートだけを削除します（このポートへのマルチキャストトラフィックの中継を抑止します）。VLAN 内のすべてのポートにグループメンバーが存在しなくなった場合にエントリ自体を削除します。

- MLDv2 Report（離脱要求）メッセージを受信した場合
  MLDv2 Report（離脱要求）メッセージを受信したポートに対して，本装置から Group-Specific Query メッセージを 1 秒間隔で 2 回送信します（Group-Specific Query メッセージの送信は，クエリア設定時だけです。未設定時は代表クエリアから送信されます）。応答がない場合にエントリからこのポートだけを削除します（このポートへのマルチキャストトラフィックの中継を抑止します）。VLAN 内のすべてのポートにグループメンバーが存在しなくなった場合にエントリ自体を削除します。ただし，マルチキャストアドレスレコードタイプが BLOCK_OLD_SOURCES の MLDv2 Report を受信した場合は，自装置へのクエリア設定を行っている場合だけ Group-Specific Query メッセージの送信および，エントリ削除処理を実行します。
- MLDv1/MLDv2 Report（加入要求）メッセージを受信してから一定時間経過した場合
  マルチキャストルータは直接接続するインタフェース上にグループメンバーが存在するかを確認するために，定期的に MLD Query メッセージを送信します。本装置はルータからの MLD Query メッセージを受信した場合，VLAN 内の全ポートに中継します。MLD Query メッセージに対する応答がない場合，エントリからこのポートだけを削除します。すべてのポートから応答がない場合は，エントリ自体を削除します。
  本装置ではエントリを削除するタイムアウト時間を 260 秒（デフォルト値）としています。260 秒間 MLDv1/MLDv2 Report（加入要求）メッセージを受信しない場合に対応するエントリを削除します。

(2) IPv6 マルチキャストパケットのレイヤ 2 中継

IPv6 マルチキャストパケットの受信 VLAN 内のレイヤ 2 中継は IPv4 マルチキャストパケット同様に MAC アドレスベースで処理します。MLD snooping の結果によるレイヤ 2 中継は，同一 MAC アドレスにマッピングされる IPv6 マルチキャストアドレスの MLD Report（加入要求）メッセージを受信したポートすべてに中継します。

24.4.2 マルチキャストルータとの接続

マルチキャストパケットの中継先にはグループ加入済みホストだけでなく隣接するマルチキャストルータも対象とします。本装置とマルチキャストルータを接続して MLD snooping を使用する場合，マルチキャストルータへマルチキャストパケットを中継するためにマルチキャストルータと接続するポート（以降，マルチキャストルータポートとします）をコンフィグレーションで指定します。

本装置は指定したマルチキャストルータポートへは全マルチキャストパケットを中継します。

また，MLD はルータホスト間で送受信するプロトコルであるため，MLD メッセージはルータおよびホストが受け取ります。本装置では MLD メッセージを次の表に示すように中継します。

表 24-4 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，他装置が代表クエリアの場合の中継動作です。自装置が代表クエリアの場合は，MLDv1 Done メッセージは中継しません。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 24-5 MLDv2 メッセージごとの動作

MLDv2 メッセージの種類		VLAN 内転送ポート	備考
Version2 Multicast Listener Query		全ポートへ中継します。	
Version2 Multicast Listener Report	加入要求の Report	マルチキャストルータポートにだけ中継します。	
	離脱要求の Report	ほかのポートにまだグループメンバーが存在する場合はどのポートにも中継しません。ほかのポートにグループメンバーが存在しない場合はマルチキャストルータポートに中継します。	※

注※
自装置にクエリアを設定し，他装置が代表クエリアの場合の中継動作です。自装置が代表クエリアの場合は，MLDv2 Report（離脱要求）メッセージは中継しません。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。

24.4.3 MLD クエリア機能

MLD クエリア機能とは，VLAN 内にマルチキャストルータが存在せず，マルチキャストパケットの送信ホストと受信ホストだけが存在する環境で，本装置が MLD Query メッセージを代理で受信ホストに対して送信する機能です。マルチキャストルータは定期的に MLD Query メッセージを送信し，ホストからの応答を受け取ることでグループメンバーの存在有無を確認します。マルチキャストルータが存在しない場合，受信ホストからの応答がなくなるためにグループメンバーを監視することができなくなります。この機能によって，VLAN 内にマルチキャストルータが存在しない場合でも，MLD snooping 機能を使用可能とします。本装置では Query メッセージを 125 秒間隔で送信します。

MLD クエリア機能を利用するためには，MLD snooping 機能を利用する VLAN に MLD Query メッセージの送信元 IP アドレスを設定する必要があります。

VLAN 内に MLD Query メッセージを送信する装置が存在する場合，MLD Query メッセージの送信元 IP アドレスの小さい方が代表クエリアとなって MLD Query メッセージを送信します。VLAN 内のほかの装置が代表クエリアの場合，本装置は MLD クエリア機能による MLD Query メッセージの送信を停止します。

代表クエリアが障害などで停止すると新たに代表クエリアを選定します。VLAN 内の他装置が障害などで本装置が代表クエリアに決定すると MLD Query メッセージの送信を開始します。本装置では代表クエリアの監視時間を 255 秒としています。

本装置で送信する MLD Query のバージョンは，MLDv1 をデフォルト値としています。装置起動以降，MLD Query のバージョンは，代表クエリアの MLD バージョンに従います。

24.5 IGMP snooping/MLD snooping 使用時の注意事項

(1) 他機能との共存

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

(2) 制御パケットのフラッディング

IGMP snooping/MLD snooping が抑止対象とするマルチキャストトラフィックはデータトラフィックであり，ルーティングプロトコルなどの制御パケットは VLAN 内の全ルータや全ホストが受信できるように VLAN 内に flooding する必要があります。そのため，本装置では，次の表に示すアドレス範囲に含まれる宛先 IP アドレスを持つパケットは，VLAN 内の全ポートに中継します。次の表に示すアドレス範囲外の宛先 IP アドレスを持つパケットは，マルチキャスト MAC アドレスの学習結果に従って中継します。

表 24-6 制御パケットのフラッディング

プロトコル	アドレス範囲
IGMP snooping	224.0.0.0 ～ 224.0.0.255
MLD snooping	ff02::/16

ただし，制御パケットのマルチキャスト MAC アドレスと重複するマルチキャストグループアドレスは使用できません。上の表に示したアドレス範囲以外のアドレスで，使用できないマルチキャストグループアドレスを次の表に示します。

表 24-7 MAC アドレス制御方式で使用できないマルチキャストグループアドレス

プロトコル	マルチキャストグループアドレス
IGMP snooping	224.128.0.0/24
	225.0.0.0/24
	225.128.0.0/24
	226.0.0.0/24
	226.128.0.0/24
	227.0.0.0/24
	227.128.0.0/24
	228.0.0.0/24
	228.128.0.0/24
	229.0.0.0/24
	229.128.0.0/24
	230.0.0.0/24
	230.128.0.0/24
	231.0.0.0/24
	231.128.0.0/24
	232.0.0.0/24
	232.128.0.0/24
	233.0.0.0/24
	233.128.0.0/24

プロトコル	マルチキャストグループアドレス
	234.0.0.0/24
	234.128.0.0/24
	235.0.0.0/24
	235.128.0.0/24
	236.0.0.0/24
	236.128.0.0/24
	237.0.0.0/24
	237.128.0.0/24
	238.0.0.0/24
	238.128.0.0/24
	239.0.0.0/24
	239.128.0.0/24

上の表に示したアドレスをマルチキャストグループアドレスに使用した場合，該当マルチキャストグループアドレス宛てのマルチキャストデータは，VLAN 内の全ポートに中継します。

トランクポートを設定している場合は，Untagged 制御パケットを受信しないように注意してください。構成上，トランクポートで Untagged 制御パケットを扱う場合は，ネイティブ VLAN を設定してください。

(3) マルチキャストルータポートの設定

(a) 冗長構成時

スパニングツリーによって冗長構成を採り，スパニングツリーによってトポロジー変更でルータとの接続が変わる可能性がある場合は，ルータと接続する可能性のある全ポートに対してマルチキャストルータポートの設定をしておく必要があります。

(b) レイヤ 2 スイッチ間の接続時

複数のレイヤ 2 スイッチだけで構成される VLAN で，マルチキャストトラフィックの送信ホストを収容するレイヤ 2 スイッチと接続するポートをマルチキャストルータポートに設定しておく必要があります。また，このような構成の場合，各レイヤ 2 スイッチで IGMP/MLD snooping 機能を有効にしてください（snooping 対応のスイッチと接続してください）。

冗長構成を採る場合は，送信ホストを収容するレイヤ 2 スイッチと接続する可能性のある全ポートに対してマルチキャストルータポートの設定をしておく必要があります。

(4) IGMP バージョン 3 ホストとの接続

本装置は IGMP バージョン 3(以降，IGMPv3 とします) をサポートしません。IGMP snooping 機能を動作させた場合，IGMPv3 のグループ加入要求は認識しないためデータパケットが中継されなくなります。IGMPv3 ホストを接続する場合は，IGMP snooping 機能を停止してください。

(5) MLD バージョン 2 ホストとの接続

本装置に MLDv2 ホストを接続する場合，必ず MLDv2 ルータを接続して該当するルータが代表クエリアになるように IP アドレスを設定してください。代表クエリアが MLDv1 ルータの場合，ネットワークが

MLDv1 モードになります。

また，MLDv2 ホストからの MLDv2 メッセージがフラグメント化されない構成で運用してください。

（6） IGMP 即時離脱機能

IGMP 即時離脱機能を使用した場合，IGMPv2 Leave メッセージを受信すると，該当ポートへのマルチキャスト通信をすぐに停止します。このため，本機能を使用する場合は，接続ポートに各マルチキャストグループの受信者の端末を 1 台だけ設置することを推奨します。

接続ポートに同一マルチキャストグループの受信者の端末を複数台設置した場合は，一時的にほかの受信者へのマルチキャスト通信が停止します。この場合，受信者からの IGMP Report（加入要求）メッセージを再度受信することで，マルチキャスト通信は再開します。

25 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。

25.1 IGMP snooping のコンフィグレーション

25.2 IGMP snooping のオペレーション

25.3 MLD snooping のコンフィグレーション

25.4 MLD snooping のオペレーション

25.1 IGMP snooping のコンフィグレーション

25.1.1 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 25-1 コンフィグレーションコマンド一覧

コマンド名	説明
ip igmp snooping (global)	no ip igmp snooping 設定時，本装置の IGMP snooping 機能を抑止します。
ip igmp snooping (interface)	指定したインタフェースの IGMP snooping 機能を設定します。
ip igmp snooping fast-leave	IGMP 即時離脱機能を設定します。
ip igmp snooping mrouter	IGMP マルチキャストルータポートを設定します。
ip igmp snooping querier	IGMP クエリア機能を設定します。

25.1.2 IGMP snooping の設定

[設定のポイント]

IGMP snooping を動作させるには，使用する VLAN の VLAN インタフェースコンフィグレーションモードで，次の設定を行います。

VLAN2 に IGMP snooping 機能を有効にする場合を示します。

[コマンドによる設定]

1.
```
(config)# interface vlan 2
(config-if)# ip igmp snooping
(config-if)# exit
```
VLAN2 の VLAN インタフェースコンフィグレーションモードに移行して，IGMP snooping 機能を有効にします。

25.1.3 IGMP クエリア機能の設定

[設定のポイント]

IGMP snooping を設定した VLAN 内にマルチキャストルータが存在しない場合，IGMP クエリア機能を動作させる必要があります。該当 VLAN の VLAN インタフェースコンフィグレーションモードで次の設定を行います。

[コマンドによる設定]

1.
```
(config)# interface vlan 2
(config-if)# ip igmp snooping querier
(config-if)# exit
```
IGMP クエリア機能を有効にします。

[注意事項]

本設定は該当インタフェースに IPv4 アドレスの設定がないと有効になりません。

25.1.4 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 のイーサネットインタフェースにマルチキャストルータを接続している場合を示します。

[コマンドによる設定]

1. **(config)# interface vlan 2**
   (config-if)# ip igmp snooping mrouter interface fastethernet 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。

[注意事項]

ポートチャネルインタフェースに属するポート番号を，マルチキャストルータポートに設定しても動作しません。

25.2 IGMP snooping のオペレーション

25.2.1 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 25-2 運用コマンド一覧

コマンド名	説明
show igmp-snooping	IGMP snooping 情報を表示します。
clear igmp-snooping	IGMP snooping の全情報をクリアします。

25.2.2 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) IGMP snooping 設定状態の確認

運用コマンド show igmp-snooping で，IGMP snooping に関する設定が正しいことを確認してください。

図 25-1 IGMP snooping の設定状態表示

```
> show igmp-snooping

Date 20XX/03/14 15:56:12 UTC
VLAN counts: 3
VLAN 3253:
  IP Address: 192.168.53.100/24 Querier: enable
  IGMP querying system: 192.168.53.100
  Fast-leave : On
  Port (4): 0/13-16
  Mrouter-port: 0/13-16
  Group counts: 5
VLAN 3254:
  IP Address: 192.168.54.100/24 Querier: disable
  IGMP querying system:
  Fast-leave : Off
  Port (4): 0/17-20
  Mrouter-port: 0/17-20
  Group counts: 5
VLAN 3255:
  IP Address: 192.168.55.100/24 Querier: disable
  IGMP querying system:
  Fast-leave : Off
  Port (4): 0/21-24
  Mrouter-port: 0/21-24
  Group counts: 5

>
```

(2) 運用中の確認

次のコマンドで，IGMP snooping の運用中の状態を確認してください。

- 学習した MAC アドレス，VLAN 内に中継される IPv4 マルチキャストアドレスとその中継先ポートリストの状態は，運用コマンド show igmp-snooping group で確認してください。

図 25-2 show igmp-snooping group の実行結果

```
> show igmp-snooping group

Date 20XX/11/14 15:59:41 UTC
Total Groups: 15
VLAN counts: 3
VLAN 3253 Group counts: 5
  Group Address     MAC Address
   230.0.0.11        0100.5e00.000b
     Port-list: 0/13
   230.0.0.10        0100.5e00.000a
     Port-list: 0/13
   230.0.0.14        0100.5e00.000e
     Port-list: 0/13
   230.0.0.13        0100.5e00.000d
     Port-list: 0/13
   230.0.0.12        0100.5e00.000c
     Port-list: 0/13
VLAN 3254 Group counts: 5
  Group Address     MAC Address
   230.0.0.34        0100.5e00.0022
     Port-list: 0/18
   230.0.0.33        0100.5e00.0021
     Port-list: 0/18
   230.0.0.32        0100.5e00.0020
     Port-list: 0/18
   230.0.0.31        0100.5e00.001f
     Port-list: 0/18
   230.0.0.30        0100.5e00.001e
     Port-list: 0/18
VLAN 3255 Group counts: 5
  Group Address     MAC Address
   230.0.0.24        0100.5e00.0018
     Port-list: 0/21
   230.0.0.23        0100.5e00.0017
     Port-list: 0/21
   230.0.0.22        0100.5e00.0016
     Port-list: 0/21
   230.0.0.21        0100.5e00.0015
     Port-list: 0/21
   230.0.0.20        0100.5e00.0014
     Port-list: 0/21

>
```

● ポートごとの参加グループ表示例を運用コマンド show igmp-snooping port で確認してください。

図 25-3 show igmp-snooping port の実行結果

```
> show igmp-snooping port 0/13

Date 20XX/11/14 16:03:28 UTC
Port 0/13  VLAN counts: 1
  VLAN 3253 Group counts: 5
    Group Address     Last Reporter      Uptime     Expires
     230.0.0.11        192.168.53.17      19:20      04:19
     230.0.0.10        192.168.53.16      19:20      04:20
     230.0.0.14        192.168.53.20      19:20      04:19
     230.0.0.13        192.168.53.19      19:20      04:19
     230.0.0.12        192.168.53.18      19:20      04:19

>
```

25.3 MLD snooping のコンフィグレーション

25.3.1 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 25-3 コンフィグレーションコマンド一覧

コマンド名	説明
ipv6 mld snooping (global)	no ipv6 mld snooping 設定時，本装置の MLD snooping 機能を抑止します。
ipv6 mld snooping (interface)	指定したインタフェースの MLD snooping 機能を設定します。
ipv6 mld snooping mrouter	MLD マルチキャストルータポートを設定します。
ipv6 mld snooping querier	MLD クエリア機能を設定します。
ipv6 mld snooping source	本装置から送信される MLD Query メッセージの送信元 IP アドレスを設定します。

25.3.2 MLD snooping の設定

[設定のポイント]

MLD snooping を動作させるには，使用する VLAN の VLAN インタフェースのインタフェースコンフィグレーションモードで，次の設定を行います。例として，VLAN2 に MLD snooping 機能を有効にする場合を示します。

[コマンドによる設定]

1. **(config)# interface vlan 2**
   (config-if)# ipv6 mld snooping
   (config-if)# exit
   VLAN2 の VLAN インタフェースコンフィグレーションモードに移行して，MLD snooping 機能を有効にします。

25.3.3 MLD クエリア機能の設定

[設定のポイント]

MLD snooping を設定した VLAN 内にマルチキャストルータが存在しない場合，MLD クエリア機能を動作させる必要があります。該当 VLAN の VLAN インタフェースコンフィグレーションモードで，次の設定を行います。

[コマンドによる設定]

1. **(config)# interface vlan 2**
   (config-if)# ipv6 mld snooping querier
   (config-if)# exit
   MLD クエリア機能を有効にします。

[注意事項]

本設定は該当インタフェースに，MLD Query メッセージの送信元 IP アドレスの設定がないと有効になりません。

25.3.4 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 のイーサネットインタフェースにマルチキャストルータを接続している場合を示します。

[コマンドによる設定]

1. **(config)# interface vlan 2**
   (config-if)# ipv6 mld snooping mrouter interface fastethernet 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。

[注意事項]

ポートチャネルインタフェースに属するポート番号を，マルチキャストルータポートに設定しても動作しません。

25.3.5 MLD Query メッセージ送信元 IP アドレスの設定

[設定のポイント]

MLD クエリア機能を使用する際に，本装置から送信される Query メッセージの送信元 IP アドレスを指定する必要があります。MLD クエリア機能を使用する VLAN の VLAN インタフェースコンフィグレーションモードで，次の設定を行います。

[コマンドによる設定]

1. **(config)# interface vlan 2**
   (config-if)# ipv6 mld snooping source fe80::1
   (config-if)# exit
   該当インタフェースの MLD Query メッセージの送信元 IP アドレスを fe80::1 に指定します。

[注意事項]

1. MLD Query メッセージの送信元 IP アドレスにだけ適用されます。
2. 送信元アドレスは，IPv6 リンクローカルアドレスを設定してください。

25.4 MLD snooping のオペレーション

25.4.1 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 25-4 運用コマンド一覧

コマンド名	説明
show mld-snooping	MLD snooping 情報を表示します。
clear mld-snooping	MLD snooping の全情報をクリアします。

25.4.2 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) MLD snooping 設定状態の確認

運用コマンド show mld-snooping を実行し，MLD snooping に関する設定が正しいことを確認してください。

図 25-4 MLD snooping の設定状態表示

```
> show mld-snooping

Date 20XX/11/14 17:21:37 UTC
VLAN counts: 3
VLAN 3001:
  IP Address:   Querier: enable
  MLD querying system:
  Querier version: v1
  Port (1): 0/12
  Mrouter-port: 0/12
  Group counts: 1
VLAN 3002:
  IP Address:   Querier: enable
  MLD querying system:
  Querier version: v1
  Port (1): 0/12
  Mrouter-port: 0/12
  Group counts: 1
VLAN 3003:
  IP Address:   Querier: enable
  MLD querying system:
  Querier version: v1
  Port (1): 0/12
  Mrouter-port: 0/12
  Group counts: 1

>
```

(2) 運用中の確認

以下のコマンドで，MLD snooping の運用中の状態を確認してください。

- 学習した MAC アドレス，VLAN 内に中継される IPv6 マルチキャストアドレスとその中継先ポートリストの状態は，運用コマンド show mld-snooping group で確認してください。

図 25-5 show mld-snooping group の実行結果

```
> show mld-snooping group

Date 20XX/11/14 17:22:05 UTC
Total Groups: 3
VLAN counts: 3
VLAN 3001 Group counts: 1
  Group Address                          MAC Address      Version   Mode
   ff80:0:0:0:0:0:99:a0a                 3333.0099.0a0a   v1        -
     Port-list: 0/12
VLAN 3002 Group counts: 1
  Group Address                          MAC Address      Version   Mode
   ff80:0:0:0:0:0:99:a0a                 3333.0099.0a0a   v1        -
     Port-list: 0/12
VLAN 3003 Group counts: 1
  Group Address                          MAC Address      Version   Mode
   ff80:0:0:0:0:0:99:a0a                 3333.0099.0a0a   v1        -
     Port-list: 0/12

>
```

● ポートごとの参加グループ表示例を運用コマンド show mld-snooping port で確認してください。

図 25-6 show mld-snooping port の実行結果

```
> show mld-snooping port 0/12

Date 20XX/11/14 17:22:45 UTC
Port 0/12  VLAN counts: 3
  VLAN 3001 Group counts: 1
    Group Address              Last Reporter              Uptime    Expires
    ff80:0:0:0:0:0:99:a0a      fe:80:0:0:0:0:0:fe00       07:10     04:20
  VLAN 3002 Group counts: 1
    Group Address              Last Reporter              Uptime    Expires
    ff80:0:0:0:0:0:99:a0a      fe:80:0:0:0:0:0:fe00       05:02     04:20
  VLAN 3003 Group counts: 1
    Group Address              Last Reporter              Uptime    Expires
    ff80:0:0:0:0:0:99:a0a      fe:80:0:0:0:0:0:fe00       05:02     04:20

>
```

付録

付録 A　準拠規格

付録 A　準拠規格

付録 A.1　TELNET/FTP

表 A-1　TELNET/FTP の準拠する規格および勧告

規格番号 (発行年月)	規格名
RFC 854 (1983 年 5 月)	TELNET PROTOCOL SPECIFICATION
RFC 855 (1983 年 5 月)	TELNET OPTION SPECIFICATIONS
RFC 959 (1985 年 10 月)	FILE TRANSFER PROTOCOL (FTP)

付録 A.2　RADIUS

表 A-2　RADIUS の準拠する規格および勧告

規格番号 (発行年月)	規格名
RFC2865(2000 年 6 月)	Remote Authentication Dial In User Service(RADIUS)

付録 A.3　NTP

表 A-3　NTP の準拠する規格および勧告

規格番号 (発行年月)	規格名
RFC2030(1996 年 10 月)	Simple Network Time Protocol (SNTP) Version4 for IPv4, IPv6 and OSI

付録 A.4　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, 100BASE-FX, 1000BASE-T, 1000BASE-X	IEEE802.2 1998 Edition	IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements - Part 2: Logical Link Control
	IEEE802.3 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
PoE	IEEE802.3af IEEE802.3at/D3.1	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
draft-ietf-magma-snoop-12.txt (2005 年 8 月)	IGMP and MLD snooping switches

付録 A.9　IPv4 インタフェース

表 A-9　IP バージョン 4 の準拠規格および勧告

規格番号 (発行年月)	規格名
RFC791(1981 年 9 月)	Internet Protocol
RFC792(1981 年 9 月)	Internet Control Message Protocol
RFC826(1982 年 11 月)	An Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware

規格番号 (発行年月)	規格名
RFC922(1984 年 10 月)	Broadcasting Internet datagrams in the presence of subnets
RFC950(1985 年 8 月)	Internet Standard Subnetting Procedure
RFC1027(1987 年 10 月)	Using ARP to implement transparent subnet gateways
RFC1122(1989 年 10 月)	Requirements for Internet hosts-communication layers

索引

数字

1000BASE-BX の SFP 挿入時の注意事項 183
1000BASE-SX2 での自動メディア検出動作および制限事項 183
1000BASE-X 接続時の注意事項 182
1000BASE-X 接続仕様 178
100BASE-FX 使用後の注意事項 182
100BASE-FX 接続仕様 177
100BASE-FX の SFP 挿入時の注意事項 182
10BASE-T/100BASE-TX 自動認識 160
10BASE-T/100BASE-TX 接続時の注意事項 164
10BASE-T/100BASE-TX 接続仕様 160
10BASE-T/100BASE-TX/1000BASE-T 自動認識 167
10BASE-T/100BASE-TX/1000BASE-T 接続時の注意事項 173
10BASE-T/100BASE-TX/1000BASE-T 接続仕様 167

G

Gigabitethernet ポートの拡張省電力機能 130

I

IGMP snooping 389
IGMP snooping/MLD snooping 概要 387
IGMP snooping/MLD snooping 使用時の注意事項 395
IGMP snooping/MLD snooping の解説 385
IGMP snooping/MLD snooping の概要 386
IGMP snooping/MLD snooping の設定と運用 399
IGMP snooping および MLD snooping 概要 387
IGMP snooping の運用コマンド一覧 402
IGMP snooping のコンフィグレーションコマンド一覧 400
IGMP クエリア機能〔IGMP snooping〕391
IGMP メッセージごとの動作 390
IPv4 マルチキャストアドレスと MAC アドレスの対応 389
IPv4 マルチキャストパケットのレイヤ 2 中継〔IGMP snooping〕390
IPv6 マルチキャストアドレスと MAC アドレスの対応 392
IPv6 マルチキャストパケットのレイヤ 2 中継〔MLD snooping〕393
IP アドレスの設定〔本装置〕73

L

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 271
LLC 副層フレームフォーマット 151

M

MAC VLAN のコンフィグレーションコマンド一覧 258
MAC アドレス学習 223
MAC アドレス学習の運用コマンド一覧 230
MAC アドレス学習のコンフィグレーションコマンド一覧 228
MAC アドレス制御方式〔IGMP snooping〕389
MAC アドレス制御方式〔MLD snooping〕392
MAC アドレスの学習〔IGMP snooping〕389
MAC アドレスの学習〔MLD snooping〕392
MAC 副層フレームフォーマット 151
MC 運用モード機能 117
MC 運用モード機能の運用コマンド一覧 122
MC 運用モード機能のコンフィグレーションコマンド一覧 121
MDI/MDI-X のピンマッピング〔10BASE-T/100BASE-TX〕163
MDI/MDI-X のピンマッピング 〔10BASE-T/100BASE-TX/1000BASE-T〕171
MLD snooping 392
MLD snooping の運用コマンド一覧 406
MLD snoopingのコンフィグレーションコマンド一覧 404
MLDv1 メッセージごとの動作 393
MLDv2 メッセージごとの動作 394
MLD クエリア機能〔MLD snooping〕394

P

PoE 186
PoE の運用コマンド一覧 199
PoE のコンフィグレーションコマンド一覧 196
PVST+ の運用コマンド一覧 299
PVST+ のコンフィグレーションコマンド一覧 294

R

RADIUS 82
RADIUS サーバグループ情報 87
RADIUS に関する運用コマンド一覧 92

RADIUS に関するコンフィグレーションコマンド一覧 89
RADIUS の解説 82
RADIUS の概要 82
RADIUS のサポート範囲 83
RADIUS の適用機能および範囲 82
Ring Protocol とスパニングツリー /GSRP の併用 379
Ring Protocol の運用コマンド一覧 377
Ring Protocol の解説 333
Ring Protocol のコンフィグレーションコマンド一覧 368
Ring Protocol の設定と運用 367

S

SFP 自動認識機能 (メディアタイプの選択) 〔100BASE-FX/1000BASE-X〕 182
SFP 自動認識機能 (メディアタイプの選択) 〔10BASE-T/100BASE-TX/1000BASE-T〕 173

T

TYPE/LENGTH フィールドの扱い 151

V

VLAN 233
VLAN 拡張機能 269
VLAN 拡張機能の運用コマンド一覧 276
VLAN 基本機能のコンフィグレーションコマンド一覧 240
VLAN の運用コマンド一覧 264
VLAN マッピング 362

い

イーサネット 149
イーサネット共通の運用コマンド一覧 159
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 154

う

運用端末の条件 38
運用端末の接続形態 38
運用端末の接続形態ごとの特徴 39
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 75
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 73

お

オートネゴシエーション〔1000BASE-X〕 179
オートネゴシエーション〔10BASE-T/100BASE-TX〕 161
オートネゴシエーション〔10BASE-T/100BASE-TX/1000BASE-T〕 168

き

強制スリープ解除 131

こ

コマンド操作 45
コマンド入力モードの切り換えに関する運用コマンド一覧 46
コンソール 38
コンフィグレーション 57
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 61
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 61

さ

サポート機能〔IGMP snooping/MLD snooping〕 388

し

時刻設定および NTP に関する運用コマンド一覧 100
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 99
時刻の設定と NTP 95
システムファンクションリソースを使用する機能 106
自動 MDIX 機能〔10BASE-T/100BASE-TX〕 163
自動 MDIX 機能〔10BASE-T/100BASE-TX/1000BASE-T〕 171
自動復旧停止状態について 113
ジャンボフレーム〔100BASE-FX/1000BASE-X〕 181
ジャンボフレーム〔10BASE-T/100BASE-TX〕 163
ジャンボフレーム〔10BASE-T/100BASE-TX/1000BASE-T〕 172
ジャンボフレームサポート機能 〔100BASE-FX/1000BASE-X〕 182
ジャンボフレームサポート機能 〔10BASE-T/100BASE-TX〕 164
ジャンボフレームサポート機能 〔10BASE-T/100BASE-TX/1000BASE-T〕 172
収容条件 19

受信フレームの廃棄条件 152
省電力機能 123
省電力機能の運用コマンド一覧 143
省電力機能のコンフィグレーションコマンド一覧 139
シングルスパニングツリーの運用コマンド一覧 307
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 302

す

スケジュール時間帯 124
スパニングツリー 279
スパニングツリー共通機能の運用コマンド一覧 331
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 327
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 288

せ

接続インタフェース：1000BASE-X 177
接続インタフェース：100BASE-FX 177
接続インタフェース：10BASE-T/100BASE-TX 160
接続インタフェース：10BASE-T/100BASE-TX/1000BASE-T 167

そ

装置管理者モード移行のパスワードの設定 79
装置構成 7
装置の管理 101
装置へのログイン 37
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 102
ソフトウェア管理に関する運用コマンド一覧 146
ソフトウェアの管理 145

た

ダウンシフト機能 172
多重障害監視 VLAN 356
多重障害監視機能 354
多重障害監視フレーム 356

つ

通常時間帯 124

て

伝送速度，全二重 / 半二重モードごとの接続仕様〔1000BASE-X〕179
伝送速度，全二重 / 半二重モードごとの接続仕様〔100BASE-FX〕177
伝送速度，全二重 / 半二重モードごとの接続仕様〔10BASE-T/100BASE-TX〕160
伝送速度，全二重 / 半二重モードごとの接続仕様〔10BASE-T/100BASE-TX/1000BASE-T〕168

と

同時にログインできるユーザ数の設定 80

に

認証方式シーケンス（end-by-reject 設定時） 86
認証方式シーケンス（end-by-reject 未設定時） 85

は

バックアップ・リストアに使用する運用コマンド一覧 107
バックアップリング 354
パッドの扱い 152

ふ

フレームフォーマット〔MAC/LLC 副層制御〕151
フローコントロール〔100BASE-FX/1000BASE-X〕179
フローコントロール〔10BASE-T/100BASE-TX〕161
フローコントロール〔10BASE-T/100BASE-TX/1000BASE-T〕169
フローコントロールの受信動作〔100BASE-FX/1000BASE-X〕180
フローコントロールの受信動作〔10BASE-T/100BASE-TX〕162
フローコントロールの受信動作〔10BASE-T/100BASE-TX/1000BASE-T〕169
フローコントロールの送信動作〔100BASE-FX/1000BASE-X〕180
フローコントロールの送信動作〔10BASE-T/100BASE-TX〕162
フローコントロールの送信動作〔10BASE-T/100BASE-TX/1000BASE-T〕169
プロトコル VLAN のコンフィグレーションコマンド一覧 250

ほ

ポート VLAN のコンフィグレーションコマンド一覧 245
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 274

ポート閉塞〔省電力機能〕 131
本装置の概要 1

ま

マルチキャストグループアドレス 386
マルチキャストルータとの接続〔IGMP snooping〕 390
マルチキャストルータとの接続〔MLD snooping〕 393
マルチプルスパニングツリーの運用コマンド一覧 320
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 314

め

メディアタイプの設定〔100BASE-FX/1000BASE-X〕 185
メディアタイプの設定〔10BASE-T/100BASE-TX/1000BASE-T〕 175

り

リモート運用端末 39
リモート運用端末からのログインの制限 80
リモート運用端末から本装置へのログイン 71
リモート運用端末と本装置との通信の確認 75
リンクアグリゲーション 201
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 213
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 205
リンクアグリゲーションの運用コマンド一覧 214
リンクダウンポートの省電力機能 130

れ

レイヤ 2 スイッチ概説 217

ろ

ログイン制御の概要 78
ログインセキュリティと RADIUS 77
ログインセキュリティに関する運用コマンド一覧 78
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 78
ログインユーザの変更 79